

SIAS 2018

10-12 October / Nancy / France

PROCEEDINGS

Scientific committee

Jean-Christophe Blaise	Institut National de Recherche et de Sécurité (INRS) – France
Thomas Boemer	Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA) – Germany
Yuvn Chinniah	Polytechnique Montréal – Canada
Marek Dzwiarek	Central Institute for Labour Protection – National Research Institute (CIOP-PIB) – Poland
Toshihiro Fujita	The Institute of Global Safety Promotion (IGSAP) – Japan
Laurent Giraud	Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST) – Canada
Nicholas Hall	Health and Safety Executive (HSE) – United Kingdom
Sandrine Hardy	Institut National de Recherche et de Sécurité (INRS) – France
Hiroyasu Ikeda	National Institute of Occupational Safety and Health (JNIOSH) – Japan
Timo Malm	Technical Research Centre of Finland (VTT) – Finland



Wednesday, October 10th 2018

Session 1 – Functional safety - Information Technology

Chairpersons: *HARDY Sandrine, France; IKEDA Hiroyasu, Japan*

Foresight of new and emerging occupational safety and health risks associated with information and communications technologies, <i>Stacey N.</i>	6
How to consider security aspects during the design of machinery, <i>Mysliwiec B.</i>	13
Analysis of Markov Models for Safety-related Systems in Security Environments, <i>Schiller F.</i>	24
An extensive method to analyze impacts of cyber-security on major hazards, <i>Massé F.</i>	32

Session 2-1 – Safety of Collaborative Systems

Chairpersons: *FUJITA Toshihiro, Japan; CHINNIAH Yuvin, Canada*

Human-robot coactivity: need's analysis, <i>Tihay D.</i>	40
Of the necessity of a uniform measurement procedure for the determination if the threshold values listed in ISO TS 15066, <i>Pilz T.</i>	48
Object Recognition for Safety Applications using Ultrasonic Holography, <i>Kirfel A.</i>	49
Reliable Planning of Human-Robot-Collaboration featuring Speed and Separation Monitoring, <i>Petersen H.</i>	55
Industrial collaborative robot application: experimental implementation of safety-rated monitored stop, <i>Sghaier A.</i>	62

Session 2-2 – Safety of Collaborative Systems

Chairpersons: *MALM Timo, Finland; GIRAUD Laurent, Canada*

Advancing Anticipatory Behaviors in Dyadic Human-Robot Collaboration: The AnDy project, <i>Maurice P.</i>	70
COVR - Towards simplified evaluation and validation of collaborative robotics applications across a wide range of domains using robot safety skills, <i>Saenz J.</i>	71
Japan's approach for the realization of Future Safety Concept by implementing collaborative safety technologies, <i>Mukaidono M.</i>	77
New collaborative safety concept in various coexistence areas for human and machinery, <i>Shimizu T.</i>	88

Thursday, October 11th 2018q

Session 3 – Autonomous systems

Chairpersons: *BOEMER Thomas, Germany; GIRAUD Laurent, Canada*

Top-Down approach for safety engineering in autonomous and semi-autonomous machinery systems, <i>Tiusanen R.</i>	96
Safety concepts for autonomous and semi-autonomous mobile work machines, <i>Malm T.</i>	103
Autonomous Driving within the Plant Functional Safety between Industrial Automation and Automotive Engineering, <i>Borowski T.</i>	109
A methodological framework to support the design of safe & secure autonomous systems, <i>Heikkilä E.</i>	110



Session 4 – Protective devices and smart systems

Chairpersons: *HALL Nicholas, United Kingdom; HARDY Sandrine, France*

Use of tablet PCs and smartphones for machine control, <i>Nischalke-Fehn G.</i>	117
General principles of smart personal protection systems design, <i>Marchal P.</i>	122
Safety related sensors used for protection of person, <i>Wüstefeld M.</i>	129
Future prospects of enabling device as an essential safety device for the safety of machinery and Safety2.0, <i>Nobuhiro M.</i>	130

Session 5 – Safety of machinery

Chairpersons: *BLAISE Jean-Christophe, France; FUJITA Toshihiro, Japan*

Challenges during risk assessment of large intelligent logistic storage system, <i>Hongbin L.</i>	140
Impact of changes in machinery during use : towards a prognostic of hazardous situations?, <i>Lamy P.</i>	147
A study on safety requirements for brake systems of the mechanical servo presses, <i>Hata Y.</i>	153
Revision of ISO 13855, <i>Görnemann O.</i>	160

Friday, October 12th 2018

Session 6 – Experiences / Practical applications

Chairpersons: *IKEDA Hiroyasu, Japan; BLAISE Jean-Christophe, France*

Serious and fatal accidents caused by mobile machinery in Quebec: More prevention is needed, <i>Burlet-Vienney D.</i>	173
Safety Assessor Qualification Impact and Influence in Thailand, <i>Patiphon K.</i>	179
Framework for Occupational Safety and Health: the eSocial, <i>Kieckbusch R.-E.</i>	185
Analysis of 139 serious and fatal machine accidents occurring in Quebec between 2011 and 2015, <i>Giraud L.</i>	191

Session 7 – Experiences / Prospects

Chairpersons: *CHINNIAH Yuvin, Canada; BOEMER Thomas, Germany*

The Safeguarding Supportive System (SSS) IV. Experimental procedure of behavior analysis to the Safeguarding Supportive System (SSS) as a safety management approach. For appropriate prediction and control of human behavior, <i>Hojo R.</i>	198
Development of Human Resources in Safety in the Fourth Industrial Revolution Period: Current Status of Safety Assessor Qualification System and the Future Development Prospect in the Fields of Robotics, Corporate Management, and Collaborative Safety, <i>Fujita T.</i>	203
Objective and Subjective Effects of Passive Exoskeleton on Overhead Work, <i>Maurice P.</i>	213

Poster session

Practical solutions for safety-related application programming, <i>Huelke M.</i>	217
The Safeguarding Supportive System (SSS) I. Study on Worker's Three-dimensional Location Detection Using Ultra-Wide Band (UWB) System under the SSS, <i>Shimizu S.</i>	223
Safeguarding Supportive System III. The new approach using ICT in IoT ear on safety management from information communication to prediction and control of human behavior, <i>Hamajima K.</i>	228
Prototype Making of a Fail-Safe Interlock System for Pneumatic Control Systems, <i>Nakamura M.</i>	230
A fundamental safety system for machine operators, <i>Otsuka K.</i>	236

Radio Wave Sensor System Which Enables Determination of Protective Separation Distance, <i>Kim E.</i>	240
The Safeguarding Supportive System (SSS) II. Study on the reliability of the Safeguarding Supportive System (SSS) in work site of the Integrated Manufacturing System (IMS) introducing a mobile robot, <i>Matsui K.</i>	245
Evaluation of Residual Risk under Risk Reduction Rules for Using Collaborative Robots, <i>Ikedo H.</i>	249
Probabilistic Risk Analysis of Human-Robot Collaboration Using the Interference Theory, <i>Kirschner R.-J.</i>	254
Work equipments' safe design: two complementary tools to take into account real working situations' variability, <i>Daille-Lefèvre B.</i>	259
An experimental evaluation of falling down damage using forearm mimics, <i>Okabe K.</i>	267
Investigation of evaluation method for bending strength of artificial bones simulated a woman's upper-limb bones by using Finite Element Analysis, <i>Yamaguchi A.</i>	272
Analysis of machinery accidents in the food processing industry during the cleaning and Disinfection phases, <i>Giraud L.</i>	277
Safety functions in pneumatic drive technology, <i>Uppenkamp J.</i>	283
A proposal to solve technical issues on ISO 13855 - Positioning of safeguards, <i>Saito T.</i>	291
Online Human Activity Recognition for Ergonomics Assessment, <i>Malaisé A.</i>	297
Assessing and improving human movements using sensitivity analysis and digital human simulation, <i>Maurice P.</i>	299
Implementation, risk assessment and safety human/robot interaction of collaborative robot UR10, <i>Menges B.</i>	300
Challenges of measuring physiological parameters as indicators of cognitive load in the context of human-machine interfaces, <i>Nowak K.</i>	301
Development of a VR based qualification module in trainings on risk assessments according to the EU Directive on Safety of Machinery, <i>Gomoll K.</i>	306
Conducting risk assessments early on serves multiple purposes, <i>Nickel P.</i>	312
Practical application and experience: Tool for the safety of industrial machinery in reduced risk conditions, <i>Aucourt B.</i>	318
Normative surveillance for Occupational Safety and Health, <i>Kieckbusch R.-E.</i>	323
A simulation based approach for work system compatibility assessment using time allowances, <i>El Mouayni I.</i>	324



Session 1

Functional safety – Information Technology

Foresight of new and emerging occupational safety and health risks associated with information and communications technologies

Stacey N.¹, Bradbrook S. D.¹, Ellwood P. A.¹, Reynolds J.², Williams A. H.², Ravetz J.², Lye D W. F.², Brun E.³, Starren A.³, Palmer K.³

¹ Health and Safety Executive Foresight Centre – Harpur Hill – Buxton – SK17 9JN – UK

² SAMI Consulting Ltd. – The Rectory – 1 Toomers' Wharf – Canal Walk – Newbury – RG14 1DY – UK

³ European Agency for Safety and Health at Work – Santiago de Compostela 12 – 48003 Bilbao – Spain

nicola.stacey@hsl.gsi.gov.uk
john.reynolds@samiconsulting.co.uk
brun@osha.europa.eu

KEYWORDS: emergence of new technologies, industries of the future, artificial intelligence, occupational risk

ABSTRACT

Information and communications technologies (ICT) and work location were identified during a consultation exercise (in 2014) across Europe as the topics most likely to have the greatest impact on occupational safety and health (OSH) in the future. ICT encompasses and enables a wide range of technologies, including industrial automated systems. ICT innovation could have significant overall implications for the workforce and others affected by work activities. It could potentially change fundamentally where we work, how we work, who will work and how people will perceive work. This paper outlines the foresight project commissioned by the European Agency for Safety and Health at Work (EU-OSHA) and delivered by the authors. It explains how key societal, technological, economic, environmental and political trends and drivers of change were identified and used to develop scenarios of the future in consultation with a range of experts. Scenarios are narratives of what alternative futures might look like, built up from an assessment of how trends and drivers of change might influence the present to create different possible futures. Each scenario presents different challenges and opportunities for OSH policy-makers and social partners. They have, therefore, been used to identify potential new and emerging OSH risks as a result of how ICT could change the future nature of work. Scenarios aid thinking and stimulate discussions about a broad range of futures enabling different perspectives and priorities to be considered when making decisions about how to manage risks and uncertainties to minimise their possible negative impact in the future.

© European Agency for Safety and Health at Work, 2018. The preparation of this paper was funded by the Health and Safety Executive (HSE) and the work it describes funded by the European Agency for Safety and Health at Work (EU-OSHA). Its contents, including any opinions and/or conclusions expressed, are those of the authors alone and do not necessarily reflect EU-OSHA or HSE policy.

1 INTRODUCTION

Information and communication technologies (ICT) and work location were identified during a consultation exercise in 2014 across Europe as the topics most likely to have the greatest impact on occupational safety and health (OSH) in the future [1]. ICT encompass and enable a wide range of technologies that potentially have significant overall implications for the workforce and others affected by work activities. It could potentially change fundamentally where we work, how we work, who will work and how people will perceive work. Technologies are diffusing much faster than in the past. For example, it took commercial television 13 years to reach 50 million households and Internet service providers three years to sign 50 million subscribers but it took Facebook just a year and Twitter even less time to reach the same milestone [2]. Seven out of the 12 disruptive technologies identified by the McKinsey Global Institute [3] were ICT enabled technologies (ICT-ETs).

A connected Digital Single Market (DSM) was made one of the European Commission's key priorities [4]. The importance of ICT was also recognised in the European Union's ten-year jobs and growth strategy [5], launched in 2010 to create the conditions for smart, sustainable and inclusive growth. This strategy, known as Europe 2020, introduced the Digital Agenda for Europe as one of seven flagship initiatives, recognising the key enabling role that ICT has to play. The Digital Agenda is expected to deliver high levels of employment, productivity and social cohesion [4], [6].

The European Agency for Safety and Health at Work (EU-OSHA) therefore commissioned and project managed a foresight project to develop scenarios of the future and identify potential new and emerging OSH risks associated with ICT-ETs and their impact on the nature of work, in particular work location. The basis of foresight is an understanding that the future can evolve in different directions, which can be shaped by the actions of various players and the decisions taken today. Scenarios are narratives of what alternative futures might look like, built up from an assessment of how trends and drivers of change might influence the present to create each different future. Their development is participatory allowing a wide range of views from different disciplines to be considered whilst creating different versions of what the future could be like. The participatory approach fosters professional collaboration which can be important in enabling decisions and actions to be made in the present that can help avoid potential risks or realise potential opportunities.

2 METHOD USED TO CREATE SCENARIOS OF THE FUTURE

2.1 Identification of trends and drivers of change

A horizon scanning approach [7] was used to identify a wide range of information relevant to trends and drivers of change in relation to ICT and its impact on the nature of work, in particular work location. This was based on a review of the following sources:

- Journal papers (limited to previous five years);
- Publications of OSH regulators in a range of countries (current publications only);
- Popular science publications (limited to previous five years);
- Magazines and web-sites of relevant professional bodies;
- Technology blogs and web-sites;
- University and European framework research; and
- Documents and information published by EU-OSHA.

The project team also drew upon their knowledge from previous foresight and horizon scanning projects with which they had been involved and consulted ICT and OSH specialist colleagues and contacts.

The information was recorded under five main categories: Societal; Technological; Economic; Environmental; and Political (STEEP). Sub-categories under each of these were created and used as the information found dictated, which allowed the scope to expand as required. The information gathered was then reviewed and grouped into themes to identify and describe, under each STEEP category, 92 distinct trends and drivers of change. These comprised 29 Societal, 29 Technological, 19 Economic, 5 Environmental and 10 Political.

2.2 Consolidation of trends and drivers of change

A purposive sample of 19 experts, drawn from a range of organisations, were interviewed by telephone to consolidate the trends and drivers of change and to obtain initial views on which trends and drivers will have the greatest impact on ICT and the nature of work. Experts were selected from countries across Europe, with expertise in a variety of different fields to provide coverage of all STEEP categories. The data forthcoming as the interviews progressed were monitored to allow the expertise of subsequent interviewees to be targeted to match any gaps that became apparent.

A semi-structured approach was taken to the interviews based on the ‘Seven Questions’ technique, which was developed by SAMI Consulting and is now widely used in scenario-building exercises [8]. The questions were designed to be ‘open’, to give interviewees the freedom to develop ideas and the interviewer the freedom to explore them in more depth, where appropriate, in a relaxed, conversational manner. The comments made by interviewees were analysed to see to what extent the interview data provided coverage of trends and drivers similar to the horizon scanning.

A two-round Delphi-like web survey was also conducted. In the first survey round, respondents were shown a brief description of each trend and driver of change under each STEEP category and first asked whether there were any that they thought were missing or with which they disagreed. Respondents were then asked to select up to three trends and drivers (under each STEEP category), which they felt were the most important and asked whether they had any final comments. The selections made by respondents were used to rank the trends and drivers under each category of STEEP. A second follow-up web survey round was conducted in order to share the results and give respondents to the first web survey round a chance to comment on the overall ranking of the importance of the trends and drivers.

The data collected via the telephone interviews and web surveys were taken together to consolidate the trends and drivers that were identified via horizon scanning. This consolidation led to further information being added to some trends and drivers, some being modified or merged and a few new ones being added.

2.3 Selecting key trends and drivers of change

The consolidated list of trends and drivers was initially prioritised according to the ranking of the trends and drivers, the comments on this ranking from the Delphi-like web survey and the prevalence in the interviews of topics relating to each trend and driver. The comments from the second web survey about the extent of respondents' agreements with the rankings produced from the first were useful for understanding any differences between the rankings and the prevalence of topics relating to each trend and driver in the interviews.

It was important that any possible bias did not result in the 'weak signals' of emerging trends or drivers of change being filtered out, as these might be important for the ends of the scenario timelines. Consideration was, therefore, given to the possibility that the data could be biased towards 'current drivers' or issues that featured heavily in the media while the interviews took place or the surveys were open. In assessing weaker signals, account was, therefore, taken of comments made during the interviews and in the follow-up web survey. Reference was also made to the information collected earlier during horizon-scanning. The overall spread of the prioritised drivers was also reviewed to ensure that they covered the key issues for the project, including those highlighted in the interviews. Trends and drivers that were related in terms of their potential impact were then grouped together.

The prioritised groups of trends and drivers were then assessed during a mini-workshop to decide which of them were key. During the mini-workshop, participants first considered whether they were happy with the prioritised groups and made any changes that they agreed were necessary. This involved:

- Discussing whether any other trends and drivers from the full consolidated list (i.e. those not included in the prioritised list) were as important and adding them to the groups that they agreed, by consensus, were the most appropriate;
- Moving individual trends and drivers from one group to another (including from one STEEP category to another);
- Merging similar groups from different STEEP categories; and
- Adding any new trends and drivers of change that they considered were missing.

Participants then ranked the groups in terms of whether they were high impact, by comparing each group with all the others. They then selected those trends and drivers that they thought not only had a high impact but also had high levels of uncertainty associated with them. These are the 'critical uncertainties' that will create the key differences between alternative scenarios of the future. The trends and drivers that have a major impact but have more predictable outcomes are also important for scenario development; these, therefore, were also identified, so that they could be taken into account across all the scenarios. In addition, several groups of technology trends and drivers were identified that were high impact but for which the only uncertainty was how quickly the technology would become available and be adopted.

2.4 Development of scenario axes

Scenario axes define the space that contains the potential scenarios [7]. They are based on the high impact-high uncertainty key trends and drivers (critical uncertainties) and were developed by considering whether:

- Plausible and internally consistent scenarios could be created;
- There was a plausible path to the future scenarios formed by the axes;
- Scenarios would allow sufficiently challenging negative and positive aspects to emerge;
- The extent of correlation or independence between the axes was appropriate.

The outcome of the debates and discussions that took place during the workshop, and afterwards by the project team, was four possible scenarios defined by the four quadrants of a scenario space, illustrated in Figure 1, created by the following two axes:

1. Governance and public attitudes.
2. Economic growth and the application of technology.

Session 1 – Functional safety - Information technology

The vertical axis combined the key drivers on the acceptance and demand for developments in ICT-ETs and the way ICT-ET innovation and implementation are governed. It was given the name ‘*Governance and public/workers’ attitudes*’ and covers the following areas:

- The environment in which ICT-ET will be exploited;
- The levels of acceptance from the public/workers; and
- The levels of leadership from governments, business and workers’ representatives.

These could either be supportive with high levels of acceptance, or resistive with low levels of acceptance.

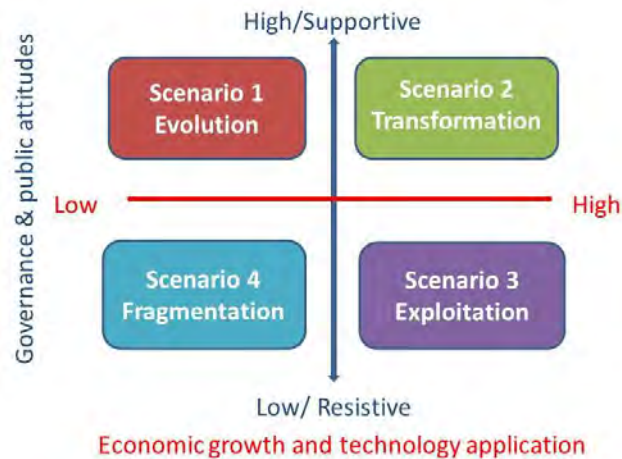


Figure 1. Scenario quadrants.

The horizontal axis combined the supply side drivers that determine the investment in developments in ICT-ET and the demand for and application of these technologies. It was given the name ‘*Economic growth and the application of technology*’ and covers the following areas:

- The level of economic growth and investments in technology and skills.
- The application of the developments of ICT-ET.
- The level of impact on the nature and locations of work; and the associated changes to business structures.

Economic growth and investment and the application of technology could be high or low.

2.5 Producing scenario descriptions

Outlines of each scenario were created by discussing the key trends and drivers that were important for each scenario in more detail and agreeing what the future could be like in each scenario in 2025 and beyond [7]. The outline scenarios were developed into provisional OSH scenarios by considering how ICT-ET will develop in the world described in each scenario and what this could mean in terms of the general OSH environment, and new and emerging OSH risks. The resulting OSH scenarios were then peer reviewed by four OSH experts and the scenarios revised to take account of their comments. Visualisations were also produced, by an artist, to help bring the scenarios to life, prompt discussion, and highlight key aspects of the scenarios and the OSH implications. Their purpose was not to represent actual events that could occur in the future but to promote broader thinking and discussion of the OSH implications of the changing nature of work.

2.6 Testing and consolidation of scenarios

The provisional OSH scenarios were tested at a workshop in Brussels with policy-makers and experts from various disciplines. The workshop participants were split into four groups that each worked with just one of the four scenarios for the whole workshop. Following a presentation of potential developments in technology, the scenarios and potential OSH implications, an initial exercise was held to enable participants to become familiar with their respective scenario. The groups then discussed the OSH challenges and opportunities in their scenario and considered potential strategy and policy responses to the new and emerging OSH challenges. These responses were then discussed and reviewed to test their robustness in the other scenarios. This process (often termed wind-tunnelling [7]) was used to check that the scenarios were sufficiently different and challenging for developing and testing actual policies. The provisional scenarios were then revised, in consultation between HSE, SAMI and EU-OSHA, to take account of the discussions held and comments made during the workshop.

3 RESULTS

Four distinct scenarios of the future [9] were created that:

- Allow policy makers to consider a range of potential OSH impacts.
- Address the critical issues that could have an impact on OSH.
- Are plausible, with a plausible route from the present and internally consistent.
- Stretch current thinking.

The development of the scenarios has shown that:

- ICT-ETs provide opportunities to reduce some existing OSH risks or manage them better.
- Existing risks will be found in new contexts and occupational sectors as a result of increased application and innovation in ICT-ETs.
- Psychosocial and organisational factors are expected to be increasingly important because ICT-ETs can drive changes in: the types of work available; the pace of work; how, where and when it is done; and how it is managed and overseen.
- Solutions to OSH challenges and how they are implemented need to take account of the prevailing and possible future social-economic environment.

Each scenario presents different challenges and opportunities for OSH policy makers, duty-holders, social partners and researchers. Some of these are due to the influence of the interaction between the two axes on the extent and impact of similar risks. Risks that are likely to be present in all four scenarios, have also been identified. Whilst the extent and impact will differ, these risks are, therefore, highly likely to be present in the actual future and are:

- The potential for automation to remove humans from hazardous environments, but also to introduce new risks influenced by workers' understanding and the transparency of the underlying algorithms.
- Increasing work-related stress, particularly the impact of increased worker monitoring made possible by advances in and increasing ubiquity of wearable ICT-ET, 24/7 availability and the gig economy.
- Increasing ergonomic risks due to the increase in online working and the use of mobile devices in non-office environments.
- New risks associated with new human-machine interfaces such as gesture controlled interfaces that could cause MSDs, or systems involving high visual, voice and/or cognitive load.
- Cyber-security risks due to an increase in the number of online smart devices / the Internet of Things.
- Increasing numbers of workers treated (rightly or wrongly) as self-employed who could fall outside existing OSH regulation.
- Changing employment hierarchies due to increased online (crowd-working), flexible working and AI, which have the potential to disrupt the current mechanisms for the management of OSH risks.
- Workers not having the necessary skills to be able to use ICT-ET, cope with change and manage their work-life balance.
- OSH risks associated with more frequent job changes and a longer working life.

From an OSH regulatory perspective, it is possible to envisage a situation in which the use of ICT-ETs drive rapid changes not only in the technologies used at work but also the nature of work, business structures, employment status, hierarchies and relationships; the combined impact of these changes could potentially challenge existing mechanisms for managing and regulating OSH. This has implications for:

- Clarity about, and actual changes to, responsibilities for managing OSH.
- Workers' skills and knowledge.
- Access to learning, information, advice and support.
- Occupational health surveillance and associated records.

There are, therefore, OSH implications for businesses, regulators, inspectors, occupational health services and worker representatives, as well as for education, training and research.

The findings and finalised scenarios have been published on EU-OSHA's website [8] and disseminated during a workshop, consisting of a blend of presentations, group exercises and plenary discussions over the course of one day, to EU-OSHA focal point representatives in Bilbao, Spain. A final project report will also be published soon.

Additional dissemination workshops are planned in different European countries with the objectives of:

- Presenting the foresight project, the scenarios developed and the new and emerging risks identified.
- Demonstrating how participants can use the scenarios as a tool to develop and test existing policies and strategies addressing the OSH challenges identified in the project.

4 DISCUSSION

The key trends and drivers [9], when considered as a whole, imply that the pace of change of ICT-ETs and how they are exploited in the workplace are likely to be dependent on various factors: the demand for and acceptance of ICT-ET by the public and workers; and how governance, management and investment-related decisions support innovations in ICT-ET. The nature of organisational and government decisions (including their timeliness and effectiveness) about use of robotics, autonomy and artificial intelligence (AI), are likely to drive fundamental changes in the nature of work, business structures and hierarchies.

The testing of the use of the scenarios and the first dissemination workshop has shown that the scenarios could be used to

- Help inform EU and Member States' decision makers, trade unions and employers, so that they can take appropriate account of changes in ICT, its use and its impact on work location, when making decisions to shape the future of OSH towards safer and healthier workplaces.
- Stimulate discussions that incorporate multi-disciplinary perspectives, about the actions that can be taken today to help avoid future problems or to influence what happens in the future.
- Test and refine policies to make them more robust and resilient to the impact of future changes to the nature of work as the result of innovation and application of ICT-ETs.

The scenarios created during this foresight project should not be treated as predictions of the future but as a tool to aid thinking and stimulate discussions about a broad range of possible and plausible futures and how to manage the associated risks and uncertainties. If risk analysis is restricted to current data and trends, potentially important future risks are likely to be overlooked. Testing policies against a range of scenarios is important, as the future is likely to contain elements of each scenario in a combination that cannot be anticipated. Such testing can help to identify which policies are robust enough to work in a range of different futures as opposed to those that will work in only one. In this way policies can be “future-proofed” resulting in a wider range of more robust policies and implementation plans that can also influence what actually happens in the future.

Scenarios, when used during a workshop, create an environment for a strategic discussion between stakeholders, challenge people's perceptions and stretch their thinking. This enables a more robust assessment and understanding of a wider range of risks than could otherwise be achieved. Scenarios can also be used for stakeholder analysis to identify which will be most affected (positively or negatively) and which are best placed to manage risks or implement policies. They can also be used to help stakeholders develop a shared understanding about the issues raised by the different potential futures and reach consensus.

5 REFERENCES

1. European Agency for Safety and Health at Work, *Scoping study for a foresight on new and emerging occupational safety and health (OSH) risks and challenges*, 2014. Available at: <https://osha.europa.eu/sites/default/files/publications/documents/en/publications/reports/scoping-study-for-a-foresight-on-new-and-emerging-osh-risks-and-challenges/Dos%20613%20-%20for%20publication.pdf>
2. Bughin, J., Chui, M. and Manyika, J., *Capturing business value with social technologies*, McKinsey Quarterly, 2015. Retrieved 6 October 2017 from: https://www.mckinsey.it/idee/capturing-business-value-with-social-technologies?response_type=embed&v=print
3. Manyika, J., Dobbs, R., Chui, M., Bughin, J., and Bisson, P., *Disruptive technologies: Advances that will transform life, business, and the global economy*, McKinsey Global Institute, 2013. Available at: <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies>
4. European Commission, *A digital single market strategy for Europe*, 2015. Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN>
European Commission, *Europe 2020: A strategy for smart, sustainable and inclusive growth*, Communication from the Commission, Brussels, 3.3.2010 COM(2010) 2020, 2010. Available at: <http://ec.europa.eu/eu2020/pdf/COMPLETE%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf>
5. Maciejewski, M. and Dimova, M., *The ubiquitous digital single market*, Fact Sheets on the European Union, 2016. Available at: http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_5.9.4.html
6. Ringland, G., *Scenario planning: Managing for the future*, J Wiley and Sons. ISBN 13 978-0-470-01881, 2006.

Session 1 – Functional safety - Information technology

7. UK Government Office for Science, Futures Toolkit: tools for strategic futures for policy-makers and analysts, 2017. Available at: <https://www.gov.uk/government/publications/futures-toolkit-for-policy-makers-and-analysts>
8. European Agency for Safety and Health at Work, *Foresight on new and emerging OSH risks associated with information and communication technologies by 2025*, Event Summary, 2018. Available at: <https://osha.europa.eu/en/tools-and-publications/seminars/foresight-new-and-emerging-osh-risks-associated-information-and>
9. European Agency for Safety and Health at Work, *Key trends and drivers of change in information and communication technologies and work location*, 2017. Available at: <https://osha.europa.eu/en/tools-and-publications/publications/key-trends-and-drivers-change-information-and-communication/view>

How to consider security aspects during the design of machinery

Bernard Mysliwiec
MySafeAutomation
bm@mysafeautomation.com
+49 172 84 22 401



What about standards

IEC TR 63069 ED1

Industrial-process measurement, control and automation- Framework for functional safety and security

2016-08

[APUB](#) 2018-09

[TPUB](#) 2019-01

IEC TR 63074 ED1

Security aspects related to functional safety of safety-related control systems

2016-07

[TDTR](#) 2018-09

[CDTR](#) 2018-11



Differences and similarities

1 Scope 63069

This Technical Report (TR) explains and provides guidance on the common application of IEC 61508 and IEC 62443 in the area of industrial-process measurement, control and automation.

1. Scope 63074

This Technical Report gives guidance on the use of IEC 62443 series related to those aspects of security threats and vulnerabilities that could influence functional safety implemented and realized by safety-related control systems (SCS) and could lead to the loss of the ability to maintain safe operation of a machine.



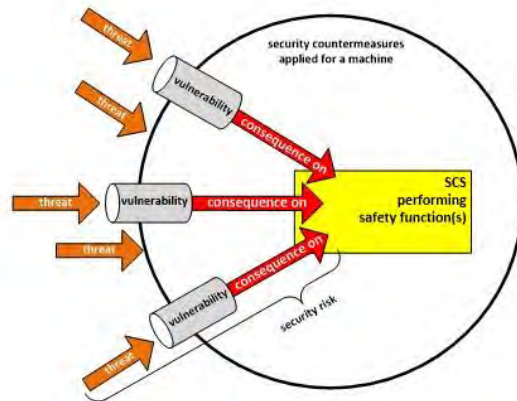
Differences and similarities 2

IEC TR 63069

IEC TR 63074



Figure 3 — Security environment



IEC TR 63069 risk assessment

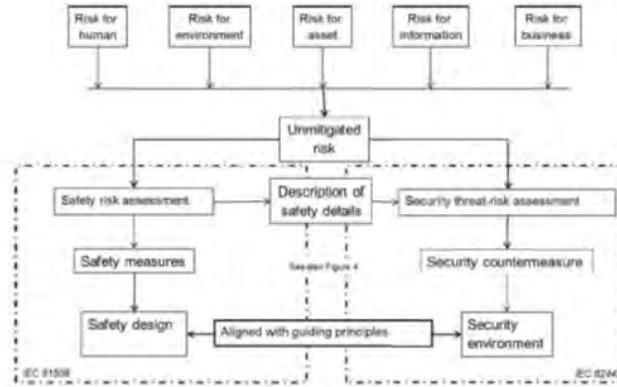


Figure 5 — Safety and security risk assessments as part of a risk assessment at higher level



Differences and similarities 3

IEC TR 63069

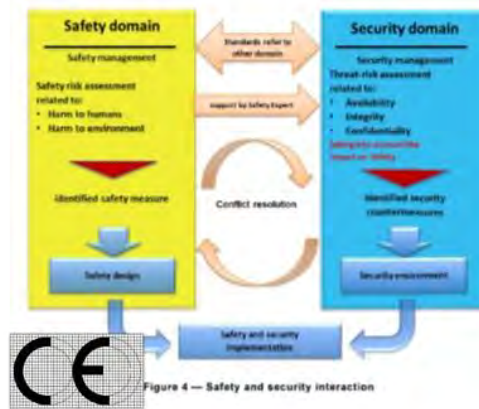
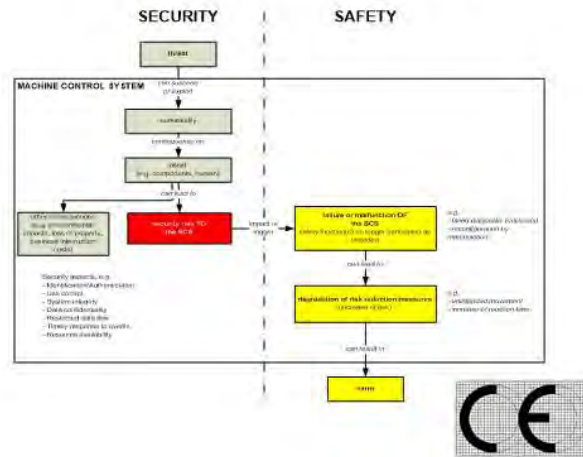


Figure 4 — Safety and security interaction



Differences and similarities 3

IEC TR 63074



Machinery Directive: CE marking and Declaration of conformity

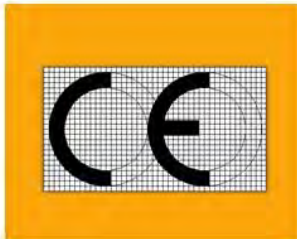
EC DECLARATION OF CONFORMITY OF THE MACHINERY

This declaration and translations thereof must be drawn up under the same conditions as the instructions (see Annex I, section 1.7.4.1 (a) and (b)), and must be typewritten or else handwritten in capital letters.

This declaration relates exclusively to the machinery in the state in which it was placed on the market, and excludes components which are added and/or operations carried out subsequently by the final user.

The EC declaration of conformity must contain the following particulars:

1. **business name and full address of the manufacturer** and, where appropriate, his authorised representative;
2. **name and address of the person authorised to compile the technical file**, who must be established in the Community;
3. **description and identification of the machinery**, including generic denomination, function, model, type, serial number and commercial name;
4. **a sentence expressly declaring that the machinery fulfils all the relevant provisions of this Directive and where appropriate, a similar sentence declaring the conformity with other Directives and/or relevant provisions with which the machinery complies**. These references must be those of the texts published in the *Official Journal of the European Union*;
5. where appropriate, the **name, address and identification number of the notified body** which carried out the EC type-examination referred to in Annex IX and the number of the EC type-examination certificate;
6. where appropriate, the **name, address and identification number of the notified body** which approved the full quality assurance system referred to in Annex X;
7. where appropriate, a **reference to the harmonised standards used**, as referred to in Article 7(2);
8. where appropriate, the **reference to other technical standards and specifications used**;
9. **the place and date of the declaration**;
10. **the identity and signature of the person** empowered to draw up the declaration on behalf of the manufacturer or his authorised representative.



TS 62443-1-1 6.2 Simplified reference model for single machine

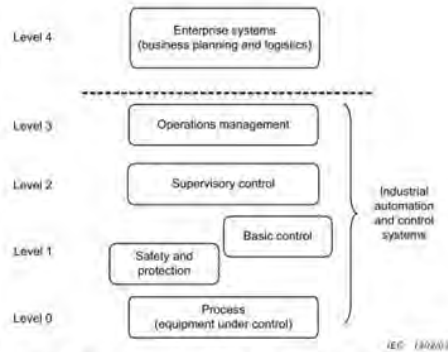
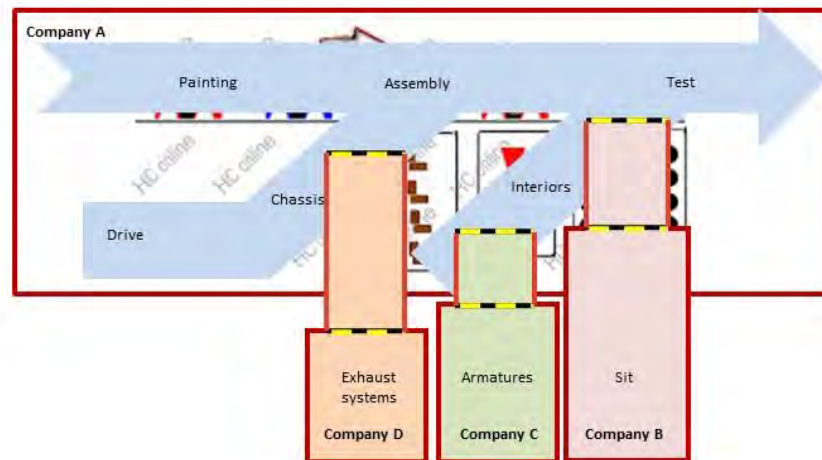


Figure 12 – Reference model for IEC 62443 standards

9



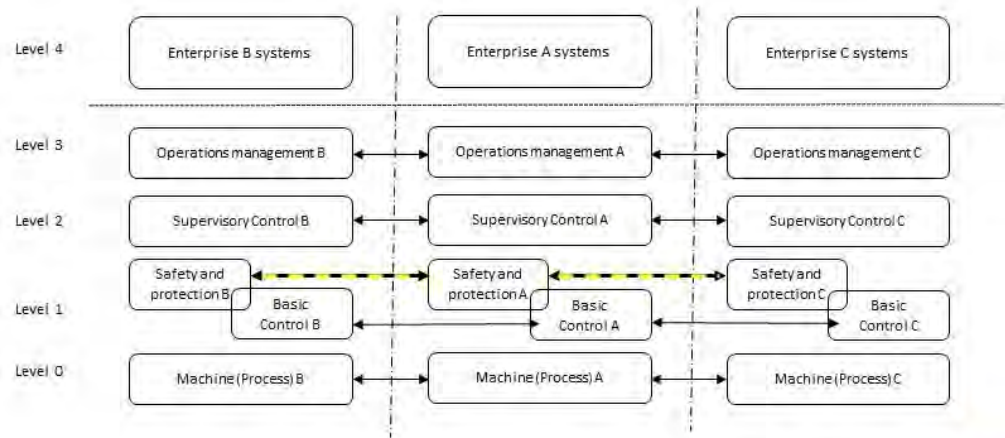
Example Automotive Industry:



10



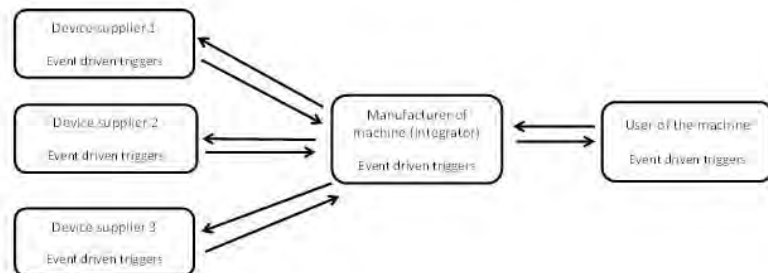
Example of production line: proposed reference model



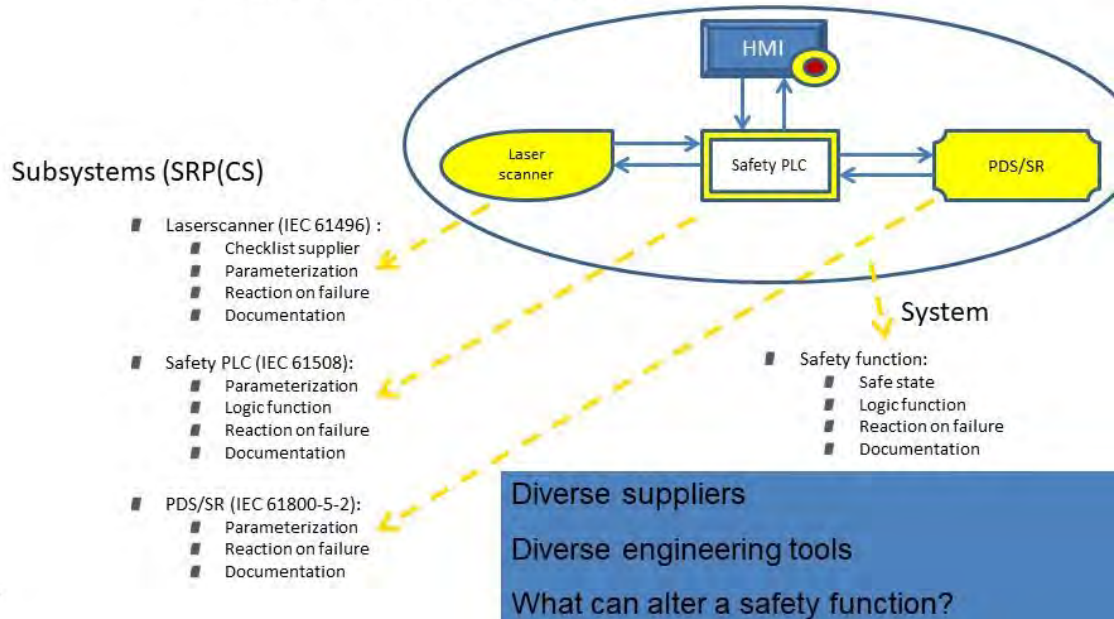
11



IEC TR 63074: Information flow: Event driven triggers



Example of safety functions



13

Examples of attacks

- Laserscanner → PLC Modified field status
- PLC → Laserscanner Parameter modification (IPar Server)
- HMI → PLC Wrong operating mode,
- PLC → HMI Altered operating conditions
- PLC → PDS/SR Parameter modification: SLS, SLT
Altered operating conditions:
Safe Stop, Setpoints
- PDS/SR → PLC Altered operating conditions: SOS, STO



What can alter a safety function?

- Modification of parameters
- Modification of logic function
- Modification of safety related information
- Modification of safety related data telegram
- Modification of time behavior
-

15



What can the safety expert do?

- + Define the information set to be protected
 - Parameter
 - Logicfunction (software)
 - Network interface (data communication, parametrization...)
 -
- + Define the imperative (must) function specification
 - Time behavior,
 - Safety distance
 -
- → Inform the security expert

Passive protection

16



What can the safety expert do? 2

- Use inherent secure devices
- Detect :
 - + Not allowed access to subsystems or system
 - Topology modification
 - + → generate an adequate reaction

Active protection

17



What can the safety expert do? 3

- Think about the
 - + attractiveness of the machine for hackers
 - Consequences:
 - + Loss of safety, production
 - Image
 - Effects on environment (public)
 - + possible ways of attacks
 - people susceptible to attack
 - + ...

Possible consequences

18



Differences and similarities

Safety protects people against machine

Security protects machine against people

Safety considers consequences

Security do not consider consequences

Safety parameters: SIL and PL

Security parameters: SL, ML and PL



Protection Levels cover security functionalities and processes



Evaluation of automation solution measures	
SL 1	Capability to protect against casual or coincidental violation
SL 2	Capability to protect against intentional violation using simple means with low resources, generic skills and low motivation
SL 3	Capability to protect against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
SL 4	Capability to protect against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

Evaluation of operational and maintenance measures	
ML 1	Initial - Process unpredictable, poorly controlled and reactive.
ML 2	Managed - Process characterized, reactive
ML 3	Defined - Process characterized, proactive deployment
ML 4	Improved - Process measured, controlled and continuously improved

Protection Levels						
Rating of operational and maintenance measures	ML 4	PL 1+	PL 2+	PL 3+	PL 4+	Rating of automation solution measures
	ML 3	PL 1	PL 2	PL 3	PL 4	
	ML 2	PL value cannot be determined				
	ML 1	SL 1	SL 2	SL 3	SL 4	
		PL 1	Protection against casual or coincidental violation			
		PL 2	Protection against intentional violation using simple means with low resources, generic skills and low motivation			
		PL 3	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation			
		PL 4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation			

Unrestricted © Siemens AG 2018

Page 6

2018-04-24

Holistic Security Concept • Produktivität umfassend schützen mithilfe der IEC 62443

Dr. Kobes PD TI AT

Pictures on courtesy of Siemens



From the Safety Experts perspective

Some proposed distinctions

- benevolent ↔ malicious
- danger to the environment ↔ threat from the environment
- unintentional ↔ intentional
- slow changes ↔ rapid changes



Saved more
than 300
peoples

Pictures on courtesy of Siemens

**The safety
expert...**

**... and the
security
expert**



Bit more than
10000
peoples only
in Germany



Analysis of Markov Models for Safety-related Systems in Security Environments

Wieczorek F.¹, Schiller F.¹, Eckert C.²

¹Beckhoff Automation GmbH & Co. KG – Ostendstraße 196 – D-90482 Nuremberg – Germany

²Technische Universität München, Chair for IT Security – Boltzmannstraße 3 – D-85748 Garching – Germany

[f.wieczorek, f.schiller}@beckhoff.com](mailto:{f.wieczorek, f.schiller}@beckhoff.com)
claudia.eckert@in.tum.de

KEYWORDS: Functional Safety, Error Models, Security for Safety, Markov Model

ABSTRACT

Markov models are commonly used as models in safety analyses. Here, their graphical representation is applied for a systematic analysis of security attacks on safety communication. Related error models and typical error detection methods are considered based on the graphical representation. It enables a systematic view on different types of attacks and different sequences of attacks as well as on the validity of model characteristics. The graphical representation of Markov models helps to understand the issues in both communities of safety and security and supports a comprehensive analysis for safety and security.

1 INTRODUCTION

Markov models [1] are commonly used as models in safety analyses. They are applied to calculate the established criteria Probability of dangerous Failure on Demand (PFD) and Probability of dangerous Failure per Hour (PFH), see e.g. [2].

However, as soon as security attacks have to be taken into account, the validity of these models have to be questioned. The issue that attacks cannot be modeled probabilistically in a proper way is widely understood [3]. There are currently intense discussions trying to separate safety and security analyses for that reason.

In addition to the apparent effects of attacks, the plain existence of security measures has influence on the safety models. This issue related to safety communication is discussed in [4] and is not treated in the following.

In the paper, we use mainly the graphical representation of typical Markov models of safety communication for a systematic analysis of attacks on safety communication. The usually underlying differential equations [5] are completely out of concern. They might get non-linear, discontinuous, and even the Markov property, which means, that the future state of a system depends on the current state and the transition rates only, might no longer hold in case of attacks.

Nevertheless, the fundamental relations are still valid and deliver a reasonable basis for further analysis.

Firstly, we apply Markov models w.r.t. random errors in communication to compare Cyclic Redundancy Check (CRC, see e.g. [6], [7]) usually applied in the domain of safety and Message Authentication Code (MAC, see e.g. [8]) usually applied in the domain of security. We demonstrate that CRC could be substituted by MAC for random errors.

Secondly, attacks are introduced. The counterpart to random data errors in security are manipulations. Many related aspects become obvious in the graphical representation of the Markov model supporting a systematic view. Mainly, different types of attacks and different sequences of attacks on the integrity of transmitted data can be distinguished and investigated. Other goals of security like confidentiality are out of scope here.

Our intention is to support a systematic view and to rethink the validity scope of Markov models modeling systems under attacks by analyzing the influence on the parameters. We intend to contribute to a common understanding of both communities of safety and security and to a comprehensive analysis of safety and security as well.

2 EXAMPLE

The exemplary safety communication is considered to be part of a simple plant consisting of a tank with a heater, a pressure sensor, a safety-related Programmable Logic Controller (PLC), and a pressure relief valve (cf. Figure 1). The considered safety function opens the valve in case of measured overpressure. The state of open valve is the safe state. If the overpressure cannot be released by the valve, a hazardous situation occurs. Whenever any safety-related error is detected the valve opens, too. For this function, safety communication between the sensor, the PLC, and the valve is necessary.

In the following, only the safety communication is considered. The communication channel is affected by random errors and attacks resulting in manipulations.

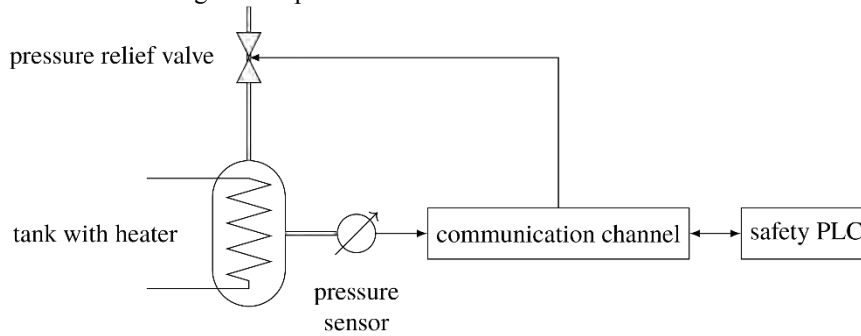


Figure 1. Example.

3 MARKOV MODEL OF A SAFETY COMMUNICATION SYSTEM

Markov models are often used to model safety systems concerning random errors [5]. By means of Markov models, the analysis of the reliability and the probability of failures can be carried out [1].

We introduce a general model for a safety communication system as a graphical description of Markov models. Often safety systems are modeled as shown in Figure 2 where

- ok error-free state
- du dangerous undetectable error state
- dd dangerous detectable error state
- safe safe state
- P_{re} residual error probability of a message
- P_{err} probability of an erroneous message
- λ_{mess} message rate
- τ rate of error detection algorithm
- μ repair rate

hold. In safety communication, often each error is assumed to be dangerous since the meaning of transmitted data or their effect on the plant, respectively, is not known in general. The rates have usually been assumed to be constant.

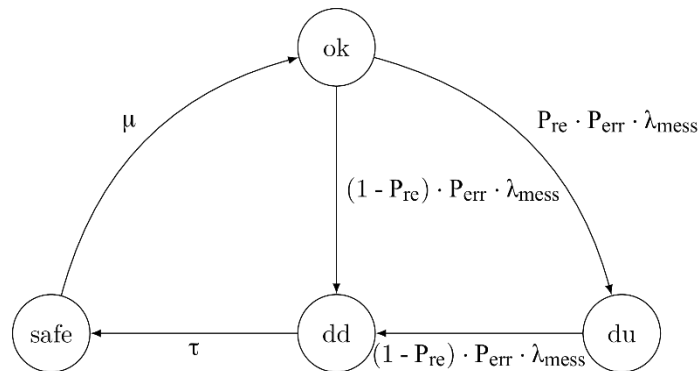


Figure 2. Commonly used Markov model to describe safety communication (in accordance with [9]).

The system is initially in the state “ok”, which means no error occurred. When an error occurs, the state transitions to either the “du” state or to the “dd” state. When an detectable error occurs in the “du” state, the system transitions to the “dd” state, too.

Then the error-handling algorithm is executed transitioning the system into the “safe” state. This state usually means to stop the operational function, i.e. the production cannot be continued or any other economic loss is suffered as the opening of the pressure relief valve interrupts the regular heating process. The repair of the system is modeled by a transition back into the “ok” state.

The communication error-detection algorithm is run on the message as input. It outputs a Boolean value indicating whether the message is correct (check_ok) or incorrect (\neg check_ok), respectively. The residual error

probability P_{re} is the conditional probability that the check outputs `check_ok` on condition that the message is erroneous, $P_{re} = P(\text{check_ok} | \text{message_is_erroneous})$.

However, in e.g. coding theory literature [6], often the term residual error probability is used for the absolute probability that the check outputs `check_ok` and the message is erroneous, i.e. $P_{re} = P(\text{check_ok} \wedge \text{message_is_erroneous})$. Therefore, we will use the specific terms conditional residual error probability

$$P_{re}^{cond} = P(\text{check_ok} | \text{message_is_erroneous})$$

and absolute residual error probability

$$P_{re}^{abs} = P(\text{check_ok} \wedge \text{message_is_erroneous}) = P_{re}^{cond} \cdot P_{err}$$

in addition to the general term residual error probability P_{re} .

If a communication error is detected then the system transitions into the safe state with rate τ . The repair of the system occurs with rate μ , for which the reciprocal value of the average repair time is usually applied.

A much more detailed analysis is enabled by inserting a hazard state as shown in Figure 3, cf. [10]. Whenever the system is in the state “du” or “dd” and a demand d like an overpressure occurs, then the hazard emerges. Obviously, the higher the detection rate τ the smaller is the probability of “dd”, i.e. the state of a detectable but not yet detected error, and the smaller is the probability of the actual transition from “dd” to the hazard.

When the system is in the hazard state there is a risk to human or environment. Since the safety system is designed to avoid the hazard state, the probability of a transition to it has to be acceptable low at each time of the life cycle, cf. PFH.

In the example of Section 2, a bit error may cause a low value of the measured pressure. If this error is an undetectable one and a demand occurs, that means that the real pressure is too high, then a hazard is caused. If this error is detectable and the error detection algorithm detects it before the real pressure gets too high then the safe state is initiated by opening the pressure relief valve.

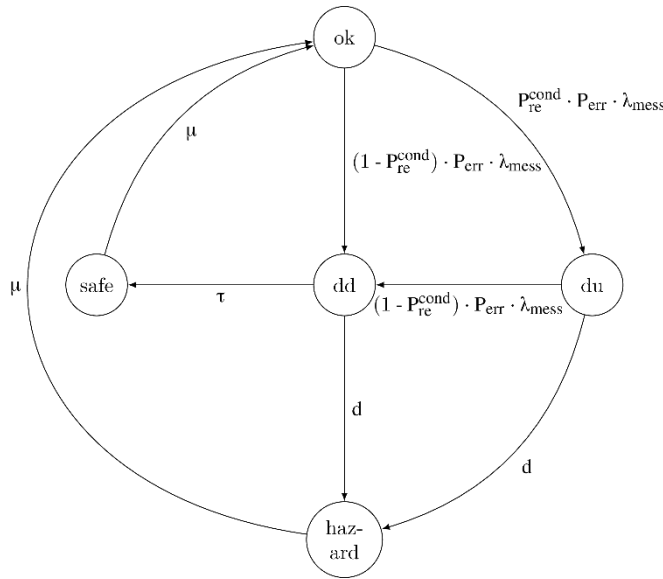


Figure 3. Markov model extended by the hazard state.

4 ADJUSTMENT AND AGGREGATION OF THE MARKOV MODEL

Whenever the check detects an error ($\neg \text{check_ok}$), the data of the message cannot be used obviously. Depending on the application, the receiver might wait for a successful check (`check_ok`) of one of the following messages and use its data instead. However, many safety communication protocols transition the system into the safe state immediately according to their specific safety argumentation. This behavior allows two adjustments to the basic Markov model (cf. Figure 4):

- The rate of error detection τ goes against infinity since each detected error causes the transition to “safe” immediately.
- The demand rate d from “dd” to “hazard” is equal to 0 since each detectable error will never be used.

Based on the adjustments, two aggregations of states are applicable (cf. Figure 5):

1. The states “dd” and “safe” can be joined to “safe, dd” since $\tau \rightarrow \infty$ and $d = 0$.
2. The resulting state “safe, dd” can be joined with “hazard” to “safe, dd, hazard” since the transition rates μ from both states to state “ok” are equal.

The second step is very unusual since the meaning of the aggregated states are very diverse, but it is conceptually correct. The transition from “du” to “safe, dd, hazard” via demand d is still the critical one, cf. PFH. The adjustments and aggregations make the following discussion clearer. For a comprehensive description of aggregation of Markov models see e.g. [11].

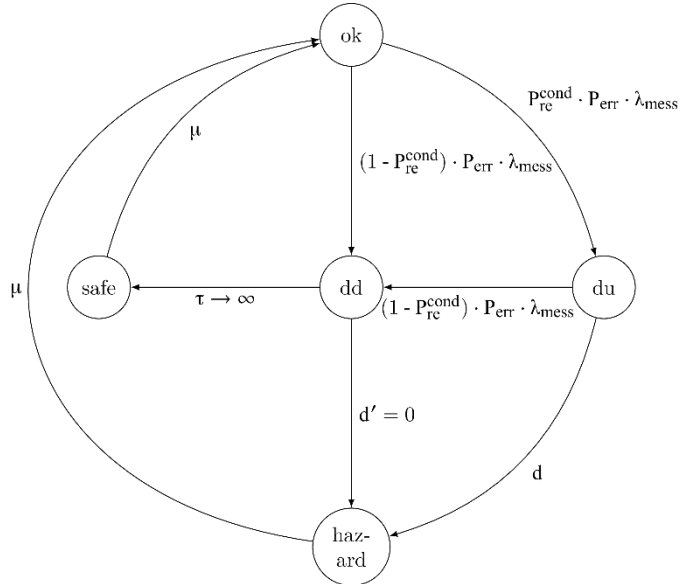


Figure 4. Adjusted Markov model. Each detectable error has no hazardous impact.

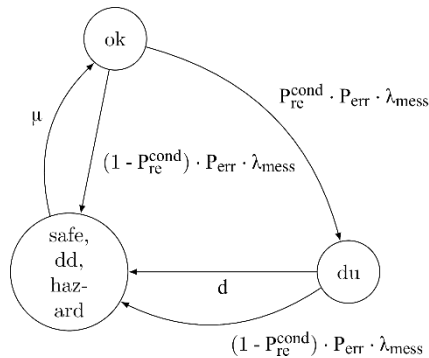


Figure 5. Aggregated Markov model.

5 RANDOM ERRORS

For safety communication systems, the error probability is usually modeled according to the Binary Symmetric Channel (BSC) [6], where

- each bit is corrupted independently of other bits and
- a bit corruption from value 0 to value 1 occurs with same probability p_{biterr} like a corruption from value 1 to value 0.

In this model, the probability of an erroneous message is

$$P_{err}^{BSC} = 1 - (1 - p_{biterr})^{|\text{mess}|}$$

where $|\text{mess}|$ denotes the number of bits of a message.

The residual error probability P_{re} in general depends on the probability distribution of error patterns and on the detection algorithm. We use two different error-detection algorithms, one is the Cyclic Redundancy Check (CRC) [6], which is only suitable for random errors [12] and an Message Authentication Code (MAC) [8] initialized with a uniformly random chosen key, which had been developed for protection against manipulation by attackers [13].

The messages are protected by an attached corresponding checksum. The absolute residual error probability of a CRC is $P_{re}^{abs} \leq 2^{-|fcs|}$, where $|fcs|$ denotes the length of the checksum (Frame Check Sequence). A proper characteristic is presupposed [14]. The maximum absolute residual error probability $2^{-|fcs|}$ is used in Figure 6.

The MAC algorithm is designed such that each error pattern is detectable with equal probability. Thus the conditional residual error probability is given by $P_{re}^{cond} \leq 2^{-|mac|}$, where $|mac|$ denotes the length of the corresponding checksum, cf. Figure 7.

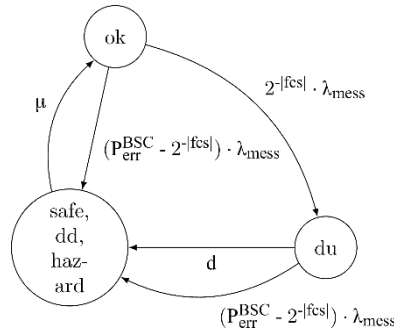


Figure 6. Markov model with check algorithm CRC. Error model is BSC.

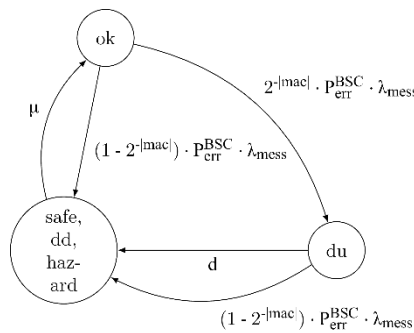


Figure 7. Markov model with check algorithm MAC. Error model is BSC.

6 PRESENCE OF AN ATTACKER

The attacker can manipulate any data such as safety-related data of the message. He might modify or delete existing messages or introduce new messages. At first sight he affects the probability of erroneous messages and rate of messages as well. But based on knowledge or assumptions about the protecting algorithm he affects the residual error probability, too.

6.1 Categorization of Attacks

An attack or a sequence of attacks, respectively, may concern different parameters of the Markov model, cf. Figure 8. Since probabilities can be formulated of each kind of events, we use the term probabilities here in order to describe points of attack or effects of attacks, respectively. In Figure 8, the conditional residual error probability represents both the conditional and the absolute residual error probability in a qualitative way. The following attacks are possible, see Figure 8:

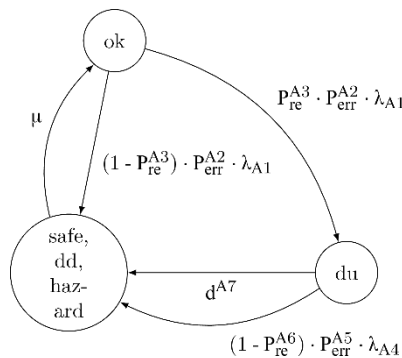


Figure 8. Aggregated Markov model with presence of an attacker. Probabilities are qualitative ones.

- A1 Attack changing the message rate:
The message rate can no longer be assumed constant, $\lambda^{A1} \neq \lambda_{\text{mess}}$. For example, the attacker can delay messages, introduce new messages, simply repeat messages. As a countermeasure, the message rate could be observed. Time expectations and differences are typically used in safety communication. Nevertheless, the algorithms or their implementations, respectively, can be compromised.
- A2 Attack concerning the probability of an erroneous message:
The probability of an erroneous message will change, $P_{\text{err}}^{A2} \neq P_{\text{err}}$. For example, the attacker can corrupt messages containing values of pressure.
- A3 Attack concerning the residual error probability:
According to the error detection algorithm and the ability of the attacker, the attacker can create undetectable error patterns, $P_{\text{re}}^{A3} \neq P_{\text{err}}$, and such the safety PLC applies incorrectly low pressure values.
- A4 Subsequent attack changing the message rate after a previously undetected successful attack:
Whenever the attacker can figure out whether he was successful, he can stop further attacks on the message rate in order to decrease the chance to be detected before a demand and a hazard occur, i.e. $\lambda_{A4} = \lambda_{\text{mess},\text{min}}$ holds. That means the system stays as long as possible in the “du” state such that a transition to the hazard will occur in case of a demand. The minimum message rate $\lambda_{\text{mess},\text{min}}$ does not activate the time supervising watch dog mechanism. If he cannot realize that the system under attack is in state “du” already then $\lambda_{A4} = \lambda_{A1}$ holds.
- A5 Subsequent attack concerning the probability of an erroneous message after a previously undetected successful attack:
Whenever the attacker can figure out whether he was successful, he can stop further attacks on the probability of an erroneous message in order to decrease the chance to be detected before a demand and a hazard occur, i.e. $P_{\text{err}}^{A5} = 0$ holds. If he cannot realize that the system is in state “du” already, $P_{\text{err}}^{A5} = P_{\text{err}}^{A2}$ holds.
- A6 Subsequent attack concerning the residual error probability after a previously undetected successful attack:
If the attacker cannot realize that the system under attack is in state “du” already then he goes on manipulating, i.e. $P_{\text{re}}^{A6} = P_{\text{re}}^{A3}$ holds. Otherwise, it does not matter since $P_{\text{err}}^{A5} = 0$ holds anyway.
- A7 Attack concerning the safety-related demand rate:
The attacker can change the demand rate d as well.

Two types of safety-related demands d should be distinguished but have not been in the safety community yet.

1. The safety-related demand is either initiated by the operational function (d_{Op})
2. or initiated by exposition of humans in the environment of the system under attack (d_{Env}).

In the example of Section 2, the overpressure might be caused by an attack in order to create economic loss. This attack on the regular, non-safety-related controller system is nevertheless safety-related. The overpressure represents a safety-related demand d_{Op} since the safety function has to react according to its specification but is initiated by the operational function.

If humans in the environment were protected by a light curtain such that the pressure relief valve opened in case of detected humans too close to the tank then the initiation of the light curtain would represent the safety-related demand d_{Env} . An attacker can change d_{Env} by means of additional different attacks to e.g. the infrastructure here.

In safety analyses, high-demand and low-demand systems are distinguished, cf. [2]. This distinction becomes obsolete obviously according to Attack A7 and must be discussed.

6.2 Integrity with CRC in Presence of an Attacker

Clearly, the CRC must not be applied in case of manipulations, cf. e.g. [12]. This section intends to demonstrate in detail how the CRC is inappropriate here by means of the graphical representation of the Markov model.

The following attacks are possible, cf. Figure 8. The result is depicted in Figure 9:

- A1 Attack changing the message rate:
The worst case in this scenario is that the attacker changes the message rate to its technically possible maximum, i.e. $\lambda_{A1} = \lambda_{\text{mess},\text{max}}$ holds.
- A2 Attack concerning the probability of an erroneous message:
According to the nature of manipulations, the Binary Symmetric Channel cannot be assumed at all (cf. Section 5). Each message can be corrupted, such that $P_{\text{err}}^{A2} = 1$ holds in the worst case.
- A3 Attack concerning the residual error probability:
The residual error probability has to be assumed to be highly controllable by the attacker, since there are error patterns, that are deterministically undetectable. For example, the generator polynomial of the CRC is

such an undetectable pattern [12]. Therefore, $P_{re}^{A3} = 1$ has to be assumed.

- A4 Subsequent attack changing the message rate after a previously undetected successful attack:
Since it has to be assumed that the attacker can figure out when he was successful, $\lambda_{A4} = \lambda_{mess,min}$ holds in the worst case.
- A5 Subsequent attack concerning the probability of an erroneous message after a previously undetected successful attack:
Since it has to be assumed that the attacker can figure out when he was successful, $P_{err}^{A5} = 0$ (no additional manipulation) holds in the worst case.
- A6 Subsequent attack concerning the residual error probability after a previously undetected successful attack:
It does not play a role since $P_{err}^{A5} = 0$ applies as worst case anyway.
- A7 Attack concerning the safety-related demand rate: See A7 in Section 6.1

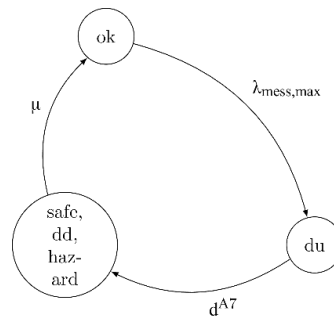


Figure 9. Aggregated Markov model with check algorithm CRC in presence of an attacker.

The parameters of the Markov model may change tremendously, and each safety analysis without consideration of attacks becomes obsolete as long as no suitable error detection algorithm is applied.

6.3 Integrity with MAC in Presence of an Attacker

In contrast to CRC, the MAC algorithm is specifically designed to detect manipulations. When an attacker is present in the communication and the integrity is protected with a MAC algorithm, the attacker has a probability of success of $2^{-\frac{mac}{2}}$ only, cf. [15].

The following attacks are possible, cf. Figure 8. The result is depicted in Figure 10:

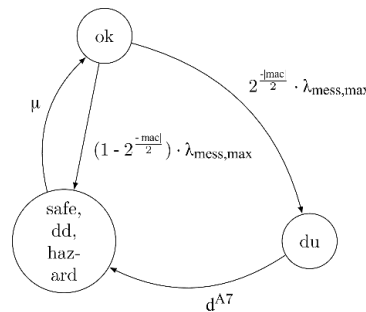


Figure 10. Aggregated Markov model with check algorithm MAC in presence of an attacker.

- A1 Attack changing the message rate:
The technically maximum message rate applies as worst case, i.e. $\lambda_{A1} = \lambda_{mess,max}$ holds.
- A2 Attack concerning the probability of an erroneous message: Each message can be erroneous, i.e. $P_{err}^{A2} = 1$ holds.
- A3 Attack concerning the residual error probability:
The conditional residual error probability $P_{re}^{A3} = 2^{-\frac{mac}{2}}$ as long as the attacker has not compromised the algorithm or the key, respectively.
- A4 Subsequent attack changing the message rate after a previously undetected successful attack:
Since it has to be assumed that the attacker can figure out when he was successful, $\lambda_{A4} = \lambda_{mess,min}$ holds in the worst case.
- A5 Subsequent attack concerning the probability of an erroneous message after a previously undetected

successful attack:

Since the attacker can figure out when he was successful, $P_{\text{err}}^{\text{AS}} = 0$ holds in the worst case.

A6 Subsequent attack concerning the residual error probability after a previously undetected successful attack: It does not play a role since $P_{\text{err}}^{\text{AS}} = 0$ applies in the worst case.

A7 Attack concerning the safety-related demand rate: See A7 in Section 6.1

7 CONCLUSION AND OUTLOOK

Markov models can be used as models for random errors only. But its graphical representation supplies a structure for related attacks that has the chance to be accepted in the safety domain where the Markov model is well known. In order to fulfill both safety and security requirements, the following can be concluded:

- Typical communication models of safety have to be rethought and replaced.
- Parameters of typical safety models are heavily influenceable by attackers (message rate, probability of erroneous messages, absolute and conditional residual error probability, demand rate).
- Two types of safety-related demands should be distinguished: demands initiated by the attacked operational function (d_{Op}) and demands concerning the exposition of humans in the environment of the system under attack (d_{Env}).
- The attacker can change the behavior depending on the state of the system.

Depending on the specific safety requirements, further measures are possible:

- The rate of accepted messages can be limited.
- The repair rate can be limited based on detected errors, that means the system stays in the safe state with increasing time.

Further research and discussions are necessary. A common understanding of the two domains require a comprehensive view, especially whenever security measures are necessary to ensure safety.

8 REFERENCES

1. Pukite J., Pukite P., *Modelling for Reliability Analysis*, IEEE Press Series on Engineering of Complex Computer Systems, 1998.
2. *IEC 61508-1: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*, 2010.
3. *IEC 62443-1-1: Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*, 2009.
4. Wieczorek F., Schiller F., Wolf J., *Security for Fail-Safe Communication in Automation*, Proc. of the 8th Int. Conf. Safety of Industrial Automated Systems (SIAS), 2015, pp. 80-87.
5. Börcsök J., *Funktionale Sicherheit – Grundzüge sicherheitstechnischer Systeme*, VDE Verlag, 2011.
6. Peterson W. W., Weldon E. J., *Error-correcting codes*, 2. Ed, MIT Press, 1972.
7. Schiller F., Mattes T., *An Efficient Method to Evaluate CRC-Polynomials for Safety-Critical Industrial Communication*, Journal of Applied Computer Science, Vol 14, No 1, Technical University Press, Łódź, Poland, 2006, pp. 57-80.
8. Katz J., Lindell Y., *Introduction to Modern Cryptography*, 2. Ed., Taylor & Francis, 2015.
9. Wieczorek F., Krauß C., Schiller F., Eckert C., *Towards secure fieldbus communication*, Proc. of 30th Int. Conf. on Computer Safety, Reliability, and Security, in: Ortmeier, F. and Daniel, P. (Eds.): SAFECOMP 2012, Lecture Notes in Computer Science, LNCS 7612, pp. 149-160, Springer, 2012.
10. Blum M., Schiller F., *Effizienter Entwurf von Sicherheitsfunktionen auf Basis von Mustern*, Proc. of Automation 2008, Düsseldorf, 2008.
11. Hauke M. et al., *Functional safety of machine controls*, BGIA Report 2/2008e, 2008.
12. U. Höfle-Ispording, *Zuverlässigkeitsrechnung*, Springer Berlin Heidelberg, 1978.
13. Schiller F., Mattes T., Weber U., Mattes R., *Undetectable Manipulation of CRC Checksums for Communication and Data Storage*, Proc. of the 3rd ICST Int. Conf. on Communications and Networking in China, CHINACOM'08, 2009.
14. *IEC 61784-3: Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*, 2016.
15. Preneel B., Oorschot P. C., *MDx-MAC and Building Fast MACs from Hash Functions*, Proc. of Advances in Cryptology CRYPTO' 95, Springer Berlin Heidelberg, 1995, pp. 1-14.

An extensive method to analyze impacts of cyber-security on major hazards

Massé F.

Institut national de l'environnement industriel et des risques (INERIS) – Parc Technologique Alata – BP 2 – 60550 Verneuil-en-Halatte – France

francois.masse@ineris.fr

KEYWORDS: Cyberphysical, Major Hazards, process Industry, risk analysis

ABSTRACT

Operators of industrial facilities must be able to control the risks that their installations pose to people or environment. To demonstrate this, they identify the major accident scenarios through preliminary and detailed risk analysis steps, then evaluate the performance of the risk control measures, and finally, risk acceptability in terms of likelihood and severity. The risk analysis methods used are adapted to evaluate accidental events.

Industrial control systems (ICS) include control systems, safety instrumented systems and communication systems. They tend to be increasingly interconnected with the company's information systems and to use technologies derived from IT. They are therefore more vulnerable to cyber-attacks which can potentially generate major hazards for people and the environment. A cyber-attack can be targeted or not, can be internal or external to the targeted industrial site and the means of carrying out future attacks are potentially new and unknown.

INERIS seeks to evaluate the impact of cyber-attacks on ICS in the process industry and particularly the possibility for the attacker to provoke dangerous effects for populations and environment. The approach should be focused on physical effects rather than on ICS vulnerabilities. A first approach, ATBT, consisted to link attack trees and bowtie diagrams (ESREL 2017, Computer and Security 2017). This allows to evaluate the likelihood of accidental and malicious causes of major hazards. This first approach relies on bowtie diagrams developed to assess accidental risks which are not exhaustive for attack scenarios. In this paper, we propose an approach to complete the identification of attack scenarios during the preliminary risk analysis. The aim of this methodology is to bridge the risk analysis related to cyber-attacks of IT and OT systems and risk analysis.

1 INTRODUCTION

The vulnerabilities of industrial control systems (ICS) and safety instrumented systems (SIS) constitute a threat to the safety of industrial installations. These systems may be vulnerable either to targeted malicious attacks or to different types of non-targeted attacks to which open systems on the Internet are exposed (viruses, ransomware, etc.). The convergence between industrial automation technologies (OT) and computer technologies (IT), the use of wireless networks, the interconnection between OT and IT (including office systems and Internet connections) are examples of vulnerabilities that can affect industrial control systems.

Various surveys show the exponential increase in incidents involving industrial systems. These attacks by revengeful employees, criminal organizations, etc. are common but are mainly aimed at stopping or damaging facilities, fraud or extortion. However, the methods used to carry out these attacks can be used to corrupt industrial control systems in such a way as to cause dangerous phenomena for the safety of operators, residents or the environment. These attacks are likely, in the same way as random failures, to cause major accidents. It is therefore necessary to assess and limit the impact of cybersecurity on the control of accidental risks.

The simultaneous handling of these two subjects is complex: the cultures of these two fields are different, the areas of analysis overlap partially (physical process and control command on the one hand, control command system and information systems on the other) but conflicting requirements can therefore emerge from the two analyses.

Various methodological frameworks have been proposed to address both functional safety and cybersecurity or industrial risk management and cybersecurity (SESAMO project, CORAS method). These are mainly methods focusing on the analysis of the control command system and its deviation but don't include the physical risks related to the chemical process.

2 PRESENTATION OF TWO FRAMEWORKS: INDUSTRIAL RISK AND CYBERSECURITY

2.1 Industrial Risks Management in French regulatory Context

2.1.1 Overall Framework

In the French regulatory context, any industrial installation likely to create risks or cause pollution or nuisances, for the safety and health of residents, is a Classified Installation (CI). Different regimes are defined for classified installations, depending on the importance of the risks. The installations presenting the greatest risks – according to the nomenclature of classified installations which sets thresholds according to the substances used or stored on the site and the type of activity - are subject to the authorization regime. For these installations, the operator must apply for an operating permit demonstrating that the risks are under control; the application must be accepted by the authorities before the installation is put into operation.

To demonstrate the acceptability of risks, the operator of a CI carries out a Hazard Study which identifies all hazardous phenomena and major accidents related to the installation that may have effects outside the site, assesses their intensity and severity (distance of effect and number of potentially exposed persons) and their probability of occurrence. The assessment of probability in Hazard Study was introduced in the environmental code by the law of 30 July 2003. Probabilities and severity are estimated according to scales defined in Annex 1 of the Ministerial Order of 29 September 2005. The gravity / probability pair makes it possible to locate the various accidents identified in an acceptability matrix and thus to assess the control of major accident risks for the establishment in question.

The approach used to assess risks in hazard studies follows three main steps:

- a qualitative risk analysis to identify all scenarios and select dangerous phenomena with potential effects outside the site;
- a detailed risk study to quantify these risks in probability and severity;
- risk control measures necessary to keep the risk at an acceptable level are identified and evaluated.

2.1.2 Step 1: qualitative risk analysis

For qualitative analysis, an approach such as Preliminary Hazard Analysis (PHA) or Hazard Operability Analysis (HAZOP) is generally used to identify risks in a systematic way.

Thus, HAZOP is a systematic analysis approach aimed at identifying the risks associated with a process. HAZOP is conducted by a multidisciplinary working group that identifies potential deviations from the physical parameters of the process and identifies their possible causes and consequences for the safety of people, the environment or assets. To facilitate the review, a system is divided into several parts (or nodes) for which the elementary functions can be defined. For each node, the HAZOP study team checks whether each property (PRESSURE, FLOW...) has a deviation that may have undesirable consequences. To identify these deviation, a system of questions with predefined guide words (DO NOT DO, MORE, LESS, REVERSE...) is used. For example, the working group examines the PRESSURE PLUS deviation in the "chemical reactor filling system" node, which includes piping, pumps, valves and instrumentation. It will be tried to determine the causes of this deviation (closing a valve downstream of a compressor), the consequences (bursting of the piping and loss of containment of a flammable substance) and the possible risk control measures (safety function on high pressure, limit switches on the valves, valve...).

Carrying out an HAZOP is a creative process that aims to systematically reviews the random and accidental deviation of a process. It is not intended to analyze several simultaneous deviations. It could be used to consider malicious causes of certain deviations (illegitimate control of the valve downstream of a compressor via the control command PLC, deactivation of the instrumented functions of high pressure safety and valve limit switch). However, the HAZOP format as it is used is not designed for this objective.

Once the main Hazardous Events are identified through PHA or HAZOP, their severity and probability are evaluated through a detailed risk analysis and necessary risk reduction measures are defined. The detailed analysis can be supported and synthesized through method like Bow-Tie diagram.

2.2 Cybersecurity of industrial systems in the French context

In France, regulatory requirements have been applicable to Vital Importance Operators (OIVs) since the last quarter of 2016 through specific decrees based on guides developed by Working Groups on Cybersecurity of Industrial Installations led by ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) which have published 2 documents: "Classification method and main measures" and "detailed measures". These guides define a three-step approach, similar to the approach of the hazard study, that can be applied to any industrial system, OIV or not:

- identification of critical information systems based on a qualitative approach;
- detailed risk analysis for these information systems;
- definition of the security measures applicable to these systems.

These steps are covered by most of risk management methods for information system security.

ANSSI guides focus on assessing the likelihood of attacks. This is the estimate of the likelihood of a threat scenario or risk occurring. It is estimated according to the technologies and functionalities of the systems, their connectivity, the management of the stakeholders and the level of potential attackers. For the assessment of severity, the guide simply presents severity scales for human and environmental impacts and for impacts following the cessation of the service provided (economic impacts). The means of accurately assessing the impacts of an attack and situating them on these scales are not presented in the guide.

The EBIOS method, mainly in use in France, is an example of cyber risk analysis method that can be used to identify and evaluate critical information systems.

2.3 A general risk analysis framework

We are seeking to define a methodology for analyzing major risks for people and environment that integrates cyber-attacks as initiating events. This methodology has to make it possible to:

3. Identify risks: list physical risks to people and environment as comprehensively as possible and rate them in terms of severity
4. Analyze risks: identify attack scenarios leading to the identified risks and rate them in probability or likelihood
5. Assess risks: conclude on the acceptability of the risk, by evaluating the different risk reduction measures and placing the scenarios on a multifactorial acceptability matrix and set requirements for additional or improved risks reduction measures.

This methodology has to apply to industrial processes and their control systems and be, as far as possible, consistent with the general risk analysis framework used for classified installations. Unlike risk analyses conducted for industrial systems, which use experience data as well as past accident analyses to predict the possible causes and frequencies of future accidents, cyberattack risk analyses require considering operating procedures that have never been observed. Indeed, several difficulties arise in the development of the method:

- the type of attackers and their motivations are variable;
- the means of attack are not known: it is not known in advance which systems are most likely to be attacked and the attack procedures are evolving in time;
- the attackers will seek - to the extent of their competence - to bypass existing security;
- evaluating the probability of an attack doesn't really make sense;
- the complexity of the system makes it difficult to analyze exhaustive attack scenarios.

INERIS has therefore developed an analysis methodology focused on targets: knowing the potential effect that can be achieved by attackers, the systems involved (actuators, sensors, controllers) and the physical behaviors of these systems that the attacker will seek to obtain to achieve these objectives will be identified, without evaluating at this step the means of attack used, vulnerabilities exploited and likelihood of the attack. The detailed analysis of the cyber-physical scenarios. The detailed analysis of the scenarios will then focus on their severity, probability for accidental causes and likelihood for cyber causes. To this end, the scenarios will be analyzed by the accident risk analysis teams on the one hand and the cyber risk analysis teams on the other.

Such an analysis requires skills on physical processes and associated risks and also specific skills on cybersecurity control that are not generally integrated into the working groups carrying out HAZOP or PHA. The methodological framework will therefore involve different working groups in the different phases of analysis:

- the working group in charge of evaluating the physical risks of the process, which is also responsible for HAZOP or PHA analyses;
- the working group in charge of the analysis of cybersecurity of the industrial control system.

The Figure 1 below shows the interactions between physical and cyber risk analysis processes. Different information must be exchanged between the two working groups:

(1) The Working Group on Physical Hazards will identify scenarios and low-level elements of the CIM pyramid which may cause damage to people or the environment. These output data will be provided to the working group responsible for evaluating the cybersecurity of the industrial system and will be integrated into their analyses as undesirable events. This working group will then identify the attack scenarios, the different IT and OT systems involved, the existing or necessary security measures and the level of residual risk (likelihood of the attack). This working group will therefore apply the cyber risk analysis method generally used by the organization to major risk scenarios for people and the environment (e.g. EBIOS method).

(2) The likelihood of the attack will then be integrated into a bow tie model integrating random and malicious causes.

(3) Finally, the requirements on risk control measures and safety measures to achieve an acceptable level of risk will be specified and implemented.

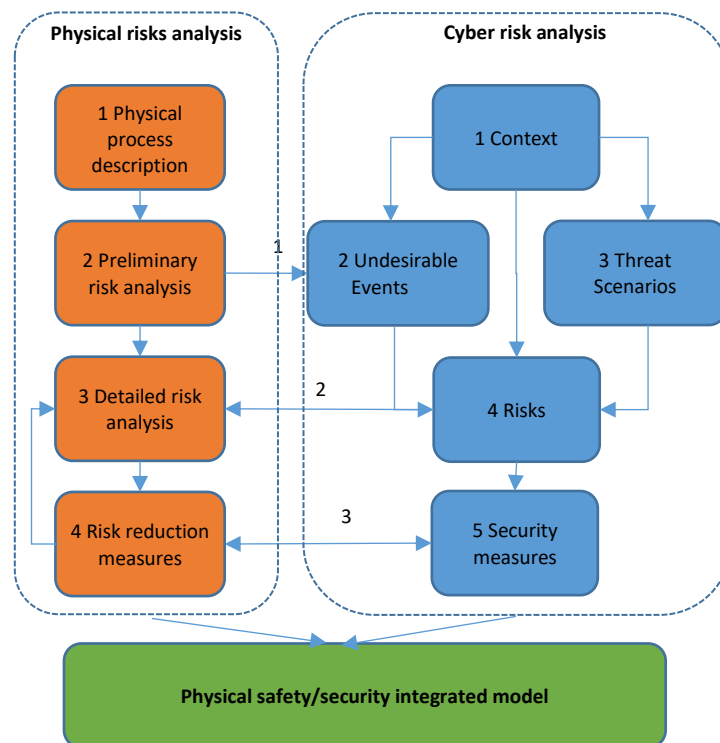


Figure 1. Interactions between accidental and cyber risk analysis.

The cyber risk analysis process is like the EBIOS method presented above with a focus on the undesirable events resulting from the physical risk analysis. It is therefore not presented in more detail in this article.

The consideration of cybersecurity events in the various stages of physical risk analysis is presented below.

3 IMPLEMENTATIONS OF THE METHOD FOR SCENARIOS IDENTIFICATION

This section presents the method developed for preliminary cyber risk analysis. The objective of this preliminary analysis is to identify cyber risk scenarios that will be evaluated during the detailed analysis.

3.1 Motivation, challenges and objectives of the method

The integration of cyber-attacks as major accident initiating events in risk analyses is not obvious: indeed, multiple attack paths on very different systems can be at the origin of the feared scenarios. In addition, an attack scenario can rely on the corruption of several systems simultaneously.

The realization of an inductive analysis, like a FMECA, starting from the different possible types of corruption of each equipment of the industrial control system and identifying their consequences as well as the consequences of the combination of concomitant corruptions of several devices is unrealistic: the programmable devices can be numerous, the modes of corruption varied (unavailability (following a detected anomaly,

corruption or data destruction), modification of thresholds, corruption of orders, modification of variables or measured values, modification of sequences of operations, modification of application software).

A deductive approach, based on undesirable events to identify possible malicious causes, is therefore preferred. The aim is to enrich the creative process, as organized by the PHA and HAZOP methods, by adding the search for malicious causes. To do this, the working group performing the accidental analysis will need a description of the different level 0 and 1 control command systems of the CIM pyramid in interaction with the studied process. When searching for the causes of the various deviations (for HAZOP) or the various feared events (for PHA), it will be necessary to identify data corruption, changes in instructions or control logic or untimely actions by actuators that could lead to these events.

In the context of Hazard Studies of chemical processes, Undesirable Events are defined as the uncontrolled loss of containment of a product (generally liquid or gas). The loss of containment itself can be the source of dangerous phenomena in some cases (explosion, fire, dispersion of toxic substances), in other cases secondary events (e.g. ignition of an explosive gas cloud) may be necessary.

3.2 Typology of hostile actions and first identification of scenarios

We therefore seek to identify for each product present on the site the possible conditions of a loss of containment that could cause a dangerous phenomenon that could affect people or the environment. The conditions for achieving containment losses are of different kinds:

- A: modification of physical parameters (pressure, temperature, flow rate...) by controlling valves, compressors, heating and cooling systems;
- B: dispersion of dangerous substance by overflowing a capacity or opening of emptying devices;
- C: contact of products reacting in a dangerous way;
- D: shutdown of a continuously operating system that maintain the process in a safe state (ventilation, suction, inerting);
- E: modification of the operating sequences (quantities of substances, duration of the different phases, order of operations)

A first identification of these scenarios is made by exploiting the existing PHA made for accidental events. In this PHA it is possible to identify basic events that can be provoked by cyber-attacks and Safety Instrumented functions that can be compromised.

This first identification of scenarios is not sufficient: PHA, as HAZOP, deals with scenarios due to the deviation of a single parameter or the failure of a single equipment or function. The cyber-attacks scenarios should include scenarios due to the modification of several parameters and the simultaneous corruption of several equipment. This is the purpose of the cyber-PHA.

In this approach, following the description of the context and of the dangerous substance on the process, some possible physical attack scenario will be identified. The identification of the scenario will be realized in working group and will be guided by the typology of sources of loss of containment listed above plus to other possible types of attacks:

- F: shutdown or reset of one or several PLC during each phase of operation (with consequences on the position of each actuators);
- G: Modification or disabling of a Safety Instrumented Function (SIF).

3.3 The Cyber-PHA methodology

The cyber-PHA model follows a systematic approach to identify which phenomena are critical, whether there are means to cause these phenomena and whether there are means to detect them or security barriers that will avoid the consequences. The proposed approach is as follows:

3.3.1 Preliminary phase

In this preliminary phase, the description of the installation used for the conventional PHA will be completed by a description of the industrial control system. The industrial process is divided in nodes and for each node, the following elements are described:

- 01- Identification of the different phase of operation;
- 02- Identification of the dangerous substances involved in this node;
- 03- Identification of the physical parameters

- 04- Identification of low level control command control equipment (sensors, PLCs and actuators) acting on this node.

3.3.2 Cyber Physical Scenarios identification

The cyber physical scenarios will be conducted on each node considering their different phase of operations. The different types of scenarios will be reviewed:

- A: Scenarios related to the variation of physical parameters, for each substance:
 - o A1- identification of critical physical parameters;
 - o A2- identification of the existence of control means to exceed these parameters;
- B: Scenarios related to the dispersal or spreading of dangerous substance, for each substance:
 - o B1- Identification of risks related to malicious spreading;
 - o B2- identification of the means (actuators) to carry out this spreading;
- C: Risk related of incompatible mixtures:
 - o C1- Realization of an incompatibility matrix to identify potentially dangerous mixtures;
 - o C2- identification of the means (actuators) to make substance into contact;
- D: Risks related to the corruption of systems maintaining the installation in a safe state:
 - o D1- Identification of these systems (pressure regulation, inerting, temperature regulation);
 - o D2- Analysis of consequence of their disabling or modification of setting points;
- E: Risks related to the modification of the sequence of operations:
 - o E1- Identification of the normal operations sequences;
 - o E2- Analysis of consequence of sequence modification;
- F: Risks related to the shutdown or reset of a logic controller:
 - o F1- Identification of logic controller acting on the node;
 - o F2- Analysis of consequence of reset or shutdown of the controller during each phase of operation;
- F: Risks related to the shutdown or reset of a logic controller:
 - o F1- Identification of logic controller acting on the node;
 - o F2- Analysis of consequence of reset or shutdown of the controller during each phase of operation;
- G: Risks related to the disabling or modification of safety instrumented function (SIF):
 - o G1- Identification of SIF acting on the node and condition of activation;
 - o G2- Analysis of consequence of disabling or modification considering the frequency of their solicitations;
 - o G3- Analysis of the consequences of spurious operation of SIF.

These seven types of physical attacks can be combined. For each node, the working group will define the possible dangerous events, the combination of illegitimate action that can provoke them and the instrumentation and control systems involved in this attack.

For each attack scenario, the detection means and safety barriers and their vulnerability to cyber-attacks will be identified. Some of the measures identified may be not programmable (e.g. valve) and not targeted by cyberattacks.

The working group will also evaluate the possibility to provoke several similar dangerous events simultaneously, for example, fire of several hydrocarbon storage

This will give a description of cyber-physical scenarios which will be studied in detail in the detailed risk study carried on by the cyber risk analysis in one hand and the accidental risk analysis on the other hand. The detailed risk analysis will be merged in an ATBT model as describe in [2].

4 CONCLUSION

The proposed methodology enables integrate cyber security into physical risk analyses and to complete scenarios leading to dangerous effects for people or the environment. Following the identification of the scenarios, a detailed study of the likelihood (malicious attacks), probability (accidental events) and severity can be carried out for each of them. This approach helps to identify critical systems for which protection, monitoring and maintenance procedures are necessary, to set up attack detection systems, or to implement non-programmable security barriers that act on both the physical effects of attacks and accidental phenomena.

5 REFERENCES

1. Abdo H., Flaus J.M., Masse F., *Towards a better industrial risk analysis: A new approach that combines cyber security within safety*. In Safety and Reliability Theory and Applications: Proceedings of ESREL (Portoroz, Slovenia), pages 179–187, 2017.

Session 1 – Functional safety - Information technology

2. Abdo H., Flaus J.M., Masse F., *A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie - combining new version of attack tree with bowtie analysis*, In *Computers & Security*, Volume 72, 2018, Pages 175-195, ISSN 0167-4048.
3. Kriaa S., Pietre-Cambacèdes L., Bouissou M., Halgand Y., *A survey of approaches combining safety and security for industrial control systems*, In *Reliability Engineering & System Safety*, Volume 139, 2015.
4. Masse F., Abdo H., Flaus J.M., *Vers une approche intégrant les exigences de cybersécurité à la maîtrise des risques d'accidents majeurs pour les ICPE*. In *12ème Congrès International Pluridisciplinaire en Qualité, Sécurité de fonctionnement et Développement durable*, Bourges, France 2017.



Session 2-1

Safety of Collaborative Systems

Human-robot coactivity: need's analysis

Tihay D., Perrin N.

Institut national de recherche et de sécurité (INRS) – 1, rue du Morvan – CS 60027 – 54519 Vandœuvre Cedex
– France

david.tihay@inrs.fr
nellie.perrin@inrs.fr

KEYWORDS: robotics, human-robot coactivity, safety, ISO10218-1

ABSTRACT

In view of the mechanical risks they generate, industrial robots are traditionally isolated from humans by physical safety fences. The working areas dedicated to them are therefore identified and delimited, so as not to allow any human action within the areas in which they operate.

Technological developments now enable manufacturers and integrators to propose robotic solutions that no longer include such physical fences between human and robot. Such industrial robotics is said to be "collaborative". One of the main challenges with regard to the human-robot coactivity that is inherent to collaborative industrial robotics is to ensure that such coactivity can be implemented with a sufficient level of safety both for users and for third parties.

This article presents the results of an exploratory survey conducted on users of industrial robotics to gather their needs and their perceptions of the potential contributions of collaborative robotics. These needs come in different forms: workspace sharing, alternated tasks or simultaneous actions. The results show that despite an undeniable interest in collaborative robotics, few companies actually use it today. The frequency of interactions between humans and robots remains low and is often limited merely to workspace sharing. This can be explained by the unavoidable constraints due to human-robot proximity which can sometimes be incompatible with the requirements of production. Industrialists are aware of the new risks associated with these "collaborative" situations and of the need for a prevention approach based both on technical measures and on organizational measures.

1 INTRODUCTION

Robots being used in industry is not new. Indeed, since the mid-1970s, the use of robots has gradually been developing for operations that are basic and repetitive (palletizing, pick & place...), that require large forces (handling and placement of heavy parts, force-fitting...) or that are dangerous (welding operations, adhesive bonding, handling hot parts, or processes generating smoke or dust...). In order to ensure the safety of operators working on or near these often fast and powerful robots, the protection strategy chosen has been to separate the space in which the robot works and moves around from the space in which the operator does by means of physical protections (guards, gratings, etc.). Consequently, in the production phase, interactions between operators and robots are almost non-existent.

Technological progress in various fields – mechanics, electronics, automation and computing - has made it possible gradually to broaden the spectrum of industrial robot applications by entrusting increasingly complex operations to robots [1]. These developments have led to it now being possible to consider "co-activity" between operators and robots, particularly when certain operations require special know-how or decision-making requiring human intervention.

Such robotics is known as "collaborative robotics" and this notion of human-robot collaboration (or coactivity) can be subdivided into three levels according to the desired degree of interaction between the operator and the robot (Figure 1).

Direct collaboration

The operator and the robot are working simultaneously on the same part



Indirect collaboration

The operator and the robot are working on the same part, but they are doing so alternately



Workspace sharing

The operator and the robot are working on different tasks and, sometimes, they have to share their work space



Figure 1. Types of human-robot coactivity [2].

These developments raise issues about the health and safety of employees at work.

Firstly, they increase certain risks because of the desired proximity between the robot and the operators: physical risks if contact occurs, or psychosocial risks when the robot's movements are beyond the command or the understanding of the operators. Standard ISO 10218-1[3] lists the main risks associated with such coactivity. Mechanical risks are numerous and different contact scenarios are envisaged [4]. These may involve direct impact that is unconstrained, partially constrained, or constrained, secondary impact, or crushing in the structure of the robot (Figure 2).

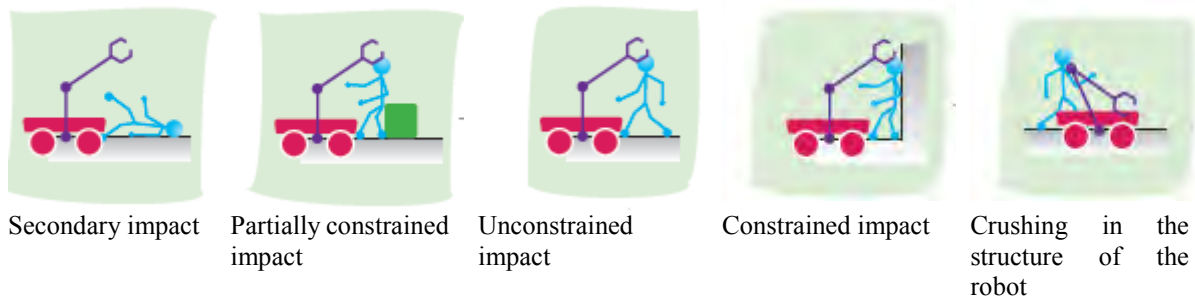


Figure 2. Contact scenarios.

These types of contact can cause injuries by crushing, shearing, impacts, shocks or, depending on the nature of the activity, severing, punctures...

Secondly, these technological developments make it possible to reconsider the above-mentioned protection strategy that is based on the separation of workspaces and that was hitherto applied.

In response to all or some of these issues, Standard NF EN ISO 10218-1 relating to the safety of industrial robots, proposes to implement one or more of the following principles:

- safety-rated monitored stop: the robot must stop when a human is in the collaborative workspace;
- hand guiding: the operator must use an enabling device to allow guided robot movement;
- speed and separation monitoring: when the operator is in the robot's workspace, the robot must maintain a determined speed and stay a separation distance away from the operator, in order to avoid any collision;
- power and force limitation: force reduction mechanisms must be integrated into the robot, in order to reduce the intensity of potential contact between human and robot.

Nowadays, manufacturers propose collaborative robotics solutions that implement these principles to industrialists. In view of the diversity of the solutions on offer and in view of the safety challenges, it is important to ensure that the proposed solutions genuinely meet the needs of the industrial robot users. This is what we tried to determine by asking them about their needs and their perception of the potential contribution of collaborative robotics.

2 METHODOLOGY

In order to identify the needs of industrial users in terms of human-robot coactivity, we decided to meet some of them in their facilities and to interview them. This method of collecting information was preferred to sending a questionnaire by post or by a mail shot. Experience shows that the number of returns often remains low and that the content of the information gathered is less rich than that obtained during an interview [5].

Within the same company, work situations involving robots can be very varied. It was therefore decided, during a preliminary exchange with the volunteer company, to identify precisely the situations that would be analyzed. This choice concerns not only the robot cell to be looked at but also the person to be interviewed who must necessarily have an operational role with the cell: operator, production manager, maintenance technician, etc. Without aiming to be exhaustive, this identification of work situations and the identification of interviewees were oriented in order to cover the broadest possible range of different sectors of activity, fields of application and profiles of interviewees.

In order not to restrict the interviewee to a choice among a few proposals and to avoid any hierarchical pressure, it was decided to set up individual semi-directive interviews. This kind of interview gives the interviewee complete freedom of expression [6]. The interview was structured around three themes addressed chronologically:

Analysis of the existing situation: through open-ended questions on functional and technical aspects, the objective of this first part was to get the interviewee to assess whether the characteristics of the robot cell were sufficient and appropriate to meet the production needs. If necessary, the limitations or constraints of the position were evoked, as well as possible ways of improvement. At this stage of the interview, the notion of coactivity was not mentioned by the interviewers, but could be spontaneously mentioned by the interviewee.

Identification of coactivity needs: during this second part of the interview, the notion of "coactivity" was discussed. The interviewees were asked to consider the robotic cell without any physical fence. They were asked whether and how they thought such a development could be of interest and about the nature of the coactivity they would like to see. The goal was to evoke an "ideal" situation without preconceptions. They were also asked to think about the limits and potential risks inherent to this new work situation.

Potential contributions of collaborative robotics: during this last part, the various different safety principles of standard NF EN ISO 10218-1: 2011 were presented to the interviewee. The means of protection to be implemented were mentioned together with their limitations (reduced speed for example). After discussing the benefits of these safety principles with the interviewee, he or she was asked to determine whether one or more of them might meet those needs.

At the end of each of these three phases, the interviewees were asked to evaluate, using a graduated scale from 1 (not at all satisfied) to 10 (very satisfied), their satisfaction with the corresponding work situations: current situation, situation with coactivity but without constraints, and situation with coactivity and taking into account the constraints associated with the safety principles of the NF EN ISO 10218-1 standard.

3 NEED'S ANALYS

More than 150 companies likely to join our panel were solicited by e-mail. Ultimately, 21 companies agreed to participate in this exploratory survey. They were of various sizes (very small enterprises, small and medium-sized enterprises, and large enterprises) and covered the main sectors of activity listed by the IFR (International Federation of Robotics) as users of industrial robots [7]. Forty-two people were asked about their needs in 27 different work situations at individual and semi-structured interviews.

Almost two thirds of respondents (64%) expressed a potential interest in human-robot coactivity (Figure 3).

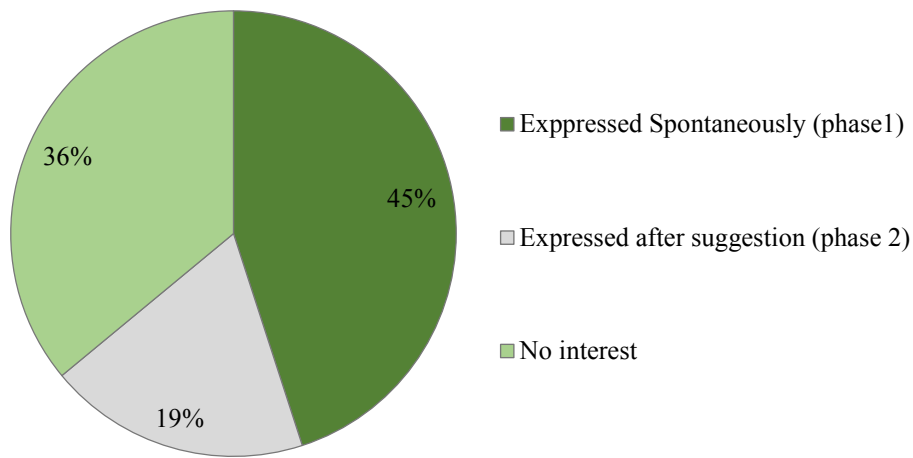


Figure 3. Expression of the need for human-robot coactivity.

In the first phase of the interview, 45% of them even mentioned it spontaneously as a way of improving the analyzed situation. Seven of them had already taken the plunge and had a collaborative robot. The needs as they were expressed more specifically are itemized in Table 1.

Table 1. Summary of human-robot coactivity needs.

Needs for human-robot coactivity	Breakdown of needs
Facilitate maintenance operations	28%
Facilitate process-related operations close to the robot	18%
Facilitate integration of the robot cell	15%
Reduce MSD risks	9%
Solve technical issues	9%
Technology showcase	9%
Facilitate setting and adjustment operations	6%
Increase mobility and reuse of the robot	6%

All these expectations are mainly aimed at improving the company's productivity and flexibility. Only items 4 (reducing musculoskeletal disorders) and 6 (technology showcase) transcribe other objectives. Although the coactivity needs expressed are numerous and varied, it is possible to group them together according to the three types of coactivity previously defined (Figure 4).

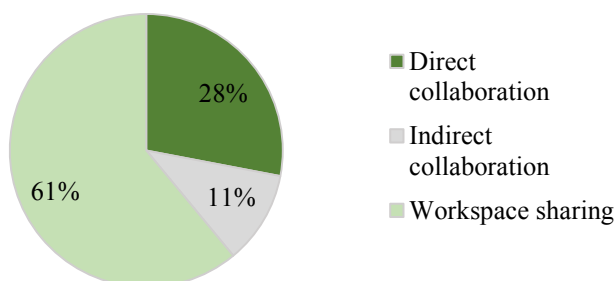


Figure 4. Types of coactivity.

The survey also shows that a very large majority of respondents (90%) are naturally aware of the risks associated with the proximity between the operator and the robot (Figure 5). The risks of impacts and collisions with the robot

are cited by 45% of respondents. Psychosocial risks are then mentioned in 25% of cases. This mainly concerns the stress that could be generated by the presence of a moving robot near the operator. Next, 13% mentioned risks related to projection or falling of the part handled by the robot. In 8% of cases, users identify risks of pinching or crushing. Other more specific risks related directly to the envisaged application were also mentioned, for example, the risks of burns and exposure to dust or smoke.

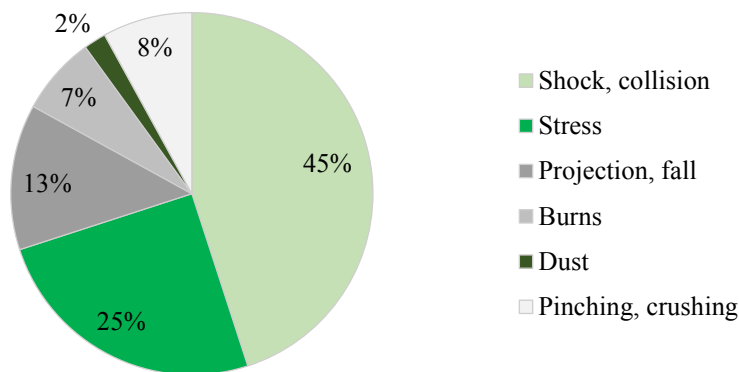


Figure 5. Identified risks.

After presentation and explanation of the safety principles proposed by standard NF EN ISO 10218-1, the main concerns expressed during the interviews regarding their implementation were:

- speed or payload reduction, in order to reduce the robot's stopping time and thus avoid human-robot contact or reduce its effects. Speed reduction is often incompatible with the cycle times imposed by production. Similarly, the limited payload is often insufficient, compared to the mass of the tools and parts to be handled;
- increased safety distances due to the removal of physical fences around the cell. The reduction in floor space or "footprint" required by manufacturers is not always achievable;
- loss of productivity due to untimely stops or slowdowns of the robot due to the absence of physical fences and to the proximity of operators or third parties moving around the cell.

Despite these concerns, manufacturers believe that the implementation principles proposed by the NF EN ISO 10218-1 standard allow them to meet their expectations. They mention specifically:

- safety-rated monitored stop: It is the opportunity to restart without operator action that seems to be the feature of most interest to those interviewed. Some of them are even considering using this mode, while keeping the physical fences around the robot so they do not have to increase the safety distances;
- power and force limitation. This mode is considered more for maintenance phases, in addition to other means of protection, rather than for production phases, because it imposes reduced speeds and limited loads, which may limit the scope of possible applications.

If we consider that for the interviewees, the potential contribution of "collaborative robotics" can be evaluated by the difference between the satisfaction levels expressed at the end of themes No. 1 ("current situation") and No. 3 ("coactivity + safety principles"), we note that this contribution can be perceived as very positive (+9) or very negative (-9) depending on the situations (Figure 6).

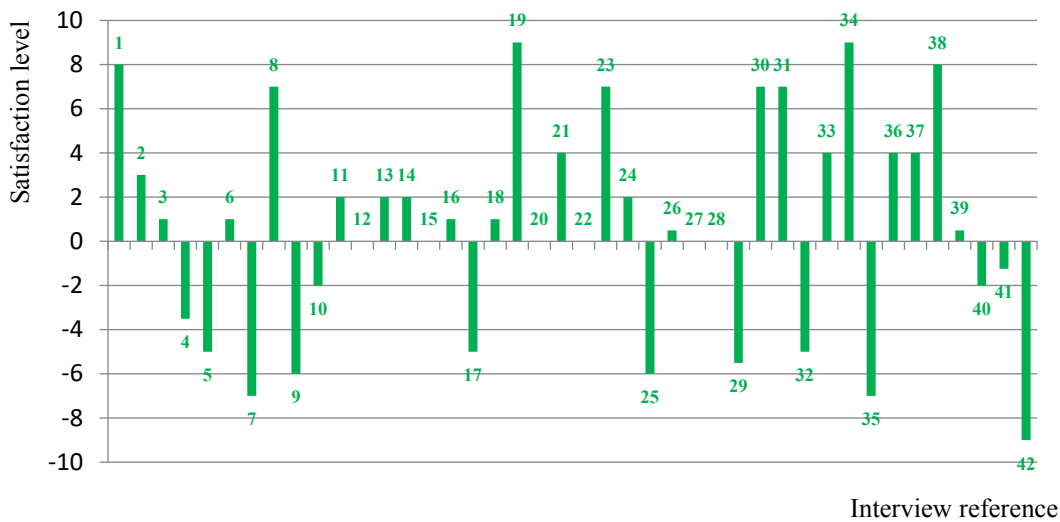


Figure 6. Potential contribution of collaborative robotics.

Several hypotheses can be put forward to explain these considerable variations in the evaluation of the contribution of collaborative robotics: the type of coactivity desired, the nature of the operation performed by the robot or the function of the person interviewed.

Type of coactivity

There is indeed a difference in perception of the contribution of collaborative robotics depending on the type of coactivity (Table 2). Thus, this contribution is considered twice as significant when the user is considering direct collaboration (50%) or sharing workspace (42%) compared to indirect collaboration (20% of responses). This can be explained by the fact that, in this type of coactivity, the need for collaboration is less pronounced than in the other two and that, as a result, the user seems less willing to accept the limitations or constraints associated with collaborative robotics.

Table 2. Contribution of collaborative robotics according to the type of coactivity.

Type of coactivity	Positive contribution	Uncertain contribution	Negative contribution
Direct collaboration	50%	25%	25%
Indirect collaboration	20%	40%	40%
Workspace sharing	42%	31%	27%

Nature of the operations performed by the robot

The different work situations analyzed were classified into four categories: handling, machining/welding, assembly and inspection. The average contribution of collaborative robotics, although positive overall, is to be considered as uncertain. Only in the case of inspection operations, is it perceived, overall, as positive (Figure 7).

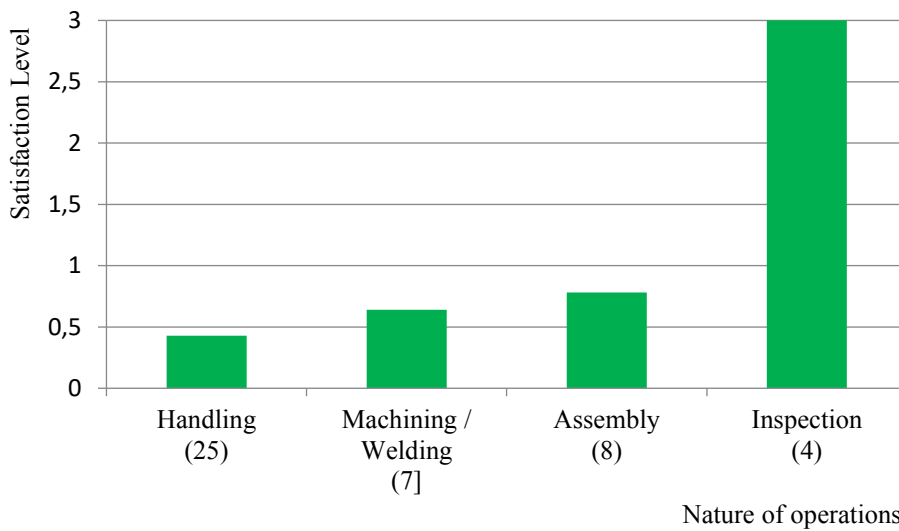


Figure 7. Evaluation of the contribution of collaborative robotics according to the nature of the operations.

Interviewees’ functions

In Figure 8, it can be seen that only people working in industrialization-related functions (methods) express a slightly positive overall interest in collaborative robotics. On the other hand, those in charge of production consider that the contribution is rather negative. These differences can be explained by different expectations: potential gains in operating methods, gains in flexibility or production on the one hand, and technical difficulties and/or additional risks on the other. For the other functions, the contribution is uncertain.

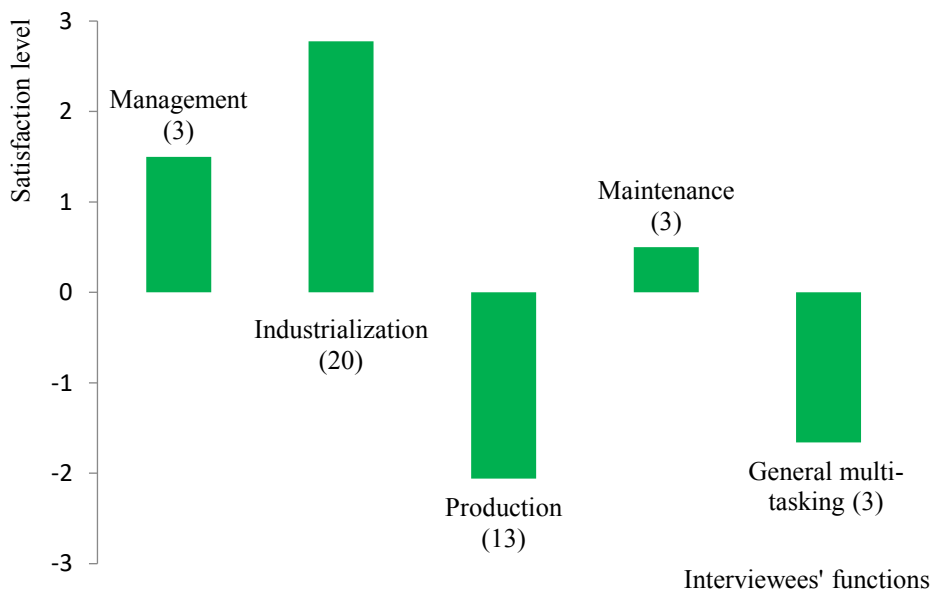


Figure 8. Evaluation of the contribution of collaborative robotics according to the interviewee’s functions.

These results clearly illustrate the comments made during interviews with manufacturers, only 40% of whom declare themselves ready to use collaborative robotics. Nevertheless, the majority of the industrialists surveyed who already own robots with collaborative functions (7 of them) say they are quite satisfied and rate the contribution positively at 4.8. However, it should be noted that, for two of them, the limitations and constraints linked to coactivity were considered to be prohibitive, and led to the implementation of a "conventional" industrial robotic cell.

4 CONCLUSIONS AND OUTLOOKS

First of all, this survey, carried out on a limited but representative sample of industrial robot users, revealed their interest in human-robot coactivity. As soon as the company was contacted, the subject raised many questions and the industrialists shared their experiences with us. During the interviews, this resulted in various needs being expressed whose main objectives are:

- productivity gain: process optimization, mitigation of technical problems... ;
- gain in flexibility: ease of robot integration, robot mobility and reuse, increased reactivity to change, easier line adaptation... ;
- improved working conditions.

However, not everyone plans to use collaborative robotics, because of:

- the risks inherent to coactivity that are sometimes considered as difficult to reduce or even unacceptable;
- the constraints associated with the proposed safety elements that may be incompatible with the process (speed, payload, etc.) and sometimes even counter-productive (risks of untimely stops of the robot due to the presence of operators in its close environment).

This shows that manufacturers are generally aware that the use of collaborative robotics cannot be envisaged without, on the one hand, a "functional" analysis in order to ensure the relevance of the solution, with regard to implementation and production constraints and, on the other hand, a risk analysis specific to the cell concerned. Although the needs expressed are generally covered by the methods of collaboration proposed by standardization, there are still few technological solutions available for implementing them, and much research & development work is still being carried out in order to develop protective devices allowing easier implementation of this type of installation and thus ensuring the health and safety of employees working near robots.

5 REFERENCES

1. CHARPENTIER P., SGHAIER A., L'homme au travail et le robot : une relation à inventer. Hygiène et sécurité du travail, 2013, n° 231, VP1, pp. 84-88.
2. Ministère du Travail, Guide de prévention à destination des fabricants et des utilisateurs pour la mise en œuvre des applications collaboratives robotisées. 2017, 50 p. http://travail-emploi.gouv.fr/IMG/pdf/guide_de_prevention_25_aout_2017.pdf
3. NF EN ISO 10218-1 - Exigences de sécurité pour les robots industriels – Robots et dispositifs robotiques - Partie 1 : Robots. Paris, AFNOR, 2011, 45 p.
4. VASIC B., BILLARD A. – Safety issues in human-robot interactions. In : robotics and automation, IEEE, 2013, 8p.
5. IMBERT G. - L'entretien semi-directif : à la frontière de la santé publique et de l'anthropologie, 2010, 102 p.
6. FENNETEAU H. - L'enquête : entretien et questionnaire. Paris, Dunod, 2015.
7. International Federation of Robotics – Executive summary, 2017, 10 p. Accessible on: https://ifr.org/downloads/press/Executive_Summary_WR_2017_Industrial_Robots.pdf

Of the necessity of a uniform measurement procedure for the determination of the threshold values listed in ISO TS 15066

Pilz T.

Pilz GmbH & Co. KG - Felix-Wankel-Straße 2 - D-73760 Ostfildern – Germany

t.pilz@pilz.de

In the paper the writer identifies the necessity of amending TS 15066 with a test procedure to be followed in order to come to reproducible measurement results.

Since the release of TS15066 the threshold values have been in the center of criticism. Meeting the pressure requirements often results in processes where the robotic application is forced to be so slow that it becomes unattractive to implement method 4 HRC applications. Consultants working in the field of CE marking applications do get challenged if their measurements are accurate. Users hope by changing the engineering company conducting the measurement brings them the desired results. This is possible because TS15066 does give no guidance on how the test set up has to be arranged and what procedure has to be applied.

Furthermore there is no industry consensus how a free push is to be measured. Voices become louder, that instead of measurement a calculation based on information of the manufacturer would be better. While this is a viable way for the design of the machine the validation of the application still does require measurement.

While the Maintenance of ISO 10218-1 and 10218-2 has started speed is of the essence since it is the goal to transform what is known as TS5066 into their ISO 10218 series of standards. While it is currently unclear if it becomes a part 3 or is included in part 2 it is evident, that without a mandatory measurement procedure reproducible and comparable results can not be produced. This however is necessary to get industry acceptance.

In the end the balance between safety of the worker and productivity of the line needs to be found and one way to get there is to bring the expert know how in how to set up a measurement and how to determine the values is standardized. This will allow for CE conform HRC applications which in return will lead to safe HRC Method 4 applications that meet productivity and safety requirements.

Object Recognition for Safety Applications using Ultrasonic Holography

Kirfel A.¹, Ostermann B.², Scheer T.¹, Jung N.¹

¹ Safety and Security Research Institute (ISF), Bonn-Rhein-Sieg University of Applied Sciences Grantham-Allee 20 - 53757 Sankt Augustin - Germany

² Institute for Occupational Safety and Health (IFA) Alte Heerstr. 111 - 53757 Sankt Augustin – Germany

alexander.kirfel@h-brs.de

bjorn.ostermann@dguv.de

tobias.scheer@h-brs.de

norbert.jung@h-brs.de

KEYWORDS: ultrasonic sensor; holography; human-robot collaboration; machine learning

ABSTRACT

Entering the work envelope of an industrial robot can result in serious injury from collisions with moving parts. The danger zone of these machines is therefore commonly enclosed in physical barriers, such as walls and fences, or virtual barriers based on non-contact protective devices, which includes light curtains and laser scanners.

In human-robot collaboration (HRC), human and machine complement one another by working in close proximity to each other. Since traditional access restriction methods cannot be applied to ensure the safety of collaboration workers, there is a growing demand for sensor systems which safely and reliably detect human body parts amidst working material and other objects. Although camera-based systems are becoming increasingly well-suited for this type of application, safety concerns remain, owing to possible detection failure in adverse lighting conditions or due to occlusion. A possible solution to this problem could be the use of additional ultrasonic sensors for physical diversity. However, conventional ultrasonic proximity sensors do not provide adequate information to discern different objects reliably in typical collaboration scenarios.

This work investigates a new approach to identify and distinguish relevant objects from human body parts based on acoustic holography. The approach is experimentally validated using a low-cost, application-specific ultrasonic sensor system made from micro-electromechanical systems (MEMS). As shown by the results, this system outperforms conventional ultrasonic sensors in terms of lateral resolution and could allow for more intelligent muting techniques without compromising safety. A next step could be the system's integration into a multimodal sensor system which combines the advantages of optical and ultrasonic technology.

1 INTRODUCTION

A major difficulty in human-robot-collaboration is to safely distinguish human body parts from workpieces and other objects. Near infrared (NIR) skin detection [1] offers a promising solution, but like any other optical system, can fail when exposed to extraneous light or dusty environments. Ultrasound is a physically diverse technology which could further improve the safety under such difficult conditions. By attaching a large number of ultrasonic proximity sensors to the surface of an industrial robot, nearby sound reflecting surfaces can be reliably detected [2]. This way, the robot can maintain a safe distance to the collaboration worker. However, the robot's availability can be negatively impacted, as it is practically impossible to distinguish the worker from other objects. This work attempts to provide a solution to this problem based on non-contact ultrasonic holography.

2 HOLOGRAPHY

Holography (Greek *holos* = whole, complete, *graphein* = to write) is a technique for recording and restoring the whole field distribution of coherent wave fields. Physically, a hologram is an interference figure which was recorded of a stationary interference pattern between an object wave and a mutually coherent reference wave. The hologram's interference fringes encode both the object wave's amplitude and phase. In conjunction, these two pieces of information completely determine the wave field within and beyond the hologram plane. Holograms therefore contain complete information on three-dimensional object shape and location. Unlike projection-based imaging techniques, holography does not require passive or active wave-guiding or beam-shaping devices, such

as lenses in a camera. Although holography was initially formulated for optical waves, it is basically free of assumptions regarding the physical nature of this linear wave phenomenon. Consequently, the holographic principles also apply to ultrasound without loss of generality.

To access the information stored in a hologram, the original wave field must be reconstructed. Analog holograms, for example recordings on photographic film, are reconstructed physically. For this, the hologram is subjected to a suitable reconstruction wave, on which the hologram acts like a diffraction grating, modulating the information encoded in its interference fringes onto the outgoing diffraction wave. This interaction with the hologram causes the first and negative first diffraction order to resemble the original object wave. Under certain conditions, an observer can experience the reconstructed wave field much like the original one, including perspective and depth of field.

This work's focus is on digital holograms, which are subject to the same basic principles as their analogue counterparts. Since digital holograms have no physical form they require numerical reconstruction. The diffraction theory of Fresnel and Kirchoff [3] provides the theoretical basis for this, as it explains the formation and propagation of diffraction waves at and beyond finite apertures.

2.1 Hologram recording

The incident sound pressure must be measured at points less than half the shortest possible trace wavelength apart to avoid imaging artifacts and low contrast due to spatial undersampling. Two complementary conditions were formulated which provide estimates of the shortest possible measuring distance z_0 for an object with size d_y along the y -axis. The same conditions apply to the x -axis.

$$z_0(d_0) > \frac{\Delta y}{\lambda} (d_y + N\Delta y) \quad (2.1)$$

$$z_0(d_0) > \frac{\Delta y}{\lambda} (d_y - N\Delta y) \quad (2.2)$$

The *strong sampling condition*, Equation 2.1, allows for maximum image quality by ensuring proper sampling of each partial reflection across the entire aperture. In practice, this condition can be difficult to satisfy when attempting to image large objects at close distances. For such cases, the *weak sampling condition*, Equation 2.2, is a first estimate of whether a particular configuration could still produce images, albeit with more or less severe quality degradation.

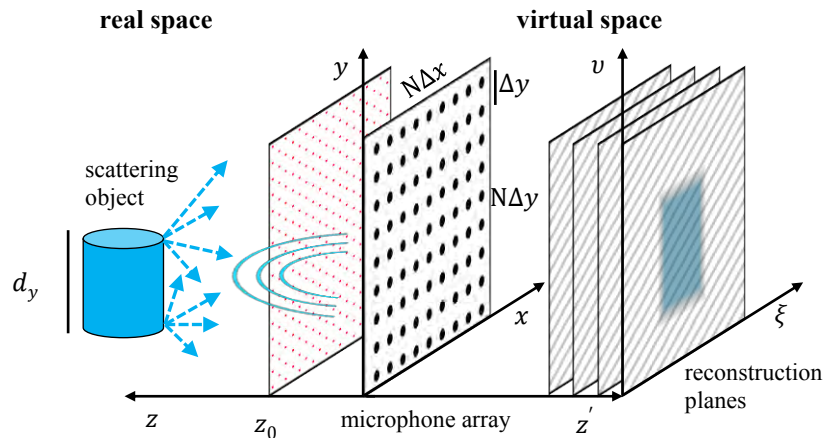


Figure 1. System setup for ultrasonic hologram recording and reconstruction

2.2 Numerical reconstruction

In optical holography, the size of the aperture and the distance to the imaged object is usually several orders of magnitude larger than the recording wavelength. Without a coupling agent similar proportions cannot be practically achieved for airborne ultrasound. There are multiple approaches to reconstruct a digital hologram, including the convolution approach, the Fraunhofer approximation and the Fresnel approximation. For the sensor system presented here the Fresnel approximation was the most suitable option. On the one hand a system which satisfies the Fraunhofer approximation was impossible to design. On the other hand the convolution approach would limit the field of view to the size of the aperture, which due to practical reasons was not desired.

Session 2-1 – Safety of collaborative systems

The holograms with $N \times N$ pixels sized $\Delta x \times \Delta y$ were evaluated at the grid points of an equidistant grid, with edge length $N\Delta x \times N\Delta y$. Due to the properties of the Fresnel approximation the reconstruction was performed at the diffraction-limited resolution of the hologram by default [3]. Consequently, the images also had exactly $N \times N$ equally large pixels, with size $\Delta \xi \times \Delta \nu$. The resulting field of view, Equation 2.3, would therefore increase naturally with reconstruction distance z at a given wavelength λ

$$N\Delta \xi \times N\Delta \nu = \frac{\lambda z}{\Delta x} \times \frac{\lambda z}{\Delta y} \quad (2.3)$$

Equation 2.4 provides the discretized reconstruction formula which was implemented in the system, where $H(n'\Delta x, m'\Delta y)$ is the acoustic hologram and $R^*(n'\Delta x, m'\Delta y)$ represents a suitable reconstruction wave. $F^{-1}\{\}$ denotes an inverse discrete Fourier transform (iDFT).

$$\Psi(n\Delta \xi, m\Delta \nu, z) = \frac{j}{\lambda z} e^{-jkz} e^{j\pi\lambda z \left(\frac{n^2}{N^2\Delta x^2} + \frac{m^2}{N^2\Delta y^2} \right)} F^{-1} \left\{ \sum_{n'=0}^{N-1} \sum_{m'=0}^{N-1} (HR^*) e^{j\frac{\pi}{\lambda z} (n'^2 \Delta x^2 + m'^2 \Delta y^2)} \right\} \quad (2.4)$$

The discrete coordinate transform, Equation 2.5, was defined to account for false pixel coordinates due to image scaling in the reconstruction plane. This retroactively corrects reconstructions at scaling factors β unequal to one.

$$f_{\text{shift}}^{-1} : (n\Delta \xi, m\Delta \nu, z) \mapsto \left(\left\{ \left[n + \frac{N}{2} \left(1 - \frac{N\Delta x^2}{\lambda z} \right) \right] \bmod N \right\} \cdot \Delta x \right)^T \quad (2.5)$$

Figure 2 shows examples of synthetically generated holograms with two different wavelengths after reconstruction. While in Subfigure a) no correction was required since β equals one, Subfigures b) and c) show images of the same object at β unequal to one before and after correction, respectively. Also note the difference in field of view between a) and c) due to dissimilar wavelengths. The same zoom-effect occurs when changing the reconstruction distance.

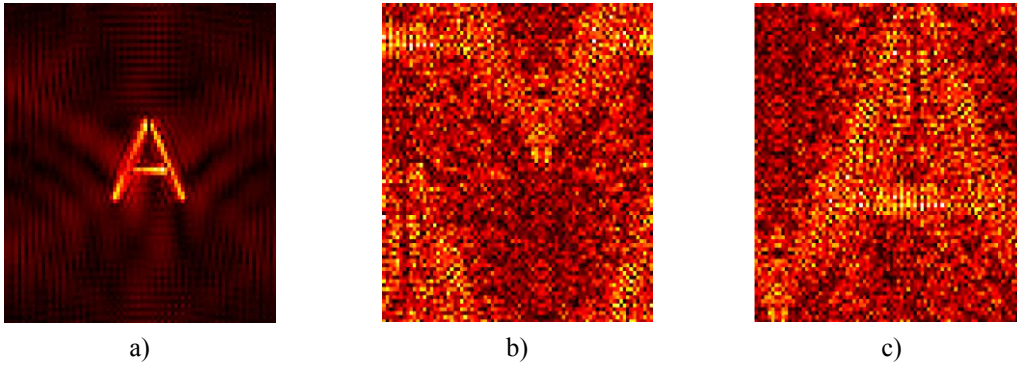


Figure 2. Numerical reconstruction

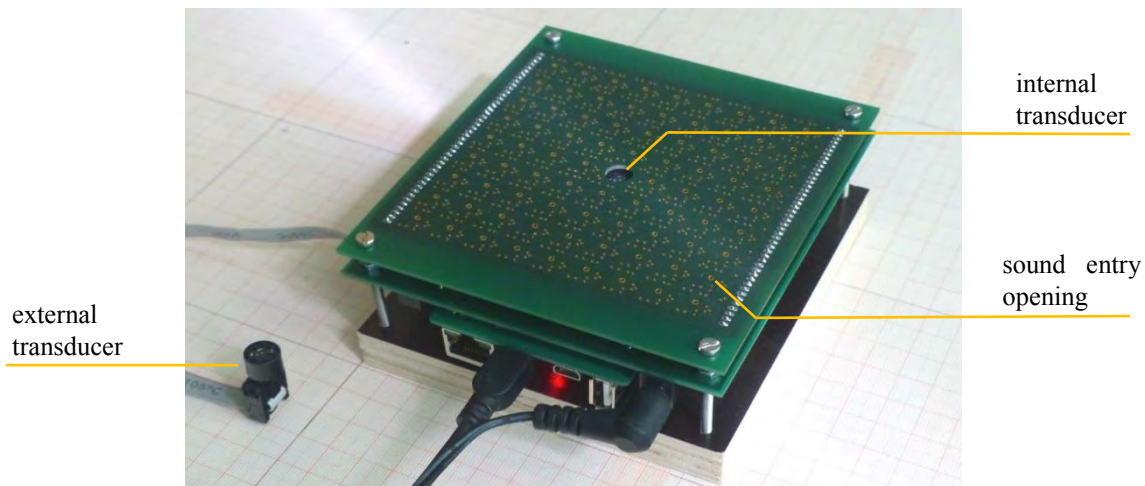


Figure 3. Demonstrator for recording ultrasonic holograms

3 DEMONSTRATOR

In order to test the holographic approach in practice, a demonstrator was developed for recording ultrasonic holograms of representative objects including human body parts.

3.1 System setup

Based on the aforementioned considerations, the demonstrator uses a 9x9 sensor array with equidistant 10mm line spacing. The array consists of 80 bottom-port MEMS microphones with ultrasonic bandwidth plus a single narrowband piezo transducer for acoustic illumination, with wide radiation characteristics at 40 kHz center frequency. Alternatively, the system can be equipped with an external transducer to enhance imaging performance by recording from synthetic apertures. The microphone selection was based on low cost, small footprint and good sensitivity at ultrasonic frequencies. Furthermore, MEMS microphones provide for almost ideal sampling points due their small sound entry opening.

3.2 Principle of operation

Ultrasonic imaging is achieved by emitting short ultrasonic wavetrains, which partially backscatter at objects. The resulting echos are picked up by the sensor matrix as location-dependent time-pressure curves, converted into digital pulse-density modulated soundstreams and buffered directly into separate SRAM modules. This way, the echo can be recorded on all 80 microphones simultaneously. When the echo subsides, each row of SRAMs is read in parallel, having its data transferred to a PC for further signal processing. A login amplifier tuned to the transducer's central frequency [4] detects the local pressure amplitude and phase at each microphone location. As the hologram contains explicit phase information, a reference wave for recording is rendered superfluous.

To capture good quality holograms, the echo is recorded during the particular timeframe in which the echo wave field is sufficiently stable and also contains the backscatter from every position in the object plane. The timeframe is therefore chosen dynamically as a function of object distance, size of the aperture and ultrasonic pulse length. Potential crosstalk between transducer and microphones is prevented by delaying the recording by the transmission length plus the maximum acoustic propagation delay of the particular system configuration. Meanwhile, the amplitude and phase accuracy of the hologram is maximized by targeting the longest transmission time for which there is no superposition between the outgoing and returning sound waves.

4 EXPERIMENTAL RESULTS

In order to characterize the system for collaboration scenarios, two series of tests were carried out. In the first series, attempts were made to recognize objects and potentially dangerous situations by means of machine-based learning, whereas in the second series the general viability of airborne ultrasound as an imaging modality was investigated.

4.1 Object recognition

It is well known from a range of applications, including medical and non-destructive testing, that structure-borne ultrasound can distinguish different materials. Since airborne ultrasound is reflected back at the surface of most solid materials, non-contact material recognition by ultrasound is not yet practically feasible. Consequently, the presented sensor system was used to investigate the possibilities of a shape-based, rather than a material-based, object recognition.

A neural network was trained to classify four differently shaped objects in terms of object type and position. The objects were placed in certain spots on a flat surface representing the collaboration area. For each combination of object and position a sequence of reconstructed images was recorded and fed to the neural network. After a few iterations the network learned to suppress measurement noise and could reliably identify and locate the objects in their trained positions. To avoid overly optimistic results due to classifier overfitting, training and testing was conducted on separately recorded datasets. For comparison reasons, the procedure was repeated for a J48 decision tree [5], which is the open source Java implementation of the C4.5 algorithm in WEKA [6]. The decision tree fell short of the neural network's accuracy and was more susceptible to deviations between training and test data. In return, it was trained within seconds instead of minutes or hours for training the neural network.

Unfortunately, it might not be realistic to account for any situation that could occur in a collaboration scenario. Since the classifiers exhibited tight tolerances for an accurate object placement, they were likely to fail if an object was misplaced, an unknown object was presented or the demonstrator was positioned different from the training process. While this behavior may not apply to a constantly changing environment, it could still be utilized to detect potentially dangerous situations in a predefined workflow. For validation, the classifiers were expanded by a fallback class to which they were trained to resort when encountering unknown scenarios. This way, the system would no longer fail randomly and identify the situation as potentially dangerous, when presented a human hand, any other human body part or unknown objects. In practice this behavior could be used to trigger a subsequent safety function.

4.2 Non-contact ultrasonic imaging

In the described reconstruction approach, image size is determined by the number of microphones on the aperture and image resolution improves with increasing aperture size. Larger sized apertures therefore provide more detailed images at the same microphone density.

To circumvent the limitations of the demonstrator's small aperture, higher resolution images were recorded from synthetic apertures with the same microphone density, but 5x5 times the size. The system was switched to the external transducer, so the sensor array could be moved independently. By keeping the transducer at a fixed position, virtually the same field distribution could be recorded on a larger aperture. Figure 4 shows an exemplary complex-valued hologram, recorded of a human arm at 0.75m distance by its amplitude a) and phase b). The resulting image is displayed in Subfigure c). The hand was directly exposed to the ultrasound and therefore appears much brighter than the forearm which was covered in clothing. Along the length of the arm only the weak sampling condition was met, whereas width-wise the strong sampling condition was satisfied. Consequently, artifacts occurred mostly at the fingers and much less to the left and right of the arm.

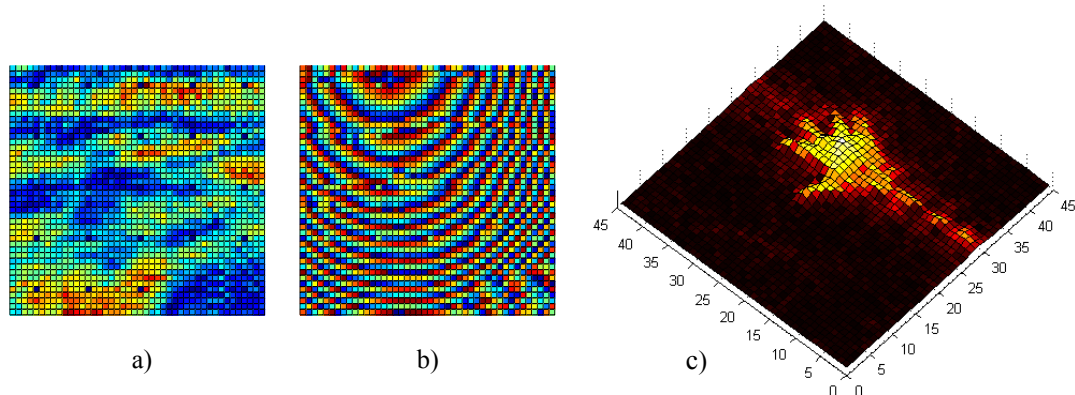


Figure 4. Non-contact ultrasonic imaging

5 DISCUSSION

In this work a non-contact imaging system based on airborne ultrasound was presented. The system was used to successfully recognize objects by their shape and to provide images that are intuitively understandable for humans. However, the experiments also revealed a number of drawbacks in using airborne ultrasound for imaging which will be discussed in this chapter.

First, the images generally had low contrast, with a maximum dynamic range of around 20dB. Furthermore, the image quality would quickly deteriorate due to specular reflections which cause information loss in the hologram. This became particularly evident for objects with large flat surfaces. It was possible to mitigate this problem by taking a series of holograms with different ultrasonic illumination which was merged into a single hologram prior to reconstruction. While these holograms usually contained more complete information about the object, some parts of the object could still be underrepresented or missing from the image. An example for this would be the fingers in Figure 4, which miss their fingertips due to a low geometric backscatter coefficient at this wavelength for an object this size.

Furthermore it should be noted, that only static scenarios without movement were investigated. Movement of the sensor or the object could potentially induce additional motion artifacts into the hologram, which would further degrade image quality. However, this type of artifact is common for all imaging modalities and will not be further discussed in this work.

6 CONCLUSION

While this work demonstrated the principle of operation, there is still room for improvement in practical scenarios. First, it became evident that the hologram quality could be improved by using several transducers for a better optimized acoustic illumination. Second, image size and resolution were limited by the low amount of microphones and the chosen ultrasonic frequency. A further increase in frequency would be beneficial, as the microphones could be arranged more densely for either smaller apertures without sacrificing resolution or higher resolution with similarly sized apertures. In theory, it should be possible to increase the frequency to around 400 - 500 kHz, i.e. by one order of magnitude. Even higher frequencies are not practically feasible due to a steep increase in atmospheric attenuation [7], which would severely limit the working distance of the sensor system. By increasing the ultrasound frequency and microphone density, comparable images could be possible for non-synthetic apertures the size of the presented demonstrator. However, this would require a different microphone with much smaller outer dimensions and suitable frequency response, which is currently not available at a reasonable cost.

7 REFERENCES

1. Sporrer, S. et al., *NIR camera based person detection in the working range of industrial robots*, Proc. Int. Conf. on Safety of Industrial Automated Systems (SIAS), 2015.
2. Ostermann B. *Entwicklung eines Konzepts zur sicheren Personenerfassung als Schutzeinrichtung an kollaborierenden Robotern*, Wuppertal, 2014, Available: <http://nbn-resolving.org/urn/resolver.pl?urn=urn%3Anbn%3Ade%3Ahbz%3A468-20140702-113540-2> [Accessed on 10.09.2018]
3. Schnars U., Jueptner W. *Digital Holography*, Berlin: Springer-Verlag, 2005
4. Orozco, L., *Use Synchronous Detection to Make Precision, Low Level Measurements*, Analog Devices Technical Article MS-2698, 2014, 1-8.
5. Quinlan, J. R., *C4.5: Programming for machine learning*, Morgan Kaufmann 38, 1993
6. The University of Waikato, *Weka 3: Data Mining Software in Java*, Available: <http://www.cs.waikato.ac.nz/ml/weka/> [Accessed on 10.09.2018]
7. Jiang W. and Wright W. MD, *Wireless communication using ultrasound in air with parallel OOK channels*, 24th IET Irish Signals and Systems Conference, 2013

Reliable Planning of Human-Robot-Collaboration featuring Speed and Separation Monitoring

Petersen H., Behrens R., Saenz J., Schulenburg E., Vogel C., Elkmann N.

Fraunhofer IFF – Sandtorstrasse 22 – D-39104 Magdeburg – Germany

Hauke.Petersen@iff.fraunhofer.de

KEYWORDS: human-Robot collaboration, computer aided safety, shared workspace, speed and separation monitoring

ABSTRACT

While human-robot collaboration (HRC) with high-payload robots is attracting the attention of industrial manufacturers, the engineering efforts and associated costs currently needed to comply with the safety requirements from standards are prohibitively high and represent a barrier to more widespread use. This paper presents a novel planning approach to reduce the aforementioned design and planning efforts. Our focus is on industrial applications featuring HRC that use Speed and Separation Monitoring (SSM) according to ISO/TS 15066 to safeguard the robot. This paper presents our novel approach that uses a cloud-based platform and provides planning services as an extension to commercially available planning tools to calculate the minimum protective safety distance between robot and humans. The benefits of our approach are a faster design process and less uncertainty about the required floor space and the achievable cycle time.

1 INTRODUCTION

We see a great potential for the use of collaborative robots in industrial manufacturing processes. Collaborative work between robots and humans could meet current demands for increased flexibility in production and also make automation possible for smaller businesses.

Safety requirements for collaborative robots confront system integrators and designers with a challenging task. From our perspective, this is due to the conventional planning and design methods used today, which ignore the specific safety requirements of HRC. For a manufacturer, a robot cell needs to fulfill its economic objectives. However, it is a challenge to determine the main cost factors for a robot application featuring HRC. One of them is the space needed to set up the robot system on the floor of a factory. Nowadays, robots are typically separated from their human coworkers and process parts without any interaction with humans. In most cases the only connection to the “human world” are feeding facilities, material gates, and safety doors. Such installations require a lot of space, are often a source of incidents, and generally increase the costs for realization, operation, and maintenance. The goal of HRC on one hand is to reduce these costs and on the other hand to ensure unobstructed access of human workers to the robot in order to establish a shared workspace (collaborative workspace) for cooperative tasks. Such an arrangement has further advantages, especially for maintaining or cleaning the robot system. Another important benefit is reduction of misuse (e.g. when humans bypass safety measures like doors or switches). This could also be a particular benefit from an insurance standpoint.

Looking at the relevant standards for robotics, which are ISO 10218 [1], [2] and the ISO-TS 15066 [3], there are four safeguarding modes. One of them is Speed and Separation Monitoring (SSM), which is the focus of this paper. SSM can be used to safeguard three of four possible forms of HRC [4] and is considered by us to be a flexible means for bringing human manpower and robotic performance together. The essence of SSM is to avoid physical contact between the human operators and the moving robot by maintaining a separation distance between both at all times. Since SSM avoids any physical contact to the robot, it is ideal when safeguarding robots moving heavy payloads (>15kg). Furthermore, SSM has no restriction regarding the shape of the parts, making it suitable for applications requiring the handling and processing sharp and pointy parts.

In the literature, there are various works addressing different aspects of SSM. Salmi et al. [5] compare the braking behavior of robots with data from simulation. They demonstrated how the robot speed has a significant influence

on the stopping distances and times. Lacevic and Rocco [6] investigated the distance between the moving robot and a human operator. They developed the concept of kinetostatic danger fields, which can be established around a whole robot. The dimension of a field depends on the joint configuration and speeds. The contribution of a moving human to the field dimension were however neglected, and their work was published years before the ISO/TS 15066 was publicly released. The work of Vicentini et al. [7] proposes a virtual envelope around the robot that is updated in real time. This method needs sufficient surveillance through safety sensors, which can be of various types. Lasota et al. [8] elaborated a process that continuously adapts the speed of a robot using a virtual environment and an altered function to calculate the separation distance. The speed adaptation relies on three discrete velocity levels, namely full speed, one reduced speed level and stop. Because latencies can vary, their system does not work with hard real time. However, the authors are confident that they can overcome this limitation with object prediction. The work of Zanchettin et al. [9] has a similar approach utilizing a continuously modulated speed scaling. It is limited to supervising the Tool Center Point (TCP) of the robot and cannot exclude contact entirely.

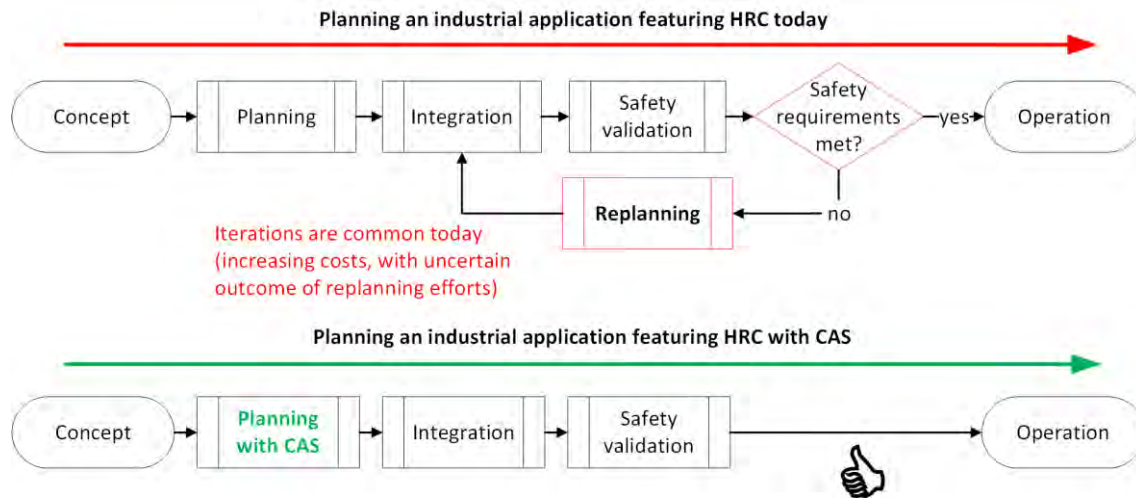


Figure 1. Planning Process of an industrial application without and with CAS.

Each of the presented works focuses on integrating aspects of SSM into the robot, but none of them consider the design phase in which the robot system is created. We see great demand for tools and methodologies that allow the system integrator to consider safety requirements of SSM when designing new applications. Our proposed, new approach, called Computer-Aided Safety (CAS), therefore is specifically tailored to the needs of system integrators when designing a safe collaborative robot system safeguarded with SSM.

As shown in the illustration at the top of Figure 1, planning for SSM today can be an iterative process, especially if the safety validation of the fully installed and commissioned robot systems reveals that some safety requirements are not fulfilled. Common adjustments in such situations, such as a reduction in the robot speed or an increase in the separation distance between humans and robots, have a negative effect on the performance of the robot system, essentially raising the cost of bringing the robot into operation. With CAS, such a situation can be avoided. It supports the system integrator to consider relevant safety requirements mandatory for SSM during the design phase, prior to implementation, and without costly iterations.

The paper is structured as follows: Chapter 2 describes the purpose of SSM and its application in detail. A key factor of SSM is the formula to calculate a minimum separation distance that must be maintained during robot operation [3]. Chapter 3 presents the concept of CAS and gives a brief description about how it works. This is illustrated by a short example of how CAS tools can be used to design a palletizing application with unobstructed access for human. The paper concludes with a summary and an outlook on our future work.

2 SPEED AND SEPARATION MONITORING

The key purpose of Speed and Separation Monitoring (SSM) is to mitigate the risk of hazardous collisions between robot and human operator. Risk mitigation is achieved by maintaining a time-dependent protective separation distance $S_p(t)$ to the robot that must not be violated by the human during robot operation. If the current distance between robot and human is S the following constraint must be fulfilled for all times t

$$S(t) \geq S_{p,i}(t) \quad . \quad (2.1)$$

For the special case the robot does not move $|\hat{v}_r(t^*)| = 0$ the separation distance is zero $S_{p,i}(t^*) = 0$. Otherwise $S_{p,i}(t)$ depends on the velocity of the robot, its braking behavior and a couple of time-invariant parameters mostly related to the installed safety sensors that measure $S(t)$. In accordance to ISO/TS 15066, the two cases give

$$S_{p,i}(t) = \begin{cases} 0 & |\hat{v}_r(t)| = 0 \\ S_h(t) + S_{r,i}(t) + S_{s,i}(t) + C + Z_d + Z_r & \text{otherwise} \end{cases} \quad . \quad (2.2)$$

Note that $S_{p,i}(t)$ represents the minimum separation distance for particle i on the robot surface, which theoretically consists of an infinite number of particles. Following this concept, $\hat{v}_r(t)$ is the velocity of the fastest moving particle i given by $\hat{v}_r(t) = \max\{v_{r,i}(t)\}$. The contribution of the moving human to $S_p(t)$ is $S_h(t)$ and is calculated as follows

$$S_h(t) = \int_t^{t+T_{rs}} v_h(\tau) d\tau \quad . \quad (2.3)$$

It depends on the velocity of the human at time t , which is $v_h(t)$, during the stopping duration T_{rs} that is the time the robot needs from detecting the violation of (2.1) to stopping all joints to velocity zero. The total duration is $T_{rs} = T_r + T_s$, including both the reaction time T_r and the stopping time T_s .

The reaction time T_r is defined as the delay from detecting the violation of (2.1) to shortly before initiating the brakes. Accordingly, the duration from this particular moment to the one at which all axes reach velocity zero is the braking time T_s . The contribution of the robot movement to $S_{p,i}(t)$ is divided into $S_{r,i}(t)$ and $S_{s,i}(t)$, which represent the displacement of the robot particles during the reaction time T_r and T_s respectively

$$S_{r,i}(t) + S_{s,i}(t) = \int_t^{t+T_r} v_{r,i}(\tau) d\tau + \int_{t+T_r}^{t+T_r+T_s} v_{r,i}(\tau) d\tau = \int_t^{t+T_r+T_s} v_{r,i}(\tau) d\tau \quad . \quad (2.4)$$

Another contribution of the robot included in (2.2) is Z_r , which is the position uncertainty of the robot. The influence of the safety sensor is expressed by its non-detectable overreaching distance C and its minimal spatial resolution Z_d also denoted as the position uncertainty of a person in the collaborative workspace.

3 COMPUTER-AIDED SAFETY: A NEW APPROACH TO DESIGNING APPLICATIONS WITH HUMAN-ROBOT COLLABORATION

Modern simulation software gives the user the ability to customize it according to their needs. For this approach, Visual Components (VC) was used as a basis. It provides an API that lets programmers write plug-ins to augment the usage of the software. In this chapter those additions and the underlying calculations will be explained in detail.

3.1 Preliminary considerations

Chapter 2 introduced all relevant states and parameters that are necessary to solve the distance equation (2.2) for each particle on the robot surface. This chapter will focus on the solution of (2.2) and its particular terms. It starts with an analysis of the robot motion and proposes a method to take the programmed motion and the motion during braking into account. The second part of this chapter considers the contribution of the human operator that works around the robot. In the last part we elaborate the parameters related to the safety sensors that are monitoring the position of the human operator to detect whether the minimum separation distance is maintained.

3.1.1 Robot motion

The state of each particle i on the robot surface consists of a position $p_i := p_i(t)$ and a velocity $\dot{x}_i := \dot{x}_i(t)$. Assuming the kinematic model of the robot is given, we can calculate the position p_i with respect to the robot base frame K_0 as follows

$$\begin{bmatrix} p_i \\ 1 \end{bmatrix} = A_k \begin{bmatrix} {}^k p_i \\ 1 \end{bmatrix} \quad . \quad (3.1)$$

The homogenous matrix $A_k \in \mathbb{R}^{4 \times 4}$ transforms the particle position ${}^k p_i \in \mathbb{R}^{3 \times 1}$, defined in the reference frame K_k of the rigid body whose surface contains particle i , into frame K_0 . Using differential kinematics leads to the velocity \dot{x}_i of particle i in K_0

$$\dot{x}_i = \begin{bmatrix} v_i \\ \omega_i \end{bmatrix} = J_i(k, {}^k p_i, q) \dot{q} \quad , \quad (3.2)$$

whereby vector $q := q(t)$ with $q = q_k$ and $q \in \mathbb{R}^{N \times 1}$ represents the robot configuration (positions of N joints) and its first derivative $\dot{q} := \dot{q}(t)$ with respect to time, which are the angular joint speeds. The Jacobian matrix $J_i \in \mathbb{R}^{6 \times N}$ of particle i in frame K_i establishes the linear connection between the robot joint speeds and the velocity of particle i in K_0 . The norm of the translational velocities is $v_i = v_{r,i} = \|v_i\|$ with $v_i \in \mathbb{R}^{3 \times 1}$ and $v_{r,i} \in \mathbb{R}^+$.

Assuming $T = \{q, \dot{q}\}$ is the programmed and known trajectory of the robot, with expressions (3.1) and (3.2) we can then predict the position and velocity of each particle i at time t . In order to determine $S_{p,i}(t)$ we need to calculate the trajectory that each particle will follow right after a distance violation occurs. From (2.2), we can derive two motion phases after the minimum separation distance has been reached by a human. The first phase is the reaction phase lasting from t to $(t + T_r)$. During this phase the robot stays on the trajectory T_r . This trajectory can be assumed as a sub-set of the programmed trajectory $T_r \subset T$, since the control unit does not yet take any action to stop the robot. The second phase is the stopping phase lasting from $(t + T_r)$ to $(t + T_r + T_s)$. Shortly before this phase begins, the safety controller of the robot receives the stop signal from a sensor. It follows the immediate initiation of an emergency stop, usually of category STOP1 (controlled stop). During this phase we can assume that the robot is probably leaving its original trajectory T and follows a braking trajectory T_s . Since T_s is not provided directly by the robot controller, it is necessary to estimate its course over time from the braking characteristics given by the robot datasheet.

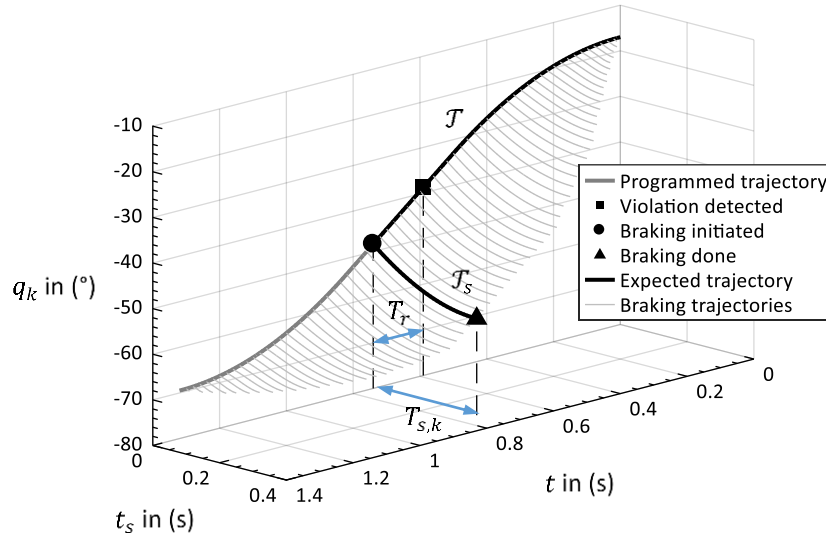


Figure 2. Exemplary stopping trajectory for a single robot joint.

Usually, the datasheet provides curves illustrating the joint displacement and stopping time during braking at STOP0 and 1. Both quantities depend on the joint speed, the distance between tool connector plate (flange) and axis 1 as well as the mass of the robot tool and workpiece (payload). These curves are usually available only in coarse resolution, why it is necessary to interpolate them. In this case, a joint-related displacement $\Delta q_s = q_{s,k}$ and stopping time $T_{s,k}$ can be determined for a specific configuration given by a certain payload, distance, and joint speed. Finally, a cubic polynomial-approach yields an estimation of the desired braking trajectory for each joint k with the following boundary conditions

$$\begin{aligned} q_{s,k}(t_s = 0) &= q_k(t + T_r) & q_{s,k}(t_s = T_{s,k}) &= q_k(t + T_r) + \Delta q_{s,k} \\ \dot{q}_{s,k}(t_s = 0) &= \dot{q}_k(t + T_r) & \dot{q}_{s,k}(t_s = T_{s,k}) &= 0 \quad . \end{aligned}$$

The overall braking time T_s corresponds to the slowest decelerating joint obtained by $T_s = \max\{T_{s,k}\}$. Note, that the joint-related braking times $T_{s,k}$ can differ from joint to joint. Therefore, asynchronous joint motion must be expected during braking. Figure 2 illustrates both motion phases for one axis for an arbitrary trajectory and joint position. The diagram has two time axes to differentiate between the trajectories. The time axis t belongs to the programmed trajectory T and axis t_s to the trajectories T_s for all joint positions along T . With both trajectories T_r and T_s known for each position along T , the separation distance $S_{p,i}$ can be calculated for each particle i according to their particular state (position and velocity) by applying (3.1) und (3.2)

3.1.2 Human motion

Today, there are no safety-rated tracking systems available for measuring the speed of a human working around a collaborative robot. Therefore, it is necessary to assume a constant value for v_h . ISO/TS 15066 specifies the velocity value 1.6 m/s, taken from ISO 13855 if alternative estimates are not available. Please note that the contribution of v_h to $S_{p,i}$ does not take the approaching direction of the human into account. Equation (2.2) considers only scalar based and non-directional velocity values.

3.1.3 Sensor capabilities

As introduced in chapter 3, the contribution of the sensor to (2.2) is obviously limited to the parameters C and Z_d . The non-detectable overreaching distance C depends on the sensor principle and on the sensor configuration. For instance, a horizontally installed laser scanner has a constant overreaching distance of $C = 0.85$ m, while the C value of a vertically installed laser scanner varies with the sensor configuration. The value for Z_d must be derived from the detecting accuracy of the sensor, which is specified in the datasheet. Besides both detection parameters, the reaction time of the sensor T_r^S must also be considered. Together with the reaction time of the robot T_r^R and the reaction time of further safety components T_r^V it adds up to the overall reaction T_r .

$$T_r = T_r^S + T_r^V + T_r^R \quad .$$

3.2 Implementation

One intention of CAS is enabling reliable decisions regarding safety provisions early in the design process. In the case of SSM, this includes the calculation of the safety zones depending on robot motion, sensor configurations, and the overall cell layout. The first step is the calculation and visualization of the safety distance around a simulated robot. While modern simulation tools for modelling robot cells can provide most of the relevant information like trajectories and joint speeds, other aspects like breaking behavior or sensor capabilities are often neglected. Our approach is to enhance existing design software with the necessary information and algorithms for a risk assessment in a simulated environment. Currently we have developed a plug-in for Visual Components (VC) to test the capabilities of CAS. In the future, plug-ins for other simulation software suites will follow.

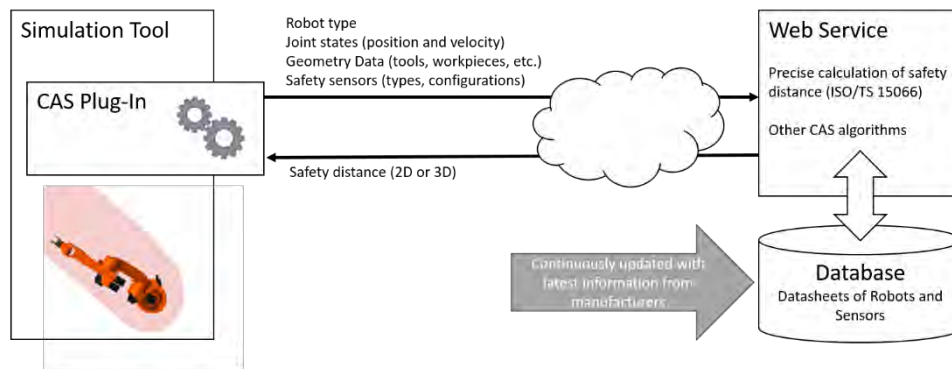


Figure 3. Shared approach of Computer Aided Safety.

Our approach uses an independent web service that provides metadata of sensors and algorithms for SSM calculations. This service can be integrated into various simulation tools via plug-ins. The service can later on be extended by larger databases and further algorithms, e.g. for Power and Force Limiting (PFL). The overall architecture is shown in Figure 3: users can design an automation process as usual while the web service provides additional data (i.e. sensor properties), from various data sheets of robots and safety sensors, which supports the users with parameters that they would otherwise have had to look up in various tables. The database can be improved continuously with more data from manufacturers. If the robot and sensor suppliers upload precise and comprehensive datasets, it also benefits them, because with accurate data, an integrator would not have to use a conservative or worst-case value e.g. for a robot braking time, increasing the likelihood of their part being chosen for use. This overall situation will then lead to robot cells that occupy less space and simulations based on better information.

The CAS extension can read out relevant data from the simulation and send it to the server. This data may include trajectories, joint speeds, geometry and mass of tools and work pieces etc. The server performs the calculations of the safety distances. The results are sent back to the application and presented to the user.

One advantage of this cloud-based system is the nearly unlimited computing power available for processing complex tasks. As described in section 3.1.1 the calculation of the safety distances is quite complex and processor intensive. It involves the calculation of the trajectory and velocity of every particle on the robot's surface including tools and workpieces, using the equations introduced in chapter 2 and 3. Even though our algorithm applies some simplifications regarding the geometry of the robot, it still has a significant run-time. Of course, the run-time depends on the length of the simulated trajectory and the desired accuracy. On a common workstation, it can range from one second to several minutes, but by the off chance that integrators are not always connected to the internet or gets connection problems, the calculations take place on their computer until it is connected again.

3.3 Application

The main benefit from using the CAS tool is that the people designing and setting up the robot cells won't have to fear any unexpected setbacks after the construction. The work of Salmi et al. [5] shows through trials that simulations are capable of predicting braking times and distances compared with real robots, meaning that computed safety areas can be relied upon. The design process is vastly accelerated as well because the designer can quickly test different variations and iterate to find good solutions.

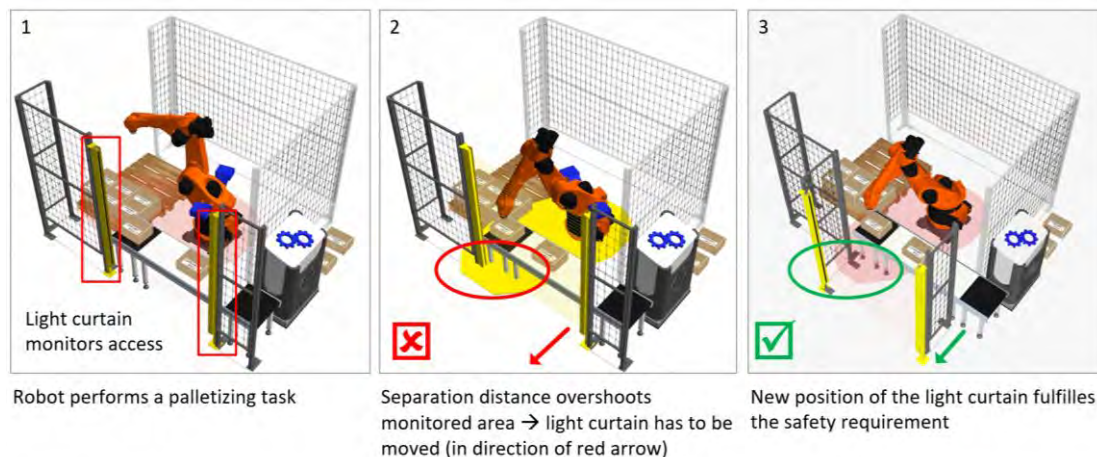


Figure 4. Safety Distance Area collides with a safety sensor (light curtain).

Figure 4 illustrates how a designer can quickly change a layout to reach a reliable and safe solution. For this example a simple palletizing scene was built in VC. The robot takes boxes from the conveyer and stacks them on the pallet. The designer used fences to safeguard most of the surroundings. There is an entrance to the conveyer in front of the robot cell, to access the pallet. A light curtain monitors this entrance (1). However, this light curtain is too close to the robot. While the robot moves to take packages from the conveyer, the minimal separation distance overshoots the area that is monitored by the safety sensor (2). With our tool, the integrator is able to recognize this problem at design time and can change the layout of the cell and sensor position, modify the robot speed, modify the trajectory or use another sensor with different parameters. In this case, the position of the light curtain is changed to sense people before the minimal separation distance is reached (3).

4 CONCLUSION

Robot integrators using CAS will be able to reliably design a layout and program the robot for applications featuring human-robot collaboration. They don't have to expect any changes after the robot cell has been built. That means they can calculate the required installation space and the possible cycle time with a high degree of confidence. Our approach, which integrates our cloud-based software into existing simulation software, makes CAS compatible for a wide range of currently available simulation programs. One of the next steps could be to integrate CAS with various software, like assembly simulation from Siemens or DELMIA from Dassault Systems. With all that in mind, CAS is the first step towards automated optimization of robot cell layouts, even extending towards automated safety certification of applications featuring human-robot collaboration.

ACKNOWLEDGMENT

This work is part of the MR_KOOP project funded by the Investitionsbank of Saxony-Anhalt under grant agreement 1704/00050.

5 REFERENCES

1. “ISO 10218-1:2011 Robots and robotic devices - Safety requirements for industrial robots - Part 1: Robots.” 2011.
2. “ISO 10218-2:2011 Robots and robotic devices - Safety requirements for industrial robots - Part 2: Robot systems and integration.” 2011.
3. “ISO/TS 15066:2016 - Robots and robotic devices - Collaborative robots.” 2016.
4. R. Behrens, J. Saenz, C. Vogel, and N. Elkmann, “Upcoming technologies and fundamentals for safeguarding all forms of human-robot collaboration,” in *8th International Conference Safety of Industrial Automated Systems (SIAS 2015)*, Königswinter, Germany, 2015, pp. 18–20.
5. T. Salmi, I. Marstio, T. Malm, and J. Montonen, “Advanced safety solutions for human-robot-cooperation,” in *Proceedings of ISR 2016: 47st International Symposium on Robotics*, 2016, pp. 1–6.
6. B. Lacevic and P. Rocco, “Kinetostatic danger field - a novel safety assessment for human-robot interaction,” in *2010 IEEE/RSJ International Conference on Intelligent Robots and Systems*, 2010, pp. 2169–2174.
7. F. Vicentini, M. Giussani, and L. M. Tosatti, “Trajectory-dependent safe distances in human-robot interaction,” in *Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA)*, 2014, pp. 1–4.
8. P. A. Lasota, G. F. Rossano, and J. A. Shah, “Toward safe close-proximity human-robot interaction with standard industrial robots,” in *2014 IEEE International Conference on Automation Science and Engineering (CASE)*, 2014, pp. 339–344.
9. A. M. Zanchettin, N. M. Ceriani, P. Rocco, H. Ding, and B. Matthias, “Safety in human-robot collaborative manufacturing environments: Metrics and control,” *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 2, pp. 882–893, Apr. 2016.

Industrial collaborative robot application: experimental implementation of safety-rated monitored stop

Sghaïer A.¹, Baudoin J.¹, Bello J.P.¹, Jocelyn S.², Burlet-Vienney D.², Giraud L.²

¹ Institut national de recherche et de sécurité (INRS) – 1, rue du Morvan – CS 60027 – 54519 Vandœuvre Cedex – France

² Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST) – 505, boul. De Maisonneuve Ouest – Montréal (Québec) - H3A 3C2 - Canada

adel.sghaier@inrs.fr
james.baudoin@inrs.fr
jean-paul.bello@inrs.fr
jocelyn.sabrina@irsst.qc.ca
damien.burletvienney@irsst.qc.ca
laurent.giraud@irsst.qc.ca

KEYWORDS: collaborative robotics, safety functions, integration

ABSTRACT

Technological innovations supported by the evolution of industrial standards helped the emergence of applications in which man and robot can collaborate. These innovative industrial applications introduce new risks for the operator that must be adequately covered. Today, almost all robot manufacturers offer a range of technical solutions that help integrators managing the risks associated with human-robot collaboration. In order to help integrators apprehending those new technical solutions, we conducted a study in which a theoretical study associated with an experimental collaborative robot application implementation was carried out. The objective of this approach was to act as an integrator in order to define the different steps to be followed and to identify vigilance points relative to the operator's safety in the collaborative workspace.

1 INTRODUCTION

As a result of the modernization of production methods in industry, the development of collaborative robotics is of growing interest to manufacturers and represents a central element of the “industry of the future¹ [1]. Today, robot manufacturers offer technical solutions that can be used to implement collaborative robot applications. In addition, the standard ISO 10218-1 [2] and the technical specification ISO/TS 15066 [3] prescribe methods combining several safety functions to control the risk associated with collaborative operations. Those two documents specify four safety methods that can be used independently or combined to manage the risk:

1. Safety-rated monitored stop: detecting a presence in the collaborative workspace triggers the robot's stop.
2. Hand guiding: the operator uses a hand-operated device that sends his or her movement intention to the control system;
3. Speed and separation monitoring: the robot avoids the operator by maintaining dynamically a certain speed and separation distance;
4. Power and force limiting by inherent design or control: the robot's kinetic energy is limited.

Among these four methods, the first one benefits the most from mature technology that allows the safe implementation of human-robot collaboration. This is why during our study we focused on the implementation of a collaborative robot application that employs the “safety-rated monitored stop”. The study presented in this paper involves a theoretical part exploring functions proposed by robot manufacturers done in collaboration with the

¹ Launched in 2013, "Industry of the Future" is a national project that aims to transform the current industrial model into a more flexible and competitive one through the use of new technologies.

IRSST and an experimental part in which a typical collaborative application was developed and implemented by the INRS.

2 METHOD

In order to cover as fully as possible the subject of collaborative robot application implementation, the study was structured in three steps:

- Theoretical study of safety-related functions proposed by robot manufacturers
- Operational and safety specification of the chosen collaborative robot application
- Implementation of an experimental collaborative application

2.1 Theoretical study

Functions embedded in safety cards or modules provided by manufacturers contribute to the achievement of global safety functions. The integrator should complete those embedded functions by integrating safety devices (e. g. detection devices) for example. These functions should therefore be referred to as "Safety-Related Functions" (SRF) to emphasize the fact that they are only processing blocks that contribute to the complete safety chain needed to protect the operator [4]. We propose to use this term in this document.

The SRF theoretical study was based on the documentation as well as information gathered from robot manufacturers. A sample of the most representative manufacturers in the robotics market that proposed solutions for collaborative robotics was selected (ABB, Yaskawa, and Universal Robot) to be studied by experts from INRS and IRSST. In order to analyze and compare safety-related functions, INRS and IRSST used a common analysis grid. Each SRF proposed by the manufacturer has been studied according to the criteria of the analysis grid. The results of this study were published in a previous SIAS article [4, 5].

The theoretical study of safety-related functions aims to answer the following questions:

- *What are the technical specifications of SRF?*

To address this question, it was necessary to explore the technical documentation provided by robot manufacturers in order to establish definitions and to classify SRFs according to their technical specifications. The purpose was to allow the integrator to select the solution that will best meet the risk prevention needs of the collaborative application to be implemented.

- *What is the impact of the implementation of SRFs on the collaborative application hardware and software architecture?*

SRF are incomplete functions. Their implementation within a complete safety function requires the addition of equipment (safety devices, safety components ...) as well as specific configuration and programming operations. A detailed analysis was carried out to identify, for each SRF, the required hardware configuration as well as specific configuration and programming needs [4, 5].

2.2 Operational and safety specification of the chosen collaborative robot application

The objective of this step is to illustrate the process of specification and development of safety functions required to protect an operator working in collaboration with an industrial robot. In this context, a collaborative robotic application has been defined as being representative of the applications present in the industrial field. That application also takes into account several scenarios of human-robot collaboration in order to implement a multitude of means of protection.

The specification of safety functions follows the traditional process of machinery risk reduction as indicated in standard EN ISO 12100 [6]. This process is the result of an iterative risk reduction approach that, applied to this case, aims to ensure the safety of the operator in collaborative robot application. The specification and development method we have adopted is based on the following points:

- Formulation of the functional specifications
- Choice of the hardware control system architecture
- Definition of standard functions
- Definition of robot trajectories
- Risk analysis and identification of appropriate preventive measures
- Safety part specification
- Virtual simulation of trajectories of robot

2.3 Implementation and experimentation of the collaborative application

The specification process is followed by the practical implementation of the selected technical solutions. The key of the safe integration of a collaborative robot application is installation of safety devices and programming of safety functions. In line with the procedure described in EN ISO 12100 [6], we followed the following implementation steps:

- Choice of the different equipment
- Implementation of operational part
- Implementation of safety functions
- Validation, tests and experiments

An experimental collaborative robot application has been implemented within INRS (see figure 1).



Figure 1. Experimental collaborative robot application.

The approach adopted consists of starting from a classical robotic cell installed by an external integrator and to convert it into a collaborative robot application. Outsourcing operations such as the installation of equipment allowed us for focusing only on the implementation of safety functions and the installation of protective devices.

This approach helped to identify difficulties that integrators may encounter when implementing “collaborative” safety-related functions. This approach was adopted with a twofold purpose:

- To propose an implementation method to the integrator
- To warn integrator about a certain number of points of vigilance in order to avoid errors that may have an impact on the operator's safety

3 RESULTS

3.1 Theoretical study: safety-related functions

The theoretical study of the safety functions proposed by the manufacturers allowed us, as a first step, to clarify the definition of certain concepts related to collaborative robotics and the associated safety functions. This has been done in order to avoid confusion and misunderstanding that can mislead the integrator. We were thus able to define the following concepts:

- Safety function
- Safety-related function
- Collaborative robot
- Collaborative robotics application

The theoretical study also allowed us to make a comparison between the safety-related functions provided by three robot manufacturers. An analogy between the families of SRFs between manufacturers was found, although there

may be technical differences between the functions offered by manufacturers. The differences observed may have an impact on the implementation of the collaborative robotics application. It is therefore necessary to select the technical solution that best suits the safety needs of the application one wants to integrate.

Finally, this study allowed us for carrying out a classification of safety-related functions. This classification contributes to a better understanding of these functions. Three families of SRFs could be identified:

- Stopping SRF: functions that cause the robot to shut down with or without power failure, due to external control, failure or anomaly (e. g. STO, SS1 or SS2 according to IEC 61800-5-2 [7]);
- Monitoring SRF: functions that monitor certain characteristics of the robot, for example to keep its shutdown under power (e.g. SOS according to IEC 61800-5-2) or to prevent it from exceeding predefined values (limit violation). These may be speed or space limits (e.g. SLS or SLP according to IEC 61800-5-2);
- General SRF: functions that are neither stop nor monitor (e. g. cyclic brake control).

3.2 Collaborative robot application design approach

Integrators are advised to follow a design method that is in line with the iterative risk reduction method proposed by EN ISO 12100 [6]. Based on the experience of practical implementation of a collaborative robot application, this method has been adapted to the domain of collaborative robotics.

The integration of a collaborative robot application must necessarily result from a real need of human-robot collaboration for achievement of the industrial process. It is therefore essential to conduct an analysis of the need before considering the integration of such application.

The determination of the robot limits allows the integrator to clearly define the different zones and thus delimit the collaborative workspace and apply the prevention measures that best meet the identified risk analysis requirements (see figure 2).

The definition of the need as well as the spaces and in particular the human-robot collaboration space is therefore an important prerequisite for taking into account the safety of the operator working in collaboration with the robot.

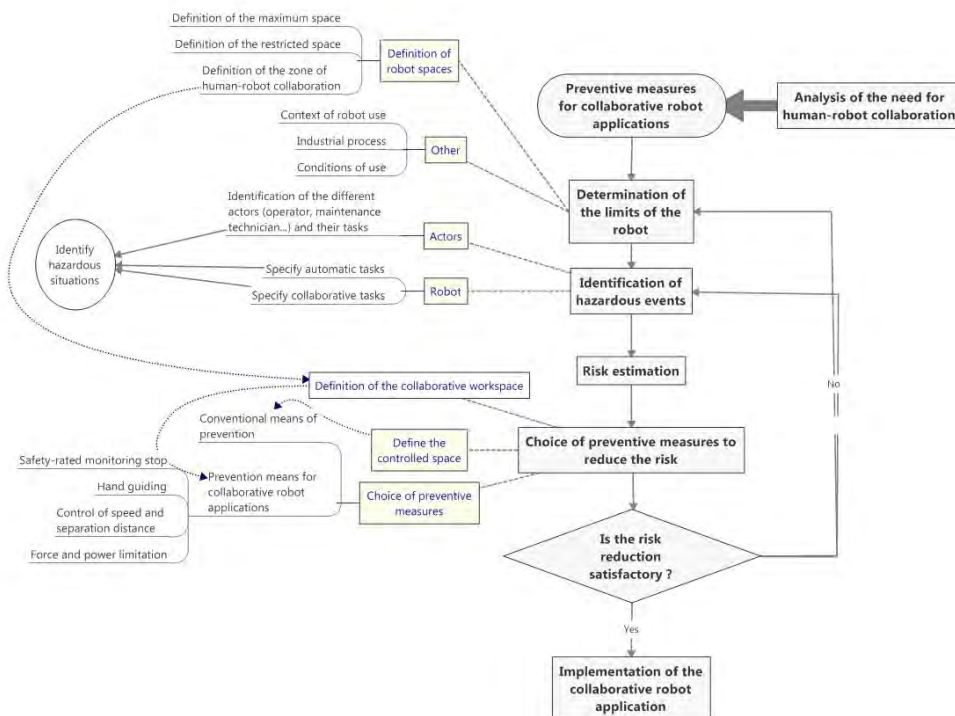


Figure 2. The proposed implementation method dedicated to the integrator.

3.3 Points of vigilance and recommendations to integrators

This study provided us with a better understanding of the safety-related functions offered by manufacturers. Many of these functions are monitoring functions. Their role is to monitor certain parameters related to the robot's trajectories (e. g. immobility, speed, space or axis limits, etc.). These functions are designed to trigger safety stops in the event of failure. The distance travelled by the robot during a failure can therefore be significant and must be taken into account when analyzing the risks in order to correctly position safeguards (determination of the safety distance).

The standard EN ISO 13855 [8], gives requirements regarding the positioning of safeguards. The aim is to ensure, even in the event of failure, that the machine stops completely before the operator reaches the danger zone. In the case of a machine for which the danger zone is fixed, this standard recommends taking into account the operator's penetration distance before detection and his approach speed to calculate the safety distance as a function of the machine's response and stopping time.

In the case of an industrial robot (either conventional or collaborative-ready), the danger zone is dynamic and depends on the position of the robot and sometimes on the safely space limits implemented. In case of combination of SRF (e.g. space limits and protective device) the distance travelled by the robot (over the space limit) before the safety stop must therefore also be taken into account in the calculation. This distance can also vary significantly depending on the type of safety stop set in the SRF. The distance travelled by the robot also depends on the response time of the SRF and the robot's braking time.

3.3.1 Immobility monitoring functions

If collaboration with the operator requires stopping the robot, the robot stop command is performed in the standard control system (in opposition to safety control system) (the robot remains energized). As this stop is not safe, it is therefore necessary to activate an SRF that monitors the immobility of the robot. This monitoring is performed by taking into account a tolerance value for each robot axis (maximum allowed movement value for each axis). If the robot initiates a movement following a failure, the monitoring SRF safely triggers a safety stop (see next point of vigilance). Thus, the robot's movement will not exceed the tolerance value. The integrator must therefore keep in mind that during a supervised stop, the robot, although stationary, can initiate a movement following a failure. In that case, the SRF stops the robot with a total stopping distance within the tolerance for each axis.

It is therefore essential to correctly define the tolerances of the immobility monitoring function in order to avoid any harm to the operator. If this sizing is insufficient, the integrator will have to use other means of prevention or will have to re-examine the design process.

3.3.2 Workspace monitoring function

The implementation of a workspace monitoring function requires the definition of areas in which the robot is authorized to operate (these areas may be defined according to Cartesian or polar coordinate system). That SRF monitors the positions of the tool center and the robot arm elbow to avoid exceeding the volume defined by the integrator. It also monitors the speed and orientation of the tool in a way that they do not exceed the values defined within the same volume. In the event of a violation of these monitors, the SRF triggers a safety stop. This function is useful for defining a safe workspace for the operator (see Figure 3).

When implementing the workspace monitoring safety function, it is essential to take into account the total stopping distance of the robot. Indeed, the safety stop is triggered when one of the monitored parameters exceeds the configured value. It is therefore essential that the integrator determines the effective stopping distance of the robot. In our example (Figure 3), positioning of the protective devices (light curtains) are calculated in relation to:

- The operator's maximum evolution speed
- The maximum response time of the SRF
- The total stopping distance of the robot

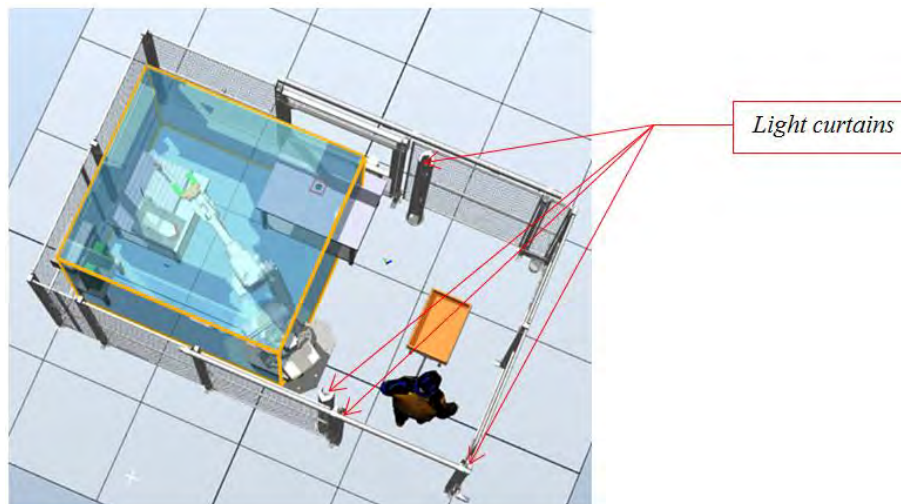


Figure 3. Example of a Cartesian workspace monitoring zone.

3.3.3 Stopping the robot

As described above, the safety-related functions offered by the manufacturers are mainly based on the principle of monitoring the robot's condition and stopping control in the event of a violation. The stop functions are therefore essential. Depending on the type of safety-related function and the manufacturer, the integrator may have the option of programming safety stops of different types in accordance with IEC 60204-1 [9]. Indeed, it is possible to stop the robot either by switching off the energy (type 0); or by decelerating and switching off the energy when the robot is stationary (type 1); or by decelerating and maintaining the stop (type 2).

The integrator shall select the stop type in accordance with the risk analysis. He also has to take into account the fact that the choice of stop type may have repercussion on the actual stopping distance of the robot. The integrator shall calculate these effective stopping distances in order to correctly position the protective devices if necessary.

4 DISCUSSION AND CONCLUSIONS

The implementation of a collaborative robot application may use recent technologies that are not yet mastered by the majority of integrators. In addition, the close proximity of the operator and the robot in this type of application greatly increases the probability of mechanical risks and in particular the risks related to moving parts of the robot and its tool (e.g. gripper). In the event that the preventive measures selected during the risk analysis use SRFs, the integrator must select the SRFs that are in adequacy with the risk and configure them correctly in order to achieve an installation that guarantees the operator's safety.

Our study focused mainly on the safety functions related to the implementation of the first safety method described by EN ISO 10218-1: "Safety-rated monitoring stop". Nevertheless, there are other safety methods allowing the implementation of human-robot collaboration based on other prevention principles. A future study will focus on those other methods. Studies will particularly emphasize the fourth safety method: "Power and force limiting by inherent design or control" since this method is of growing interest to industrials [10]. In this subject, a first work initiated by INRS and DGT² led to a technical document providing samples and initial recommendations for the implementation of that fourth safety method [11].

² DGT is the directorate general for labor. It prepares leads and coordinates labor policy in order to improve collective and individual relations and working conditions in companies.

5 REFERENCES

1. Industrie du Futur : transformer le modèle industriel par le numérique. Le portail de l'économie et des finances 2015, Available from: <http://www.economie.gouv.fr/lancement-seconde-phase-nouvelle-france-industrielle>.
2. AFNOR, EN ISO 10218-1 Robots and robotic devices — Safety requirements for industrial robots — Part 1: Robots, 2011, 43 p.
3. AFNOR, ISO TS 15066 Robots and robotic devices - Safety requirements for industrial robots - Collaborative operation. 2016, 33 p.
4. Sghaïer, A., Jocelyn, S., Burlet-Vienney D., Giraud L., Etude des principales fonctions de sécurité disponibles pour la robotique collaborative, The 8th International Conference Safety of Industrial Automated Systems, Königswinter, Germany, 2015, pp. 61-70.
5. Jocelyn, S., Burlet-Vienney D., Giraud L., Sghaïer A., Robotique collaborative - Évaluation des fonctions de sécurité et retour d'expérience des travailleurs, utilisateurs et intégrateurs au Québec, Rapports scientifiques, IRSST, Editor. 2017, 97 p.
6. AFNOR, EN ISO 12100 Safety of machinery - General principles for design - Risk assessment and risk reduction, 2010, 77 p.
7. AFNOR, IEC 61800-5-2 Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional. 2016, 65 p.
8. AFNOR, EN ISO 13855 Safety of machinery - Positioning of safeguards with respect to the approach speeds of parts of the human body. 2010, 40 p.
9. AFNOR, IEC 60204-1 Safety of machinery - Electrical equipment of machines - Part 1: General requirements. 2016, 127 p.
10. Tihay, D., Coactivité homme-robot : analyse des besoins, INNOVORG: Innovation technologique, changements organisationnels : quels enjeux pour la prévention ?, 2017.
11. Direction Générale du Travail, Guide de prévention à destination des fabricants et des utilisateurs pour la mise en œuvre des applications collaboratives robotisées, Direction Générale du Travail, 2017, 50 p.



Session 2-2

Safety of Collaborative Systems

Advancing Anticipatory Behaviors in Dyadic Human-Robot Collaboration: The AnDy project

Maurice P.¹, Ivaldi S.¹, Fritzsche L.², Babic J.³, Stulp F.⁴, Damsgaard M.⁵, Graimann B.⁶, Bellusci G.⁷, Pucci D.⁸,
Nori F.⁸

¹ Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France

² IMK automotive GmbH, Amselgrund 30, 09128 Chemnitz, Germany

³ Jožef Stefan Institute, Jamova cesta 39, SI-1000 Ljubljana, Slovenia

⁴ German Aerospace Center (DLR), Institute of Robotics and Mechatronics, Wessling, Germany

⁵ AnyBody Technology A/S, Niels Jernes Vej 10, 9220 Aalborg East, Denmark, Denmark

⁶ Otto Bock Healthcare GmbH, Duderstadt, Germany

⁷ Xsens Technologies B.V., P.O. Box 559, 7500 AN Enschede, The Netherlands

⁸ Fondazione Istituto Italiano di Tecnologia, via Morego 30, Genova, Italy

pauline.maurice@inria.fr

KEYWORDS: Collaborative robots, Ergonomics, Wearable Sensors, Human Movement Prediction

In the near future, robots collaborating with human operators in industries will need more and more anticipation capabilities to properly react to human actions and provide efficient collaboration. To achieve this goal, new technologies are needed that not only estimate the motion of the humans, but that fully describe the whole-body dynamics of the interaction and that can predict its outcome. These hardware and software technologies are the goal of the European project AnDy.

The AnDy project leverages existing technologies to endow robots with the ability to control physical collaboration through intentional interaction in order to maximize ergonomics for the user. To achieve this goal, AnDy relies on three technological and scientific breakthroughs. First, AnDy innovates the way of measuring human whole-body motions by developing a wearable AnDySuit, which tracks motions and records forces. Second, AnDy develops the AnDyModel, which combines ergonomic models with cognitive predictive models of human dynamic behavior in collaborative tasks, learned from data acquired with the AnDySuit. Third, AnDy proposes AnDyControl, an innovative technology for assisting humans through predictive physical control based on AnDyModel.

By measuring and modeling human whole-body dynamics, AnDy will provide robots with a new level of awareness about human intentions and ergonomics. By incorporating this awareness on-line in the robot's controllers, AnDy paves the way for novel applications of physical human-robot collaboration in manufacturing, health-care, and assisted living.

We present the goals and methods of the AnDy project, as well as first year results. Technical advances on the AnDySuit – using inertial motion capture and sensorized shoes – along with the development of an on-line inverse dynamics software tool now allows real-time monitoring of human dynamics. The information provided thereby is used in the controller of a robot physically interacting with the human, so that the robot reactively adapts its movement to the human's movement. Experiments with a real robot have shown promising results. The next step is to couple the robot controller with an automatic ergonomic assessment tool. Thereby, the robot will be able to detect and anticipate critical situations, and will react in order to optimize the ergonomics of the human movement.

COVR – Towards simplified evaluation and validation of collaborative robotics applications across a wide range of domains using robot safety skills

Saenz, J.¹, Aske, L.², Bidard, C.³, Buurke, J.H.⁴, Nielsen, K.², Schaake, L.⁴, Vicentini, F.⁵

¹ Fraunhofer IFF (IFF) - Sandtorstrasse 22 - 39326 Magdeburg - Germany

² Teknologisk Institut (DTI) - Gregersensvej 1- Taastrup 2630 - Denmark

³ CEA, LIST, Interactive Robotics Laboratory, F-91191 Gif-sur-Yvette - France

⁴ Roessingh Research And Development BV (RRD) - Roessinghsbleekweg 33- Enschede 7522 AH - Netherlands

⁵ Consiglio Nazionale Delle Ricerche (CNR) - ITIA – via Alfonso Corti 12 – 20133 Milan - Italy

jose.saenz@iff.fraunhofer.de

KEYWORDS: international standardization, practical applications and validation, industrial collaborative robotics, rehabilitation robotics

ABSTRACT

Challenges surrounding human safety have become one of the main barriers to the promotion and availability of collaborative robotics technology in different domains. The EU-funded project “Being safe around collaborative and versatile robots in shared spaces” (COVR) aims to break down these barriers to support more widespread use of collaborative robots in a wide range of industries and domains (e.g. manufacturing, logistics, healthcare and rehabilitation, agriculture). In this paper, we will describe our approach to engage various stakeholders and encourage widespread use of collaborative robots. This includes the development of a toolkit employing a methodology based on robot safety skills, and the development of a set of testing protocols that clearly define the safety-related validation procedures. A crucial aspect of the project is active consultation with regional stakeholders from standardization, national agencies, accident insurance, and safety verification bodies to create a consensus on the validity of the toolkit and protocols. Additionally, the COVR consortium is opening their doors to operate as shared safety facilities, where interested third parties can receive training, gain access to measurement systems for validation, and receive support in using the toolkit and applying the protocols. Finally, COVR will offer over five million Euros in funding to third parties seeking to engage with COVR, to test and expand the toolkit and protocols with specific use-cases, and to provide background research and experimental data for determining best practices.

Besides a description of the various project mechanisms, the first project results including the toolkit design and initial set of protocols for safety validation will be presented in this paper.

1 INTRODUCTION

The need for collaboration between robots on human tasks is evident in all sectors of the European market, as demonstrated in the Strategic Research Agenda¹ from euRobotics aisbl. Collaboration however inevitably raises safety issues, and European legislation is very careful to promote the protection of workers, elderly and weak subjects as a top priority. Market operators therefore perceive the need for “certification”, i.e. the compliance with mandatory Essential Requirements of Safety and Health, as a pressing need.

In our experience with end-users, robotics components manufacturers, and system integrators, safety has become a barrier to the promotion and availability of collaborative robotics technology in all domains. This is due to a number of issues, both technical (e.g. robotics are complex, reconfigurable systems that can change their behaviour over time) and non-technical (e.g. understanding and correctly applying the current standards and directives to prove compliance is a challenge, especially for smaller companies).

The EU-funded project “Being safe around collaborative and versatile robots in shared spaces” (COVR) aims to systematically break down current barriers to support more widespread use of collaborative robots in a wide range of industries and domains. Our particular focus in the project is on manufacturing, logistics, agriculture, healthcare and rehabilitation.

In this paper, we will describe our approach to engage various stakeholders and encourage widespread use of collaborative robots.

¹ https://www.eu-robotics.net/cms/upload/topic_groups/SRA2020_SPARC.pdf

2 COVR APPROACH FOR SUPPORTING STAKEHOLDERS

As mentioned in the introduction, COVR aims to foster the use of collaborative robots in a variety of domains, by specifically addressing challenges regarding safety. In order to ensure a meaningful impact, it is necessary to have a clear understanding of who the main stakeholders for this issue are and how they relate to one another. In particular, we have identified three main types of stakeholders, namely those who state the rules on safety and check that they are being fulfilled (e.g. accident insurers, safety verification bodies, and national agencies), those who define best practice (e.g. standardization bodies and the research community), and those who use and/or sell robots and robotic components (manufacturers, end-users, system integrators). Figure 1 depicts these stakeholders and identifies how COVR interacts with them to take their individual needs into account.

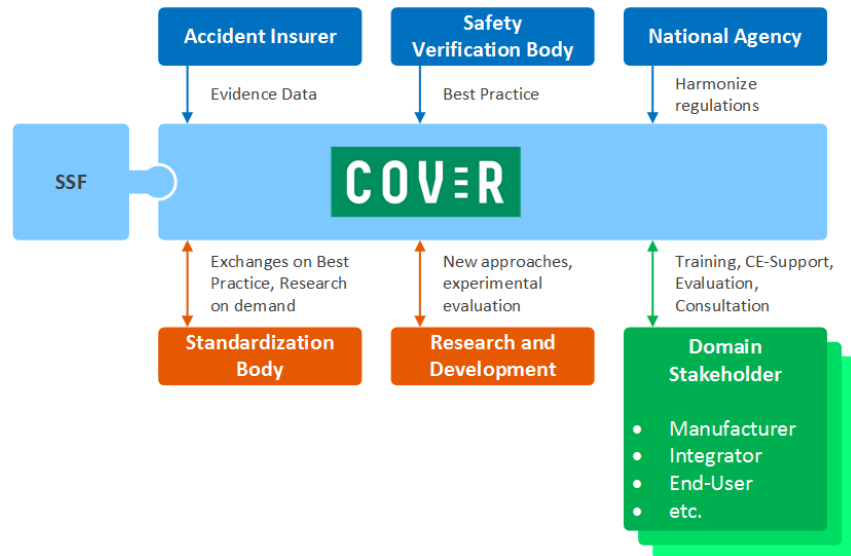


Figure 1. COVR Stakeholders and their interactions with the project

COVR will offer four different means for supporting the stakeholders. First, we are developing a *toolkit* to advise domain stakeholders when identifying the relevant standards and guidelines for their application and domain. The toolkit relies on the concept of robot safety skills – i.e. a complex combination of safety functions and protective behaviours that are valid across domains. Second, we are writing *validation protocols* that are easy to follow, so user of collaborative robot (so called “coboteers”) can prove that their systems fulfil the necessary requirements. Third, we are updating our laboratories to become *shared safety facilities*, where third parties can receive training, gain access to measurement systems for validation, and receive support in using the toolkit. Finally, we are offering over five million Euros in funding to third parties from the robotics community seeking to engage with COVR, to “stress test” the toolkit and protocols with specific use-cases, and to provide background research and experimental data for determining best practices. The following section will describe these four means in detail.

It should be noted that none of these activities will have a meaningful impact unless we have accident insurers, safety verification bodies and national agencies on board and willing to accept our approach. Therefore, a further important aspect of the COVR project is dissemination and consensus building activities with these stakeholders, so that the entire community can agree on best practices.

2.1 Toolkit

The COVR toolkit is a guided procedure for listing the requirements to be satisfied for compliancy with relevant safety directives. It can be used by coboteers with different levels of knowledge about the processes of safety assessment according to ISO 12100 [1] and ISO 14971 [2]. The main steps of the safety assessment, as specified in ISO 12100 are:

- hazard identification,
- risk estimation,
- risk evaluation,
- risk mitigation,
- validation of protective measures.

The purpose of the toolkit is to assist users when carrying out different activities along the lifecycle of the safety assessment and evaluation. It provides explanations about the process with the goal of simplifying the finding and interpretation of mandatory procedures that are available in published normative materials. It consists of a graphical-user interface (GUI) which provides a walkthrough along the analytical steps necessary to derive the safety requirement checklists. Furthermore, the toolkit provides support to identify the necessary methods for validation of implemented risk mitigation solutions, including a collection of validation protocols for selected risk mitigation solutions. Each protocol represents a step-by-step guide on carrying out the required measurements for safety validation. If necessary, the toolkit also supports novice robotics users in taking the preliminary steps to assess hazards and associated risks of applications, entire systems, or particular components.

While the toolkit may be helpful along steps of the risk assessment and evaluation, it is not primarily intended to implement such methodology. The COVR toolkit is NOT intended to be:

- A replacement for risk analysis and assessment
- An automatic selection of risk mitigation solutions to be implemented (The users will be given a list of possible risk mitigation solutions; they will have to choose them according their risk assessment or possibly look for other solutions)
- A certification.

The COVR toolkit will be accessible as a web service. It offers multiple entry paths, depending on the level of knowledge about the domain, the regulations and standards, and the safety skills and safety functions used. The technical design of the GUI and web services is currently in implementation. A first version of the toolkit will be available to COVR Awardees by spring 2019. Section 3 describes the toolkit design and our methodology in detail.

2.2 Validation protocols

Validation is defined as a set of actions to evaluate (i.e. provide evidence through metrics) that a (set of) *safety functions* meets a set of *target conditions*. Safety validation is the evaluation of whether or not a product, service, or system complies with a defined operational condition characterized by a given level of risk. Safety validation serves as a public evidence that a product (including functions and algorithms), or system meets a set of safety requirements agreed by stakeholders.

One of the main objectives of the COVR project is to provide support for the validation of protective safety measures. This entails assistance for creating the necessary documentation (e.g. checklists for showing compliance to individual requirements), as well as step-by-step instructions for performing the validation tests themselves. Especially regarding the validation of systems, we see a lot of uncertainty in the robotics community today. One reason is the complexity of robotics installations, as discussed in [4]. Furthermore, some of the standards applicable to robotics safety were published prior to the existence of collaborative robots, such as the ISO 13855 [3].

The COVR consortium has applied two distinctive methodologies to identify protocols. On one hand, by focusing on the two relatively mature domains of manufacturing and rehabilitation, we have identified safety functionalities that require verification by standardized measurement. This methodology can be termed to be a “standards-based” approach. We consider this approach to be valid, as the required measurements for validation are the state of the art and mandatory for collaborative robotics manufacturers and end-users, when relying on the given safety skill. In order to investigate domains that do not yet have advanced standards, we used a “top-down” methodology, whereby collaborative robotics applications from specific domains were the starting point for identifying protocols. In this methodology, we briefly described specific applications, identified corresponding risks and hazards, before describing options for the risk mitigation. These risk mitigation measures can be considered to be safety skills, and the means to validate their proper function under the appropriate conditions are the validation protocols we are developing.

2.3 Shared safety facilities (SSFs)

The COVR partners within the project are upgrading their facilities and equipment to become shared safety facilities (SSFs) within their domains of specialization. Currently, COVR partners specialize in the domains for manufacturing, healthcare and rehabilitation, logistics, agricultural, and civil domains. At the SSFs we can offer a range of services on a fee basis such as:

- Safety validation (either at the SSF or on-site w/ customer)
- Individual consultancy for the customer’s particular case with relation to human-robot collaboration and safety
- Training courses on cobot safety (generic content plus specialist options, depending on customer needs, including different content for various domains such as healthcare, industry, etc.) – the term “customer” includes:
 - o Large end-users (training for their safety experts and unions)
 - o Small companies and spin-offs making new components for collaborative robot use (e.g. sensors, grippers, peripheral components, or even robots themselves)
- Support in preparing for ethical procedures and related documentation for clinical research with medical devices.
- CE certification of a medical device not only requires technical safety to be evaluated, but also a clinical investigation may be mandatory to support the claimed purpose of the medical device. Many smaller companies, especially when starting in the field of medical devices, are not always fully aware of how to set up and perform a clinical evaluation. Therefore, for rehabilitation robots, some COVR SSFs will offer support in preparing a clinical evaluation for ethical approval by a Medical Ethical Committee and compiling the required documentation.

Additionally, we will provide to FSTP beneficiaries and other interested parties services and training on use of the toolkit and protocols.

2.4 Financial support for third parties to run realistic trials

One special aspect of the COVR project is the financial support to third parties for realistic trials. By realistic trials, we understand a number of activities around the COVR project that a single institution or small consortiums (between two and four partners) can carry out to support the development of new protocols, or to evaluate and improve existing protocols or the toolkit. A single institution can be awarded up to 60.000 Euro for a single award and a maximum cumulative total of 100.000 Euro for multiple awards. There are three rounds of open calls planned during the course of the COVR project coming up in November 2018, July 2018 and March 2019. There are many unique use-cases featuring collaborative robotics in a variety of domains. In acknowledgement of this challenge, the COVR consortium has designed the open calls to serve as a kind of outreach, allowing users and developers of robots with very specific and non-mainstream use-cases to answer open questions in standardization and to investigate best practice for their specific application. Ideally, the standardization community will also use COVR awards to test hypotheses and determine for example the pros and cons of certain methods for validating the safety of specific systems or components.

2.5 Concept of safety skills

An important concept of COVR and its idea to support a cross-domain approach are *safety skills*. This concept arose out of the current challenge with domain specific standards. In the current situation, a domain stakeholder would start the process of evaluating the safety of a system by first identifying which domain is applicable, and then gathering requirements from the relevant directives and standards. This may work for well-established domains such as manufacturing or healthcare, but for other domains (e.g. agriculture), there are often no relevant standards. This further implies that for a large number of domains there are currently no validation protocols available, leading to uncertainty on the part of domain stakeholders. To overcome this situation, the toolkit unifies the protocols according to abstract “safety skills”. We have defined safety skills as an abstract representation of the ability of a robot system to reduce some risk, deploying a suitable risk-reduction measure or displaying an inherently safe design feature. Skills have specific instances (i.e. actual methods for implementation) which depend on the specifics of the application. Validation protocols are then derived from these skills and consider domain-specific conditions, without requiring the availability of domain-specific standards. This skills-based approach to safety will need to be discussed with all stakeholders to gain consensus and acceptance in practice.

3 INITIAL TOOLKIT DESIGN

The toolkit was designed by first identifying the target users and surveying them to learn about their needs regarding safety. Target users as defined by COVR include:

- System integrators of various level of expertise
- Robot developers and manufacturers
- Robot end-users, including:
 - o End-user from management of large /small company

- End-user from technical staff with intermediate skills (people who work with automation technology, engineering, planning)
- Rehabilitation specialist (nurse, occupational therapist)
- Rehabilitation patient (to be informed)
- Certification institutes
- Developers/manufacturers of safety components for robots and robot applications (e.g. safety sensor)
- Safety consultants.

The primary needs of the identified users with respect to general usage of collaborative robots, across all domains, are:

- Preliminary risk and hazard identification
- Knowledge of “best practices”
- Reassess the risk after a robot work-cell modification
- Identify a measurement protocol to validate a risk reduction solution.

Based on the users’ needs, we derived a general usage profile. A user has a number of open issues about different aspects and steps in the risk assessment and validation process, depending on his/her level of expertise. A general understanding of the need for conformity is usually present among stakeholders (so-called safety “certification”), but exact procedures are not clear.

The toolkit is designed to unify the protocols according to abstract “safety skills”. Domain-, product- or function-specific protocols are then derived from these skills. The user is in charge of understanding and selecting the adequate safety skills (themselves often composed of specific safety functions) for attaining risk reduction, and then responsible for performing the associated validation tests.

The analysis of applications or devices does not follow a linear workflow, especially when specifications and/or regulations are partially known or unclear to the user. The toolkit allows for multiple paths of entry through separate perspectives, which are interactive controls in a website dedicated to grouping homogeneous sets of analytical tools (questions, flowcharts, etc.). The perspectives we have designed to date are:

- Document Finder: a set of perspectives that enable the user to browse through the analytical steps using multiple entry points and cross-links. Main navigation tracks are designed (i.e. “by Directive”, “by standard”, “by product”) in order to help the user in finding the correct references to requirements to attain.
- Skill Finder: a perspective for giving the user some limited knowledge about the methodology of risk assessment and help the user to identify “skills” to be validated. This perspective redirects the user to the “Document Finder” in order to reach a final checklist or protocol to implement.

The toolkit will be available to COVR Awardees by spring 2019.

4 INITIAL SET OF VALIDATION PROTOCOLS

Based upon the bottom-up method of identifying validation protocols from known robotics safety standards from the domains of industrial manufacturing and healthcare, as well as the top-down method of identifying robotics safety skills for a wide variety of domains, we have created an initial list of six safety skills, which feature a range of safety functions. These main safety skills are:

- Ability to limit the power and force during a collision
- Ability to stop travel before colliding
- Ability to reduce the impact effect during contact
- Ability to restrict a single mobility degree of freedom
- Ability to restrict multiple mobility degrees of freedom to defined area or volume
- Ability to compensate for effects of joint misalignments

These skills are by definition cross-domain and can be used for safeguarding a wide range of applications. For each of these safety skills we have then defined a set of validation protocols, which a user can carry out to validate the skill. One important issue to consider is the difference between verification and validation. Verification is defined as a set of actions that provide evidence (i.e. metrics needed) that a safety function meets a set of design specifications. Validation on the other hand is defined as a set of actions that provide evidence (i.e. metrics needed)

that a safety function result meets a set of target conditions. While the safety skills and validation protocols are generic and cross-domain, the target conditions for a specific application and domain are necessarily coded into the protocol. This means for a single generic protocol, there can exist a large number of related sub-protocols with specific conditions and parameters under which the validation should be carried out.

5 DISCUSSION

In this paper, we have briefly highlighted some of the main barriers to more widespread use of collaborative robots with regard to safety. In particular, there is a lot of uncertainty regarding which standards and directives to apply, as well as how to validate that the safety of a system has been correctly implemented. This is a particularly large challenge when robots are applied to domains outside of manufacturing and healthcare, where standards and best practice are often non-existent and where technological capabilities are further along than the regulatory framework. We introduced the four main actions that the EU project COVR is undertaking to systematically reduce uncertainty and support the all stakeholders involved in the safety of collaborative robots. These include:

1. A web-based toolkit to support robotics users in identifying the applicable standards and directives,
2. the development of validation protocols that are a step-by-step guide for how to measure and prove that safety systems for a specific application are correct,
3. the transformation of our laboratories into Shared Safety Facilities (SSFs) to offer the community a range of services around the safety of collaborative robotics, and
4. COVR Awards where we fund third party work to support the development and improvement of the toolkit and validation protocols.

Furthermore, the concept of using “safety skills” as a representation of the risk reduction measure was put forth by the COVR consortium. We view this approach, together with the toolkit and the validation protocols as having a large potential to support users and developers of collaborative robotics applications, regardless of the domain of interest.

One major goal of COVR is to build consensus with all relevant stakeholders so that our approach is approved within Europe and all over the world. We look forward to the discussion with relevant stakeholders from standardization, occupational and health insurance, safety verification bodies, and national regulation agencies, and the robotics community about whether this approach will be acceptable, how it can be improved, and how it can be successfully implemented to remove current barriers to safety.

6 REFERENCES

1. ISO 12100 : 2010 : Safety of machinery -- General principles for design -- Risk assessment and risk reduction.
2. ISO 14971 : 2012 : Medical devices. Application of risk management to medical devices.
3. ISO 13855 : 2010: Safety of machinery -- Positioning of safeguards with respect to the approach speeds of parts of the human body.
4. Marvel J.A., Norcross R., *Implementing speed and separation monitoring in collaborative robot workcells*, Robotics and Computer-Integrated Manufacturing, Vol. 44 p.144–155, 2017.

Japan's Approach for the Realization of the Future Safety Concept by Implementing Collaborative Safety Technologies

Mukaidono M.^{1,2}, Takaoka H.^{1,3}, Ogihara H.^{1,4}, Ariyama M.^{1,5}, Fujita T.^{1,6}

¹ The Institute of Global Safety Promotion (IGSAP) – 2-7-53 Nishimiyahara, Yodogawa-ku, Osaka, Japan

² Meiji University – 1-1-1 Kandasurugadai, Chiyoda-ku, Tokyo, Japan

³ Japan Industrial Safety & Health Association – 5-35-2 Shiba, Minato-ku, Tokyo, Japan

⁴ Nikkei Business Publications, Inc. – 4-3-12 Toranomom, Minato-ku, Tokyo, Japan

⁵ Japan Certification Corporation – 2-7-53, Nishimiyahara, Yodogawa-ku, Osaka, Japan

⁶ IDEC Corporation – 2-6-64 Nishimiyahara, Yodogawa-ku, Osaka, Japan

masao@meiji.ac.jp

h-takaoka@jisha.or.jp

ogihara@nikkeibp.co.jp

ariyamam@institute-gsafety.com

fujitat@institute-gsafety.com

KEYWORDS: Future Safety Concept, Safety2.0, collaborative safety, top-down management, Vision Zero

ABSTRACT

In Japan, the government has released a policy stance regarding the robotic revolution and “connected industries,” a move that may lead to a new growth model. “Collaborative safety” concept and Safety2.0 approach to achieve the concept were proposed in 2015. The objective was to connect people and things through information and communication technology (ICT), and ensure safety and *anshin* (a sense of trust and assurance without any fear or stress) in an environment where people and things coexist [1]-[3]. In order to realize this vision, it is essential for companies to promote initiatives with a top-down management approach. For this purpose, the Future Safety Concept, which contains eight policy principles, was unveiled in 2017 [4]. This article presents an overview of the concept's developments in Japan, and explains how these developments are synchronized with the global Vision Zero campaign initiated in 2017 and the introduction of the concept of collaborative safety.

1 INTRODUCTION

The Fourth Industrial Revolution, a technological revolution driven by new technologies such as internet-of-things (IoT), big data, robotics, artificial intelligence (AI) is rapidly unfolding throughout the world. Germany, France, and Japan, are pursuing “Industry 4.0,” “Industry of the Future,” and “Connected Industries” initiatives respectively, with the entire nation involved in the endeavor in each case. Especially in Japan, Prime Minister Shinzo Abe gave a speech at an OECD Ministerial Council Meeting in 2014 calling for a robotic revolution to promote the use of robots in all industrial sectors, and together with conventional industrial robots, so-called service robots are now being introduced for various purposes. Meanwhile, work-style reform is another important measure pursued by the Japanese government, as it seeks to allow people to thrive as dignified human beings in a work environment in which they will not be forced to work excessively or be pressured to work excessive overtime. New technologies, people, the Fourth Industrial Revolution, and work-style reforms are the new challenges facing Japan today. A point to be seriously considered about these challenges is how to further ensure people's safety and *anshin* more than before. The crucial keywords therefore, are safety and *anshin*. The Japanese government strongly stated in the strategy to “make Japan the Safest Country in the World,” decided by the Cabinet in 2013. It was absolutely necessary to make Japan a county where its people could live their daily lives being and feeling safe, and where visitors from around the world would also feel the same way, ahead of the 2020 Tokyo Olympic and Paralympic Games. Thus, this present paper will provide a comprehensive summary regarding safety with respect to technology, human resources, and management, by introducing the issues that are now being debated in Japan and the progress that has been made, and explain how these developments are in line with new international safety trends in the world.

2 CHANGES IN SAFETY CONCEPT; THE COLLABORATIVE SAFETY SAFETY2.0 INITIATIVE BEING DELIBERATED IN JAPAN

The idea of safety has changed with the times, as seen in Figure 1. Taking for example a production site at a manufacturing company, the most rudimentary form is Safety0.0, in which ensuring safety solely relies on workers' attention and judgment. Until the 1980s, in order to prevent accidents involving dangerous machines, workers simply tried to be vigilant as seen in Figure 1 (a). However, it is difficult to ensure safety under Safety0.0 because people are prone to make mistakes. Therefore, a transition was made to Safety1.0, in which safety was ensured by the design of machine systems. Particularly in the industrial sector, various international safety standards for machinery, such as those of ISO and IEC, began to be developed from around 1990 until 2000, predominantly in Europe. As a result, it has become common practice to conduct risk assessments to reduce risks, and design fail-safe and foolproof machinery fulfilling the requirements of various safety standards. This approach seeks to ensure safety, e.g. by determining the operating areas of machines and those of humans, installing safety guards and interlocks accordingly to prevent people from entering the safety guards when the machine is in operation, and allowing them to enter only after the machine is stopped. In other words, Safety1.0 ensures safety through the machinery safety principle of isolating and stopping machines, as seen in Figure 1 (b).

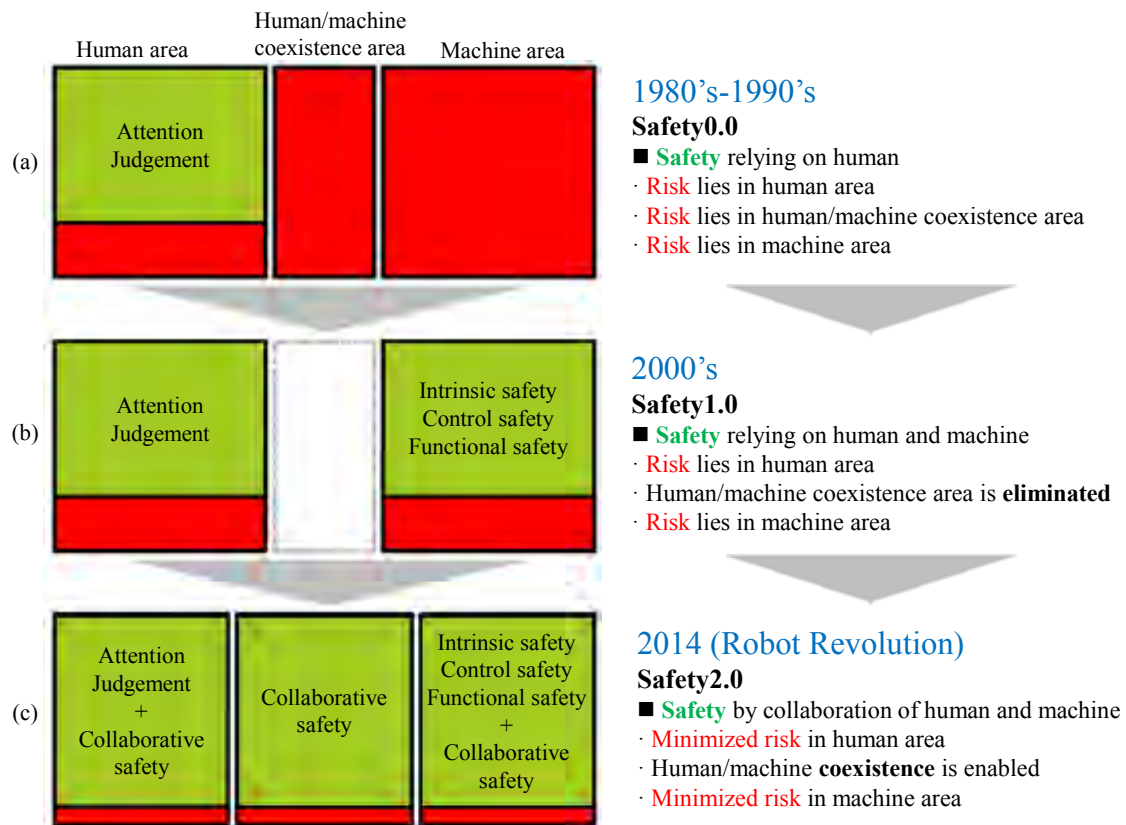


Figure 1. Safety evolution from Safety0.0, Safety1.0, and to Safety2.0.

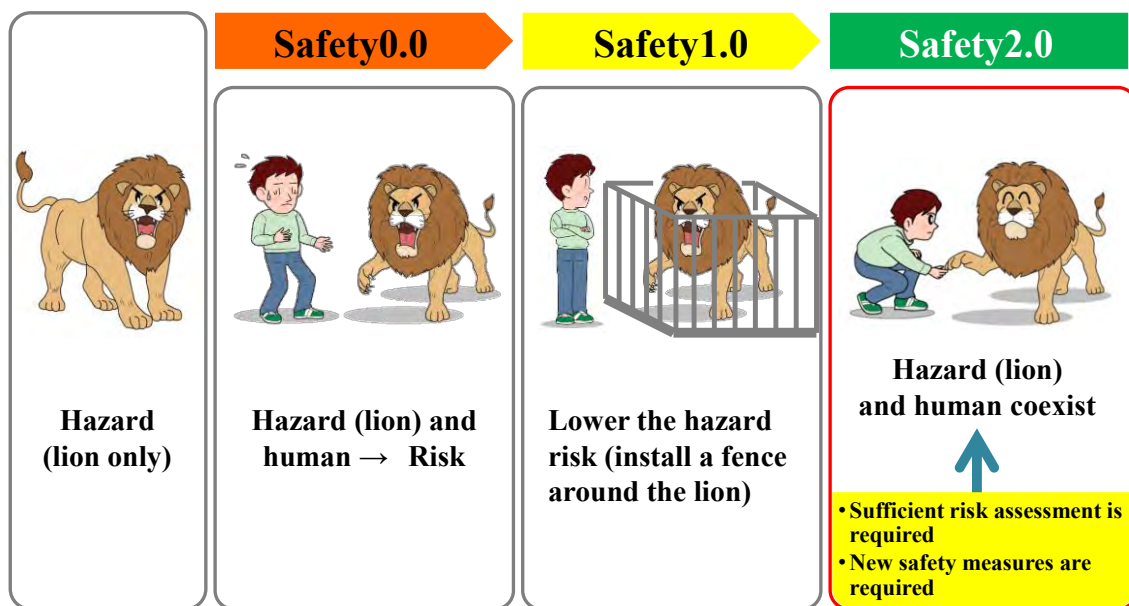
Recently, questions have been raised from automobile and other major industries as to whether Safety1.0 is really the optimal approach. Under Safety1.0, industrial robots must be surrounded by safety guards and these robots stop operating whenever a door is opened. This has raised questions as to whether such robots must always be stopped no matter who opens the door (the person could be an experienced worker or a new worker) and whether it could be possible to keep the robots working or reduce their speed according to the person's qualifications. The fact that using safety guards requires more space calls for alternative solutions. In order to achieve more flexibility and higher productivity, machines must be in operation as much as possible, and the machine area and the human area may be in proximity to each other. Furthermore, there has been increasing demand for a collaborative area, where machines and people share the same space. All this makes it increasingly difficult to ensure safety through the principles of isolating and stopping machines.

Therefore, Safety2.0, a new approach to realizing collaborative safety between people and machines at a higher level, has become necessary so that people and machines can work together in the same area without safety guards,

while ensuring safety and improved productivity. Safety2.0, built on collaboration among people, things, and the work environment, and it is an essential safety concept for creating systems (collaborative safety) which involves the rapid spread of collaborative robots, as seen in Figure 1 (c). The pioneering concept of Safety2.0, developed in 2015 by a group of safety experts in Japan, is currently being introduced to the world. The requirement of Safety2.0 functions are defined as follows [1] [2]:

1. Connects people, things, the work environment, and other constituent elements through ICT
2. Monitors and provides risk-related information (risk/safety information)
3. Upon receiving risk-related information, the system is led by the principles of safety through autonomous control (on its own) or heteronomous control (by people or things in its proximity).

In the above-mentioned case of robots, the introduction of Safety2.0 (collaborative safety) will make it possible for people and machines to work collaboratively without being separated by safety guards. As a result, machines do not have to be stopped repeatedly, people and machines will be able to work in proximity to each other, and machines' downtime during non-routine, human-attended work will be significantly reduced. The average operating rate of the machines will increase and significantly contribute to improving productivity. In addition, the introduction of Safety2.0 will eliminate the need for safety guards, allowing for smaller workspaces and reduced energy consumption. For such benefits to be realized, Safety2.0 must be widely spread, recognized, and adopted. For this purpose, it is essential that based on the new safety concept of Safety2.0, safety levels such as of human-machine collaborative safety be established in such a way that they can be made a global benchmark (international standard). Furthermore, the dissemination and promotion of Safety2.0 on a continuous basis would require more than standardization of Safety2.0 itself. All-encompassing international standards are needed for the associated certification systems, Safety2.0-related technologies, and capability assessments and certifications of human resources essential for the realization of Safety2.0. The example with robots has been cited here as it is perhaps the easiest way to explain the concept. However, Safety2.0 goes beyond this example, as will be explained later. In fact, it can be applied to a wide range of fields other than industrial machinery, or manufacturing itself.



Source of reference: Ministry of Health, Labour and Welfare, Japan Industrial Safety and Health Association

Figure 2. An analogy of the risk and safety establishment concept (lion model).

Figure 2 describes the differences between Safety0.0, Safety1.0, and Safety2.0 using an illustration that can easily be understood. Here, a lion is used in place of a dangerous machine. First, only the lion exists, posing no risks unless there are people present. However, under Safety0.0, a person and the lion coexist in the same space. Staying vigilant is the only way to keep the person from getting injured. This involves a huge risk, as an accident can occur at any time. Safety1.0 ensures safety by putting the lion in a cage and isolating it from the person. Under Safety2.0, the dangerous lion, released from the cage, is trained so that it can coexist with the person in the same environment. This requires thorough risk assessment and a new safety mechanism.

3 SAFETY2.0: FIELDS OF APPLICATION AND DEMAND FOR IMPLEMENTATION

In a pilot study for this project, certified safety assessors who are experts in machinery safety were contacted regarding a questionnaire survey on whether they believe that Safety2.0 will become necessary in the future. As Figure 3 shows, 35% of the respondents said that it will become necessary soon, and 56% said that it will become necessary in the near future. Thus, more than 90% of the safety engineers recognize the necessity for Safety2.0, indicating that Safety1.0, the current approach to machinery safety and functional safety, is widely believed to be inadequate.

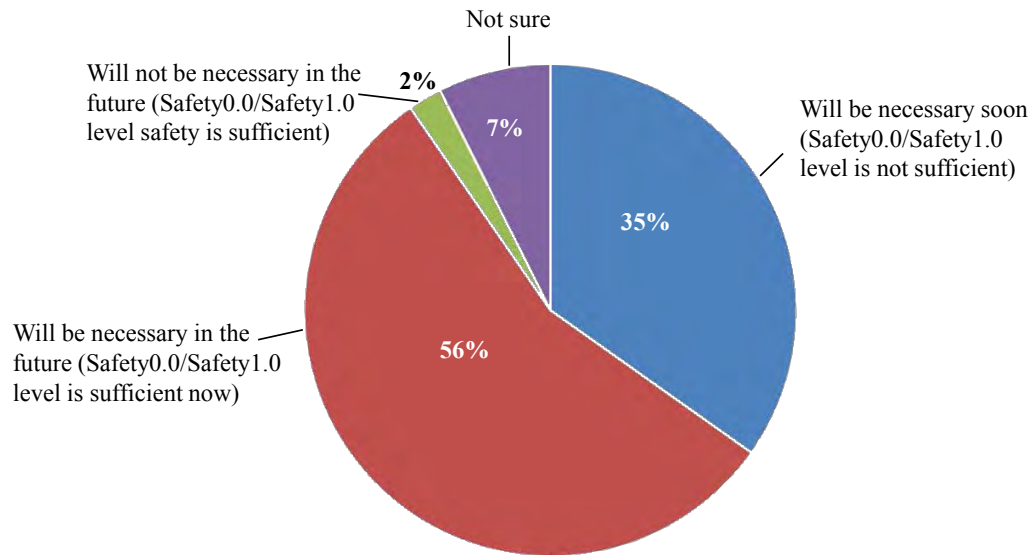


Figure 3. The necessity of Safety2.0 — a questionnaire of qualified safety assessors.

The application fields of Safety2.0 are not limited to manufacturing. In manufacturing, Safety2.0 is expected to improve both safety and productivity by allowing for flexible control options of machine operations, in accordance with the capabilities of the worker. According to a study conducted by Nikkei BP, Safety2.0 (collaborative safety) can meet the needs of diverse fields, including civil engineering and construction, medical and nursing care, transportation, public facilities, infrastructure, and housing, in addition to manufacturing [5].

Safety2.0 is expected to be adopted in the fields of Safety0.0 sites where Safety1.0 is difficult to implement, and where workers are responsible for reducing many of the risks themselves. The safety implementation process will generally begin with Safety0.0, proceed to Safety1.0, and then move to Safety2.0 in factories or other locations where machines are used. However, there are many fields where Safety0.0 must be upgraded directly to Safety2.0, skipping completely over Safety1.0. This is exactly where future growth lies.

4 MANAGEMENT SHOULD BE KEENLY AWARE OF THE IMPORTANCE OF SAFETY AND START MAKING INVESTMENTS TO KEEP UP WITH THE NEW SAFETY TRENDS

Under Safety1.0, safety experts and engineers have been able to manage risks using risk-assessment methods and risk-reduction methods based on international safety standards. However, Safety2.0 will require systemic concept formulation and risk-assessment at a higher level. Thus, senior managers and supervisors must identify the changes that are currently taking place and foresee future developments, instead of leaving the matter entirely to employees who are directly responsible. The first priority for companies should be safety management. However, senior managers are often reluctant to invest in safety, hoping to reduce safety expenses and maximize profits. Is this a correct approach? Figure 4 provides some interesting data.

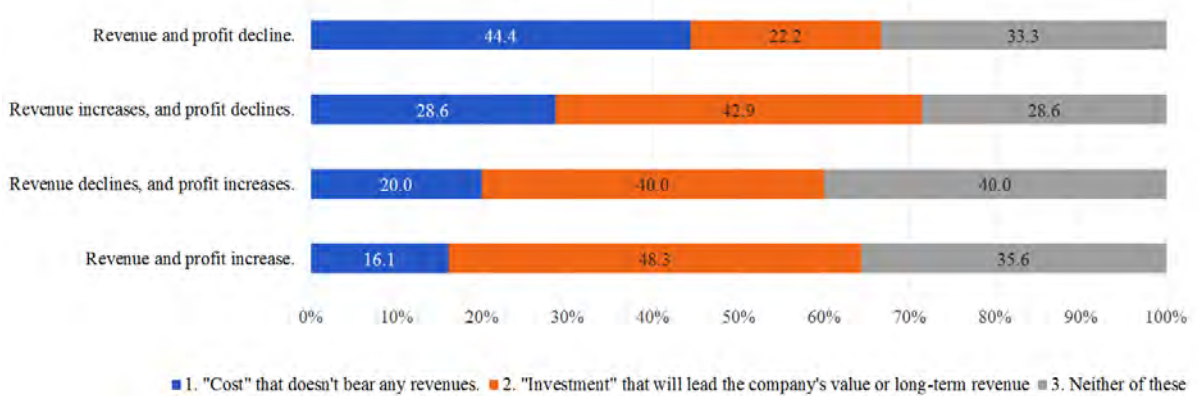


Figure 4. Correlation between corporate business performance and top management's attitude toward safety.

This is the result of a survey conducted by the Institute of Global Safety Promotion (IGSAP) in the spring of 2017 involving members of the Safety Assessor Council in Japan, which is made up of people who hold certifications under the Safety Assessor (SA) qualification system sponsored by the Nippon Electric Control Equipment Industries Association. The survey indicates that companies that regard safety measures as an investment tend to have higher revenue and profits, while those that regard safety as a cost often have lower revenue and profits. The same survey also sought to identify the job positions of employees who are responsible for safety (i.e., executives, managers, or persons in charge). The respondents, certified safety assessors, were also asked whether their companies were strategically pursuing safety measures, or handling safety issues in a haphazard manner. The result is shown in Figure 5. According to the survey, only 20% of the respondents said that executives in their companies were directly involved (shown CZ in Figure 5), and that these executives were pursuing the efforts strategically from the perspective of improving corporate value. A total of 40% said that executives at their companies were not involved and that their companies did not have any strategies regarding this matter.

The survey revealed that the situation in Japan is, in fact, dismal, even as the nation promotes the goal of becoming the safest country in the world. As long as executives persist in their erroneous view that safety is a cost, despite the new safety trends, there remains a danger that they could end up implementing superficial measures only. In fact, safety investments are the very means by which people can regain their human-centered work-style, accomplish a true work-style reform, improve productivity, and help companies improve earnings. Executives should keep this in mind.

- I. First-class executives believe that "safety and productivity is compatible."
- II. Second-class executives think "safety and productivity cannot be compatible, but safety is important."
- III. Third-class executives do not even want to spend money on safety.

Source of reference:
 "Thoughts on Safety and Health" by Hiroyuki Takaoka, Safety Lead Assessor (SLA)
 Auditor of Japan Industrial Safety and Health Association, Management System Audit Center and The Institute of Global Safety Promotion

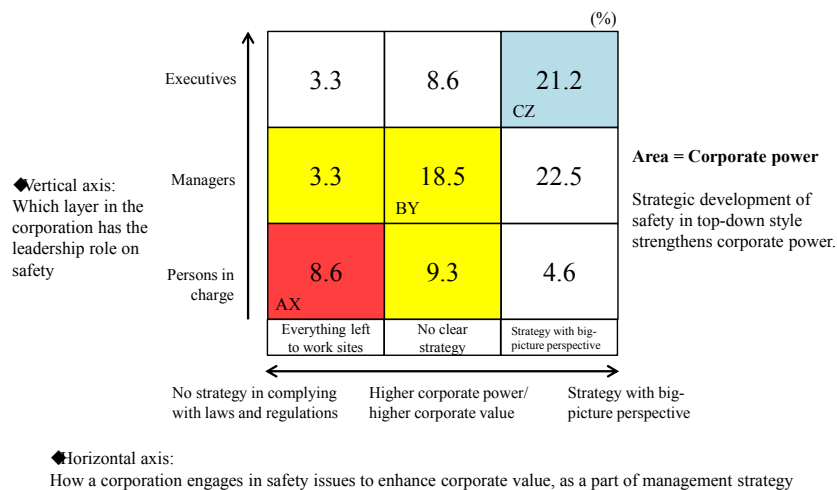


Figure 5. Top management's attitude toward occupational safety and health.

5 THE FUTURE SAFETY CONCEPT WITH EIGHT PRINCIPLES

Against this backdrop, the Future Safety Concept is proposed here [4]. The concept was developed to serve as a signpost for the creation of a future society. It provides guidelines for the establishment of an advanced society amid the Fourth Industrial Revolution, with a society centered around human beings who are the source of added value amid work-style reforms, and the world's safest society for the Tokyo Olympic and Paralympic Games. Specifically, the Future Safety Concept is made up of eight principles, as shown in Figure 6.

Future Safety Concept

1. Drive safety in top-down management style
2. Safety is an investment, not a cost
3. Invest in safety human resource development
4. Invest in the latest safety technology
5. Society must evaluate safety properly
6. Safety must be established by country, companies, and individuals
7. Observe safety from an unbiased, comprehensive viewpoint
8. Data of accidents and risks are society's shared assets

Figure 6. The Eight principles of the Future Safety Concept.

First, safety should be pursued in a top-down style. In Japan, corporate safety management has primarily been handled in a bottom-up manner based on the voices of actual factory workers. Since 1973, the Japan Industrial Safety & Health Association (JISHA) has been aggressively urging Japanese companies to conduct hazard prediction activities, known as KY activities (with “K” standing for “*kiken* [hazard],” and “Y” for “*yochi* [prediction]”) to help create safer workplaces. Such activities were extremely effective in identifying risks and sharing information through risk assessment. These efforts, in conjunction with quality control (QC) activities, have achieved a great deal of success. Even so, those at worksites do not normally have the authority with respect to investing resources on safety measures. Thus, in order for companies to implement effective safety measures based on risk assessment, it is essential that the issue be handled in a top-down style with the management providing impetus and exercising decision-making authority. Safety can be achieved when not only the conventional bottom-up approach but a strong top-down management approach is taken.

Secondly, safety should be regarded not as a cost but as an investment. According to studies conducted in Japan and Europe, the cost-benefit ratio of safety investments is greater than 200%. In any event, the idea that safety does not produce value is clearly a misconception. This gives rise to the question: in which areas should investments be made? The answer is in the third and fourth proposals.

The third proposal calls for investments in human resource safety development. The way in which safety is achieved will drastically change from isolation to collaboration, particularly when driving the Fourth Industrial Revolution. Japan's Safety Assessor (SA) qualification system has been in operation since 2004 and produced some 15,000 qualified safety assessors to advocate workplace safety, which is reported at the 9th International Conference on Safety of Industrial Automated Systems (SIAS 2018) in the Nancy, France [6]. In addition to fostering engineers, Japan must establish a mechanism in which all corporate employees – from senior executives and managers to rank-and-file workers – acquire basic knowledge on, and an approach to, safety as well as proper safety awareness.

The fourth proposal relates to investments in the latest safety technologies. One of the upcoming challenges in Japan is that there will be an increase in the number of elderly workers. Their safety will be enhanced if a decline in their physical and cognitive functions is supplemented by the use of information technology. With respect to technological sophistication, complications, and expansion, an extensive sensor surveillance network should be able to handle the risks that can no longer be detected with human eyes. Safety2.0, as discussed above, will provide critical technologies to facilitate innovation in various fields.

In the fifth proposal, it is essential that companies that are aggressively investing in safety, or making other sincere efforts to build safety structures, are properly evaluated by society.

Sixth, safety must be established by the government, companies, and individuals. Up until now, safety has been maintained mainly through national regulations and efforts on the part of companies. However, in the midst of great social changes many risks have emerged that cannot be controlled either by the government or companies. A typical example would be malicious security breaches that can occur in a networked environment. Flippant behavior and the carelessness of individuals can instantly turn their devices into weapons. Individuals must become aware, more than ever before, that they bear the ultimate responsibility to deal with risks.

These six proposals have been made from a viewpoint of active safety. This does not mean, however, that accidents and disasters will completely disappear. What is important for the industrial sector is how to respond to an accident once it occurs. The focus should be on why it occurred, not who caused it. The seventh proposal, therefore, is to observe safety from an unbiased and a comprehensive viewpoint. Those involved in safety tend to focus so much on their own field of responsibility that they sometimes lose perspective, and forget their role in the whole initiative. They also tend to be overly caught up in details when investigating the cause of an accident. It is important that they seek to grasp the true nature of things from an unbiased and comprehensive viewpoint. In addition, data on accidents and risks are society's shared assets, and, as such, should be shared by society. This is the final proposal. When the true nature and the cause of an accident are elucidated, the data should be shared to the greatest extent possible, instead of keeping everything classified.

In Japan, the Public-Private Council for Safety Measures in Manufacturing Industries, established by the Ministry of Health, Labour and Welfare, the Ministry of Economy, Trade and Industry, JISHA, and 10 major manufacturing industry associations for the purpose of bolstering safety measures in manufacturing industries, held a special session in Kobe in November 2017. There the council released a statement, the Kobe Declaration, which, under the guiding principle of respecting human life ("each and every individual person is irreplaceable"), put forth the following four management principles [7]:

1. Strengthen mechanisms to enable management to exercise leadership and communicate with safety personnel and manufacturing personnel, so that the voice of the workplace will always be heard
2. Promote safety investments based on the understanding that new initiatives are being pursued in tandem with the technological revolution, even though the situation remains difficult due to the aging of facilities
3. Expand safety training and strengthen the nurturing of safety personnel, including employees of partner companies, by tailoring training programs according to workers' job positions, in line with changes in the work environment, such as a decline in the number of experienced employees and an increase in work outsourcing
4. Identify priority issues to be dealt with, study their cause and countermeasures, and share the outcomes of the study with those inside and outside the industry

The Future Safety Concept, advocated by IGSAP, shares the same goal as the Public-Private Council for Safety Measures in Manufacturing Industries. This vision calls for the nurturing of a corporate safety culture and the implementation of safety measures through a top-down management approach in all industrial sectors.

The developments up to the present, amid these new safety trends, are shown in Figure 7.1 in the form of a 3x3 matrix. The horizontal axis lists Safety0.0, Safety1.0, and Safety2.0, showing chronological changes and the evolution of people's attitudes toward occupational safety. On the vertical axis, the bottom section shows field activities and technologies, the middle section personnel training and qualifications, and the top section the vision and management.

First, here is what has been happening in Japan. Since 1973, JISHA has been calling for people's improvement in safety skill in a bottom-up manner, as stated above and shown in Figure 7.2 (a). The practice has firmly taken hold in Japanese society. In addition, as Figure 7.2 (b) shows, many manufacturers in Japan have adopted measures to improve machinery safety and functional safety, and have achieved a reduction in workplace risks as machinery safety was widely spread (Safety1.0). The Safety Assessor/Safety Basics Assessor (SA/SBA) qualification system was introduced to train and certify workers, as seen in Figure 7.2 (c) [8].

Now, these qualifications are starting to be established as Japanese Industrial Standards Committee (JIS) or international standards by the IECCE. In Japan, upper management has not been fully committed to safety issues, as explained above. Thus, as seen in Figure 7.2 (d), the Public-Private Council for Safety Measures in Manufacturing Industries is calling for a top-down management approach to improving workplace safety.

In addition to the above developments, the Future Safety Concept has been proposed in preparation for the arrival of the Safety2.0 era, a period of emerging new technologies, as shown in Figure 7.2 (e-1). In order to lay the groundwork for Safety2.0, various efforts are initiated to develop new technologies, to make international standard proposals, and to study the prospective certification system scheme, as shown in Figure 7.2 (e-3). Furthermore, as shown in Figure 7.1 (e-2), qualification systems for robot safety assessors and safety officers are being developed as new systems to foster human resources aligned with the above developments. At the same time, proposals for new international standards are also being prepared.

As these changes unfold, organizations such as IGSAP, JISHA, Nippon Electric Control Equipment Industries Association (NECA), Japan Robot Association (JARA), Japan Institute of Occupational Safety and Health, Japan (JNIOSH) and some of the progressive companies in Japan, are participating in various forums and committee meetings to achieve the goals described in Figure 7.2 (e-1) through (e-3) with the support of government ministries and agencies.

	Safety0.0 Safety depending on human attention	Safety1.0 Safety by isolating machines from humans	Safety2.0 Collaborative safety by linking humans, machines, and environment)
Vision/ System			
Personnel training			
Field technology			

Figure 7.1. Safety 3x3 matrix roles.

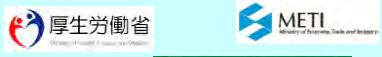



	Safety0.0 Safety depending on human attention	Safety1.0 Safety by isolating machines from humans	Safety2.0 Collaborative safety by linking humans, machines, and environment)
Vision/ System	Ministry of Health, Labour and Welfare Ministry of Health, Economy Trade, and Industry (d) (Since 2017)  Public-Private Council for Safety Measures in the Manufacturing Industry		(e-1) (since 2017)  Future Safety Concept (IGSAP)
Personnel training	(a)  (since 1973) Zero Accident Campaign (JISHA)	(c) (since 2004)  Safety Assessor/ Safety Basic Assessor qualification	(e-2) (since 2018) Robot Safety Assessor Qualification System Safety Officer Qualification System
Field technology		(b) (since 1995) Machinery Safety Functional Safety	(e-3) (Since 2015) Safety2.0 implementation

Figure 7.2. Safety 3x3 matrix roles and the evolution of safety concepts in Japan.

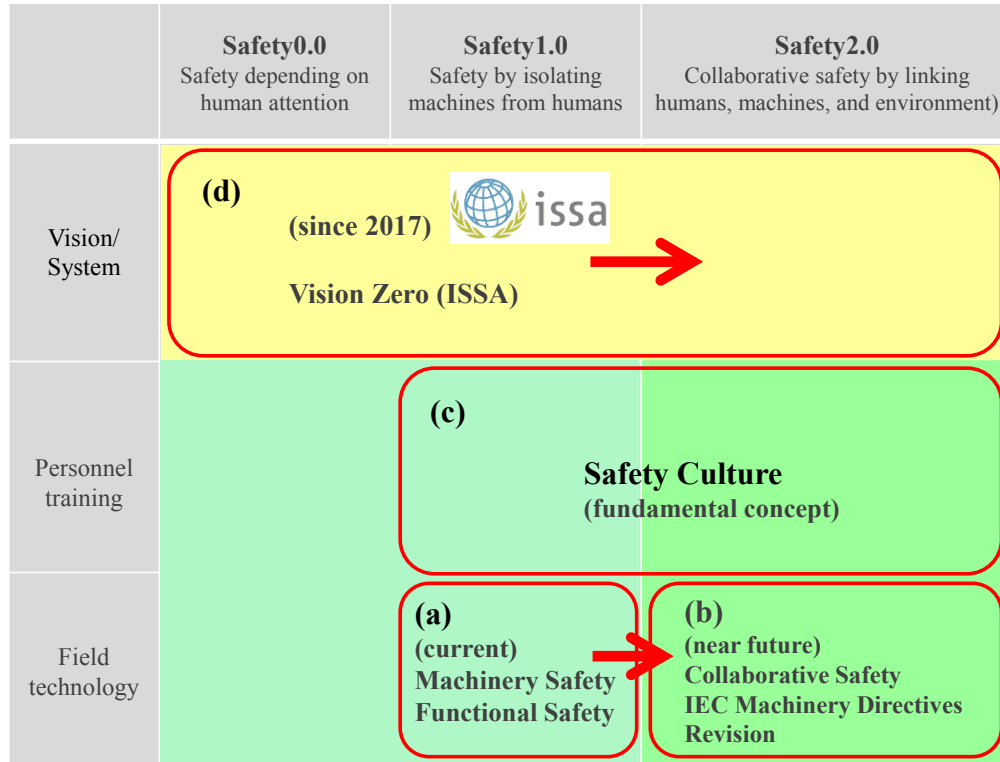


Figure 7.3. Safety 3x3 matrix roles and the evolution of safety concepts in Europe.

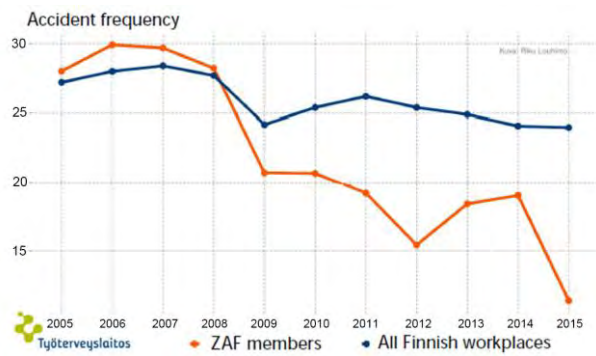
6 THE EUROPEAN COMMISSION’S ANNOUNCEMENT AND NEW DEVELOPMENTS INVOLVING VISION ZERO

The developments, which are taking place in Japan, are also in accordance with what is happening in many other parts of the world. It is expected that such developments will become a global trend with respect to technology, human resources, and management. For example, in May 2018, on the European Commission website there was a reference to this technological aspect: “The Commission will launch a study to further look into certain aspects of emerging technologies, such as issues arising from human-machine collaboration, which are not explicitly addressed by the directive [9].” How to apply the collaborative safety (Safety2.0) concept to society will inevitably become the most important issue following this discussion over the next few years. Proposals for the necessary international standards and certification systems are planned to be considered along with new human resource systems.

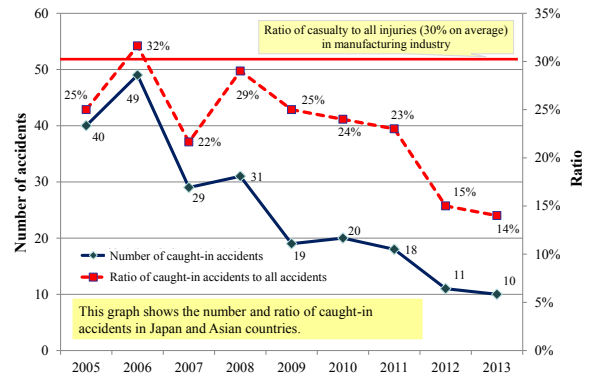
Another important development regarding management and human resources is the concept of Vision Zero, which was launched by the International Social Security Association (ISSA) in September 2017 [10]. The goal is to achieve a high level of safety, health, and wellbeing, not through a conventional management methods, but through the proactive sharing of ideas on safety and the implementation of such ideas under the direct leadership of top executives, as well as the (bottom-up) involvement of workers [11]–[13]. In Europe, as precursors to a Vision Zero, Zero Accident Forum based on the Zero Accident Vision was developed in Finland, Germany, and Holland, where companies benchmark in good practice, and positive proactive key safety performance indicators [14].

The developments in Europe are shown in Figure 7.3 (a). Machinery directives regarding machinery safety and functional safety, along with onsite safety activities, will be transitioned to collaborative safety, as indicated in Figure 7.3 (b). Strong safety culture that forms the basis for training personnel in Safety1.0 remains important in Safety2.0, as shown in Figure 7.3 (c). Since Vision Zero, an overarching concept, will be pursued by top management, it can be understood in terms of its location within Figure 7.3 (d).

As mentioned above, from a historical standpoint, the Zero Accident Campaign originally started in 1973 and spread widely throughout Japan [15]. For this reason, Japan is the world’s leading promoter of zero accident initiatives. However, these campaigns have been implemented in a bottom-up manner in Japan, with a top-down approach rarely being pursued. In practice, it is important to integrate both top-down and bottom-up approaches, and these two approaches are the key to a new movement, the new Zero Accident Campaign.



(a) Comparison of accident rates between all Finnish workplaces and ZAF member companies



(b) Caught-in accidents at AGC Inc. in Japan and Asian countries

Source of reference: Finnish Institute of Occupational Health (FIOH), AGC Inc.

Figure 8. The trend of accidents in Finland and AGC Inc. (Japan and Asian countries).

Describing details about Vision Zero would require a vast amount of space. Thus the outcome of only a few cases will be cited below. For example, a comparison of 400 companies participating in the Zero Accident Forum (ZAF) in Finland indicates that the ZAF member companies that have executives involved in the initiative are far more likely to reduce the number of accidents than non-member companies, as shown in Figure 8 (a). The member companies have succeeded in drastically reducing the number of accidents. In Japan, AGC is a successful case. AGC has significantly reduced the number of accidents thanks to the commitment of President Kazuhiko Ishimura, and the various safety measures as shown in Figure 8 (b). The company’s introduction of SA qualification system turned out to be extremely effective, according to President Ishimura, who spoke at a meeting of the Public-Private Council for Safety Measures in Manufacturing Industries held in September 2017 at the Ministry of Economy, Trade and Industry [16]. If such a management method becomes an international standard, it could contribute to a reduction in accidents on a global scale. In fact, this is the idea behind Vision Zero, which is in full accord with Japan’s Future Safety Concept.

With these developments and the Zero Accident Forum (which is successful in Finland) as benchmarks, a Safety Management Forum has also been launched in Japan this year. What is unique about Japan’s efforts is that parallel initiatives are also being undertaken to implement Safety2.0. These activities will be bolstered even further. The introduction of new Safety2.0 technologies, the nurturing of various human resources and the strengthening of management, are some of the initiatives to be undertaken. These initiatives will be strongly promoted so that progress will be reported at the upcoming SIAS conferences.

7 CONCLUSION

This paper provided a summary of new safety and *anshin* initiatives that are being undertaken in Japan from the aspects of technology, management, and human resource development. In Japan, engineers used to take the leadership in such efforts, with a focus on machinery safety which has subsequently developed into functional safety. However, in the Fourth Industrial Revolution era, safety should be viewed from a broader perspective and pursued in a more comprehensive manner. Now is the time for the world to unite to develop a new approach to safety, and jointly establish international safety standards. Japan will do its part in this endeavor. Opinions and criticism are most welcome regarding this paper. Readers are also strongly encouraged to visit Japan, where the Robot Revolution is rapidly progressing, and to take part in various discussions.

8 REFERENCES

1. Nikkei Business Publications Safety2.0 Project, *Safety2.0 – Concept*, 2015 (in Japanese).
2. Mukaidono M., *The Japan Society of Information and Communication Research Journal*, Vol. 34, No. 1, 2016-6, pp.41-46 (in Japanese).
3. Nikkei Business Publications Safety2.0 Project, *Safety2.0 – Applications*, 2017 (in Japanese).
4. The Institute of Global Safety Promotion, Nikkei BP Intelligence Group, *Future Safety Concept – Safety2.0 Leads a New Society*, 2017 (in Japanese).
5. Dohi M., *Proposal of collaboration safety guide at agenda item 11.2*, presentation document at IEC/Advisory Committee on Safety (ACOS) meeting, Delft, Holland, June 28, 2018.

6. Fujita T., Kubota A., Ariyama M., Kodaira N., Maeda. I., Kanamaru H., Matsuura H, Kajiya T., and Mukaidono M., *Development of Human Resources in Safety in the 4th Industrial Revolution Period: Current Status of Safety Assessor Qualification System and the Future Development Prospect in the Fields of Robotics, Corporate Management, and Collaborative Safety (in press)*, 9th International Conference on Safety of Industrial Automated Systems (SIAS), France, 2018.
7. The Public-Private Council for Safety Measures in the Manufacturing Industry <https://www.jisha.or.jp/seizogyo-kyogikai/> (in Japanese).
8. Fujita T., Shiomi M., Ishikawa K., Nonaka S, Kanamaru H., Tochio M., Ariyama M., Sagawa K., Takaoka H., Kuroda A., Mukaidono M., *Current situation of safety assessor and safety basic assessor (SA/SBA) qualification system: Reduction of accidents achieved by a Japanese company and recommendation by Japanese Ministry of Health, Labour and Welfare*, 8th International Conference on Safety of Industrial Automated Systems (SIAS), Germany, 2015.
9. European Commission - Daily News 07/ 05/2018
http://europa.eu/rapid/press-release_MEX-18-3723_en.htm.
10. Vision Zero (ISSA) <http://visionzero.global/>.
11. Zwetsloot G. I. J. M., Kines P., Ruotsala R., Drupsteen L., Merivirta M., Bezemer R.A., *The importance of commitment, communication, culture and learning for the implementation of the Zero Accident Vision in 27 companies in Europe*, Safety Science, Vol. 96, 2017, pp. 22-32.
12. Zwetsloot G. I. J. M., Leka S., & Kines P., *Vision Zero: From accident prevention to the promotion of health, safety and well-being at work. Policy and Practice in Health and Safety*, Journal Policy and Practice in Health and Safety, Vol. 15, 2017, Issue 2, pp. 88-100.
13. Jain A., Leka S., Zwetsloot G. I. J. M., *Managing Health, Safety and Well-Being, Ethics, Responsibility and Sustainability*, Springer Science+Business, Dordrecht, 2018.
14. Zero Accident Forum (FIOH) <https://www.ttl.fi/en/training-and-advisory-services/zero-accident-forum/>.
15. Zero Accident Campaign <http://www.jisha.or.jp/zerosai/zero/index.html> (in Japanese).
16. Takaoka H., *The day Japan realizes the safest workplace in the world*, Gold Prize, A Collection Short Essays to Commemorate the 100th anniversary of OSH movement, 2011, pp. 4-14 (in Japanese).

New Collaborative Safety Concept in Various Coexistence Areas for Human and Machinery

Shimizu T., Fujitani S., Maeda I., Okada K., Dohi M., Fujita T.

IDEC CORPORATION – 2-6-64, Nishimiyahara, Yodogawa-ku, Osaka, Japan

t.shimizu@jp.idec.com

s.fujitani@jp.idec.com

i.maeda@jp.idec.com

k.okada@jp.idec.com

m.dohi@jp.idec.com

t.fujita@jp.idec.com

KEYWORDS: safety of machinery, robot, human factor, collaborative safety, CSL

ABSTRACT

The world is entering the new era of the Fourth Industrial Revolution. ICT has made it possible to connect various things via networks and to utilize the cloud and AI technologies to achieve optimization and efficiency. Manufacturing sites are also transforming their modes significantly on a global scale. In order to respond to the increasingly diversifying market needs, it is necessary to establish collaborative area where the machine-operation area and human-operation area can overlap, while ensuring safety and productivity to achieve flexible production. For this purpose, collaborative work by human and machines that runs without the need of stopping machines is required. In such a situation, it is difficult to apply the conventional safety principle of “isolation and stop” that a human cannot enter a dangerous area while the machine is moving, and can enter a dangerous area only while the machine has stopped moving. To meet the new challenge in the transforming manufacturing sites, we present the Collaborative Safety Level (CSL), a new collaborative safety benchmark based on the Safety2.0 concept. This is a new, ideal safety collaborative safety concept for ensuring productivity and safety in human-machine collaborative environment. In an environment where humans and machines work collaboratively, it is essential to take parameters of humans into consideration, not only of machines. CSL is completely a new, unconventional safety benchmarking method, with an epoch-making concept to realize the Fourth Industrial Revolution, which enables high-level realization of both productivity and safety by way of utilizing the data of human, machine and environment. This paper reports on the actual examples of production system constructed with Safety2.0 and CSL concepts [1]-[7].

1 SAFETY2.0 OVERVIEW

In factory automation environment of recent years, collaborative robots have been developed and introduced to the market to allow them work without stopping to the maximum extent possible, in collaborative areas where the robot area and human area are overlapped [8]-[10]. Collaborative robots not only enable humans and robots to work in shared areas but can replace human operations to improve work efficiency and flexibility. Thus, improved production efficiency and cost reduction can be expected in various types of fields. Collaborative area of humans and robots/machines are expected to increase in various applications, far beyond factory automation.

Meanwhile, conventional safety concept is becoming less applicable in human-machine collaborative areas. The conventional safety concept to secure safety by training personnel and by isolation/stop principle is about to change reflecting the change in manufacturing sites. The most elemental way to ensure safety is Safety0.0, in which safety depends on human’s attention and judgement alone as shown in Figure 1 (a). Humans, however, are prone to make mistakes and Safety0.0 is not enough to ensure safety, therefore the concept has developed to Safety1.0 to secure safety with machine system designs as shown in Figure 1 (b).

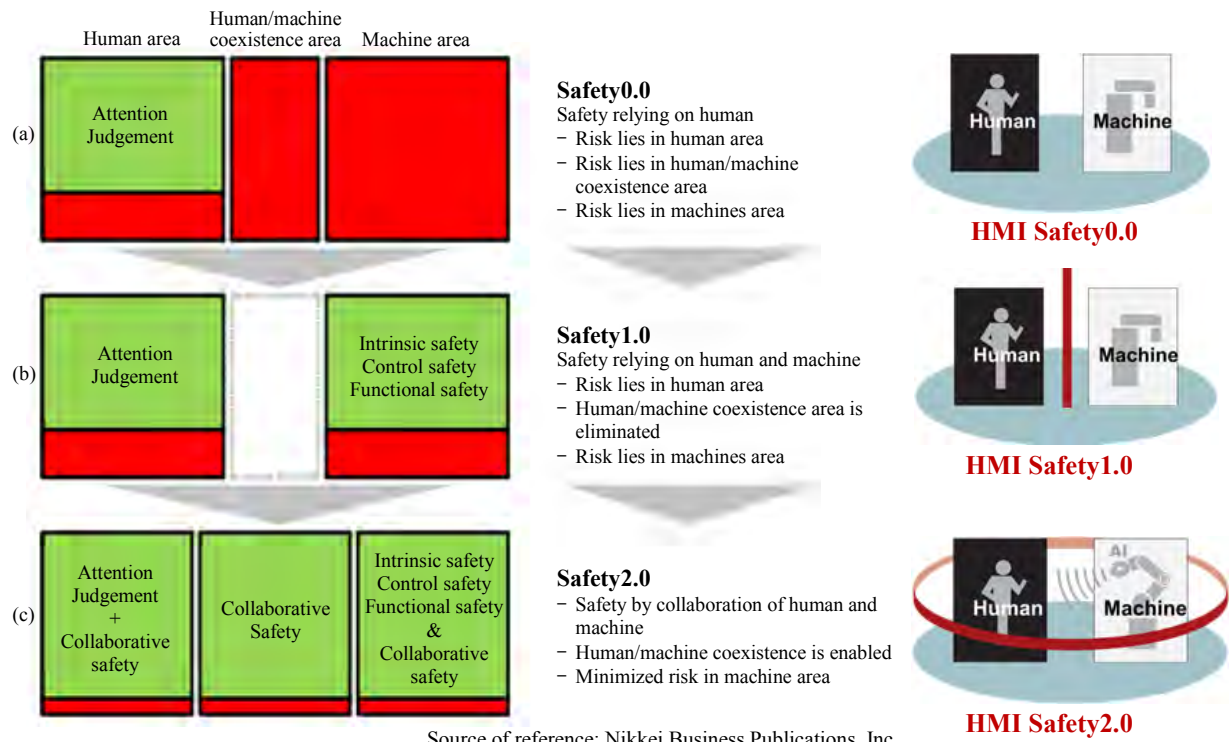


Figure 1. Safety evolution from Safety0.0, Safety1.0, and to Safety2.0.

In factory automation, many international safety standards are available for the safety of machinery provided by ISO and IEC. Fail-safe and fail-proof machines can be designed by conforming to the requirements of these standards. Examples of applying such standards would include a system that ensures safety by firstly defining the ranges of machine-movement and human-movement, and installing a fence or interlock device of adequate specifications to make sure that humans do not enter the hazardous area while the machine is running, and to allow humans to enter the area only when the machine has stopped. This is Safety1.0 concept to ensure safety by the safety of machinery principle: isolation and stop [11].

In recent years, a new safety concept named Safety2.0 has emerged, where human-robot collaborative safety is achieved at a high level. Use of collaborative robots is exploding rapidly, and Safety2.0 concept by the collaboration among humans, machines, and environment is an integral part when constructing systems with collaborative robots (collaborative safety) as shown in Figure 1 (c). In various manufacturing industries of medicines, cosmetics, food, and other industries such as nursing care/service and civil engineering/construction, there are settings where the conventional Safety1.0 concept is not applicable, because humans and machines cannot be separated — where humans and machines need to coexist. In order to establish safety in such environment, collaborative safety based on Safety2.0 concept is necessary.

2 CSL CONCEPT

Performance Level (PL) is one of the most classic safety benchmarks in the conventional safety concept Safety1.0, which is a performance level of safety-related part in machine systems. The level does not include human parameters, because humans and machines are separated in Safety1.0 and only the safety performance of machine systems needed to be taken into consideration [12]. In environments where humans and machines are present at the same time, human aspect is an indispensable parameter, requiring a new safety benchmark. In Safety2.0, safety is established by the collaboration among human, machines, and environment as shown in Figure 2. Data from humans control machines, and data from machines induce humans to take action. The human-machine environment is optimized by employing technologies such as ICT. Data from humans consist of static and dynamic information. Static information include knowledge of machinery safety, work-related roles (e.g., maintenance personnel, administrator), and competency of operators based on job experience. Dynamic information include location, vital (e.g., pulse, body temperature), behaviour (instant reaction, motion), and operation. Feeding these data to machines can optimize speed and other controls.

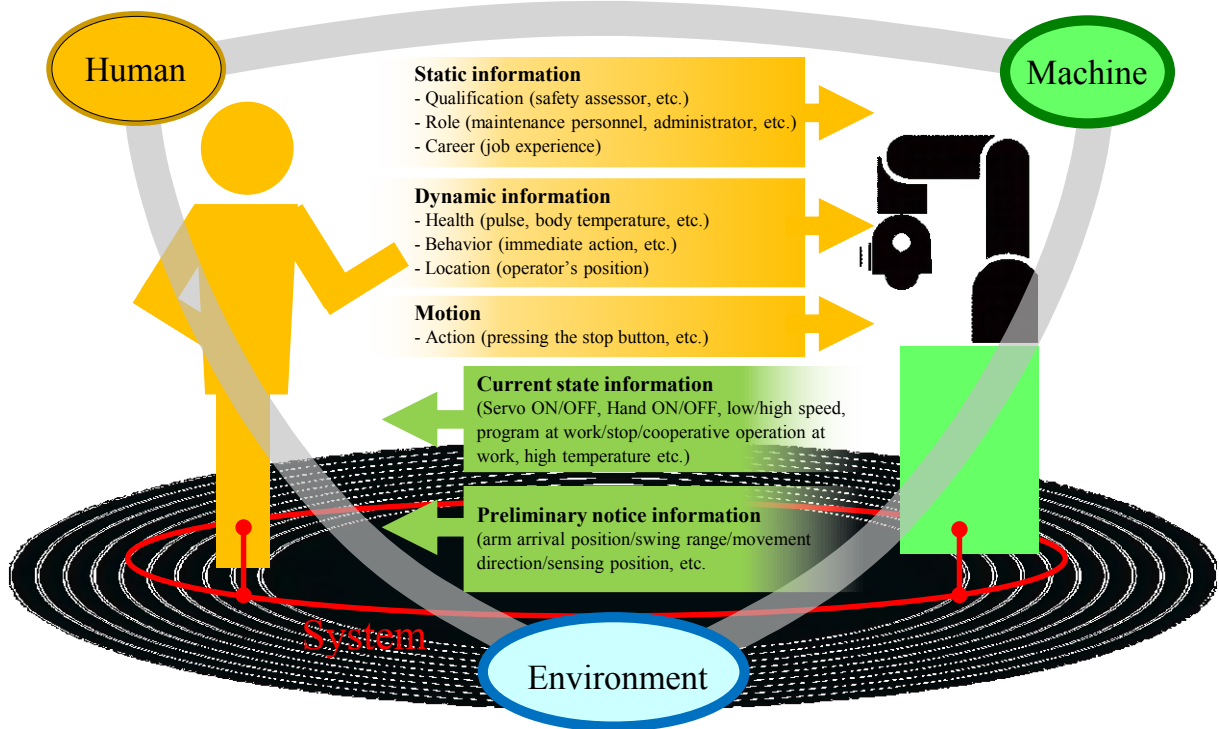


Figure 2. Collaborative safety by connecting human and machine.

The Collaborative Safety Level (CSL), shown in Figure 3, is the new collaborative safety benchmark in four levels CSL1, 2, 3, and 4. Figure 4 shows the concept examples of CSL. Among four levels, CSL1 is the most basic level that requires operators to satisfy two requirements: basic knowledge of safety of machinery, and securing means to stop machines from anywhere in the work area to ensure *anshin* for operators (*anshin*: a sense of trust and assurance without any fear or stress).

In CSL2, in addition to the CSL1 requirement, properly controlling the machines by utilizing human information is required. In CSL3, in addition to the CSL2 requirement, machine information needs to be sent to humans to induce required action. And in CSL4, the condition of humans and machines need to be maximized, in addition to the requirements of CSL3. The CSL concept is completely different from that of conventional safety, yet CSL does not deny the conventional concept. Rather, it complements the conventional concept. Performance Level (PL) and Safety Integrity Level (SIL) are used as benchmarks to define the safety level of safety-related parts in machine systems, with factors such as the failure rate of dangerous failures [13]. CSL defines human-machine collaborative safety, and evaluates the entire environment where humans and machines coexist.

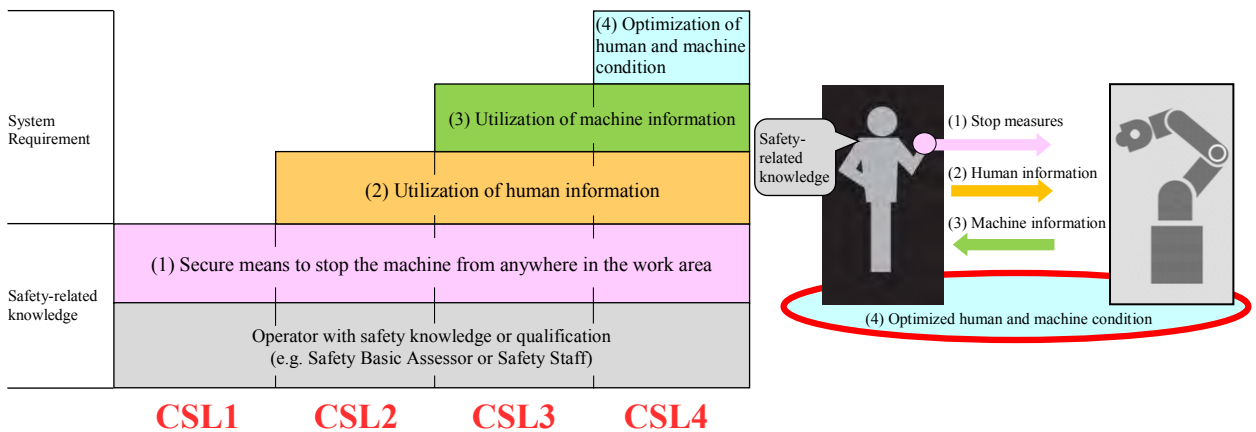


Figure 3. Collaborative Safety Level (CSL).

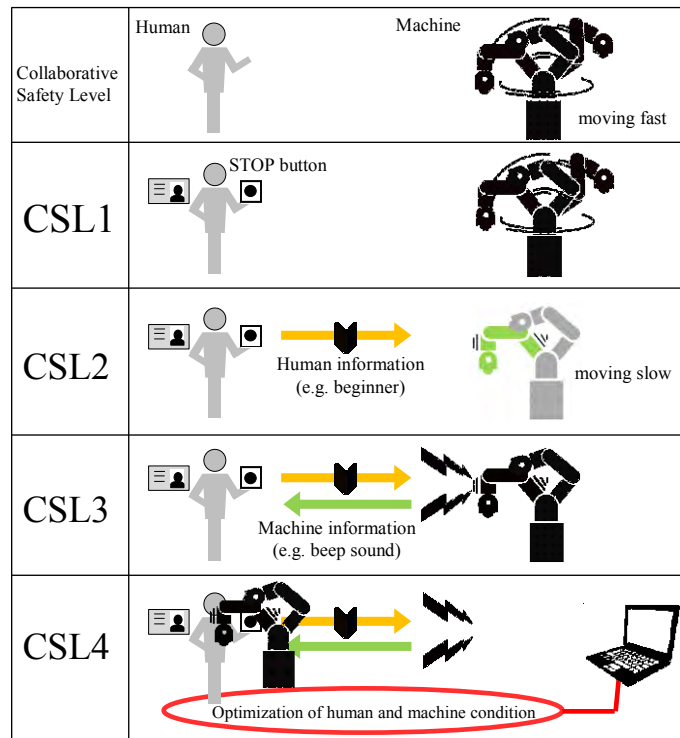


Figure 4. Concept examples of CSL1 to CSL4.



	PL/SIL (Performance Level/ Safety Integrity Level)	CSL (Collaborative Safety Level)
Basic concept	Safety1.0	Safety2.0
Evaluation Target	Machine system 	Area where humans and machines coexist 
Purpose of Index	To define safety of machine's Safety-related system based on dangerous failure rate, etc.	To define collaborative safety of humans and machines
Classification	PL: a, b, c, d, e SIL: 1, 2, 3	CSL: 1, 2, 3, 4

Figure 5. Comparison between PL/SIL and CSL.

3 WORKPLACES SUBJECT TO SAFETY2.0

A production system employing a collaborative robot with Safety2.0-based CSL concept is explained here. Figure 6 shows a testing/marketing system for IDEC control component products. In this system, finished products are stored in trays that are then transferred to a cart. The cart is placed on the pre-test lane by an operator. The collaborative robot takes out the product from the pre-test lane and places it on the test system, where the product receives performance check and laser marking. The collaborative robot then takes the finished product back to the tray. After all products on a tray finish testing and marking, the tray moves to the test-complete lane. The next tray appears, with products waiting for testing and marking. The close-up image of the collaborative robot and the details of testing system are shown in Figure 7.

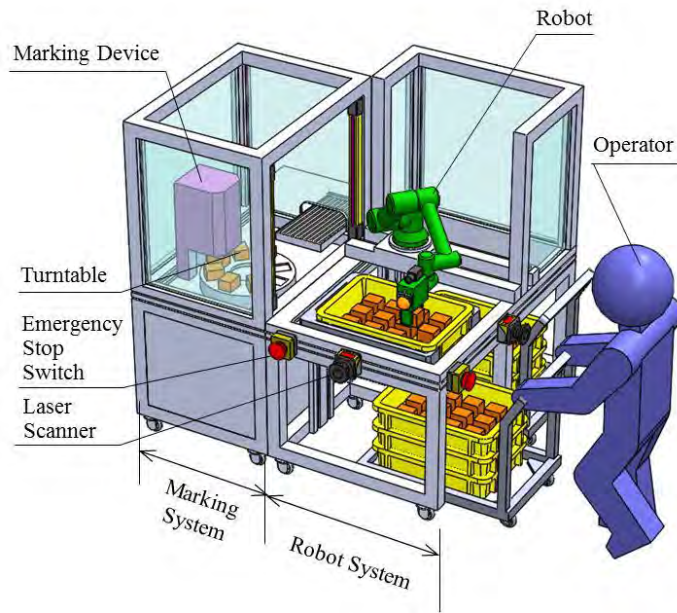


Figure 6. The entire system consisting of marking and robot systems.

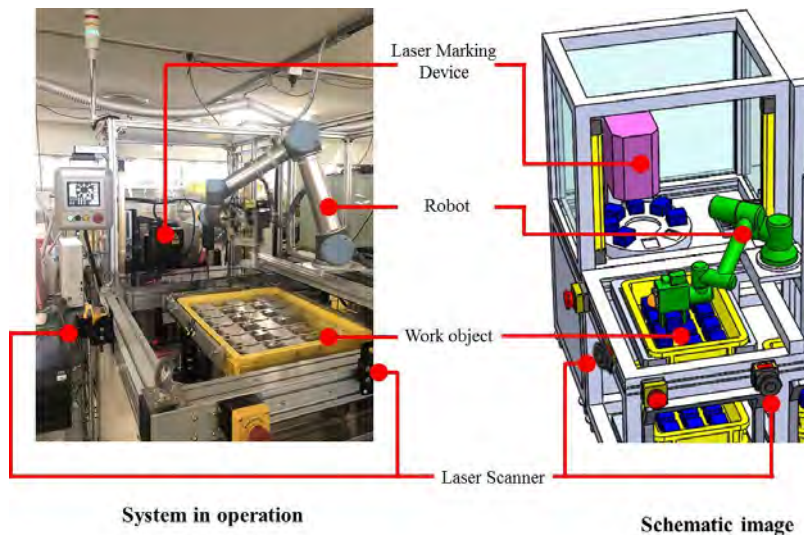


Figure 7. Actual example of human-robot collaborative operation system.

As shown in Figure 8, an operator places products on test equipment in conventional systems. In the new system using a collaborative robot, the test and robot systems can be separated and reconnected easily. Test system and robot system are configured as separate systems, and the test system can operate stand-alone. Robot system has auto-calibration function using image analysis, and can be reattached to the test system easily. By utilizing robots when producing small variety of products in large quantities, and by having an operator to work on the production of various types in small quantities, high productivity and efficiency can be attained in testing and marking.

The CSL concept was introduced as a test case to the production/testing system to make it Safety2.0 compliant, in order to further improve safety and productivity. In the system using a collaborative robot, safety is ensured by the robot's safety functions. However, because there is no protective guard between the robot and operator, the operator feels unsafe about the robot, and it is not possible to prevent the contact between the robot and the operator's head/face. The CSL test case was conducted to address its practical utility. The operator of the system is a skilled worker who has mastered the work process with the knowledge of system's operation specifications, and the usage and purpose of safety products. Emergency stop switches are installed around the system to ensure the means to stop the machine at anywhere in the work area, so that an operator can stop the robot immediately. By securing operator's knowledge on safety and the means to stop machine at anywhere in the work place, the system environment can be categorized into CSL1.

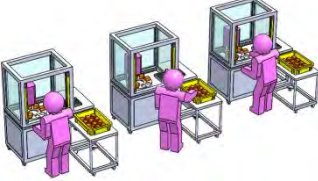
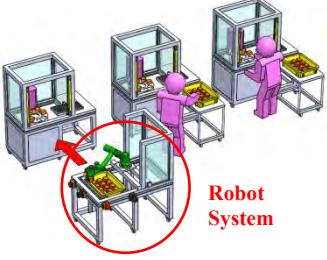
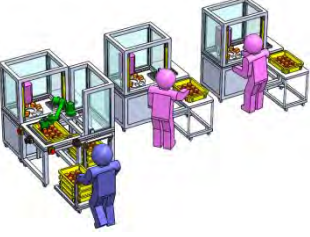
Production by humans	(Robots introduced)	Human-Robot Collaborative Production
		
<ul style="list-style-type: none"> - Production by humans - Insecure or unstable workforce due to labor shortage and lack of skilled worker - Full automation is difficult, due to limited production volume and number of product types. 	<ul style="list-style-type: none"> - Robots are introduced to replace humans. - Robots can be introduced to work in place of operators who suddenly take time off from work, or required production volume is higher than usual. 	<ul style="list-style-type: none"> - Both humans and robots operate in the same environment. - Flexible production system where humans and robots work collaboratively.

Figure 8. System transition to human-robot collaborative system.

To utilize the human information to control machines, laser scanners are used to detect humans. Humans approaching the robot arm are detected, and the robot is controlled to slow down or stop moving. Although the robot is operated with the energy of certain level to reduce the risk of collision with humans, there still remains some concern, and the collision with head/face is unavoidable. For this reason, installing sensors to detect the presence of humans to control the speed/stop of robot is an effective way to prevent robot from hitting operators. Therefore, controlling by utilizing human information, in addition to the operator’s skill and emergency stop switch, can be categorized into CSL2. To further upgrade the CSL of the system, an LED pilot light, which shows the status of robot movement, was installed on the robot as a device to send machine information to humans to motivate operator’s action. Preinforming the status of robot actuator, i.e., of the machine to operators with LED pilot light, reduces risk and gives a sense of *anshin* to humans and improves production efficiency. This can be categorized into CSL3.

Figure 9 summarizes the devices and requirements of CSL1, CSL2, and CSL3. In the robot system, a safety system consists of a collaborative robot and various safety products. The system has Safety1.0 function, where the risk is reduced to a sufficient degree. By utilizing CSL compliant products in the system, humans and robots are mutually pre-informed to minimize the loss of productivity caused by unintentional stops. Elevated sense of *anshin* is also expected to contribute to the improved work productivity. In the future research, we will continue developing products that optimize the human-machine status, which is necessary to improve both safety and productivity. We will also verify the possibility of introducing CSL to not only factory automation but also to various fields of industry.

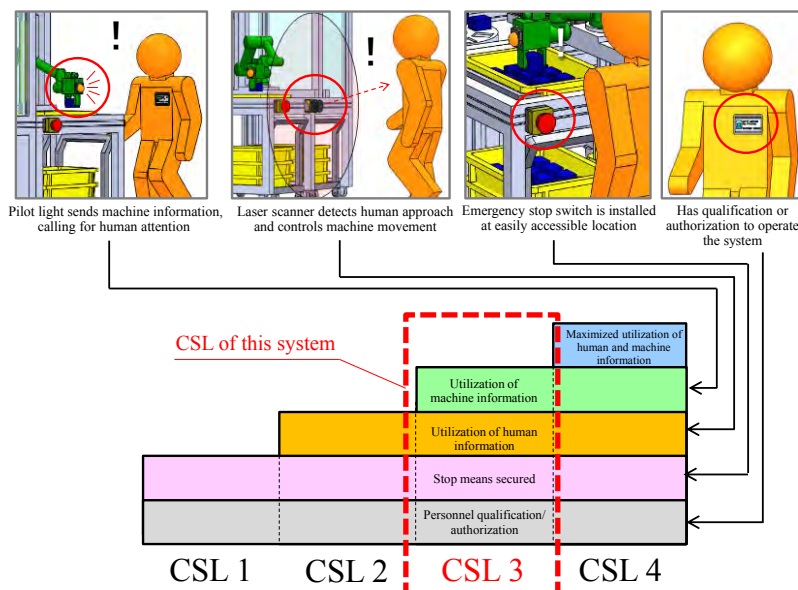


Figure 9. CSL evaluation example of human-robot collaborative operation system.

4 FUTURE PROSPECT

With the development of ICT, human-machine interface environment is changing dramatically. In order to correspond to the change and to achieve safe and *anshin* workplaces, the CSL is an indispensable evaluation benchmark. As explained, with the CSL, utilizing the information of humans, machines, and environment makes it possible to achieve high-level productivity and safety. The CSL, a collaborative safety evaluation benchmark, is a breakthrough concept to realize the Fourth Industrial Revolution. By embodying and establishing the CSL, Safety2.0 can complement the conventional Safety0.0 and Safety1.0 concepts, and the optimum safety and *anshin* environment can be established in various kinds of workplaces and industries.

5 REFERENCES

1. Mukaidono M., Takaoka H., Ogihara H., Ariyama M., Fujita T., *Japan's Approach for the Realization of Future Safety Concept by Implementing Collaborative Safety Technologies* (in press), 9th International Conference on Safety of Industrial Automated Systems (SIAS), France, 2018.
2. Dohi M., Okada K., Maeda I., Fujitani S., Fujita T., *Proposal of Collaboration Safety in a Coexistence Environment of Human and Robots*, 2018 IEEE International Conference on Robotics and Automation (ICRA), pp. 1924-1930, Australia.
3. Maeda I., Nobuhiro M., Shimizu T., Okada K., Dohi M., Fujitani S., Inada K., Fujita T., *New concept of safety to realize improvement of higher productivity and safety in an environment of human-robot collaboration, and proposal of the concept of Collaboration Safety Level*, International Symposium on Robotics, pp. 468-473, Germany, 2018.
4. Fujitani S., Okada K., Maeda I., Inada K., Dohi M., Fujita T., *New Interface concept for collaboration safety in a coexistence environment of human and robots*, Human Interface Symposium, p.669-674, Japan, 2017.
5. Fukui H., Shimizu T., Maeda I., Dohi M., Fujita T., *Collaboration safety system realizing compatibility between safety and productivity in human-machine coexistence environment*, Human Interface Symposium, pp. 533-538, Japan, 2018.
6. Shimizu T., Okada K., Dohi M., Fujita T., *New concept for collaboration safety in a coexistence environment of human and machinery*, IEICE Technical Report Vol.117 No.365, pp. 21-24 (SSS2017-30); The Institute of Electronics, Information and Communication Engineers, Safety, Japan, 2017
7. Nobuhiro M., Dohi M., Maeda I., Okada K., Fujita T., *The concept of Human-robot collaborative safety and 3-position enabling switches as key devices to achieve it*, IEICE Technical Report Vol.117 No.521, pp. 21-24 (SSS2017-36); The Institute of Electronics, Information and Communication Engineers, Safety, Japan, 2017.
8. ISO 10218-1: 2011, Robots and robotic devices — Safety requirements for industrial robots —Part 1: Robots.
9. ISO 10218-2:2011, Robots and robotic devices — Safety requirements for industrial robots — Part 2: Robot systems and integration.
10. ISO/TS 15066:2016, Robots and robotic devices —Collaborative robots.
11. ISO 12100:2010, Safety of machinery -- General principles for design -- Risk assessment and risk reduction.
12. ISO 13849-1:2015, Safety of machinery -- Safety-related parts of control systems -- Part 1: General principles for design.
13. IEC 62061: 2005, Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems.



Session 3

Autonomous systems

Top-Down approach for safety engineering in autonomous and semi-autonomous machinery systems

Tiusanen R.¹, Malm T.¹, Ronkainen A.²

¹ VTT Technical Research Centre of Finland Ltd (VTT) – Tekniikankatu 1 – FI - 33101 Tampere – Finland

² Natural Resources Institute Finland (Luke) – Latokartanonkaari 9 – FI-00790 Helsinki – Finland

risto.tiusanen@vtt.fi
timo.malm@vtt.fi
ari.ronkainen@luke.fi

KEYWORDS: autonomous, mobile machinery, risk assessment, safety

ABSTRACT

Needs to improve productivity, cost efficiency and safety are driving the development in industrial sectors towards highly automated or autonomous work-machine systems. The shift towards automated mobile work-machine systems takes machine safety considerations to a higher, system safety, level. The full utilisation of work machine automation and improved productivity require also a change in safety strategies and safety concepts. Traditional isolated operating areas and fixed machinery safety solutions based on single risk reduction need to be changed into adaptive and proactive system-safety solutions utilising protection layers, situational awareness information and dynamic risk assessment. A Top-Down approach for safety risk management is needed to integrate risk control options systematically from all system levels and to consider all available risk reduction measures.

To answer this need a new three-level approach for the assessment of safety risks in automated work-machine systems has been developed following the general systems engineering principles and processes. New virtual engineering tools and machinery specific system simulators have also been developed and applied to support this risk assessment approach and the design and evaluation safety solutions.

The results from case studies have shown that safety of complex mobile machine application cannot be solved by machine level safety solutions. The top-down safety engineering approach supports the sharing of system safety information and improves the common understanding of the system operations, human-system integration and interactions between sub-systems. System thinking and top-down approach support the allocation of the risk control options and safety measures to right system levels considering technical solutions and operational, managerial and organizational actions. The recently published machinery safety standard for autonomous work-machine systems, ISO 17757:2017, also emphasises the importance of systematic and hierarchical risk assessment process, the integration of the autonomous system in the overall site planning and the utilisation of different protection layers in safety solutions.

1 INTRODUCTION

When discussing about autonomous machinery the term autonomous should be defined to share the common understanding what it really means in this context. The term **Automated** that is widely used has been defined so that when an automated equipment or automated system is automated it ‘*is made to operate by machines or computers in order to reduce the work done by humans*’ [1]. **Autonomous mode** has been defined to be ‘*the status of vehicle operation where technology that is a combination of hardware and software, remote and/or on-board, performs the dynamic driving task, with or without a natural person actively supervising the autonomous technology’s performance of the dynamic driving task*’ [2]. **An autonomous vehicle** ‘*is operating or driving in autonomous mode when it is operated or driven with the autonomous technology engaged*’ [2].

In the mobile work-machine sector the first safety standard on autonomous machine systems, ISO 17757 ‘Earth-moving machinery and mining – Autonomous and semi-autonomous machine system safety’ defines terms autonomous operation and autonomous machine as follows [3]:

Autonomous operation: ‘*It is the mode of operation in which a mobile machine performs all machine safety-critical and earth-moving or mining functions related to its defined operations without operator interaction. The operator could provide destination or navigation input, but is not needed to assert control during the defined operation.*’

Autonomous machine: *‘Autonomous machine is a mobile machine that is intended to operate in autonomous mode during its normal operating cycle’.*

In practice the terminology is still very varied. One can see terms: Driverless, Unmanned, Highly Automated, etc... used in articles and in standards.

Development from single automated machines to autonomous or semi-autonomous machine systems has brought out difficult questions like: How to specify system-level safety requirements for unique machinery applications? How to allocate safety requirements to different sub systems? How to define all necessary protection layers and their functional safety requirements? How to validate safety concepts and safety solutions in autonomous machinery applications? Among mobile work-machine manufacturers and system suppliers, the biggest concern are the new automation-related threats, possible unexpected hazardous events and unforeseeable consequences. New safety threats are seen in complex human–machine interactions, complex system operations and maintenance situations, systematic or random system failures in control systems, and system interfaces within the operation environment. It has been clearly stated that the safety of autonomous work-machine systems cannot be solved only by machine-level on-board safety solutions. It has also been said that failure to implement system safety through proper analysis and protection layers may result in loss of system usability or productivity. Hazard analysis, risk estimation, and risk evaluation efforts should be scheduled and connected to the systems-engineering decision making stages at different system levels, depending on what is the objective of the risk assessment and what is the purpose of use of the assessment results [4].

Systems engineering in general links together technical and human-centred disciplines such as industrial engineering, automation engineering, and job planning and project management. Today the use of modern modelling and simulation techniques is essential in systems engineering work to create, demonstrate and validate assumptions or theories on a system level and the interactions within the system and its subsystems [5]. Analysis methods that allow early detection of possible hazards, threats, human factors and technical failures, in system safety engineering, should be integrated into the system design process. Commonly expressed motivation for systems engineering approach is the practical knowledge that decisions made at the beginning of a project whose consequences are not clearly understood can have enormous implications later during system development and during the actual operation [6]. It is also stated that the systems-engineering process should be performed iteratively at each level of the system hierarchy (Top-down) and the risk assessment activities should be closely connected to this process phases: requirements’ analysis; functional analysis and synthesis; and system-analysis.

According to system safety literature [7], [8], and systems engineering standards [9], [10], the risk assessment is a continuous process. From safety engineering point of view this means continuous efforts to make things as safe as possible in the early stages of the system lifecycle by using engineering and management tools. This approach involves well-planned, systematic safety engineering tasks aiming to identify and control hazards before losses occur, with different analysis methods, at different stages at its life cycle [8].

Based on the systems engineering approach and system safety principles a three-level approach to risk assessment of autonomous or semi-autonomous machinery systems has been developed in VTT in co-operation with industrial partners. VTT and Luke have been developing, demonstrating and implementing these new approaches and simulator assisted safety-engineering methods together with system suppliers and machine manufacturers in Finland. In this paper we shortly introduce the three-level approach, supporting methods and experiences of their use.

2 THE THREE-LEVEL APPROACH FOR SAFETY ENGINEERING

The three-level approach is a simplified system-safety approach utilising selected risk-analysis methods focused on system-level safety issues arising from the shift from individual manual mobile machines to highly automated machinery systems [4]. The approach integrates and utilises elements from current machinery safety engineering [11], industrial safety engineering [12], and system-safety-engineering practices [7], [8]. The three-level approach is based on the system thinking and system-modelling principles adopted from the general systems-engineering approach, such as its phases in the system life cycle; system-development breakdown; and system modelling with a three-level system hierarchy: the overall system level, the upper system level, and the lower system level [6]. The overall system level in this approach covers the work-site-related issues, including the machinery system under study, its operation environment and interfaces to other systems and activities in the operation environment in the various phases of the system life cycle. Upper system level corresponds to system operations, operation modes, system functions, and human–technology interactions that extend through the entire

machinery application horizontally or vertically. Lower system level corresponds to subsystem-level functions, specific safety systems, and on-board functions, and human–technology interfaces.

The three-level approach to risk assessment links system-safety tasks to specific phases in system development and levels of system analysis, with certain risk analysis methods employed: Preliminary hazard analysis (PHA) [7], [8], Operating hazard analysis (OHA) [7] and Hazard and operability studies (HAZOP) [13] levels. The main idea is that the risk assessment work proceeds systematically throughout the full process of system development, in all its phases, and the higher level analysis results are used as input to lower level analysis.

PHA is for the overall-system-level assessment. The objective at PHA level is the identification and assessment of the major automation related system risks affecting the overall machinery application. This includes the most significant risks associated with the automated machinery, risks linked to the system’s operation environment, and other work-site-level safety constraints. OHA is for the upper-system-level assessment. The objective at OHA level is the identification and assessment of the operations risks related to the planned and designed system operations and to maintenance procedures, system functions, and human–technology interaction. HAZOP study is for the lower-system-level assessment. The objective in HAZOP studies is the identification and assessment of functional safety risks related to possible technical failures, software errors and human error in subsystem functions, on-board functions, and human–technology interfaces.

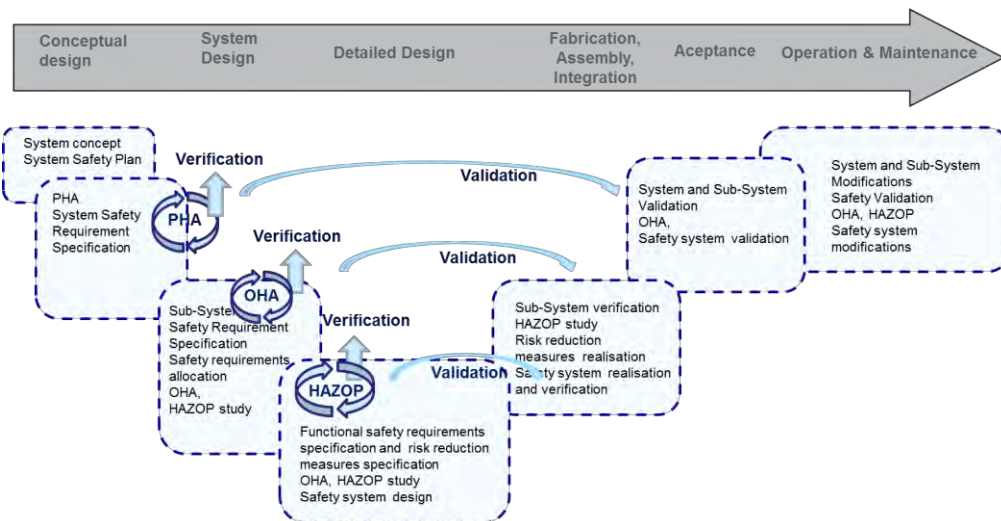


Figure 1. Outline the risk assessment levels linked to the system life cycle phases, system hierarchy levels and main system safety tasks.

3 SIMULATOR-ASSISTED SAFETY ENGINEERING

Analysis of complex machinery applications, different operating scenarios and evaluation of safety solutions is made possible today by virtual environments and simulator-assisted engineering methods. A new process model following the three-level approach and agile virtual design principles have been demonstrated to support safety engineering from conceptual system design to the design of safety functions.

3-D modelling, system simulation and virtual environments are used commonly in systems engineering and machinery design. Virtual environments provide system viewpoints related to simulations and simulators. It is well known from various industrial sectors’ automation applications that virtual environments and system simulator environments offer a good possibility to develop, test and demonstrate different automation concepts with different system functionalities. However, the use of machine simulators and virtual environments in risk analysis and safety engineering is still quite uncommon. Current risk analysis and safety engineering practices in early life cycle phases of a machinery system typically use static system models such as 3-D models of machinery and facilities, preliminary layout drawings of the work site environment and functional descriptions.

Research work on the simulator assisted safety engineering approach has been going on in Finland in co-operation with mobile work machine manufacturers, machine control system designers, VTT, MTT Agrifood Research Finland and Technical University of Tampere. Objective of the approach has been to support system

analysis and risk management in systems engineering process from the early system requirement specification through system design and verification up to the requirement validation phase.

The advance of simulators and virtual reality environments depends on the phase of the development process. At the risk analysis phase, they are utilized for visualizing the machine and demonstrating the work cycles. That helps designers to identify potential risks. In the risk evaluation phase, simulators and virtual reality environments can support the assessment of the properties of the hazards and a probability of the identified risks during the work cycle. At the verification of the risk control options, the simulator can be utilized for a testing of scenarios and verification of selected risk reduction methods. In the system validation phase the simulator can be utilized for validation and demonstration that the designed system operates safely in different work cycles.

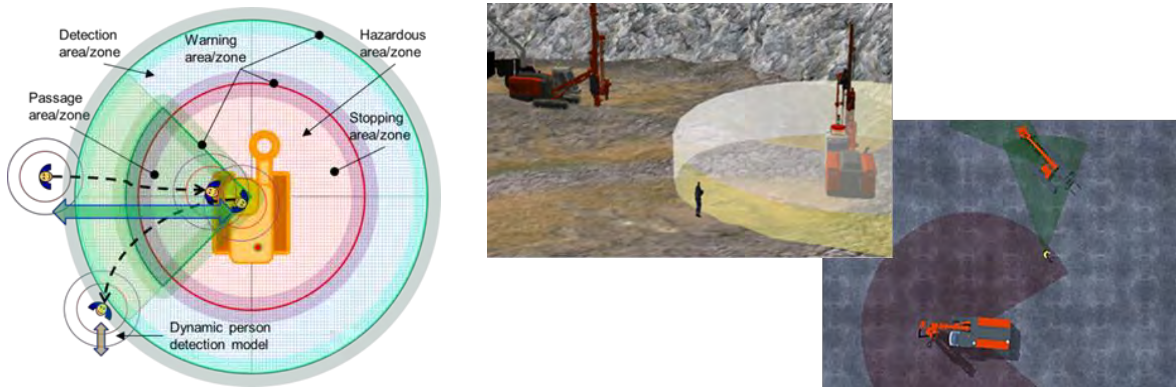


Figure 2. An example of an adaptive safety concept visualisation (in the left) and snapshots of the demonstrations in a virtual reality environment and in a machine specific simulator environment (in the right).

4 ISO 17757 GUIDELINES FOR SAFETY ENGINEERING

ISO has last year published the first standard on safety requirements for autonomous mobile machinery. The ISO 17757 standard provides safety requirements for Autonomous and Semi-Autonomous Machine Systems (ASAMS) used in earth-moving and mining operations. It specifies safety requirements for the machines and their associated systems and infrastructure, and provides guidance on safe use in their defined functional environments during the machine and system life cycle. The overall ASAMS concept is outlined in (Figure 3).

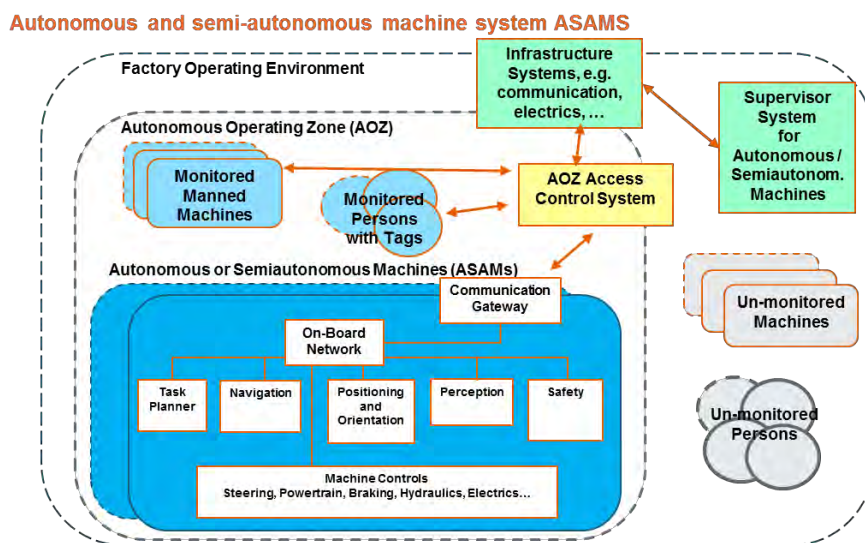


Figure 3. An illustration of the main elements of the ASAMS concept modified from ISO 17757 [3].

The standard is developed for autonomous earth-moving machinery and mobile mining machinery systems but its principles and many of its provisions can be applied to other types of autonomous or semi-autonomous

machines used on different worksites. The standard defines the ASAMS including all supporting systems, infrastructure and machine on-board subsystems are needed to enable the autonomous operation [3].

The standard highlights the importance of the hierarchical and systematic risk management process. Risk control options and safety measures should be evaluated according to the risk assessment results by identifying uncertainties, failure modes and risks and assessing what level of measures should be taken to be prepared for risks them from the perspective of the whole system. The functional characteristics of the safety related systems and the required safety integrity levels should be based on the actual risks in the specific operating environment.

Baseline for the risk assessment comes from the principles of ISO 12100 [11] but the special focus should be on identification of hazardous situations not normally encountered on a conventional manned worksite with manual machinery. Recommended methods for hazard identification are among others HAZOP, LOPA and FMEA and workplace inspections. At the risk analysis stage the following three viewpoints should considered:

- **the operational environment** (scale, complexity and physical environment of operations and activities),
- **the operational processes** (work processes, maintenance procedures, internal and external interactions)
- **the autonomous machine systems** (functionality and performance, safety and resilience features)

Risk evaluation and risk management is advised to be accomplished by applying a hierarchy of risk controls and safety measures:

- **Primary controls** aiming to avoid, remove or change the risk type
- **Contingency controls** aiming to minimize the effects in case of an incident following the LOPA principle
- **Prevention and management controls** aiming e.g. to minimize interactions with ASAM fleet and to develop safe work procedures

5 DISCUSSION

Risk assessment procedure for autonomous machinery is not a single phase in the system life cycle but an essential part of the systems-engineering process and supportive effort for decision making in various phases in the system life cycle. The results of our studies and our practical experiences confirm that the safety engineering problems in the design and development of automated mobile machinery systems can be solved by utilising system-safety approach and systematic risk analysis and risk evaluation processes. It is important to keep in mind what is the objective of the risk assessment and what is the purpose of use of the assessment results in different systems-engineering decision-making stages at different system levels. When proceeding systematically top-down the safety risks at various levels of the system can be identified at the right time and the risk reduction measures can be assigned to the appropriate level of the organisation for evaluation.

Experiences of the use of modern virtual reality environments and machinery system simulators offer good possibilities to explore develop and evaluate safety concepts with different system functionalities in different operating conditions. These new engineering tools also helped sharing of system information and improved the common understanding of the overall system and interactions between subsystems among the risk analysis team that consists of expert from different technological background. The simulator-assisted approach could bring in new verifiable and traceable evidence for the acceptance of adaptive safety functionalities and safety solutions in autonomous work-machine applications.

System safety approach for autonomous machinery applications has been outlined ISO 17757 standard. The standard defines autonomous machinery systems in a conceptual level as a complex socio-technical entity, its basic elements, subsystems and human-technology interactions. It also introduces procedures for system integration and risk-conscious system design. The standard highlights the principle that the requirements should be defined based on the uncertainties and the risks related to the actual case and technologies to be utilised at the site. It also emphasises the importance of human-technology interaction and consideration of human factors to ensure overall safety, which fits well with the general system safety principles that have been applied for years in complex safety critical applications in aviation, transportation and energy sectors. It would be useful if the standard could give more guidance how the intelligence required by autonomous operation should be divided between the "On-board" system and the "Supervisor" system. In addition, more guidance for the design of the interactions between the "Access control system" - "Mission planner" - "Supervisor system" could be helpful.

ISO 17757 does not give any fixed SIL or PL requirements for any subsystem or safety related function. It guides system designers to define safety requirements according to the application-specific risk assessment results. This systems engineering approach developed for earth-moving and mining applications differs from the approach that has been developed for driverless trucks and AGV type of machinery in ISO/DIS 3691-4 'Industrial trucks -- Safety requirements and verification -- Part 4: Driverless industrial trucks and their systems' [14]. In manufacturing industry in indoor machine applications, safety systems can be build using certified or well-known components. In outdoor work-machine applications there are still many uncertainties to be solved for autonomous operation. The performance of sensors and actuators can be inadequate in harsh and complex environment. In addition, the high reliability of safety logics can be difficult to achieve, because of uncertain situational awareness information and lack of resilient components.

In industry group position papers, some components can be found to implement the presented top-down methodology. Committee for European Construction Equipment (CECE) released a document "Working safer with construction machines" [15], which presents worksite management as a tool for managing safety. Worksite management is also required in directive 92/57/EEC on temporary or mobile worksites in a form of health and safety plan. The plan requires planning of traffic and danger areas and operations in the worksite. The key takeaway from these documents is that the highly automated or autonomous worksites are limited concepts and do not require preparedness for every possible interaction. This gives the limits for PHA phase risk assessment.

Identification and assessment of operational risks in OHA phase depends on the safety system concept defined for the autonomous machines: collision avoidance system and cooperative system. The collision avoidance systems rely on the perception system carried by the machine and its purpose is to detect and prevent collisions. Examples of these systems can be found e.g. in the standard ISO 18497 for machinery in agriculture [16] and in a document from Earth Moving Equipment Safety Round Table's (EMESRT) called 'Proximity Detection Device Interoperability' [17]. Both of these documents set the performance target for such systems without taking explicitly a position on how these systems are to be implemented. Examples for cooperative systems, where machines share information between other machines (M2M) or with supervisory system, to maintain safe state can be found in the above mentioned ISO 17757 or EMESRT 'Vehicle Interaction System' [18] document.

Currently, it is clear that safety of autonomous work machines is difficult to handle only by on-board safety solutions. A system level approach is needed to find alternative risk control options and safety measures to solve the safety problems. If a safety problem cannot be handled in one level, then it needs to be considered in upper level. The idea is close to layer of protection analysis (LOPA) in design process.

Research work on safety of autonomous machinery applications continues actively in Finland in close co-operation with industrial partners. A new Alliance for Autonomous Systems (RAAS) has been established to advance research on autonomous transport and logistics in global markets. Smart safety and risk management is one of the themes in the research agenda of the research alliance [19].

6 REFERENCES

1. <https://dictionary.cambridge.org/dictionary/english/> sited on 1.10.2018
2. <https://definedterm.com/a/document/10823> sited on 1.10.2018
3. ISO 17757:2017, Earth-moving machinery and mining -- Autonomous and semi-autonomous machine system safety
4. Tiisanen, R., An approach for the assessment of safety risks in automated mobile work machine systems. Dissertation. Espoo: VTT. 2014
5. Cellier, F.E.; Floros X & Kofman, E., The Complexity Crisis – Using Modelling and Simulation for System Level Analysis and Design. In the proceedings of the 60th Anniversary Seminar "Automation and Systems without Borders - beyond Future" 21 May 2013 in Helsinki, Finland. The Finnish Society of Automation. Helsinki. 2013.
6. INCOSE, SE Handbook, Systems Engineering Handbook A guide for system life cycle processes and activities. INCOSE, San Diego. 2011.
7. Vincoli, J. W., Basic Guide to System Safety. Hoboken, NJ: John Wiley & Sons, Inc. 2006
8. Stephans, R., System safety for the 21st century. Hoboken, NJ: John Wiley & Sons. 2004
9. ISO IEC 15288:2008, Systems and software engineering – System life cycle processes (IEEE Std 15288-2008); Second edition.
10. ISO IEC 26702:2007, Systems engineering – Application and management of the systems engineering process (IEEE Std 1220-2005); First edition.

Session 3 – Autonomous systems

11. ISO 12100:2010, Safety of machinery. General principles for design. Risk assessment and risk reduction.
12. BS 18004:2008, Guide to achieving effective occupational health and safety performance. BSI.
13. IEC 61882:2016, Hazard and operability studies (HAZOP studies) - Application guide
14. ISO/DIS 3691-4, Industrial trucks -- Safety requirements and verification -- Part 4: Driverless industrial trucks and their systems
15. CECE, Working safer with construction machines. Committee for European Construction Equipment. 2017. <https://www.cece.eu/news/working-safer-with-construction-machines-project-results> sited on 1.10.2018
16. ISO 18497:2018, Agricultural machinery and tractors -- Safety of highly automated agricultural machines -- Principles for design
17. EMESRT, Proximity Detection Device Interoperability. Earth Moving Equipment Safety Round Table. 2016. <http://www.acarp.com.au/abstracts.aspx?repId=C24034> sited on 1.10.2018
18. EMESRT, Vehicle Interaction Systems. Earth Moving Equipment Safety Round Table. 2016. <https://emesrt.org/wp-content/uploads/2017/01/EMESRT-PR-5A-Vehicle-Interactions-2.pdf> sited on 1.10.2018
19. <https://autonomous.fi/> sited on 1.10.2018

Safety concepts for autonomous and semi-autonomous mobile work machines

Malm T., Ahonen T.

VTT Technical Research Centre of Finland (VTT) – Tekniikankatu 1 – FI - 33101 Tampere – Finland

timo.malm@vtt.fi
toni.ahonen@vtt.fi

KEYWORDS: safety, autonomous mobile work machines, safety systems

ABSTRACT

Development of autonomous mobile work machines is on the agenda of increasing number of machine vendors since the customers' interest has also increased significantly. Autonomous mobile work machines are operating in closed environments. Compared to the applications currently available, introduction of the current technologies in outdoor mobile work machine systems is more complex than what it may seem, since sensors operate well only indoors, safety of the outdoor sensors is limited and the safety requirements are not unambiguous.

Increase in the level of automation sets more requirements to the system and also increases the responsibility of the manufacturer. A situation where manual and automated machines operate simultaneously in the area presents challenges from the safety point of view, since both human errors and machine failures may cause hazardous situations. The means for better safety include detecting persons and machines, applying access control systems for machines and humans, limiting allowed machine movements and speed, enabling movements by applying suitable devices, increasing situational awareness of machines and persons, and defining proper rules for humans and machines. Risk assessment is an essential tool in selecting suitable methods for the specific application.

This paper introduces the approaches relevant for mobile machine vendors in considering the safety on the path towards an autonomous system.

1 INTRODUCTION

The interest for development and implementation of autonomous mobile work machines has increased dramatically during the past two years. One has seen that autonomous cars have appeared in traffic in specific conditions, AGVs are commonplace at factories and autonomous mobile work machines are operating in closed environments. Compared to the applications currently available, introduction of the current technologies in outdoor mobile work machine systems is more complex than what it may seem, due to the limitations of these applications. Sensors operate well only indoors, safety of the outdoor sensors is limited and the safety requirements are not unambiguous.

The level of automation clearly affects the safety requirements. The more automated system, the more requirements there are to the system, and the more manufacturer needs to take responsibility. In manual systems, the operator/driver takes great share of responsibility of the operations, and in automated systems, the manufacturer has more responsibility. In many cases, the intention is to increase the level of automation gradually, leading to situations where both manual and automated machines operate at one time. From the safety point of view, this is difficult, since both human errors and machine failures may cause hazardous situations.

There are currently safety problems with autonomous outdoors mobile work machines, if the system is not closed and free access is not prohibited technically. Following important differences can be identified between indoors and outdoor mobile machines:

- Sensor technology is not yet adequate for rough outdoors use. However, it is possible that a well-functioning sensor system will be introduced in the near future.
- The speed of mobile work machines is higher than the speed of indoor machines. There is an increasing need for productivity where machine speed is one influencing factor.
- Most of the sensors cannot see behind corners or obstacles. This is a problem for on-board sensors, which would be (otherwise) a good solution for areas with free access.
- It is more difficult to arrange access control outdoors, since there are seldom natural walls and the area is large. Autonomous systems are becoming ever larger and fences become more expensive.

2 AUTOMATION LEVEL, SAFETY AND REQUIREMENTS

There are already requirements for some autonomous mobile machine systems. The standards define precisely that all access inside the system must be controlled. If some kind of bumpers or virtual bumpers, like, laser scanners or radars are applied, the maximum speed is low (e.g. 1.2 m/s). In some cases low speed like 0.3 m/s can justify leaving bumpers away. Typically, safety devices for human detection need to be according to PL d requirements (ISO 13849-1) [1]. Many of the autonomous machine standards are still in draft phase and also the current existing standards will evolve. The standards are expected to become more precise as we learn the performance of the autonomous systems. Here are standards and standard drafts for common autonomous mobile machines:

- ISO 17757:2017. Earth-moving machinery and mining — Autonomous and semiautonomous machine system safety. [2]
- ISO/DIS 3691-4:2018 (draft). Industrial trucks — Safety requirements and verification — Driverless trucks. [3]
- ISO/DIS 18497.2: 2016 (draft). Agricultural machinery and tractors — Safety of highly automated agricultural machines — Complementary element. 18 p. [4]
- EN ISO 13482:2014 "Robots and robotic devices. Safety requirements for personal care robots". [5]
- ISO/WD 21815-1:2018. Earth-moving machinery -- Collision awareness and avoidance -- Part 1: Performance requirements and tests. [6]

The requirements of the above mentioned standards lead easily to slow or isolated systems. It is obviously the current state of the art.

3 STRATEGIES TO IMPROVE SAFETY OF AUTONOMOUS SYSTEMS

The strategies to improve safety include principles and methods for how adequate safety level can be reached. Each strategy needs to consider the relation to humans, technology and environment [7]. During the past years, typically only one strategy has been applied in one case. Each strategy has its costs and therefore, applying two strategies should provide advantage to justify the additional costs. This could be increased safety, since adequate safety level can be hard to achieve by applying only one strategy. Two strategies together can fulfil the safety requirements. It can be close to “layers of protection” approach. It is also possible to apply different strategies in different parts of the system or two strategies at one place in order to increase safety level.

One can divide safety strategies of autonomous mobile work machine systems into three groups (see Figure 1):

1. Rules for moving in the restricted area. This means that only authorised persons and machines may enter the restricted area. The entering persons must know the rules. This is typical for manual systems, and safety depends very much on the person at the area. This resembles traffic and the rules of the road. Typically, also other strategies need to be applied to reach adequate safety level in autonomous machinery systems.
2. Isolated area. The restricted area is isolated and persons enter through access control system, which stops the autonomous machines at the area. The restricted area may consist of several areas and autonomous machines are stopped only if person/manual machine and autonomous machine are at the same area. The safety can be adequate for all kinds of autonomous systems.
3. Safe separation distance. On-board sensors detect persons and manual machines in front of the autonomous machine or near it. The separation distance can be arranged also with central control system, which know all the time the locations of all machines and persons. This requires usually active tags or transmitters, which send their location to the central system. One advantage of the central system is that persons can be observed even behind corners and obstacles. The safety is adequate for indoors systems, but for outdoors solutions, usually, some additional means are required.

The colours in Figure 1 represent the typical safety capability of the safety strategy. Red colour represents low capability and green stands for high capability. Each corner is dedicated to a strategy described above. There are also several safety concepts and strategies, which are not in the corner of the triangle, but somewhere between corners.

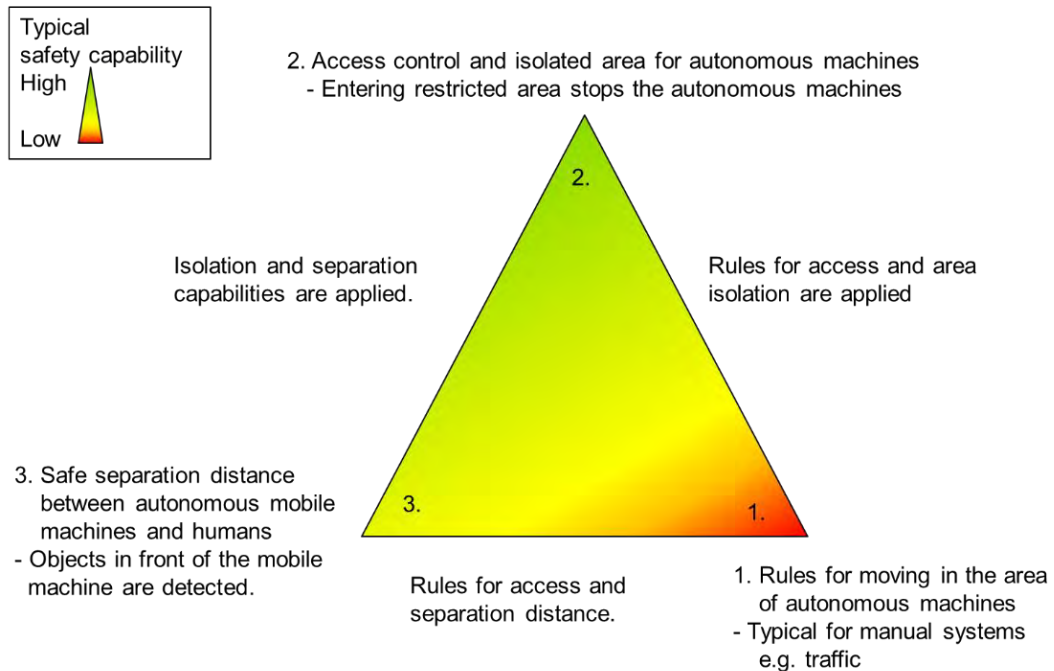


Figure 1. Safety strategies for autonomous mobile work machine systems.

4 SAFETY CONCEPTS

Each strategy often leads to the use of specific safety concepts. However, safety concepts and strategies can be linked and different solutions can be applied in different parts of the system. Table 1 describes selected examples on how strategies and different technologies can be combined.

Table 1. Examples of combining strategy and safety concepts.

Safety \ Strategy concepts \	Rules for automated area	Isolated area	Safe separation distance
Rules for applying automated area	Rules, devices to better situational awareness, training, semi-automated operations under supervision, hold-to-run devices, traffic lights	Additional means needed for isolation	Additional means needed for detection
Remote control	Rules for applying remote control	Some tasks may need human supervision e.g. access to another area or handling of objects in delicate conditions	Camera control/supervision, line of sight control, alarms, hold-to-run-devices, detection of correct connection to objects
On-board safety system	Specific lanes for machines and persons, restricted area for trained personnel	Safety level optimization, lines of defence approach, safety actions according to the area	Limited speed, stopping and rerouting, radar, lidar, proximity sensors, safety bumpers
Centralized positioning system	All actions at the automated area can be predesigned and optimized for machines	Central system can occupy areas in advance and optimize speed of the machines	Central system optimize the routes, speed and separation distances of the machines, only tagged persons are allowed to enter the area, UWB, RFID
Isolated area	Rules for persons allowed to enter the restricted area.	Access control, stop the system when a person or a manual machine enters the restricted area, fences, light curtains	Safety level optimization, lines of defence approach.

4.1 Rules for all using the restricted area

A strategy with only rules and almost no technical means (except e.g. traffic lights or traffic signs) to ensure safety is typically not adequate for autonomous mobile machines. Additional means are thus required. Solutions, for example, hold-to-run devices to allow machines to run when a person is there, cameras and remote control, can be applied. Operator may also allow access to the restricted area by opening the doors remotely. Remote control is applied, when persons are at the restricted area or automated movements can be done if they are out of human reach (e.g. very high).

In traffic, one has to rely on rules. On a road, one must rely on all the other drivers keeping their lanes, since a violation of the rule would mean crossing movement, to which a safety system could not respond in time. The separation distance between two lanes is too short to respond against driving on a wrong lane. Currently, for autonomous mobile work machines the situation is under discussion.

4.2 On-board safety systems

Sensors to detect objects beside the machine can be placed on-board the machine (see Figure 2). The detection of an object may cause reduced speed, stop or rerouting to avoid collision with the detected object. Typical sensors to be applied in this approach are: lidar, laser scanner, radar, UWB, 3D-camera, IR-camera, proximity detectors (ultrasonic, optical, capacitive) and tactile bumpers. In order to overcome the weaknesses of an individual sensor type, one can apply sensor fusion. The concept includes challenges to detect objects behind corners and objects next to a large object. For most of the mentioned technologies it is difficult to detect a person beside a wall (or a large object). If the machine and large object position were accurate, it would be possible to adjust the detection range to be close to the wall, but not always.

Right side of the Figure 2. describes a mobile machine containing on-board detector and all moving objects (persons and moving machines) carrying active tags. The detectors on machines detect all actively transmitting tags; usually UWB or RFID technology is applied. Active tags may be detected in good conditions also behind objects, but it depends on the situation. One needs to consider actions against dead battery or faulty transmitter detection and the need for a redundant system.

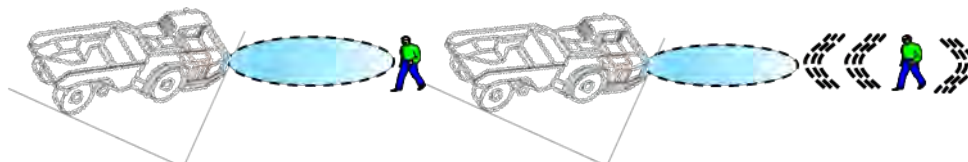


Figure 2. On the left on-board safety system on the autonomous mobile work machine. On the right side a detector on each autonomous mobile work machine and active tags at each moving object. (Figure dumper hauler [8]).

4.3 Centralized systems

Centralized safety system continuously controls precise location of all vehicles and persons at the site (see Figure 3.). Each object has a system, which can localize its own position. Usually several systems are applied to ensure the position information in all places and to improve the accuracy. Objects are detected also behind a corner and obstacles. Fleet management can control crossings by controlling speeds and rerouting automated machines to avoid collisions. Typical technologies for positioning objects are: UWB, GPS, IMS (inertia measurement system), odometer and optical measurement systems. In addition, all moving objects need to communicate with central control unit to inform location and to check that the route ahead is free.

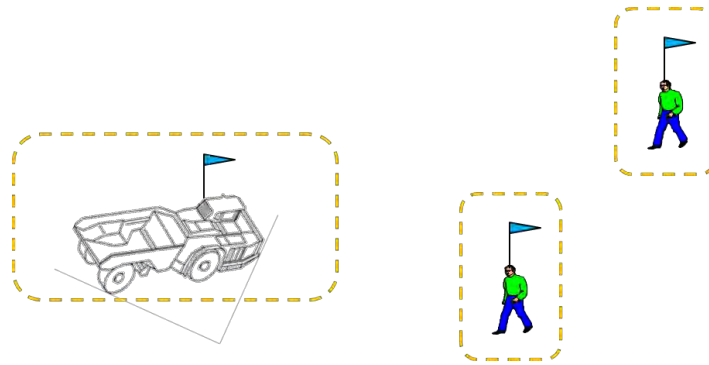


Figure 3. Each moving object sends their position to the central control unit. (Figure dumper hauler [8]).

4.4 Isolated area

Safety system controls access to each area of the site and occupies areas respectively (see Figure 4.). If a machine enters occupied area, it stops. Machine needs to stop also beside an occupied area. This is required to ensure that the separation distance between objects is adequate. The isolation can be made with fences and gates or light curtains (or other contactless sensors). Gates can be applied to prevent access to occupied area and then a person may have safe access beside the occupied area.

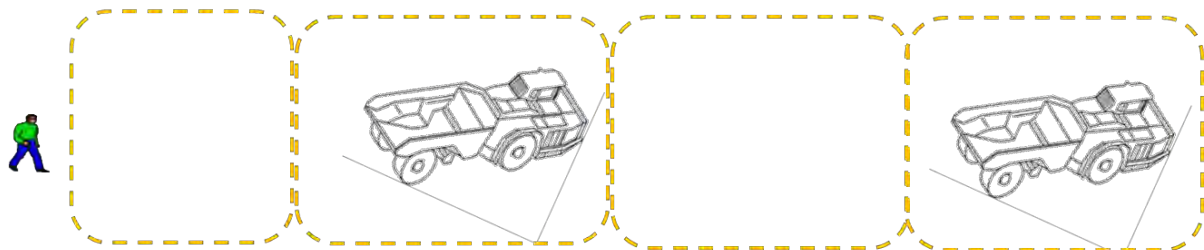


Figure 4. The restricted area of the autonomous mobile work machines is divided into sectors, which each object can occupy. (Figure dumper hauler [8]).

5 DISCUSSION

By applying current technology, isolation is the clearest way to ensure safety of an autonomous mobile work machine system. For relatively small systems, isolated machine area is a practical strategy to achieve adequate safety. In large open systems barriers become hard to realise i.e. barriers become too long. This means that isolation is not a well scalable strategy and it may become expensive.

Rules for the autonomous system is a scalable and economical strategy, but the safety of these solutions is considered relatively low. The strategy requires some expenses, because traffic lights, traffic signs and road markings may be needed and, in addition, all personnel needs training for the system. If we compare the situation with car traffic, there is also a penalty for those, who violate the rules of the road. It is difficult to say, what could be the equivalent penalty for those who violate the rules of the autonomous system. The person at the autonomous systems needs to be urged to obey rules in order to have better safety environment. A good safety culture may be a prerequisite for this.

Safe separation distance is a strategy with a clear technology orientation, since the distance between a person and a moving machine must be measured. The distance can be measured straight from the machine to a person or all objects can be localized and the distance is calculated by the central control unit. Currently, all sensors have weaknesses in some conditions or environment, however, sensors are getting better all the time and the prices are getting lower. Also sensor fusion can tackle the weaknesses of individual sensors. Safety issues of indoor cases are usually tackled by applying low speed and safety sensors capable for situation. Outdoor use is the problem, since sensors are not that reliable in rain, fog or mud and due to long distances, the need for relatively high speed is obvious (manual driving speed vs. automated driving). Many machines applied in outdoor applications are bigger than indoor machines and they may have e.g. large booms or buckets, which may hinder the detection of objects. The separation distance strategy is to some extent scalable, but each object at the area requires more technology and the price is getting higher. Safety is not a problem for indoor applications, but for outdoor applications it depends on the circumstances and the environment.

One way to improve the safety level and to optimize expenses is to apply two strategies. Typically, only one strategy is applied at a time and the requirements are related to devices, which are often related to a specific strategy. By applying two strategies, it may be tempting to, for example, increase training and situational awareness in order to justify lower PL or SIL of the safety system. If the frequency and/or probability of hazardous interactions between persons and machines become lower, this may be possible. Thus, in specific situations, two strategies like in “lines of defence / layers of protection approach” can be a good solution.

In all of these three strategies, one challenge is how to treat uncertainty. In the “rules” strategy it is uncertain, whether all persons will obey the rules. In “separation distance” strategy the sensor performance of outdoor applications is uncertain in specific environment. In “isolation” strategy the means of isolation may vary. Locked doors and high fences guarantee good isolation, but there are situations, when persons need to enter the area. Complete isolation is not practical. Keys or rules for entering the system can ease the isolation, but then also uncertainty increases. The designers of the autonomous mobile machine systems need to accept some degree of uncertainty, but the risk must be well in control. Currently, there are not yet many good examples of safe and practical autonomous mobile machine systems. More examples are needed and also the standards need to evolve in order to express more clearly the acceptable level of uncertainty and risk.

6 ACKNOWLEDGEMENTS

The authors gratefully acknowledge Business Finland for funding the research project. The companies involved in the research are gratefully acknowledged for their funding and participation.

7 REFERENCES

1. SFS-EN ISO 13849-1. 2015. Safety of machinery – Safety-related parts of control systems – Part 1: *General principles for design*. Finnish Standards Association SFS. 193 p.
2. ISO 17757:2017. Earth-moving machinery and mining — *Autonomous and semiautonomous machine system safety*. 36 p.
3. ISO/DIS 3691-4:2018. (draft). Industrial trucks — Safety requirements and verification — Part 4: *Driverless industrial trucks and their systems*. 42 p.
4. ISO/DIS 18497.2: 2016 (draft). Agricultural machinery and tractors — *Safety of highly automated agricultural machines — Complementary element*. 18 p.
5. ISO 13482:2014. Robots and robotic devices - *Safety requirements for personal care robots*. 79 p.
6. ISO/WD 21815-1:2018. Earth-moving machinery -- *Collision awareness and avoidance -- Part 1: Performance requirements and tests*. 45 p.
7. Tiisanen R., *An approach for the assessment of safety risks in automated mobile work-machine systems*, VTT Science 69, Doc. thesis, 2014, 200 p. + app. 6 p.
8. ISO/DIS 19296.2:2015. Mining and earthmoving machinery — *Mobile machines working underground — Machine Safety*. 47 p.

Autonomous Driving within the Plant Functional Safety between Industrial Automation and Automotive Engineering

Borowski T.

Institut fuer Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA) - Alte Heerstr. 111 - 53757
Sankt Augustin - Germany

torsten.borowski@dguv.de

KEYWORDS: autonomous driving, pedestrian protection systems, solutions and standards in automation and automotive technology

Autonomous Guided Vehicles (AGVs) and Systems have been used safely for fully automated internal transport for a long time. Thanks to well-engineered protective devices such as safety laser scanners, which are designed in accordance with international standards such as EN 1525 *Safety of industrial trucks - Driverless trucks and their systems* and IEC 61496 *Safety of machinery - Electro-sensitive protective equipment*, accidents with AGVs are hardly ever occurring. Organisational and technical measures in the infrastructure, such as the limitation to indoor use, traffic routes for industrial trucks separated from pedestrians and additional support by intelligent guidance and navigation systems, make this deployment possible in the first place. However, the demand for autonomous mobility for logistics is growing and affects not only the 'on-road' transport sector with autonomous trucks, but also internal plant transport in the outdoors.

The presentation shows application examples of a future development; they illustrate the enormous challenges to be faced, but they also show that solutions are already being tested. Not addressed are the economic benefits of highly automated technology solutions or the technical peculiarities of the autonomous logistics concept. Rather, the example of protective measures for anti-collision protection, i. e. pedestrian safety, is chosen to depict the status quo and the further development of safety systems on the borderline between machines and automobiles. Technology of the automotive supplier industry is increasingly being used in the industrial sector, with the Machinery Directive 2006/42/EC and own standards for functional safety (IEC 62061 and ISO 13849) in force there. Examples are driver assistance systems (ADAS), vehicle control systems with functional safety (safety ECUs) and 'ASIL ready' processors according to ISO 26262.

There is a growing demand for the integral application of FS standards in the automotive and machine sectors, and the need for further coordination among experts. Not only the developers are challenged here, but also the Notified Bodies (like the IFA). The topic of pedestrian protection systems is intended to underline that functionally safe systems do call for more than considering hardware and software aspects of programmable units (PES). As a matter of fact, the safety integrity of the entire system is at stake here. The application of safety-relevant anti-collision sensors also shows that there are (still) significant differences between safe system solutions in automation and automotive technology.

A methodological framework to support the design of safe & secure autonomous systems

Heikkilä E., Välisalo T.

VTT Technical Research Centre of Finland Ltd. – Visiokatu 4 – P.O.Box 1300 – FI-33101 Tampere – Finland

eetu.heikkila@vtt.fi
tero.valisalo@vtt.fi

KEYWORDS: autonomous systems, safety, security, risk management, design methodology

ABSTRACT

Advances in robotics, artificial intelligence, and communication technology are enabling increasingly autonomous systems. Different systems have different levels of autonomy and different levels of openness, which introduce different risks for safety and security in different industries. These risks are not static. Rather, risks change as organizations seek to bring together new devices and machines into use within wider systems. Currently, however, there are only general guidelines and limited domain-specific standards for designing safety and security into autonomous systems. Even in these, the focus is on providing general performance guidelines instead of prescriptive design requirements. Hence, there is a gap between the current standards base and technologies being developed. This gap leaves technology developers with an increasing responsibility for ensuring safety. Consequently, there is need for technology developers to be able to take a holistic view of safety and security issues throughout the systems engineering process. In the first part of this paper, we discuss the implications of different levels of autonomy and openness of the use environment, and review selected key safety issues in autonomous systems development. In the second part, we discuss the risk analysis methods for autonomous machines development, and propose a preliminary methodological framework that can support product development of safe and secure autonomous systems.

1 INTRODUCTION

Increasing autonomy of machine systems is a global trend in industry. Autonomous systems are seen as a potential way to increase productivity, cost efficiency, and safety. This can sometimes be achieved by reducing the amount of work done by humans, but often also by enabling completely new types of approaches and business models. In the marketing of autonomous technologies, safety is especially presented as an advantage, to be achieved by autonomous operation in dangerous work environments or by implementing situational awareness systems that exceed human capability. On the other hand, new technologies are also likely to introduce new and modified risks that the system developers need to address.

The concept of autonomy has no single agreed definition and the terms “automation” and “autonomy” are sometimes used interchangeably. Generally, autonomy can be seen to go beyond traditional automation by enabling self-governing behaviour and intelligent decision-making ability in a challenging environment [1]. In different industries, various categorizations have been developed to describe the level of autonomy, ranging from human operated to fully autonomous, with various levels of human-machine interaction in-between.

In addition to the level of autonomy, the operating environment needs to be considered. Autonomous systems can be divided roughly to two major categories: open and closed systems (see examples in Table 1). Open systems are systems that can operate in an environment, where the system can be in touch with other autonomous systems, humans, animals etc. that are not trained to cooperate with the autonomous system. Maybe the best example of fully autonomous system that operates in open environment is autonomous passenger car. Those cars operate in normal traffic on open roads and they can face situations that cannot be comprehensively identified beforehand. The other users of the roads cannot identify the autonomous cars easily from the traffic by the appearance of the car, therefore they react similarly to cars with or without human drivers.

Open system can also be restricted. This means that there are no physical fences etc. that prevent outsiders from entering the autonomous system working area, but the system operates only in a certain area that is supervised by operator or control system, depending on the level of autonomy. For example, an autonomous train operates only on the tracks, it cannot move freely to all directions. Some working areas might be controlled with optical sensors that identify if someone enters the area and slows down or stops the unmanned machines.

Closed systems are systems where other systems in the same area are known and humans are trained to work with the systems present. One example of this kind of environment is an open quarry mine, where autonomous dumpers can operate in a specific and physically limited area and all the other systems and workers at the site know which one of the systems has operators on board and which do not. The vehicles can be fully autonomous also in this kind of an application. Usually industrial robots are a part of closed system; they are surrounded by protective fences and if someone enters the cage, the robot interrupts its operation.

Table 1. Some examples of levels of autonomy in different environments.

	Human operated = baseline	Supervised	Mixed initiative	Fully autonomous
Open environment	Human operated work machine on the road, e.g. snowplough.	Remote controlled drones.	Airplane with autopilot.	Autonomous passenger car.
Restricted environment	Human operated forklift inside an industrial site.	Remote controlled mobile work machine inside an industrial site.	GPS-navigated tractor in a field.	Autonomous train.
Closed environment	LHD machine in an underground mine.	Remote operated mining truck in an underground mine.	Production drilling rig in a mine.	Autonomous underground train.

2 SAFETY AND SECURITY CHALLENGES IN DESIGN OF AUTONOMOUS SYSTEMS

Increasing autonomy brings new challenges in all phases of a product development process. To demonstrate this, we follow a systems engineering V-model, which is a typical way of facilitating a top-down design process of a complex system. Following a generic V-model (Figure 1), we have identified safety and security related design challenges typical for development of autonomous systems. The issues in different design phases include (but are not limited to) the following [2].

1. Concept design: Autonomy increases the demand for high-quality system description and requirements management procedures. It is especially important to identify the level of autonomy, and the type of the operating environment (open, closed or restricted), thus making the system description broader than in traditional systems. If the system is open, the estimated interactions between the system and its environment and relevant stakeholders need to be documented.
2. Architecture design: Safe and secure handling of large amounts of data is a major challenge. Careful planning is needed to ensure that sufficient data collection and processing capabilities will be implemented. Further issues include connectivity and cyber security, including planning of actions when connectivity is lost.
3. Detailed design, implementation and integration: The algorithms and AI technologies needed to enable autonomy pose several challenges. In addition to traditional tasks, the phases involve teaching the autonomous system to operate in its intended environment. Here, a major challenge is how to ensure that the system learns all the required skills, for example without becoming biased in some way. The designers need to implement reliable learning algorithms, ensure that relevant data is used, and verify that the results are acceptable. The transparency of the machine learning principles adds further challenges, as some of the methods fail to provide justification for the results they provide (so called “black box” solutions). Physical security, including vulnerability to adversarial attacks, also needs to be considered.
4. Verification and validation: V&V activities are performed against system requirements, part of which have been traditionally available from standards. In autonomous machines the requirements are increasingly set by the technology developers, based on the risk analysis activities. Thus, robust methods are needed to comprehensively demonstrate that the requirements are satisfied.
5. Operation and maintenance: Change management, e.g. in case of software updates or changes in the operational environment can be especially problematic.

The above limited overview of key challenges demonstrates the vast number of issues that autonomous system developers are likely to face. In many cases, the available standards rely heavily on risk analyses in terms of

safety assurance. In the following chapters, we discuss some risk management methodologies suitable for autonomous systems development and provide suggestions in the form of a preliminary methodological framework.

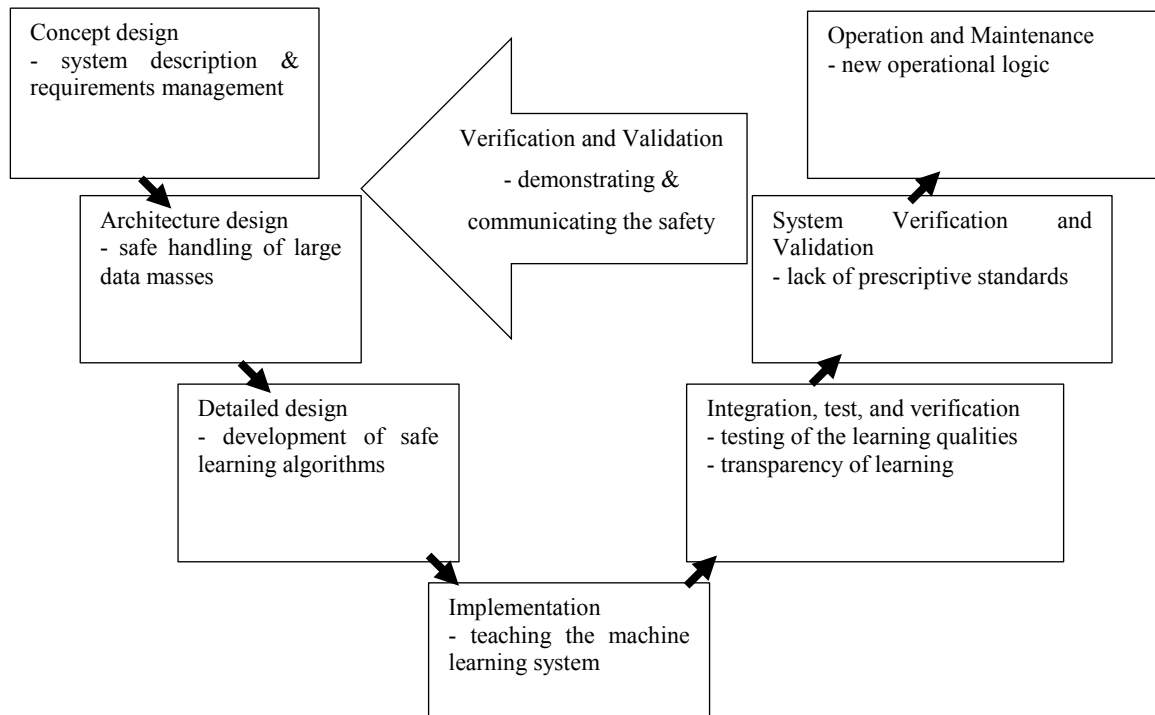


Figure 1. A generic systems engineering V-model (adapted from [3]), describing the development phases of an autonomous machine system. In each step, selected challenges have been presented that are central in autonomous systems development.

3 INTEGRATION OF RISK MANAGEMENT IN AUTONOMOUS SYSTEM DEVELOPMENT PROCESS

3.1 Analysing the safety risks of autonomous systems in development phase

Generally, risks are easiest to mitigate in the early phase of the product development process, and the identification of risks is advisable to be conducted early. The following chapters include discussion how the risks could be identified in closed and open systems, and how a methodological framework can be used to support safety-related design. Supervised and mixed initiative levels include elements from both open and closed systems risk identification procedures.

There are not too many standards that give guidance for managing RAM properties of a system, but there are a lot of standards concerning safety related issues. However, safety of autonomous systems is not very strictly standardized, at least not yet. Instead of the traditional prescriptive nature of standards, the few available standards focus more on providing general performance guidelines [4]. For example, ISO 17757, “Earth-moving machinery and mining -- Autonomous and semi-autonomous machine system safety” emphasizes heavily the importance of risk assessment [5]. The required actions are related to risk assessment; if the risk is assessed to be on an acceptable level no specific actions are required.

As the risk assessment consists of risk analysis and risk evaluation, they both must be applicable for assessing autonomous systems. ISO 17757 refers that the risk assessment should be accomplished according to ISO 12100. This standard gives general principles for risk assessment and risk reduction, but it is not especially tailored for assessing safety of autonomous systems.

In risk analysis process described in ISO 12100 (Figure 2), the first two phases, determination of limits and hazard identification, are the most crucial ones considering the outcome of the analysis [6]. But how the limits should be defined and how the possible hazards can be identified in the case of autonomous machines?

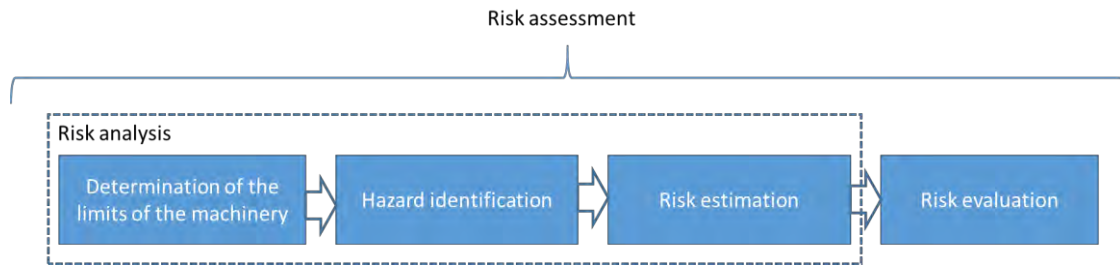


Figure 2. Risk analysis as a part of risk assessment process (adapted from [6]).

Common for all closed systems is that the operating environment is physically limited. Despite the limitations, the system can still face many different situations. In a closed system, the other actors in the area, e.g. human operators and other automatic systems are aware of the operating autonomous systems. Because of this fact, the risk analysis can be limited to the interaction between other systems and operators. In many cases, the number of operations in the closed system are also limited. These work procedures must be described in a systematic way for the risk identification procedure. One possibility is to describe the procedures utilizing SADT -based method. With SADT-type of functional blocks (Figure 3), it is possible to identify all the relevant factors that are needed to realize this function and it is also possible to identify risks that threaten this function to be fulfilled.

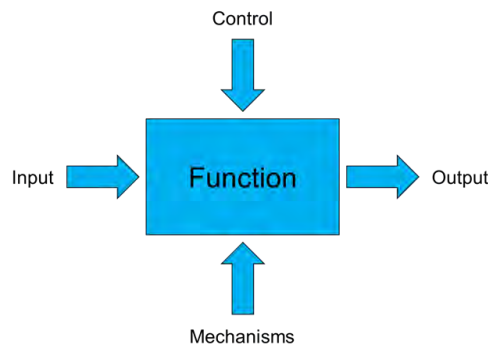


Figure 3. SADT basic element (adapted from [7]).

Risk analysis for open autonomous systems is a more complex task than for the closed systems. In open systems, it is not possible to limit the potentially hazardous situations, there might occur some unexpected problems in the area the system works. Autonomous cars are an example of very challenging open autonomous system: Cars are operating in normal traffic and there are infinite number of situations that the system might encounter. Some of the situations can be limited by the traffic legislation orders but in the real life, the human drivers and pedestrians do not follow the legislation all the time. The only way to manage the safety issues is to increase the number of sensors in the system. However, it is not easy to conclude what is a safe state in each case; e.g. stopping the system can be extremely dangerous in some occasions.

Because of the infinite number of situations the autonomous system might confront in open environment, the risk analyses of open autonomous systems have to be based on experiences from humans. One possibility is to crowdsource the identification of hazards by using semi-structured brainstorming technique to large number of people. For example, silent brainstorming by utilizing online messaging services might produce a massive amount of hazardous scenarios that could not be generated by a small number of engineers and other specialists that are involved in the development work. After the initial scenarios are generated, a smaller group of experts can classify and prepare them for thorough analysis. After this kind of open scenario collection, the risk analysis can be done in a same way than in conventional risk analysis, a group of scenarios at the time. This analysis method is called potential problem analysis, PPA [8].

3.2 Methodological framework to support development

Based on the challenges and methods discussed above, we propose a preliminary framework to support development of autonomous systems (Figure 4). The framework follows a systems engineering V-model, with additional features that take into account the system’s autonomous nature. In addition, we provide suitable methods to be used in some phases of development.

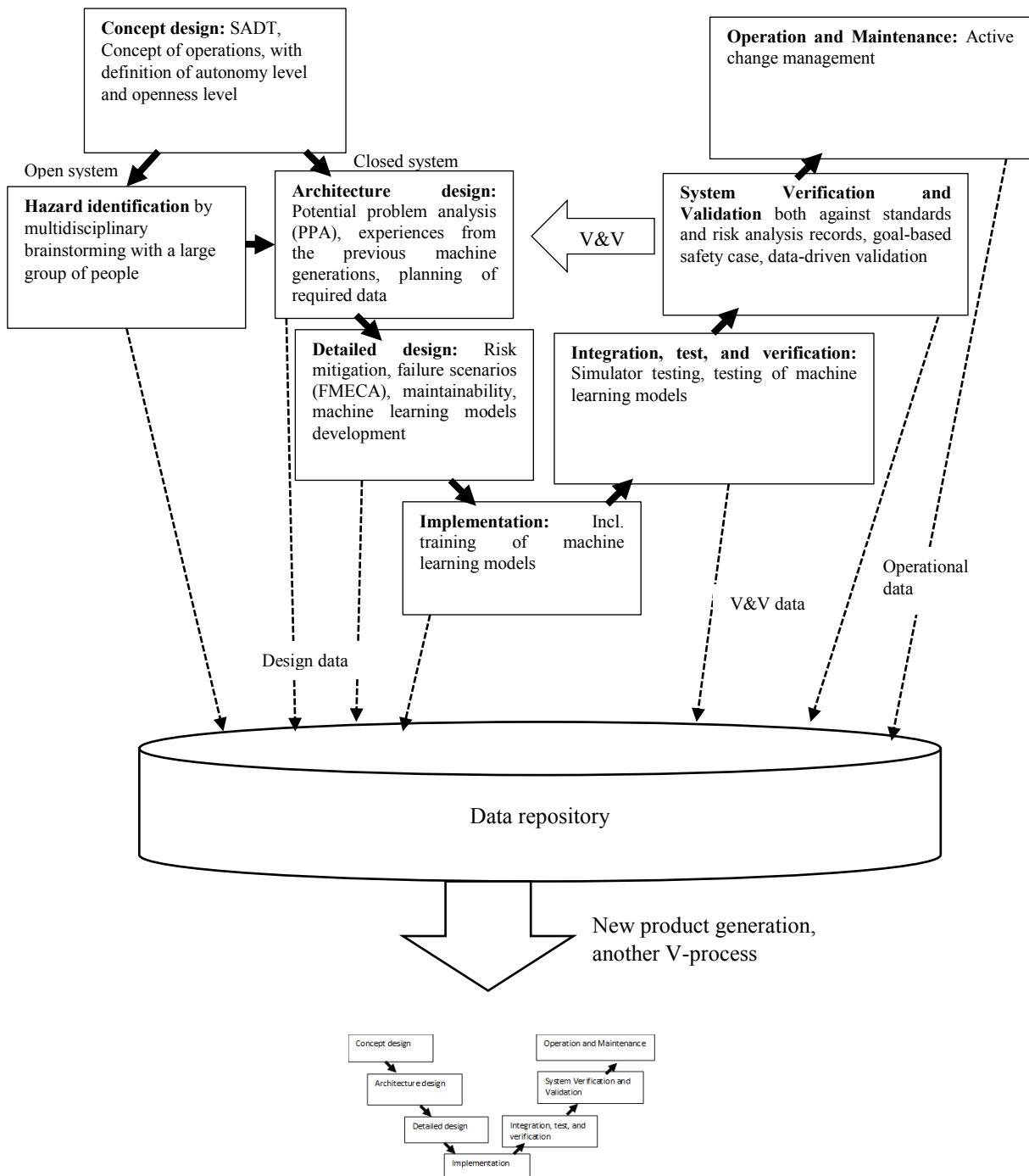


Figure 4. A proposed methodological framework for development of autonomous systems, including the collection of data to enable continuous improvement of autonomous systems.

The proposed framework expands on the traditional V-model in several ways. In the concept development phase, a robust system description methodology, such as Concept of Operations approach (see e.g. [9]), is suggested to be used. The pursued level of autonomy, as well as openness of the environment of use shall especially be described in detail. If the case is an open or restricted system, an additional step is added to the V-model. This represents a hazard identification phase, where the potential hazards of the system concept are identified in a workshop preferably involving several people from different disciplines.

In the architecture design phase, the framework emphasizes the accumulation of design knowledge within an organization. Increasing autonomy level is likely to cross-cut various product lines and generations, and it is essential that the knowledge is gathered into a structured database. In the framework, this is represented as a data

repository, where data is collected from all development phases, and which is to be used as a basis for future products.

In the detailed design, implementation and integration phases, autonomous capabilities are challenging especially when machine learning capabilities are involved. Here, the machine learning models and their desired results need to be carefully designed and tested, both from the algorithm development and data-driven points of views. As a potential approach for this, a “W-model” has been proposed to account for the effects of machine learning capabilities in autonomous systems [10]. In the W-model methodology, a parallel process is introduced to facilitate data-driven training and validation of the machine learning application. In our approach, we have incorporated the data-driven approach as a part of the framework, without overlaying another V-model. In practice, it is likely that extensive simulator testing will be required to carry out the necessary tests.

In the verification & validation (V&V) phases, we emphasize the importance of linking the produced safety evidence to the risk analysis findings and system requirements. A goal-based safety case approach has been proposed as a potential method to communicate the relationship between the system requirements and safety validation results [11].

4 DISCUSSION

Increasing autonomy in industrial systems is increasing the technology developer’s responsibility for ensuring safety and security of new systems. As the current standards rely on risk analyses to ensure safety, robust methodologies need to be in place to ensure that an adequate level of safety is achieved. The preliminary framework presented in this paper provides a general process that can be followed to improve safety-related design practices. It takes into account the differences between open and closed systems, and incorporates . The suggested methods can be used The framework also serves as basis for further developments towards a more holistic methodology to ensure that autonomous systems can be implemented in a safe and secure way.

5 REFERENCES

1. NFA Norwegian Society of Automatic Control: *Autonomous Systems: Opportunities and Challenges for the Oil & Gas Industry*. NFA, 2012.
2. Heikkilä, E., Tiusanen, R., Helaakoski, H., *Safety Considerations in the Design and Validation of Autonomous Machine Systems*. Proc. of the 2nd Annual SMACC Research Seminar 2017. Tampere University of Technology, pp. 49-52.
3. SFS-EN 61508-3:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 3: Software requirements.
4. Danks D. & London A., *Regulating autonomous systems: Beyond standards*. IEEE Intelligent Systems. Vol. 32:1., 2017.
5. ISO 17757:2017. Earth-moving machinery and mining – Autonomous and semi-autonomous machine system safety. ISO.
6. ISO 12100:2010. Safety of machinery. General principles for design. Risk assessment and risk reduction. International Organization for Standardization.
7. Ahmed, F., Robinson, S., Tako, A., *Using the structured analysis and design technique (SADT) in simulation conceptual modelling*. Proc. of the 2014 Winter Simulation Conference, IEEE. pp 1038-1049.
8. Reunanen, M. *Potential Problem Analysis*. In: Rouhiainen, V. & Suokas, J. (ed.). Quality Management of Safety and Risk Analysis. Amsterdam, 1993, Elsevier Science Publishers B.V. 291 p.
9. Osborne L. et al., *Clarus: Concept of Operations*, USA:Federal Highway Administration, Washington D.C., 2005.
10. Falcini F., Lami G., *Deep Learning in Automotive: Challenges and Opportunities*. Communications in Computer and Information Science, vol. 770. 2017, Springer.
11. Heikkilä E., et al. *Safety Qualification Process for an Autonomous Ship Prototype – a Goal-based Safety Case Approach*. Marine Navigation: Proc. of the 12th International Conference on Marine Navigation and Safety of Sea Transportation (TransNav 2017). CRC Press, pp. 365-370



Session 4

Protective devices and smart systems

Use of tablet PCs and smartphones for machine control

Nischalke-Fehn G.

Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA)
Alte Heerstrasse 111, 53757 Sankt Augustin, Germany

georg.nischalke-fehn@dguv.de

KEYWORDS: wireless machine control, smart device, IFA tablet frame, enabling function, emergency stop

ABSTRACT

Safe control devices for machinery are expensive, and with the right app, the smartphone in the user's pocket serves just as well. This might well be the view of Joe Public or for that matter a business analyst.

The focus of this paper however lies more on the technical aspects of a safe machine control employing a smartphone or a tablet PC. It will first describe the general (industrial) and technical safety (normative) requirements upon mobile control devices for machinery. A second focus of the paper is the presentation of a research study of this topic conducted at the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA).

The research study, which was prompted by consulting with accident insurance institutions and machinery operators, is intended to show the general conditions under which such devices can be used for the safe operation of machinery. In order to demonstrate the operating concept, a functioning model was produced. CAD software was used to design a tablet frame, which was then fabricated using 3D printing technology.

A standard tablet can be inserted into this frame. In addition to an emergency-stop button and two enabling buttons, electronics for processing the safety-related signals was integrated into the tablet frame. The safety-related emergency-stop and enabling signals are processed by the electronics in the frame, and packaged in a safety-related data message. The data are then transmitted by Bluetooth to the software (machine app) installed on the tablet. In turn, the machine app transfers these safety-related and non-modifiable data to the machine control system, for example by WLAN, together with its own machine data. The machine control system thus receives both the data from the machine app and the safety-related data message from the tablet frame. The concept is based upon the black-channel principle familiar from data transmission in safety technology. Commands are input by means of the buttons and safe electronics installed in the tablet frame. The tablet serves only as a medium for transmission. Neither a defect in the tablet or its failure, nor substitution with a different tablet or modification of the operating interface (machine app) therefore influence performance of the safety function.

1 INTRODUCTION

Modern working life is now inconceivable without tablet PCs and smartphones. They serve as communication devices, assume navigation tasks, provide support in logistical planning, and are now used to obtain or access information during the maintenance of machinery. Why then should these devices not be used to control machinery?

The driver of a goods vehicle, for example, could control equipment mounted upon it by means of a smartphone. A service engineer could operate machines to be serviced by means of a tablet PC, on which circuit diagrams or procedures are already loaded and can be displayed.

A software application for the operation of machinery can be programmed with little effort in the form of an app for tablet PCs or smartphones. Programming such an app clearly entails a lower cost and time overhead than that for developing the hardware of a control device. The user interface of the app can also be customized more easily for the most diverse of machine types, and is easier to modify should the machine undergo modifications or retrofitting.

Further advantages of the use of apps for machine control are that a single device can be used to control machines, parts of machines or even entire installations. Rather than needing a number of control devices in order to perform service/maintenance tasks on several machines, the service engineer need only install multiple machine apps on his tablet PC. To control the next machine, he need only switch app.

2 BACKGROUND

If smartphones or tablet PCs are to be used in an industrial environment, possibly even to control machines, they must of course satisfy the same requirements that apply to other control devices used for these purposes.

In the first instance, the various requirements applicable in industrial areas of application and the standard consumer sphere spring to mind; an obvious example being the ambient conditions prevailing in an industrial environment. Criteria such as adequate ingress protection, mechanical strength, immunity to climatic conditions and satisfaction of the EMC requirements and wireless transmission are for example considerably stricter in industrial applications than for devices in the consumer sphere. Display legibility, glare and reflections in sunlight, or operation of the device by users wearing work gloves, may give rise to difficulties in some applications. Use under conditions such as these therefore requires at least standard tablet PCs to be encased in protective sleeves or rugged tablets to be used.

In addition to these general requirements however, the safety requirements and provisions of standards governing mobile control devices, such as those for safe cableless remote control, must be observed. It goes without saying that these requirements must be met by control concepts employing tablet PCs and smartphones.

Detailed requirements concerning the functional safety of machine controls can be found both in Annex I of the EU Machinery Directive 2006/42/EC [1] and in further harmonized standards. The safety-related parts of a control system and its subsystems must satisfy the relevant requirements of standards governing functional safety, such as ISO 13849 [2] or EN 61508 [3].

Functional requirements upon cableless control devices, for example concerning wireless communication and safety-related functions such as start, stop and emergency stop, are set out in IEC 62745 [4]. General requirements concerning the electrical equipment of machinery are described in IEC 60204-1 [5]. This standard contains supplementary functional requirements applicable to cableless control devices, for example concerning the association of a given control device to one or more machines, the initiation of hazardous movements by means of an enabling function, and also requirements concerning the emergency stop function. In the new edition of this standard, the emergency stop function is for the first time permissible on portable cableless control points.

Requirements specifically concerning the emergency stop function can also be found in ISO 13850 [6]. This standard describes, for example, the requirements concerning the operating conditions, the design of the actuator (both electrical and in form), the availability/accessibility, and the measures for avoidance of confusion between active and non-active emergency stop devices.

Assistance with the topic of mobile control devices can be found in the two test principles GS-ET-07 [7] and GS-VL-36 [8] of DGUV Test. These contain requirements and test descriptions for user information, external design (actuators, display elements, materials, ergonomics), and measures against unauthorized use. Further requirements are directed at the environment (mechanical strength, climatic conditions, IP ingress protection), the electrical/electronic specification, EMC and radio transmission, functional aspects (emergency stop, control of the operator's location, data transmission), and communication between an operator control device and the machine's control system.

If these diverse requirements are all considered, it soon becomes clear that concepts in which smartphones and tablet PCs are used for the operation of machinery and installations cannot be implemented as easily as initially thought. Based on current information, no operating concepts are available on the market that satisfy the requirements described above solely by means of tablet PCs or smartphones. Implementing safety-related control functions by means of these devices alone does not appear possible at present.

Many of the requirements described above are not immediately comprehensible to the layperson. The relevance of such requirements can be demonstrated very easily with reference to the aspect of "transfer of data/information from the control device to the machine". If a wireless link is used for this purpose, aspects such as loss, delay or injection of a message must be controlled as well as falsification of a message and the identifiability of sender and receiver. These safeguards are not implemented adequately for safety-related data in the conventional transmission media such as WLAN or Bluetooth, and additional measures are therefore required.

The topic of security is also increasing in importance in the area of machine control, and must be considered here accordingly. Unauthorized persons or devices must be prevented from gaining access over the communication channel, since malware or hacker attacks could manipulate or falsify machine data and thereby give rise to unwanted situations.

Finally, the wireless link makes the cable link between control device and machine unnecessary, but results in the operator's location no longer being controlled. Where required by the application in question, alternative means must be sought of ensuring that operation is possible only from outside a hazardous area or within a specified safety area.

3 MOTIVATION

Despite these – in some cases demanding – requirements, a range of apps for machine visualization, up to and including machine control, can already be found in the app stores. For example, apps are available delivering both diagnostics and control functionality for equipment fitted to commercial vehicles.

Apps are now also being used sporadically for the control of machine tools; in these cases however, the machines are generally in automatic mode, and external safeguards are active. Control concepts in which hazardous movements are initiated solely through an app installed on a smartphone or tablet PC are not known at this point in time.

It is now normal for automated guided vehicles to move completely freely and independently through factories. Provided certain rules are observed, it is also permissible for these vehicles to be controlled manually by means of smartphones or tablet PCs for the purpose of servicing or in an emergency. The relevant provisions can be found in a FAQ issued by the DGUV's Trade and logistics expert committee [9].

4 ACTIVITIES OF THE IFA

Prompted by consultations and discussions of the use of tablet PCs and similar devices for control purposes, the IFA conducted a concept study. The purpose of this study was firstly to consider the functional aspects and the interests of industry, and secondly to describe an approach to operating machinery safely by means of such a consumer device.

A concept was developed in the study by which a machine can be controlled safely by means of the two safety functions "enabling" and "emergency stop" in combination with a machine app installed on a tablet PC. The two safety functions have to be implemented in such a way that neither the tablet PC nor the machine app can have an influence relevant to safety upon their execution. Besides theoretical examination of the subject, the functional prototype shown in Figure 1 was manufactured in order to provide a better understanding of its functional principle and handling.



Figure 1. Functional prototype of the IFA tablet frame.

A frame was designed by means of CAD software and manufactured by 3D printing. A standard 10" tablet PC can be inserted into the frame, called IFA tablet frame.

In order to demonstrate the functional principle, an emergency-stop button and enabling switches were built into that frame together with the necessary electronics. The electronics detect the states of the emergency-stop actuator and the two enabling switches and transfer them by Bluetooth to a software app installed on the tablet PC. Addition of a machine simulation function to the functional prototype is still in progress.

5 CONCEPT

The concept is based upon the principle that proper execution of the safety functions is assured entirely by the "frame" and the safe machine control, independently of the operating software on the tablet PC or smartphone. Figure 2 contains a schematic representation of the principle of operation.



Figure 2. Principle of operation.

The electronics built into the frame detect the states of the enabling switches and the emergency-stop actuator. This information is processed in the electronics and "packaged" in a safety-related data message. This data package can be transmitted to the app wirelessly, for example either by Bluetooth or WLAN or by USB, in order for the machine to be controlled. The machine app installed on the tablet PC receives the safety-related data and transfers them, together with the control data from the application, to the machine control system.

The machine control system thus receives both the standard data from the machine app, and the safety-related data message containing the safety-related information from the tablet frame. This machine control system must of course be a safety-related control system that determines whether the safety-related data received from the frame are valid and not falsified, and only then executes the control commands selected by means of the machine app. Alternatively, a standard control system can be used to control the machine, provided the safety-related data from the frame are processed in an external safety module which is responsible for carrying out the safety functions.

The tablet PC or smartphone thus serves only as a means of transferring the safety-related information generated by the electronics in the frame to the machine control system. Experts term this a "black channel" approach, which is now the usual means of transmitting safety-related messages.

Since proper execution of the safety functions is ensured by the electronics built into the frame and by the machine control system, failure of the tablet PC or the machine app has no influence upon execution of the safety functions. Nor do replacement of the tablet PC or modifications to the user interface (machine app) influence the functional safety.

When implementing the concept, it must be taken into account that the safety-relevant components (e.g. actuators, electronics built into the frame) must satisfy the relevant safety requirements of the machine application. If the application scenario allows the machine to be controlled only when the operator is located within or outside a defined area, suitable measures must be implemented that enable localisation of the control device to be detected, e.g. using RFID or NFC technology or other sensors. It must also be ensured that the frame is active only when the relevant control device (tablet PC or smartphone) is inserted into it. This is to ensure that the machine cannot be operated from the tablet PC – which is not a safe device – unless the user also has access to the accompanying frame and its emergency stop actuator. Ergonomic aspects such as weight and handling must not be forgotten when designing the frame.

6 CONCLUSIONS

The concept study described a solution by which safe control of a machine operation could be implemented using smartphones or tablet PCs. The publications to date on the subject and the IFA's close contacts with industry are engendering interest among companies. The IFA is currently discussing implementation of the concept presented here with a number of electronics manufacturers. Manufacturers and operators of machinery are also being involved in the discussions, in order for the concept to be trialled in applications in the field. Further information on this topic, such as the presentation "Machine operation via tablet and smartphone - but safe!" [10] and the publications "Use of Tablet PCs and Smartphones for Machine Control" [11] and "Verwendung von Tablets und Smartphones zur Maschinensteuerung" [12] are available on the website of the Institute for Occupational Safety and Health Protection of the German Social Accident Insurance (IFA) [13].

7 REFERENCES

1. EU Machinery Directive 2006/42/EC, *Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast) OJ EU (2006) L 157, pp. 24-86; <http://eur-lex.europa.eu>.*
2. *ISO 13849-1: Safety of machinery – Safety-related parts of control systems Part 1: General principles for design* (2015-12).
3. *IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems – Parts 1 to 7* (2010-04).
4. *IEC 62745 Safety of machinery – Requirements for cableless control systems of machinery* (2017-03).
5. *IEC 60204-1: Safety of machinery – Electrical equipment of machines – Part 1: General requirements* (2016-10).
6. *ISO 13850: Safety of machinery – Emergency stop function – Principles for design* (2015-11).
7. *Test principle GS-ET-07 of DGUV Test: Principles of testing and certification of wireless control equipment for machinery safety requirements* (2010-03) https://www.bgetem.de/arbeits-sicherheit-gesundheitschutz/pruefen-zertifizieren/pruef-und-zertifizierungsstelle-elektrotechnik/pruefgrundsaeetze/GS-ET-07/at_download/file.
8. *Test principle GS-VL-36 of DGUV Test: Grundsätze für die Prüfung und Zertifizierung von kabellosen Steuerungen für Fahrzeugaufbauten und Maschinen auf Nutzfahrzeugen* (2015-07) https://www.dguv.de/medien/dguv-test-medien/_pdf_zip_doc_ppt/pruefgrundsaeetze/vl/gv-vl-36_funkfernstrg.pdf
9. *Questions and answers on the subject of "Automated guided vehicles"*.
10. <https://www.dguv.de/fbhl/sachgebiete/foerdern-lagern-logistik/fahrerlose-flurfoerderzeuge/faq/index.jsp>
11. Nischalke-Fehn G., *Presentation: Maschinenbedienung via Tablet und Smartphone – aber sicher!*
12. https://www.dguv.de/medien/ifa/de/fac/arbeiten_4_0/tabletrahmen.pdf, 2018.
13. Nischalke-Fehn G., Bömer T., *Use of tablet PCs and smartphones for machine control*.
14. https://www.dguv.de/medien/ifa/en/pub/ada/pdf_en/aifa0398e.pdf, 2018.
15. Nischalke-Fehn G., *Verwendung von Tablets und Smartphones zur Maschinensteuerung*.
16. Betriebliche Prävention, sicher ist sicher, Sonderausgabe TRENDS & Innovationen 2018/2019, pp. 4-8.
17. http://www.dguv.de/medien/ifa/de/pub/grl/pdf/2018_048.pdf
18. DGUV web page: Use of tablets and smartphones for safe machine control.
19. <http://www.dguv.de/ifa/fachinfos/arbeiten-4.0/industrie-4.0/sicher-mit-tablet-und-smartphone/index-2.jsp>, 2018.

General principles of smart personal protection systems design

Marchal P., Baudoin J.

Institut national de recherche et de sécurité (INRS) – 1, rue du Morvan – CS 60027 – 54519 Vandœuvre Cedex
– France

patrice.marchal@inrs.fr
james.baudoin@inrs.fr

KEYWORDS: Smart, Personal Protective Equipment, Definition, Design, Analysis

ABSTRACT

The emergence of "smart" personal protective systems (SPPS) is raising many questions. Firstly for manufacturers, who need to know what safety requirements are applicable when designing such systems, and secondly for user companies, who have questions about their performance and their limitations. In order to provide some answers, this article proposes a definition of an SPPS, and an approach, illustrated by an example, for steering analysis of the safety of such systems.

1 INTRODUCTION

Riding the boom in technology related to the Internet of Things, a new generation of personal protective equipment (PPE) has emerged, namely "smart" personal protective systems (SPPS). On this highly dynamic market, new solutions [1] are appearing regularly and, with them, new questions and issues for occupational risk prevention. In order to give some answers to these questions, it seems necessary, first and foremost, to propose a definition of a SPPS. We can observe that the adjective "smart" is applied by PPE manufacturers to a broad spectrum of functions and features ranging from merely adding an energised accessory to the PPE to integrating sensors into a processing system that is then capable of dynamically changing the behaviour of the PPE or of an external system. For example, such smart products may be heated jackets or gloves, connected safety footwear, or safety helmets or goggles equipped with augmented reality systems (displaying information in real time on the goggles or on the screen of the helmet).

After having recalled the general prevention principles applicable to these products, this article proposes an approach based on the functional properties claimed by the manufacturers of such devices, so as to guide them in choosing the applicable safety guidelines and reference frames. This approach will also be useful to end-users for guiding their choices when acquiring this type of product.

2 DEFINITION OF A SMART PERSONAL PROTECTIVE SYSTEM (SPPS)

Since a SPPS is first and foremost a piece of personal protective equipment (PPE), we should, firstly, go back to the definition of such equipment. According to Regulation (EU) 2016/425 [2], PPE means "*shall mean any device or appliance designed to be worn or held by an individual for protection against one or more health and safety hazards*". Two concepts supplement this definition, namely the concepts of "system" and of "smart". A "system" is an "*assembly of apparatuses or devices made up of various elements integrated into the equipment and making it possible to provide one or more particular functions*". The adjective "smart" as applied to automatic machines, or indeed to materials such as textiles, characterises their capacity to react automatically following changes in the environment or following an external signal [3]. Applied to PPE, this adjective of "smart" may thus, for example, designate a system that reacts automatically:

- by informing the wearer or a third party by indicating a value, a position, etc., e.g. a pair of goggles equipped with a sound level meter and with the ambient noise level being displayed on one of the lenses;
- by alerting the wearer or a third party by indicating a threshold value has been exceeded, e.g. a jacket for giving protection against heat that is equipped with an inside temperature detector that triggers an alarm in the event a predefined threshold is exceeded;
- by changing its protective function (for example: adapting the filtration of an active welding mask) or by controlling another item of equipment (shutting down a dangerous machine when the wearer is close to it).

On the basis of these details, the following definition is proposed: *A smart personal protective system (SPPS) is an assembly of devices or elements that is designed to be worn or held by a person for protection against one or more health and safety hazards, and that reacts automatically, either to changes in its environment or to an external signal.*

Therefore, conversely:

- items of conventional PPE or of conventional combined PPE¹ are not SPPSs because they lack any "smart" function;
- supplemented with an energised device, PPE is not necessarily an SPPS. For example, goggles that incorporate manually actuated lighting constitute a personal protective system (PPS) that, even so, may not be said to be "smart";
- an item of equipment or a system that is said to be "smart" and that is worn or held by an employee (connected T-shirt, connected watch, tablet, etc.) but that does not protect that person, in the sense of the definition of PPE, is not an SPPS.

3 APPROACH FOR ANALYSING A SPPS

In order to guide manufacturers and notified bodies in assessing the level of safety of SPPS as defined, we propose an approach that is based both on the general principles applicable to PPE, and also on a functional analysis.

3.1 General principles

As indicated above, SPPS are first and foremost personal protective equipment. Their manufacturers must therefore, before they are put on the market, make sure that they meet the essential health and safety requirements defined by Regulation (EU) 2016/425 in terms of protection levels, effectiveness, comfort, ergonomics, innocuousness, and strength.

Thus, adding devices or components to make PPE "smart" should not adversely affect its initial level of personal protection. The additional devices should operate properly under all foreseeable conditions of use of the SPPS. They should not generate any additional discomfort or new risk for the wearer, even in the event of a malfunction. Therefore, an SPPS should be assessed on the basis of the essential health and safety requirements and of the testing standards applicable to the corresponding PPE. This assessment is performed by the manufacturer itself (self-certification) or by a notified body (EU type-examination) depending on the category as defined in Regulation (EU) 2016/425 (cf. Table I). It should be performed on the entire SPPS, even if the added components or devices are removable or disassemblable.

It is therefore incumbent on the manufacturer of the SPPS to define precisely:

- the personal protection function(s) claimed, in order to define the essential health and safety requirements applicable, their category (and thus the procedure for assessing conformity to those requirements), and the applicable testing standards;
- The devices or components added to the basic PPE, in order to define the configuration of the tested system.

Table 1. Categories of PPE.

Regulation (EU) 2016/425 defines 3 categories of PPE depending on the nature of the risk against which the PPE protects. It also gives an exhaustive list of the risks covered by PPE of categories I and III. A specific procedure for assessing conformity with the essential safety requirements corresponds to each of these categories.	
Category I	Protection against minimal risks
Category II	Protection against risks other than those define in categories I and III
Category III	Protection against risks that may have very serious consequences, or indeed be fatal

¹ Combined PPE: a unit constituted by several devices or appliances which have been integrally combined by the manufacturer for the protection of an individual against one or more potentially simultaneous risks (as defined in the Regulation EU 2016/425). See: For further information.

3.2 Analysis of the functions of the SPPS

In addition to these general principles relating to the personal protection functions, the manufacturer, or the testing body, should question themselves about all of the functions claimed for the SPPS:

- are the personal protection functions provided by the SPPS "smart" or not?
- are the "other" functions proposed safety functions or not?

By analogy with the definition of a safety function in the field of machinery (as defined in Standard NF EN ISO 12100 [4]), we have chosen the following definition of a safety function for SPPS: "*function of equipment whose failure can result in an immediate increase of the risk*". In the case of an SPPS, this definition may apply to the personal protection functions and to the "other" functions.

On the basis of this analysis and of the general principles mentioned, a four-step approach is proposed for assessing the level of safety of these systems and thus for guaranteeing user safety. It is then applied to an example.

Step 1: Identifying the functions of the SPPS

The object of this step is to list all of the functions claimed by the manufacturer of the product: the personal protection functions and the "other" functions, regardless of whether or not they are safety functions and of whether or not they are smart.

Step 2: Analysing the personal protection functions

The aim of this step is to specify and to estimate the risks against which the personal protection functions protect and, finally, to define the means to be implemented to cover those risks. As indicated above, this information makes it possible to determine the category of the system (cf. Table I), the essential health and safety requirements pursuant to Regulation (EU) 2016/425, and the applicable testing standards.

When the personal protection function incorporates a "smart" portion, e.g. a dynamic filter for a welding facemask, or an active attenuation device for a personal protector against noise, it is necessary:

- to ensure the smart portion is innocuous. For example, if an energy source is used, it should not generate any risk for the wearer of the SPPS.
- to check its suitability for performing the function and its behaviour in the event of failure and/or of environmental disturbances.

As regards the latter point, the principles of the approach proposed by INRS and its German counterpart IFA in the 2000s [5] remain valid. However, it is necessary to update that approach in order to take account of the changes in standardization. Therefore, we propose to qualify the level of safety of the "smart" portion by defining a required performance level (PLr) as defined in NF EN ISO 13849-1 [6]. Thus, in the case of an active protector for protecting against noise, discussed in that previous article, category "B" as defined by standard NF EN 945-1 [7] required for the active attenuation device would be replaced with the required performance level "PLb" as defined in standard NF EN ISO 13849-1.

Step 3: Analysing the "other" functions

This third step concerns the "other" functions claimed by the manufacturer: i.e. those that are not personal protection functions.

Firstly, it is necessary to make sure they are innocuous under the foreseeable conditions of use of the SPPS.

Then it is necessary to check the texts that are applicable depending on the nature of the function (safety function in the sense of the "Machinery" Directive 2006/42/CE [8] for example), or on the technical solutions used for performing the function ("EMC" Directive 2014/30/EU [9] if electrical and electronic equipment is used in the technical solution or the "Low Voltage" Directive 2014/35/EU [10] for electrical equipment where applicable, etc).

Step 4: Compatibility between the functions

The last step consists in making sure all of the functions of the SPPS are mutually compatible. After assessing the various functions individually, it is important to check that they do not disturb one another. For example, an electronic system of one function should not be disturbed by the electrical power supply of another function.

Similarly, the innocuousness of the combination of all of the functions should be checked, for example, if a PPE manufacturer wishes to add a multitude of alarm devices to a protective jacket, that manufacturer will need to make sure that the weight of the jacket remains reasonable so that it continues to have a satisfactory ergonomic level.

It is important to remember that the analyses and tests conducted during the various steps should concern the entire SPPS, even if the added components or devices are removable or disassemblable.

4 EXAMPLE OF APPLICATION OF THE APPROACH

In order to illustrate the approach proposed in the preceding chapter, we put ourselves in the place of a designer of a protective helmet who wishes to take advantage of the boom in connected objects. He decides to upgrade its product by adding a detection system making it possible to detect whenever the helmet (and therefore the wearer) intrudes into a dangerous area around a machine so as then to cause the machine to shut down. This SPPS is fictitious but it is realistic because it is imagined on the basis of projects identified in the literature [1]. In order to provide this detection function, three modules are imagined (shown in blue in Figure 1): a detection system (sensors), a processing and wireless transmission unit, and a unit for receiving and using the signal. The first two elements are integrated into the helmet. The third is to be integrated into the control circuit of the machine from which the wearer is to be protected.

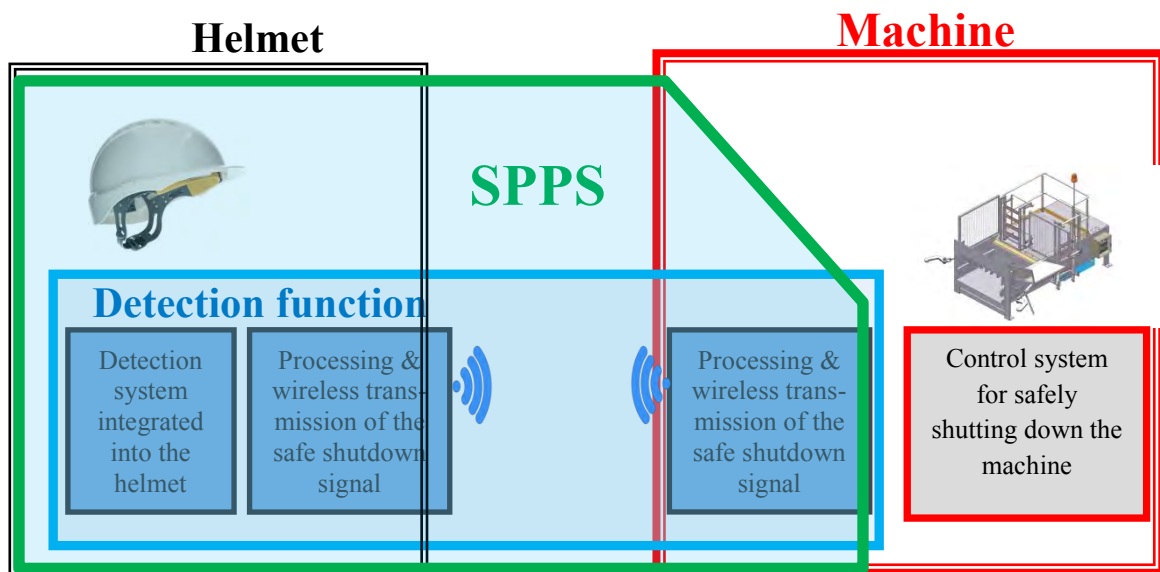


Figure 1. Illustration of the structure of the fictitious SPPS.

Step 1: List of functions of the SPPS

The SPPS used as an example has two functions. A conventional personal protection function for protecting against the risks of impacts to the head, and a detection function that can be said to be "smart" because it automatically causes another item of equipment to shut down.

Step 2: Analysing the personal protection function

The helmet is PPE function and it should comply with the essential requirements of Regulation (EU) 2016/425. For that purpose, it is possible to follow the recommendations of harmonised European Standard NF EN 397, which defines all of the characteristics and tests that protective helmets have to satisfy.

In the present case, the category for the envisioned personal protective function is Category II.

The various tests, in particular the mechanical strength tests, should be conducted on the entire SPPS in order to check that integrating detection and processing/transmission modules does not weaken the helmet. Similarly, it is necessary to make sure that those modules do not generate any discomfort for the wearer of the helmet (weight, etc.).

Step 3: Analysing the "other" function.

In this example, the "other" function is to detect the wearer of the helmet intruding into a dangerous area so as to issue a shutdown order that is usable by a machine.

First of all, the manufacturer should make sure that this function does not create any new risks for the wearer or for third parties: electrical risks if the modules are powered by a battery for example

As this detection function is a safety function in the sense of the "Machinery" Directive 2006/42/CE, the manufacturer must respect the essential health and safety requirements that apply to this function. For this he could use the harmonized European Standard NF EN 61496-1 [9] that provides general design, construction and testing requirements for contact less electro-sensitive protective equipment specifically designed to detect persons within a safety-related system.

In particular, the manufacturer of the SPPS should firstly characterise the function precisely: response time, sensitivity of the detection, dimensions of the detection area, and conditions of use (temperature, humidity, shocks and impacts, etc.).

He must also define a “Type” for this electro sensitive safety function accordingly to the risks to be covered. Three types are defined (2, 3 and 4) by the NF EN 61496-1. They characterize the behavior of the system in the presence of defects and under the influence of environmental conditions. For that purpose, the manufacturer may also use Standard NF EN ISO 13849-1 to define a performance level for the control system (PLr: Performance Level required).

Tableau 2. “Types” and “PLr” for an electro sensitive safety function.

Electro sensitive protective equipment				
	TYPE 1	TYPE 2	TYPE 3	TYPE 4
Safety performance according to NF EN ISO 13849-1	Non applicable	PLr c	PLr d	PLr e

Then, depending on the “Type” and the “PLr” chosen by the manufacturer for the detection function, the SPPS can be used for applications of various levels of risks. If the manufacturer of the SPPS intends its "smart helmet" to be used for detecting the wearer of the helmet in the event of frequent exposure within the danger area of a machine having risks of high potential seriousness (cutting or severing) and little possibility of avoidance, the required “Type” would be “4” and the PLr would be "PLe".

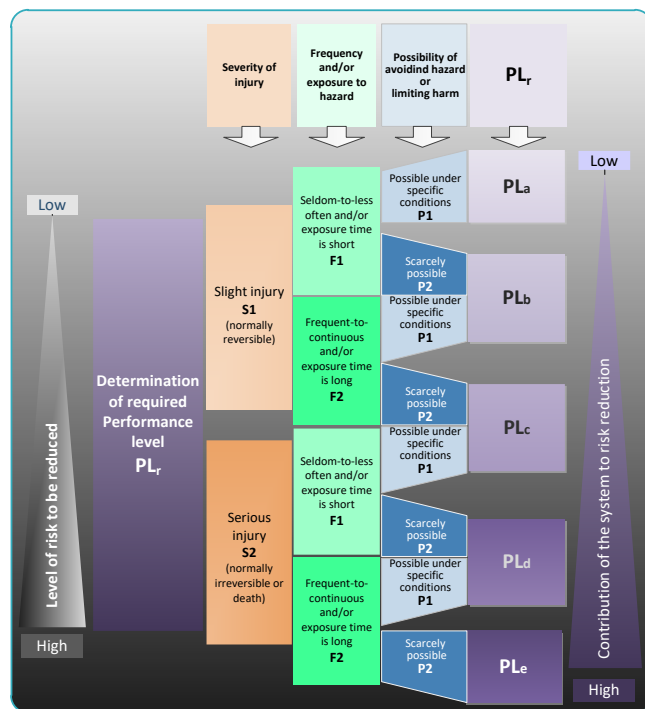


Figure 2. Illustration of the chart for determining the required performance level (PLr) [7].

It is important to remember that since the "other" function of the SPPS is designed to act on the control for shutting down the dangerous moving elements of a machine, this portion of the machine shutdown control system should have a PLr as defined in NF EN ISO 13849-1 that is greater than or equal to the PLr of the "other" function.

As an electrical energy source is envisaged, the manufacturer of the SPPS should also make sure the SPPS conforms to the EMC Directive 2014/30/EU.

Step 4: Compatibility between the functions

Under the intended conditions of use, the manufacturer of the SPPS must check that the 2 functions of the SPPS in question are mutually compatible. For example, the function of providing protection against impacts and shocks to the head should not degrade or prevent the transmission of the signal from the detection function.

The innocuousness of the combination of the two functions should also be checked.

5 CONCLUSION

New items of personal protective equipment that are said to be "smart" are regularly appearing, and, with them, come new questions and issues for occupational risk prevention.

First and foremost, a definition is proposed of such items of equipment that we are calling "Smart Personal Protective Systems" ("SPPS").

On this basis, an SPPS, which is above all an item of PPE, must meet the essential health and safety requirements defined by Regulation (EU) 2016/425 in terms of protection levels, effectiveness, comfort, ergonomics, innocuousness, and strength. In order to guide manufacturers and notified bodies, we propose a four-step approach to analysing SPPS. The analysis should be established on the basis of the conditions and limitations of use claimed by the manufacturer of the SPPS or by the person or entity responsible for putting it on the market.

All of the functions of the SPPS should be listed. The personal protection functions, be they smart or otherwise, are distinguished from the "other functions" that do not provide any personal protection function.

The conventional personal protection functions can be analysed by using the usual normative reference frames and guidelines applicable to PPE. When these functions are "smart", it is necessary to determine how they will behave in the event of failure and/or of environmental disturbances depending on the analysis of their contribution to reducing the risk. To that end we propose to update the approach proposed by INRS and IFA in the 2000s in order to take into account how the standards have changed. Thus, we propose to qualify the level of safety of the "smart" portion by defining a required performance level (PLr) as defined in NF EN ISO 13849-1.

Analysing the "other" functions should make it possible to check that they are innocuous under the foreseeable conditions of use of the SPPS, and to identify the regulatory texts that are applicable to it (EMC Directive, Machinery Directive, etc.). In particular, if one of these "other" functions is a safety function in the sense of the "Machinery" Directive, its performance level (PLr) should be defined.

Finally, the compatibility between all of the functions making up the SPPS should be checked to ensure both that they can operate properly and that they are innocuous, whether they are "PPE functions" or "other functions".

To conclude, the approach proposed shows that if a PPE manufacturer wishes to make its product smart by adding functions "other" than functions related to personal protection, it must then look at the other standards or texts applicable to such other functions: e.g. the Machinery directive as in the example presented. Conversely, if it is another manufacturer who wishes to add additional elements to PPE (a badge in a helmet, lighting on the arms of goggles, etc.), it must obtain the consent of the PPE manufacturer to perform a new assessment of the entire PPE system.

The work of INRS on the subject of SPPS is continuing, in particular in order to compare the proposed approach with the various different foreseeable configurations of products, since these "technological" products are evolving continuously. As recalled by Henk Vanhoutte in a preceding article published in *Hygiène et Sécurité du Travail* [9], such products are bound to come under different and not necessarily harmonised regulations: PPE Regulation, Machinery Directive, Low-Voltage Directive, Electromagnetic Compatibility (EMC) Directive, etc.

6 REFERENCES

1. Gralwicz G. (Ph.D), Owczarek G. (Ph.D) *An inventory of selected electronic, textronic, mechatronic and ICT-based solutions for safety-related applications in smart working environments*, CIOP, Mars 2015, 54 pages
2. Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC.
3. FD CEN/TR 16298, *Textiles intelligents*, March 2012, 29 pages
4. NF EN ISO 12100 *Safety of machinery – Genral principles for design – Risk assesement and risk reduction*, December 2010, 77 pages
5. Buchweiller J.P., Klein R., Iotti J.M., Kusy A., Reinert D., E. Christ E., *Protective equipment individual including electronic circuits*, Safety sciences, 2003, 14 pages
6. NF EN ISO 13849-1 - *Safety of machinery – related parts of control system, Part 1 : General principles for design*, March 2016, 86 pages
7. EN 954-1 - *Safety of machinery – related parts of control system, Part 1: General principles for design*, December 1996, 35 p.
8. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC.
9. Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility
10. Directive 2014/35/EU of the European Parliament and of the Council of of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limit.

Session 4 – Protective devices and smart systems

11. NF EN 61496-1 *Safety of machinery – Electro-sensitive protective equipment –Part 1: General requirements and tests*, May 2014, 54 p.
12. Vanhoutte H., *Hygiène et sécurité au travail*, No. 247, June 2017, 2 pages

Safety related sensors used for protection of person

Wüstefeld M.

SICK AG, Erwin-Sick-Str. 1, 79183 Waldkirch, Germany

martin.wuestefeld@sick.de

Safety related sensors are applied to machinery presenting a risk of personal injury. They provide protection by causing the machine to revert to a safe condition before a person can be placed in a hazardous situation.

Existing sensor standards provides specific design and performance requirements for manufacturer and integrators of sensors into safety related control systems. The specific design and performance requirements gives a clear but limited guideline for specific sensor technologies (like optical sensors) , specific sensing functions (like capability to detect the presence of a specified object in a configured protection zone) or consider only the detection of objects representing parts of body of adults with limited range of properties (like minimum size or reflectivity).

Applications of Autonomous systems like Automated guided vehicles, Service Robotics or Human Machine Interaction in Industries show an increasing demand for new sensor technologies (e.g. Radar, Ultrasonic sensors), new kind of sensor functions (e.g. classification of objects, position of an object) or combination of different sensor technologies in a sensor system.

Sensor manufacturers or integrators use in such cases generic functional safety standards as guideline for the safety related product design. Generic functional safety standards like IEC 61508 or sector specific machinery standards like IEC 62061 or ISO 13849 are general and product design can be carried out without limitations, which are inappropriate for the requirements given by the specific application. Applying these standards would require a dedicated analysis of systematic capabilities of a sensor or sensor system (e.g. dependability of the sensing function under tolerance conditions and environmental influences). There is not enough guidance given in these standards to prevent design failures or insufficient capability to detect the specified object in certain environmental conditions. This may result in an intolerable risk for persons.

The new standard IEC/TS 62998-1 fills the gap for the examination of systematic capabilities between design specific sensor standards and generic functional safety standards of electrical, electronic or programmable electronic control systems.

Future Prospects of Enabling Device as an Essential Safety Device for the Safety of Machinery and Safety2.0

Nobuhiro M., Dohi M., Maeda I., Okada K., Fujita T.

IDEC CORPORATION – 2-6-64, Nishimiyahara, Yodogawa-ku, Osaka, Japan

m.nobuhiro@jp.idec.com

m.dohi@jp.idec.com

i.maeda@jp.idec.com

k.okada@jp.idec.com

t.fujita@jp.idec.com

KEYWORDS: Safety of machinery, 3-position enabling switch, robot, collaborative safety, Safety2.0

ABSTRACT

The isolation/stop principle has been applied to implement safety measures in safety of machinery, which is based on the concept to ensure safety by isolating the running machine from operators with a guard, or stopping the machine when operators approach it. Machines' modes is classified into two; automatic-operation mode when operators are isolated from the machine, and human-attended operation mode when operators work near the machine that has stopped running for human-attended operations such as maintenance and/or changeover, etc. Most industrial accidents occur either during human-attended operation or when switching between operation modes. During human-attended operation mode, the machine sometimes needs to run while the operator is nearby, raising the possibility of fatal physical contact. When switching the operation mode, the machine may start unexpectedly and also raising the possibility of fatal physical contact. The ergonomically designed enabling device was developed by taking into account the human's involuntary movement in sudden danger. Operators in danger either release or grasp the device. The device disables machine operation when released or grasped tightly and enables machine operation only when being maintained in the middle position. Use of enabling device is recognized as an essential measure for teaching industrial robots [1]-[3]. New industrial movements are taking place in recent years, including Industry 4.0 in Germany and Connected Industries in Japan. The setting is changing, as clearly shown in the number of enabling devices we have delivered over 20 years, and also the number of industrial robots used during the same period. The drastic increase of enabling devices and industrial robots indicates that collaborative robot system has been adopted in more actual applications, and that conventional principle of isolation/stop may not be sufficient in some applications. These are where Safety2.0, new collaborative safety concept, is applicable to ensure safety and productivity in areas where humans and machines/robots work collaboratively [4]-[10].

1 INTRODUCTION

With the coming of the Fourth Industrial Revolution, information and communications technology (ICT) connects various things in a network, and optimization and efficiency are achieved with the use of cloud computing and artificial intelligence (AI). As a result, manufacturing sites are also undergoing major transformation on a global scale, and meanwhile, manufacturing sites in Japan are changing day by day. In addition to an expansion of the Internet-of-things (IOT) industry and the robotic revolution, a move toward "Connected Industries" is in development. This is an initiative to aim at building a new solution-oriented industrial society making use of technology and on-site expertise that are necessary resources for the progress of digitalization.

Against this background, there has been increasing demand for a next-generation manufacturing site that is both flexible and productive to meet diversifying customer needs in a timely manner. In the field of factory automation, people and robots need to share the same space and engage in collaborative work. In such an environment, it is difficult to ensure occupational safety only through conventional approaches. This paper discusses the future prospects of the three-position enabling switch, a key device for achieving safety in an environment of collaboration between people and robots, in addition to the changes in the idea of safety along with the evolution of manufacturing sites.

2 THE CONVENTIONAL IDEA OF SAFETY: SAFETY0.0 AND SAFETY1.0

The concept of safety has changed with the change of manufacturing sites, as seen in Figure 1. The initial concept is Safety0.0, in which ensuring safety solely relies on workers’ attention and judgment. However, it is not realistic to ensure safety under Safety0.0 alone because people are prone to make mistakes and machines fail.

Therefore, the concept of safety has changed to Safety1.0, in which safety was ensured by the design of machine systems. This is based on the principle of isolating and stopping machines, a principle of machinery safety in the industrial field. The fundamental idea of Safety1.0 is to design fail-safe and foolproof machinery in accordance with the requirements of various international safety standards for machinery, such as those of ISO and IEC. For example, under the principle of isolating machines, the operating areas of machines and those of people are determined and safety guards are installed to prevent people from approaching machines in operation. At the same time, under the principle of stopping machines, if people need to go inside the guards for system changeover or maintenance, the interlocks attached to the safety guards or other devices allow people to approach machines only when they are not in operation. Safety1.0 ensures safety by creating such machine systems.

However, in order to achieve more flexible and more productive operation, there has been increasing demand for a collaborative working area where machines and people share the same work space so that people and machines can work collaboratively with minimal downtime of machines. In this case, it becomes increasingly difficult to ensure safety through the conventional principle of isolating and stopping machines.

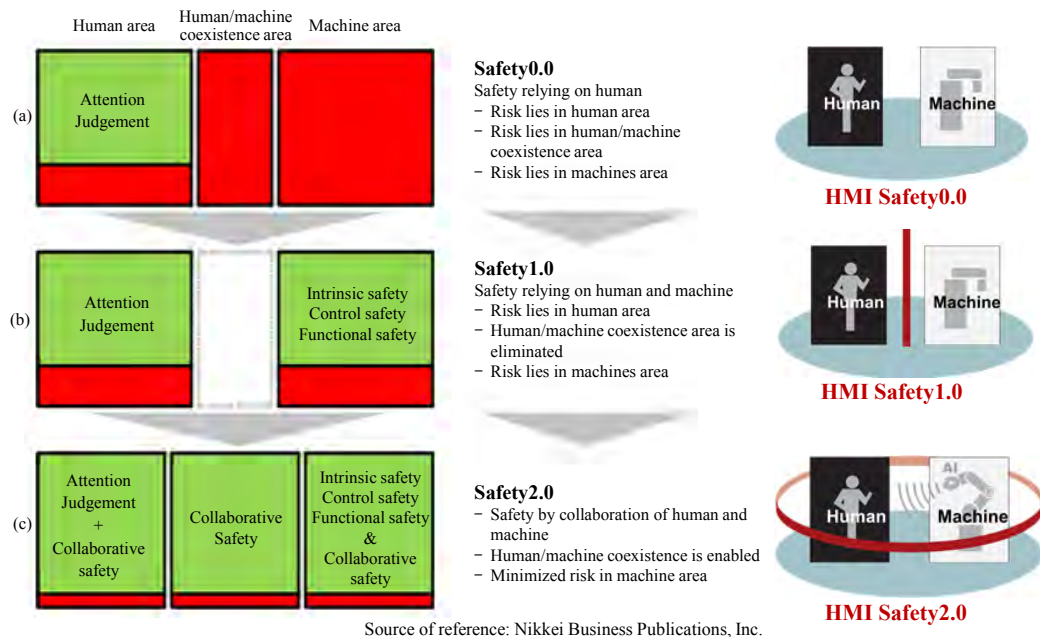


Figure 1. Safety evolution from Safety0.0, Safety1.0, and to Safety2.0.

3 THE IDEA OF SAFETY GOING FORWARD: SAFETY2.0

The collaborative robot system is one way for people and machines to work together as mentioned above. In order for people and collaborative robots to achieve both flexibility and high productivity in a collaborative work space while ensuring safety, human-robot collaborative safety is necessary in which people and robots are connected through information. Safety2.0, a new approach to realizing collaborative safety between people and machines at a higher level, is essential for the creation of the collaborative robot system, which is rapidly becoming widespread.

As shown in Figure 2, Safety2.0 promotes safety by connecting people, things (machines and robots), and the work environment through information to make them collaborate with one another. In other words, people control machines using their information, and machines prompt people to take action using their information. In this way, the work environment for people and machines will be optimized via ICT technology.

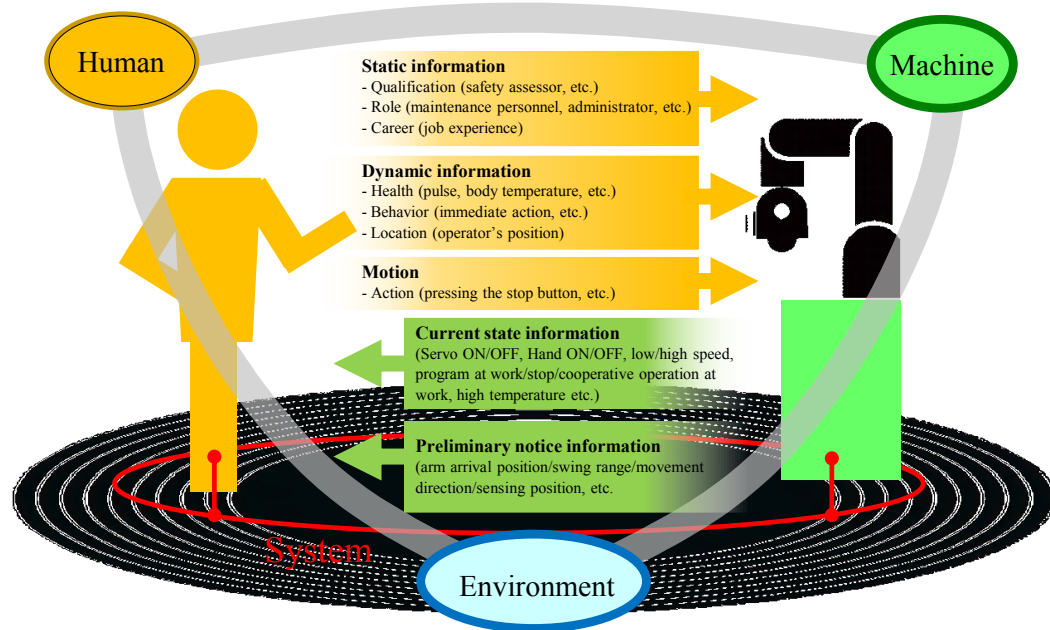


Figure 2. Collaborative safety by connecting human and machine.

Information on people includes: static information on safety assessor qualifications and other qualifications regarding machine safety, roles as maintenance workers and administrators, and workers' abilities with respect to safety based on their work experience; dynamic information on workers' location, their health including pulses and temperatures, and their prompt action; and motion information on the operation of buttons, etc. Inputting such information to machines enables the optimization of their speed control and other functions.

Motion information under Safety2.0 includes reactions that people exhibit when they are surprised. A method to quickly and easily convey such information to the machine is the use of an enabling device. The purpose of this paper is to discuss the future prospects of enabling devices, which are one of the key devices of Safety2.0. Before exploring the future prospects, the role of enabling devices under Safety1.0 will be reviewed.

4 THE ROLE OF ENABLING DEVICES UNDER SAFETY1.0

Under Safety1.0, safety was ensured through the principle of isolating and stopping machines, as discussed earlier. According to this principle, operation modes of machines are classified into two types. One is the "automatic operation" mode, under which machines run automatically, separated from workers, based on the principle of isolating machines. The other is the "human-attended operation" mode, under which people work near a machine that has been stopped for maintenance or process changeover purposes. This is based on the principle of stopping machines.

There are many situations in which people must operate machines manually even though the entire system is automated, as in the case of the industrial robot system. For example, system setup, teaching, process changeover, failure handling, repair, cleaning, and maintenance require that people work inside the hazardous areas. Figure 3 shows the flow of the use of an industrial robot. Under the automatic operation mode, the probability of an accident is usually low because people stay away from the machine with the principle of isolating machines. Under the human-attended operation mode, the risk does not become noticeably higher even for work inside the hazardous areas as long as the industrial robot is stopped based on the principle of stopping machines. Even so, under the human-attended operation mode, there should be situations in which industrial robots must keep operating. These situations include teaching, trial runs, and maintenance. The probability of an accident will drastically increase in such a case. In particular, machines could start unexpectedly when the automatic operation mode and the human-attended operation mode are being switched over. Operators could also make mistakes if they are losing concentration during teaching, which usually takes a long time. Extra attention must be paid in handling robots under such circumstances. For this reason, it is important to reduce the risks associated with the human-attended operation mode, as indicated by the arrows in Figure 3.

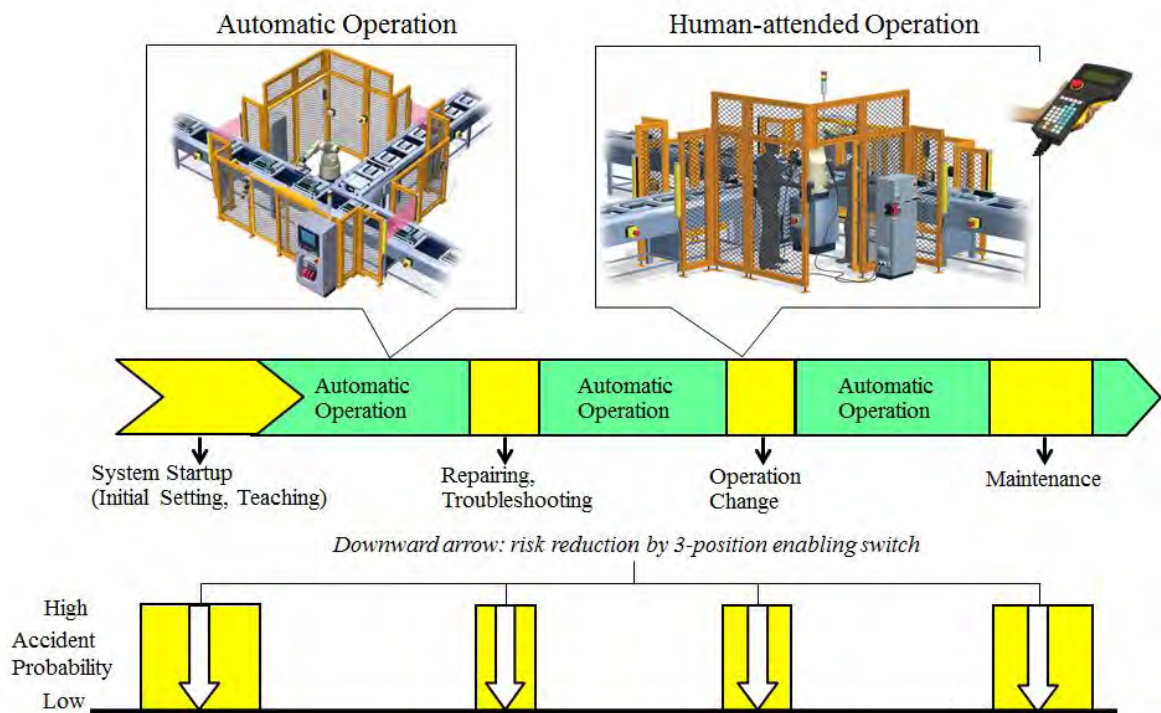


Figure 3. Comparison of accident probability in automatic operation mode and human-attended operation mode, and risk reduction by using 3-position enabling switch.

One effective method of ensuring safety in such a situation is the use of an enabling device with a built-in three-position enabling switch, as reported at past SIAS conferences. An enabling device is mainly installed in a teaching pendant used to teach industrial robots. As seen in Figure 4, the device sends the enabling signal to keep the machine operating only when a worker grips the device at the intermediate position. When the worker takes his/her hand off the device, or grips it harder, the permission is cancelled, and the machine stops operating. This is a safety mechanism designed to stop the operation of an industrial robot by cancelling the enabling signal with either movement of the worker’s hand. It is based on ergonomic features of unconscious reactions of workers who are surprised in the face of danger. In addition, the device is designed in such a unique way that once the worker cancels the enabling signal by gripping the device harder, the signal cannot be transmitted until the device is returned to its initial position (Position 1) and then gripped at the intermediate position again. This feature is to protect the worker from a potential danger of unexpected transmission of the enabling signal. This situation could arise if the worker feels relieved and loosens his/her grip after the machine stops following the enabling signal cancellation by the worker, who was surprised at the danger and gripped the device harder.

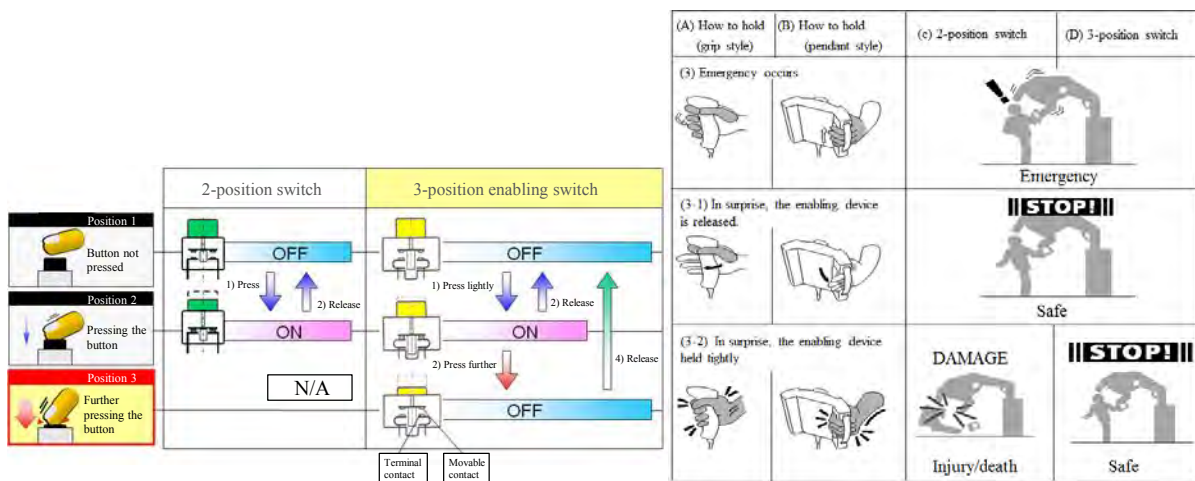


Figure 4. Operation modes of 2-position pushbutton and 3-position enabling switch; and operation comparison between 2- and 3-position enabling switches.

5 REQUIREMENTS FOR ENABLING DEVICES UNDER INTERNATIONAL STANDARDS

As described above, the use of enabling devices is a means of reducing the risk for people working near a hazard, such as industrial robots in a human-attended operation mode. Thus, the need for enabling devices is stated in various international standards as shown in Table 1 [11]-[16].

Table 1. Requirements of enabling switch/device specified in various international standards.

Standards	Description
ISO12100:2010 Safety of machinery - General principles for design - Risk assessment and risk reduction	6.2.11.9 Control mode for setting, teaching, process changeover, fault-finding, cleaning or maintenance b) permits operation of the hazardous elements only by continuous actuation of an enabling device, a two-hand control device or a hold-to-run control device,
IEC60204-1:2016 Safety of machinery - Electrical equipment of machines - Part 1: General requirements	10.9 Enabling control device Enabling control devices shall be selected and arranged so as to minimize the possibility of defeating. Enabling control devices shall be selected that have the following features: – designed in accordance with ergonomic principles; – for a three-position type: • position 1: off-function of the switch (actuator is not operated); • position 2: enabling function (actuator is operated in its mid position); • position 3: off-function (actuator is operated past its mid position); • when returning from position 3 to position 2, the enabling function is not activated. NOTE IEC 60947-5-8 specifies requirements for three-position enabling switches.
ISO 10218-1:2011 Robots and robotic devices - Safety requirements for industrial robots - Part 1: Robots	5.8.3 Enabling device The pendant or teaching control device shall have a three-position enabling device in accordance with IEC 60204-1. When continuously held in a centre-enabled position, the enabling device shall permit robot motion and any other hazards controlled by the robot.
ISO 10218-2:2011 Robots and robotic devices - Safety requirements for industrial robots - Part 2: Robot systems and integration	5.3.15 Enabling devices Pendant and additional enabling devices and their integration shall comply with ISO 10218-1. When more than one person is required to be protected within the safeguarded space, an enabling device shall be provided to each person.
IEC 60947-5-8:2006 Low-voltage switchgear and control gear - Part 5-8: Control circuit devices and switching elements - Three-position enabling switches	1.1 Scope These switches are used as components of enabling devices described in 10.9 of IEC 60204-1 to provide signals that, a) when activated, allow machine operation to be initiated by a separate start control, and b) when de-activated, i) initiate a stop function, and ii) prevent initiation of machine operation. NOTE 1 The enabling control function is described in 9.2.6.3 of IEC 60204-1.
ISO/TS 15066:2016 Robots and robotic devices - Collaborative robots	5.4.3 Stopping functions Examples of means to stop robot motion can include, but are not limited to: a) an enabling device; b) an emergency stop device; c) stopping the robot by hand, in the case of robots that include this feature. 5.5.3 Hand guiding 5.5.3.2.2 Guiding device The robot system shall be equipped with a guiding device that incorporates an emergency stop (ISO 10218-1:2011, 5.5.2 and 5.8.4) and an enabling device (ISO 10218-1:2011, 5.8.3), unless the enabling device exclusion requirements of 5.4.5 are met.

For example, ISO 12100, Subclause 6.2.11.9, which lists basic safety principles applicable to all kinds of machinery, stipulates that, with regard to the human-attended operation mode for “setting [or retooling], teaching, process changeover, fault-finding, cleaning or maintenance of machinery,” it “permits operation of the hazardous elements only by continuous actuation of an enabling device.”

IEC 60204-1, Subclause 10.9, an electrical safety standard, stipulates that enabling devices should be designed in accordance with ergonomic principles, and have three-position features.

ISO 10218-1, Subclause 5.8.3, a standard for industrial robots, requires that a three-position enabling device in accordance with IEC 60204-1 be installed on pendants or teaching control equipment.

ISO 10218-2, Subclause 5.3.15, safety requirements for industrial robot systems, requires the installation of an enabling device in accordance with ISO 10218-1. It also requires that when multiple persons work within the hazardous area, an enabling device is provided to each person, and that the work is allowed only when all people within the hazardous area grips the device.

In addition, ISO/TS 15066, Subclause 5.4.3, a technical specification for collaborative robots published in 2016, requires that these robots be equipped with a mechanism to allow people to stop their operations. The use of enabling devices is at the top of the list of such mechanisms. Furthermore, Subclause 5.5.3, a standard for hand-guiding equipment, also requires the installation of enabling devices.

Figure 5 shows the hand-guiding equipment newly presented by FANUC at AUTOMATICA, held in Germany in June 2018. The equipment features both safety and usability for workers. For example, (1) the hand-guiding equipment has three-position enabling device, required by ISO/TS 15066, Subclause 5.5.3., for the safety of workers. Further, enabling devices are installed at four locations and can be gripped anywhere on the circular handle. The nature of hand-guiding work is such that it is difficult to specify the location of the worker and the part of the hand-guiding equipment the worker should grip. For this reason, enabling devices are installed at four locations so that the worker can grip one from any location. It is particularly noteworthy that this hand-guiding equipment has a chucking/unchucking switch, which has its own three-position enabling device. It is inevitable that the risk level generally rises at a work transition point, whether or not the work involves chucking/unchucking operations. The three-position enabling device is installed on this hand-guiding equipment for the safety of workers at a transition point, in this case the transition point of chucking/unchucking.

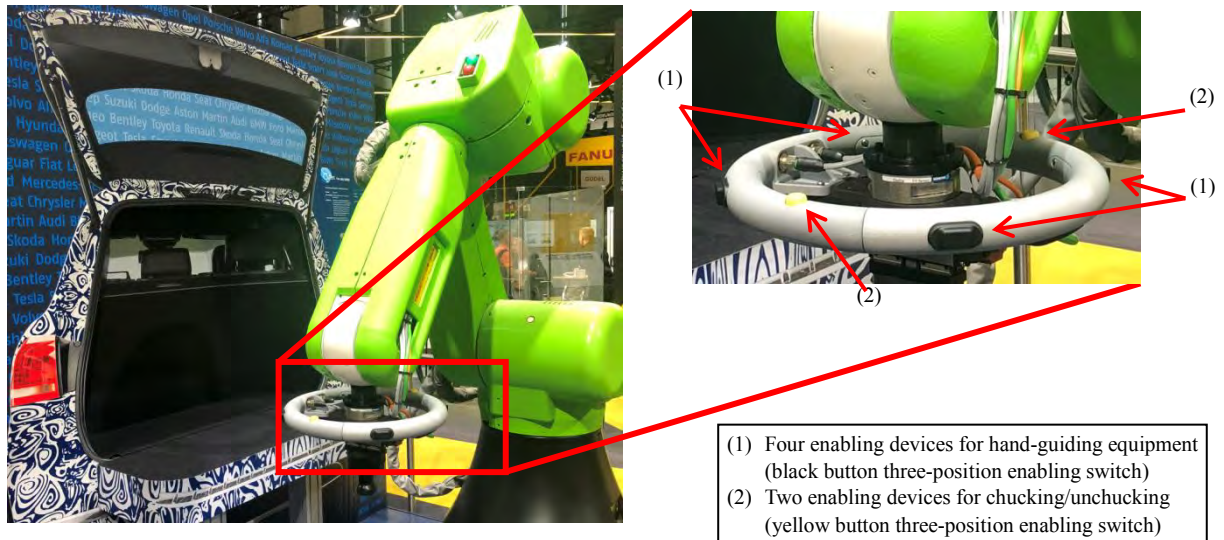


Figure 5. A hand-guiding equipment with three-position enabling devices at six locations.

6 CHANGES IN THE ENVIRONMENT AS SEEN FROM SALES TREND OF THREE-POSITION ENABLING SWITCHES

Since the first-ever three-position enabling switch was put on the market in 1997, we have been trying to raise awareness of the importance of enabling devices, presenting papers at the SIAS and other occasions. Efforts have also been made to make IEC 60947-5-8, an international standard for the three-position enabling switch. As a result, the enabling device has begun to gain recognition and widespread use as an essential safety mechanism, particularly at the time of teaching industrial robots.

In recent years, there have been some signs that “Industry 4.0” and “Connected Industries,” advocated by Germany and Japan, respectively, are about to gain widespread acceptance. Changes to the environment surrounding enabling devices are also being observed. In Figure 6, the striking change is shown by the trend comparison of sales volume of enabling devices and industrial robots over the past two decades.

Many users have adopted our enabling devices since they were released in 1997. An increase was seen in the number of enabling devices used worldwide following Phase 1, the introductory period, along with an increase in the worldwide usage of industrial robots. In recent years, a surprising development has occurred: the rate of increase in shipments of our enabling devices has outpaced that of shipments of industrial robots.

The reason behind the above trend is not just an expansion of the use of robots worldwide. There are signs that the collaborative robot system, which involves people and robots sharing the same work space, is about to become more prevalent. In addition, the trend must be associated with the fact that the number of manufacturing sites is increasing where the traditional principle of isolating and stopping machines is no longer applicable, representing Safety2.0, a new approach from Japan to safety under which people, machines, and robots collaborate with one another while ensuring safety and productivity at the same time.

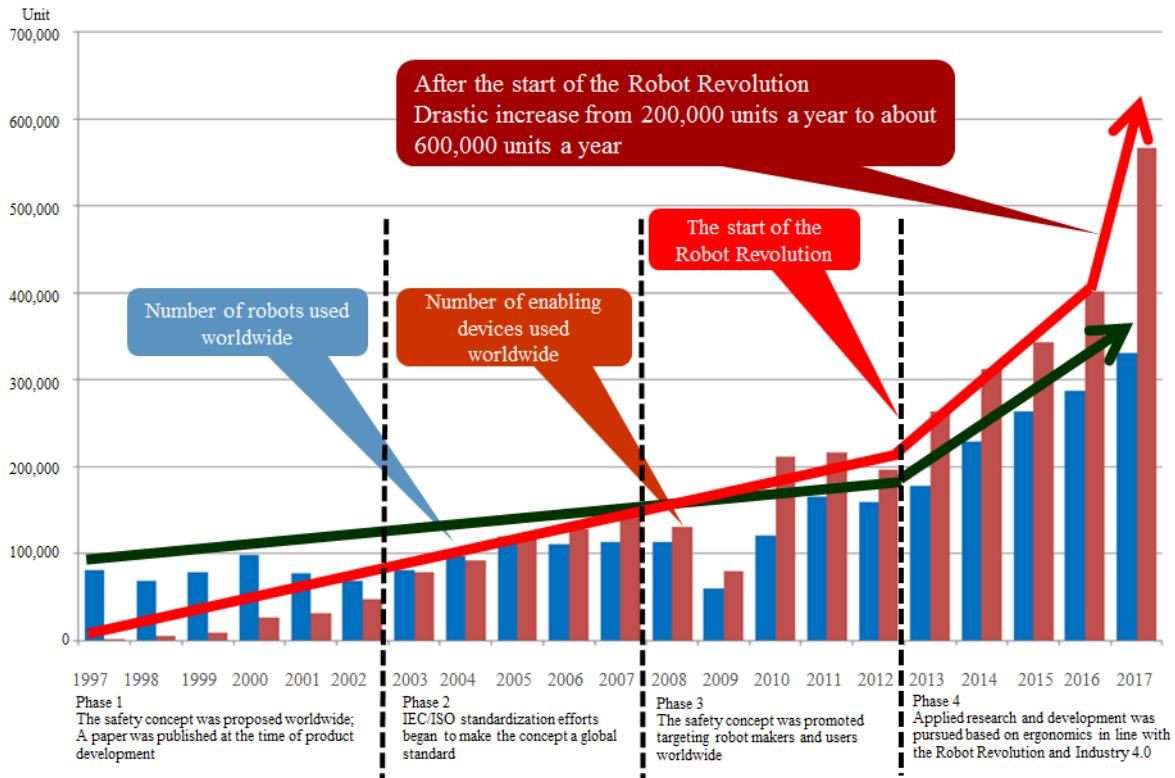


Figure 6. Trend of number of units used: IDEC enabling devices and worldwide industrial robots.

Safety2.0, as stated above, connects people, robots, and the work environment through information so that they can exchange such information, thereby allowing people and robots to work in cooperation to achieve safety. Under Safety2.0, enabling devices are now attracting attention as a means of communicating information about people to robots easily and quickly. In other words, there is no option than three-position enabling switches that can more optimally convey the unconscious response of a worker in danger.

7 FURTHER POTENTIAL FOR THE USAGE OF ENABLING DEVICES

ISO 12100, Subclause 6.2.11.9, stipulates the necessity and usefulness of enabling devices during the operation of hazardous elements of a machine in the human-attended operation mode, such as setting (or set-up), teaching, process changeover, fault-finding, cleaning or maintenance of machinery. However, an overwhelming majority of the enabling devices produced by us in the past were used for the teaching of industrial robots required under ISO 10218-1, -2.

Even so, increasing usage of enabling devices in recent years, as shown in Figure 7, may indicate that these devices are being used for purposes other than teaching. In addition, in terms of the potential of the devices to be used in wider applications, there is a recent development that should not be ignored, which is associated with the international standard IEC 60947-5-8 for three-position enabling switches. Although no official decisions have been made at this point, a planned revision to IEC 60947-5-8 is expected to include a series of additional figures, as shown in Figure 7, indicating potential expansion of uses other than teaching to the industrial robot systems. The additional uses may include hoist controllers, manual pulse generators, grip-type enabling devices for hand-held machines, foot actuated enabling devices, and joystick type enabling devices.

This revision is to be made due to the recognition that enabling devices, which have mainly been installed on teaching pendants, are useful and that their usefulness is also applicable to situations in which safety can be ensured by stopping the machine. Such situations are, as specified in ISO 12100, Subclause 6.2.11.9, setting (or retooling), process changeover, fault-finding, cleaning or maintenance of machinery. The features of enabling devices, in short, are as follows:

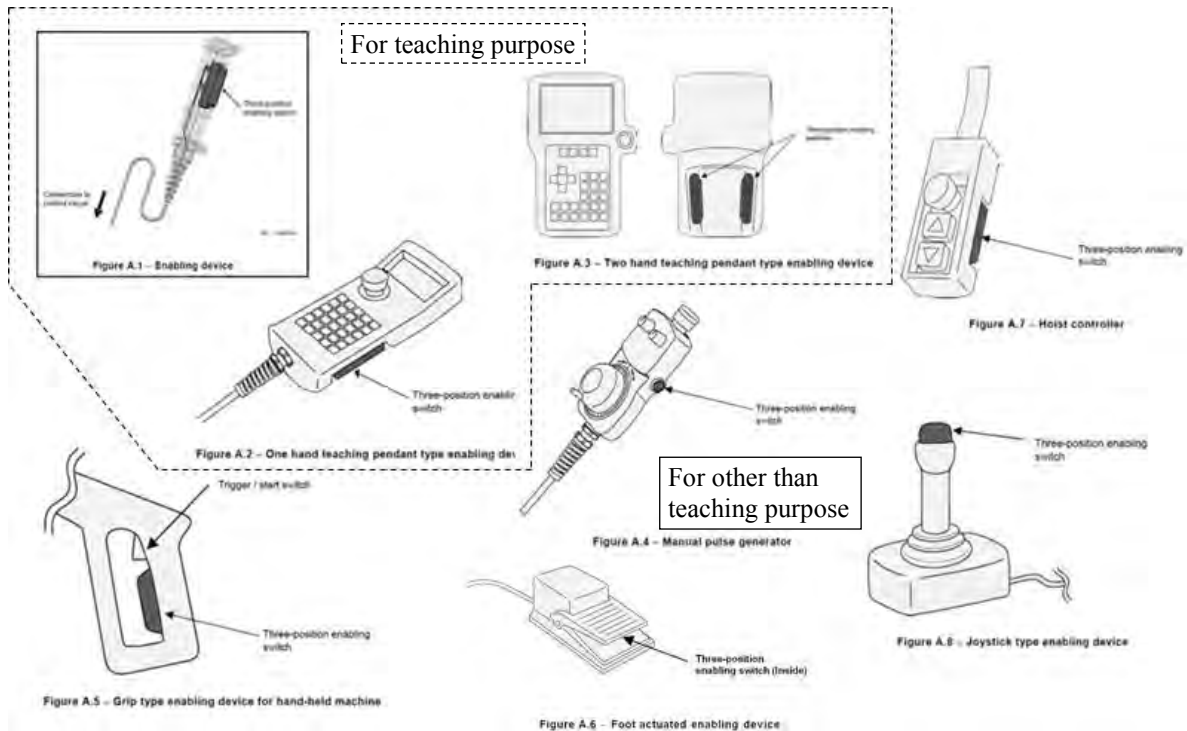


Figure 7. Application examples of 3-position enabling switch described in IEC60947-5-8 due to be revised.

Enabling devices

- Reduce the probability of the occurrence of hazardous incidents by quickly and easily communicating information on the unconscious response of people who feel danger to machines.
- Are easy to use (easy to install, easy to operate).
- Provide the user with a sense of being in control of the machine and a sense of safety.
- Are cheaper than light curtains or scanners.
- Allows the user to have only one free hand. This disadvantage, however, should be regarded as an advantage in that the user cannot approach the hazard for he/she needs to keep the other hand on the enabling device.

There are many cases in which these features of enabling devices may prove useful, in addition to the examples shown in Figure 7. Under Safety2.0, as well as Safety.1.0, enabling devices are expected to be developed even further as conventional yet new key devices for safety measures.

8 REFERENCES

1. Fukui T., Nobuhiro M., Matsumoto A., Fujita T., *Application of Three-Position Grip Switch for Inherent safety of Machinery*, International Conference on Safety of Industrial Automated Systems (SIAS), France, 2003.
2. Matsumoto A., Nobuhiro M., Fukui T., Fujita T., *Ergonomics and Usability of Pendant Terminals for Improved Safety*, International Conference on Safety of Industrial Automated Systems (SIAS), France, 2003.
3. Okada K., Maeda I., Sugano Y., Higuchi N., Nishihara I., Fujita T., *Risk Assessment of Robot Cell Production System That Achieved High Productivity and Safety in HMI Environment*, International Conference on Safety of Industrial Automated Systems (SIAS), Japan, 2007.
4. Mukaidono M., Takaoka H., Ogihara H., Ariyama M., Fujita T., *Japan's Approach for the Realization of Future Safety Concept by Implementing Collaborative Safety Technologies* (in press), 9th International Conference on Safety of Industrial Automated Systems (SIAS), France, 2018.
5. Dohi M., Okada K., Maeda I., Fujitani S., Fujita T., *Proposal of Collaboration Safety in a Coexistence Environment of Human and Robots*, 2018 IEEE International Conference on Robotics and Automation (ICRA), pp. 1924-1930, Australia, 2018.

6. Maeda I., Nobuhiro M., Shimizu T., Okada K., Dohi M., Fujitani S., Inada K., Fujita T., *New concept of safety to realize improvement of higher productivity and safety in an environment of human-robot collaboration, and proposal of the concept of Collaboration Safety Level*, International Symposium on Robotics, pp. 468-473, Germany, 2018.
7. Fujitani S., Okada K., Maeda I., Inada K., Dohi M., Fujita T., *New Interface concept for collaboration safety in a coexistence environment of human and robots*, Human Interface Symposium, p.669-674, Japan, 2017.
8. Fukui H., Shimizu T., Maeda I., Dohi M., Fujita T., *Collaboration safety system realizing compatibility between safety and productivity in human-machine coexistence environment*, Human Interface Symposium, pp. 533-538, Japan, 2018.
9. Nobuhiro M., Dohi M., Maeda I., Okada K., Fujita T., *The concept of Human-robot collaborative safety and 3-position enabling switches as key devices to achieve it*, IEICE Technical Report Vol.117 No.521, pp. 21-24 (SSS2017-36); The Institute of Electronics, Information and Communication Engineers, Safety, Japan, 2017.
10. Shimizu T., Okada K., Dohi M., Fujita T., *New concept for collaboration safety in a coexistence environment of human and machinery*, IEICE Technical Report Vol.117 No.365, pp. 21-24 (SSS2017-30); The Institute of Electronics, Information and Communication Engineers, Safety, Japan, 2017.
11. ISO 12100:2010, Safety of machinery – General principles for design – Risk assessment and risk reduction.
12. IEC 60204-1:2016, Safety of machinery – Electrical equipment of machines – Part 1: General requirement
13. IEC 60947-5-8:2006, Low-voltage switchgear and controlgear – Part 5-8: Control circuit devices and switching elements – Three-position enabling switches
14. ISO 10218-1: 2011, Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots.
15. ISO 10218-2:2011, Robots and robotic devices – Safety requirements for industrial robots – Part 2: Robot systems and integration.
16. ISO/TS 15066:2016, Robots and robotic devices – Collaborative robots.



Session 5

Safety of machinery

Challenges during risk assessment of large intelligent logistic storage system

Hongbin L.¹, Taiwei L.²

¹ TÜV SÜD Certification and Testing (China) Co., Ltd. - M Building - No. 7 Wangjing Zhonghuan Nanlu-
Chaoyang District - Beijing 100102- P.R. China

² TÜV SÜD Certification and Testing (China) Co., Ltd. - M Building- No. 7 Wangjing Zhonghuan Nanlu-
Chaoyang District - Beijing 100102- P.R. China

hongbin.liu@tuv-sud.cn

taiwei.li@tuv-sud.cn

KEYWORDS: Intelligent logistic system, risk assessment, explosion

ABSTRACT

The system is mainly consisted of rail guided vehicle (RGV), automatic warehouse (storage rack), automatic transportation system (chain conveyor and roller conveyor), stackers, pallet lifts, logistic control and management system. Considering its large and complicity, the whole system is divided into nine areas based on its function. For each area, every operation including foreseen maloperation is analysed combined with EN ISO 13849-1 and EN 62061 for control systems. After identifying safety function, based on the risk level matrix, determining related devices quantity and position which are summarized in safety interlock matrix, and then finish safety hardware architecture. Simultaneously, the materials in the storage system is liquid spice which is flammable, that means explosion safety also need to be considered. This paper examines the main hazards associated with the intelligent logistic system during the phases of its life cycle. Risk assessment is followed by risk reduction which summarizes the iterative process for eliminating hazards as far as possible and for implementing safety measures.

1 INTRODUCTION

In the globalized economy, rapid response for inconstant customer demands plays key role especially for e-business. The speed and accuracy movement of cargos is essential to the development of company, e.g. Alibaba, amazon. According to the statistics, on average, 1 billion packages need to be processed every day by Alibaba in China. Supporting the efficient packages transportation is the large intelligent logistic storage system.

The Intelligent Logistic System described in this paper is designed for a Switzerland company whose plant is located in China. Tough it is not located in EU; client want the safety comply with latest EU requirements. The system is mainly consisted of Logistic Storage System and Rail Guided Vehicle (RGV) System. Logistic Storage System includes automatic warehouse (storage rack), material automatic transportation system (chain conveyor and roller conveyor), stacker, pallet lift, logistic control & management system, etc. (Figure 1.)

The system is divided into the following areas for risk assessment.

- Area 1 automatic warehouse including total 4 stackers
- Area 2, buffer zone in front of the warehouse (mainly chain conveyors)
- Area 3, tunnel 1 area including RGV and conveyor
- Area 4, Loading, Debitage and unloading area
- Area 5, Tunnel 1 and Tunnel 2 transshipment area (mainly 2 pallet lift (2 floors), RGV and conveyors)
- Area 6, Tunnel 2 area located in the second floor, which is used for transferring load by RGV
- Area 7, Unpacking area in the first, second and third floor (mainly two pallet lifts, conveyors)
- Area 8, Independent pallet lift area (total three)
- Area 9, Mini loader area (total two mini stackers, storage rack, total nine load inlet and outlet)

Machinery safety starts always with risk assessment. The goal is to minimize the (remaining) risk to to a justifiable amount! Before risk assessment, we have to face many challenges.

First, the whole system is large and complicity and need high cooperation among systems (above areas mainly). Second, flammable liquid is storage in the warehouse and that means we shall consider the explosion protection measures during design.

Third, the risk assessment task involves the cross application of two independent technologies.

Risk assessment is an important tool both when designing a new machine or when assessing risks on used machines. A well thought-out risk assessment supports manufacturers/ users of machines to develop friendly safety

solutions. This minimizes the risk of the safety system being defeated. There is the following requirement in Machinery Directive 2006/42/EC:

“The manufacturer of machinery or his authorized representative must ensure that a risk assessment is carried out in order to determine the health and safety requirements which apply to the machinery. The machinery must then be designed and constructed taking into account the results of the risk assessment.”

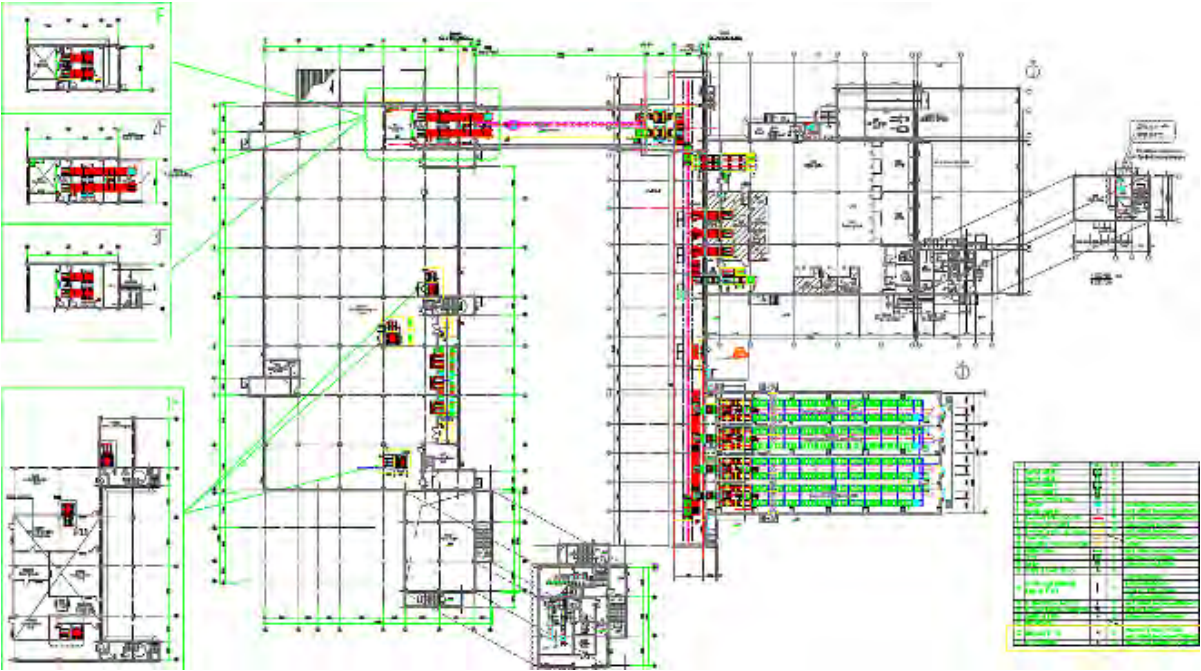


Figure 1. The whole system layout

Safety is a relative term in the directives and standards. In fact, it is impossible and not necessary to implement the so-called ‘zero risk guarantee’ where nothing can happen under operating conditions. This is why we permit residual risk exist. After the risk has been identified, a risk evaluation should be made as part of an iterative process to achieve the required safety level. In every step, we have to decide whether it is necessary and/or enough to reduce the risk. If it is to be further reduced, suitable protective measures shall be selected and applied. The evaluation must then be repeated. It is clear that the addition of protective measures as a means of risk reduction has the effect of reducing the ‘Probability of occurrence of that harm’ element of the risk. The degree to which risk is reduced is proportional to the probability of the protective measure performing its function. This ‘reliability’ of the safety function is the basis of functional safety (FS).

We should prioritize safety measures based on the below five steps. (Figure 2.)

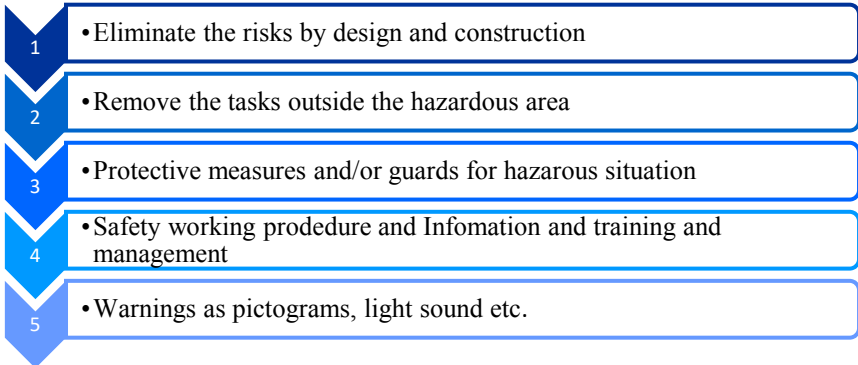


Figure 2. Five steps for risk reduction

It is important that all of the parts and components that involved in implementing the safety relevant function fulfills FS requirements. Based on our project experiences, always one or some components are not considered during design safety architecture especially those in “end circuit”.

2 RISK ESTIMATIONS

Mangy standards and/or regulations or other documentation describe the relationship between safety control level and the impact factors of Hazard Severity/Frequency/Probability/Avoidance Categories. Based on our lots of project experiences, and considering actual application that is not machinery solely, we reference some useful info in process safety fields and made below table 1. and table 2. for determine the final control level. The Table 2. is for general guidance and should not be used for conversion purposes. The full requirements of the respective standard shall be taken into account. New standard ISO/IEC 17305 will improve and merge the EN ISO 13849 and IEC 62061 in near future. * stands for use next control level in Table 2.

3 SAFETY CONTROL SYSTEM

3.1 General

For ensure control system reach required safety level, there are some factors given in related standards, e.g. EN ISO 13849-1, EN 62061 etc.

- Hardware architecture
- Components reliability
- DC
- CCF
- Processing

Before using FS standard, we should know which one is more appropriate for the control system. Their scope shall be clear in your mind. Refer to below Figure 3. Based on the actual control technologies, we used EN ISO 13849 and IEC 62061 for design the systems.

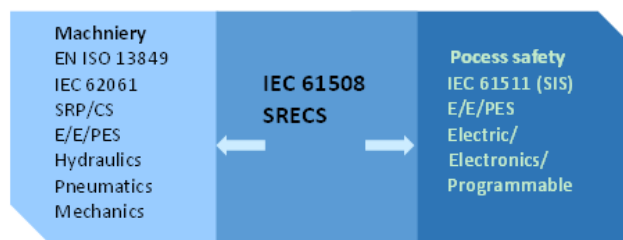


Figure 3. Scope of generic standards related to FS

The design of safety control system is planned acc. to Figure 4. procedure and in each step, documentation shall be prepared.

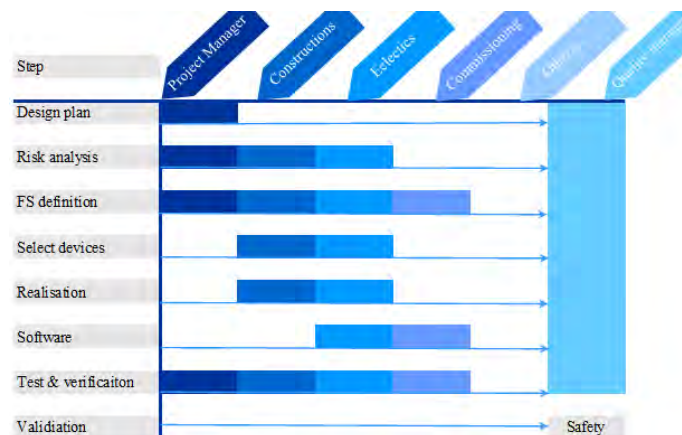


Figure 4. Design of safety control systems

3.2 Interlocking

Output devices monitoring

Safety control hardware architecture is category 3 acc. to standard definition. One point that usually is ignored by designer is output device monitoring, e.g main contactors, hydraulic valves etc.

For better diagnostics, output state reliable feedback is necessary and this is realized by using contactors provided "Mechanically Linked," positively guided contacts which are required in feedback circuits for safety applications.

Session 5 – Safety of machinery

During its whole life cycle, NC and NO contacts always are not closed simultaneously. For bigger rating devices, usual called “mirror contact”. In this system, client select AB 100S-F series contactors. Figure 5.

Avoid faults masking

Acc. to table 3. Interlocking matrix, more interlocking devices used and normally they are connected in series to safety input module. However, such design has an obvious disadvantage – faults masking. More interlocking devices used and more operating frequency, leads to higher faults masking and lower DC; even if end users perform regularly function check and/or maintenance every year, performance level can reach up to PLd and this is decided by safety management (human factor). (Figure 6. & Figure 7.)

Based on above reasons, and considering flammable liquid is stored in system, client select ABB Eden coded non-contact safety sensor which is self-checked more than one time by its electronics every second and it is easily reach up to PLe. And such design no need operator’s function checks in intervals.

Table 1. Hazard Severity/Frequency/Probability/Avoidance Classification

FACTOR	CATEGORY	CRITERIA
Severity (Se)	1 Moderate	Minor injuries with the possibility of time away from work (lost time accident). Reversible adverse health effects. Medical Treatment / Loss Time
	2 Major	Major injuries to personnel not resulting in fatality. Irreversible health effects -Full disability case or partial disability.
	3 Critical	Fatality on site (One to three deaths), Major Injuries on site >3 severe irreversible adverse health effects/ permanent damage /full disability cases / requiring extended periods of hospitalization. Life changing / Major Injuries off-site
	4 Catastrophic	Multiple Fatalities (>3) on-site fatalities or single off-site fatality. Major Injuries on ≥5 on site or cases off site major injury resulting in severe irreversible adverse health effects / permanent damage /full disability cases / requiring extended periods of hospitalization.
Frequency and duration of exposure (Fr)	2 If duration<10min, select above lower level.	>1year
	3	>2 weeks to ≤1 year
	4	>24h to ≤2 weeks
	5	>1h to ≤24h
	5 Any time	≤1h
Probability of occurrence of hazardous event (Pr)	1 Negligible 10 ⁻⁵ y	Unlikely to happen in the life time of the asset or facilities. Rare occurrences in similar facilities internal or external to the company.
	2 Rarely 10 ⁻⁴ y	Unlikely to happen in the life time of the asset. Some occurrences noted in similar facilities internal or external to the company.
	3 Possible 10 ⁻³ y	Slight possibility, similar events have occurred within the life of this asset, similar facilities internal or external to the company.
	4 Likely 10 ⁻² y	Similar event has occurred, or is likely to occur within the life of this asset.
	5 Very high 10 ⁻¹ y	Likely to occur once a year, or has probably happened in the last ten years
Probability of avoiding or limiting harm (Av)	1 Probable	– sudden, fast or slow speed of appearance of the hazardous event;
	3 Rarely	– spatial possibility to withdraw from the hazard;
	5 Impossible	– the nature of the component or system, i.e. electricity is dangerous by nature but not visible;

Table 2. Relationship among impact factors for safety control systems

--	Probability of harm	IEC 62601	EN ISO 13849-1 (EN 954-1)	EN ISO 13849-1	Risk level IEC 61508	Probability of dangerous failure EN ISO 13849-1	Maximum acceptable safety system failure
Se	Class Fr + Pr+ Av	SIL	Category	PL	RL	1/h	
1	--	--	B,2,3	a	I	≥ 10 ⁻⁵ to < 10 ⁻⁴	One risk failure every 10000 hours
	14-15	SIL 1	B,1,2,3	b	II	≥ 3x10 ⁻⁶ to < 10 ⁻⁵	One risk failure every 1250 days
2	11-13	SIL 1	B,1,2,3	b	II	≥ 3x10 ⁻⁶ to < 10 ⁻⁵	One risk failure every 115.74 years
	(14-15)*	SIL 1	1,2,3	c	II	≥ 10 ⁻⁶ to < 3x10 ⁻⁶	
3	8-10	SIL 1	1,2,3	c	II	≥ 10 ⁻⁶ to < 3x10 ⁻⁶	One risk failure every 115.74 years
	11-13 (14-15)*	SIL 2	2,3	d	III	≥ 10 ⁻⁷ to < 10 ⁻⁶	
4	3-10	SIL 2	2,3	d	III	≥ 10 ⁻⁷ to < 10 ⁻⁶	One risk failure every 1,157.41 years
	11-15	SIL 3	3,4	e	IV/V	≥ 10 ⁻⁸ to < 10 ⁻⁷	

Table 3. Some interlocking matrix (not list completely)

No.	Interlock	Number and position	PLr / SIL	Function	Reset/restore required	Compliant design
1	PILZ / PSENmag Safety interlocking door	4 located in right and 2 located in side Area 1	PLd/ SIL2	Monitor if there is a person in the laneway area.	Manual reset Yes	Yes
2	PILZ / PSENmag Safety interlocking door Area 1	1 Located in the maintenance passage	PLd/ SIL2	Monitor if there is person in passage. interlocked with stackers (STO)	Manual reset Yes	Yes
3	Leuze / MLC Safety light curtain Area 1	4 Located in emergency escape way	PLd/ SIL2	Monitor if there is person enter adjacent laneway through escape way. Interlocked with stackers (STO)	Manual reset Yes	Yes
4	TURCK / B15-M18-Y1X-H1141 Safety pin monitor	1 Each platform Area 4,7,8	PLd/ SIL2	Monitor if the safety pin insert or not when maintenance, also monitor if it is pulled out after maintenance	No	Yes
5	Leuze/ MLC Safety light curtain Area 2,4,9	2 Located in loading & unloading opening	PLd/ SIL2	Monitor if there is person enter tunnel 1 area through opening, interlocked with STO (RGV)	Manual reset Yes	Yes



Figure 5. AB 100S-F series main contactors

Number of frequently used movable guards ^{a) b)}	Number of additional movable guards ^{c)}	Fault masking probability Level (FM)	Protected multicore cable with or without positive (+U) voltage wire					
			position switch arrangement	cabling	Signal evaluation of redundant channels with	Maximum achievable DC		
						FM=3	FM=2	FM=1
0	2 to 4	1	redundant arrangement	Branch/Star	same polarity (+U / +U)	medium	medium	medium
	5 to 30	2			inverse polarity (+U / GND)	none	low	medium
	> 30	3		dynamic signals	medium	medium	medium	
1	1	1		Loop	same polarity (+U / +U)	medium	medium	medium
	2 to 4	2			inverse polarity (-U / GND)	none	low	medium
	≥ 5	3			dynamic signals	medium	medium	medium
> 1	≥ 0	3						

Figure 6. Estimation of the fault masking probability & Max. achievable DC

Safety software

Failures of software are inherently systematic in nature. Failures are caused by the way it is conceived, written or compiled. So, software failures are mainly caused by system under which it is produced, not by application. However, we do not need to go into details inside the software architecture, e.g. classic V model. In actual application, most programmable safety devices are provided with “certified” function blocks or routines. This simplifies the validation task for designer and/or end user, but it shall be noticed that the completed application program still needs to be validated. The used safety blocks and their link and parameterized also shall be proved correct and valid for the intended task. Siemens S7-1500 CPU 1511F-1PN and ET200SP input/output safety modules are used in this system. Acc. to SIMATIC Configuring and Programming Manual, we prepare below table.4 for verify final application of software.

Table 4. check list for safety program

No	Main checklist for safety software
1	Hardware Configuration (F-I/O, CPU, addresses) ; Safety-related parameters of all configured F-I/O
2	Collective signature (F block & Safety program)
3	Utilized elements of the internal system libraries (from "Instructions" and F blocks) along with ver.
4	Information about the F-runtime groups (F-monitoring time, F-monitoring time warning limit, F-blocks and names)
5	Safety relevant communication (instructions, addresses, calling block and calling F-runtime G)
6	Absolute addresses and names of the F-shared DB tags that can be accessed from the standard program
7	safety function is all realized by calling for standard FB? Is there block related to safety which is programmed by user?
8	Consistency of the safety program
9	Completeness of the safety program
10	Compliance of F-Block (name, function, associated F-runtime group, signature) with the NB certificate
11	Correctness of the communication configuration
12	Validity check for data transfer from standard to the safety program
13	Related Safety Function Test

Safety control level requires calculations. To do this in a manageable way a software tool provides excellent help. We choose to use SISTEMA, a software tool developed by BGIA, now called IFA. With SISTEMA it is possible to “build” safety functions, verify them and generate the technical documentation required.

4 EXPLOSION RISK

The whole system is designed acc. to GB explosion protection standards which is mandatory by government. All electrical equipment is selected and installed based on GB 3836 series (equivalent IEC 60079 series). As basic, firstly, we, manufacturer and end users have brainstorm meeting for ignition sources assessment which is important for using which Ex protection /prevention technology later. We focus on the mechanical moving parts and static discharging. In such storage system, many moving parts in inside it, e.g guided wheels on the rail. To avoid mechanical sparks when emergency stop or braking, the contact materials have to be analyzed. During design, manufacturer want to use beryllium bronze materials, but after running for one month on test samples, it was found worn seriously and not satisfy end user’s requirements. After more analysis, measurement and test, finally we select polyurethane in which manufacturer adds antistatic materials and special agent to ensure its strength performance simultaneously. (Figure 7.)



Figure 7. Polyurethane wheels on RGV

Usually, if material surface resistance is less than $10^9\Omega$, it is considered can avoid static discharging in normal operation conditions. After we receive test sample, its measured resistance is about $580M\Omega$ and end user accepts this value in their classified zone 2. After many tech communications with manufacturer and end user (operator, maintenance persons, plant manager), the system using, operating and procedure shall be familiar in mind. All potential ignition sources in GB 25285.1 (equivalent EN 1127-1) were assessed in risk assessment report.

5 SUMMARY

In the past, we focus on productivity/ efficiency and disregard safety. This leads to increased injury and risks. Today most of manufacturer and end users considered safety as important as productivity. We use safety related devices and implement the directives & standards, and adopt better diagnostics. In near future, obviously, integrated and intelligent safety controlling systems will be used especially in Industry 4.0. More advanced control algorithm and sensors will be widely used in robot, AGV/RGV or other automatic equipment. Safety devices will be configurable and programmable with safety network. In general, future safety will be transparent for designer and user.

6 REFERENCES

1. 2006/42/EC THE European PARLIAMENT AND THE COUNCIL ON Machinery directive.
2. EN ISO 12100:2010 Safety of machinery — General principles for design — Risk assessment and risk reduction (ISO 12100:2010).
3. EN ISO 13849-1:2015 Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design (ISO 13849-1:2015).
4. EN 62061:2005 Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems IEC 62061:2005.
5. www.fortressinterlocks.com
6. ISO/TR 24119 Safety of machinery — Evaluation of fault masking serial connection of interlocking devices associated with guards with potential free contacts.
7. SIMATIC Industrial Software – Configuring and Programming manual 03/2007.
8. Siemens Safety Integrated - Navigating Standards for Safety-Related Parts of Control Systems.
9. 2014/34/EU the European parliament and the council on the approximation of the laws of the Member states concerning equipment and protective system intended for use in potentially explosive atmosphere.
10. EN 1127-1:2011 Explosive atmospheres — Explosion prevention and protection Part 1: Basic concepts and methodology.
11. EN 13463-1:2009 Non-electrical equipment for use in potentially explosive atmospheres Part 1: Basic method and requirements.
12. CLC/TR 50404:2003 Electrostatics- Code of practice for the avoidance of hazards due to static electricity.
13. IEC 61882:2016 Hazard and operability studies (HAZOP studies) - Application guide.

Impact of changes in machinery during use: towards a prognostic of hazardous situations?

Lamy P., Perrin N.

Institut national de recherche et de sécurité (INRS) – 1, rue du Morvan – CS 60027 – 54519 Vandoeuvre Cedex
– France

pascal.lamy@inrs.fr

nellie.perrin@inrs.fr

KEYWORDS: violation, detection, ergonomic approach, machines

ABSTRACT

Disturbing events when using a machine or an automated system in operation, such as the jamming of a part or the clogging of raw materials, can disturb the normal production process. To offset the effects of these dysfunctions, and often in order to catch up with production, the operator can intervene and place themselves in a hazardous situation.

We intend to see whether it is possible to prevent such hazardous situations, anticipate them and perform a prognostic. We propose an approach based on the activity observation method which allows identifying links between disturbing production events, the responses of the operator following these disturbing events and the associated risks. The approach, composed of four steps, uses expertise to determine hazard scenarios following disturbing events and to analyze the risks. This approach was applied to an industrial case to verify its feasibility. In view to automating and prognosing the occurrence of such dysfunctional situations, we explain the perspectives considered: the identification of disturbing events by modeling the work situation, including the interactions between the operator and the machines, a dysfunction analysis and the definition of the monitoring to be implemented. This monitoring will use production data.

1 INTRODUCTION

One of the causes of accidents to operators of machines or automated installations is the bypassing of protection devices. This subject was raised during previous SIAS congresses. In 2005, Charpentier [1] showed that for 457 accidents with automated installations, 30% were due to bypassed protection systems. At the SIAS of 2010, Apfeld [2] showed that 37% of protection devices installed on metalworking machines were also bypassed. Likewise, Shaw [3] mentioned the bypassing of protection systems as one of the causes leading to accidents. In his article of 2015, Chinniah [4] demonstrated that out of 106 accidents, 14 were linked to the raising of physical protection devices or by bypassing safety equipment.

When a machine or production system is in service, everything is done to ensure that the quality of fabrication is as good as possible. Nonetheless, the operating situation (thermal ambiance, hygrometry, etc.), the equipment and the product's characteristics tend to drift (ageing, deterioration of raw material quality, etc.). Disturbing events such as the jamming of parts can then occur. If recurrent, this disturbing event becomes a disturbance liable to change the normal use of the equipment. Confronted by this situation, the operator adapts by establishing a strategy in response (physical action). For example, if the production system is blocked, the operator will often use the system in a way different from that for which it was designed (instructions) to guarantee production. This response can lead the operator to violate the rules and place themselves in a hazardous situation (Figure 1).

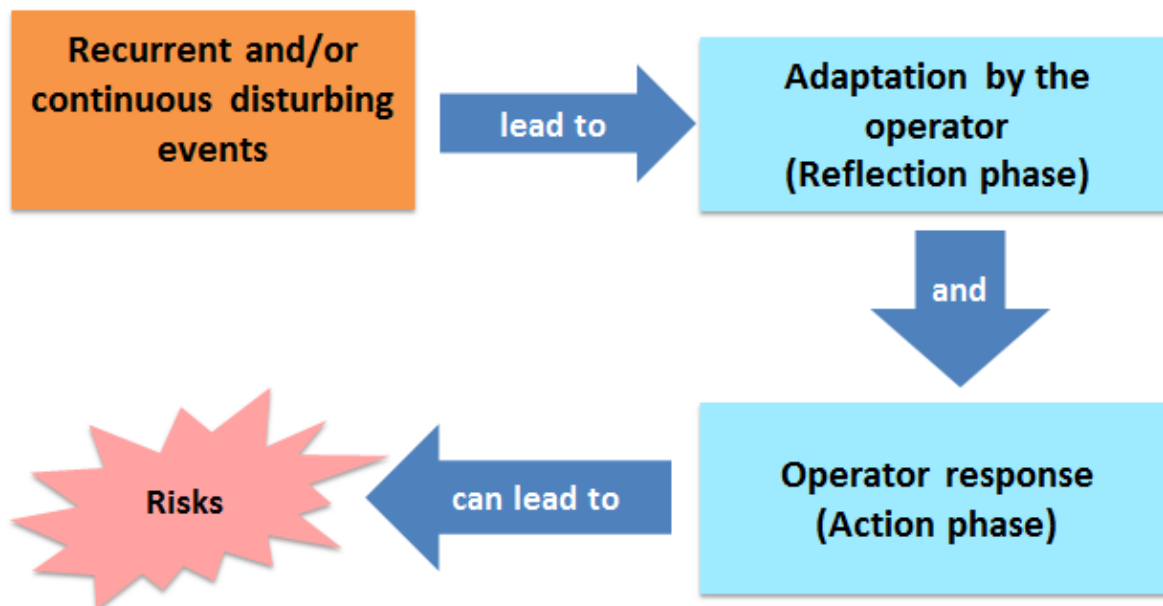


Figure 1. Consequences of disturbing production events.

There are different types of disturbing events. For example:

- a need, not originally foreseen, to observe in detail the work done by the machine;
- a need to offset poor visibility of the fabrication process (for example a transparent protection that becomes opaque). For example, on a numerically controlled machine, these needs can result in working with the “protection open” and thus bypassing the protection device;
- a need, not originally foreseen, to diagnose or correct the non-conformity of a part, making it necessary for the operator to intervene on the machine. The operator’s response could be, for example, to bypass the protection device to take a sample during production or to use a non-adapted operating mode (such as the setting mode);
- recurrent problems of clogging or jammed parts, leading to interventions with the safe mode disabled or with a non-adapted mode;
- the use of the setting mode during standard production phases. The operator (unqualified for this mode) may use it deliberately or not following a maintenance action, for example (troubleshooting, tool-changing).

An analysis [5] performed using the work accident database EPICEA¹, on specific types of machine (press brake, die-stamping press), confirmed these findings. It showed that out of 364 accidents involving these types of machine, at least 12% were related to the operator’s response following a disturbing event, leading them to place themselves in a hazardous situation. This value is a minimum since in this database, the descriptions of the accidents do not always allow determining the specific causes of the accident.

Based on this observation, we wanted to see whether it was possible to identify such hazardous situations resulting from disturbing events in order to predict them. Therefore, we sought to know whether it was possible to use an approach based on the observation of a work situation to identify disturbing events.

2 IDENTIFICATION OF DISTURBING EVENTS THROUGH THE ERGONOMIC OBSERVATION OF THE WORK SITUATION AND THEIR IMPACTS

2.1 Presentation of the approach

We formulated an approach based on the activity observation method resulting from the ergonomic analysis of work. An observation grid was drawn up depending on the specific characteristics of the work situation to take into account the interactions of the operator with their environment. The observation focused on the operator and

¹ EPICEA is a French national, anonymous database containing more than 23,000 cases of occupational accidents sustained by employees covered by the general social security system. These accidents are fatal, serious or significant to prevention. The EPICEA database is not exhaustive since not all occupational accidents are listed on it. Its aim is to reveal the causes and sequence of events underlying accidents of a given type. A simplified version can be consulted on-line at <http://www.inrs.fr/publications/bdd/epicea.html>.

their movements. In particular, this grid contains a functional description of the work situation and allows collecting exploitable data: operator actions, information gathering, communications and movements. Formalization was achieved by observing the real activity and by searching the operators' instructions. We then presented these observations to different actors in the company. This approach was formulated by following an iterative process including field observations and exchanges between machine safety experts.

The observation was conducted from a dual perspective: technical and ergonomic to observe technical disturbing events and the operator's responses to them, to take into account the technical aspects and the man-machine interactions involved. In the first step, the data from the documentation and those resulting from the observations allowed formalizing the work situation by distinguishing the prescribed activity from the real activity. In the second step, the observations focused on the production disturbing events and the operators' responses. Two examples are presented:

- a disturbing event is observed to which the operator responds,
- a non-prescribed response is observed but not the disturbing event. In this case, the cause must be sought to detect the disturbing event.

The observations were performed over a relatively short period (1 to 2 observations per week for 5-6 weeks) so as not to produce a bias linked to the modification of the work post.

The third step of the approach focused on the production of hazard scenarios following the observations collected during the first two steps. Finally, the last step consisted in analyzing and evaluating the risks.

2.2 Feasibility for an industrial case

We observed an installation composed of a number of machines: an oil pump assembly line (automobile sector). This line is composed of several islands in which assembly operations are performed: for example, screwing, positioning parts, the automatic control of the finished product. An operator is responsible for supervising this line and positioning several parts on a base at the entry of the line. The base is used to convey the manufactured product along the whole production line. In operation, this line gives rise to a large number of micro-stops (30s to 6 min.) as well as longer stops. Thus, the operator is responsible for carrying out the initial interventions in the case of dysfunctions and is thus competent for intervening on all the islands.

The observation highlighted the disturbing events. An example of a disturbing event is the falling of the parts composing the pump onto the floor. In this example, the pumps arrived without covers at the entrance of this zone (normally, all the pumps must be covered by a cover which is screwed on upstream on the line). As the robot does not detect the absence of a cover, it continues its cycle and returns the pump during the movement instead of positioning it on the defective pump conveyor. By turning the pump, the parts fall to the floor in the robotized zone.

The instructions say that the parts must be picked up during the weekly cleaning and occasionally during production stoppages. The hazard scenario established is that if the situation deteriorates and that more and more parts fall onto the floor, the operator would be led to pick up parts more often and even tempted to do so while the production line is in operation. The analysis of the risks (Figure 2) consecutive to this hazard scenario highlighted MSD (MusculoSkeletal Disorders) risks linked to posture and the duration of exposure, and PSR (PsychoSocial Risks) linked to the stress generated by the loss of time and the impact on production. One possible non-prescribed response is to take the pump without its cover on the conveyor. The analysis of the risks following this scenario did not show any mechanical dangers for the operator given the low energy used by the conveyor, but this analysis should be performed again if the shape of the part conveyed or the energy used to move the conveyor should change.

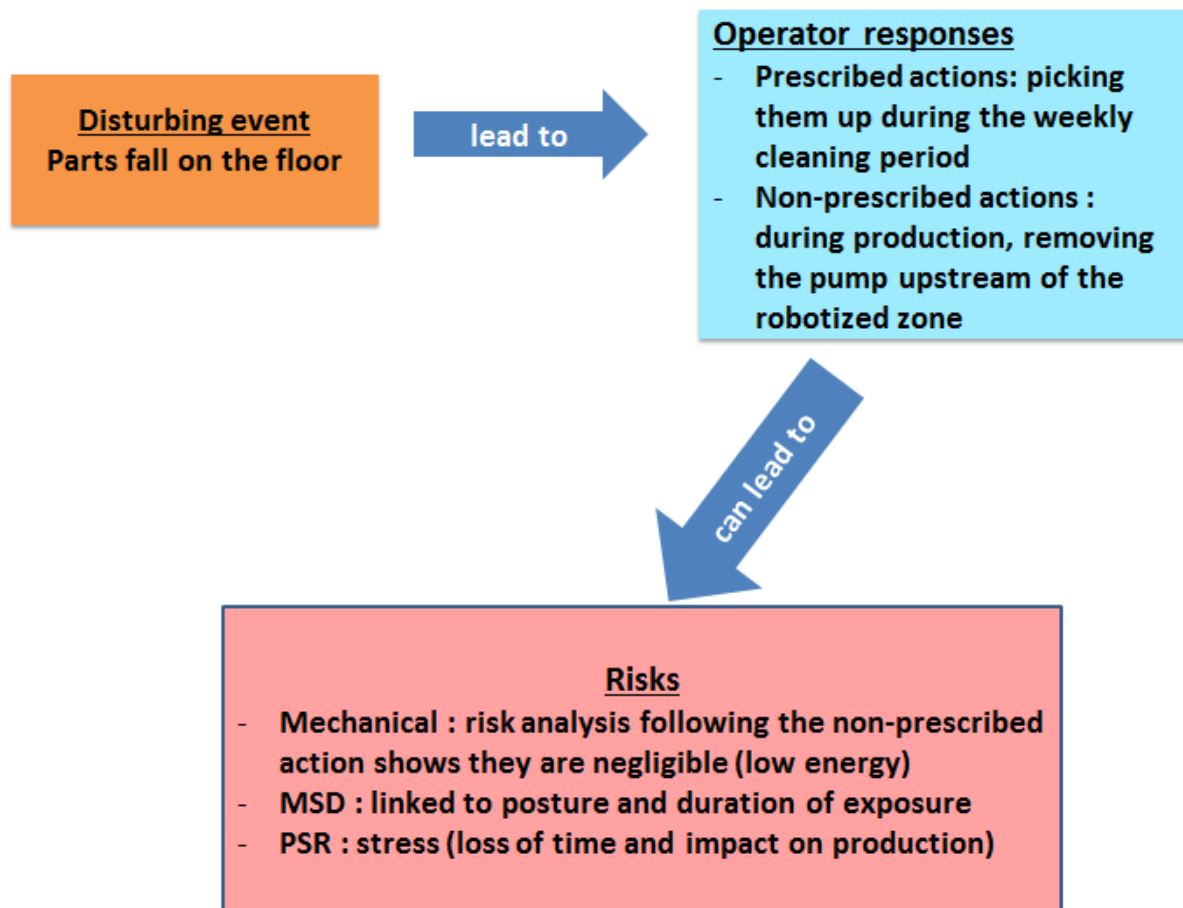


Figure 2. Disturbing event, responses and risk resulting from the case analyzed.

In conclusion, in such situations, with repeated disturbing events liable to cause the operator to react in order to maintain production rates, they could be tempted to bypass the protection device and enter the zone during production.

To avoid these hazardous situations, we sought to determine whether it is possible to prognose hazardous situations on the basis of pertinent indicators such as recurrent production disturbing events and the possible bypassing of protection devices:

- a bypassed mobile protection device, whose opened/closed information is therefore inhibited; a drift from the expected (prescribed) scenario;
- the frequency of opening the protection device is higher or lower than that planned, for example, in the case of manual loading in which the protection device must be opened at each cycle;
- running the machine more frequent than planned in setting mode. This may reveal a dysfunction (problem of quality of the finished product or during its fabrication) liable to lead the operator to eventually bypass the protection device.

By analogy, recurrent disturbing events and possible bypassing correspond to weak signals [6], defined as a group of items, facts, anomalies and dysfunctions which, taken singly, do not necessarily have an impact on the safety performances of the system in question but whose recurrences, accumulations and positioning may lead to more serious incidents.

3 PERSPECTIVE: TOWARDS A PROGNOSTIC OF HAZARDOUS SITUATIONS?

The aim is to formalize an approach based on the technical “drifts” of the system in view to determining, on the basis of these drifts, if the operator is liable to find themselves in a hazardous situation. This is done by using data stemming from production.

To identify these drifts, we propose to monitor the different technical elements of the system (the machine, the product, the environment) and their interactions. The operator is examined only through their interactions with these elements. These could be their positioning in relation to the machine, the activation of the protection device (or more generally the monitoring of barriers in the meaning given by Polet [7]) or their action via the MMI.

With this monitoring approach we want to show the feasibility of finding precursor indications linked to the drifts of the system that potentially lead to hazardous situations. The approach requires:

- identifying the drifts of the system and the responses associated with the operator;
- determining the pertinent properties of the system that have to be monitored;
- analyzing the system data that can be examined dynamically in real-time and determining whether it is possible to predict this hazardous situation by defining the relevant indicators making it possible to recognize that a particular situation is becoming hazardous.

We limit this approach to the case of an assembly system type installation.

To achieve this, we consider the three-step approach presented below and in Figure 3.

3.1 Modeling the work situation and interactions

To start, we consider modeling the work situation by taking into account the interactions between the machine, the operator and the product within this work situation, and the possible impact of the physical environment capable, for example, of influencing the production process. The modeling considered is performed from a dual perspective: static and dynamic. A reference model of work situations, composed of several “trade” models is formulated. This model will contain the knowhow required to describe any specific case of work situation in normal operating conditions.

3.2 Dysfunctional study and identification of situations to be monitored

On the basis of the reference work situation model done in the previous step, we intend to complete this approach with a dysfunctional analysis of the work situation. To do this, we aim to work on a dysfunctional approach to interactions combined with more classical approaches focused on machines (for example, FMECA) and flows (for example, HAZOP). On this basis, it will be necessary to continue by identifying hazardous situations using dysfunctional situations. This approach must incorporate existing procedures pertinent to the goal desired. This is done by implementing a novel method, i.e. the dysfunctional analysis of interactions. This approach is intended to study and characterize all the events leading to a dysfunction and the causal relations between these dysfunctions.

Regarding these two parts, we consider proceeding by abductive reasoning (which mixes induction and deduction): this entails analyzing two real cases, generalizing them on this basis and developing contributions to modeling and dysfunctional analysis, taking into account existing scientific knowledge. These contributions will then be reapplied to another case to validate their pertinence.

On the basis of the dysfunctional analysis and by using expert judgement of risk analysis, we consider deducing and characterizing those of the dysfunctional situations that are hazardous and result from the possible responses of the operator outside the actions prescribed. It will be necessary to list and rank the hazardous situations, notably as a function of indications of frequency linked to initiating events such as technical failures, drifts in interactions and drifts in the product’s characteristics. It will also be necessary to find the most pertinent initiating events to monitor. This approach will then be applied to a third case to evaluate its credibility.

3.3 Monitoring hazardous situations

To terminate and move towards automating the approach, we wish to implement the operational monitoring of the hazardous work situations identified previously. We will use the third case of application and, on the basis of ranking the hazardous situations, it will be necessary to:

- define the monitoring resources to implement; choose the instrument technology, choose the variables to monitor and the frequency of analyses. This entails providing a set of indicator values or statuses of situations for the employee at the work post;
- propose a set of treatments for these indicators to provide pertinent elements for aiding decision.

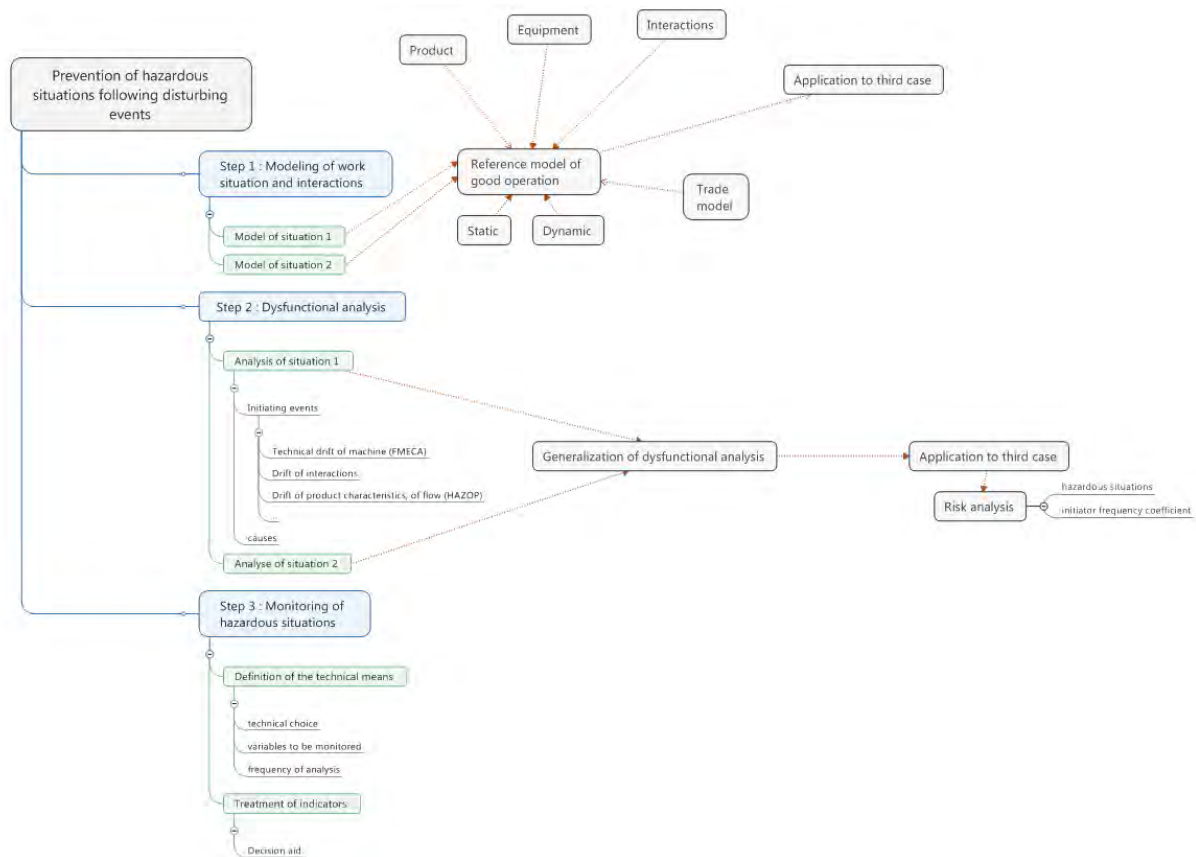


Figure 3. The approach considered.

4 REFERENCES

1. Charpentier P., *Safety of machinery: experience feedback on automated accidents from the EPICEA database*, Proc. of the 4th International Conference on Safety of Industrial Automated Systems, Chicago, US SIAS 2005
2. Apfeld R., *Stop defeating the safeguards of a machine*, Proc. of the 6th International Conference of the Safety of Industrial Automated Systems, Tempere, Finland, 2010
3. Shaw S., *Machinery accidents-contributory factors*, Proc. of the 6th International Conference of the Safety of Industrial Automated Systems, Tempere, Finland, 2010
4. Chinniah Y., *Analysis and prevention of serious and fatal accidents related to moving parts of machinery*. Safety Science, 75 (2015), pp. 163-173.
5. Lamy P., Tissot C., *Analyse de récits d'accidents du travail pour identifier des situations de dérives d'usage et apport des outils de Traitement Automatique de Langues*, Proc. of the 20^{ème} congrès λμ, Saint-Malo, France, 2016.
6. Bringaud V., Verges P., *Concevoir et déployer une démarche signaux faibles sur un site nucléaire de production*. Proc. of the 16^{ème} congrès λμ, Avignon, France, 2008.
7. Polet P., *Modélisation des franchissements de barrières pour l'analyse des risques des systèmes Homme-Machine*. Thèse de l'Université de Valenciennes et Hainaut-Cambrésis, 2002, 192 p.

A study on safety requirements for brake systems of the mechanical servo presses

Hata Y.¹, Saito T.²

¹ Japan Forming Machinery Association (JFMA) – Kikaishinko Bldg. 3-5-8 Shibakoen, Minato-ku, Tokyo - 105-0011 – Japan

² National Institute of Occupational Safety and Health, Japan (JNIOOSH) – 1-4-6 Umezono, Kiyose, Tokyo - 204-0024 – Japan

uhh03796@nifty.com
saitot@s.jniosh.johas.go.jp

KEYWORDS: press machine, servo press, brake system, stopping performance

ABSTRACT

Establishment of the international safety standard ISO 16092-2 of the mechanical power press machine (or mechanical press) is progressing. In the conventional mechanical presses, for the start and stop functions of the presses, the clutch and brake system operated by air or hydraulic valves is utilized and the safety-related control system is established as the system to control these valves. However, unlike the mechanical press, various stop control mechanisms are adopted in the mechanical servo press (or servo press) which began to spread since around A.D.2000. Although the start control mechanisms of the servo press are realized by mechanical connection to the servo motor directly or through a belt, the stop control mechanisms of the servo press are provided as combinations of mechanical brake(s) and a stop control system of servo motor. And the various types of mechanical brake such as those which use air or hydraulic valves or electromagnetic brakes are adopted in addition to the servo drive control to stop the servo motor.

For this reason, the safety requirements for each stop control mechanism of the servo press are also various in each country, and therefore, it becomes a problem that the common validity of each requirement is not clearly shown. The purposes of this paper are to classify various stop control mechanisms of the servo presses which are composed of the different servo motor control and the different mechanical brakes and to clarify the risk generated by each stop control mechanism. Furthermore, common safety requirements for the stop control mechanisms to be used as effective risk reduction measures and to maintain their stopping performances are described. Common validity check requirements are also discussed.

The results of the above considerations will be expected to contribute to the establishment of ISO16092-2.

1. INTRODUCTION

In recent years, the utilization of servo presses that are mechanical presses designed to transmit energy to a tool by mechanical means using a servo drive mechanism without clutch mechanism [1](ISO 16092-1) has spread, they are being more popular than conventional mechanical power presses. Various starting and stopping systems are adopted in the servo press. And some servo presses are designed the stop control by the stop category 1 or 2 so that the mechanical brake is not used for deceleration of the slide by the normal stop, emergency stop and protective stop. On the other hand the servo press shall be designed so that the mechanical brake actuates when the fault is detected. [2] This paper focuses on the safety of the servo press stopping system, and shows the requirements for it including the servo press mechanical brake structure and the brake control system.

First of all, we summarize structure requirements for the brakes of servo presses and mechanical power presses with clutch and brake, which are shown in ISO16092-1[1]and ISO/DIS 16092-2[2] based on the current European, American and Japanese standards.[3,4,5]

Next, the stopping mechanisms of various servo presses and hazardous events adversely affecting the stopping performance of each stopping mechanism are described, and the safety requirements to maintain the stopping performance for each stopping mechanism are clarified. Finally, we propose "Servo press stop mechanism and maintenance of brake performance" for establishing international standards for press machine.

2. SERVO PRESS IN MECHANICAL PRESS

2.1 Structure of typical mechanical press

Figure 1 shows examples of mechanical presses shown in ISO 16092-1 in a) a servo press and b) a press with a friction clutch (or a friction clutch press). [1,2] In the conventional machining energy transmission of the friction clutch press, energy of the main motor is stored in the flywheel as rotational energy and the stored energy is imparted to the drive unit by the engagement of clutch and transmitted to the slide. The stoppage of operation of the friction clutch press is achieved by disengaging the clutch and engaging brakes to the drive unit.

On the other hand, the servo press has a structure that transmits the energy of the servo motor directly to the slide by mechanical force and energy transfer mechanism. When stopping the servo press, turn off the power supply of the drive unit transmitting energy to the servo motor (i.e., stop category 0) and stop and hold the slide by using a mechanical brake, or decelerate and stop the servo motor and turn off the power (i.e., stop category 1) and maintain a state in which the slide stopped by a mechanical brake.

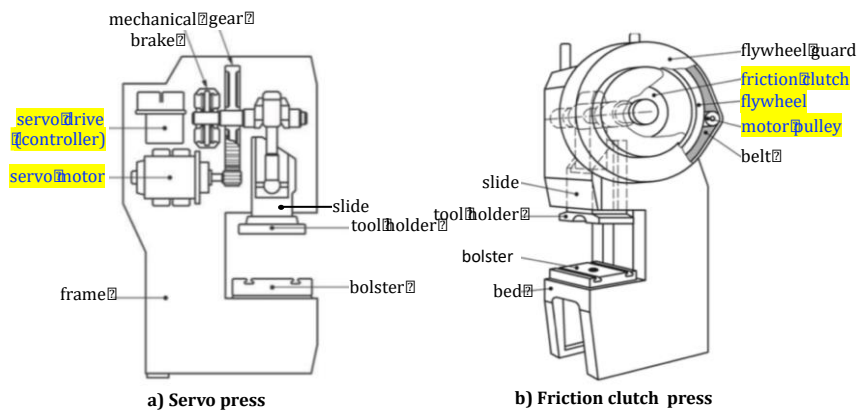


Figure 1. Typical mechanical press (tools area safeguards not shown)[1].

2.2 Main SRP/CS of typical mechanical press drive system

Figure 2 shows main safety-related control components of slide stop control system of the servo press and friction clutch and brake (C/B) control system of the friction press. The main components for the friction clutch press are a dual valve to control clutch and brake, a mechanical clutch and brake and safety-related part of control system (SRP/CS), for example a safety PLC.

On the other hand, the main components for the servo press are main contactors, servo drive (converter), mechanical brakes and SRP/CS to control the servo drive and the brake (using a dual valve or contactors).

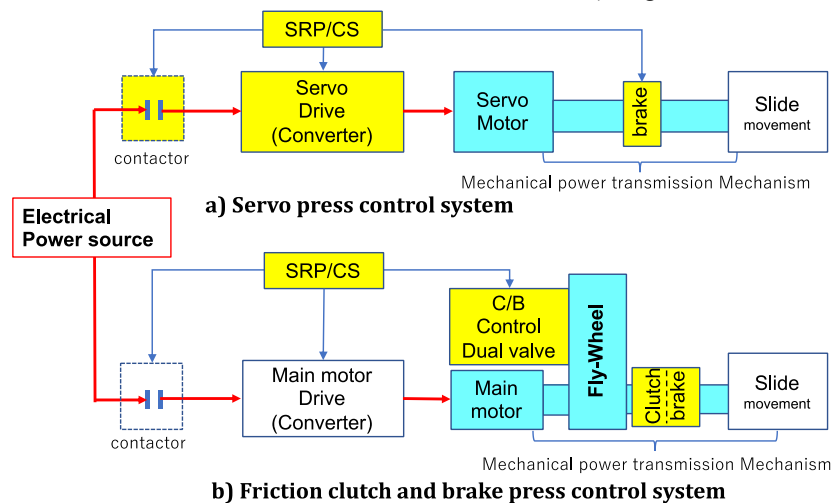


Figure 2. Main SRP/CS of typical mechanical press drive system.

3. SAFETY REQUIREMENTS FOR BRAKE SYSTEM OF MECHANICAL PRESS OF CURRENT STANDARDS

3.1 Mechanical friction brake requirements for servo press

The common requirements for mechanical brake of servo presses and friction clutch presses is stated in ISO 16092-1. These are some requirements for regarding the mechanical brake as a well-tried mechanical component of the slide stop control system.[1,7]

However, the mechanical brake is not always used for the normal stop control in cases of the servo press so designed that the stoppage of the slide of the servo press in the normal operation (e.g., one stroke operation, inching operation) is performed by the stop category 2 stop function and the emergency stop and the protective stop of the slide are achieved by stop category 1 stop function. In this type of servo press, mechanical brake is used to only restrain the slide after it stops. Therefore, in the current version of the draft of ISO 16092-2[2] (DIS 16092-2), the following are added to the common requirements for the brake system of servo presses:

- ◇ the brake shall always be engaged when the servomotor is de-energized
- ◇ if the brake(s) is designed only for holding the press slide and its attachments (e.g. tool) at any point in the cycle with the drive motor de-energized, the brake(s) shall be capable of a holding torque at least twice the torque which is generated by the mass of the press slide and its attachments in the worst case.
- ◇ On servo presses, the slide shall be stopped by the servo motor, by the friction brake, or by a combination of the servo motor and the friction brake.
- ◇ If any circumstances of drive motor de-energization cause the friction brake to be the primary means of stopping the slide, the brake shall be capable of stopping the slide quickly.

The requirements are based on the provisions of the existing industrial standard issued in each country [2,3, 4, 5] related to the safety of power press machine.

4. START/STOP CONTROL MECHANISM OF SERVO PRESS

4.1 Start/stop control structure of servo press

The clutch and brake of friction clutch press is always installed on the drive mechanism. However, for the servo press, there are mainly 5 kinds of start/stop mechanism (mechanical structure) and the various combination of stop categories 0, 1 and 2 is applied to each mechanism. Basically, the start/stop mechanisms consist of the press drive structure and the mechanical brake structure (i.e., the position where the brake is mounted).

Figure 3 shows 5 kinds of start/stop mechanism. In the structure 1 and 2 that the braking torque generated by the brake or the servo motor is transmitted to the drive shaft by the drive belt, the strength of the belt and the fault detection of breakage of the belt must be considered.[8,9,10] However, as other issues, we focus on the stop mechanism of the servo press in this paper to propose requirements of the brake structure, the brake control system and the frequency of brake maintenance test.

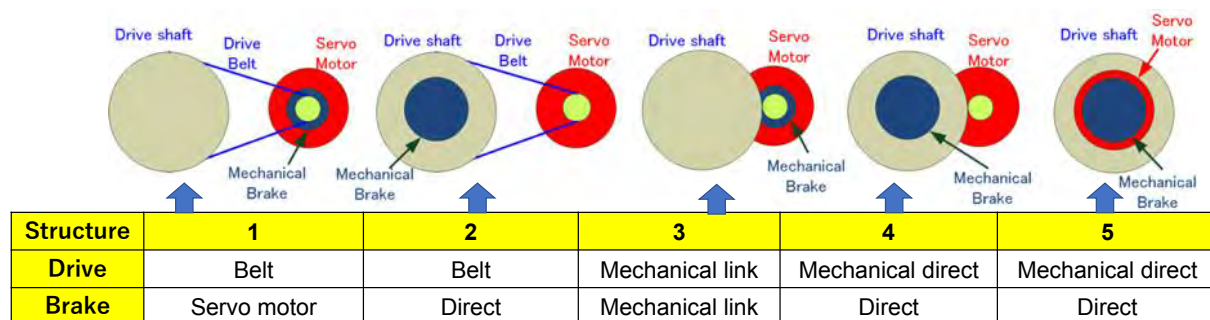


Figure 3. Main SRP/CS of typical mechanical press drive system[11].

4.2 Stop control systems of servo press

The brake control system of the friction clutch presses only controls the clutch and brake control valve and performs a stop function similar to the stop category 0 by shutting down the pneumatic (or hydraulic) fluid power to release the brake. On the other hand, the brake control system of the servo presses stops the slide by several combination of stop category 0, 1 and 2. In many cases, the stop category 2 stop function is applied to stop the slide in the normal operation such as inching and single stroke, but the-emergency stop and the protective stop function either as the stop category 0 or 1. Table 1 shows classification and notes of the servo press stop methods.

Table 1. Classification and notes of servo press stop method.

Stop category	Decelerating and Stopping the slide	Stop by Power shutdown	Stop and hold the slide by Mechanical brake	Notes for checking the stopping performance (by stopping performance monitoring)
0	Not applied	Servo Power shutdown And mechanical brake		Consideration to faults such as in braking resistor is required .
1	Deceleration and stop by the servo control	Power shutdown of servo drive and engagement of mechanical brake		The consideration to failure of stop function by the servo stop control system is required.
2	Deceleration stop of the slide and maintenance of the position of the slide by the servo control	Not applied		Not applied (The emergency stop, protective stop and stop in cases that any fault occurs is not allowed.)

4.3 Hazardous event of each stop category of brake control system

When the brake control system performs the stop category 0 stop function for the emergency stop or the protective stop, the stopping performance of the mechanical brake including the related control system and brake mechanism can be checked. However, when the brake control system performs the stop category 1 stop function for the emergency stop or the protective stop, the stopping performance of the brake is not always checked. Because in case of the stop category 1 stop function, the mechanical brake is not used for the deceleration of the slide and used only for the maintenance of the slide position after the stopped slide. Therefore, the mechanical brake performance test must be implemented to detect any failure of the brake control system of in the case that the stop category 1 stop function is used.

Figure 4 shows a typical brake control system which includes the stopping performance monitoring function and brake test function. Position sensors to measure the die height and the crank shaft angle and a motor encoder to measure the drive shaft angle are required to be additionally equipped to perform the intended monitoring and brake test functions.

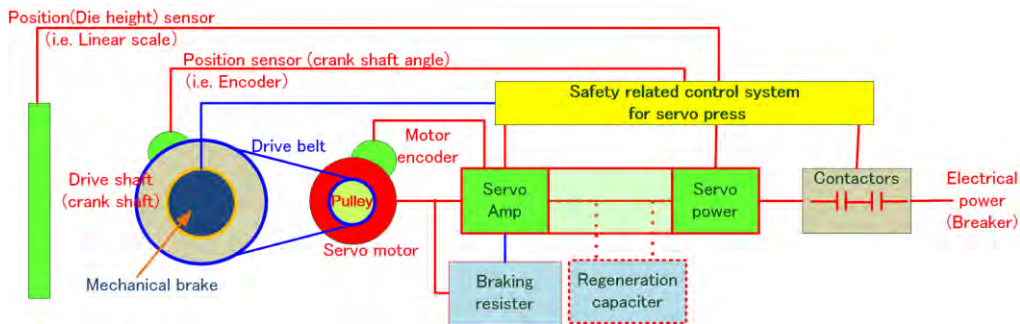


Figure 4. Example of brake control system of servo press [8].

When considering the hazardous event by deterioration or malfunction of the brake mechanism of servo press including its control system, the stopping performance must be checked same as the conventional friction clutch press. Especially, when the mechanical brake is not actuated during the deceleration process of the slide, stopping performance must be checked.

As the requirement of brake performance check for servo press, it is being discussed in the international technical committee TC39/SC10/WG1 that the stopping performance monitoring, the static brake test and the active brake test would be required.

The purpose of stopping performance monitoring is to ensure the stopping time and the stopping position does not exceed a specified value, that is the minimum distance is effective when the protective stop is initiated. The purpose of the static brake test is to ensure the brake torque is sufficiently generated to hold the slide. And the purpose of the active brake test is to ensure the appropriate stopping time/performance and the sufficient brake torque. And also when considering each test, the sufficient functioning by each test is different with the stop category of the stopping performance control.

5. PROPOSAL FOR BRAKE CONTROL REQUIREMENTS OF SERVO PRESS

ISO-CD16092-2 requires the static brake test and active brake test for servo press. The brake control system of the friction clutch presses only controls the clutch and brake control valve and executes the stopping performance monitoring at every top stop and confirm the normality of the mechanical brake by the stopping performance. Figure 5 shows the static brake test and the active brake test which are being discussed in TC39/SC10/WG1.

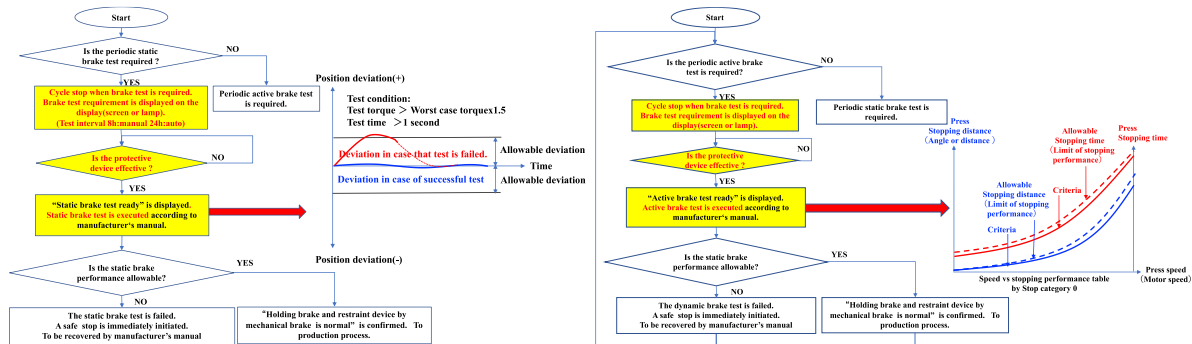


Figure 5. Example of static brake test and active brake test of servo press[2,8].

5.1 Static brake test of servo press [2]

The static brake test is required to execute once every 8 hours for the press by manual loading and unloading and once every 24 hours for other press (i.e. automatic loading and unloading press).[2]Table.2 shows the static brake test is not enough effective for the stop function. The static brake test may detect the deterioration of the brake pad and the breakage of the springs by the static friction torque of the brake. But the abnormality of stopping performance may not detect because the dynamics frictional torque of the brake never be checked by the static brake test. The purpose of static brake test is to ensure the sufficient torque to hold and restraint the slide plus other attachments mass of the worst case. Figure6 shows a example of the procedure of the static brake test.

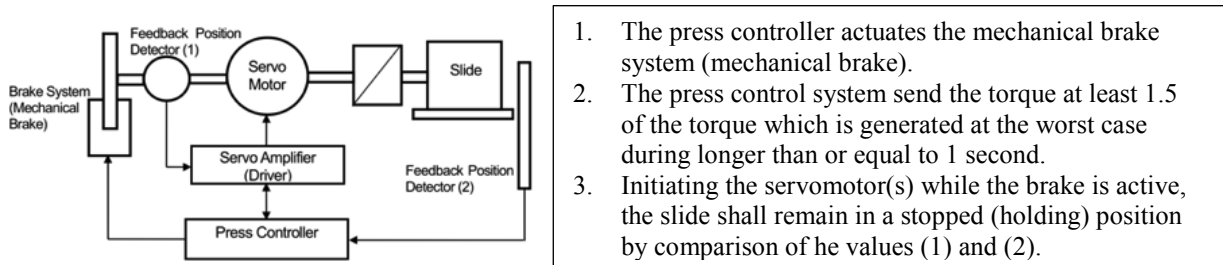


Figure 6. Example of the procedure of the static brake test.

5.2 Active brake test of servo press [2]

At the present stage, the active brake test is required to execute minimum once a year and is required which shall be performed during closing stroke, when the slide is moving at maximum speed (at the speed of which the stopping performance is practicably evaluated) by stop category 0 .Table.2 shows the active brake test is effective for the detection of deterioration and malfunction of brake mechanism of servo press which includes the electrical components(i.e braking resistor ,see Figure.5).Because the active brake test is executed by the actual brake system which includes machanical brake , electrical braking unit and other power shutdown system of the brake system of servo press.

5.3 Proposal of additional requirement for Stopping performance monitoring

Table.2 shows the both brake test is not enough effective for the stop category 1 or 2 stop function, because the press stop process by servo system may not detect by the static brake test. The stop category 1 or 2 stop function should monitor the stop process during deceleration process before the overrun detection by the stopping performance monitor. Figure.7 shows the purpose of stop performance monitor and additional monitoring flowchart and function and the control concept of each monitoring.

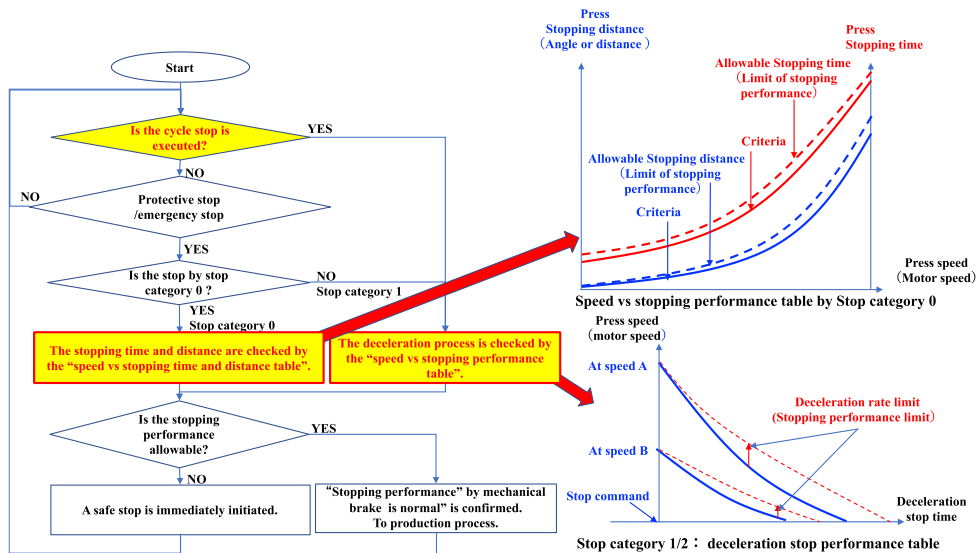


Figure 7. Proposal of stopping-performance(overrun) monitoring function of servo press[2,8].

Table 2 shows the availability for the detection against each failure regarding the protective stop which is operated by the combination of brake system and stop category.

And in the table ,the proposal of new static brake test function and the additional requirements of the stopping performance monitoring for the normal stop and the protective stop by the stop category 0/1/2 is added for the improvements of the safety and fault detection.

Table 2. Availability for the detection against each failure and new static barke test function.

X: Available N/: Not Available

No.	Abnormality of brake system (Fault)	Possible abnormal Detection item (Failure)	Stopping performance monitor			Static brake test	Active brake test	New Static brake test
			Stop cat.0	Stop cat.1	Stop cat.2			
1	Less friction	Wearing brake pad	X	N/A	N/A	X	X	X
2	torque of brake	Breakage brake spring	X	N/A	N/A	X	X	X
3	Abnormal Time lag of brake engage/disengage	Malfunction of brake valve	X	N/A	N/A	N/A	X	X
4		Brake pressure release structure	X	N/A	N/A	N/A	X	X
5		Breakage brake mechanism	X	N/A	N/A	N/A	X	X
6		Malfunction of control system	X	N/A	N/A	N/A	X	X
7	Abnormal Stop control by servo system	Breakage braking resister	X	N/A	N/A	N/A	X	N/A
8		Breakage regenerating capacitor	-	X	X	N/A	N/A	N/A
9		Malfunction of power shutdown	X	X	N/A	N/A	X	N/A
10		Malfunction of speed control	-	X	X	N/A	N/A	N/A

The static brake test is not considered effective for nomal stop function and protective stop function except the holding and retrain of the slide stop position.Because the static brake test may confirm normality of the static brake torque but the actual stopping performace may not confirm by static brake test. If the function of new static brake test shown in Figure.2 , the combination of the nes static brake test and additional stopping performance monitoring may be more effective as same level as the active brake test for the detection of the failure of servo press .

On the other hand, the active brake test for the stop function by the stop category 0 may confirm the stopping performance.But the active brake test is not considered effective for nomal stop function and protective stop function by the stop category 1 except the holding and retrain of the slide stop position.If the nomal stop function and protective stop function by the stop category 1and the stop category 2 are applied for the servo press , the combination of additional stopping performance monitoring function must be applied to the servo press.

6. CONCLUSION

The static brake test is effective for ensuring the static torque to hold the slide at the worst case,and the combination of of the new static brake test and the motion process monitoring by the new proposal of the stopping performance monitering function is expected to improve the brake system safer than the active brake test.

Session 5 – Safety of machinery

The active brake test is effective for ensuring the stopping performance by stop category 0 of servo press, but is not effective for ensuring the stopping performance by stop category 1/2 of servo press.

If stopping performance monitoring by the stopping process monitoring function shown in Table 2 and Figure 7 is applied for the servo press, the stopping performance by stop category 0/1/2 of servo press may be ensured its stopping performance and the mechanical brake actuation .

These considerations is expected to be reflected to ISO 16092-2 to improve the confirmation of the secure stopping performance by mechanical barke of servo press.

7 REFERENCES

1. ISO 16092-1: Part 1: Machine tools safety - Presses - General safety requirements
2. ISO CD16092-2: Part 2: Machine tools safety - Presses -Safety requirements for mechanical presses
3. EN692:2005+A1-2009: Machine tools - Mechanical presses - Safety
4. ANSI B11.1-2009: Safety Requirements for Mechanical Power Presses
5. JIS B6410-2008: Safety Requirements for Servo Presses
6. ISO13849-1-2015:ISO13849-2-2012:
7. KOMATSU Technical report 2003 q VOL. 49 NO.151: Introduction of Safety control of AC servo press
8. JFMA-TI103 : Servo presses-Safety requirements and Safety Measures
9. JNOSH-SD-No.26 (2010) :A Study on Procedure for Determining the Protective Stopping Time of Mechanical Servo Presses
10. JISH Power press machine specific voluntary inspection manual

REVISION OF ISO 13855

CONSIDERATION OF POSSIBLE ITEMS

Otto Görnemann - SICK AG
Central Department for Safety Management & Innovation
Chris Soranno – SICK Inc - Product & Competence Center
Americas
2018 – 10 – 14

REVISION OF ISO 13855:2010

MINIMUM DISTANCE OF VEHICLES AND MOVEABLE PLATFORMS



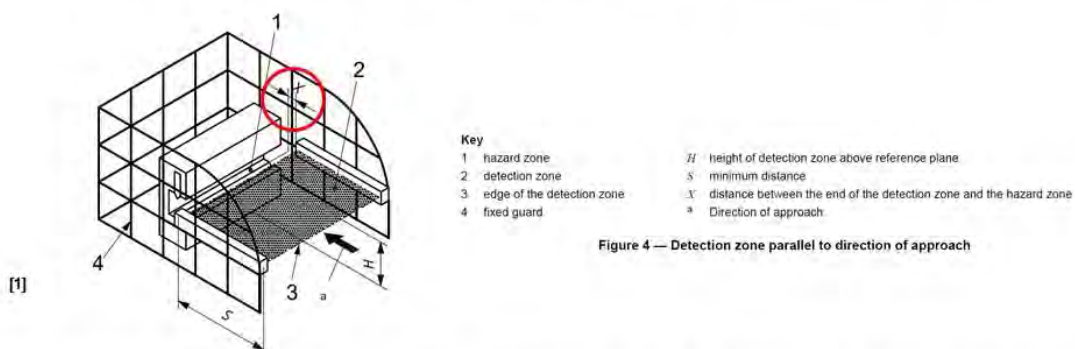
- Correction of existing editorial and technical errors
- Consistency between values to avoid reaching over vertical and horizontal detection fields (including depth of sensing field for horizontal)
- Consideration of anthropometric interpretation of the minimum distance equations
- Consideration of dynamic hazard situations and their corresponding dynamic minimum distances (☞ Dr. Saito NIOSH / Japan)
- Consideration of a generic approach for minimum distance of vehicles and moveable platforms
- Consideration of reaching manual control devices (from inside of safeguarded zones)
- Consideration of reaching under and around for ESPE
- Address VBPD applications
- Consideration of reaching when using single actuating control for protection of persons (inch/jog, hold-to-run, etc.)

REVISION OF ISO 13855:2010 INTENDED REVISION ITEMS – POSSIBLE HARMONIZATION WITH ANSI B11.19

- Address supplemental factors (Z) which must also be considered (B11.19, G.6)
- Consider further clarity of time (T) factors (B11.19, G.4)
- Consideration of reaching with non-guard locking interlocked guards (B11.19, H.8)
- Consideration of location of safety edge/bumper devices (B11.19, H.9)
- Consider further general harmonization (terminology, variables, constant values, etc.) with B11.19, Annexes G, H, I, J & K
- Address 'safe conditions' where $v \geq 0$ or anything other than full stop / standstill (B11.19, Annex J & K)

REVISION OF ISO 13855:2010 CORRECTION OF ERRORS

- Some editorial errors need to be corrected
- Those errors are not relevant since obvious to the reader e.g.
 - ESPE mounted with angle = 30° (Tolerances are given but this is not understood)
 - Depth of the undetected zone between detection zone and machine elements (frame)

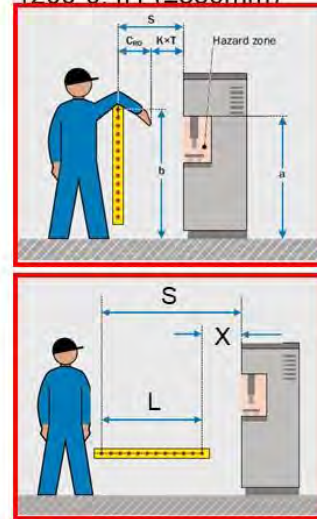


When using the device as both a trip and presence-sensing device, the distance X (see Figure 4) shall not be less than the detection capability, d .

REVISION OF ISO 13855:2010 CONSISTENCY BETWEEN VALUES TO AVOID REACHING OVER

- For vertical detection zones (orthogonal approach) those values are given in Table 1
- For horizontal detection zones (parallel approach) $C_{RO} = 1200 - 0.4H$ ($>850\text{mm}$)
- The values at detection zone heights > 800 mm are not coherent !

Height of the detection zone in mm	Resulting C_{RO} in mm	C_{RO} according to Table 1 in mm
1000	850	0 to 1200 depending on hazard zone height
900	850	0 to 1200 depending on hazard zone height
800	880	n.a.
700	920	n.a.
600	960	n.a.
500	1000	n.a.
400	1040	n.a.
300	1080	n.a.
200	1120	n.a.
100	1160	n.a.
0	1200	n.a.

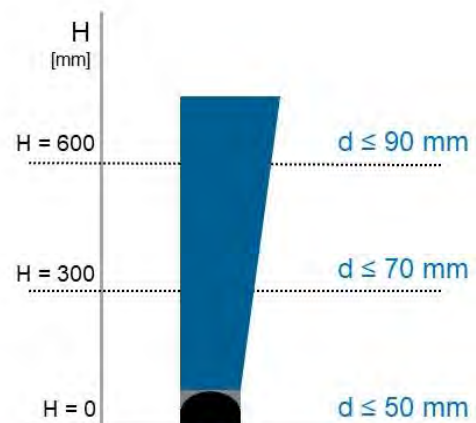
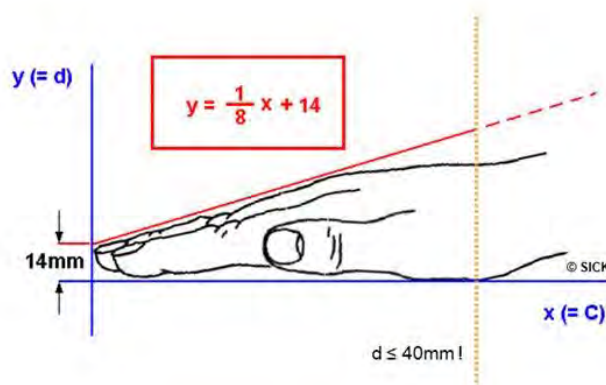


Otto Gömmernann / © SICK AG 10/2018 / SIAS 2018

7

REVISION OF ISO 13855:2010 CONSIDERATION OF ANTHROPOMETRIC INTERPRETATION OF THE EQUATIONS

- Why $C = 8 * (d-14)$ (6.2.3.1)
- Why $d = 50 + H/15$ (6.3)

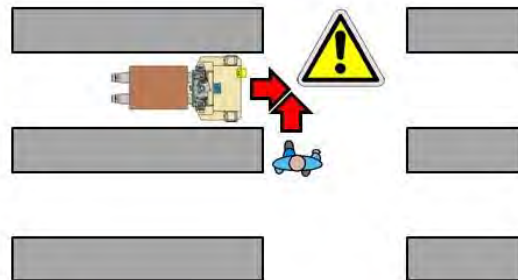


Otto Gömmernann / © SICK AG 10/2018 / SIAS 2018

8

REVISION OF ISO 13855:2010 MINIMUM DISTANCE OF VEHICLES AND MOVEABLE PLATFORMS

- Existing standards (e.g. EN 1525) do not consider a person deliberately approaching a vehicle moving in the persons direction
- The penetration factors (length of arms or legs and bowing of the torso) shall be considered depending on the application (location of zones with mechanical hazards)
- The consideration of an orthogonal approach to an unknowingly approaching vehicle crossing a lane end should not lead to additional distances since this does not really solve the problem

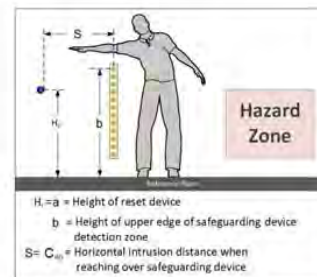
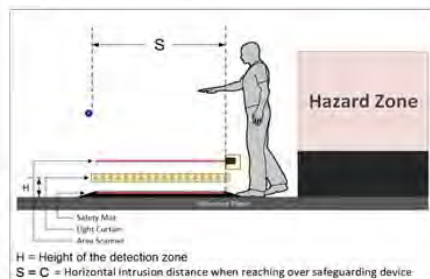


Otto Gömemann / © SICK AG 10/2018 / SIAS 2018

9

REVISION OF ISO 13855:2010 CONSIDERATION OF REACHING MANUAL CONTROL DEVICES

- Reset and restart interlocks are deactivated by actuation of manual control devices
- Such devices shall be mounted such they cannot be actuated from inside the hazard zones (safeguarded zones)
- There is no standard which provides guidance for proper positioning. It is reasonably to enlarge the scope of ISO 13855 to cover this issue
- Basically the same approach for the penetration factor to avoid access to hazardous zones by reaching over or around can be applied (without overall response time)

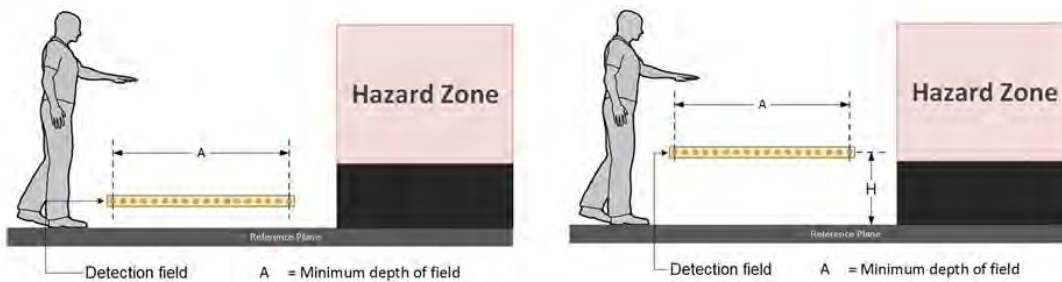


Otto Gömemann / © SICK AG 10/2018 / SIAS 2018

10

REVISION OF ISO 13855:2010 DEPTH OF SENSING FIELD FOR HORIZONTAL APPLICATIONS

- ISO 13855 does not state the required length of an horizontal detection field
- Depending on the height H of an horizontal detection field a certain length will be required to avoid easy undetected crawling under (see ISO 12100 6.3.3.1)
- This length may be differ from the length required to avoid stepping over
- Recent survey by the IFA [2] shows that a certain probability for easily crawling under is given for detection fields at a height of 300mm even for field lengths up to 2000mm.

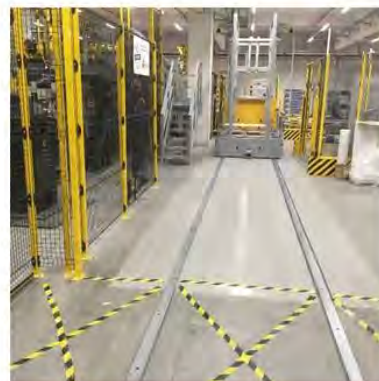


Otto Gömemann / © SICK AG 10/2018 / SIAS 2018

11

REVISION OF ISO 13855:2010 DEPTH OF SENSING FIELD FOR HORIZONTAL APPLICATIONS

- Horizontal detection fields at H=0 have shown to be easily defeated (by jumping over) even if such fields are larger (1350 mm) than required for floor mounted safety mats (750mm)
- ISO 13855 should state the required detection field length to avoid easy stepping and jumping over independently from the device providing the safety function
- This field length should be related to his height



Otto Gömemann / © SICK AG 10/2018 / SIAS 2018

12

REVISION OF ISO 13855:2010 ADDRESS VBPD APPLICATIONS (3D)

- Where detection of the persons approaching a hazard zone is done within a space (3D) the actuation of the ESPE as trip device occurs at the boundary of the 3D volume (surface), typically in single detector device as a combination of a cylinder and a cone.
- In order to reduce the minimum distance the height of the cylinder shall be such that the remaining cone shape results in an orthogonal approach to the hazard zone
- First drafts of the IFA (Germany) propose the determination of the additional distance C as follows:

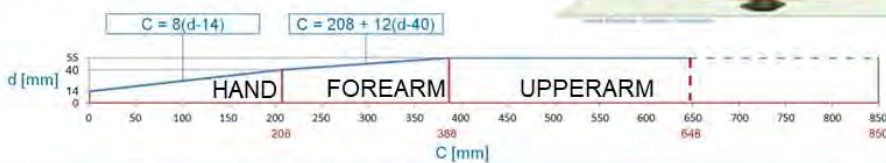
$$C = DPF + CTZ + d$$

where:

d = detection capability

CTZ = position uncertainty (manufacturer)

DPF = C_{RT} as:



Otto Gömemann / © SICK AG 10/2018 / SIAS 2018

13

REVISION OF ISO 13855:2010 CONSIDERATION OF REACHING UNDER (C_{RU}) AN ESPE

- Where detection zones of ESPE do not extend to the access plane (floor), undetected access to hazardous areas by reaching under the protective field shall be prevented.
- On vertical detection zones, the height G of the zone (starting from the floor or access plane) in which intrusion detection is not ensured is defined by the following equation:

$$G = H + d$$

H = height of the lowest edge of the detection zone

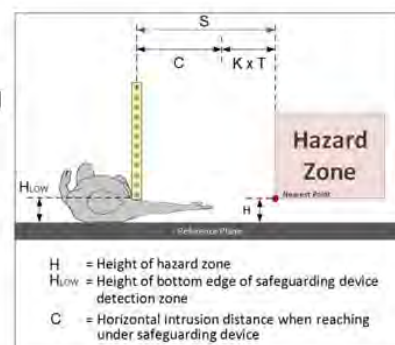
d = the detection capability of the electro-sensitive protective device

- To prevent access to hazardous zones by reaching under electro-sensitive protective equipment the following can be applied:

- for reaching under detection fields of devices with $G \leq 40\text{mm}$;

$$S = C_{RU} = 8 \times (d-14)$$

- for reaching under detection fields of devices with G between 40mm and 300mm, values according to table V4



H = Height of hazard zone
 H_{low} = Height of bottom edge of safeguarding device detection zone
 C = Horizontal intrusion distance when reaching under safeguarding device

Otto Gömemann / © SICK AG 10/2018 / SIAS 2018

14

REVISION OF ISO 13855:2010 SAFETY DISTANCES FOR REACHING UNDER VERTICAL DETECTION ZONES

- The table is based on the values of Table 1 for $b=1400$ mm. Considering that a person lying on the floor and trying to reach a hazardous area has a reach which is symmetrical to the reach of a person standing in front of a vertical detection zone with a height equal to the shoulder height and trying to reach a hazard zone located at the same height or below.
- According to Table 1, line 4.4.1 of ISO 7250-3:2015 the value for the 95% for the shoulder height is 1625 mm. A correction factor of -200mm has been taking into account to consider the shoulder and arm thickness in a worst case assumption- The height values for "a" in Table 1 for reaching downwards between 1400 mm. and 600 mm. correspond symmetrically to the values for a in the following table for reaching upwards between 0 mm. and 800 mm.

Height a of the safety-related control device in mm.	0	200	400	600	800	≥ 1000
Minimum distance S in mm.	850	850	800	700	450	0

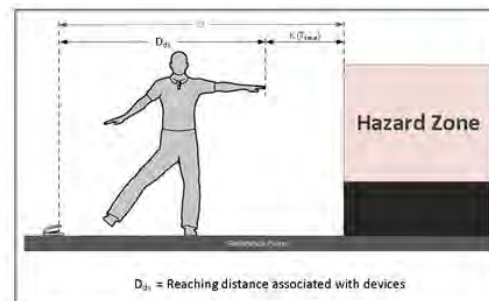
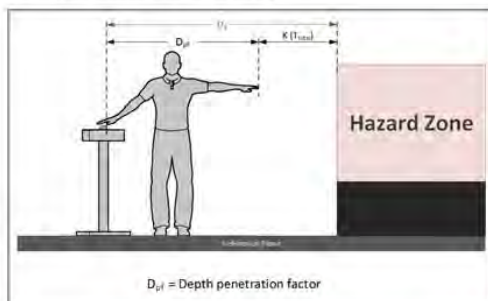
- Where the height of the zone (G) in which intrusion detection is not ensured exceeds 300 mm., the protective device will not prevent full body access.
- Where it is foreseeable that ESPE employing AOPD will be used in non-industrial applications, for example in the presence of children, the minimum distance S to prevent reaching under detection fields of devices with $G \leq 40$ mm shall be calculated with $C = CRU = 8 \times (d-14)$ and be increased by at least 75 mm.

REVISION OF ISO 13855:2010 REACHING SINGLE ACTUATING CONTROL FOR PROTECTION OF PERSONS

- To prevent actuation of a safety-related control device while being able to reach (access) a hazard zone with the upper or lower limbs the minimum horizontal distance S between the safety-related control device and the nearest hazard should be:

- for hand actuated safety-related control devices: $S = 2200$ mm

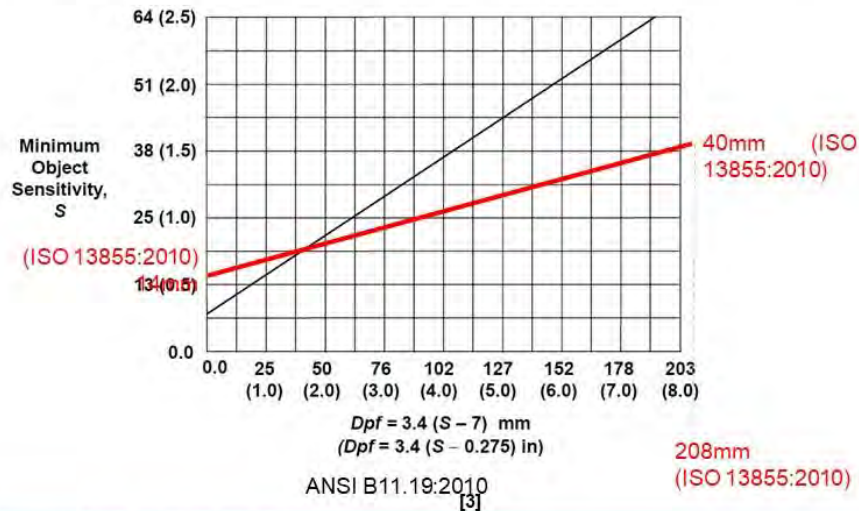
this value results from adding two times the standard arm reach (850 mm) to the acromial shoulder width (456 mm) for the 95% for the male according to 4.2.8 of ISO 7250-3:2010, and then rounded for simplicity



REVISION OF ISO 13855:2010

POSSIBLE HARMONIZATION WITH ANSI B11.19 – DPF ?

- The depth penetration factor for orthogonal approach for devices with a detection capability $\leq 40\text{mm}$ (ISO) and minimum object sensitivity $\leq 65\text{mm}$ (ANSI) differ in gradient & maximum range



REVISION OF ISO 13855:2010

INTENDED REVISION ITEMS – POSSIBLE HARMONIZATION WITH ANSI B11.19

- Address supplemental factors (Z) which must also be considered (B11.19, G.6)
- Consider further clarity of time (T) factors (B11.19, G.4)
- Consideration of reaching with non-guard locking interlocked guards (B11.19, H.8)
- Consideration of location of safety edge/bumper devices (B11.19, H.9)
- Consider further general harmonization (terminology, variables, constant values, etc.) with B11.19, Annexes G, H, I, J & K
- Address 'safe conditions' where $v \geq 0$ or anything other than full stop / standstill (B11.19, Annex J & K)
- Consideration of reaching when using single actuating control for protection of persons (inch/jog, hold-to-run, etc.)

REVISION OF ISO 13855:2010 CONSIDERATION OF MINIMUM BODY DEPTH FOR FULL BODY ACCESS



- Although ISO 13855 states the approach speeds (1.600 and 2.000 mm/s) it does not state the minimum body deep which is necessary to consider the minimum detection time of an ESPE when intended to detect full body access
- The actual IEC standards for AOPDDR state 150mm as the length of a testing rod which shall be used for verification of the product requirements
- This maximum length may be appropriate for testing purposes but it is unsuitable for real applications in industry



Otto Gömmernann / © SICK AG 10/2018 / SIAS 2018

19

FULL BODY ACCESS WALKING PHASES



- The 8 phases of humans walking according to Perry (1992)

[4]



Walking phases	IC	LR	MST	TST	PSW	ISW	MSW	TSW
	Initial contact	Loading response	Mid Stance	Terminal Stance	Pre Swing	Initial Swing	Mid Swing	Terminal Wwing
Walking cycle	0 %	0 - 12 %	12 - 31%	31 - 50 %	50 - 62 %	62 - 75 %	75 - 87 %	87 - 100 %
Hip	20° Flexion	20° Flexion	0° Flexion	-20° Hyperextension	-10° Hyperextension	15° Flexion	25° Flexion	20° Flexion
Knee	0°-5° Flexion	20° Flexion	0°-5° Flexion	0°-5° Flexion	40° Flexion	60°-70° Flexion	25° Flexion	0°-5° Flexion
Ankle	0°	5°-10° Plantar Flexion	5° Dorsal Flexion	10° Dorsal Flexion	15° Plantar Flexion	5° Plantar Flexion	0°	0°
Active Muscles	Quadriceps femoris	Quadriceps femoris	Gastrocnemius	Gastrocnemius	Gastrocnemius	Extensor hallucis I	Semimembranosus	Semimembranosus
	Tibialis anterior	Tibialis anterior	Soleus	Soleus	Soleus	Flexor hallucis longus	Semtendinosus	Semtendinosus
	Gluteus medius	Gluteus medius		Flexor digitorum longus	Rectus femoris	Sartorius	Biceps femoris	Biceps femoris
	Gluteus maximus	Gluteus maximus		Flexor hallucis longus	Adductor longus	Iliacus	Tibialis anterior	Tibialis anterior
	Ischiocrurali	Adductor magnus		Tibialis posterior		Tibialis anterior		Quadriceps femoris
		Tensor fasciae latae		Peroneus longus				
		Tibialis posterior		Peroneus brevis				
		Peroneus longus						
Functions	- Heel contact with ground	- Shock absorption at knee and ankle - Load transfer and stabilization by hip - Forward movement by heel rocking	- Controlled forward movement of the tibia - Shifting of center of balance	- Controlled dorsal extension at the ankle with heel separation from the ground	- Passive knee flexion of 40° - Plantarflexion of the ankle	- Minimum of 55° knee flexion to achieve sufficient ground clearance	- Increasing hip flexion up to 25° - Dorsal extension of the ankle up to the neutral position	- Knee extension up to the neutral flexion - Preparation of the stance phase

Otto Gömmernann / © SICK AG 10/2018 / SIAS 2018

20

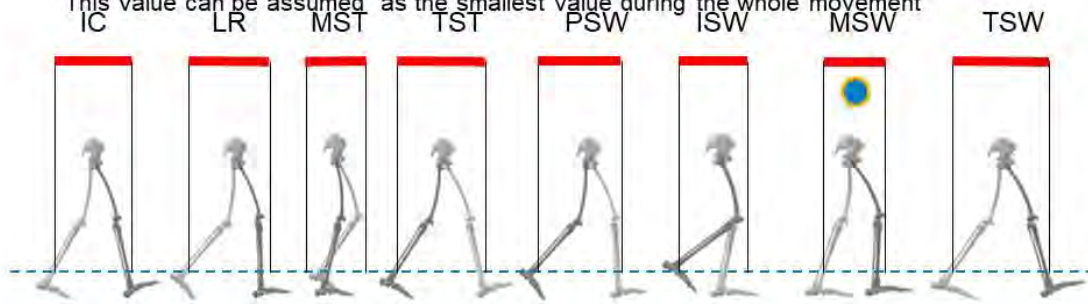
FULL BODY ACCESS

HORIZONTAL PROJECTION (DEPTH) IN THE WALKING PHASES



- Generally IC or ISW Phases can be considered as the possible initial phases
- Therefore LR or MSW phases follow as motion phases.
- The length of the horizontal projection (T_x) of the human body shall ~~be~~ considered
- The projection height shall be limited to the height which corresponds with 70mm detection capability, therefore allowing the detection of the human rump or legs starting from 300mm height.
(EN ISO 13855:2010, Subclause 6.4 Formula 8)

- The resulting lowest value of the horizontal projection is T_{MSW} . This value can be assumed as the smallest value during the whole movement



[1]

Otto Gömemann / © SICK AG 10/2018 / SIAS 2018

21

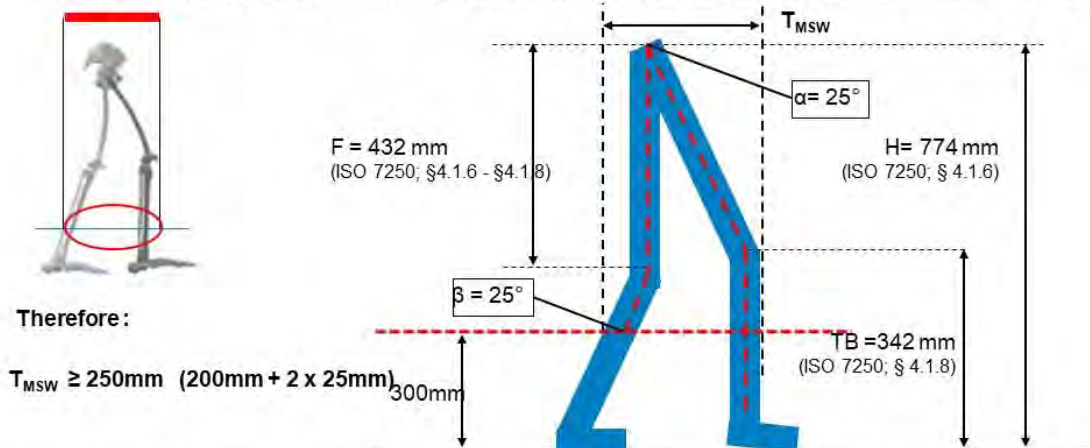
FULL BODY ACCESS

HORIZONTAL PROJECTION IN MSW – VALUES ACC. ISO



7250-3:2015

- The lowest (smallest) value of the horizontal projection is T_{MSW} & can be assumed as the smallest value during the whole movement
- From this a simple geometrical model for the bone structure can be derived and applied to the anthropometric data given in ISO 7250-3:2015. (5 percentile)*
(The femoral length is considered as the difference between the Spina-Iliaca height & Tibial height)
- An overall thickness of the soft tissues surrounding the bone (Muscles, fat, skin) of 25mm is assumed)



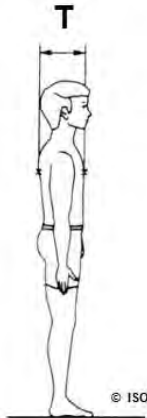
ISO 7250-3:2015-08 Basic human body measurements for technological design Part 3: Worldwide and regional design ranges for use in product standards

Otto Gömemann / © SICK AG 10/2018 / SIAS 2018

22

FULL BODY ACCESS COMPARISON OF THE HORIZONTAL PROJECTION (DEPTH)

- Generally 3 different body postures can be assumed.



Standing – arms clinging
 $T \geq 185 \text{ mm}$ (ISO 7250; §4.1.10 – P5)
 $V \text{ possible} = 0$
 (only hopping, not realistic)



Walking – arms clinging
 $T \geq 200 \text{ mm}$ (T_{MSW} – see page 5)
 $V \text{ possible} = 1,1 \text{ m/s}$ (ca. 4km/h)
 (normal walking speed)



Walking + reaching
 $T \geq 200 \text{ mm}$ (T_{MSW} – see page 5)
 $V \text{ possible} = 1,6 \text{ m/s}$ (ca. 6km/h)
 (According ISO 13855:2010)

Access/Approach not possible without collision
 = unrealistic approach

FULL BODY ACCESS APPLICATION : RESPONSE TIME SAFETY LASER SCANNERS

- The test body length (150mm) for safety laser scanners adopted in the draft IEC 61496-3: 2016 does not currently correspond to the minimum length of the vertical projection of a human body assuming the 5 percentile of the anthropometric body measurements according to ISO 7250-3:2015. Assuming the possible test body lengths (3) and approach speeds (2), the following detection times result

Horizontal projection of the part of the body to be detected in mm	Minimum detection time in ms. according to the application approach speed	
	1,1 m/s	1,6 m/s
200	182	Not applicable
250	227	156
350	318	219

- Excerpt from ISO 13855:2010(Scope)

The values for approach speeds (walking speed and upper limb movement) in this International Standard are time tested and proven in practical experience. This International Standard gives guidance for typical approaches. Other types of approach, for example running, jumping or falling, are not considered in this International Standard.

NOTE 1 Other types of approach can result in approach speeds that are higher or lower than those defined in this International Standard.

REVISION OF ISO 13855 CONCLUSIONS - CREDITS / REFERENCES



- The revision of ISO 13855 is not only due but necessary for several reasons
 - The main goal of such a revision should be to improve the usability for machinery manufacturers and Type C standard writers
 - Additional surveys may be necessary to support actual considerations
-
- [1] ISO 13855:2010. Safety of machinery – Positioning of safeguards with respect to the approach speed of parts of the human body. ISO – International Organization for Standardization. ISO Central Secretariat. Chemin de Blandonnet 8. CP 401 – 1214 Vernier, Geneva, Switzerland
- [2] DGUV-Information. 3D-Schutzraum: Anordnung der BWS. Bestimmung des Sicherheitsabstands in Anlehnung an DIN EN ISO 13855. Entwurf 12/2013 FB HM-072. Deutsche Gesetzliche Unfallversicherung.
- [3] B11.19 Performance Criteria for Safeguarding
Secretariat and Accredited Standards Developer B11 Standards, Inc., 42293 Young Lane, Leesburg, VA 20176, USA
- [4] Pathophysiology of juvenile idiopathic arthritis induced pes planovalgus in static and walking condition – A functional view using 3d gait analysis. Figure 2, modified. June 2015. Pediatric Rheumatology 13(1):21. DOI:10.1186/s12969-015-0022-z Source: PubMed. License: CC BY 4.0
Authors : J. Merker, M. Hartmann, F. Kreuzpointner, A. Schwirtz, J-P. Haas



Session 6

Experiences / Practical applications

Serious and fatal accidents caused by mobile machinery in Quebec: More prevention is needed

Burlet-Vienney D.¹, Chinniah Y.², Belmekki T.², Aucourt B.², Ouali M.-S.²

¹ Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST) – 505, boul. De Maisonneuve Ouest – Montréal (Québec) – H3A 3C2 – Canada

² Polytechnique Montréal – University of Montreal, P.O. Box. 6079, Station Centre-ville – Montréal (Québec) – H3C 3A7 – Canada

dambur@irsst.qc.ca
yuvin.chinniah@polymtl.ca
taha.belmekki@gmail.com
barthelemy.aucourt@polymtl.ca
msouali@polymtl.ca

KEYWORDS: mobile machinery, accidents, safety of machinery, practical applications and experience

ABSTRACT

Mobile machinery is often raised as an issue by national occupational fatality statistics. However, no exhaustive and qualitative analysis of accident reports on mobile machinery as a group is available, as compared to stationary machinery. The objective of this paper is therefore to analyse reports of serious and fatal accidents caused by mobile machinery in the province of Quebec where data on stationary machinery have already been examined. All the investigation reports for serious and fatal accidents occurring between 2000 and 2013 were analysed. Road accidents were not included. 281 investigation reports were retained over the period. This represents 25% of work-related fatalities in Quebec over the period and a rate of 0.45 fatalities per 100,000 workers. Road transportation equipment is the type most involved in accidents (33%). Regular operation-related accidents account for 77% of the total. Mobile machinery caused annually three times more fatal accidents than stationary machinery in Quebec, and involved experienced workers and regular operations in a larger proportion. Accident reports also revealed types of accidents specific to mobile machinery as a group such as runover, rollover, contact with power lines, loads falling and presence of gravitational energy during maintenance.

Such risks on mobile machinery are not new. The problem seems to lie mainly in the non-application of existing prevention principles. Mobile machinery is often excluded by companies during risk assessment and control of hazardous energy methods. Given the statistics, mobile equipment as a group should be targeted by labour inspectors and companies in Quebec as it was done for stationary machinery 10 to 15 years ago. More research is still needed in the integration of innovative technologies in real applications in order to reduce risk. Examples include driving assistance technologies, remotely controlled and autonomous vehicles such as tractors, mobile robots, self-driving vehicles and drones.

1 INTRODUCTION

Machine presenting hazards due to its mobility is defined in the European Machinery Directive as follows: “machinery the operation of which requires either mobility while working, or continuous or semicontinuous movement between a succession of fixed working locations, or machinery which is operated without being moved, but which may be equipped in such a way as to enable it to be moved more easily from one place to another” [1]. Mobile machinery includes, for example, loaders, lift trucks (forklifts), snowblowers, snowplows, dump trucks, mobile robots, mobile cranes, tractors, aerial basket lifting devices and abrasive spreaders.

According to [2], in the United States (U.S.), from 1992 to 2010, equipment involved in the largest number of deaths by sector were (1) tractors in agriculture, forestry and fishing, (2) excavators in construction and (3) lift trucks in several other industries. These machines are all types of mobile machinery. Although the number of mobile machinery accidents decreased between 1992 and 2010 in the United States, this trend remains lower than for industrial stationary machinery. Moreover, 61% (116/188) of the occupational fatalities in Australia in 2014 involved mobile machinery or motor vehicles [3].

Several studies in Australia, Sweden, India, the U.S. and Canada show that construction, agricultural, forestry, fishing and mining sectors have high accident rates and that it is mostly due to the extended use of mobile machinery [4-8].

Based on this data, mobile safety of machinery should be an important issue for companies. However, mobile machinery is sometimes perceived by companies as a separate category of machines with respect to regulation and prevention. For example, mobile machinery was not taken into account in Quebec when municipalities implemented their hazardous energy control program (lockout/tagout) even if this type of equipment was widely involved in serious and fatal accidents during non-production phases in the municipal sector [9]. Moreover, it should be noted that the detailed studies on fatal accidents found in literature target either a type of mobile machinery or a specific sector of activity. There seems to be no exhaustive analysis of mobile machinery as a group of machines, as could be done for stationary machinery in order to identify the main common gaps and prevention actions (e.g., [10]).

Thus, this paper aims to analyse qualitatively all reports of serious and fatal accidents caused by mobile machinery in the province of Quebec between 2000 and 2013 where data on stationary machinery have already been examined [10]. Considering mobile machinery as a group is an approach that would allow (1) identifying the main mechanisms of accident, (2) comparing the extent and the type of safety issues with stationary machinery, and (3) targeting prevention actions for companies beyond regulatory obligations.

2 METHODS

The originality of this study lies in the fact that mobile machinery is considered as a group of machines. In this paper, mobile machinery is defined as self-propelled, towed, or transported equipment that is not designed solely to transport personnel. On a methodological point of view, no keyword extraction was performed to track reports on the database of the *Commission des normes, de l'équité et de la santé et de la sécurité du travail* (CNESST) [11]. The decision to select a report was made by reading the summary of the accident. In Quebec, the CNESST insures 85 % of active workers and investigates nearly-all fatal accidents that occur within the province and fall under its jurisdiction, with the exception of regular road accidents and assaults. The investigation reports are standardized (e.g., summary of the accident and its consequences, summary of the causes retained by the OHS inspectors, etc.) and made public with a view to preventing the recurrence of similar accidents. Serious accidents are also investigated according to criteria such as severity, media coverage and technologies involved.

The investigation reports were analysed using a pivot table which provides the following information for each accident report: (i) year and month in which the accident occurred, (ii) industry sector, (iii) equipment involved, (iv) brief description of the accident, (v) summary of the causes retained by the inspectors, (vi) type of accident, (vii) type of energy involved, (viii) location of the accident, (ix) number of fatalities or injured workers, (x) occupation and experience of the workers involved.

A total of 813 investigation reports for serious and fatal accidents occurring during the targeted period (2000-2013) were available. 306 reports (38%) involving mobile machinery as previously defined were initially retained. Two researchers performed the selection for the most contentious cases. Of these 306 reports, 25 (8%) concerned traffic accidents and were excluded from this study which focuses on safety of machinery. In the end, 281 accident investigation reports related to mobile machinery over the period 2000 to 2013 in the province of Quebec were retained. It accounts for 35 % of all-cause accident investigation reports over the period. These accident reports involved 305 victims including 260 deaths.

3 RESULTS

3.1 Overview

Over the study period (2000-2013), there was an annual average of 21.8 victims of serious or fatal accidents caused by mobile machinery in Quebec including more than 18 fatalities per year. It represents more than 25 % of work-related fatalities in Quebec over the period (occupational diseases excluded) and a rate of 0.45 fatalities per 100,000 workers. The annual average of mobile machine-related victims decreased by 17.3 % when comparing 2000-2006 and 2007-2013 periods (23.9 victims/year to 19.7 victims/year). This decrease is comparable to that of all work-related fatalities in Quebec over the same period (16.8%).

Table 1 shows the number of victims of serious or fatal accidents related to mobile machinery in Quebec during the 2000-2013 period, by industry sector and equipment type. The sector most affected is Buildings and Public Works (31%). This sector uses a lot of heavy machinery (e.g., loader, dumper). Road transportation equipment (e.g., trucks, dump trucks, tow truck) is the type of equipment most involved in accidents (33%). Many other types of equipment are also involved (e.g., snowblower, harvester); they are included in the "Other" category.

Table 1. Number of victims of serious or fatal accidents related to mobile machinery in Quebec from 2000 to 2013, by industry sector and equipment type.

Industry sector	No. of accident victims	Equipment type	No. of accident victims
Buildings and Public Works	96 (31%)	Trucks and dump trucks	101 (33%)
Other Business and Personal Services ¹	56 (18%)	Forklifts	43 (14%)
Forestry, Logging and Sawmills	39 (13%)	Loaders	29 (10%)
Transportation and Warehousing	37 (12%)	Agricultural tractors	16 (5%)
Mines, Quarries and Oil Wells	31 (10%)	Other	116 (38%)
Agriculture and Agri-Food	25 (8%)		
Trade (Wholesale and Retail)	21 (7%)		

¹ This sector includes: Maintenance and repair services, roadside and towing services, personal care services, religious, grant-making, civic, professional and similar organizations, Private households.

3.2 Accident type and work activity

The results for this section are presented in two parts: maintenance and regular operation-related accidents. Maintenance operations included activities such as inspection, repair, unjamming and cleaning. Regular operation included specific activities such as normal start-up, parking, unloading/loading, docking and undocking. Maintenance-related accidents with 69 victims (including 56 fatalities) account for 23% of the total. Regular operation-related accidents with 236 victims (including 204 fatalities) account for the remaining 77%.

3.2.1 Accidents related to maintenance performed on mobile machinery

Table 2 shows the number of victims of serious or fatal accidents related to maintenance performed on mobile machinery in Quebec during the 2000-2013 period, by accident type. Examples of accidents are provided. The three most represented categories are (i) fall of equipment, or equipment part, from a height (29%), (ii) a moving part of the equipment (28%) and (iii) a moving vehicle (19%). Closer analysis of the accidents reveals that those in the “fall of equipment, or equipment part, from a height” category tend to have technical causes (e.g., strength of the blocking mechanism), whereas accidents in the “moving vehicle” or “moving part” categories are often due to organizational or communication problems. Lastly, agricultural equipment appears to be particularly affected by the “moving part” problem, in this case, power take-off (PTO). Data also suggest that nearly 80% of maintenance-related accidents occur outside the workshop or garage. In most cases, an improvised intervention procedure that did not comply with the manufacturer’s specifications was applied. The three main accident types documented were directly related to a problem in applying a lockout/tagout procedure. In nearly two-thirds of the cases, it was neither a mechanic nor a technician performing the task.

Table 2. Number of victims of serious or fatal accidents related to maintenance performed on mobile machinery in Quebec from 2000 to 2013, by accident type.

Accident type	No. of accident victims	Example of an accident involving maintenance for each accident type
Fall of equipment, or equipment part, from a height	20 (29%)	A worker is changing a hydraulic hose on a forklift. The mast is supported by a beam resting on the ground. The beam moves, causing a section of the mast to hit the worker’s head.
Moving part	19 (28%)	An employer initiates the upward movement of the body of his truck. It stops going up. A worker climbs under the body to add oil to the lifting system. He accidentally activates the body lowering lever.
Moving vehicle	13 (19%)	A worker is lying underneath a loader truck. The accident occurs when the loader truck moves forward and the left rear wheels run over the worker.
Tire blowout/Rim roll-off	8 (12%)	A truck driver is injured by the blowout of a tire on his road tractor. The accident occurs when the worker is stretched out under the vehicle to check the brake chamber of the wheel.
Tank explosion	5 (7%)	A worker is repairing the pneumatic braking system of a truck. Equipped with a propane torch, he heats the purge valve. The secondary tank explodes and hits the worker.
Poisoning	4 (6%)	An employer is poisoned and loses consciousness after entering a tank that had been used to transport liquefied cow manure.

3.2.2 Accidents related to regular operation of mobile machinery

Table 3 shows the number of victims of serious or fatal accidents related to the regular operation of mobile machinery in Quebec during the 2000-2013 period, by accident type. The three leading causes retained are (i) movement of the whole piece of equipment, (ii) equipment rollover/tipover, and (iii) the fall or movement of the load. Mechanical energy was involved in most of the accidents. This type of energy is often related to risks such as being crushed, run over, or struck by equipment. Gravitational energy is also associated with several types of accidents such as equipment rollovers or tipovers and people or loads falling.

Table 3. Number of victims of serious or fatal accidents related to regular operation of mobile machinery in Quebec from 2000 to 2013, by accident type.

Accident type	No. of accident victims	Example of an accident related to operation of mobile machinery for each accident type
Moving equipment/runover	97 (41%)	During garbage collection, the garbage truck backs up. The garbage collector is crushed to death by the truck.
Rollover/Tipover	39 (17%)	The operator of a hydraulic excavator is crushed to death when the excavator tips onto its side as it is being loaded onto a trailer.
Fall/Movement of load	37 (16%)	The workers are installing the front roofing on a modular home. The roofing, which is being lifted by a crane truck, falls onto the workers.
Moving part	30 (13%)	During recycling collection, a worker is caught by the gripping claw of the truck when it accidentally descends.
Fall of victim	23 (10%)	A worker is working on an elevating platform. He falls approximately 5.5 metres when the platform suddenly detaches and falls.
Electrocution	6 (<1%)	During the handling of roof trusses, the lifting cable of a crane truck is less than 3 m from the power line (25 kV). An electric arc is produced.
Poisoning	2 (<1%)	The worker starts up his self-propelled concrete saw in the warehouse. Carbon monoxide fills the warehouse and asphyxiates the victim.
Other	2 (<1%)	-

3.3 Worker’s experience

For the victims where information was available, it was found that almost 50% of them had more than five years of experience, 30% had between 1 and 5 years of experience, and 20% had less than 1 year of experience. The same trend was observed for maintenance and regular operations of mobile machinery. Thus, even the most experienced workers on mobile machinery were vulnerable.

4 DISCUSSIONS

4.1 Comparison with stationary machinery

In Quebec, serious and fatal accidents related to moving parts of stationary machinery were analysed between 1990 and 2011 [10]. That study used the same source as the present study and allows us to compare serious and fatal victims related to mobile and stationary machinery in Quebec as shown in Table 4. For a more accurate comparison, the period 2000-2011 was considered as far as possible for stationary machinery.

Despite limitations (i.e., reference period, types of accidents targeted for stationary machinery), this comparison points out to some differences between mobile and stationary machinery:

- The number of victims is more than three times greater for mobile machinery even while keeping only the accidents in relation to moving parts.
- The downward trend in the number of victims is more pronounced for stationary machinery (-58%) than for mobile machinery (-17%) since 2006. These results are consistent with the statistics observed in the U.S. [2].
- Accidents on mobile machinery concern more experienced workers (> 5 years of experience) than on stationary machinery. The fact that mobile machinery is used in a changing and sometimes unknown environment would be an assumption to be verified. Supervision and respect of safety procedures are also more difficult to enforce [6].
- Concerning the type of activity at the time of the accident, it appears that the problem largely relates to maintenance activities for stationary machinery and regular operations for mobile machinery.

Table 4. Comparison of serious and fatal victims on mobile and stationary machinery in Quebec.

Item	Stationary machinery	Mobile machinery
Data source	CNESST	CNESST
Period of study	1990-2011	2000-2013
Annual average	6.1 (73 victims/12 years) ¹	21.8 (305 victims/14 years)
Trend (2000-2006 and after 2006)	-58% ¹	-17%
Work activity		
Maintenance	65%	23%
Regular operation	35%	77%
Worker's experience		
> 5 years	30 %	50 %
< 5 years but > 1 year	26 %	30 %
<1 year	44 %	20 %

¹ (2000-2011) was the period taken into consideration for a better comparison.

4.2 Preventive actions

The previous comparison with stationary machinery and the number of victims indicates that mobile equipment, as a group, should be targeted by labor inspectors and companies in Quebec as it was done for stationary machinery 10 to 15 years ago. At that time, moving parts were specifically addressed by promoting the use of fixed and mobile interlocked guards and protective devices (e.g., safety mats, safety light curtains, and scanners). Accident statistics indicate a major improvement on this issue for stationary machinery [12].

Based on the accidents, preventive action plan by labor inspectors and companies in Quebec should address the following elements:

- Driving issues: equipment stability (e.g. rollover), machine-pedestrian collisions particularly during back-up manoeuvres.
- Lifting issues: loads falling, overloading, load stability.
- Environment issues: moving parts, ground stability, contact with overhead or underground power lines or cables, excavations in the presence of underground water or gas pipes.
- Trip and fall issues: falling when entering or exiting the cab, falling from the top of the equipment.
- Maintenance issues: absence of control of hazardous energies (e.g., no lockout procedure, gravitational energy present during maintenance, inadvertent start-up), interventions by unspecialized workers, tire blowout, tank explosion.

Most of these issues are not new and are subject to legislation (e.g., [13]) and standards (e.g., [14-16]). The literature also contains more specific recommendations regarding risk reduction measures dedicated to mobile machinery. For example, a number of technologies for detecting the presence of people in the vicinity of mobile machinery can be used, provided they are used properly [17]. RFID systems, scanners, visual or audible alarms, traffic aisles with protectors, and speed limitation devices are means that can be used to improve pedestrian safety [18]. On another topic, specific guidance for maintenance interventions is now also available [19].

Thus, solutions exist. The problem therefore seems to lie mainly in the non-application of existing prevention principles by companies. Even experienced workers are concerned. Supervision and respect of safety procedures are also more difficult to enforce due to the mobility of equipment. Beyond the coercive aspect with labor inspectors, companies and workers need to be informed about the extent of the problem and its specificities. According to [2], “while stationary machines have a long history of engineering out hazards, mobile machine safety may still be too dependent on educating workers to work safely on and around equipment.” Thus, additional research is needed in the integration of existing technologies in real applications in order to reduce risk. Examples include remotely controlled and autonomous vehicles, such as tractors, mobile robots, self-driving vehicles and drones in order to remove the worker from the risk area.

5 CONCLUSION

A qualitative study which analyses all accident reports of serious and fatal accidents caused by mobile machinery in the province of Quebec was carried out. Considering mobile machinery as a group of machines allowed targeting specific issues as well as comparing them to stationary machinery.

With an annual average of more than 18 fatalities, mobile machinery caused more accident than stationary machinery in Quebec. Moreover, since 2006, the downward trend in the number of victims in Quebec for stationary machinery is not seen for mobile machinery. In spite of the fact that mobile machinery cause 25 % of work-related fatalities in Quebec, it is often not perceived as hazardous as stationary machinery. As such, mobile machinery is often excluded by companies during risk assessment and control of hazardous energy methods. This confirms once again the need for prevention for this group of equipment in Quebec.

The main accident types identified for regular operation activities with mobile machinery are (i) forward, backward or sideways movement of the equipment, (ii) equipment rollover/tipover and (iii) the fall or movement of the load. The main accident types identified for maintenance activities performed on mobile machinery are (i) fall of equipment, or equipment part, from a height (29%), (ii) a moving part of the equipment (28%) and (iii) a moving vehicle (19%). Ignorance of the risks, lack of supervision, inexistent/unsafe work procedures are the main causes identified.

As it was discussed, the problem seems to lie mainly in the non-application of existing prevention principles. Mobile equipment, as a group, should be targeted by labor inspectors and companies in Quebec as it was done for stationary machinery 10 to 15 years ago. Driving, lifting, environment, trip and fall and maintenance issues should be addressed in priority. Other countries seem to have the same issue (e.g., the U.S., Australia). Therefore, more research is still needed in the integration of existing technologies in real applications.

6 REFERENCES

1. European Parliament and the Council of the European Union, 2006. Machinery directive 2006/42/EC. Official Journal of the European Union, Brussels.
2. Marsh S.M., Fosbroke D.E., 2015. Trends of fatalities involving machines, United-States, 1992-2010. *American journal of industrial medicine*, 58(11), 1160-1173.
3. Safe Work Australia, 2015. Work-Related Traumatic Injury Fatalities, Australia, 2014. Safe Work Australia, Canberra, Australia.
4. DeGroot J.M., Isaacs C., Pickett W., Brison R.J., 2011. Patterns of fatal machine rollovers in Canadian agriculture. *Chronic diseases and injuries in Canada*, 31(3), 97-102.
5. Franklin R.C., Mitchell R.J., Driscoll T.R., Fragar L.J., 2001, Agricultural work-related fatalities in Australia, 1989–1992. *Journal of agricultural safety and health*, 7(4), 213-227.
6. Kumar R., Ghosh A.K., 2014. The accident analysis of mobile mine machinery in Indian opencast coal mines. *International journal of injury control and safety promotion*, 21(1), 54-60.
7. McCann M., Cheng M.T., 2012. Dump truck-related deaths in construction, 1992–2007. *American journal of industrial medicine*, 55(5), 450-457.
8. Thelin A., 2002, Fatal accidents in Swedish farming and forestry, 1988–1997. *Safety science*, 40(6), 501-517.
9. Chinniah Y., Burlet-Vienney, D., 2013. Study on lockout procedures for the safety of workers intervening on equipment in the municipal sector in Quebec. *International Journal of Occupational Safety and Ergonomics*, 19(4), 495-411.
10. Chinniah Y., 2015. Analysis and prevention of serious and fatal accidents related to moving parts of machinery. *Safety science*, 75, 163-173.
11. CNESST - Commission des normes, de l'équité, de la santé et de la sécurité du travail, 2018. [Online]. Available at <http://www.centredoc.csst.qc.ca/zones/> (Jan., 2018).
12. CNESST - Commission des normes, de l'équité, de la santé et de la sécurité du travail, 2016. Rapport annuel de gestion 2015 [2015 Annual management report]. Montréal, CNESST.
13. Quebec Government, 2017. Regulation respecting occupational health and safety (ROHS, c. S-2.1, s.223). Québec, Éditeur officiel du Québec.
14. Canadian Standards Association, 2015. CSA B335-15: Safety standard for lift trucks. Mississauga, ON.
15. American National Standard Institute, 2012. ANSI Z245.1-2012: Mobile Wastes and Recyclable Materials Collection, Transportation, and Compaction Equipment - Safety Requirements. Washington, ANSI.
16. European Committee for Standardization, 2011. CEN/TR 614-3:2011: Ergonomic Principles for the Design of Mobile Machinery. Brussels, CEN.
17. Institut National de Recherche et de Sécurité (INRS), 2015. Prévenir les collisions engins-piétons – La place des dispositifs de détection et d'aide visuelle. INRS, technical guide, ED6083, Paris, France.
18. Teizer J., Allread B.S., Fullerton C.E., Hinze J., 2010. Autonomous pro-active real-time construction worker and equipment operator proximity safety alert system. *Automation in Construction*, 19(5), 630-640.
19. Burlet-Vienney D., Chinniah Y., Aucourt B., 2017. Safe Maintenance Work on Mobile Equipment - Issues and Recommendations, *Professional safety*, 62(12), 26-32.

Safety Assessor Qualification Impact and Influence in Thailand

Patiphon K.¹, Hiroo K.²

¹ Technology Promotion Association (Thailand-Japan)(TPA) -- 534/4 Soi Pattanakarn 18, Pattanakarn Rd.,
Suanuang - Bangkok – Thailand

² Nippon Electric Control Equipment Industries Association(NECA) -- 1-17 Hamamatsucho 2chome Minato-ku
- Tokyo - Japan / Mitsubishi Electric Corp. -- 8-1-1 Tsukaguchi-Honmachi Amagsaki - Hyogo – Japan

Patiphon@tpa.or.th
Kanamaru.Hiroo@db.MitsubishiElectric.co.jp

KEYWORDS: safety assessor qualification, risk assessment, safety officer, personnel competency

ABSTRACT

In order to design a safety machine compliant with ISO/IEC safety standards, a safety engineer who well understands these standards shall be needed. For training the safety engineers and designers, the Safety Assessor Qualification (SAQ) system had been developed in Japan in 2004. Over 10 years operation of the system and its effects have been well-known to the world. And some countries would introduce the SAQ and operate by themselves. Technology Promotion Association (TPA) in Thailand started a project to transfer SAQ system from Japan in 2013, and operated it from 2016. Today, there are 768 qualifications as SBA, and 16 qualifications as SSA in Thailand. However, to achieve reasonable occupational safety and health level in Thailand, we would have more professional qualifications. To increase SAQ person, we analyze the impact and influence of SAQ in Thailand with questionnaires from qualifications. In this paper, we would describe about the result.

1 INTRODUCTION

Many countries promote to design industrial machines compliant with ISO/IEC safety standards in their occupational safety and health policies. For example, EU machinery directive (2006/42/EC) requires that a machinery installed in EU shall comply to ISO 12100 etc. For that purpose, professional persons who understand such machinery safety standards are needed. Only they can design and install a safety machinery objectively. NECA (Nippon Electric Control Equipment Industries Association) has developed SAQ (Safety Assessor Qualification) system and has started to operate the system in 2004 to develop such professionals [1]. During 15 years experiment, we have over 15 thousands qualified personnel. And many industrial companies in Japan have introduce SAQ in order to install safety machines. Today, SAQ of NECA is the most famous safety training system in the world [2].

As a result of this success of Japan, Asian countries would like to introduce SAQ to their own countries. Thailand which has large machinery industries related to automobiles faces to emergency problems of safe and automated manufacturing against the increasing labor costs. Therefore, TPA (Thailand-Japan Technology Promotion Associates) has started a project to transfer SAQ from Japan to Thailand in 2013, and has operated SAQ in 2016 [3]. The main mission was to develop native safety instructors including interpretation textbooks and materials in training. Today, we have 784 qualified personnel in 195 companies in Thailand.

Whether SAQ will be stable in Thailand or not? It is depend on the success of qualified personnel in Thailand. Thus, we have researched interviews to them what their activities related machinery safety in their factory. The results shows that their risk assessment of machines are useful and effective for safety factory, and the managers are understand their acclivities.

This paper would describe that the circumstance of the transferring SAQ from Japan, and describe the results and analysis of interviews from qualified personnel in Thailand.

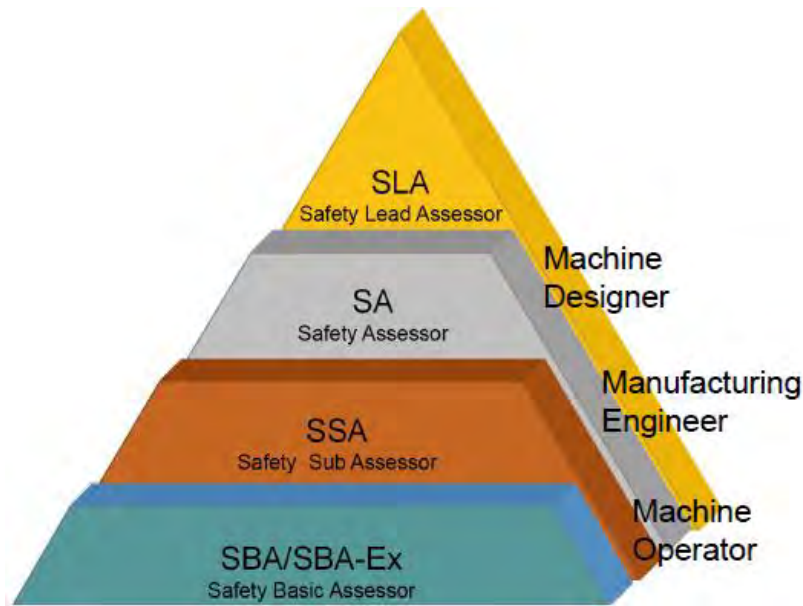


Figure 1. Structure of SAQ.

2 SAFETY ASSESSOR QUALIFICATION

In former Japan, safety measures in factories were based on attention of field workers, and technical measures were not taken into consideration. Later, as overseas factory construction progressed, machinery engineers began to be required to design safe machines conforming to ISO/IEC international standards. However, since these standards related to machine safety are enormous, they needed a systematic educational program to learn these safety technology.

Therefore, in order to train personnel capable of designing safe machines based on international standards, NECA developed the SAQ system. The composition of the SAQ system is shown in Figure 1. SAQ consists of SBA (Safety Basic Assessor) for a machine operator, SSA (Safety Sub Assessor) for a manufacturing engineer, SA (Safety Assessor) for a machine designer and SLA (Safety Lead Assessor) for an objective safety evaluator. This system has been in operation since 2004, and currently almost 15,000 people have SA related qualifications. Figure 2 shows the trend of increasing qualifiers [4]. It is the world's most successful safety personnel certificate, with 14 years of experience.

The Japanese Ministry of Health, Labor and Welfare (MHLW) requires machine providers to create residual risk maps that illustrate the dangers of machines and notify users. In addition, MHLW requires that those who create this residual risk map have knowledge of risk assessment, risk reduction and related laws and regulations [5]. Since the SAQ curriculum contains these three knowledge fields, MHLW considers SAQ qualifiers to be capable of creating machine residual risk maps. With government approval, the SAQ qualified persons are increasing more and more in Japan.

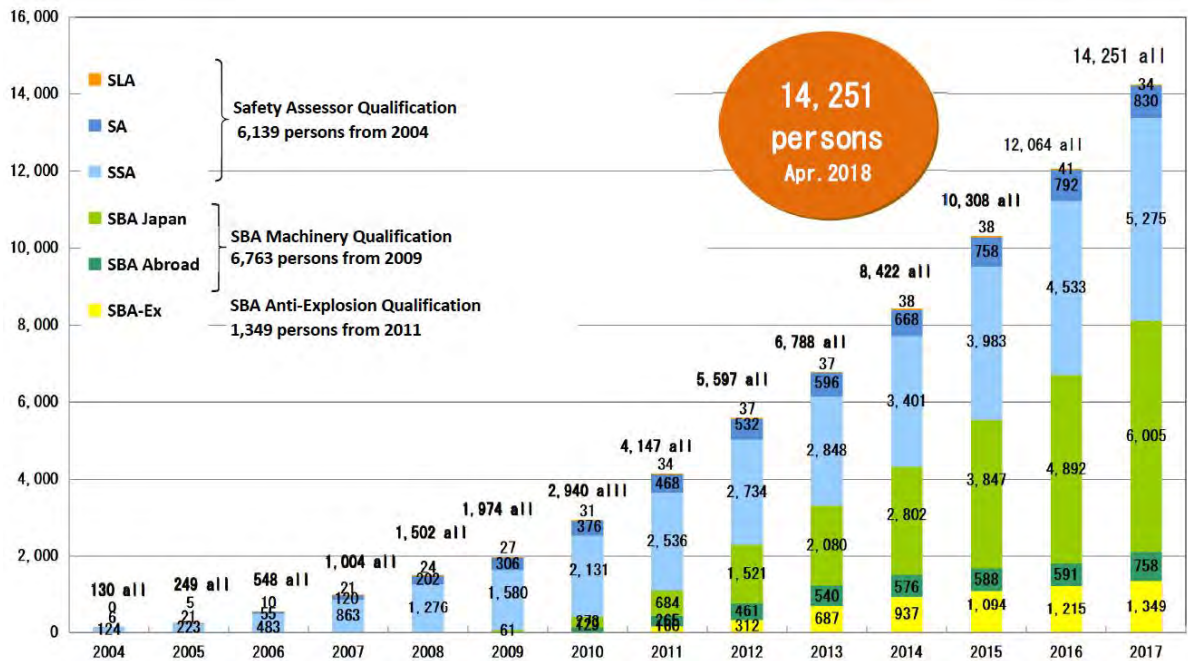


Figure 2. Trend of SAQ persons (excluding the qualified by TPA).

Companies that introduced SAQ tried to introduce it not only in Japan but also overseas factories. In general, SAQ can be used in all countries because safety regulations of each country are technical based on international standards. Therefore, Japanese companies proactively advanced overseas deployment of SAQ. Figure 3 shows the number of SAQ qualifications in East Asia. However, these qualifiers received a test sent in Japan or from Japan. Because there were still no countries that operated the organized SAQ system.

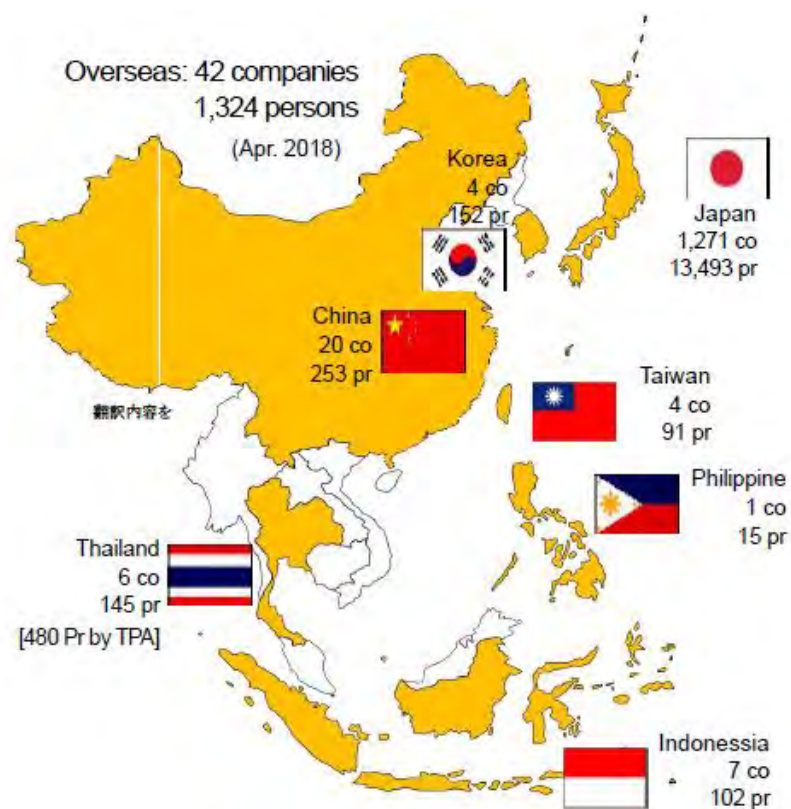


Figure 3. SAQs in Asian countries.

3 TRANSFERRING SAQ TO THAILAND

Thailand is the largest machine-industrialized country in Southeast Asia and has a machinery industrial area mainly in the automobile industry around Bangkok. The past time, Thai government had implemented policies aimed at industrial promotion rather than occupational safety and health. Therefore, occupational accidents had remained high as shown in Figure 4 [6]. However, the government and companies become involved in occupational health and safety as important because of human resources shortage by dueing to the development of industry.

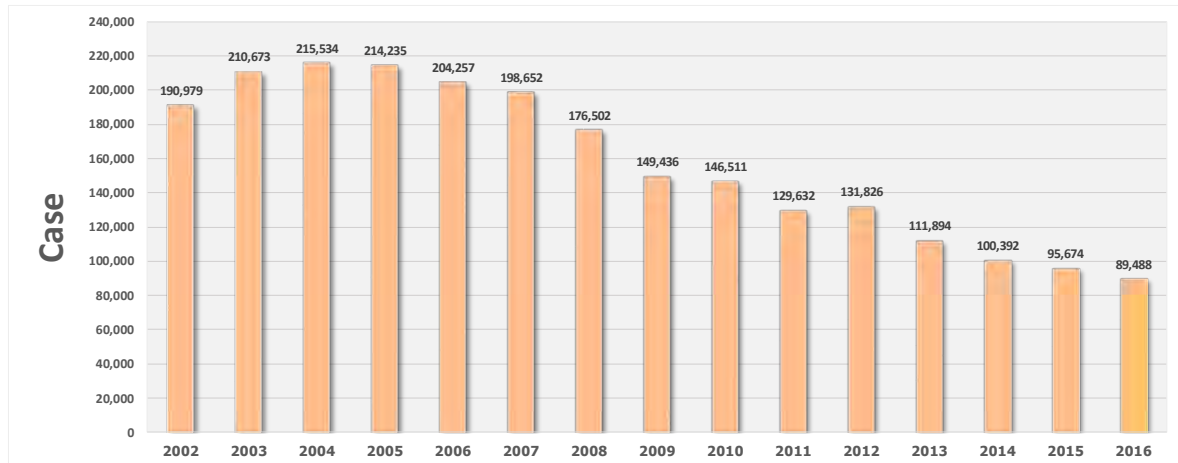


Figure 4. The trend of occupational accidents in Thailand.

The Thai government enacted the Occupational Safety and Health Law and the TIS 18000 Occupational Safety and Health Management Standard in 2011. Each company appoints a safety officer and promotes the introduction of occupational safety and health management.

However, the safety officer faces a problem when implementing safety measures for factory equipment and machinery. There is no safety engineer who can know which part of the machine is dangerous and what kind of counter measure should be given if it is appropriate. The safety officer is an administrator, not a engineer. Indeed, there are few safety engineers familiar with the ISO / IEC international safety standards in Thailand. Cooperation between a safety officer and a safety engineer is needed for safety of factory facilities.

Therefore, in 2013, TPA (Technology Promotion Association (Thailand-Japan)), which has developed curriculum of manufacturing and maintenance in cooperation with Japan, started the project of transferring NECA's SAQ system to Thailand. This project was implemented with expert dispatch from AOTS (The Association for Overseas Technical Cooperation and Sustainable Partnerships) under the support of the Ministry of Economy, Trade and Industry of Japan [7].

First, TPA selected instructors candidates from the staff, and SAQ experts in Japan taught them the concept and technology of machine safety. Next, in cooperation with each other, they translated SAQ textbooks used in Japan and modified them according to laws and circumstances in Thailand. Because there was no ISO / IEC machine safety standards written in Thai, translation had taken time. Thai language slides for lectures were created based on translated textbooks by candidate instructors. The lectures are SBA for 1 day, SSA for 3 days and SA for 2 days. The lecture also includes exercises on risk assessment and guard design. Finally, Thai lecturer candidate rehearsed inside TPA using their textbooks and slides created, and Japanese experts advised to them. In addition, exam questions and scoring procedure were also prepared by Japanese experts, and confirmed by candidate instructors taken the examination.

The SAQ transferring project was begun in 2013. In 2015, TPA announced the start of the SAQ system in Thailand, and in November TPA conducted the first training and tests. Subsequently, SSA was started in February 2017, SA was started operation in 2018[8]. However, plans to implement SLA in Thailand are undecided.

As of September 2018, TPA qualified persons are SBA 768 people, SSA 16 people and SA 0 people. Especially, because there are many applicants for SBA as the first step of SAQ, instructors often visit to the customer's site and conduct lectures and tests.

4 IMPACT AND INFLUENCE BY SAQ

In order to know what kind of safety contribution SAQ qualifiers contribute to each company, we conducted a questionnaire survey on them. From the responses of 62 company, 62 person qualified person, the following was obtained.

- Machine risk assessment implemented = 75%
- Implemented risk reduction measures on machinery = 75%
- Would to increase SAQ qualified persons in the future = 100%

Even though the SBA / SSA system has been until two years, 75% of the safety qualified people are contributing to the safety of machines in their workplaces. In order to construct a safe machine, risk assessment and risk reduction according to ISO 12100 etc. are important. The qualified persons have shown that the training they had was effective and practical. In addition, a management of each company understands this and wants to increase safety qualified people. Moreover, from the interview results, it was also found that the automobile industry has a strong interest in SAQ.

We describe an example where SSA conducted a risk assessment on existing facilities in the factory. Prior to having a qualified person, this company had conducted risk assessment on all 688 machines in his factory. When SSA conducted the risk assessment again, there were 4,284 issues pointed out. Table 1 shows the number of issues for each risk level. The qualified person performed counter measures according to safety standards. However, since Level III and above are insufficient only with complementary measures, only authorized workers can operate the work.

Table 1. Issues pointed out by risk assessment.

Risk Level	Number of issues
I	2,186
II	2,050
III	30
IV	18

Another company also conducted a risk assessment, and 53 issues were pointed out, of which 32 critical items were subjected to safety measures. As a result, the number of accidents occurred before and after countermeasures was reduced by 22.2%. We would like to continue to check whether this number is temporary or continually decreasing.

5 CONCLUSION

TPA had transferred SAQ from Japan to Thailand, and had started operation. We have 784 qualified person in Thailand. According to their questionnaire results, they have carried out risk assessment on machines in their factories, and applied appropriate safety measures compliant with standards. In addition, managers of their companies recognize that the safety qualified person is beneficial, have a good effect on the safety of the factory, and has a positive impact on other employees. Therefore, almost companies want to increase the safety qualified persons.

Only two years experiment in Thailand, a role and value of SAQ are recognized in manufacturing industry. We would like to promote SAQ towards the introduction of machinery safety by continuously investigating qualified personnel.

6 REFERENCES

1. NECA0901 - *Standard for certification of safety assessor*, Nippon Electric Control Equipment Industries Association, 2014.

Session 6 – Experiences / Practical applications

2. Toshihiro Fujita, etc., *Current situation of safety assessor and safety basic assessors (SA/SBA) qualification system: Reduction of accidents achieved by a Japanese company and recommendation by Japanese Ministry of Health, Labor and Welfare*, Proceedings of SIAS 2015.
3. Patiphon Koompai, Hiroo Kanamaru, *Start up Safety Assessor Qualification to Educate Safety Engineers in Thailand*, Proceedings of SIAS 2015.
4. *Introduction of the Safety Assessor Qualification*, Japan Certification, 2017.
5. *The guideline for the promotion of notification hazards of machines by machine venders*, Notification No.132-2012 Ministry of Health, Labour and Welfare, Japan.
6. *OSH accident report*, Thai Gov.
7. TPA seminar 2015.
8. TPA SAQ leaflet.

Framework for Occupational Safety and Health: the eSocial

Kieckbusch R.-E.¹, Santos A.-C.²

¹ National Confederation of Industry - Brazil (CNI) – SBN - Quadra 1 - Bloco C, Ed. Roberto Simonsen, Brasília – DF, CEP 70040-903 - Brazil

² Brasilia University (UnB) – Universidade de Brasília- UnB - Faculdade de Tecnologia - Núcleo de Engenharia de Produção - Campus Darcy Ribeiro Asa Norte - Brasília DF, CEP 70904-970 - Brazil

rkieck@cni.com.br
andreasantos@unb.br

KEYWORDS: labor law, social security, occupational health and safety, information system, eSocial

ABSTRACT

Since 1970, the Brazilian government has promoted changes in legislation in order to impose on companies to reduce workplace accidents. During this period, work accidents decreased from 147.4 per thousand workers to 12.5 in 2016. Until then, the obligations imposed by the government were for specific areas of companies, lacking a systemic view of the business. Labour information (contract of employment, occupational hazards in the workplace, etc.), social security (compulsory charges, accident insurance, etc.) tax on the hiring and use of labour by were passed on to different supervisory boards and control by different functional areas of business. Currently, there is provision of duplicate data, the need for separate deliveries controls, regulatory conflicts between government regulatory agencies and the use of paper forms. In 2013, government organizations announced a new joint initiative called eSocial. The eSocial is to establish a single electronic form, that is, initiatives and legal obligations implemented in recent decades would become unified and provided in electronic form by the companies in a single platform. The purpose of this article is to present a framework of information system for occupational health and safety (eSocial). To build the framework interviews have conducted with companies, organizations of employers and workers, specialists, developers of software management, promoted meetings and discussions with government entities. As a means of validation, a deployment case study has conducted in a large company that has demonstrated the importance of redesigning business processes, definition of monitoring indicators, the role of leaders and managers, as well as their responsibilities, and the adoption of an integrated approach between functional areas of safety and occupational health. The forecast of mandatory eSocial will be from 2018, involving five government agencies, where 7 million companies will submit data on occupational health and safety of 48 million workers.

1 INTRODUCTION

Brazilian labor legislation (CLT) covers the urban and rural private sector, published by Decree-Law 5,452 / 1943 (Brasil, 2018). The public sector, on the other hand, has its own legislation and is less comprehensive than the private occupation health and safety (OSH) legislation. Since 1943 the issue of occupational safety and health (OSH) has been addressed in private employment contracts.

However, in 1977 the OSH CLT chapter was reformulated and expanded. The following year, in 1978, a total of 28 occupational safety and health standards regulations were published. During this period, work accidents decreased from 147.4 per thousand workers to 12.5 in 2016 (Ministério da Fazenda, 2016). Until then, the obligations imposed by the government were for specific areas of companies, lacking a systemic view of the business.

Unfortunately, the systemic view of the implementation of new obligations imposed by the government has been lost. Registration of information on labor contracts, occupational risks, social protection, labor rights, etc., has been managed by independent government departments. As a result, the labor information (contract of employment, occupational hazards in the workplace, etc.), social security (compulsory charges, accident insurance, etc.) tax on the hiring and use of labor by were passed on to different supervisory boards and control by different functional areas of business. Currently, there is provision of duplicate data, the need for separate deliveries controls, regulatory conflicts between government regulatory agencies and the use of paper forms. In terms of employment contracts, Brazilian labor legislation intersects with the tax, social security and labor accident insurance legislation. An expressive part of the federal government's tax collection comes from payroll taxes.

In order to reduce bureaucracy and duplicity of information submitted by employers, the federal government announced a new joint initiative called eSocial. The eSocial is to establish a single electronic form, that is, initiatives and legal obligations implemented in recent decades would become unified and provided in electronic form by the companies in a single platform.

The purpose of this article is to present a framework of information system for occupational health and safety on eSocial. For this, as a research problem to be answered are the minimum requirements related to occupational health and safety that must be electronically routed by companies through eSocial and that ensure that workplaces have the minimum conditions set forth in Brazilian regulatory standards.

To build the framework interviews have conducted with companies, organizations of employers and workers, specialists, developers of software management, promoted meetings and discussions with government entities. As a premise for the construction of the framework, the interviewees informed that the framework should conform to the current and dynamic patterns of work safety, so that they incorporate and value the technological innovations available to offer the maximum degree of safety to the workers. Thus, it is necessary that the framework is technically, financially feasible and balances the obligations imposed on the companies and the protection to the worker.

This article is structured in five sections, in addition to the introduction. The second section briefly describes the methodology adopted, followed by the section that addresses the eSocial model in Brazil. The fourth section the discussions that occur in the work groups and the fifth presents the framework developed. At the end the conclusions and the bibliography.

2 METHODOLOGY

Methodologically the article is based on the elaboration of a case study, based on the survey of the minimum requirements present in Brazilian safety and health legislation and the application of the proposed framework in a large steel company. For Gil (2008), the scientific research does not provide explanations containing value judgment, but rather testable data from the presented variables. However, the issues raised in the case study start from a pre-existing context: a) Brazilian occupational safety and health legislation; (b) replacement of existing legal obligations; c) integrate requested data to employers by government departments.

A case study was carried out at a manufacturing located in Ipatinga-MG (Brazil), with approximately six thousand employees, with the participation of occupational health, information technology and human resources teams. The application of the case study occurred in 2018, based on the discussions that were carried out in the occupational safety and health working group that began in 2016. At the end of the process, all considerations were presented to the government's staff as a subsidy for the construction of the framework of occupational health and safety.

3 ESOCIAL ARCHITECTURE

In 2013, five government departments announced a new joint initiative called eSocial. The five departments are Ministry of Labor, Social Security Department, Federal Revenue, National Social Security Institute and FGTS (labor guarantee fund). The eSocial is to establish a single electronic form, that is, initiatives and legal obligations implemented in recent decades would become unified and provided in electronic form by the companies in a single platform. eSocial's emphasis on the provision of labor, social security, tax and tax information regarding the hiring of labor and the use of labor onerous, with or without employment relationship. In addition to other information provided for in the social security legislation. The objective is to (Brasil, 2014):

- Enabling the guarantee of social security and labor rights to Brazilian workers;
- Simplify compliance with obligations; and
- Improve the quality of information on labor, social security and tax relations.

The eSocial architecture consists of adopting the eXtensible Markup Language (XML) protocol with the use of digital certification and unique identifiers of employers and workers (Brasil, 2018c). Figure 1 shows the communication scheme between employers and the national environment. Each employer generates the data in the XML protocol, according to specific layouts, and sending it to the national environment (eSocial). Each submission is validated the identification of the employer and the identification of each employee in the Federal Revenue and Social Security databases. With this, a confirmation of delivery protocol and confirmation receipt of processing by the national environment are returned to the employer. The five government departments take the data stored in the national environment. Each employer is required to have all data stored in an owner information system and communication takes place by the Internet.



Figure 1. Relationship between Employers, National Environment (eSocial) and Government Departments.

The architecture is designed to work with specific layouts grouped into:

- a) **Organization of the company:** set of standard business data, such as positions and functions of employees, working hours, payroll, etc.;
- b) **Legal and natural persons:** identification of each locality of the company, as well as the identification of each of the employees in the standard adopted by the Federal Revenue and Social Security;
- c) **Working life of workers:** each stage of the employee's working life in the company, such as admission, dismissal, work contract, occupational safety and health, etc.;
- d) **Labor remuneration:** information about the payroll, that is, how much each employee received of salary, paid of taxes and contributed to the social security.

eSocial's information technology is completely different from the current information systems adopted by the government to obtain data from employers. The current technology is more than 30 years old and only covers a small part of the scope of eSocial. Only data on workers' compensation, taxes and social security contributions are forwarded. The last major system information update by the government happened in 1999.

Based on the scope of the eSocial, the five government departments have defined a target set of legal obligations that are replaced. The base began with the records of labor contracts, payroll and data that employers are already required to send to any of the government departments involved. It was also opted for the substitution of labor and social security obligations associated with occupational health and safety. In all, approximately, twelve obligations began to compose eSocial.

A second point has also been defined. The strategy of updating and identifying the unique records of Brazilian workers. Unfortunately, each of the five departments had its own worker identification codes. After two years of initiation of the record update for the unification, approximately 90% of Brazilian workers are with the updated registers and the databases among the five synchronized departments. It is expected to reach 100% when the full implementation of eSocial will be completed by the end of 2019.

With the initial scope of obligations to be replaced by eSocial defined, the five government departments invited a group of the 100 largest Brazilian companies to join a working group with the government. This group was established in 2014 and has since contributed to the refinement of layouts that will replace legal obligations. In 2018 eSocial began to be deployed in the largest Brazilian companies and the forecast is that by the end of 2019 all employees will be covered by eSocial.

4 EMPLOYERS' WORKING GROUPS AND THE GOVERNMENT DEPARTMENTS

The first initial proposal of the five government departments was to start implementing the eSocial in 2015. The establishment of the working group with the largest Brazilian employers initially had the proposal to monitor the implementation of eSocial. However, it was realized that the complexity and difficulties of starting a huge project. It was clear that the initial scope proposed by the government needed to be revised. With strong resistance from members of government departments, based on discussions with the working group, it was decided to separate the project into two groups. The first group would follow the theme linked to payroll and the second the theme of occupational health and safety. Each group has the participation of the government departments members.

In order to facilitate the process of communication and conduction of the discussions in the two working groups, a technical confederation group (GT) was formed. The GT is composed of the main employer's organizations, information technology entities and the responsible for each of the five government departments involved. This group has the objective of monitoring the implementation and defining the priorities. From 2015 to June 2018, 25 follow-up meetings were held.

During the years of 2015 and 2016 the entire description of payroll layouts was redesigned by first group. The discussions with the companies participating in the working group demonstrated a different reality when it is intended to combine in a single channel countless law (labor, social security and tax). The target was nearly 7

million businesses and nearly 48 million active labor contracts. In early 2017 the new payroll layouts project was ready.

The second group involved in occupational safety and health had a different path. It started from the need to build a specific information system framework for occupational health and safety within eSocial. To build the framework have conducted interviews with companies, organizations of employers and workers, experts, developers of software management, promoted meetings and discussions with government entities.

The main challenge was to build a framework that would allow the digitization of the occupational health and safety areas of companies. In almost all the application forms were sent to the government on paper by the companies. As a means of validation, a deployment case study has conducted in a large company that has demonstrated the importance of redesigning business processes, definition of monitoring indicators, the role of leaders and managers, as well as their responsibilities, and the adoption of an integrated approach between functional areas of safety and occupational health.

During the process of building the framework, a new labor legislation was approved in Brazil (Brasil, 2018b). Basically, new types of employment contracts were allowed. Another point was the permission of unrestricted outsourcing. Elements of the European Directive 89/391/EEC dealing with the implementation of measures to promote the improvement of the safety and health of workers at work have also been incorporated into the Brazilian legal system.

5 FRAMEWORK FOR OCCUPATIONAL SAFETY AND HEALTH: THE ESOCIAL

The occupational health and safety framework adopted at eSocial focuses on the identification of occupational hazards factors at the workplace, individualized appointment by employee, and employee health monitoring. It should be noted that the five sets of risk factors recognized in Brazilian legislation are physical, chemical, biological, ergonomic and accident risks (Rodrigues, 2011). The entire health worker monitoring rule, as well as the prioritization of risk factors, follows the technical criteria present in Brazilian OSH regulatory standards. Based on this, Figure 2 presents the schema generated by the OSH framework in eSocial.

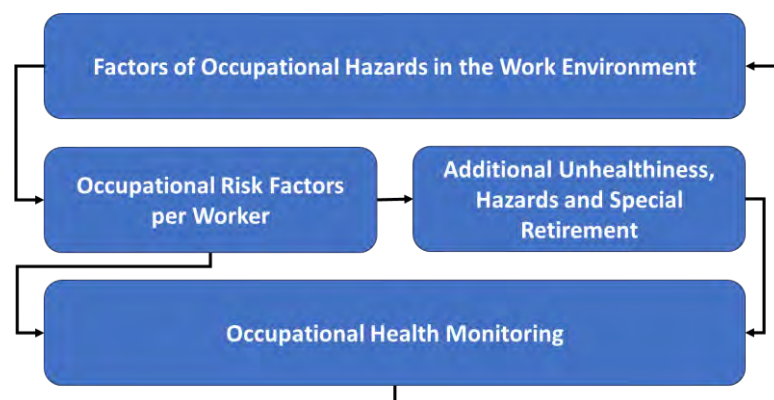


Figure 2. Framework for Occupational Safety and Health on the eSocial.

The Brazilian legislation contains two basic programs for the prevention and monitoring of workers' health in the workplace. Based on the Environmental Risk Prevention Program (PPRA), risk factors in workplaces are identified, considering the activities developed by the employees, the productive process and the economic sector of the company. In turn, the Occupational Health Medical Control Program (PCMSO) has regulations to ensure the health of work. With the combination of the two, it is possible to identify individually the risk factors that Brazilian workers are exposed to (Ministério do Trabalho, 2018).

Unfortunately, Brazilian legislation has a particularity. It requires the payment of an additional unhealthy if a worker is exposed above the allowed limit. These additional complements the employee's salary. Other information that will become electronic refers to special retirement. Currently, the form is completed by the employer and physically referred to social security. Special retirement is the condition in which an employee is exposed to a certain risk factor and before he becomes ill, is retired early. This information is forwarded to eSocial by employers.

During the process of constructing the framework, when applying the new model proposed in a major Brazilian steel mill, it was identified the importance of redesigning the business processes, defining which indicators of occupational health and safety will be monitored, training and engagement of the leaders, as well as, their

responsibilities. Additionally, it became clear the necessary integration of the functional areas of occupational safety and occupational health is the key point. Unfortunately, with the loss of systemic vision in the updating of the regulatory norms promoted in the last years, the two areas walked different paths.

In interviews with the largest Brazilian companies, software developers and specialists from the three areas (safety, health and human resources), all defended their systems individually. However, for a better eSocial implementation, it will be necessary for Brazilian companies to have information systems that integrate the functional areas of occupational safety, occupational health and human resources. Unfortunately, we realize that this integration process will take a long time to complete.

Therefore, the beginning of the implementation of the OSH framework in eSocial will only occur in the middle of 2019 with completion expected in 2020 in the largest Brazilian companies.

6 CASE STUDY OF THE DEVELOPED FRAMEWORK

In operational terms, each Brazilian company must comply with both the legislation and the occupational health and safety regulatory standards. With the adoption of the occupational health and safety framework, which meant replacing three legal obligations, data are sent to each eSocial every month. In practical terms, there was a 33% increase in the amount given, however, there was an improvement in the specification of these data. Previously, the fields in the paper forms were free and, in the electronic case, the unit of measurement, standardized tables of risk factors, standardization of worker identification, etc., were required.

In order to send the data electronically, it was necessary to redesign the company's internal business processes, integrating the functional areas of human resources, work safety and occupational health. The challenge of developing new procedures so that everything is always up to date. For every month, the company needs to check if there is any alteration and, if it exists, to communicate electronically to eSocial.

Figure 2 highlights the occupational risk factors for work environments. In the case of the company were organized the almost 6 thousand employees in approximately 2 thousand places of work. As a result, there was an operational difficulty in simultaneously managing the business process and eSocial. From the discussions in the working group, there was a simplification in the concept of work environment. Thus, of almost 2 thousand environments, the company has only 5. Approximately 150 items have been revised, excluded and / or simplified in the legal obligations with the entry of the eSocial framework.

Brazilian legislation requires that, by employee, the occupational risk factors that are subject in the work environment be indicated. In addition, follow-up of the health of the worker. This data is also electronically routed to eSocial. Each data, before the eSocial, was individually recorded by companies, without a standard and, in many cases, on paper forms. With the entry of eSocial it is expected to gain in the quality of the information and in the adoption of more appropriate management practices.

In summary, the main requirements identified for the framework based on the discussions and the application of the case study were: a) standardization of a Brazilian table of occupational risk factors; b) standardization of the concept of work environment; c) individualization per employee and per exposed risk factor; d) annotation of any deviations; e) integration of functional areas of human resources, occupational safety and occupational health. That is, with this standardizes all the documentation on the occupational health and safety of Brazilian workers.

7 CONCLUSION

One of the main obstacles encountered throughout the process was the formation of a collaborative team between the representations of the employers, the largest participating companies and the members of the five government departments. This process reached a satisfactory level of maturity after many rounds of discussions. Only the Ministry of Labor, among the five governmental entities, had experience in collective construction with the participation of society.

Another identified point is the distancing of the managerial practices of the companies and the need for regulation by the competent governmental entities. During the construction of the framework of occupational health and safety it was perceived the imposition of a bookkeeping vision of the whole process by the government representatives. The specialists and the representatives of the companies looked for all the time to focus on the indicators and the results that one wishes to achieve. Unfortunately, this vision comes from a loss of systemic vision of the norms of safety and health at work adopted in Brazil.

It became clear the need to redesign the business processes of companies from the inside out. That is, the technical teams of the companies began to revisit the labor and social security legislation proposing new business processes for the management of their operations. Bringing ready-made solutions based on the current software vision has been a waste of time. Software developers have also returned to the drawing boards to rethink their business models.

It is expected that from 2019 a new wave of maturity will begin in Brazil in the fulfillment of legal obligations. It also includes the full adoption of new labor legislation, a more modern view of occupational risk management and the opening of a review of regulations that integrate a systemic view.

8 REFERENCES

- Brasil. Decreto que institui o Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas - eSocial e dá outras providências, 2014. Accessible in: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/decreto/d8373.htm. Date: 13/09/2018.
- Brasil. Consolidação das Leis Trabalhistas, 2018. Acessível em: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del5452.htm. Data: 13/09/2018.
- Brasil. Moderniza a Consolidação das Leis do Trabalho, 2018b. Accessible in: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13467.htm. Date: 13/09/2018.
- Brasil. Manual de Orientação do eSocial (versão 2.4), 2018c. Accessible in: <http://portal.esocial.gov.br/manuais/mos-manual-de-orientacao-do-esocial-2-4-publicada.pdf/view>. Date: 13/09/2018.
- GIL, Antônio Carlos. Métodos e Técnicas de Pesquisa Social. 6. ed. São Paulo: Atlas, 2008
- Ministério da Fazenda. Secretaria de Previdência, Anuário Estatístico de Acidentes do Trabalho, 2016.
- Ministério do Trabalho. Normas Regulamentadoras Brasileiras. Accessible in: <http://www.trabalho.gov.br/seguranca-e-saude-no-trabalho/normatizacao>. Date: 13/09/2018.
- RODRIGUES, Celso Luiz Pereira. Conceitos Básicos Sobre Segurança do Trabalho. In: MATTOS, Ubirajara; MÁSCULO, Francisco (Orgs.). Higiene e Segurança do Trabalho. Rio de Janeiro: Elsevier/Abepro, 2011. p. 35 - 49.

Analysis of 139 serious and fatal machine accidents occurring in Quebec between 2011 and 2015

Giraud L.¹, Desmarais L.², Hébert R.², Cadieux J.²

¹ Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST) – 505, boul. De Maisonneuve Ouest – Montréal (Québec) – H3A 3C2 – Canada

² Université de Sherbrooke – École de Gestion – 2500, boulevard de l'Université – Sherbrooke (Québec) - J1K 2R1 – Canada

giraud.laurent@irsst.qc.ca
lise.desmarais@usherbrooke.ca
rachele.hebert@usherbrooke.ca
jean.cadieux@usherbrooke.ca

KEYWORDS: Maintenance, Accident Analysis, Machine Safety, Task Performed

ABSTRACT

Accidents involving machines (3,552 in 2011, excluding the construction industry) and resulting in fatalities (7 in 2011) are still quite common in Quebec, although their numbers have been declining for several years. These accidents occur during all phases of the machine life cycle, from initial installation to dismantling, but especially during the main phases that are machine use and machine maintenance, as well as during transitional phases, such as commissioning, shutting down or restarting.

To prevent accidents with machines, it is necessary to know what the different causes are, at what time the accidents occur and what tasks are being performed at the time they occur. With the statistical data currently available in Quebec, however, it is impossible to know what task was being performed at the time of the accident. As a result, it is impossible to differentiate between accidents that occur during production use of the machine and those that occur during machine maintenance. To compensate for this lack of data, research is currently being conducted on accidents that occurred between 2011 and 2016 in Quebec in five sectors: forestry and pulp and paper, mining, agriculture, metal products manufacturing and transportation equipment manufacturing.

A total of 2,053 accidents were identified, along with 139 reports of serious and fatal accidents that occurred between 2011 and 2015 involving machines in all sectors. The reports concern accidents that occurred not just with stationary or immobile machines (e.g., towers), but also with mobile temporarily fixed machines (e.g., rock drilling machines with wheels) and mobile machines (e.g., forklifts).

This article focuses on the 139 accident reports, which were analysed both statistically (number, occurrence, etc.) and textually (presence of certain terms in the investigation report, vocabulary used, etc.). In total, 61 accidents were linked to production tasks, while 32 were linked to maintenance work and 36 to production continuity tasks (unblocking, breakage, raw material quality, etc.). In addition, 6 accidents were classified as fortuitous, i.e., the injured person did not habitually work with the machine or was not usually in the area of the accident-related machine, 3 were classified as machine installation accidents and 1 as a machine dismantling accident.

We hope that the results of this study will help focus and guide future prevention efforts according to the stages in the machine life cycle (installation, use, maintenance, etc.).

1 INTRODUCTION

For the 2011 calendar year, Quebec's Commission des normes, de l'équité, de la santé et de la sécurité du travail (CNESST) recorded 3,552 machine accidents, not including the construction industry, and 7 machinery-related fatalities. Some 800 accidents were caused the same year by moving parts [1].

A number of studies [2, 3, 4, 5, 6] note that accidents that occur during machine maintenance are different from those that occur during routine machine use. To gain a better understanding of how these machine accidents occur and especially to determine what phases of the machine life cycle are associated with them, the IRSST began a study in 2014 [7]. The purpose of the study was to compare machine accidents that occur during production use with those that occur during machine maintenance, based on five separate sources of information: injured workers, companies, worker compensation data (costs, length, permanent consequences, etc.) from the organization

responsible for insurance (the CNESST), CNESST public reports on serious and fatal accidents, and CNESST inspection reports.

This paper focuses solely on an analysis of the public reports on serious and fatal accidents.

2 METHOD

2.1 CNESST public reports on serious and fatal accidents

CNESST inspectors regularly investigate serious and fatal accidents to identify accident causes and circumstances.¹ When an investigation has been completed, a public report containing the following information is published:

- A description of the facts of the accident
- A description of the consequences suffered
- An analysis of the causes of the accident
- Requirements regarding hazardous situations to be corrected and, if necessary, recommendations

The investigation report helps to raise employer and worker awareness of the hazards in their workplace and possible ways of eliminating or controlling them. It is therefore a powerful accident prevention tool. One of the objectives of publishing the investigation reports on serious or fatal accidents is to help prevent similar accidents in the future. To raise employer and employee awareness of the importance of taking responsibility for occupational health and safety, the CNESST makes the reports public through its documentation centre.

2.2 Accident selection

The following parameters were used to select the reports for our study: accident with a machine, with part of a machine or with a tool used to maintain the machine; accident that occurred between 2011 and 2015, inclusive. All types of machines were included: stationary or immobile (lathes, milling machines), mobile temporarily fixed (drilling rigs) and mobile (trucks) for all industries.

A total of 208 reports were identified for the targeted years, 139 of which were categorized as accidents with a machine on the basis of the report summary. Reading the actual reports enabled us to confirm the selection of the 139 cases and enter some 60 variables into a spreadsheet. The main ones were the following: case number, date, whether or not the accident was covered by the CNESST, corrective measures required by the inspector, worker's task at time of accident, cause, type of machine, energy involved and type of accident.

We separately took into account from the database a major accident (no. 1) that occurred on Thursday, November 8, 2012, and that resulted in 3 direct fatalities and 24 associated psychological injuries. The accident happened when a process was being started up again after a maintenance operation in which a programmable logic controller was replaced. We also separately took into account a second accident (no. 2), with no human injuries or fatalities, that happened on Wednesday, July 13, 2011. That accident occurred during maintenance on an extraction machine in an underground mine: the two brake actuators were deactivated for two different maintenance operations, causing the cage to drop down the shaft in the presence of six workers, who were fortunately not injured, and resulting in costly material damage.

2.3 Accident classification

We used the different times in the machine life cycle to describe the task being performed when the accident occurred. In addition to the installation of the machine, its use, maintenance and dismantling, we also added the task "continuity of production" and took into account "fortuitous" accidents and "psychological" injuries.

Continuity of production refers to "all actions, tasks, etc., that enable production of a good or service to be maintained despite problems that may arise." These actions and tasks are not production tasks, as they do not result in finished products; nor are they maintenance tasks, as they do not contribute to putting the machine back in working order.

A **fortuitous** accident is one involving a machine that is not reasonably linked with the injured person in the normal performance of his or her duties. Only six accidents were classified in this category.

¹ http://www.csst.qc.ca/prevention/enquetes_rapports/Pages/rapports_enquete.aspx, July 25, 2018.

We also searched the CNESST’s databases for cases of **psychological** trauma associated with the 139 accidents. For these searches, if a case of psychological trauma was reported in the same company, the same day as the investigated accident and if the two were connected through certain variables, then the psychological trauma was associated with the accident.

3 DATA ANALYSIS

3.1 Industries in question

We used the North American Industry Classification System (NAICS) to classify the accidents by industry (Table 1). The five industries with the most accidents were Manufacturing 35; construction 26; Agriculture, forestry, fishing and hunting 19; Mining, quarrying, and oil and gas extraction 14 and Transportation and warehousing 13. These five industries accounted for 77% of all the accidents and 77% of the injured workers when accidents no. 1 and no. 2 were included.

Table 1. Number of accidents and injured workers by industry.

NAICS code	Description	Number of accidents	Number of injured
11	Agriculture, forestry, fishing and hunting	19	22
21	Mining, quarrying, and oil and gas extraction	14	20
22	Utilities	1	3
23	Construction	26	39
31-33	Manufacturing	35	86
41	Wholesale trade	5	9
44-45	Retail trade	4	6
48	Transportation and warehousing	13	18
53	Real estate and rental and leasing	2	2
54	Professional, scientific and technical services	2	4
56	Administrative and support, waste management and remediation services	7	13
71	Arts, entertainment and recreation	2	3
81	Other services (except public administration)	6	8
91	Public administration	3	7
	Total	139	240

In six industries, no investigated accidents occurred over the five-year period (51 Information and cultural industries; 52 Finance and insurance; 55 Management of companies and enterprises; 61 Educational services; 62 Health care and social assistance; 72 Accommodation and food services).

3.2 Worker’s task at time of accident

The workers involved in the 139 accidents were classified by machine life-cycle phase as follows (Table 2).

Table 2. Number of accidents and injured workers by life-cycle phase.

Life-cycle phase	No. of accidents	% of accidents	No. of people directly involved	No. of cases psycho trauma	Total	People/accident ratio
Installation	3	2.2	3	1	4	1.33
Production	61	43.9	74	41	115	1.88
Continuity of production	36	25.9	38	21	59	1.64
Maintenance	32	23	39*	13	52	1.62
Dismantling	1	0.7	1	0	1	1
Fortuitous	6	4.3	6	3	9	1.5
Total	139	100	7	79	240	1.73

*Including 6 people not injured

3.3 Time and month of accident

The months with the most accidents were September, with a total of 20 accidents, followed by August, with 15, and then March, November and December, with 14 each (Figure 1). The months with the fewest accidents were April and June, with a total of 7 each, October with 8 and May with 9. Figure 1 shows the breakdown of accidents by seriousness (no one injured, serious, fatal or psychological) and whether or not they were covered by the CNESST.

Regarding the times the accidents occurred, 79% happened between 7 a.m. and 4 p.m. and involved 79% of the injured workers. This time of day was when most of the stationary machine accidents occurred: 85% of them happened between 8 a.m. and 4 p.m. and accounted for 87% of the injured workers. It was also when the vast majority of temporarily fixed machine accidents occurred: 90% of them happened between 6 a.m. and 3 p.m. and involved 92% of the injured workers.

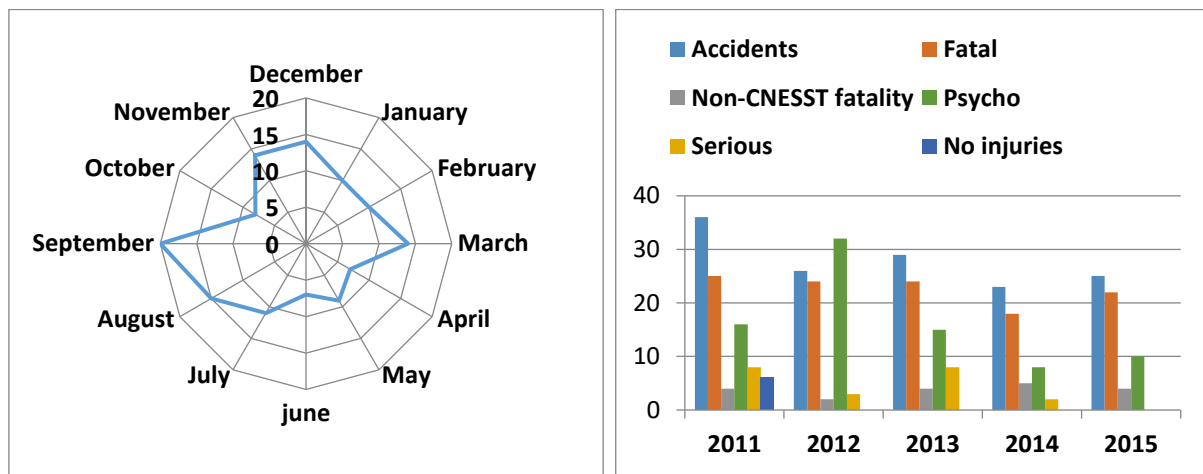


Figure 1. Number of accidents per month (left) and annual breakdown of accidents and injured workers (right).

3.4 Machine type

Stationary machines caused 26 accidents, with 36 workers directly injured and 34 suffering psychological trauma; **temporarily fixed machines** 31 accidents, with 37 workers directly injured and 12 suffering psychological trauma; and **mobile machines** 82 accidents, with 86 workers directly injured and 33 suffering psychological trauma. This includes the special case of the explosion of an extraction reactor (accident no. 1), considered to be a stationary machine, which caused 3 fatalities and inflicted psychological trauma on 24 people.

3.5 Energy involved

The forms of energy involved by type of machine for the people injured are shown in Table 3. The explosion of the extraction reactor is included under “chemical energy.” The 81 cases of psychological trauma have not been taken into account, as it was impossible to associate a form of energy with them.

Table 3. Energy involved (grouped together) by type of machine.

Energy	Stationary		Fixed		Mobile		Total	
	Acc	Ppl	Acc	Ppl	Acc	Ppl	Acc	Ppl
Electric arc + electricity	5	6	5	7	1	1	11	14
Kinetic	4	9	2	2	9	9	15	20
Mechanical and machine potential	8	8	7	7	24	24	39	39
Potential	5	6	15	19	43	46	63	71
Chemical + thermal + asphyxiation	4	7	2	2	5	6	11	15
Total	26	36	31	37	82	86	139	159

4 DISCUSSION

4.1 Psychological trauma

As some reports noted that some workers had suffered psychological trauma associated with the main accident, a systematic survey of these trauma cases was conducted using the CNESST database. The survey is incomplete, however, as it was impossible to match up many companies with a given accident, such as when a subcontractor from company A, for instance, was injured in an accident with company B. With current CNESST data, only workers from company A would be identifiable using our method. The survey is therefore only an initial general overview.

With the exception of the major accident that resulted in 24 cases of psychological trauma and 3 fatalities, 10 accidents with machinery led on average to 4 cases of psychological trauma, which means psychological trauma was the second biggest type of injury associated with the accidents. There was no statistically significant difference in the distribution of these psychological injuries by machine type.

4.2 Combining data: time, day, season and machine type

When accidents are grouped by season (winter = January, February and March, and so on), statistically significant differences can be seen with respect to machine type. With a confidence level of 95%, a significant relationship can be said to exist between machine type and season:

- For stationary machines, fall accounts for 50% of injured workers.
- For temporarily fixed machines, there are proportionally more workers injured in the spring than in the other seasons.
- For mobile machines, there are fewer injured workers in the spring, but more in the summer.

When accidents are grouped by the time they occur (6–8:59 a.m.; 9–11:59 a.m.; and so on; 6 p.m.–5:59 a.m. = evening and night), statistically significant differences can be seen by machine type. With a confidence level of 95%, a significant relationship can be said to exist between machine type and time of accident:

- For stationary machines, early afternoon (12–2:59 p.m.) accounts for 46% of workers injured in accidents.
- For temporarily fixed machines, workers are injured in accidents chiefly between 6 and 11:59 a.m., and between 3:00 and 5:59 p.m.
- For mobile machines, injuries are spread more evenly throughout the day except for the early afternoon.

There are also some statistically significant differences by day of the week, according to machine type, when the plant explosion is excluded:

- More workers are injured in temporarily fixed machine accidents on Mondays.
- More workers are injured in mobile machine accidents on Fridays.

4.3 Injured workers/accidents ratio

The mean “number of injured workers/number of accidents” ratio is a way of assessing the seriousness of an accident. The mean was 1.73 when the two extreme accidents were included, and 1.51 without them. Roughly speaking, two serious or fatal accidents will result in three or more people injured.

4.4 Energy and machine types

When forms of energy involved are grouped into major categories, statistically significant differences can be seen by machine type:

- Electric arc (and electricity)—More associated with temporarily fixed machines (contact with power line), but also with stationary machines
- Chemical (fire, explosion, thermal, asphyxiation)—More associated with stationary machines
- Kinetic—More associated with stationary machines, primarily because of accident no. 2
- Potential—Less associated with stationary machines and more with mobile machines (movement of part of machine or falling transported load) and fixed machines (falling material)
- Mechanical and machine potential—Essentially associated with mobile machines (crushed under or struck by)

5 CONCLUSION

Accidents with mobile machines account for most machinery accidents, representing 59% of accidents and 54% of workers directly injured in accidents. There were proportionally more accidents involving mobile machines in the period 2011 to 2015 than in the years 2000 to 2013, when they represented 38% [8].

The continuity of production phase, which comes between production and maintenance, is a crucial one that accounts for 26% of accidents and 24% of workers directly injured in accidents. Nevertheless, the greatest proportion of accidents (44%) and the greatest share of workers directly injured in accidents (46%) are in the production phase. With data for past years for each life-cycle period (production, continuity of production, maintenance), it should be possible to identify the life-cycle phase that is proportionally the most hazardous.

Last, psychological injuries should be included in the total cost of accidents, as their consequences are far from negligible.

6 REFERENCES

1. Commission de la santé et de la sécurité au travail (CNESST), “*Rapport annuel de gestion 2011*,” DC400-2032-5, 2012, p. 42.
2. Paques J.-J., Bélanger R. & Massé S., *Sécurité des méthodes de cadencage d'équipements de scieries*, IRSST, Report R-028, 1989.
3. Ray S. P., Batson G. R. et al., *Impact of Maintenance Function on Plant Safety*. Professional Safety, Vol. 45, #8, p. 45-48, 2000.
4. National Occupational Health and Safety Commission (NOHSC), *Work-related fatalities associated with design issues involving machinery and fixed plant in Australia, 1989 to 1992*, NOHSC, Sydney, 2000.
5. Grusenmeyer C., *Les accidents liés à la maintenance. Étude bibliographique*; Institut National de Recherche et de Sécurité pour la prévention des accidents du travail et des maladies professionnelles (INRS, 2005)
6. Giraud L., Ait-Kadi D., Ledoux É., Paques J.-J., Tanchoux S., *La maintenance - État de la connaissance et étude exploratoire*, Report R-578, Montréal, IRSST, 2008, 61 pages
7. <http://www.irsst.qc.ca/en/ohs-research/research-projects/project/i/5246/n/analyse-comparee-des-accidents-machines-en-phase-de-maintenance-et-de-production-2013-0045>
8. Burlet-Vienney D, Chinniah Y., Aucourt B., *Implantation du cadencage des équipements mobiles dans le secteur municipal, Étude exploratoire*, IRSST, Report R-975, 2017.



Session 7

Experiences / Prospects

**The Safeguarding Supportive System (SSS) IV
Experimental procedure of behavior analysis to the Safeguarding Supportive System
(SSS) as a safety management approach.
For appropriate prediction and control of human behavior**

Hojo R.¹, Hamajima K.¹, Umezaki S.¹, Tsuchiya M.², Shimizu S.¹

¹ National Institute of Occupational Safety and Health, Japan (JNIOSH) – Umezono 1-4-6 – Kiyose – Tokyo – 204-0024 – Japan

² Advantage Risk Management Co., Ltd. – Nakameguro GT Tower 17F 2-1-1 – Kamimeguro – Meguro-ku – Tokyo 153-0051

hojo@h.jniosh.johas.go.jp
hamajima@s.jniosh.johas.go.jp
umezaki@s.jniosh.johas.go.jp
m-tsuchi@umin.ac.jp
shimizu@s.jniosh.johas.go.jp

KEYWORDS: Safeguarding Supportive System (SSS), behaviour analysis, human factor, residual risk, safety management

ABSTRACT

The Safeguarding Supportive System (SSS) was established to prevent human error and intentional unsafe behavior of workers at workplace of integrated manufacturing system. The SSS controls and prevents human error and intentional unsafe behavior using proper combination of Information and Communication Technology. In the present study, validity of the SSS was evaluated with a procedure of behavioral analysis. Ten students were engaged to the experiment. A virtual experimental workplace was built up in our institute (JNIOSH), assuming the work place as a manufacturing industry, including none-routine work such as cleaning robot. All subjects participated under the following 2 experimental conditions 4 times each. 1) SSS condition: Under the SSS, the workplace was divided by three work zones. If worker entered a target zone, three machines in the zone out of nine machines of whole workplace were stopped, and the rest kept working. A subject with a tag entered to the work place from gateway, hung the tag over main and sub controller, for stopping 3 machines, for confirmation of own authority and for working in zone 1. The subject was required to press button at work point. Subject hung a tag to sub and main control boards again after the work and pushed the restart button of the restart board. 2) Usual stop condition: After stopping all machines by pushing emergency button, subject moved from the gateway to zone 1 directly, and was required the same button pushing. After leaving from zone 1, the subject released emergency, restarted all machines. Half and the rest of subjects were assigned to feedback and no-feedback conditions, respectively.

For subjects in the feedback group, button-press and total times from the start to the end were shown, but subjects in the no-feedback condition were not told anything about the time. Average total time of the SSS was longer than that of usual stop condition. We assumed that none-routine work occurred once per 30 min out of 8-hour-work time. Then mechanical outage time was calculated using average total time of each condition. The machine outage time of SSS was shorter than that of the usual stop conditions. Decrease rates of total time from the first work of the feedback group was greater than that of the no-feedback condition. Usage of feedback might be applied as a good promoter for self-encouragement for working. These results suggest that introduction of the SSS guarantees both safety and operation efficacy.

1 INTRODUCTION

Recently, the percentage of non-regular and short-term employees has increased, while the percentage of expert workers who have supported safety at the workplace with long-term experience have decreased in Japan. Therefore, the method of ensuring safety through individual awareness is no longer suitable in Japan. As well as tunnel work site in Japan is not an exception. Aging of workers at tunnel construction is developing. Some of manual works in tunnel should be automated as much as possible and managed safety of workers by electronic devices such as ICT not depending upon human attentiveness. At the same time, it would be necessary to promote some standardized systematic operational manual for workers with short time of experience. In particular in

manufacturing industry, accidents by workers who lack experience in non-routine work such as cleaning robots, inspection, maintenance and setup still occur at workplaces that have introduced an integrated manufacturing system (IMS). The 3-step method of inherently safe design measures, safeguard and providing complimentary protective measures and information for use is a risk-reduction measure for safety ensured by ISO 12100/JIS B 9700, which is the safety standards for machines (Safety of machinery—Basic concepts, general principles for design). However, dangerous point-approach work occurs at actual workplaces, such as driving, adjustment, processing, troubleshooting, maintenance, repairing and cleaning machines during operating of these machines. Therefore, risk cannot be reduced sufficiently through safe standards for machines alone. New risks occur in IMSs from combining mechanical equipment. ISO11161—"Safety in an Integrated Manufacturing System"—does not offer an effective method of ensuring safety in dangerous point-approach work. Some users at actual work sites sometimes still employ risk-reduction methods, depending on the workers' attentiveness. Therefore, many uncertainties exist in this risk-reduction method. A severe accident might occur if human error happens and the expected effect cannot be obtained as a result.

In the present study, we tried to apply the SSS to tunnel construction site. Once human error occurs, it would be connected to severe accident in the tunnel. Based on the worldwide situation, it is necessary for the Japanese tunnel construction to consider risk-reduction strategies that match real work site. We have established a new risk-reduction method named the safeguarding supportive system (SSS), which targets the tunnel construction site. The SSS focuses on the residual risk after implementing the 3-step method of ISO 12100/JIS B 9700. The aim of the SSS is to provide effective residual risk-reduction using a combination of appropriate information and communication technology (ICT) equipment without depending on workers' attentiveness. Workers' qualifications (licenses) and rights (provided by ability and skill), the target machine, the work content, the place of the work and the operation time would become clear by introducing SSS. Under the SSS, work will only be allowed when ID information and the target machine of the tag held by a worker are matched with information from the control machine located in the work area. Therefore, it is possible to prevent dangerous side errors caused by human error. Nevertheless, the SSS should be used in parallel with the "protection plan"—the education and training management already introduced in Japan. The SSS is not a substitute for the protection plan.

2 AIM OF THE PRESENT STUDY

The "Safeguarding Supporting System (SSS)" was established to prevent human error and intentional unsafe behavior of workers at workplace of integrated manufacturing system (IMS). The SSS is the system to control and prevent human error and intentional unsafe behavior from the mechanical side (hardware side) using appropriate combination of Information and Communication Technology (ICT). In the present study, the effectiveness and usefulness of the SSS were evaluated with behavioral analysis procedure. In addition, change of fatigue of subjects (workers) for recent one month was measured with self-report questionnaire before and after experiment.

3 MATERIALS AND METHODS

1) The SSS condition: Three machines in zone 1 were stopped, and the rest kept working. A subject entered to the work place from the gateway (Figure1A), hung a tag (3 x 3cm, Omron, Japan) over the main (Figure 1B) and the sub control boards (Figure1C), for stopping 3 machines, for confirmation of own authority and for selecting work in zone 1. After that the subject moved to a button place (Figure 1D). The subject was required to press button 4 times each at upper and bottom locations of the belt conveyor as a work. The subject hung a tag to the sub and the main control boards again after the work and pushed the restart button of the restart board (Figure1E). **2) Usual emergency stop condition:** After stopping all machines by pushing an emergency button of an emergency stop board (Figure1F), subject moved from the gateway to zone 1, and was required to push the button 4 times each at upper and bottom locations of the belt conveyor at the button place. After leaving from zone 1, the subject released the emergency, moved to the restart board. Half subjects and the rest of them were assigned to feedback condition and no-feedback condition, respectively. **Feedback condition:** Five subjects in the feedback group were able to see the button-press time (work time) on the screen of the tablet, and described the total time (time from the start to the end) by experimenter immediately after the session. **No-feedback condition:** Rest of five subjects were assigned to the no-feedback condition. The work time on the tablet screen was hidden by a sheet of paper. Also, the total time was not told to subject in no-feedback group. Average total times of the SSS condition and usual emergency stop condition were compared and analyzed by Student's t-test. Statistical analyses of the effects of repeated sessions were performed with repeated one-way analysis of variance (one-way ANOVA). All numerical values are expressed as the mean and se. Values of $p < 0.05$ were considered statistically significant. All statistical analyses were performed using EZR software version 1.27 (Saitama Medical Center, Jichi Medical University, Saitama, Japan).

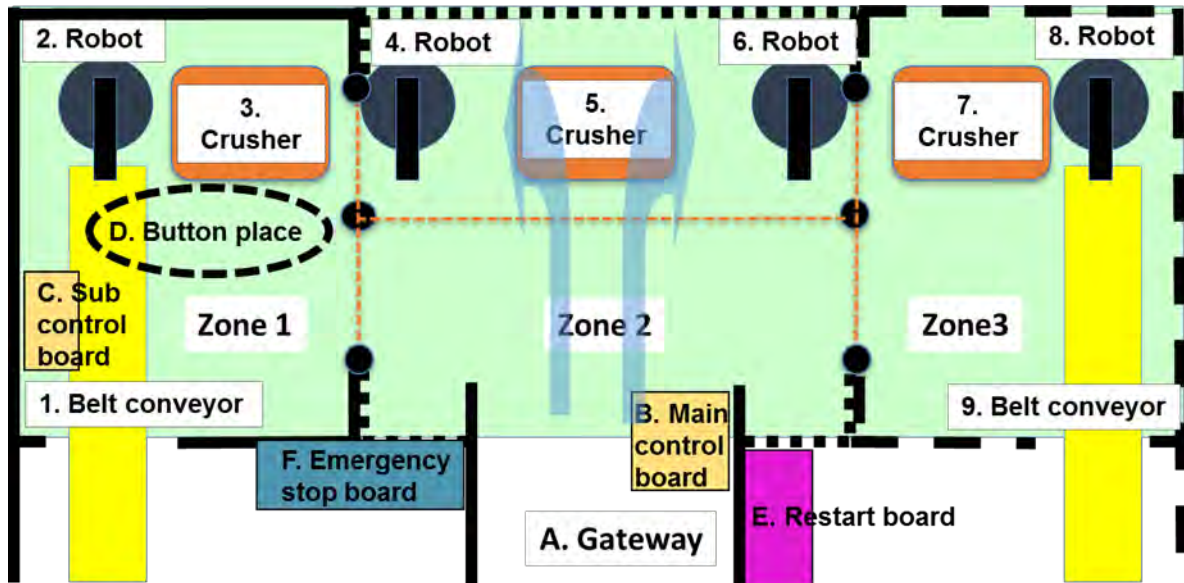


Figure 1. Work place for the present experiment.

The numbers 1-9 mean machines in the work place. Zone 1 (Left, Solid line) has a belt conveyor, a rock crusher and a robot. Zone 2 (Middle, Dotted line) has 2 robots and a rock crusher, assuming rock crush work. Zone 3 (Right, Broken line) has same machines as zone 1. Under the SSS condition, machines 1-3 are stopped, and all machines are stopped in the usual stop condition. A. Gateway, B. Main control board, C. Sub control board, D. Button place, E. Restart board, F. Emergency stop board.

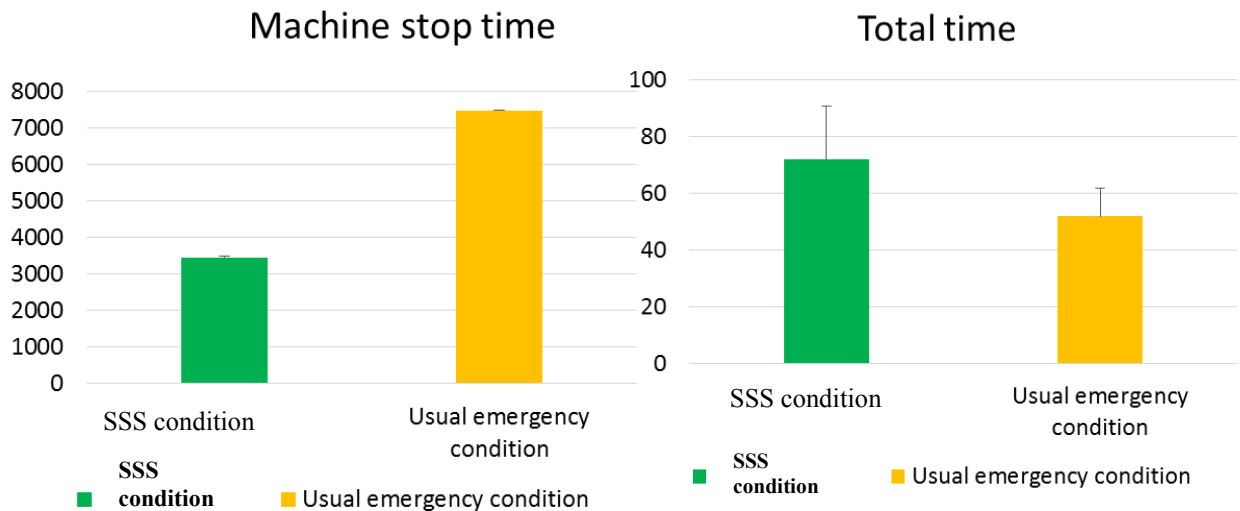


Figure 2. Total time (sec) of the SSS condition and usual emergency condition group.

Figure 3. Machine stop time (sec) of the SSS condition and usual emergency condition group.

4 RESULTS

Average total time of the SSS and the usual stop condition groups were 78±8.7 and 54±4.4 seconds, respectively (Figure. 2).

We assumed that irregular work occurred once per 30 min out of 8-hour-work time. Then mechanical outage time was calculated using average total time of each condition (16 times x the number of outage machine x total time). The machine outage time of SSS and the usual stop conditions was 3744sec (62.4 min) and 7776 sec (129.6 min), respectively. There was no difference in work time of the upper and the bottom locations of belt conveyor between the SSS and the usual stop conditions, but repeated factors were effective in both conditions. Decrease rates of total time from the first work of the feedback group was greater than that of the no-feedback condition. In self-reported questionnaire, 7 subjects reported stress decrease or no-change during experiment.

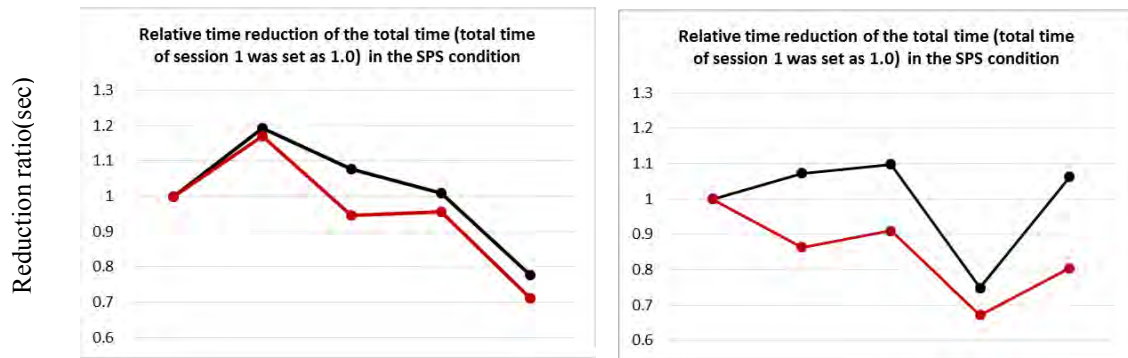


Figure 4. Relative time reduction with session repeat. Total time of session 1 was set as 1.0.

5 DISCUSSION

Even if the total time took longer in the SSS condition than that of the usual stop condition, machine outage time was shorter in the SSS condition than that in the usual stop condition. In addition, it was suggested that some feedback to the work possibly promote further work. Usage of feedback might be applied as a good promoter for self-encouragement for working. These results suggest that introduction of the SSS guarantees both safety and operation efficacy. It is possible that some feedback to the work promote further work. Also, it was suggested that repeated factor of the work in the present study played the role as promoter for work. Result of self-report indicated that the present experiment was not stress for more than half of subjects.

6 PERSPECTIVE

It would be possible that more precise analysis of reinforcement procedure including feedback helps to establish more effective learning process of the work.

Then, the SSS would be suitable for tunnel site.

7 REFERENCES

1. EN ISO12100: 2010, Safety of machinery –Basic concepts of general principles for design (2003), (in Japanese).
2. International Organization for Standardization, ISO11161, Safety of machinery – Safety of integrated manufacturing systems – Basic requirements (2007).
3. Japanese Industrial Standard, Safety of machinery-General principles for design-Risk assessment and risk reduction –Part 2, JIS B 9700-2 (2004), pp.4-15, (in Japanese).
4. Massimi P and Van Gheluwe JP, Community legislation on machinery comments on directive 89/392/EEC and directive 91/368/EEC, Nikkei Mechanical, Nikkei Business Publication Inc. (1994).
5. Ministry of Health, Labor and Welfare, Ordinance of Industrial Safety and Health (Revision), Article24-3 (2014). <http://www.mhlw.go.jp/bunya/roudoukijun/anzenisei14/dl/120521_01.pdf>, (accessed on 20 September, 2017).
6. Ministry of Health, Labor and Welfare, Sekkei Gijutsusha, Seisan Gijutsukanrisha ni taisuru Kikaianzen ni kakawaru kyouiku ni kannshi chuisubeki jikou ni tsuite (2014), <<https://www.jaish.gr.jp/anzen/hor/hombun/hor1-55/hor1-55-32-1-0.htm>>. (accessed on 20 September, 2017), (in Japanese).
7. Ministry of Health, Labor and Welfare, Section 9 Industrial Robot (Articles 150-3 to 151) (2015), <<http://www.japaneselawtranslation.go.jp/law/detail/?id=1984&vm=04&re=01>>, (accessed on 20 September 2017).
8. Ministry of Health, Labor and Welfare, Guidelines for comprehensive safety standards of machinery (Overview), revision (2007), <<https://www.jaish.gr.jp/anzen/hor/hombun/hor1-48/hor1-48-36-1-0.htm>>, (accessed on 20 September, 2017).
9. NihonKantokushiKyokai, Human Error Taisaku Book (2011).
10. Rodo Shinbun Sha (2017), <<https://www.rodco.jp/column/10133/>>, (accessed on 21 September, 2017), (in Japanese).

Session 7 – Experiences / Prospects

11. The Japan Machinery Federation, Subcommittee report 2014, Supporting Protective System under Integrated Manufacturing System (2014), (in Japanese).
12. The Japan Machinery Federation, Subcommittee report 2015, Supporting Protective System under Integrated Manufacturing System (2015), (in Japanese).
13. The Japan Machinery Federation, Subcommittee report 2016, Supporting Protective System under Integrated Manufacturing System (2016), (in Japanese)

Development of Human Resources in Safety in the Fourth Industrial Revolution Period: Current Status of Safety Assessor Qualification System and the Future Development Prospect in the Fields of Robotics, Corporate Management, and Collaborative Safety

Fujita T.^{1,2,3,4}, Kubota A.¹, Ariyama M.^{1,2,5}, Kodaira N.^{2,3,6}, Maeda. I.^{1,2,4}, Kanamaru H.^{1,2,7}, Matsuura H.^{1,8},
Kajiya T.^{2,5}, and Mukaidono M.^{2,9}

¹ Nippon Electric Control Equipment Industries Association (NECA) - 2-1-17 Hamamatsu-cho, Minato-ku, Tokyo, Japan

² The Institute of Global Safety Promotion (IGSAP) – 2-7-53 Nishimiyahara, Yodogawa-ku, Osaka, Japan

³ Japan Robot Association (JARA) – Kikaishinko Bldg., 3-5-8, Shibakoen, Minato-ku, Tokyo, Japan

⁴ IDEC Corporation – 2-6-64 Nishimiyahara, Yodogawa-ku, Osaka, Japan

⁵ Japan Certification Corporation (JC) – 2-7-53 Nishimiyahara, Yodogawa-ku, Osaka, Japan

⁶ Mitsubishi Electric Corporation – 2-7-3, Marunouchi, Chiyoda-ku, Tokyo, Japan

⁷ Mitsubishi Electric Corporation – 8-1-1 Tsukaguchi Honmachi, Amagasaki, Hyogo, Japan

⁸ OMRON Corporation – Shinagawa Front Building 7F, 2-3-13, Konan, Minato-ku, Tokyo, Japan

⁹ Meiji University – 1-1-1 Kandasurugadai, Chiyoda-ku, Tokyo, Japan

t.fujita@jp.idec.com

kubota@neca.or.jp

ariyamam@j-cert.com

Kodaira.Norio@eb.MitsubishiElectric.co.jp

i.maeda@jp.idec.com

Kanamaru.Hiroo@db.MitsubishiElectric.co.jp

hiroshi_matsuura@omron.co.jp

kajiya@institute-gsafety.com

masao@meiji.ac.jp

KEYWORDS: safety assessor, safety of machinery, robot, collaborative safety

ABSTRACT

In the coming era of the Fourth Industrial Revolution, new safety approaches such as Vision Zero and Collaborative Safety “Safety2.0” are emerging globally, and Robot Revolution has taken place in Japan. Many robot manufacturers are developing collaborative robots that are being used in actual applications not only of industrial systems but of service industry to meet the challenges of labor shortage. In such a trend, there is an urgent need to develop and foster skilled personnel who can promote and implement safety of machines and facilities. Those skilled personnel must possess the latest safety knowledges based on international ISO/IEC safety standards. To foster safety personnel, the Nippon Electric Control Equipment Industries Association (NECA) founded the Safety Assessor (SA) Qualification System in 2004 the Safety Basic Assessor (SBA) Qualification System in 2009 with the support of the Japan Ministry of Economy, Trade and Industry (METI). Furthermore, the Institute of Global Safety Promotion (IGSAP) established and implemented operation of Robot Safety Assessor qualification system in 2018. These qualification systems have been adopted in diverse industries including automobile industries and proved its effectiveness promoting safety in workplaces. This paper reports the current situation of these qualification systems and the future prospects of developing Safety Officer Qualification System and Collaborative Safety Assessor Qualification System.

1 INTRODUCTION

In this age of the Fourth Industrial Revolution, new innovative technologies such as IoT, AI, and big data are coming into practical use at a dramatic speed across society. In Japan, where the automobile industry has long used numerous industrial robots, the Robot Revolution is in progress and many robot manufacturers have developed collaborative robots that are becoming common across the food industry and the service sector. What has driven these developments is the industrial and service sectors’ growing awareness that they need to rely on robots to make up for labor shortages, and this way of thinking is spreading further. For example, the Ministry of Economy, Trade and Industry (METI) and the Japan Robot Association (JARA) took the lead in establishing the FA & Robot System Integrator Association (SIer) and, as soon as the association began operation, 130 companies

from the system integrators and robotics businesses joined it [1]. However, while robot system integrators' engagement is vital to the success of the Robot Revolution in Japan, SIER has only limited knowledge about workplace safety. Hence, it is imperative that Japan develops human resources well-versed in the latest knowledge about workplace safety that follows the ISO/IEC international safety standards to promote the safety of machine and equipment systems. Furthermore, the use of robots in environments without guards is increasing. This creates a climate in which both international standardization and technological development for collaborative safety "Safety 2.0" are urgently needed to enable the shift from the conventional safety using guards to safety without guards [2]-[4].

These enormous changes as part of the Fourth Industrial Revolution have caused various paradigm shifts. How important safety is and how it should be ensured must be understood by not only engineers but also managers of plants and business offices, and top management, so that safety can be pursued in a top-down approach. This idea matches the campaign of top-down promotion of safety put forward as "Vision Zero" with the method of focusing 7 Golden Rules launched by the International Social Security Association (ISSA) in Singapore in September 2017 [5]. This paper reports that, under these circumstances, the Safety Assessor (SA) Qualification System was established in Japan in 2004 to foster human resources having the universal knowledge of machinery safety. This paper also reports what the system has achieved along with the overview of the Robot Safety Assessor Qualification System newly founded as a developed version of the SA Qualification System. It also presents the need for a new safety qualification for managers. The reporting particularly focuses on what kind of knowledge the programs are designed to require. It also covers the status of the international standardization for competence required for these qualifications, on which the IECEE has already started working [6].

2 CURRENT STATE OF THE SAFETY ASSESSOR QUALIFICATION SYSTEM

In Japan, in order to train safety personnel with assistance from the Japanese government's METI, the Nippon Electric Control Equipment Industries Association (NECA) built the Safety Assessor (SA) Qualification System in 2004 and the Safety Basic Assessor (SBA) Qualification System in 2009. The overview of these safety qualification systems were presented at the SIAS conferences* as part of the reports on how the qualification systems of SA and SBA had evolved and been adopted by companies, and how common they had become across Asia [7]-[11].

* Held in the United States in 2005, Tokyo in 2007, Finland in 2009, Canada in 2012, and Germany in 2015

It is essential to study various safety standards in order to understand machinery safety. Engineers working for companies, however, had few opportunities to acquire knowledge about machinery safety, and they had no means to measure their levels of understanding about workplace safety. Hence, with METI providing assistance and Japan Certification Corporation serving as the administrative organization, NECA introduced qualification systems designed to teach the safety knowledge needed by automobile and auto parts manufacturers as well as other businesses of any size in a wide range of industries, and to certify applicants who have passed the exams. Figure 1 shows the structures of the systems.

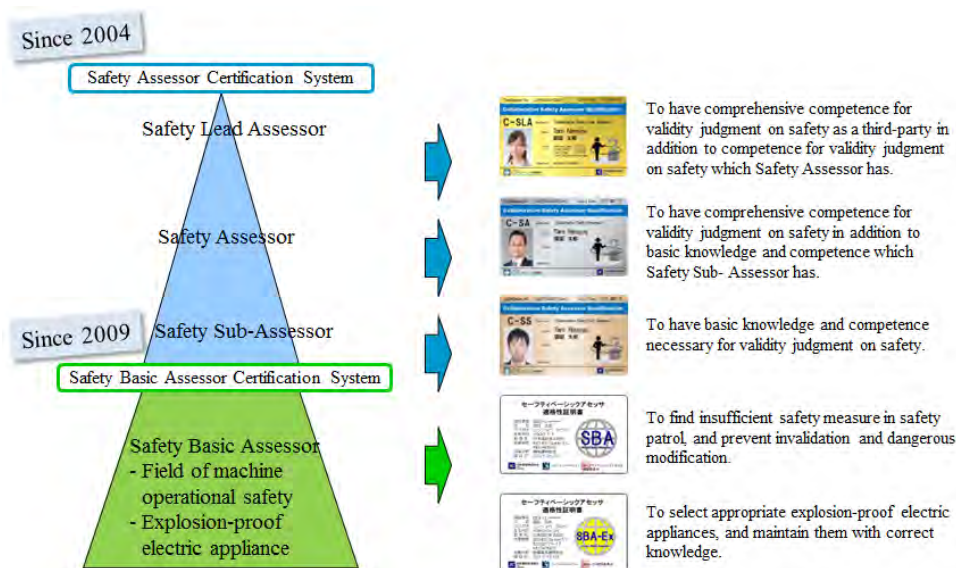


Figure 1. Hierarchy systems of Safety Assessor and Safety Basic Assessor Qualification System.

The total number of certified SAs and SBAs has increased to about 15,000, and the number of companies that have adopted the qualification systems has risen to about 1,300 over the last 14 years. Figures 2 and 3 show how the numbers have grown. In 2014, the Japanese government’s Ministry of Health, Labor and Welfare issued a notification that described these systems as valuable, and advised companies to adopt them, which helped to considerably increase the number of certified SAs and SBAs. Moreover, seven other Asian countries adopted the SBA system. The Japanese government transferred the SBA system to Thailand, which it acknowledged as a model country for the system, through an ODA project. The qualification systems will likely be adopted by more countries across the globe.

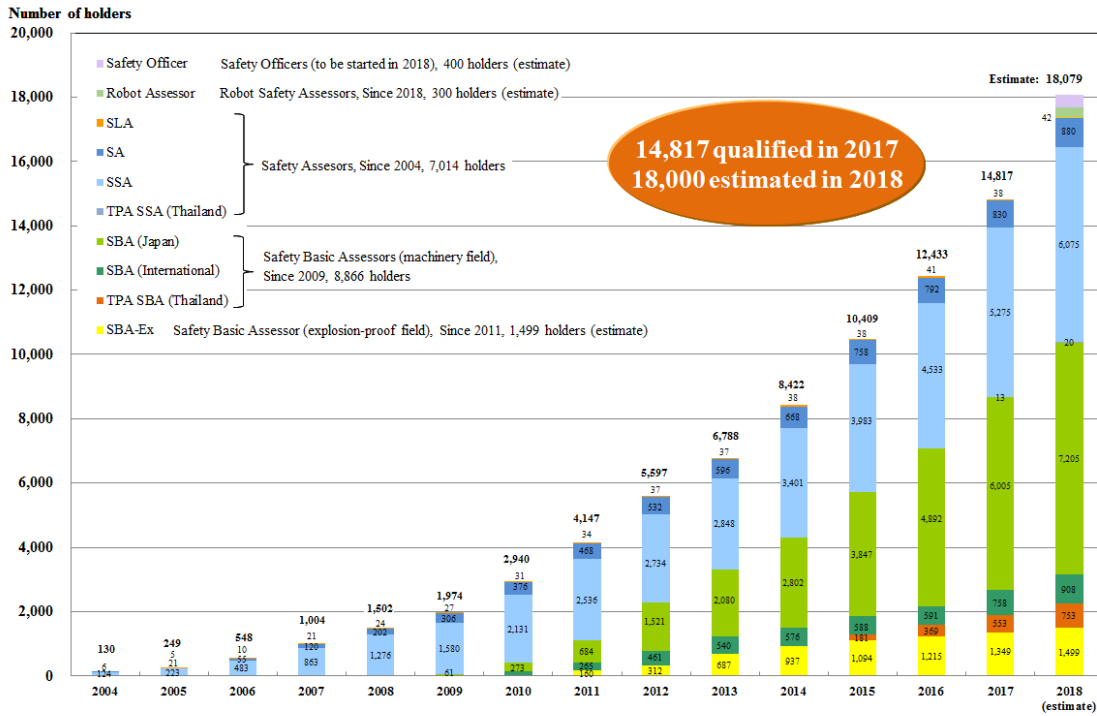


Figure 2. Number of holders of Safety Assessor, Safety Basic Assessor, Robot Assessor, and Safety Officer.

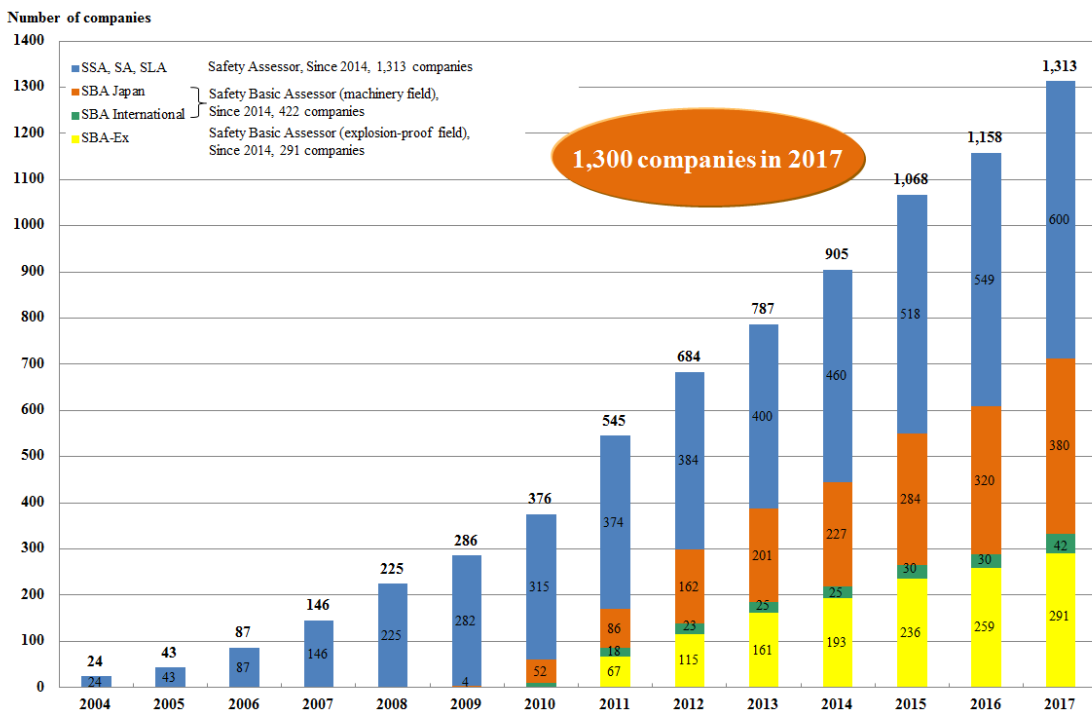


Figure 3. Number of companies adopting Safety Assessor and Safety Basic Assessor Qualification System.

As the numbers of certified Safety Assessors were steadily on the rise in Japan and overseas, the training of robot system integrators with a solid understanding of robot safety standards became increasingly important. Eventually, the Robot Safety Assessor Qualification System was officially launched in July 2018, and 139 people have passed the trial and first official exams to become certified Robot Safety Assessors. Figure 4 (a) shows the pass rate of the Robot Safety Assessor Qualification System exam broken down by the level of holders of Safety Assessor Qualification. As the figure shows, pass rate of Safety Lead Assessor and Safety Assessor holders were 100% and 90.8%, respectively. In contrast, less than 50% of Safety Sub Assessor and those who have no assessor qualification were qualified as Robot Safety Assessor. This shows that those who have high understanding level of machinery safety also have excellent comprehension of robot safety. Figure 4 (b) shows the distribution of ages among examinees. As the figure shows, over 70% of examinees were in their 20’s, 30’s, and 40’s, indicating that younger generation who will engage in robot safety in the coming era feel the need of possessing the Robot Safety Assessor Qualification.

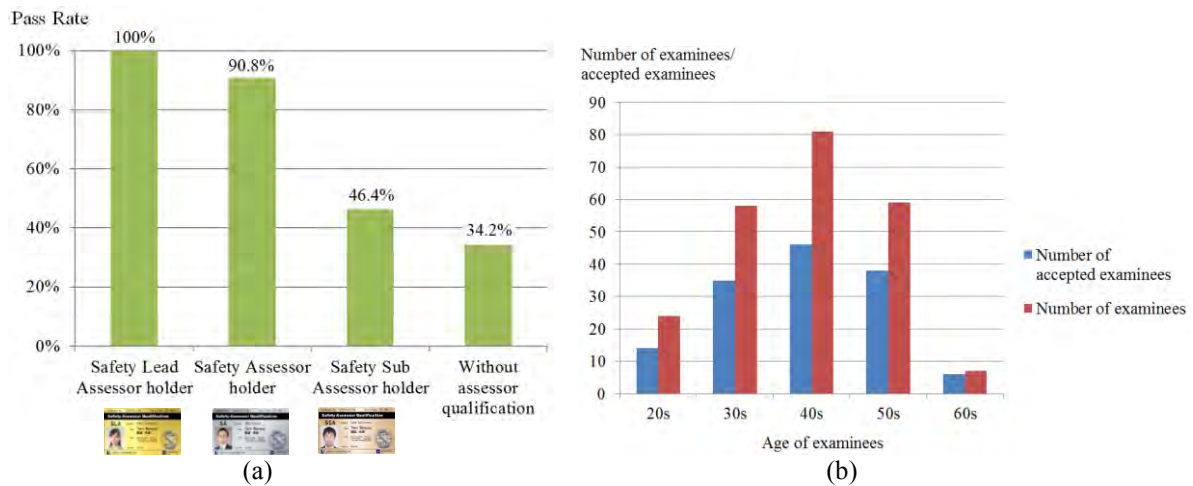


Figure 4. Pass rate of Robot Safety Assessors broken down by the level of holders of Safety Assessor qualification (a) and ages (b).

The new system is expected to serve as a tool for the development of human resources who understand the importance of risk assessment and risk reduction so that certified assessors’ knowledge will be leveraged to achieve advanced robot applications in Japan.

System integrators will play an increasingly important role. Besides, the implementation of automated systems that use robots will need more human resources with knowledge about workplace safety than ever, which means the SA and SBA Qualification Systems will become even more important. Above all, the upcoming age of robots and humans coexisting and collaborating will require collaborative safety “Safety 2.0”. Given these factors, a new safety personnel training system which assesses personnel’s understanding of collaborative safety “Safety2.0”, coupled with top management’s understanding of workplace safety, has become necessary. Steady efforts toward these will eventually lead to a future safety vision that adopts new technologies, and to society that will achieve Vision Zero. The next chapter explains what certified Safety Assessors (SLA, SA, SSA) and Robot Safety Assessors are required to understand, which international standards their knowledge as well as lectures and qualification examinations are based on, and what competence is required of these certified human resources.

3 KNOWLEDGE REQUIRED OF CERTIFIED SA/ROBOT SA

Table 1 shows skills and knowledge required of a certified Safety Assessor as specified in the NECA standards for the Safety Assessor Qualification System [12]. The knowledge required by the Safety Assessor Qualification System that NECA has advanced is stipulated in accordance with the technical requirements for machinery safety (e.g., international safety guidelines; international safety standards). The contents are based on basic safety requirements applicable to a wide range of machines, that is, ISO/IEC Guide 51 (basic safety guidelines), basic safety standards for machines (Type A standards), and group safety standards for machines (Type B standards). Therefore, the knowledge is useful for designers of various machines as well as machine engineers and operators, etc. As Table 1 indicates, certified Safety Assessors (SAs) and Sub Assessors (SSAs) need comprehensive knowledge. On this note, certified Safety Lead Assessors (SLAs) are required to demonstrate profound experience and insight at an interview conducted separately from the exam, in addition to the knowledge indicated below. Since passing the interview is quite a challenge, only around 40 of 15,000 applicants have been certified.

Table 1. Knowledge requirement for Safety Assessors and Safety Sub Assessors (excerpt from NECA standard 0901: 2016).

No	Required knowledge/standard	Safety sub-assessor	Safety assessor
1	Basic safety standard ISO/IEC Guide51	Structure and overview of machine safety standards with ISO/IEC Guide51 as the main standard	Same as left
2	Risk assessment and risk reduction ISO 12100	Principle of essential safety, isolation, and disconnection. Basic knowledge about, 1) Risk assessment approach 2) 3-step method 3) Protection measures etc.	Knowledge about the items mentioned on left
3	Guard and interlock safety and isolation ISO 14119, 14120, 13854, 13855, 13857	Basic knowledge about, 1) Design of guard and interlock 2) Safety and isolation of upper arm and lower arm 3) Positioning of safety and protective items on the basis of approach speed of body parts	Knowledge about the items mentioned on left
4	Electrical equipment of machines-Part 1 IEC 60204-1	Basic knowledge about, 1) Protection from electric shock 2) Protective bonding 3) Control function (hold to run, operations with both hands, enabling) 4) Operator interlock (emergency stop, display lamp, push button) 5) Categories of stopping the machine 6) Warning display	Knowledge about the items mentioned on left
5	Safety related parts of control systems – Part 1 ISO 13849-1	Basic knowledge about, 1) Definition of PL 2) Factors required for PL calculation (category, MTTFd, DCavg, CCF) (Not including the calculation methods of PL)	Knowledge about the items mentioned on left
6	Safety related parts of control systems – Part 2 ISO 13849-2	—	1) Determining appropriateness 2) Safety principles that are adequately examined with the basic safety principles
7	Functional safety of E/E/PES control systems IEC 62061	—	Knowledge about, 1) Definition of SIL 2) Factors required for SIL calculation (architecture, hardware fault tolerance, PFHD, SFF, CCF, DC) (Calculation of SIL itself is excluded)
8	Safety principles of machine safety ISO 12100, 14118	Basic knowledge about, 1) Safety confirmation type system 2) Restart prevention control 3) Safety related parts and non-safety related parts	Knowledge about the items mentioned on left
9	Engineers ethics	Knowledge about, 1) Current status of industrial accidents and accidents due to machines, and case examples of accidents 2) Engineers ethics, adherence to laws and regulations (compliance), etc.	Knowledge about the items mentioned on left
10	Laws and regulations of different countries (Stipulated in the exhibits of each country)	Knowledge about, 1) Structure of laws and regulations 2) Overview of main domestic laws and regulations 3) Main international laws and regulations 4) Others (Overview of OHSMS) However, with regard to 3) and 4), specific details shall not be included and only basic parts shall be covered.	Knowledge about the items mentioned on left
11	Case examples of machine safety measures	Actual safety measures taken on the basis of international safety standards	Knowledge about the items mentioned on left
12	Knowledge about residual risk (Stipulated in the exhibits of each country)	Understanding and preparing basic contents of residual risk map and residual risk list	Preparing residual risk map and residual risk list

Table 2 shows additional knowledge required by the Robot Safety Assessor Qualification System [13]. Among the required knowledge, the individual safety standards for robots (Type C standards) are included in addition to the basic safety standards (Type A standards) and group safety standards (Type B standards) required by the Safety Assessor Qualification System. Regarding robot safety, the knowledge about basic machinery safety is inadequate to ensure the safety of the personnel such as system integrators who install robots at manufacturing plants. Hence, certified Robot Safety Assessors must have safety knowledge that covers functions unique to specific robots and the latest technologies including collaborative robots, that is, knowledge of individual safety standards for robots.

Table 2. Knowledge requirement for Robot Safety Assessors (excerpt from IGSAP standard 0901: 2016).

No	Required knowledge/standard	Robot Safety Assessor
1	Robot Safety Standard ISO 10218-1	1) Terms and definitions 2) Hazard identification and risk assessment 3) Safety requirements and protective measures 4) Verification and validation 5) Information for use
2	Robot System Safety Standard ISO 10218-2	1) Terms and definitions 2) Hazard identification and risk assessment 3) Safety requirements and protective measures 4) Verification and validation 5) Information for use
3	Collaborative Robot ISO/TS 15066	1) Terms and definitions 2) Collaborative industrial robot system design 3) Requirements for and design of collaborative robot system applications 4) Speed and time monitoring and power and force limiting in collaborative operation 5) Information for use
4	Related laws/regulations in Japan	Ordinance on Industrial Safety and Health, Article 150 (Japan)

As you see, individual safety standards for each technological field will likely be needed in addition to basic safety knowledge in order to ensure safety in technologically innovative sectors as well as the safety of systems, etc. that combine machines and devices. The key is to implement change according to the needs of the times.

4 NEED FOR NEW QUALIFICATION SYSTEMS FOR MANAGERS IN THE AGE OF VISION ZERO AND COLLABORATIVE SAFETY

Figure 5 shows various qualifications on safety standards which will be indispensable in the new age. As explained above, the SA Qualification System (I) launched with assistance from METI and the new Robot SA Qualification System (II) are intended solely for engineers. They have grown as tools that support designers and industrial engineers in acquiring a securely and globally shared understanding of safety. Below these 3-level (gold, silver, and bronze) systems, the Safety Basics Assessor (SBA) Qualification System (aluminum) was set up in 2009 as a qualification system created for on-site workers who need machinery safety and/or protection from explosion. Such efforts to ensure workplace safety part of overall plant management have continued for the last 15 years.

Safety qualification systems for engineers and on-site workers are important, and the great response to the newly-established Robot SA Qualification System seems to herald the growth of the system as an educational qualification program that suits society’s needs. However, no safety learning or training programs for top management and managers (e.g., corporate executives and plant managers) are available in Japan, and management tends to turn to stopgap measures at a time of crisis. Their lack of safety knowledge has led to the current reality where safety awareness is not shared across a company, no matter how hard engineers make efforts. This situation should be changed. Therefore, in addition to the machine safety qualification systems for engineers (I) (II), the Safety Officer (SO) Qualification System (III) for managers and top management is now promoted. Furthermore, since the new collaborative safety “Safety2.0” will spread into the society as more managers and those in top management have more understanding in safety, establishment of Collaborative Safety Assessor Qualification System (IV) is expected in a few years.

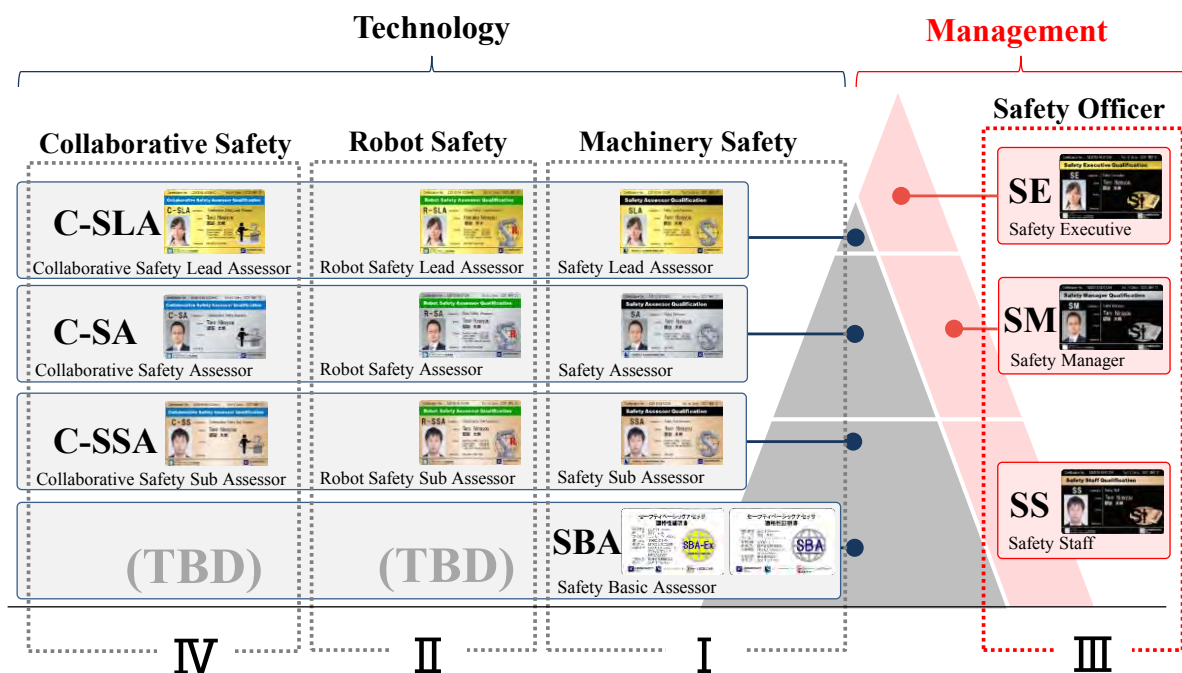


Figure 5. Success case of Safety Assessor Qualification (I), and evolution to Robot Safety Assessor (II), Safety Officer (III), and Collaborative Safety Assessor (IV).

The Safety Officer Qualification System (III) consists of three levels defined as follows:

- Safety Executive (SE) Qualification System for top management
The objectives of this system are to help executives acquire the correct knowledge about and deep insight into workplace safety, and to train them to exercise leadership as Chief Safety Officers (CSO), etc. in pursuing safety, thereby raising their employees’ safety awareness.
- Safety Manager (SM) Qualification System for managers
The objectives of this system are to help managers acquire the correct safety knowledge, and to train them to exercise leadership as safety supervisors capable of providing their employees with correct guidance on workplace safety.
- Safety Staff (SS) Qualification System for corporate employees
The objectives of this system are to help corporate employees acquire basic safety knowledge, and to train them to take correct action for workplace safety in accordance with their companies’ safety policies, etc.

The knowledge required for these qualification systems has been defined as "Safenology," which is classified into the following four categories: Basic Safenology (philosophical aspect); Management Safenology (organizational aspect: action); Society Safenology (organizational aspect: framework); and Structural Safenology (technical aspect). Figure 6 shows an overview of these categories. Figure 7 summarizes two of the four categories (Management and Society Safenologies) as examples and shows the courses that prospective SEs, SMs, and/or SSs should take [14] [15].

Top management’s solid understanding of workplace safety is a key to the Future Safety Concept that is in the works in Japan and, given that Vision Zero may be adopted across the world, we believe that our attempt to create an SO qualification system will constitute the world’s pioneering work [16].

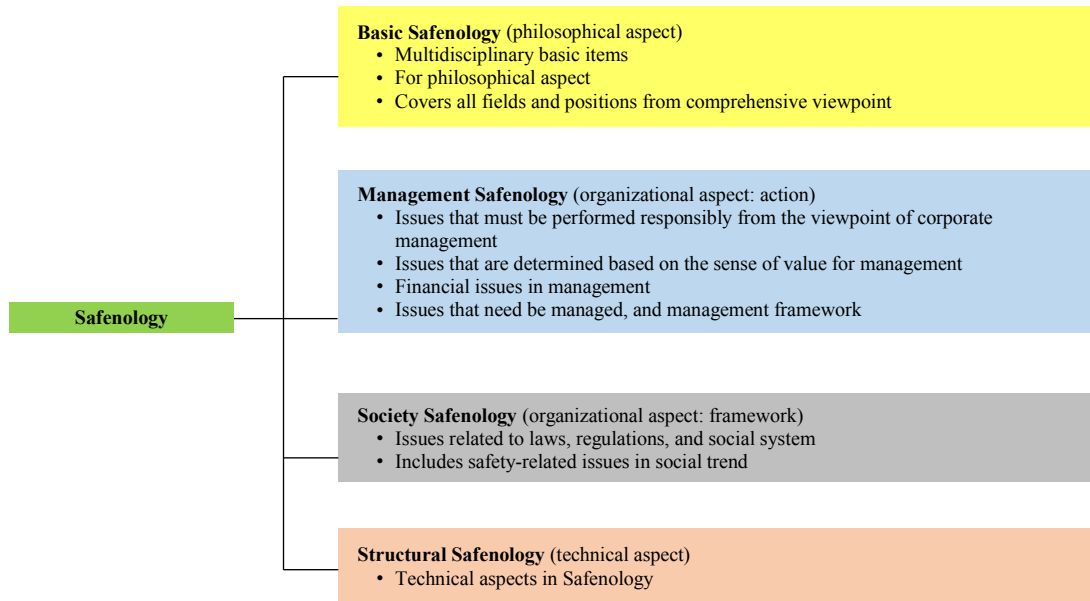


Figure 6. Four Safenology curriculums for Safety Officer Qualification System.

	Assessor Level		
	SE	SM	SS
Management Safenology introduction			
Management purpose and safety	1	1	
Risk for corporate management	1	1	
Trend of the times for safety and <i>anshin</i>	1	1	1
Top executive's role in safety	1	1	
Top executive's safety philosophy	1	1	
Corporate competitiveness lies in safety	1	1	1
Safety is a value	1	1	1
Safety investment	1	1	
Cost effectiveness of safety	1	1	
Safety and productivity	1	1	1
Human error and training	1	1	1
Response to accidents	1	1	
Management system and risk assessment	1	1	
Occupational safety and health management system	1	1	1
Personnel training and safety qualified personnel	1	1	1
Establishing a safety culture	1	1	1
Future Safety Concept	1	1	1
Management Safenology conclusion			

	Assessor Level		
	SE	SM	SS
Society Safenology introduction			
Social system for society		1	1
Laws and regulations for safety		1	1
Occupational Safety and Health Law	1	1	1
Insurance system of safety		1	1
Safety and responsibility	1	1	1
Structure and system for accident investigation		1	
Safety standardization and safety standards		1	
Certification system		1	
Preventing and reducing accidents	1	1	
Consumer safety		1	
Safety for the elderly and children		1	
Cyber security and IoT technology		1	
Changes of the times and risk diversification		1	1
New era for safety	1	1	1
Safety must be created by society as a whole	1	1	1
Society Safenology conclusion			

Figure 7. Courses for Management Safenology and Society Safenology for Safety Officer Qualification System.

5 STATUS OF INTERNATIONAL STANDARDIZATION FOR GLOBALIZED CERTIFICATION

One example of a global qualification system for safety human resource development is a Certification of Personnel Competence (CoPC) launched and managed by the International Electrotechnical Commission System for Certification to Standards Relating to Equipment for Use in Explosive Atmospheres (IECEX System). This is one of the conformity assessment systems administered by the International Electrotechnical Commission (IEC). CoPC was established on the recognition that human resource development is essential to accurately segment hazardous areas and select, install, inspect, and maintain the right machines and equipment in order to ensure the safety of explosion-proof systems, apart from product certification of explosion-proof machines and equipment. About 2,000 people have received the certificate since the inaugural certification in 2010.

Moreover, in the IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE), which is another of the conformity assessment systems managed by the IEC, it is also believed that certification given solely to products that meet safety requirements is insufficient to ensure the safety of products and systems that have been increasingly systemized, sophisticated, and built into networks in this age of the Fourth Industrial Revolution. Therefore, it has been considered as necessary to develop a safety assessment that covers a wide range of additional requirements, and training competent human resources (personnel's skills) is drawing attention as one of the key elements of the assessment. With this background, the IEC recognized the Safety Assessor Qualification System adopted by Japan and other Asian countries as a program that has successfully trained workplace safety personnel. The IEC (IECC) set up a new task force (TF) for CoPC to explore whether the IEC should offer the personnel competence certification system.

At the IECEE Certification Management Committee (CMC) meeting held in France in June 2018, the Safety Assessor Qualification System was presented as a personnel certification system for machinery safety in Japan along with its achievements. The meeting highly acclaimed the system and officially decided that the IEC would start developing personnel competence certification systems, and that one for machinery safety would have priority. The decision eventually led to the plan that the IEC would develop a personnel competence certification system for machinery safety as its CoPC based on the Safety Assessor Qualification System, with Japan playing a leading role in the project as the convener of the TF [6]. The IEC's launch of the CoPC for machinery safety will likely serve as a catalyst for the advent of similar systems in other various safety fields that need human resource development and personnel qualification (e.g., robots; collaborative safety). In the same way, the international standardization of technical knowledge requirements designed for designers, operators, and workers as well as the personnel qualification systems for managers will be continually developed and promoted. The latter qualification systems require applicants to demonstrate their appropriate attitude toward workplace safety as well as basic knowledge and skills. The international standardization will push forward such systems designed for corporate executives and business proprietors who play the key role in ensuring safety in a top-down management framework around the world.

6 CONCLUSION

The Safety Assessor Qualification System that NECA launched in 2004 with help from the Japanese government's METI has been internationally recognized as a system that makes a significant contribution to workplace safety. Consequently, it has been adopted in and outside Japan, and the IEC now considers standardizing the system internationally. This paper reported that the Robot Safety Assessor Qualification system was launched under the circumstances that collaborative robots are being developed and put into use in society across the world. Furthermore, the contents of the Safety Officer Qualification System along with the new Collaborative Safety Assessor Qualification System were also reported.

As Vision Zero and collaborative safety will be pursued around the world and corporate governance will be more highlighted in relation to corporate social responsibility (CSR), realizing safety and *anshin* (a sense of trust and assurance without any fear or stress) is essential to higher corporate value. Hence, the pursuit of safety and *anshin* will be advanced further in the coming years.

7. ACKNOWLEDGMENTS

Today's achievements of Safety Assessor Qualification System and many other qualification systems in Japan and overseas are all attributed to the METI's Standards and Conformity Assessment Projects. We are deeply grateful to all those concerned from METI who have provided us with invaluable advice and guidance for many years.

8. REFERENCES

1. Kodaira N., *System Integration in Robot Industry*, ROBOT, Japan Robot Association (JARA), pp. 3-8. 2018 (in Japanese).
2. Nikkei Business Publications Safety2.0 Project, *Safety2.0 – Concept*, 2015 (in Japanese).
3. Mukaidono M., *The Japan Society of Information and Communication Research Journal*, Vol. 34, No. 1, 2016-6, pp.41-46 (in Japanese).
4. Nikkei Business Publications Safety2.0 Project, *Safety2.0 – Applications*, 2017 (in Japanese).
5. Vision Zero (ISSA) <http://visionzero.global/>.
6. IEC e-tech, Issue 04/2018, *IECEE work benefits the environment, workplace and homes*, 2018, https://iecetech.org/Conformity-Assessment/2018-04/IECEE-work-benefits-the-environment-workplace-and-homes?bitly_hash=V5HcACzez3&utm_source=IEC+e-tech&utm_campaign=a01df89f4b-EMAIL_CAMPAIGN_2018_07_23_12_20&utm_medium=email&utm_term=0_00eeae4a79-a01df89f4b-142424777
7. Ishida Y., Yamamoto T., Matsueda Y., Maeda R., Mukaidono M., Fujita T., *The Creation of a Safety Assessor Accreditation System in Japan*, 4th International Conference on Safety of Industrial Automated Systems (SIAS), USA, 2005.
8. Kumazaki I., Maeda R., Arai T., Ishida Y., Mukaidono M., *Safety Assessor Program Association*, 5th International Conference on Safety of Industrial Automated Systems (SIAS), Tokyo, 2007.
9. Tochio M., Nakayama K., Arai T., Nonaka S., Shiomi M., Kanamaru H., Kojima H., Toyama H., Fujita T., Kasai H., Mukaidono M., *The Implementation of Safety Basic Assessor System to Expand the Awareness of Safety Complied with International Standards for Engineers and Non-engineers in Japan and Asian Countries*, 6th International Conference on Safety of Industrial Automated Systems (SIAS), Finland, 2010.
10. Tochio M., Nakayama K., Arai T., Nonaka S., Shiomi M., Kanamaru H., Toyama H., Fujita T., Takaoka H., Mukaidono M., *The Improvement of Industrial Safety Achieved by the Introduction of Safety Assessor/Safety Basic Assessor Qualification System and its International Operations*, 7th International Conference on Safety of Industrial Automated Systems (SIAS), Canada, 2012.
11. Fujita T., Shiomi M., Ishikawa K., Nonaka S., Kanamaru H., Tochio M., Ariyama M., Sagawa K., Takaoka H., Kuroda A., Mukaidono M., *Current situation of safety assessor and safety basic assessor (SA/SBA) qualification system: Reduction of accidents achieved by a Japanese company and recommendation by Japanese Ministry of Health, Labour and Welfare*, 8th International Conference on Safety of Industrial Automated Systems (SIAS), Germany, 2015.
12. NECA STANDARD, *NECA 0901: 2016, Standard for certification of Safety assessor*, Nippon Electric Control Equipment Industries Association.
13. The standard for a certification of robot safety assessors, *IGSAP S0201: 2018*, The Institute of Global Safety Promotion (in Japanese).
14. International Electrotechnical Commission. Advisory Committee on Safety (ACOS), ACOS/868/INF Documentation arising from the 11th ACOS workshop held in Tokyo, Japan, 2017-06-26: Safety considerations for next generation industrial automation.
15. International Electrotechnical Commission. Advisory Committee on Safety (ACOS), ACOS/869/RM Unconfirmed minutes of the ACOS meeting held in Tokyo, Japan, on 2017-06-28/29.
16. The Institute of Global Safety Promotion, Nikkei BP Intelligence Group, *Future Safety Concept – Safety2.0 Leads a New Society*, 2017 (in Japanese).

Objective and Subjective Effects of Passive Exoskeleton on Overhead Work

Pauline Maurice¹, Jernej Camernik², Dasa Gorjan², Benjamin Schirrmeister³, Jonas Bornmann³, Luca Tagliapietra³, Daniele Pucci⁴, Serena Ivaldi¹, Jan Babić²

¹ Universite de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France'

² Jozef Stefan Institute, Jamova cesta 39, SI-1000 Ljubljana, Slovenia' ³Otto Bock SE & Co. KGaA, Duderstadt, Germany

³ Fondazione Istituto Italiano di Tecnologia, via Morego 30, Genova, Italy

pauline.maurice@inria.fr

1. INTRODUCTION

Work-related musculoskeletal disorders (MSDs) are the first cause of occupational disease in developed countries and therefore represent a major health issue [1]. MSDs develop when biomechanical demands exceed the worker's physical capacity. In this regard overhead work is often cited as a MSDs risk factor [2,3]. Overhead work yet remains very common on assembly lines, especially in the automotive industry. Indeed many complex tasks cannot be fully automatized because they still require human cognitive skills. One solution to relieve workers while keeping them in control of the task execution is then to assist them with an exoskeleton [4].

Recently several industrial exoskeletons have been developed to support arms and/or tool weight during overhead tasks [5–11]. Many of them showed promising results regarding the reduction of physical workload. However, these studies present only partial assessments of the benefit provided by the exoskeletons. They exclude some important aspects like side-effects, adaptation, or user acceptance. In this work we present an exhaustive assessment of a novel passive exoskeleton for overhead work.

2. METHOD

The benefit provided by the use of an exoskeleton cannot be assessed solely based on the reduction of effort in the targeted limb. An exoskeleton is a wearable device, therefore its use might disrupt human movements or require additional effort. Supplemental effort can be caused by the weight of the device or, with passive exoskeletons, by the transfer of force from one joint to another. In addition, users' opinion of the device also affects its effectiveness. An exoskeleton that is ill-perceived by the user might remain unused, or cause psychological stress if use is imposed. Therefore we propose an assessment process that addresses the following aspects:

- *Task performance*: The task performance should be at least as good with the exoskeleton as without it.
- *Fatigue*: The exoskeleton should reduce metabolic demand and delay the apparition of fatigue.
- *Physical effort*: The exoskeleton should relieve the limb that is directly impacted.
- *Side-effects*: The exoskeleton should not significantly increase effort in limbs that are not directly impacted, nor cause bad postures.
- *Adaptation*: Using the exoskeleton should not require a long training nor cause after-effects at removal.
- *Acceptance*: Users should feel better when using the exoskeleton compared to when not using it.

A. Exoskeleton Description

Within the European project AnDy [12], the provided exoskeleton prototype is an upper-limb passive exoskeleton intended for supporting the weight of the arms, and possibly of manipulated tools, while the user is working overhead. This exoskeleton does not enhance the human's strength, but renders his/her arms virtually weightless, thereby relieving the shoulder joint. Being passive, hence without motors, the exoskeleton is light, not bulky, and easy to wear.

B. Experiment

Twelve participants performed an overhead pointing task with a portable tool, with and without the exoskeleton (Fig. 1). The participants' physical and physiological state was monitored with whole-body inertial motion capture, ground reaction force, EMG on shoulder and back muscles (right anterior deltoid and right erector spinae longissimus), oxygen consumption, and heart rate. The tool motion was recorded with optical motion capture to evaluate accuracy and completion time. Following the experiment, the perceived workload was assessed with the NASA Task Load Index (NASA-TLX) [13]. In addition, participants answered a questionnaire and a semi-directed interview was conducted to evaluate technology acceptance.

C. Measures

a) *Task performance*: Task performance was assessed with the movement accuracy and completion time.

b) *Fatigue*: Oxygen consumption and heart rate were used to evaluate objective metabolic demand and fatigue, while the NASA-TLX indicated subjective fatigue. Evolution of task performance over time was used as an additional indicator for fatigue.

c) *Physical Effort*: Given that the exoskeleton aimed at supporting the arms weight, the shoulder joint was directly impacted by the use of the exoskeleton. Therefore, activation of the anterior deltoid and estimated shoulder torque were used to assess the physical demand on the impacted limb. Joint torques were computed with inverse dynamics based on the recorded whole-body kinematics and ground reaction force [14].

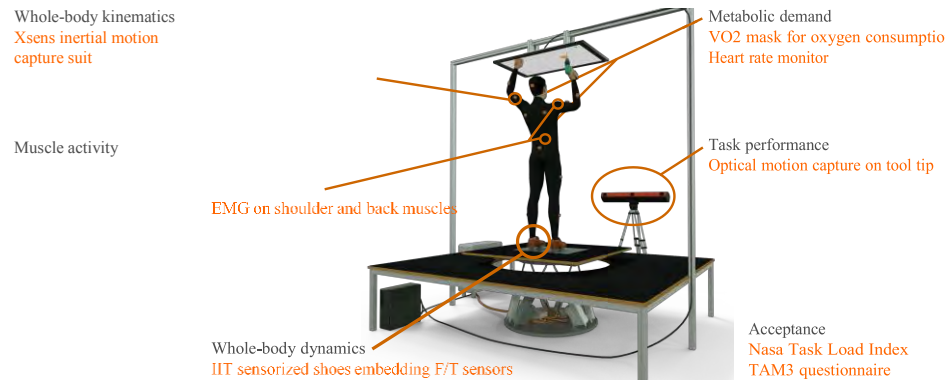


Fig. 1. Experimental set-up and sensors used to assess the exoskeleton.

d) *Side-effects*: Activation of erector spinae and back and hip torques were used to assess potential increase in effort in non-directly impacted limbs. Joint angles obtained by whole-body kinematics served to evaluate postural changes.

e) *Adaptation*: The tool 3D trajectory as well as trajectories of the shoulder, elbow and back in joint space were used to compare movement strategy with and without the exoskeleton. Evolution of task performance over time was used to detect learning and after-effects.

f) *Acceptance*: Score obtained in the technology acceptance questionnaire was used to quantitatively assessed acceptance of the exoskeleton, while opinions expressed during the interview served to shed light on some of the questionnaire answers.

3. RESULTS

Comparison of the two conditions with and without exoskeleton revealed that muscle activation, oxygen consumption and heart rate were significantly reduced when using the exoskeleton. Conversely, task performance was affected neither positively nor negatively. Importantly, the reduction in overall workload observed with objective measurements was also observed in subjective measurements: the task not only was, but also felt, less demanding when wearing the exoskeleton. Eventually, acceptance score was high and participants all said that they would choose to use the exoskeleton again for such a task.

4. CONCLUSION

Future work will be directed towards evaluating the exoskeleton on different tasks, including bending, crouching and walking to assess its transparency and potential disturbances of the users movements. Experiments on industrial sites are also planned. Furthermore, results from the evaluation will serve to guide the development of an intuitive adaptation of the level of support provided by the exoskeleton.

5. ACKNOWLEDGMENT

This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No.731540 (An.Dy). The content of this publication is the sole responsibility of the authors. The European Commission or its services cannot be held responsible for any use that may be made of the information it contains.

6. REFERENCES

- [1] A. Parent-Thirion, G. Vermeulen, G. van Houten, M. Lyly-Yrjinen, I. Biletta, and J. Cabrita, “Fifth european working conditions survey, publications office of the european union,” 2012.
- [2] J. R. Grieve and C. R. Dickerson, “Overhead work: Identification of evidence-based exposure guidelines,” *Occupational Ergonomics*, vol. 8, no. 1, 2008, pp. 53–66.
- [3] J. K. Sluiter, K. M. Rest, and M. H. Frings-Dresen, “Criteria document for evaluating the work-relatedness of upper-extremity musculoskeletal disorders,” *Scandinavian journal of work, environment & health*, 2001, pp. 1–102.
- [4] M. P. de Looze, T. Bosch, F. Krause, K. S. Stadler, and L. W. OSullivan, “Exoskeletons for industrial application and their potential effects on physical work load,” *Ergonomics*, vol. 59, no. 5, 2016, pp. 671–681.
- [5] N. Sylla, V. Bonnet, F. Colledani, and P. Fraise, “Ergonomic contribution of able exoskeleton in automotive industry,” *International Journal of Industrial Ergonomics*, vol. 44, no. 4, 2014, pp. 475–481.
- [6] E. Rashedi, S. Kim, M. A. Nussbaum, and M. J. Agnew, “Ergonomic evaluation of a wearable assistive device for overhead work,” *Ergonomics*, vol. 57, no. 12, 2014, pp. 1864–1874.
- [7] S. Spada, L. Ghibaud, S. Gilotta, L. Gastaldi, and M. P. Cavatorta, “Analysis of exoskeleton introduction in industrial reality: Main issues and eaws risk assessment,” in *International Conference on Applied Human Factors and Ergonomics*. Springer, 2017, pp. 236–244.
- [8] J. Theurel, K. Desbrosses, T. Roux, and A. Savescu, “Physiological consequences of using an upper limb exoskeleton during manual handling tasks,” *Applied ergonomics*, vol. 67, 2018, pp. 211–217.
- [9] B. M. Otten, R. Weidner, and A. Argubi-Wollesen, “Evaluation of a novel active exoskeleton for tasks at or above head level,” *IEEE Robotics and Automation Letters*, vol. 3, no. 3, 2018, pp. 2408–2415.
- [10] K. Huysamen, T. Bosch, M. de Looze, K. S. Stadler, E. Graf, and L. W. O’Sullivan, “Evaluation of a passive exoskeleton for static upper limb activities,” *Applied Ergonomics*, vol. 70, 2018, pp. 148–155.
- [11] E. B. Weston, M. Alizadeh, G. G. Knapik, X. Wang, and W. S. Marras, “Biomechanical evaluation of exoskeleton use on loading of the lumbar spine,” *Applied Ergonomics*, vol. 68, 2018, pp. 101–108.
- [12] S. Ivaldi, L. Fritzsche, J. Babic, F. Stulp, M. Damsgaard, B. Graimann, G. Bellusci, and F. Nori, “Anticipatory models of human movements and dynamics: the roadmap of the andy project,” in *Digital Human Models (DHM)*, 2017.
- [13] S. G. Hart and L. E. Staveland, “Development of nasa-tlx (task load index): Results of empirical and theoretical research,” in *Advances in psychology*. Elsevier, 1988, vol. 52, pp. 139–183.
- [14] C. Latella, N. Kuppuswamy, F. Romano, S. Traversaro, and F. Nori, “Whole-body human inverse dynamics with distributed microaccelerometers, gyros and force sensing,” *Sensors*, vol. 16, no. 5, 2016, p. 727.



Poster session

Practical solutions for safety-related application programming

Huelke M., Lungfiel A., Janik A.

Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) –
Alte Heerstrasse 111 – 53757 Sankt Augustin – Germany

michael.huelke@dguv.de

andy.lungfiel@dguv.de

albert.janik@dguv.de

KEYWORDS: safety-related control systems, application software, specification and validation, practical solutions

ABSTRACT

Manufacturers of machinery are increasingly using application programming of safety controls in order to implement safety functions. The ISO 13849-1 and IEC 62061 standards define requirements concerning the development of software employed for safety functions. The essential requirement imposed by these standards is the observance of a structured development process: the V model. The further requirements concerning measures for the avoidance and control of errors during development are formulated in the standards in the usual very general terms. Furthermore, few examples and proposals for implementation of these requirements have been published to date. Interpretation of the standards during software development in machine construction is therefore often unclear, and presents difficulties during implementation.

The IFA began addressing the subject of safety-related application software many years ago. Between 2011 and 2013, Project FF-FP0319 concerning standards compliant development and documentation of safety-related user software in machine construction was successfully completed at the Bonn-Rhein-Sieg University of Applied Sciences in conjunction with numerous partner bodies from the machine construction sector and with funding from the DGUV. For this purpose, a procedure – the IFA matrix method – was developed, and evaluated and documented with reference to examples from industry, for implementation of the requirements concerning the development of software for machine safety functions.

The IFA matrix method can be used to specify, validate and document the application software of safety functions in accordance with the standards. In order for the IFA matrix method to be implemented efficiently, the IFA is developing SOFTEMA, a software tool. In the summer of 2018, the IFA will be launching the supporting tool SOFTEMA, in beta test at about hundred German companies.

1 INTRODUCTION

Manufacturers of machinery are increasingly using application programming of safety controls in order to implement safety functions. In the past, EN 954-1 defined the requirements concerning the implementation of safety functions. By the end of the 2000s however, this standard had ceased to reflect the state of the art, and was replaced by ISO 13849-1 [1] and IEC 62061 [3], either of which can be applied. The new standards include definitions of requirements concerning the development of software employed for safety functions. The requirements are intended to prevent hazardous systematic errors in the application software employed for a machine. How these new requirements are to be implemented in detail remains unclear to the software developers of safety functions. This is partly because by their nature, requirements in standards are formulated only in very general terms, and up to now virtually no examples of implementation have been published. This situation prompted the German Social Accident Insurance (DGUV), at the IFA's instigation, to fund the project described below.

2 DGUV RESEARCH PROJECT FF-FP0319

In DGUV project FF-FP0319 (Norm compliant development and documentation of safety related application software in manufacturing system engineering) [4] (2011-2013), the project partner, Professor Dr Norbert Becker and his team at the Bonn-Rhein-Sieg University of Applied Sciences, developed several specific procedures for implementing the requirements set out in the new standards concerning the development of safety-related application software for machinery, and evaluated and documented these procedures with reference to industrial examples. The aim was to describe both the procedures and their application in a research report, which was then to be presented to the public as part of a new IFA Report 2/2016 [6].

Two committees were formed for evaluation of the project results during the project term:

- A user group consisting of local industrial companies
- The research support group, comprising representatives of control product manufacturers, accident insurance institutions, the IFA, the VDMA, TÜV Rheinland Akademie, KAN and users

In addition, the method was presented and discussed at a number of industrial companies. The project was divided into the following tasks: development of a method and subsequent evaluation of the method by the user group and the research support group.

Several methods for specification of application software were studied:

- Description of application software as a finite state machine
- Specification by means of checklists
- Specification by means of tables

Describing the application software of an actual machine as a finite state machine in which all operating states are considered is generally a very complex process. Subsequent programming of the application software in a graphical or text-oriented programming language is also completely different. This particularly applies to safety-related software, for which the use of certified function modules is common. Procedures in which finite-state machines are described are not common in machine construction. Finite-state machines are used in the specification of complex safety-related function modules (library modules), which however was not the primary topic of this research project.

A checklist-based method was also developed. The safety functions are described in this method by forms based upon checklists. These forms are progressively refined in the course of further specification. Following presentation in the user group and the research support group, it soon became evident that the checklist-based method was also unsuitable for the development and documentation of safety-related software in an industrial context.

Many companies are however already documenting and specifying safety-related software in the form of tables. Based upon this activity, a matrix-based procedure for specifying and documenting safety software was developed. This met with much greater acceptance when presented to industry.

This procedure, described below as the "IFA matrix method", was positively received by the user group and the research support group. The discussions resulted in numerous improvements to the presentation. Several examples were integrated into this form of presentation in order for as many cases relevant to practice as possible to be described. In addition, a more comprehensive example of a machine tool was implemented in order to demonstrate the IFA matrix method's suitability for describing larger installations.

The IFA matrix method was presented to the public as an interim result of the project at the VDMA workshop on functional safety application software, held on 8 November 2012 in Frankfurt. It was subsequently presented on several occasions to companies and to test bodies. These presentations and publications [5] met with a largely positive reception and resulted in further constructive suggestions.

3 THE IFA MATRIX METHOD

Research project FF-FP0319 has been published in the form of a research report and ten examples illustrating the matrix method. These publications are available online [4][6].

The essential characteristics of the matrix method are:

- The V model of ISO 13849-1 can be simplified and broken down into two small V models. One V model is used for the development of safety-function software, the other for the development of project-specific function modules.
- Definition of documents for execution of the V models. Many of these documents should already be present in the project implementation.
- Breakdown of the software into a pre-processing level, a de-energization logic to be specified, and a post-processing level.
- This enables the de-energization logic to be specified by a cause and effect (C&E) table (Figure 2). The test coverage can be completed by additional test lines in the C&E table.
- Integration of test and verification fields into the documents.
- The quality of the software in accordance with the specifications is assured by the test steps of verification, code review and software validation.

In order to describe the matrix method and its boundary conditions, this paper makes reference to the highly detailed presentations found in the freely available literature [4] [5] and to the SIAS presentation slides, which are also available.

It was intended from the beginning of research project FF-FP0319 that its results would subsequently be formulated and published in an IFA Report [6] on the topic. Besides presenting the development method itself,

the IFA Report will provide the target group with further essential information and interpretations regarding the normative requirements to be met by application software. The changes in the ISO 13849 series of standards, Parts 1 [1] and 2 [2], will also be considered with regard to their relevance to application software.

The project examples are presented in a data format suitable for automated handling by future development tools, such as SOFTEMA, the IFA tool described below. The IFA Report 2/2016 [6] was published in PDF format and also as print version in German language. The revised examples will also be available for download. This new IFA Report thus supplements the familiar IFA Report 2/2017 (updated edition of 2/2008), "Functional safety of machine controls" [9], which is focused more upon the reliability of the control hardware and upon calculation of its probability of failure.

4 THE IFA SOFTEMA TOOL

In order for the IFA matrix method to be implemented efficiently and with assured quality, the IFA is developing the SOFTEMA software tool (refer to the project information page of IFA Project 5137 [7]). Like IFA's SISTEMA tool, SOFTEMA will be available for download free of charge. This paper provides only an overview of the tool's planned features and functions. Further information and assistance for users is made available separately on the SOFTEMA download site or at the SOFTEMA help menu.

The examples using the IFA matrix method that are available for download can be viewed in SOFTEMA (Figures 1 to 3). Users can also use SOFTEMA to create and edit their own projects. SOFTEMA opens a project-specific file for specification and documentation of an application program. Multiple instances of SOFTEMA can however be opened in order for multiple projects and application programs to be worked on simultaneously.

SOFTEMA uses the Microsoft Excel worksheet (*.xlsx) format for its project files. The files can be edited either in SOFTEMA or in Microsoft Excel itself, as preferred. All tables can be edited freely in Excel. In SOFTEMA, the content is write-protected by the user management function. The specialized SOFTEMA functions described below are available only in SOFTEMA. In Excel however, additional table worksheets can be added and used for development and documentation, for example for hardware engineering. SOFTEMA will initially support the following functions:

- Automatic updating of tables following modification of input data
- Formal verification of tables (for missing, conflicting or double entries)
- Management of project members
- Role-based user permissions
- Support during verification, validation and testing
- Support with modifications
- Dedicated editors for the different forms of cell content
- Management of documents and changes
- Specific print functions and reports

The German beta version of SOFTEMA is available for download on the IFA's website [8] from the winter of 2018 onwards. The tool is to be available for use free of charge following registration.

5 SOFTEMA ENGINEERING PROCEDURE

A typical engineering procedure in SOFTEMA is outlined below. Procedures and tips can be found in the "SOFTEMA cookbooks". General descriptions of the SOFTEMA user interface and functions and of the data structures can be found in SOFTEMA Cookbook 1. For subsequent software specification of a safety function, the protective devices and actuators used in this function must be known. Precise definition of the safety functions is therefore indispensable for the subsequent steps (see SISTEMA Cookbook 6 and its examples).

For a new project, open an empty but preformatted project template in the working folder specified at installation. Complete the project description ("Project" table). Then enter the safety functions and their properties such as the PLr, operating mode, priority, etc. in the "AI safety functions" table (Figure 1). Enter/import the input and output signals with their respective variable names and hardware/network addresses in the "A2.4 IO list" table. External content can also be copied and pasted into all tables via the clipboard.

Poster session

_Nr	_SFK	_Beschreibung	_Schutz	_BMK	_NQuit	_SQuit	Q1	B1	B2	B3	_PLr	_Reaktionszeit	_Priorität	_Betriebsart	_Sperr	_Validierung
SF1	-SF10.1	Wenn Not-Halt EMST dann Motor M1 abschalten Motor M2 in STO, Motor M3 abschalten, mit Quittetaster ACK quillieren	Not-Halt	EMST			ACK/Quittetaster	A	STO	A	d	100ms	1	B0: Alle	x	OK
SF2	-SF11.1.1	Wenn Schutzür 301 geöffnet, dann Motor M1 abschalten, mit Quittetaster ACK quillieren	Schutzür	SG1			Q1	A			d	100ms	2	B1: Automatik	x	OK
SF3	-SF11.2.2	Wenn Schutzür 302 geöffnet, dann Motor M2 in STO, mit Quittetaster ACK quillieren	Schutzür	SG2			Q1		STO		d	100ms	2	B1: Automatik	x	OK
SF4	-SF11.3.1	Wenn Schutzüren SG2 und SG3 geöffnet, dann Motor M1 abschalten, mit Quittetaster ACK quillieren	Schutzüren	SG2 & SG3			Q1	A			d	100ms	2	B1: Automatik	x	OK
SF5	-SF11.4.3	Wenn Sicherheitsleiste Schnellläufer SL_SG2 betätigt, dann Motor M3 abschalten, mit Quittetaster ACK quillieren	Sicherheitsleiste Schnellläufer	SL_SG2			Q1		A		d	100ms	2	B1: Automatik	o	
SF6	-SF14.1.2	Wenn Schutzür 302 geöffnet und S55 geschlossen und Zusammentaster 3S1 betätigt, dann Motor M2 in SLS, mit Quittetaster ACK quillieren	Verknüpfung	SG2 & ISG3 & 3S1			Q1		SLS		d	100ms	2	B2: Einrichtbetrieb	x	not OK
SF7	-SF14.2.2	Wenn Schutzür 302 geöffnet und S53 geschlossen und Zusammentaster 3S2 betätigt, dann Motor M2 in SLS, mit Quittetaster ACK quillieren	Verknüpfung	SG2 & ISG3 & 3S2			Q1		SLS		d	100ms	2	B2: Einrichtbetrieb	x	not OK

Figure 1. List of safety functions in SOFTEMA.

_Nr	_Betriebs	_Test	I7	I5	I6	I3	I4	I1	I2	I8	I11	I12	_SF_Prio	_SF-Nam	O1	O3	O4	O2	_Sperr	_Verifikati	_Validierung
C0			1	1	1	1	1	1	1	1	1	0	0	ALLOK	ON	ON	ON	ON	x	OK	OK
C1	B0: Alle	C0	0	1	1	1	1	1	1	1	1	0	0	SF1 (1) Wenn Not-Halt	OFF IM1:	OFF IM1:	NOP	OFF IM1:	x	OK	OK
C2	B1: Automatik	C0	1	0	0	1	1	1	1	1	1	0	0	SF2 (2) Wenn Schutzür	OFF IM2:	NOP	NOP	NOP	x	OK	OK
C3	B1: Automatik	C0	1	1	1	0	0	1	1	1	1	0	0	SF3 (2) Wenn Schutzür	NOP	OFF IM3:	NOP	NOP	o		
C4	B1: Automatik	C0	1	1	1	0	0	0	0	1	0	0	0		NOP	NOP	NOP	x	OK	OK	
C5	B1: Automatik	C0	1	1	1	0	0	1	1	1	0	0	0		NOP	NOP	OFF IM6:	x	OK	OK	
C6	B2: Einrichtbet	C8	1	1	1	0	0	1	1	1	1	1	1		ON not IM5:	OFF IM5:	NOP	o			
C7	B2: Einrichtbet	C8	1	1	1	0	0	1	1	1	1	0	0	SF7 (2) Wenn Schutzür	ON not IM5:	OFF IM5:	NOP	x	OK	OK	
C8	B2: Einrichtbet	C0	1	1	1	0	0	1	1	1	0	0	0	TF1 (2) SG2 offen, SG3	NOP	OFF	ON	NOP	x	OK	OK
C9	B2: Einrichtbet	C8	1	1	1	0	0	1	1	1	1	1	1	TF2 (2) SG2 offen, SG3	NOP	OFF	ON	NOP	x	OK	OK

Figure 2. C&E-Matrix for the software specification of a project in SOFTEMA.

Poster session

The catalogue of measures for error avoidance and the programming rules can be selected and adjusted in the "A3 Measures" table. The safety functions, the peripheral hardware and the I/O list result in a list of the required function blocks for the preprocessing and actuator operation level. These can be managed in the "B3 Module architecture" table. Following these preparations, the "B4 Matrix C+E" table can be completed (Figure 2). The buttons for automatic updating for I/O signals and safety functions are used for this purpose.

The software specification proper is then produced in the "B4 Matrix C+E" table by entry of the logic linking the signals for the switching operations to the output signals (right-hand area in Figure 2). This is required for coding of the actuation logic. A specialized editor assists in creation of this link. At this point at the latest, all available functions for formal verification of the tables referred to must be used, in order for omissions, duplications and contradictions to be detected and corrected.

Following verification of all input documents and the specification described above, the program can be coded. The code is also verified. This process is documented in detail in a number of tables and is also summarized in the "C1 Code review" table. The program is then validated, which is also documented in detail in a number of tables and summarized in the "D1 Validation" table (Figure 3). The questions can be adapted and extended if needed in Tables C1 and D1. Persons subsequently reviewing the project can also document and annotate their task.

Should the safety functions or the I/O signals be modified, the modifications in these tables are in turn automatically updated in the specification table, and edited by the user. All modifications are initially highlighted in colour (yellow). The highlighting is deleted manually when coding, verification and validation of these modifications has been completed again.

_Nr	_Beschreibung	_Referenzblatt	_Validierung	_Kommentar	_Kommentar_Prüfen
Wurden die Aktivitäten durchgeführt?					
V1	Validierung Sicherheitsfunktionen (D1)	A1 Sicherheitsfunktionen	not OK		
V2	Validierung I/O-Check (D1)	A2.4 IO-Liste	OK		
V3	Validierung normativer Anforderungen (D1)	A4 Anforderungen	OK		
V4	Verifikation der Modularchitektur (V1)	B3 Modularchitektur	OK		
V5	Verifikation der Matrix (V1)	B4 Matrix C+E	not OK		
V6	Validierung Matrix (D1)	B4 Matrix C+E	not OK		
V7	Verifikation Codereview	C1 Codereview	not OK		
V8	Prüfung der Peripheriegeräte		OK		
V9	Prüfung der Sensoren		OK		
Ist die Dokumentation komplett?					
D1	Dokumente des V-Modells aus diesem Excel-Dokument		OK		
D2	PDF-Ausdruck aller sicherheitsrelevanten Software inkl. Checksumme		OK		
D3	PDF-Ausdruck der Hardwarekonfiguration (mit allen Einstellungen) inkl.		OK		
D4	Archivierung der Handbücher aller Systemkomponenten		OK		
D5	PDF-Ausdruck der Konfiguration von Peripheriegeräten inkl. Checksummen		OK		
D6	Abnahmevorschriften der Hersteller (z.B. Parametrierung von		OK		
D7	Einzuhaltende Vorgaben aus C-Normen		OK		

Figure 3. Validation sheet of a project in SOFTEMA.

6 CONCLUSION

This paper and the SIAS presentation slides describe a pragmatic and transparent method together with a new tool of meeting the requirements of ISO 13849-1 concerning safety-related application software for machinery. The method is based upon the results of a project funded by the DGUV [4] and forms the basis of the IFA Report 2/2016 [6] on the subject. The basic concepts of the method have already been included in the drafts of ISO 13849-1 [1] and IEC 62061 [3]. The IFA matrix method also forms the basis of IFA's new SOFTEMA tool [7][8], which is for the first time presented more detailed in this paper.

The IFA matrix method presented here can be used for standards-compliant specification, validation and documentation of the application software of safety functions. The procedure is non-proprietary and not specific to a particular programming language or Performance Level. Provided the procedures are followed, it can be assumed that the safety-related application software satisfies the relevant requirements of ISO 13849-1. Besides this procedure, other equally valid methods doubtless exist by means of which the requirements can be met. The IFA matrix method therefore lays no claim to be the only means of satisfying the requirements of the standards.

7 REFERENCES

1. ISO 13849-1: *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (12/2015)*, ISO, 2015.
2. ISO 13849-2: *Safety of machinery – Safety-related parts of control systems – Part 2: Validation (2/2013)*, ISO, 2013.
3. IEC 62061: *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems (10/2005 + A1:2012)*, IEC, 2012.
4. Project page FF-FP0319, *Norm compliant development and documentation of safety related application software in manufacturing system engineering*. DGUV, Sankt Augustin, Germany, 2014. <http://www.dguv.de/webcode/ep54444>.
5. Huelke M., Becker N., *IFA Matrix Method for development of safety related application software*, Proc. of the 8th Int. Conf. Safety of Industrial Automated System, Königswinter, Germany, 2015.
6. Huelke M. et al., *IFA Report 2/2016 - Safety-related application software for machinery – The IFA matrix method (only available as German version)*, IFA/DGUV, Sankt Augustin, Germany, 2016. <https://www.dguv.de/webcode/d1023063>.
7. Project page IFA5137, *SOFTEMA - Tool für sicherheitsgerichtete Anwendungsprogrammierung an Maschinen*. IFA/DGUV, Sankt Augustin, Germany, 2015. <http://www.dguv.de/webcode/dp102081>
8. SOFTEMA Homepage, IFA/DGUV, Sankt Augustin, Germany, 2015. <https://www.dguv.de/webcode/d1082520>.
9. Hauke M. et al., *IFA Report 2/2017 - Functional safety of machine controls (soon be available as English version)*, IFA/DGUV, Sankt Augustin, Germany, 2017. <https://www.dguv.de/webcode/d1099283>.

The Safeguarding Supportive System (SSS) I. Study on Worker's Three-dimensional Location Detection Using Ultra-Wide Band (UWB) System under the SSS

Shimizu S.¹, Ohtsuka H.², Hamajima K.¹, Umezaki S.¹, Matsui K.³, Fukuda T.⁴, Itou H.³,
Takahashi S.³, Hojo R.¹

¹ National Institute of Occupational Safety and Health, Japan (JNIOSH) – Umezono 1-4-6 – Kiyose – Tokyo – 204-0024 – Japan

² ECSSA Consulting & Co – Shinkoiwa 3-4-1 505 – Katsushika ward – Tokyo – 124-0024 – Japan

³ Nihon University – Narashinodai 7-24-1 – Funabashi city – Chiba Prefecture – 274-8501 – Japan

⁴ Nagaoka University of Technology – Kamitomioka1603-1 – Nagaoka City – Niigata Prefecture – 940-2188 – Japan

shimizu@s.jniosh.johas.go.jp
h.otsuka_auto-id@air.ocn.ne.jp
hamajima@s.jniosh.johas.go.jp
umezaki@s.jniosh.johas.go.jp
cskt14086@g.nihon-u.ac.jp (Matsui K)
t-fukuda@vos.nagaokaut.ac.jp
cskt14086@g.nihon-u.ac.jp (Itou H)
takahashi.sei@nihon-u.ac.jp
hojo@h.jniosh.johas.go.jp

KEYWORDS: Safeguarding Supportive System (SSS), ultra-wide band (UWB) System, human factor, residual risk

ABSTRACT

Most of industrial accidents by human factor frequently occur during non-routine work at integrated manufacturing system in Japan. One of the reasons is that safety management system has been accomplished depending on human attentiveness. In addition, it is concerned that machine users at work site do not appropriately perform reduction method of residual risk, which are remained risk after machinery makers applied risk reduction measure. It is necessary to manage worker's entering and leaving the work site perfectly by ICT equipment. Even if worker exists in a blind spot, the existence of him/her should be detected by a third person using some security measure for prevention of dangerous condition, such as miss-restart. In the present study, a 3-dimensional Ultra-Wide Band (UWB) position detecting system, which developed in our laboratory, was used to detect the location and the posture of worker who was existed in a blind spot in the automated manufacturing line. A pilot experiment which examined the usefulness of the 3-dimensional UWB position detecting system was performed. As a result, the 3-dimensional UWB position detecting system could measure the location and posture of the worker appropriately. It is concluded that the 3-dimensional detecting system used in the present study can contribute to guarantee safety of workers in integrated manufacturing system without depending on human attentiveness. Further, the 3-dimensional UWB position detecting system not only prevents the accident when a automated manufacturing line restarts, but also can be applied to check the vital of workers such as heat exhaustion measures.

1 INTRODUCTION

In Japan, Integrated Manufacturing System (IMS) which contains a combination of single machine such as robot, press and/or belt conveyor has been introduced to some industries such as automobile and general machinery industries. Under the IMS, a various type of materials is produced automatically. Under the IMS, workers are usually prohibited to step into the worksites during routine work, that is, when robots are working. If workers need to access to the IMS worksites during routine work, workers must stop all machines existing in the IMS. Though “the principle of isolation and stop” which is described in the risk reduction method in the ISO12100 is still valid and rigorous, we have to prepare a novel safety protective system which is available for the recent

working style in Japan. This is because workers sometimes are required to work without stopping machines, for example, maintenance, cleaning and teaching works for robots as none-routine work. In fact, almost of all labour accidents has happened during the none-routine work because safety at such work is dependent on workers' attentiveness. According to Umezaki et al. (2005), 44%, out of 124 lethal accidents in Japan during 1989-2005 have occurred at danger point approach work. Especially, one of the most severe problems is mis-restart by the third person who cannot recognize another worker working at the worksite. If locations of all workers in the IMS can be detected with information and communication technology (ICT) equipment instead of human attentiveness, the risk of labour accidents during none-routine work under the IMS would be reduced. In addition, with setting up the 3-dimensional ICT, not only location detection at blind area but also posture and/or health check of workers would be measurable. We established a novel safety system named Safeguarding Supportive System (SSS) focusing on the residual risk after taking the three-step method for safety. The SSS monitors entering and leaving of the IMS work site and worker's location, and controls qualification and authorization of worker and location of work by the combination of ICT equipment.

2 PURPOSE

In the present study, we focused on detecting location and posture of workers using 3-dimensional ICT equipment, Ultra-Wide Band (UWB) position detecting system, as a part of the SSS. We aimed to quantitatively measure the location and posture of worker for estimating condition of worker. By this, indexes acquired in the present study would be able to be applied to actual work sites in near future.

3 MATERIALS AND METHODS

A model of an IMS work site (an area surrounded by pale red in Figure 1A) was built in an experimental room of the National Institute of Occupational Safety and Health (JNIOSH, Tokyo Japan). The experiment was conducted from 10:00am. **Experimental work site:** The experimental work site was surrounded by metal grids of 3.5cm pitch (Figure1A). **Work area:** We estimated worker's behaviour in the work site by measuring line of flow and height of subject by the 3-dimensional UWB system. A measurement space where movement of worker was measured was selected as a work area (Figure 1B).

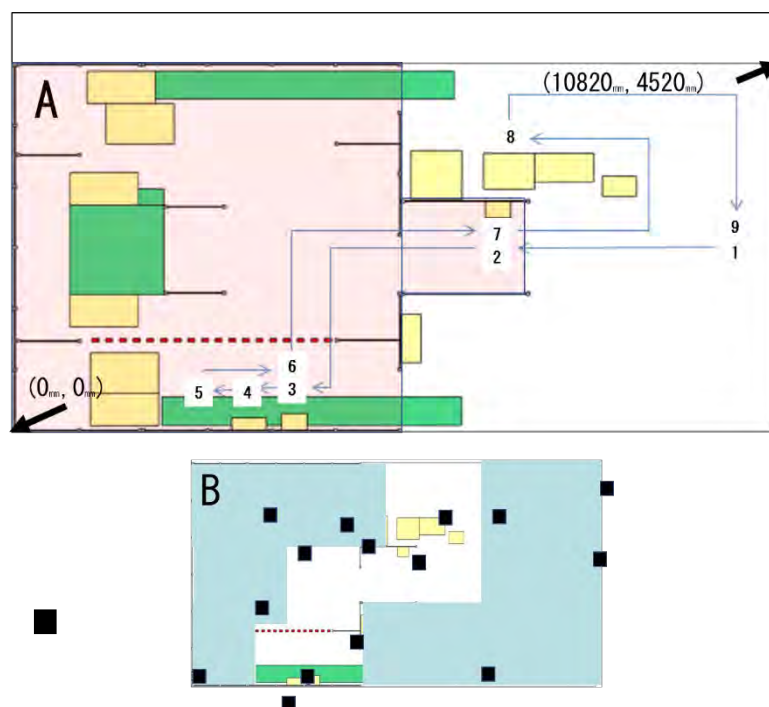


Figure 1. A) Experimental work site (surrounded by black lines). Yellow and green squares are machines located in the work site. Numbers from 1 to 9 express the order of movement of the worker. B) Measurement area (white floor) by the UWB system. Black squares indicate fixed equipment (signal receivers) of the UWB system.

We estimated the worker's status in the work area by measuring line of flow and height of subject by the 3-dimensional UWB system. **Subject:** A male subject holding an active mobile equipment, a radio frequency identifier (RFID) tag, in his chest pocket attended the experiment. When the experiment started, he moved from 1 to 9 (Figure 1A), in the experimental work site and conducted easy work, button pushing, at 5 (Figure 1A). At the

5, he pressed button with standing posture and then did the same thing with bending posture. Range of the height of the subject was set as 150-180cm. **Measurement of the line of flow and movement of the subject:** 1) He operated a main terminal at the entrance of the experimental work site, then stepped into the experimental work site. At the main terminal, he registered himself as a worker who would work at a work area of the experimental work site, and selected a work area and content of the work. Then he entered the work area. 2) At the work area, he operated an area terminal then registered himself as the worker and the content of work. 3) He was started a button pressing work with standing posture. Then he was engaged in the same button pressing work with bending posture. 4) At the work area, he operated the area terminal and declared completing the work after the button press work, then he got out from the work area. 5) He operated the main terminal and operated the completion of the work. (6) He went to a control box which was located out of the experimental work site, and he restarted whole machines in the work area. **Measurement of the Z axis:** We measured position of the worker by a change of the height, and acceleration and inclination of the RFID tag for estimation of the worker's status. **Fixed equipment and coordinates:** There were 15 fixed equipment in the measurement area (black squares in Figure 1B), coordinates from (0mm, 0mm) to (10820mm, 4540mm), for receive the signal from the RFID tag (Table 1). **Definition of posture status of the subject:** We defined posture of standing and bending of the subject with each axis before experiment. We defined heights of standing and bending as >1400mm and bending <600mm with Z axis. Also, inclination of standing and bending were defined as around 90 degree and <90 degree with X axis, and acceleration of standing, around 125mm/s² and bending, >85mm/s²(Figure 2).

Table 1. Location of fixed equipment and coordinates.

		unit[cm]		
	Fixed Equipments #	Coordinates		
		X	Y	Z
1	1001	607	249	170
2	1002	313	14	153
3	1003	473	288	211
4	1004	246	279	193
5	1007	1077	230	173
6	1008	765	25	47
7	1009	450	97	33
8	1011	395	349	155
9	1013	1093	389	203
10	1014	196	398	152
11	1015	192	159	181
12	1016	5	22	49
13	1017	852	338	83
14	1018	278	-45	18
15	1019	675	345	130

4 RESULTS

4.1 Posture of the worker

Change of posture of the worker was measured by signal from an accelerator built in the RFID tag. By plotting the signal chronologically, status of worker was able to classify as walking, stop and bending (Figure 2). As actual posture were not fit to defined data, we redefined the posture estimation as Table 2.

4.2 Inspection of change in Z axis by X coordinate axis.

Bending and standing postures were seen in the working area (Figure 3). Such changing posture was detected by the change of z axis.

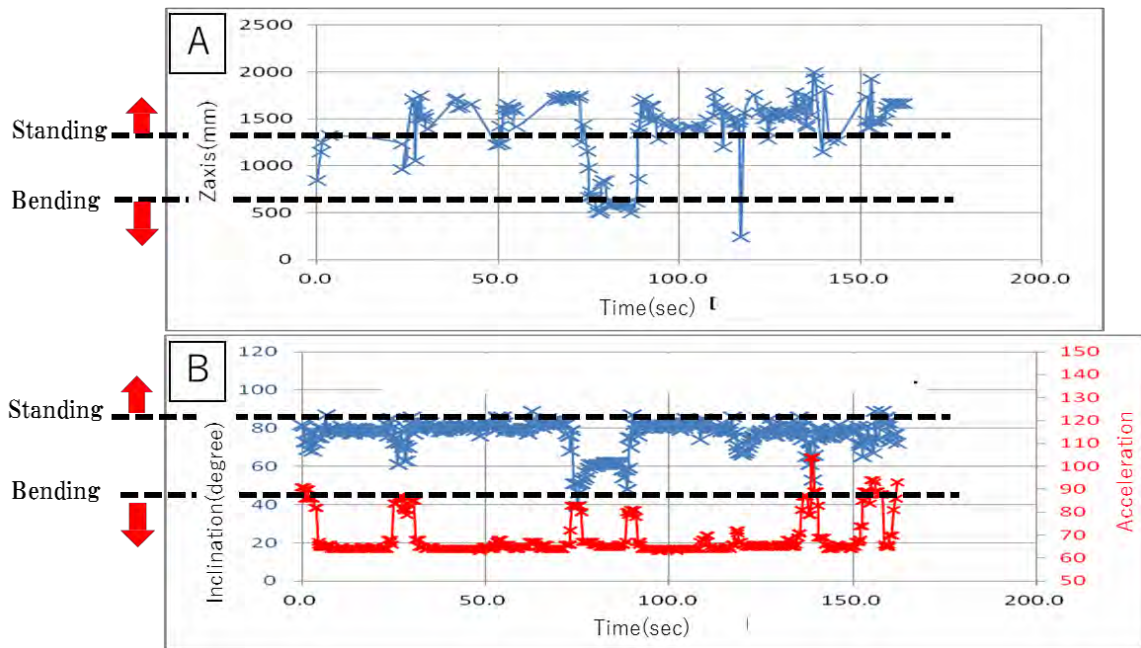


Figure 2 A) Defined heights of standing (>1400mm) and bending (<600mm) by data from Z axis. B) Defined inclination (blue) of standing (around 90 degree) and bending (<90 degree), and defined acceleration (red) of standing (around 125mm/s²) and bending (>85mm/s²). All data was plotted by time.

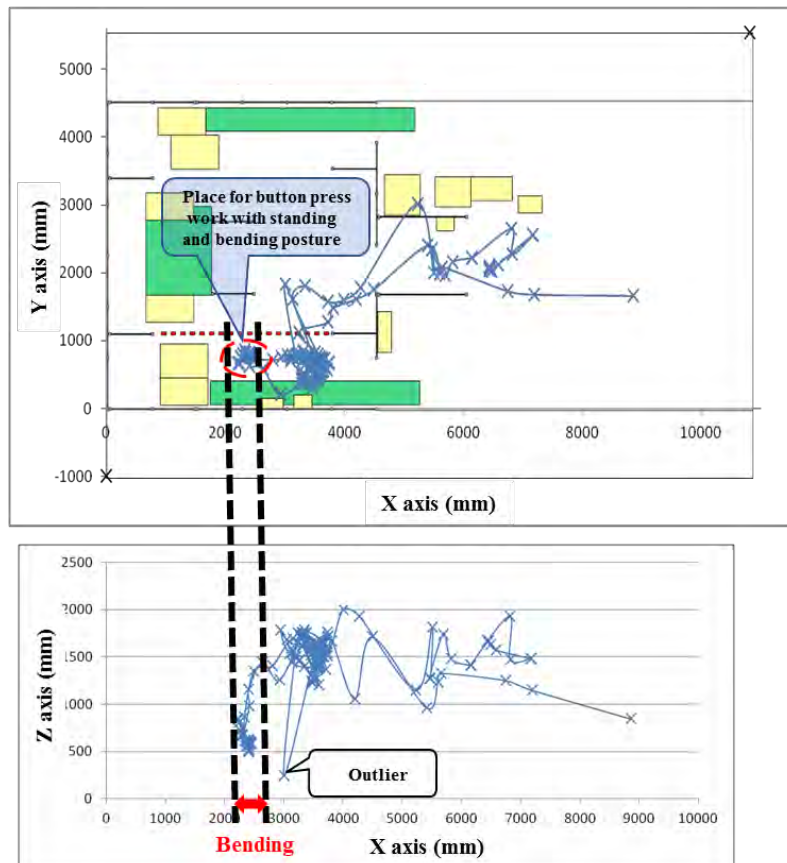


Figure 3. Upper panel indicates movement trace of the worker in the experimental work site. Horizontal and vertical axis were data from X and Y axis (mm), respectively. Bottom panel was indicated height (Z axis) of the worker. Horizontal axis was X axis. The worker was bending at the point between beaked lines.

Table 2. Actual estimation of the worker's status by inclination, acceleration, height and the time.

Status	Inclination (degree)	Acceleration (G)	Hight of Z axis	Results of measurement	Time	Estimation
Falling	30>	200<	1m	Measurable/not moving	Longer than setting time	Falling
Crouching	30>	200>	1m	Measurable/moving		Normal
Walking	30<	200>	1m	Measurable/moving		Normal
Galloping	30<	200<	1m	Measurable/moving		Normal

5 DISCUSSION

As results of the present study, it was clarified that estimation of the worker's status in the work site was possible by combination measurement of Z axis, elapsed time, inclination, acceleration and propriety of measurement. It was suggested that worker's status was able to estimate precisely if appropriate number and location of the fixed equipment were considered. By use of a combination of an acceleration sensor which was installed in the RFID tag and the RFID tag, measurement of the Z axis and monitoring of the subject was precisely and substantially enabled. In addition, place of the present study for a position estimating can be requested with a detail because it's flexible in an installation site. More this equipment can be improved by readjusting after beginning of the mission.

6 REFERENCES

1. Umezaki S., Shimizu S., Analysis of Fatal Accidents Caused by Industrial Machines, Specific Research Reports of the National Institute of Industrial Safety, NIIS-SRR-NO.33(2005), 53-67.

Safeguarding Supportive System III

The new approach using ICT in IoT ear on safety management from information communication to prediction and control of human behavior

Hamajima K.¹, Shimizu S.¹, Umezaki S.¹, Tsuchya M.², Hojo R.¹

¹ National Institute of Occupational Safety and Health, Japan (JNIOOSH) – Umezono 1-4-6 – Kiyose – Tokyo 204-0024 – Japan

² Advantage Risk Management Co., Ltd. – Nakameguro GT Tower 17F 2-1-1 – Kamimeguro – Meguro-ku – Tokyo 153-0051 – Japan

hamajima@s.jniosh.johas.go.jp

shimizu@s.jniosh.johas.go.jp

umezaki@s.jniosh.johas.go.jp

m-tsuchi@umin.ac.jp

hojo@h.jniosh.johas.go.jp

KEYWORDS: information technology (IT), Safeguarding Supportive System (SSS), safety management system, behaviour analysis, internet of things (IoT)

ABSTRACT

Recently, there is increasing interest in Industry4.0 and/or Safety2.0 in all of the world. Also, some proper evaluation method to a safe management system are desired for worker's safety in Japan. A safety management system using information technology (IT) has been proposed and developed in our laboratory in 2008. With the development of the current information system, the safety management system began to attract attention to people who manage safety at various work sites in Japan again. At the developing period of the management system, we performed interview and subjective questionnaire as evaluation methods of the system from Psychological point of view. However, we realized that the interview and the questionnaire did not present objective, direct and quantitative change of work performance before and after the management system introduction, because the interview and the questionnaire did not directly measure behavior of workers. We realized that objective methods should be introduced in evaluation of the safety management system.

Now we newly established another safety management system named Safeguarding Supportive System (SSS), which focuses on prevention of residual risks derived from human factors with combination of IT equipment. From scientific point of view, prediction and control of human behavior, and quantitative evaluation are indispensable for safety management using IT equipment. Under some experiments for evaluation of the SSS, we found that behavior analysis, which is one of Psychological approach, was useful for measurement of human behavior. Based on this indication, we propose that the essential meaning of using information and communication technology in the field of industrial safety is not to increase the efficiency and safety of operations but to predict and control human behaviors. We also propose that to realize this, theories in psychology are required, specifically knowledge of behavior analysis.

1 INTRODUCTION

Recently, interest in Industry4.0 and/or Safety2.0 are increased in all of the world. It is because many manufacturing industries in Japan introduce integrated manufacturing system (IMS), safety management system is now shifted from stop and isolation principles to cooperative safety. Also, some proper evaluation method to a safe management system are desired for worker's safety in Japan. More than 10 years ago, Japanese government, Ministry of Health, Labor and Welfare (JMHLW), has tried to introduce safety management system using information technology (IT) because Japan has faced to a serious crisis that was so-called '2017 problem'. The problem was about loss of full-experienced workers, who supported work progress and safety at all over the workplace in Japan. During the period of high economic growth, the workers have built up economic superpower and contributed to develop manufacturing system in Japan. Huge number of these workers have been retired on 2017. In addition, 40% of lethal labor accidents in Japan happens under conditions in which are difficult to apply the equipment measures. In such conditions, safety relies on the attentiveness of human. These were the reason why Japanese government decided to introduce IT to workplace for management of workers safety instead of attentiveness of human. In our institute, National Institute of Occupational Safety and Health,

Japan (JNIOH), a project of safety management system using IT has been studied from 2008-2011 as a collaboration with JMHLW and The Iron and Steel Institution of Japan (ISISJ).

2 The PROJECT of SAFETY MANAGEMENT SYSTEM using IT in 2008-2011

[Purpose of the project]

At that time of the project, project team had clear vision of the goal. It was establishment of the safety management system which was hard to evoke unsafe behavior. We thought that the most important things were secure delivery of information and construct of understandable information for prevention of error, mistake and/or unsafe behavior of workers because behavior of workers was guided by information. In other word, we tried to establish the safety management system for control of worker's behavior, though a word as "control behavior" was not used in the project then.

[Results and products of the project]

The products of the project were design guide books for entrepreneurs who were planning to introduce the IT management system in their industries. The contents of these books were about a basic idea of the IT management system, the way of select the spec of the IT and considerations. We interviewed workers and gave questionnaires to workers whether the safety management system using IT was useful and/or effective. Answers of both interviews and questionnaires were totally positive.

[Problems]

Even if correct information is given to workers using ICT, safe behavior may not increase. We had to evaluate the behavior modification of workers based on the procedure of behavior analysis. We asked workers effectiveness of the IT management system by the interview and questionnaire, but that wasn't objective evaluation. We only asked workers' impression about the safety management system using IT. There was another problem. It was the procedure of interview and questionnaire. The interviews and questionnaires were carried out in front of the members of the project. We now think that those should be done with blind. Workers did not have atmosphere to choose negative answer against the safety management system using IT.

[Future perspectives]

We are planning to introduce behavior analytical procedure for evaluation of the safety management system using IT. Specifically, we'll measure change in workers' safety behavior quantitatively. We will compare safety behavior before and after introduction of the safety management system using IT. Then we think that we will be able to acquire the objective evaluation of the effectiveness of the safety management system using IT.

Prototype Making of a Fail-Safe Interlock System for Pneumatic Control Systems

Nakamura M.¹, Ino M.¹, Mitsuhashi K.¹, Sasaki T.¹,
Hara K.¹, Ichikawa O.¹, Chiba M.¹, Sujino T.², Ishizuka T.³

¹Polytechnic University of Japan - 2-23-1- Ogawanishi-machi - Kodaira-shi - Tokyo - 187-0035 - Japan

²Bergische Universität Wuppertal - Gaußstr., 20 - D-42119 Wuppertal - Germany

³R&D Division, Sanwakouki Corporation - 12-2 - Sanwa Bldg.- Kandamikura - Chiyoda-ku,
Tokyo - 108-0038 - Japan

nakamura@uitech.ac.jp
sujino@uni-wuppertal.de

KEYWORDS: pneumatic driving system, fail-safe interlock, safety control, regulating (Avoidance) control

ABSTRACT

In general, various components used for pneumatic control systems are higher in power density required for driving than electric motors, etc. For this reason, they are widely used as a high-output device in various fields. However, various components configuring a pneumatic control system might cause harm to humans due to container explosion, high-pressure air blowoff or the like attributable to hazardous side failure (error) derived from failure or improper control, or resultant fly-off of flinders or parts. In view of these problems, an interlock system, which can resolve hazardous side failure in pneumatic control systems based on the principle of safety (confirmation) has been proposed (hereinafter referred to as “interlock system”). In these circumstances, this research makes a report on the design and manufacture of experimental equipment using the configuration and pneumatic circuits of a typical pneumatic control system for being equipped with the interlock system, prototype making of a monitoring device using window characteristics (window monitoring device) for detecting pressure behavior, and an experimental method to confirm the operation of the interlock system and verifying the performance thereof.

1 INTRODUCTION

Pressure control in a pneumatic control system might cause harm (accident) due to high-pressure air blowoff, container explosion or the like attributable to hazardous side error of control and hazardous side failure (error) of various components configuring a pneumatic control system. In view of this, the authors proposed configuration logic of an interlock system in 2013, which was capable of resolving hazardous side failure in pneumatic control systems based on the principle of safety (confirmation) as the ground for the validity of safety (hereinafter referred to as “interlock system”)^[1]. The authors concluded that the interlock system was a practical safety-related unit (system) compatible with the International Standard (ISO)^[2] in 2014, though the authors have not yet made a prototype of the proposed interlock system. In these circumstances, in order to promote the practical use of the interlock system, this research paper makes a report on how to make a prototype of the window monitoring device, and how to check the operation of the interlock system and verify the performance thereof by experiment using a prototype of the window monitoring device.

2 CONFIGURATION LOGIC OF THE FAIL-SAFE INTERLOCK SYSTEM FOR PNEUMATIC CONTROL SYSTEMS

The interlock system is safety confirmation type configured with the ground of the validness of safety based on the principle of safety (confirmation) that “the permission of hazardous mechanical operation is conditional on the confirmation of safety” in order to cope with hazardous side failure in the pneumatic components and hazardous side error (pressure increase) in the regulator^{[3],[4]}. In the operation of the interlock system, a threshold is set each at the upper limit and lower limit of pressure, and when pressure is detected inside the range between the upper-limit threshold and the lower-limit threshold (hereinafter called “window”), the shutoff valve “opens” and compressed air is supplied to the driving system, and when pressure is detected outside the window, the shutoff valve “closes” and the supply of compressed air is shut off and the remaining compressed air is exhausted. As shown in Fig. 1, the interlock system is installed in such a way that a sensor for monitoring the window (hereinafter called “window monitoring device”) is set between the power control unit and the directional control valve inlet, and a shutoff valve is set between the dryer and the safety valve. The window monitoring device and the shutoff valve are set in a portion assumed to be the weakest (piping) among all

components configuring the pneumatic control system of Fig. 1. As shown in Fig. 2, the interlock system is made up of 3 components: window monitoring device, window comparator^[5] and shutoff valve. These components have asymmetric failure mode characteristics requesting safety side failure. As shown in Fig. 3, the window monitoring device, among them, is configured in such a way that the distal end of the bourdon tube has a slit to enable power control to be maintained to the normal level while light passing through the slit is being detected by the photointerrupter, and, in case of failure, current is mechanically prevented from being outputted, though a prototype of the window monitoring device has not yet been made.

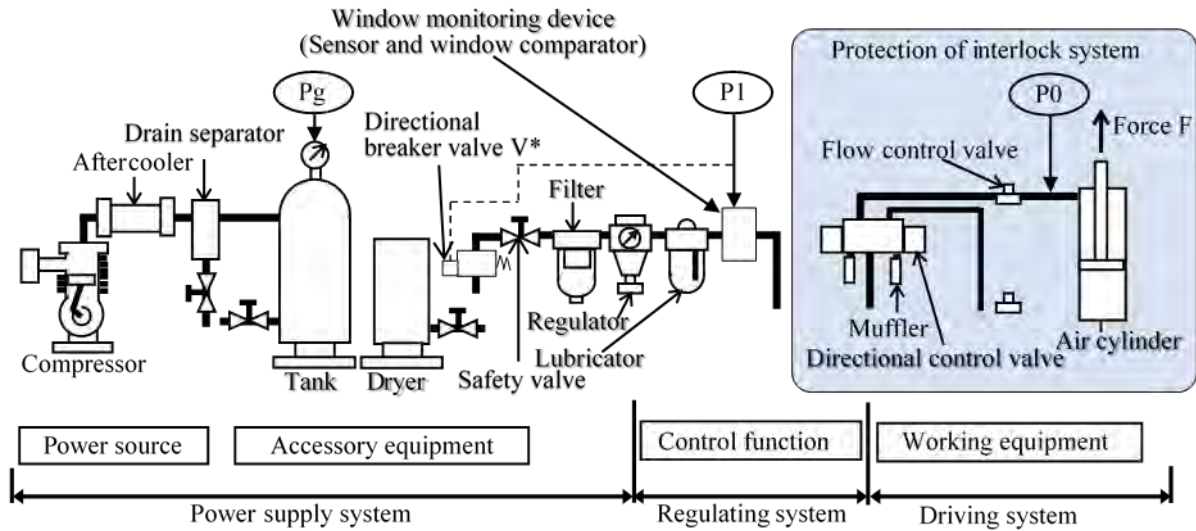


Figure 1. Typical configuration of pneumatic control system^[1].

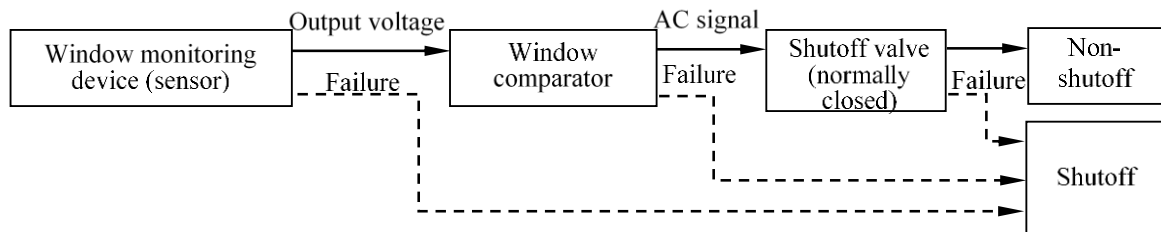


Figure 2. Configuration and operation of interlock system^[6].

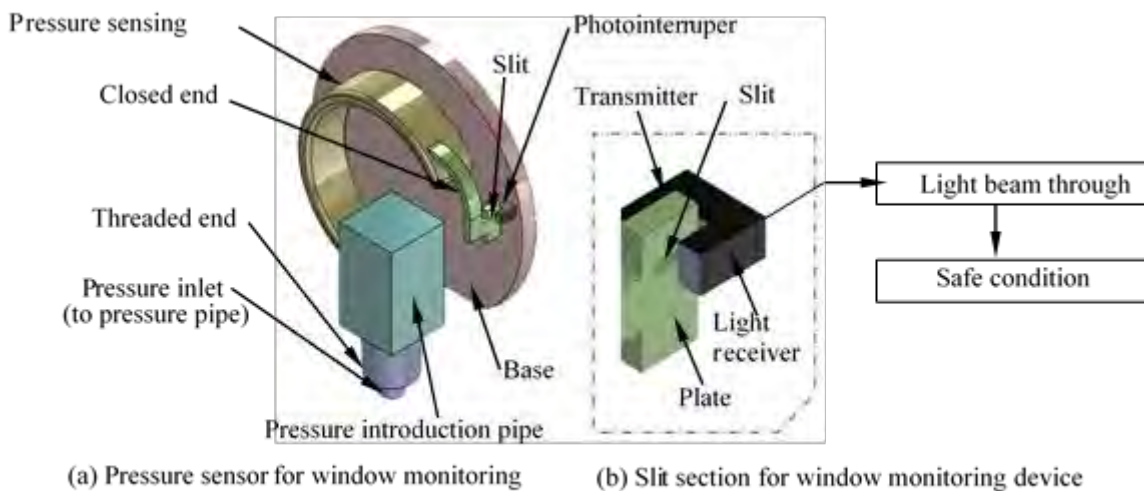


Figure 3. Configuration of window monitoring device (window comparator)^[1].

In the window monitoring device, where the power control unit output is P1, the upper limit threshold of the window is Pu, and the lower limit threshold of the window is Pd, and the window monitoring device output is B1, the thresholds are expressed as shown by Equation (1):

$$B1 = 1; Pu \geq P1 \geq Pd \tag{1}$$

$$B1 = 0; P1 \geq Pu \text{ or } P1 < Pd$$

Furthermore, where the output for window monitoring device and power shutoff is B0, the establishment of the relation as shown by Equation (2) (unate logical relation) is a condition of operating permission with the shutoff valve in the “OPEN” position. That is, according to this relation, when the window monitoring device output is zero (B1 = 0), there is no output for power shutoff^[5].

$$B1 \cong B0 \tag{2}$$

Equation (2) requests for a configuration which does not permit the shutoff valve to “open” in case that the interlock system fails, and also energy (high-pressure air) is invariably exhausted. Fig. 4 shows the configuration logic of the interlock system, where M indicates the normal operation by the regulator. The interlock system can be expressed by equation as shown in Equation (3), where P1(S) indicates the secondary power source output where the machine operation output is S and the power source is P1, P1* indicates the normality of power shutoff, and &* indicates the interlock function (logical AND function).

$$P1(S) = B1(Si) \cdot M \cdot P1^* \cdot \&^* \tag{3}$$

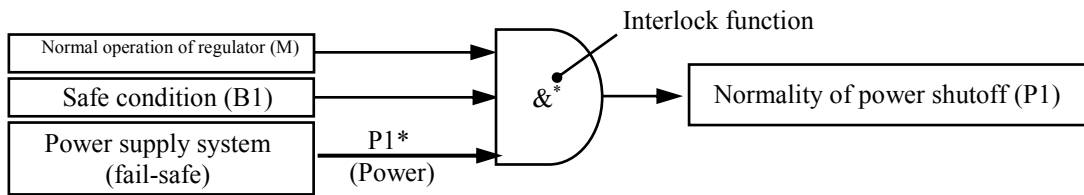


Figure 4. Fail-safe interlock for pneumatic driving system^[5].

3 PROTOTYPE MAKING OF WINDOW MONITORING DEVICE

The window monitoring device used for the interlock system is one of the safety confirmation type systems. It is designed in such a way that the following requirements (1) through (4) can be satisfied:

- (1) Output is permitted when the safety has been confirmed.
- (2) Fail-safe characteristics are provided which does not permit output if the safety has not been confirmed (hazardous, unsafe).
- (3) Hazardous side error is not permitted.
- (4) No error is permitted for the safety conditions.

Fig. 5 shows a prototype of the window monitoring device with a slit of 0.4mm × 1.6mm wide and a window of 0.2MPa wide based on the window monitoring device configuration of Fig. 3. The optical axis of the photointerrupter passes through the slit in the plate, and is detected by the light receiving unit. In this state, the LED is ON, and AC signal is outputted on condition that it transmits the output. However, if the pressure cannot be confirmed to be within the thresholds, the optical axis is blocked out by the plate to disable the detection by the light receiving unit. In this state, the LED remains OFF and the AC signal remains not outputted. Furthermore, according to the configuration, even if any of the components of the window monitoring device fails, the AC signal remains not outputted.

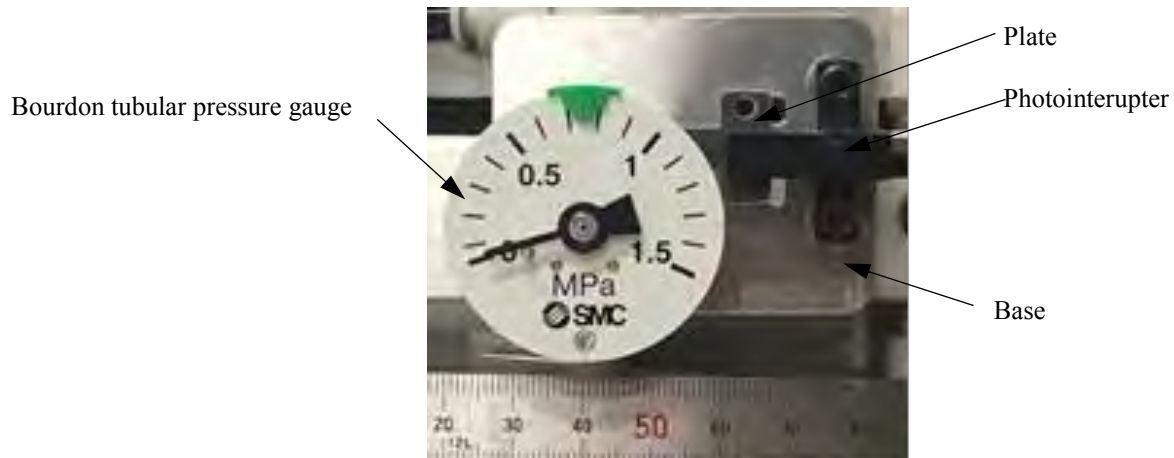


Figure 5. Prototype of window monitoring device.

4 METHOD OF EXPERIMENT

4.1 Objective of experiment

The objective of this experiment is to verify the below-listed items (1) through (4) by making a prototype of the interlock system based on the configuration logic described in Chapter 2 above and incorporating the prototype into actual equipment. For the experiment, experimental equipment made up of pneumatic components within the protective range of the interlock system and test equipment which can reproduce the failure mode are manufactured.

- (1) Confirming the validity of FMEA (Failure Mode and Effects Analysis) for the pneumatic components and the interlock system
- (2) Confirming the operation and verifying the performance of the interlock system
- (3) Confirming the fail-safe characteristics of the interlock system
- (4) Confirming the stopping performance of the of the interlock system

4.2 Experimental equipment

In the experimental equipment shown in Fig. 6, the pneumatic control system normally operates to monitor the pressure behavior through the window monitoring device, generate the failure mode which causes hazardous side failure to various pneumatic components, and thereby confirm the operation and verify the performance of the interlock system. For this purpose, the pneumatic circuit of the experimental equipment is configured as shown in Fig. 7. The pneumatic circuit shown in this figure is made up of two circuits: A-circuit which normally operates, and B-circuit which causes hazardous side failure to various pneumatic components to activate the interlock system. In examining the interlock system, failure analysis (FMEA) is performed, and the hazardous side failure and the safety side failure are examined for the case of failure mode generation in order to verify the relation between the failure in various pneumatic components and the pressure behavior and the fail-safe characteristics of the components configuring the interlock system. In this context, test equipment is manufactured with various components incorporated with the failure mode extracted by FMEA in order to experimentally reproduce hazardous side failure and safety side failure in case of failure mode occurrence. In experiment, the test equipment incorporated into the B-circuit of Fig. 7 is used to practically perform the verification items (1) through (4).

4.3 Experimental method

The experiment is conducted on the air cylinder, the speed controller and the solenoid directional switching valve, which make up the B-circuit, 5 different pneumatic components, which make up the driving system for the piping, and 3 different components of the window monitoring device, the window comparator and the shutoff valve, which make up the interlock system. In the experiment, the test equipment is incorporated in the B-circuit of Fig. 7 and normally operated in the A-circuit to switch the A-circuit to the B-circuit through the operation of the system switching valve and confirm the stopping operation (power shutoff: Shutoff valve in the “CLOSE” position) by the interlock system, and thereby the verification items (1) and (2) can be verified. For the

verification item (3), the test equipment for 3 different components, which make up the interlock system, are incorporated into the experimental equipment, and whether the interlock system is activated to stop the pneumatic control system (safety side failure) or not (hazardous side failure) in case of its failure. For the verification item (4), change in the output signals from the window monitoring device and the window comparator, and the time required to stop the pneumatic control system are measured for a period from failure to stop, and thereby the stopping performance by the interlock system is verified.

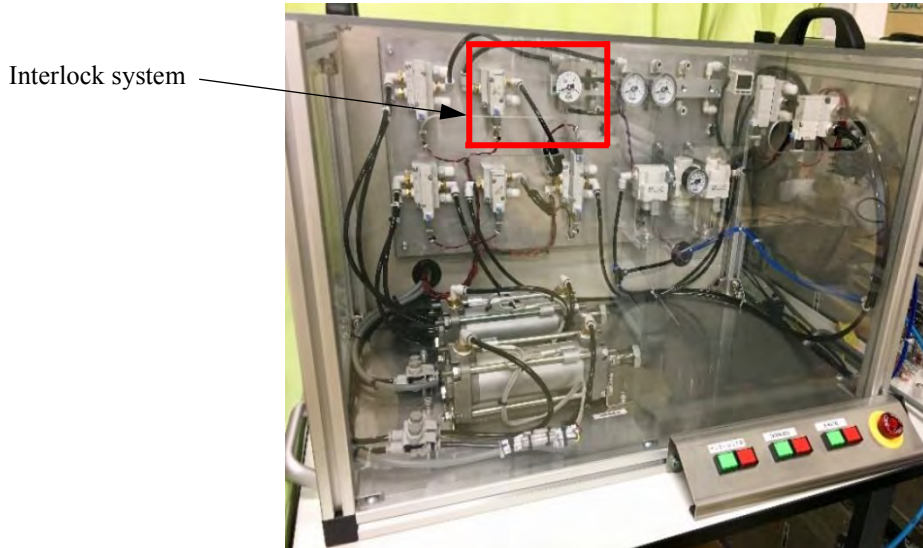


Figure 6. Experimental equipment.

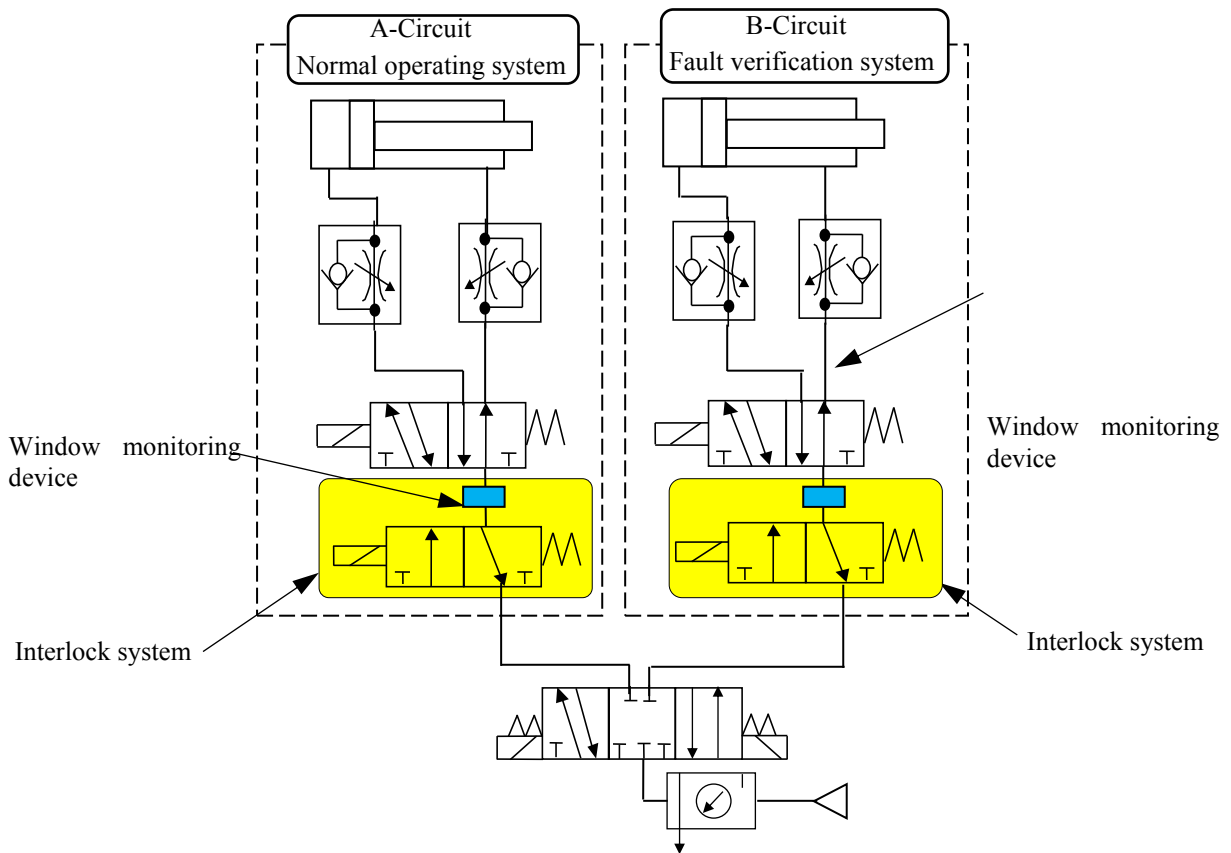


Figure 7. Pneumatic control circuit of experimental equipment.

5 CONCLUSION

This research paper reports the configuration logic of the interlock system, the prototype making of the window monitoring device, and the experimental equipment and method. Until now, the manufacture has been completed for the experimental equipment and the testing equipment. For the window monitoring device, as many devices as required for the reproduction experiment of the failure mode have been manufactured. Also, the window monitoring device is comparatively checked with commercially available pressure switches having window characteristics. For the window comparator, because commercially available one has been searched for but in vain, the authors are considering the manufacture on their own. In addition, the authors are examining the procedure for conducting an experiment on the stopping performance of the interlock system.

In the future, the authors will repeat the experiment on the verification items (1) through (4) of Section 4.1 and present the requirements for productization. This research is undertaken with the grant of JSPS (Japan Society for the Promotion of Science) Grant-in-Aid for Scientific Research Fund JP16k01310.

6 REFERENCES

1. Nakamura M., Tanaka S., Sugimoto N., *Proposal of interlocking system for solving hazardous side of error in pneumatic driving system*, Trans. JSME, Series C, Vol. 79, No. 805 (2013), pp.167-177 (in Japanese).
2. Tanaka S., Sugimoto N., Nakamura M., *Validation of interlock-system of pneumatic driving system as a safety related parts defined in ISO 13849*, Trans. of the JSME, Series C, Vol. 80, No. 814 (2014), pp.1-17 (in Japanese).
3. Sugimoto N., Kumekawa S., Fukaya K., Shimizu S., Umezaki S., Ikeda H., Houshi T., Futsuhara K., *Fundamental structure of safety of the safety confirmation type: About the condition of safety confirmation structure*, Transactions of the JSME, Series C, Vol.54, No.505(1988), pp.2284-2292 (in Japanese).
4. Sugimoto N., Futsuhara K., *Principles of safety*, Trans. JSME, Series C, Vol. 56, No. 530 (1990), pp.2601-2609 (in Japanese).
5. Futsuhara K., Mukaidono M., *A method for constructing interlock system using fail-safe logic device with window characteristics*, Transactions on Electrical and Electronic Engineering, Series C, Vol.109, No.9(1989), pp.676-683 (in Japanese).
6. Nakamura M., Okabe M., Sugimoto N., *Consideration of Interlock System Applicable to Pneumatic Driving Systems as the Safety System (EN764-7)*

A fundamental safety system for machine operators

Otsuka K.¹, Sujino T.², Hoshi T.¹, Nakamura M.³, Sugimoto N.¹

¹ Nagaoka University of Technology - 1603-1 Kamitomioka - Nagaoka - Niigata - 940-2188 - Japan

² Bergische Universität Wuppertal - Gaußstr.20 - D-42119 Wuppertal - Germany

³ Polytechnic University of Japan - 2-23-1 Ogawanishi-machi - Kodaira-shi – Tokyo - 187-0035 - Japan

s145043@stn.nagaokaut.ac.jp

sujino@uni-wuppertal.de

KEYWORDS: risk management, occupational safety, risk assessment

ABSTRACT

Accidents are inherently hard to predict. Nevertheless, one can make deductions about the possibilities of accidents happening while generating a new product.

The safety zone is defined as the time between realizing that there might be an accident and the accident happening. “Outside of the safety zone” means that there is no knowledge about accidents happening. There is a point in time that defines a crossroad between realizing the accident (inside the safety zone) and not realizing it (outside of the safety zone). A definitive safety system can be established from that point. The authors called it fundamental safety system.

At first this paper refers to two different safety approaches, the probabilistically-based and the deterministically-based, to emphasize the necessity of the aforementioned innovative safety system.

Second, new indicators for safety are shown, which focus more on human life, while at the same time not reducing social risk.

Third, these safety measures are explained. Specific safety zones, which are required to ensure the “halt before the accident”, along the time axis are defined.

<Sr> is the monitoring of safety, <Se> is the qualified safety deducting the time for halt before the hypothetical accident. <Sc> is the confirmed safety including uncertainties deducting the time for preparation to stop. These specific safety zones shall have an unate logic. This fundamental safety system is compatible with the safety confirmation system, providing deterministic measures to keep harm from the operators.

Eventually, this safety system is proven as the logical structure of safety with factors of time, space and preventing harmful hazard by cutting off energy transmission.

1 INTRODUCTION

Generally, the safety evaluation of machinery follows the risk-based approach. It can be a key index of expected damage(s) to the society. However, it may fail to respond to the purpose of safety engineering in some points. For instance, the safety system aims at anticipating future accident and to establish a mechanism which can stop the event or avoid the occurrence. Preventing accidents or disasters is the inherent purpose of safety. On the other hand, the risk is interpreted as a social concept to reduce negative factors to the society. The purpose of a safety system is to prevent a damage-causing accident of a human, emphasizing on the individual (basically the scope of safety is human life). In contrast the purpose of risk management in probability-based systems is to reduce negative impact to the society to an acceptable level. This inconsistency of the purposes of safety and risk, however, is not widely recognized. The ISO/IEC Guide 51^[1] defines safety as ‘freedom from the risk which is not tolerable’, which is what can be obtained as a result of the risk reduction process in probability-based systems.

This paper aims at clarifying the open aspects of the risk-based safety and to propose a deterministically-based approach for operators' safety.

2 RISK-BASED EVALUATION IN ISO/IEC STANDARDS

ISO/IEC Guide 51^[1] including ISO 12100^[2], requires risk reduction by a three-step method to ensure product safety. Tolerable risk in above mentioned safety definition is explained as ‘level of risk that is accepted in a given context based on the current values of society’. In this context, safety is not a personal but a social issue. IEC 61508-5^[3] added a cost-effectiveness factor to this risk-based concept according to the ALARP principles, stating ‘a cost-benefit assessment is required either explicitly or implicitly to weigh the cost and the need or

otherwise for additional safety measures.’ It should be noted that the risks which are classified within the ALARP region still include catastrophic or critical consequences, even though their probabilities are estimated as low. Safety defined by ISO/IEC Standards implies some uncertainties due to its probabilistic and/or cost dependent factors of safety measures and therefore risk management is required for those uncertainties. However catastrophic or critical consequences is a personal issue to those who would suffer the events. Moreover, the loss of human life is not recoverable by any compensation through insurance. Hence, the safety is not social issue. It is prevention from a personal catastrophic event.

3 RISK REDUCTION BASED ON RELIABILITY

Occupational accidents can be categorized into two types, A or B, as proposed by Umezaki^[4]. Type A is for those that are non-fatal but of high probability and type B is for the fatal ones, which have a low probability. If safety could be ensured by risk reduction, these two types, A or B, might be evaluated in the same category of the same risk index. It should be noted that type A are of lesser importance for the purpose of safety, due to their less severe and shorter harm, bringing fewer inconveniences for the people’s life. For those accidents, due to the smaller expected harm, high reliability of machines would be satisfactory to reduce total risk, and the residual risks are not relevant to safety. On the other hand, concerning type B accidents, highly reliable machines are already used but still the possibility of severe accidents is remaining and relevant. Therefore, the safety structure should be prepared to prevent the type B accident. If an accident can be defined as an interference of a person and a machine, a specific condition must be defined in advance in which people and machine are separated by an appropriate distance in the field and/or in the time to avoid their contact. The interlocking of the safety structure keeps the condition of the machine outside of contact with people theoretically and the original function will be stopped before any harm is done whenever the system detects any influence that goes beyond the specified threshold. In the case where a potential danger cannot be ruled out, this area outside the safety threshold can be defined as the zone of “uncertainty”, where stopping of the system is required not because of any detection of danger but because it is not confirmed “safe” anymore.

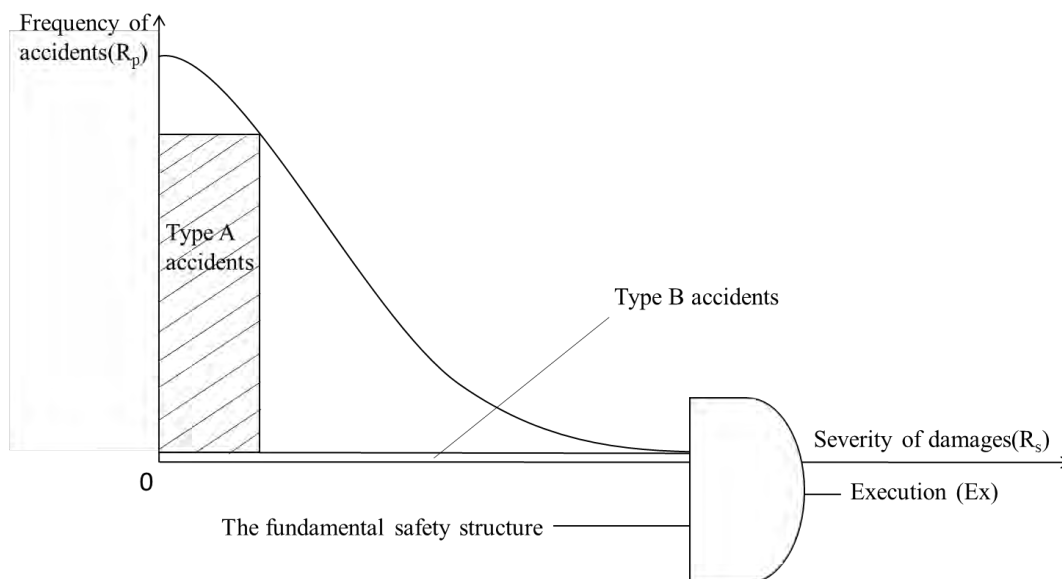


Figure 1. Relationship between the probabilistically-based safety and the deterministically-based safety.

Here it is clarified that definition of safety is required for type B accidents instead of probability index, while the probability index is required for type A accidents to improve the reliability of machines. Safety is distinguished from reliability and risks should be evaluated by the severity of harm, excluding probability factor.

4 ENSURING OF SAFETY BY NEW INDICATOR

For the purpose of safety type B occupational accidents cannot be tolerated at all. The purpose of safety mechanisms is to protect people from harm of interferences with a machine. Therefore, it shall be focused on how to make the system integrity secure enough to always stop the system itself before actual harms occurs. ISO/IEC Guide 51^[1] refers to risks as the combination of the severity of harm and its probability - the frequency of accidents is obtained as statistical data from actual accidents. However, it is required to set up preventive measures in advance rather than ex-post countermeasures to avoid harm by accidents. Preventive measures shall be designed based on determinism, requiring detection of accidents along the timeline and integrity of controls.

If future accidents can be detected along the timeline, they are independent from the statistical data but can be controlled by means of deterministic measures. In other words, it should not show that an accident occurs once a year, but it should show that for example in 10 minutes it becomes too dangerous to use machine. In that way the importance of the deterministic stopping structure is revealed. This deterministically-based safety system can be ensured by the mechanism consisting of detection sensors and implementing measures to “stop completely before an accident”. This mechanism is based on the normality, which maintains the function of the system and the failsafe structure. Moreover, the system shall work to be stopped out of the confirmed safety zone, however, it never allows stopping failures and requires oriented failure mode. Here accidents are assumed an issue of the normality of the safety confirmation mechanism, and safety performance of the system can be denoted as below:

$$[\text{Safety performance}] = [\text{conformity of the design (to stop before the accident)}] \times [\text{normality}]$$

5 OPERATIONAL SAFETY AND SAFETY CONFIRMATION SYSTEM

Conventional risk reduction (to zero level) concept assumes inherent safe design, giving the priority to removing hazard(s), stopping the system and then separating by safe guards sequentially. The Safety Confirmation System which is created and developed by Sugimoto, Futsuhara, Mukaidono and et.al, ^{[5] [6] [7] [8] [9] [10]} requires stopping whenever the safe condition is not confirmed. It considers the uncertainty as a danger, requiring physical separation to prevent interference of people and hazard.

The Operational Safety System is created by Sujino, Sugimoto, Fiedrich ^[11] and proposes a separation in the timeline when the hazard(s) can neither be removed nor separated by physical structure. In such a situation, accidents can be defined by the delay in stopping failure before the accident. Safety is denoted as <S> by deducting the stopping interval from an assumed accident. Conventional safety measures do not preclude a time factor and therefore it is required to investigate the validity of the proposed concept of Operational Safety System with the Safety Confirmation System.

The Safety Confirmation System implements safety measures whenever the information concerning the specified safe condition is not received. When the condition for safe operation of the machine is confirmed, the signal that permits machine operation is generated. When the safe condition is not confirmed the system implements safety measures to stop the system itself. To avoid making wild guesses, from a failsafe structure of the oriented failure mode to a safer condition is required. It never allows the signal to show safe condition when the device fails. If machine and operators share the same working space, machine or operators work only after confirming the other party is at their own space rather than the shared working space. Safe condition specified as no interferences of machine and operator, is defined as S=1. The safe condition at the shared space is confirmed by the sensor that periodically sends noise signals to confirm its normality <N*>, which is defined as Sc=1. Execution <Ex> of the work at the shared space is denoted with the formula (1) below.

$$S > S_c > Ex \quad (1)$$

Formula (1) keeps the unate relation of each factor and therefore the work will not be executed without the safety condition confirmed. It should be noted that uncertainties within the field S include the probability of an accident and the phase before that accident can be defined as the conditional safety <S'=1>, which is the boundary field to the uncertainties. Now <S'> is the failsafe interval where a true accident <-S>, will not be caused and the safety confirmation structure is shown in the formula below (2).

$$S > S' > S_c > Ex \quad (2)$$

Next is the new concept for a fundamental operators' safety system, which is derived from the Safety Confirmation System, but includes a new factor to secure the safe condition. For the space sharing by machine and operator, the safe condition is confirmed by the information about the occupation of the other party in their own space. For moving vehicles and trains, on the other hand, the safe condition is confirmed by means of the stopping interval <Se=1> as to not interfere with other users based on the safe distance. Hazard is confirmed within the stopping mechanism, which can be expressed by the formula (3):

$$S > S' > S_r > S_e > S_c > Ex \quad (3)$$

<S'> is the assumed accident defined by uncertainties and <S_r> is the limit of monitoring for the assumed accident <S'>. This limit of monitoring shall be the threshold of the range and then <S_e> is finally defined by deducting the stopping interval from <S_r>. This <S_e> is the safe space secured by the stopping interval whenever the safe condition cannot be confirmed, without relying on chances.

6 LOGICAL PROOF OF FUNDAMENTAL SAFETY SYSTEM FOR OPERATORS

As stated in article 4, safety performance can be evaluated by the conformity of the design to stop before the accident and by keeping its normality through oriented failure mode. In this paper another performance indicator of stopping before an accident was evaluated.

An accident can be defined by the fatal harm to any person. This event can be translated as the result of the energy transmission <E> of fatal harm to the human body, caused by the interference of the hazard and the operator in the space <P> at the time <T>, expressed as <¬T·¬P>.

$$\text{Accident: } \neg S = \neg (T \cdot P) \cdot E \quad (4)$$

Safety can be defined by reversing the formula (4).

$$\text{Safety: } S = (T \cdot P) \cdot \neg E \quad (5)$$

T=1 signifies the proper preparation during the time of the machine and the operator, while P=1 signifies the one in space. If no interference of the hazard and the operator takes place, no energy transmission occurs <¬E>. Therefore, the formula (5) signifies that the safe condition for operators is maintained by keeping the distance both in time and in space. The integrity of the stopping mechanism is based on this formula (5) and shall be the safe condition in the fundamental safety system. The evaluation of that mechanism can be done by the indicator of normality of the function, i.e., the level of the oriented failure performances.

7 CONCLUSION

Risk-based safety does not provide satisfactory solutions for all hazardous events due to its probability-dependent indicator. This paper is suggesting the deterministically-based new solution, as well as a new evaluation indicator for safety performances.

This fundamental safety system is compatible with the Safety Confirmation System, providing deterministic measures to avoid harm from hazards for operators.

This system also provides a logical structure of safety with factors of time, space and preventing harmful hazard by cutting off energy transmission.

8 REFERENCES

1. ISO/IEC Guide 51, *Safety aspects Guidelines for their inclusion in standards*, 3rd edition, 5, 2014, 1–16.
2. ISO 12100, *Safety of machinery General principles for design Risk assessment and risk reduction*, 2010, 7.
3. IEC 61508 -5, *Functional safety of electrical/electronic/programmable electronic safety related systems*, 2010, 5.
4. Umesaki S., Hamajima K., Shimizu S., Ito K., Itagaki H., Saito T., Yamagiwa K., Kwangseok C., Takahashi H., Odo K., *Well understand ! Safety engineering for managers at working place*, Union of Japanese Scientists and Engineers, 2013 (in Japanese).
5. Futsuhara K., *The basic of safety engineering*, Society of safety Technology and Application, 2008, 25-41 (in Japanese).
6. Sugimoto N., Futsuhara K., Mukaidono M., *The principle and Logical Structure of Safety in Man-Machine System.*, T.IEE Japan, Vol. 107-D, No.9, 1987, 1092-1098 (in Japanese).
7. Futsuhara K., Sugimoto N., Mukaidono M., *Structure of Man-Machine Interlocking System for Safe Operation.*, T.IEE Japan, Vol.107-D, No.9, 1987, 1099-1206 (in Japanese).
8. Sugimoto N., Kumekawa S., Fukaya K., Shimizu S., Umesaki S., Ikda H., Hoshi T., Futsuhara K., *Fundamental Structure of Safety of the Safety Confirmation Type (About the Condition of Confirmation Structure)*, Transaction of the JSME, Series C, Vol.54, No.505, 1988, 2284-2292 (in Japanese).
9. Futsuhara K., Sugimoto N., *A Logical Consideration of Safety Operation System of the Safety Confirmation Type*, Transaction of the JSME, Series C, vol.56, Nr.529, 1990, pp2378-2385 (in Japanese).
10. Sugimoto N., Futsuhara K., *Principles of safety*, Transaction of the JSME, Series C, Vol. 56, No. 530, 1990, 2601-2609 (in Japanese).
11. Sujino T., Sugimoto N., Fiedrich F., *A Proposal of Logical Assistance-Giving Means in Tsunami Disaster Prevention Activities*, Proceedings of the 3rd Plano Cosmo International Conference, In Indonesia, Bandung, (26-27/Oct/2015).

Radio Wave Sensor System Which Enables Determination of Protective Separation Distance

Kim E., Yamada Y., Okamoto S.

Nagoya University, Furo-cho, Chikusa-ku, Nagoya, 464 8601, Japan

kim.eugene@a.mbox.nagoya-u.ac.jp
yoji.yamada@mae.nagoya-u.ac.jp
okamoto-shogo@mech.nagoya-u.ac.jp

KEYWORDS: ISO/TS 15066, Human Robot Collaboration, Radio Wave Sensor, Speed and Separation Monitoring

ABSTRACT

In the study, we propose a safety-related sensor system that enables human approaching motion detection in the three-dimensional space by using radio-frequency sensor system with a Frequency Modulation-Continuous Wave (FM-CW) method the components of which are widely used in automotive industry and nursing facilities. Not only the position of human and robot, but also their relative velocity is an important parameter for maintaining the Protective Separation Distance (PSD) in Speed and Separation Monitoring (SSM). Nonetheless, the uncertainty of velocity detection is not yet intensively discussed in the SSM. Therefore, we carried out an experiment to examine whether the uncertainties satisfy the safety integrity level of the position and the speed measurements required in the framework of IEC/DTS 62998. We demonstrate those by integrating the data from multiple radio wave sensors which could measure the position and the speed simultaneously.

1 INTRODUCTION

A safety function that maximizes the efficiency of manufacturing is demanding [1] for highly interactive collaborative robot systems. Especially, when an industrial robot possesses a highly hazardous tool which can easily harm the operator, non-contact based safety securing function shall be introduced to the workspace. In this study, we focus on the speed and separation monitoring (SSM) function listed in the ISO/TS 15066 standard and discuss a method for determining the measurement uncertainty that satisfies the safety integrity level [2]. With extant human detection technology, safety sensors which ensure the human safety and to increase productivity at the same time are still being expected for development. We use a radio wave sensor as a safety sensor [3] and evaluate its performance of human presence detection based upon the requirement that is stated in IEC/DTS 62998: we follow the procedure of determining the interval of the measurement uncertainty based on the measurement error including position and speed measurements. Specifically, the originality of this paper lies in the evaluation of speed measurement uncertainty.

2 SAFETY STANDARDS AND ITS TREND

In this section, safety requirements of the cooperative robot described in the International Safety Standard (ISO/IEC), especially the safety guidelines of safety related sensors are highlighted.

2.1 Protective Separation Distance

The protective separation distance (PSD) is a minimum tolerable distance between human and the robot which is a distance function involved in the SSM safety function [4]. According to the protective stop function of ISO 13855, operation or task generation of the robot that violates the PSD is not allowed [5]. Equation of PSD S_p at time t_0 can be expressed as follows.

$$S_p(t_0) = S_h + S_r + S_s + C + Z_d + Z_r \quad (1)$$

where S_h , S_r and S_s denotes distance that is expected for human to travel until the robot reacts and completely stops, for the robot to travel until it reacts to a human approach, and for the robot to travel from reaction until it stops completely, respectively. In addition, C , Z_d and Z_r represent an intrusion distance which is listed in the ISO 13855, an uncertainty for measuring the human position and determination of the robot position, respectively.

Here, letting the reaction time of the robot as T_r and estimated stopping time as T_s , equation (1) can be rewritten as follows.

$$S_p(t_0) = v_h(t_0)(T_r + T_s) + v_r(t_0)T_r + B + C + Z_d + Z_r \quad (2)$$

where v_h and v_r represent the velocity of the human and the robot respectively which can be the function of time excluding the worst case where the v_h is constant (=2.0 m/s) [5]. Here, B is the distance that the robot travels during the robot issues to stop and stops completely, and it depends on the deceleration of the robot. The B can be written as follows:

$$B = \int_{t_0+T_r}^{t_0+T_r+T_s} v_s(t)dt \quad (3)$$

where v_s denotes the velocity of the robot when is in the state of braking along the T_s .

2.2 Measurement uncertainty and coverage interval

Human and robot collaborative system, especially the safety-related parts are required to meet the required safety integrity level $PLr = d$ [6]. However, the measurement uncertainty which is the component of the protective separation distance has no strict rule on its determination and neither discussed in the ISO/TS 15066. In the latest IEC/DTS 62998 standard issued in 2018, an idea of coverage interval is suggested which allows quantitative evaluation of measurement uncertainty assuming that the measurement error follows Gaussian distribution [7]. Letting the probability of failure in hour as PFH , the coverage probability as C_p can be written as follows:

$$C_p \leq 1 - \frac{PFH_u}{r^d} \quad (4)$$

where r^d represents the demand rate of collaborative system. In the case of required safety integrity level is $PLr = d$, the upper limit of PFH is 10^{-6} and the suggested demand rate r^d is around $4h^{-1}$. Therefore C_p which satisfies corresponding safety integrity level is calculated as $1 - 2.5 \times 10^{-7}$. Finally, the coverage interval that includes such probability is $\pm 4.76\sigma$ which can be derived by statistical measurement error of the sensor system. The calculated width corresponds to acceptable error and measurement data which belongs to the beyond the border is treated as unacceptable error.

3 EVALUATION

3.1 Experiment Setup

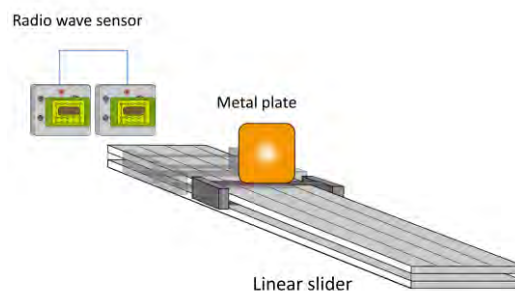


Figure 2. Experiment setup using linear slider.

Figure 2 shows the experiment setup using radio wave sensors and a linear slider. The target object was a metallic plate. Though we do not mention in detail about other materials also tested as target objects, we can tell that they exhibited similar characteristics in terms of motion (distance and speed) detectability. The linear slider was used to move the target object. The couple of wave sensors were allocated side by side, 5 mm apart from each other and placed as a sensor system facing the slider's moving direction. The motion data of the linear slider based upon the encoder values and the values directly measured by the two sensors and integrated as a system were compared to evaluate the sensor system. The sampling frequency of the radio wave sensors was 200

KHz. FFT analysis with 2048-point window size was used to obtain the modulation frequencies to compute the distance and velocity of the target object [8], [9].

3.2 Experiment Results

Figure 3 shows the histogram of measurement errors of distances between the optical encoder of the linear slider and the single radio wave sensors. The speed of the linear slider was set as 0.5 m/s and moved along the slider 0.2 m to 1.0 m from the radio wave sensors were placed. The whole experiment was conducted during 15 min.

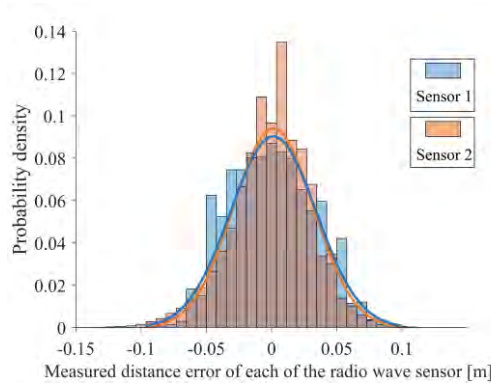


Figure 3. Measurement error of distance between linear slider and single radio wave sensors.

The standard deviations of the errors were 0.030 m and 0.032 m for each of the two radio wave sensors. In order to investigate the improvement of measurement performance when multiplexing the couple of sensors, the identical experiment was conducted using the radio wave sensor system. Figure 4 shows the histogram of the measurement error between the distance measured by the linear slider and that as the sensor system. Average was taken integrally from the values read from the two sensors. The standard deviation of the measurement error was 0.025 m. Compared to the single radio wave sensor, the performance of distance measurement improved by 17.7% and 23.3%.

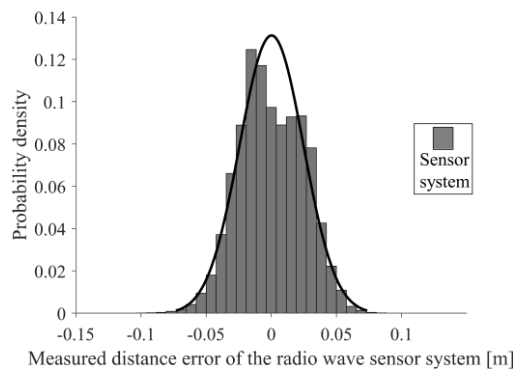


Figure 4. Measurement error of distance between linear slider and radio wave sensor system.

Next, the speed measurement error of the radio wave sensors was investigated. Figure 5 shows the histogram of speed measurement error of a single radio wave sensor when the linear slider was accelerated and decelerated at $\pm 1.25 \text{ m/s}^2$ and maximum speed was 1 m/s.

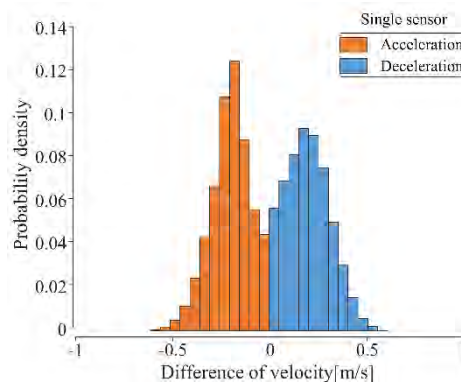


Figure 5. Measurement error of velocity between linear slider and radio wave sensor.

The standard deviation of the velocity measurement error of the single radio wave sensor was 0.098 m/s and 0.110 m/s when accelerating and decelerating phases, respectively. The velocity measurement error was also investigated when the radio wave sensors were multiplexed to construct a radio wave sensor system. Figure 6 shows the histogram of velocity measurement error of the radio wave sensor system.

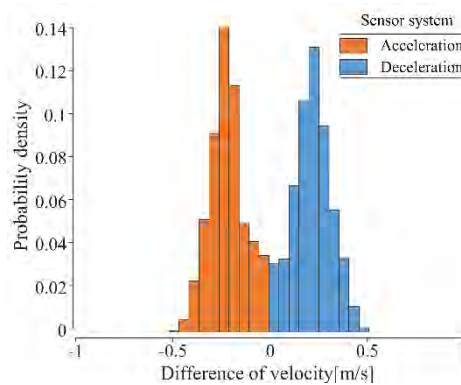


Figure 6. Measurement error of velocity between linear slider and radio wave sensor system.

The standard deviation was 0.081 m/s and 0.083 m/s when the target object was accelerated and decelerated respectively. Therefore, the error produced as the radio wave sensor system decreased by 17% and 25% in the acceleration and deceleration respectively.

4 DISCUSSIONS

First, the integrally obtained values of both distance and speed well agreed with the statistics that the standard deviation of the average value is reduced by $\sigma^{-1/2}$. Secondly the measurement uncertainty of the relative speed is not being explicitly considered in the ISO/TS 15066 to formula (2). In the study, however, the uncertainty of the relative speed was measured based upon the actual experiment. The Z_d , which literally represents position uncertainty of the human, can also include another uncertainty term originating in speed measurement. We propose Z_d comprising $Z_v = (T_s + T_r) \times \Delta v_h$ which can be substituted with obtained uncertainty of the relative speed. Where T_s , T_r and Δv_h are the stopping time, reaction time of the robot and uncertainty of the speed measurement. Therefore, it unnecessary to take the worst case v_h in the calculation of the protective separation distance by which the shared workspace between human and the robot can be eventually saved by adopting expense of the additional Z_v .

5 CONCLUSIONS

In this study, we dealt with evaluation of radio wave sensors for the purpose of constructing a safety-related sensor system. Since ISO/TS 15066 does not specify determination of measurement uncertainty in speed and separation monitoring safety function, we adopted the concept of coverage interval specified in IEC/DTS 62998 that defines a level of confidence meeting safety integrity level. We exemplified this concept by using the measurement data of radio wave sensors. The uncertainty of distance measurement of single radio wave sensor which meeting PLr = d was 0.14 (4.76 σ) m. In addition, the uncertainty of velocity measurement of single radio

wave sensor was 0.46 m/s and 0.51 m/s at the accelerating and decelerating phases, respectively. By use of the two radio wave sensors at the same time, the uncertainty of distance measurement decreased by 0.11 m, and the uncertainty of velocity by 0.38 m/s and 0.39 m/s at the accelerating and decelerating phases, respectively. Therefore, by use of the Coverage Interval stated in the IEC/DTS 62998, measurement uncertainty of human position and speed can be quantitatively evaluated.

ACKNOWLEDGMENT

This research was conducted through "Knowledge Hub Aichi" project (Stage II) which is financially supported by the Aichi Science & Technology Foundation.

6. REFERENCES

1. KULIĆ, Dana; CROFT, Elizabeth. *Pre-collision safety strategies for human-robot interaction*, Autonomous Robots, 2007, 22.2: 149-164.
2. ISO/TS 15066, *Robots and robotic devices– Collaborative robots*, 2015.
3. Kim, Eugene, Yoji Yamada, and Shogo Okamoto., *Improvement of safety integrity level by multiplexing radio wave sensors*, Proceedings of IEEE International Symposium on System Integration, pp. 942-947, 2017.
4. Marvel J. A., Norcross R., *Implementing speed and separation monitoring in collaborative robot workcells*, Robotics and computer-integrated manufacturing 44, 2017, pp. 144-155.
5. ISO 13855, *Safety of machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body*, 2010.
6. IEC 61508, *Functional Safety of Electrical Electronic/Programmable Electronic Safety-Related Systems*, 2010.
7. IEC/DTS 62998, *Safety of machinery - Electrosensitive protective equipment - Safety-related sensors used for protection of person*.
8. Lin, Jau-Jr, et al., *Design of an FMCW radar baseband signal processing system for automotive application*, SpringerPlus, 5.1, (2016): 42.
9. Brooker, Graham M., *Understanding millimetre wave FMCW radars*, 1st international Conference on Sensing Technology, 2005.

The Safeguarding Supportive System (SSS) II. Study on the reliability of the Safeguarding Supportive System (SSS) in work site of the Integrated Manufacturing System (IMS) introducing a mobile robot

Matsui K.¹, Hojo R.², Itou H.¹, Hamajima K.², Umezaki S.², Ohtsuka H.³, Fukuda T.⁴, Takahashi S.¹, Shimizu S.²

¹ Nihon University – Narashinodai 7-24-1 – Funabashi city – Chiba Prefecture – 274-8501 – Japan

² National Institute of Occupational Safety and Health, Japan (JNIOSH) – Umezono 1-4-6 – Kiyose – Tokyo – 204-0024

³ ECSSA Consulting & Co – Shinkoiwa 3-4-1 505 – Katsushika ward – Tokyo – 124-0024 – Japan

⁴ Nagaoka University of Technology – Kamitomioka 1603-1 – Nagaoka City – Niigata Prefecture – 940-2188 – Japan

cskt14086@g.nihon-u.ac.jp (Matsui K)

hojo@h.jniosh.go.jp

cskt14086@g.nihon-u.ac.jp (Itou H)

hamajima@s.jniosh.go.jp

umezaki@s.jniosh.go.jp

h.otsuka_auto-id@air.ocn.ne.jp

t-fukuda@vos.nagaokaut.ac.jp

takahashi.sei@nihon-u.ac.jp

shimizu@s.jniosh.go.jp

KEYWORDS: Safeguarding Supportive System (SSS), Integrated Manufacturing System (IMS), mobile robot, residual risk, beacon sensor system

ABSTRACT

Nowadays, industrial accidents evoked by human factors are huge problem in Japan. As high-spec protective devices are developed and installed on a single machine recently, the number of savior accidents has been decreased in the last 20 years.

Since multiple machines are located in the work site of the integrated manufacturing system (IMS), security measures depends on management by human. Under such condition, industrial accident by human factor still occurs. Many accidents have occurred under these situations as follows;

- A worker has mistakenly restarted because the worker could not recognize that another worker existed behind a machine in the work site.
- A worker has entered a prohibited work site.
- A worker has touched the machine which was not allowed to operate without license.

We developed the Safeguarding Supportive System (SSS) in our laboratory. The SSS was newly established to reduce residual risks which are evoked by human factors. The validity of the SSS was examined in a virtual IMS in our laboratory. The IMS had a mobile robot for transportation in the work site. In the present study, a beacon sensor system was introduced to acquire information of worker's location. As one of experimental indices, we examined the usefulness of the beacon system for detecting worker's position. Information of worker's position detection acquired by an UWB system, which was used in the previous study, and that by beacon system was qualitatively compared. As a result, the information acquired by the UWB sensor system was more precise than that of the beacon sensor system. On the other hand, beacon sensor would be useful to acquire biometric information of workers such as pulse rate, body temperature, and posture, etc. In the further study, we are planning to use devices that meet the need of the work sites.

1 INTRODUCTION

In Japan, many industries, for example, automobile and general machinery industries in Japan now installs Integrated Manufacturing System (IMS). The IMS is the manufacturing system which contains a combination of single machine such as robot, press and/or belt conveyor. Under the IMS, a various type of materials is produced automatically. Workers are usually prohibited to step into the work sites during routine work, that is, when robots are working. If workers need to access to the IMS work sites during routine work, all machines existing in the IMS must be stopped. The IMS decreases physical burden of workers and maintains some degrees of

producibility. However, many labour accidents have occurred during none-routine work because there are some works which have to operate without stopping, such as maintenance, cleaning and teaching works for robots. Under such none-routine works, safety is sometimes completely dependent upon worker's attentiveness. In addition, recent IMS often has an interaction of mobile machines (transportation robots, etc.) and workers. Therefore, we have to establish a novel safety protective system which is available for the recent working style in Japan. One of the most severe problems is mis-restart by the third person who cannot recognize another worker working at the worksite. If locations of all workers in the IMS can be detected with information and communication technology (ICT) equipment instead of human attentiveness, the risk of labour accidents during none-routine work under the IMS would be reduced. We established a novel safety system named Safeguarding Supportive System (SSS) focusing on the residual risk after taking the three-step method for safety. The SSS monitors entering and leaving of the IMS work site and worker's location, and controls qualification and authorization of worker and location of work by the combination of ICT equipment. Besides of the function of the SSS, we have to select appropriate device for location detection of worker in the IMS work site. A simulated IMS work site having a mobile robot was built in our laboratory (Figure 1) as a part of the SSS system.

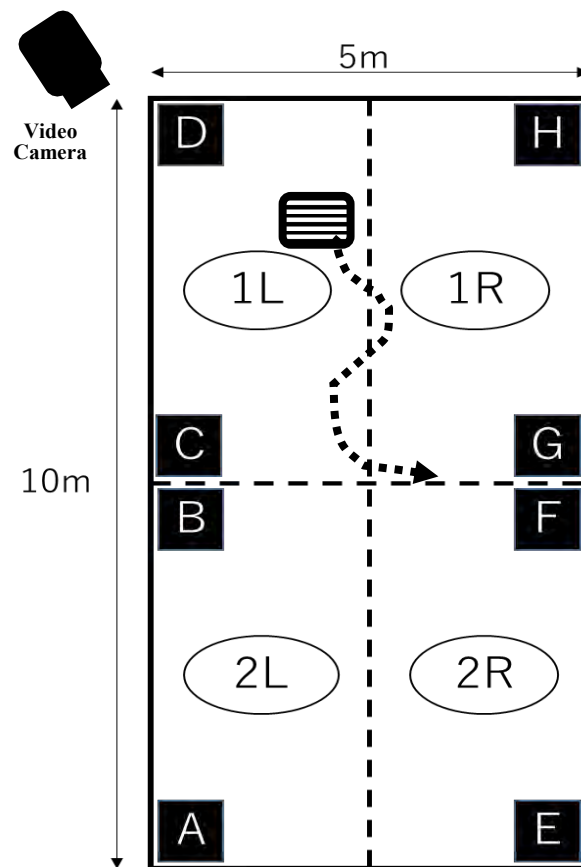



Figure 1. A simulated work site established in the National Institute of Occupational Safety and Health. The work site was 5m x 10m. The work site was divided by 4 work zones, 1L, 1R, 2L and 2R. There were 8 receivers, A-E. One video camera was set at a corner of the work site. A Mobile robot () was moving with 0.9m/s in the work site.

2 PURPOSE OF THE PRESENT STUDY

In the present study, we examined the validity of a beacon sensor system (EXBeacon made by WHERE company, Tokyo Japan) focusing on the location detection of a worker. Then, the result was compared with another location detection system, an Ultra Wide Band (UWB) system (PDK4, Japan GIT co Ltd., Shiga Japan), which was used in the previous study.

3 MATERIALS AND METHODS

A work site, 5m x 10m, was established in the National Institute of Occupational Safety and Health (JNIOSH, Tokyo Japan) for acquisition of position information of a worker in the work site. A mobile robot (OEM-LD60, OMRON, Tokyo Japan) was existed in the work site. Though the mobile robot usually uses with 1.8m/s, it was used with 0.9m/s in the present study. One video camera (TS-HDE230ZN, 3D Corporation, Tokyo Japan) was set at a corner of the work site (Figure 1) and recorded all movement of robot and subjects. The work site was divided into 4 (1L, 1R, 2L and 2R, in Figure 1) as work zones. A mobile equipment (a tag) was held in the chest pocket of subject and 8 fixed equipment (receivers) were set at 8 points (A~H, Figure 1) in the work site. Although 10 subjects (5 males and 5 females) attended the present study, one data of a subject was randomly selected and used. The location of the subject in the work site was identified by the three-point measurement method by the tag held by the subject and 2 receivers. The location information derived from the beacon sensor system was compared with the video data. The log data of the beacon sensor system was collected by 5-second pitches. The location information of the beacon sensor system was distributed to 3 categories with conformity of the video data. One category was correct identification, which was corresponded to location in the video data. The second category was the slip distinction. In the slip identification, the beacon sensor system misidentified the location of the subject. In the video camera data, the subject was actually in the next zone. In the third category, the wrong identification, the beacon sensor system identified that location of the subject stayed at completely different zone. In addition, correctness of the beacon sensor system and Ultra Wide Band (UWB) sensor system used in the previous study were compared. As well as the beacon sensor system, every 5 seconds was used as calculation.

4 RESULTS

As shown in Figure 2A, the correct identification of the beacon sensor system was 41%. The log data of the beacon sensor system was collected by 5-second pitches. The slip identification and the wrong identification were 41% and 17%, respectively (Figure 2A). The correct identification of the UWB sensor system was 80%. The log data of the UWB sensor system was collected by 5-second pitches. The slip identification and the wrong identification were 20% and 0%, respectively (Figure 2B).

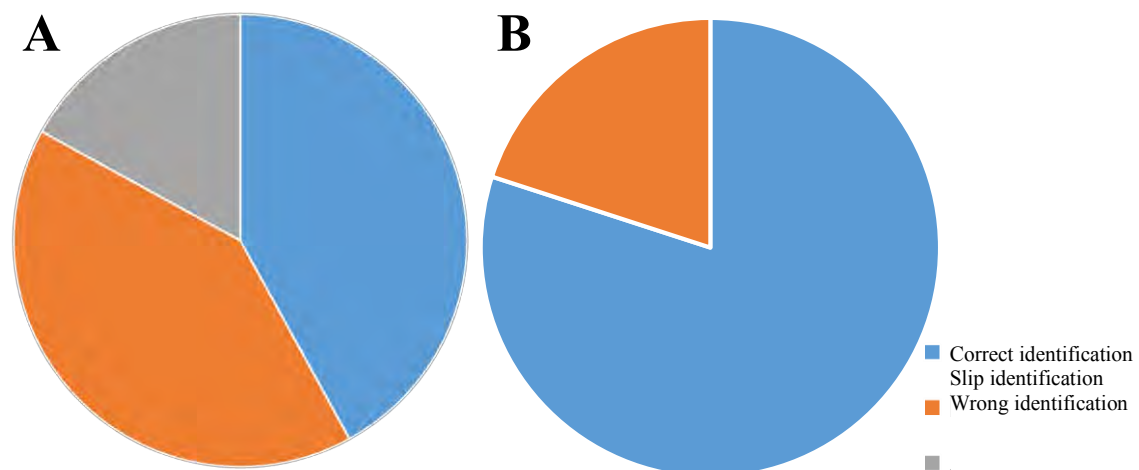


Figure 2. A) The result of the location of the subject derived from the beacon sensor system. B) The result of the location of the subject derived from the UWB sensor system. Blue, orange and grey colours indicated the correct identification, the slip identification and the wrong identification, respectively.

5 DISCUSSION

The result in the present study indicated that the enough precision wasn't obtained by the beacon sensor system as compared with the UWB sensor system which was used in the previous study. We decided to use 8 receivers in the experimental work site because the available measure distance of the receiver was about 5m [1]. However, more precise identification of the location of subject would need more than eight receivers for the work site in

Poster session

the present study. If more than 8 receivers would be used, the identification would become more precisely. Another solution for more precise identification may be the setting location of receivers. If a receiver would be located at the centre of the work site, slip identification will be decreased. For the wrong identification, Radio wave absorbent may need to install to the work site. We concluded that the UWB sensor system is suitable for the location detection. However, the mobile equipment of the UWB sensor system is much bigger than that of the beacon sensor system. In addition, the UWB sensor system is still expensive in Japan, the expense would be decreased if it would be popular in near future. On the other hand, the beacon system is cheap as compared with the UWB sensor system. The beacon sensor system enabled to measure vital signs because it had noncontact type pulse sensor inside. In addition, if the beacon sensor would additionally have aerotonometer, and/or 9 axis sensor which contains azimuth meter, accelerator and gyroscope inside, precise 3-dimensional location detection including posture information of worker would be possible. We think that appropriate usage of these two sensor systems needs to be used by purpose after understanding an advantage and the weak points.

Evaluation of Residual Risk under Risk Reduction Rules for Using Collaborative Robots

Ikeda H., Saito T., Okabe K.

National Institute of Occupational Safety, Japan (JNIOSH) - 1-4-6, Umezono, Kiyose, Tokyo, Japan

ikeda@s.jniosh.johas.go.jp

saitot@s.jniosh.johas.go.jp

okabe@s.jniosh.johas.go.jp

KEYWORDS: risk reduction, safe design, robot, collaborative safety

ABSTRACT

Designers of collaborative robots take protective measures for risk reduction, but these measures could exert influence on the usefulness of robot operation. Since safety and usefulness have a tendency to be contrary to each other as just described above, a balance should be kept properly between safety and usefulness.

For this purpose, the basic configuration of a human-robot collaboration system is discussed in the “Confirmation document of Safe Design and Specifications” to promote the segmentation of respective roles of humans and robots. Based on the segmented roles of humans and robots, the residual risk of robots is grasped, and measures for risk reduction during robot operation are summarized. Also, by proclaiming an idea of trade-off between safety and usefulness, risk mitigation from the robot user side is made possible.

To be specific, it is possible to express the effect of residual risk reduction worked on by a user in the form of the factor of the “provision of information or means from the designer” multiplied by the “degree of implementation of the measures by the user” and the “trade-off coefficient.” Involved in the degree of implementation of the measures are sub-factors, such as the attentiveness maintenance, understanding depth and proficiency level of the user and the environmental conditions. According to these sub-factors, the degree of implementation of the measures prepared by the designer is determined. On the other hand, four different trade-off coefficients are conceived: “influence on the usefulness,” “loss in robot capability” and “cost increment / technical difficulty” as minus coefficients, and “consideration of benefit” as a plus coefficient. By applying the above rules, the effect of the residual risk reduction worked on by robot users can be properly evaluated.

1 INTRODUCTION

As represented by wearable assist devices for use in nursing care, rehabilitation and heavy material handling, collaborative robots working for humans often receive involvement from humans, and, therefore, safety securement during the use of robots is inevitably depending on humans. Although robot designers work out safety design based on risk assessment to reduce risks of robots, the reduction of residual risks during robot operation has no choice but to resort mainly to each robot user.

The effect of risk reduction expected by robot designers is dependent on results of risk reduction measures taken by robot users, but, on the other hand, the influence thereof on the usefulness of robot operation should also be considered. In this research, in order to evaluate the effect of residual risk reduction considering balance between the safety and usefulness of collaborative robots, evaluation items are organized in sequence by referring to the confirmation note of safe design specifications, and then rules for trade-off for the safety are proposed, and the rules are applied to walking assist devices.

2 REDUCTION OF ROBOTIC RISKS, AND DEALING WITH RESIDUAL RISKS

2.1 Process of risk reduction

In the risk assessment procedure to be taken by robot designers, the conditions (restrictions) of a target robot are defined, and then analysis and risk evaluation are made on individual hazards. ISO 12100[1] stipulates the safety design procedure, including the risk reduction process following the risk assessment.

The risk reduction process requests three protective measures to be taken one by one from the top of the process (which is called “3-step method”[1]). Among them, inherently safe design (Step 1), and safeguarding and complementary measures (Step 2) are chiefly engineering means. In these steps, risk reduction is implemented by measures, such as protective device provided in robots. However, as shown in Figure 1, it should be noted with care that an emergency stop device, which is a measure of Step 1, cannot produce the risk reduction effect

expected by the robot designer unless the robot is actually operated by the robot user. Also in usage information (Step 3), the risk reduction effect cannot be produced unless specific protective measures (lower part of Figure 1) are taken by the robot user. In general, however, because the implementation of protective measures by the robot user may have an influence on the usefulness of the robot, the trade-off for the usefulness should be considered.

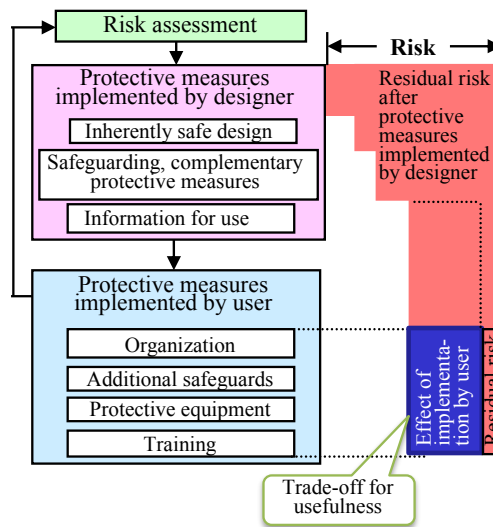


Figure 1. Risk reduction process described in ISO 12100.

2.2 Dealing with residual risks by robot designers

In the risk assessment process, whether the protective measures taken by the robot designer have met the risk reduction level target is determined by the validation of the protective device whether, for example, the device is compliant with relevant safety standards or the device has realized the safety performance target. However, for such protective devices that need the involvement from robot users, the effectiveness of device operation by the user should also be considered. For this purpose, the device developer provides the device user with the following contents as “usage information” of Step 3:

- (1) Information setup
Warnings, signals, indications, signs, etc. from or on the device
- (2) Accompanying documents
Information related to risk assessment, validation information, etc.
- (3) Instruction manual
Information of conveyance, treatment and robot itself, information of use (residual risk, adaptation and contraindication, additional measures, (if necessary) training and protective equipment, maintenance, disuse, disposal, dealing with emergency, etc.

In particular, because the instruction manual contains the risk reduction measures to be taken directly by robot users (such as emergency stop operation), it is necessary to give enough thought to the description so that the actual risk reduction effect can be obtained by information provision. The effect of residual risk reduction that robot designers expect when designing robots is dependent on how properly and understandably the information should be provided (not to cause misunderstanding). For this reason, the information to be provided is also requested to have appropriateness, definiteness and correctness.

2.3 Dealing with residual risks by robot users

How a robot user works on risk reduction based on the “usage information” provided by the robot designer relates not only to the user himself but also to the operational establishment and organization. That is, the requirements for achieving the effect of direct risk reduction measures include the maintenance and improvement of the user’s attentiveness, comprehension of the task and robot functions, and familiarity with the task and crisis prevention, and use environment (illumination, atmosphere). In order to effectively promote the fulfillment of these requirements, it is necessary to establish a system which can provide education and training to robot users. However, it is important for both the robot designer and the robot user to conclude an agreement for the sharing of responsibility (after compensation, relief) for all accidents which could occur as a result of the residual risk reduction by the robot user.

2.4 Preparation of confirmation note of safe design specifications

Following the above procedure, residual risks are grasped after the reassessment of risks in the risk assessment process, and the confirmation note of safe design specifications as shown in Table 1 is prepared. This confirmation note is designed for the robot designer to declare the basic concept of safety design, organize in sequence the risk reduction measures selected based on the risk assessment results, grasp the residual risks which cannot be reduced only by the robot designer, and sum up how to deal with these risks by the robot user. Furthermore, anticipating the final productization, the robot designer declares the concept of trade-off between the safety and the usefulness, and thereby the robot user can consider the risk mitigation.

For some actual products, the effect of risk reduction aimed at by the robot designer cannot be achieved. The relationship inconsistent with the safety may take place. For example, the usefulness is impaired in exchange for the functions of risk reduction, the cost for realizing the safety functions is excessively high, and the functions themselves are technically difficult to achieve. Although these inconsistent items are dealt with mainly by the robot user, it is necessary for the robot designer to describe how to assume the trade-off for the safety in the confirmation note of safe design specifications, and reasonably explain the safety degradation when the trade-off is implemented (time extension may be required depending on the case).

Table 1. Confirmation note of safe design specifications (prototype of transfer robot equipment).

Target: Transfer robot (lift type)				Prepared by: (Designer name)	
No.	Major item	Medium item	Minor item	Description (example)	
1	Safe design concept	Roles of man and machine		(Core of safety securement)	
		Definition of safe state		(Description of purposeful safe state and unconditional safe state)	
		Scheme of safety functions before detailed design work	Dealing with hazardous state by equipment		(Main preparation of equipment for hazard and hazardous state (event))
			Dealing with hazardous state by user		(Main dealing with hazard and hazardous state (event) by user) (Notification to operator)
			Dealing with hazardous state by operator		(Main dealing with hazard and hazardous state (event) by operator) Operation of emergency stop device
2	Safety functions of equipment	Functions of existing equipment		(Functions as a requisite stipulation in regulations, etc., and concomitant functions)	
		Addition after RA analysis		(Functions to be added)	
		Confirmation method of normality of safety functions		(Response to and checkup for failure and abnormality)	
3	Dealing with residual risks	Size of residual risks (overall)		(Size and trend of residual risk)	
		Dealing with while using	Dealing with by operator		(Monitoring, Attention calling, Training, Protective gear)
			Dealing with by user		(Monitoring, Attention calling)
			Dealing with by third person		(Attention calling)
Other methods		(Insurance)			
4	Relation between safety and usefulness	Relation resulting in trade-off		(Safety vs usefulness, feasibility, cost)	
		Optimization method for trade-off		(Meeting point of both-side relation, and its method), concerned risks	

3 TRADE-OFF RULES FOR RESIDUAL RISKS

The relation of trade-off for the safety, which should be described in the confirmation note of safe design specifications, should be determined comprehensively and reasonably with the involvement of the robot stakeholder target. In view of this, the trade-off is analyzed to establish the following basic rules:

a. Influence on the usefulness

If the realization of risk reduction, which is intended by the robot designer, affects the usefulness of robot use, reduction in use frequency or avoidance of use could be resulted in. In view of this, the robot designer anticipates loss in the effect of risk reduction taking into account hazard (particularly the disregard of ergonomics) which may form after the application of protective measures.

b. Loss of robot capability

Control of robot output by means of inherently safe design, which may impair the originally intended

operating functions of robots, is applied to such an extent that the practical usefulness cannot be impaired. While residual risks are resorted to the output control by a protective device or the like, the addition of the capability by the user is not applied in principle.

c. Increase of cost (technical difficulty)

If the application cost of the protective measures largely pushes up the cost of the robot body, the practical use of the robot itself could be blocked. For this reason, the total cost is set first, and the priorities of their application are determined second so as not to exceed the total cost set. If there is any technical difficulty in realizing the protective measures, the priorities of their application are determined in the same way as priority determination for cost control.

d. Consideration of benefits

If the user, who has understood residual risks, can place a priority on benefits from the robot use, the robot user can set off the residual risk. This is an act of reducing residual risks in the robot using phase, which the robot designers cannot make do, and the effect of risk reduction depends on the attributes of the robot user. Accordingly, based on the basic configuration of the man-machine system, it is necessary to define who will enjoy the benefits and who will reduce the risks.

4 EVALUATION OF RISK REDUCTION EFFECT

4.1 Equation of effect evaluation

Based on the examination made in Chapter 3, the authors make a proposal of a simplified evaluation method for robot designers to evaluate the effect of residual risk reduction after applying the protective measures. To be specific, the effect of residual risk reduction by the robot user can be expressed as the product of “the factor of ‘the provision of information or means from the robot designer’” and “the degree of implementation of measures by the robot user” and “the trade-off coefficient” (See Figure 2). Involved in the degree of implementation of measures are secondary factors, such as the attentiveness maintenance, comprehension and familiarity of the robot user and the environmental conditions. According to these secondary factors, the degree of implementation of measures by the robot developer is determined.

When the risk reduction effect of the risk reduction means (including information provision) set by the robot designer for risk assessment is Rd , the actual risk reduction effect Rr is calculated by the following Equation (1), where the coefficient of risk reduction by the robot designer as described in Section 2.2 is km , the coefficient of risk reduction by the robot user as described in Section 2.3 is ku , and the coefficient of risk reduction by the trade-off as described in Chapter 3 is kt : $Rr = km \cdot ku \cdot kt \cdot Rd$ (1)

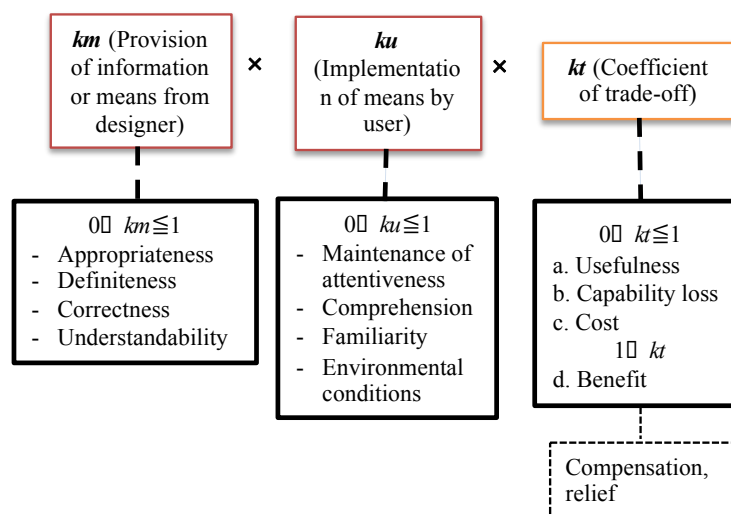


Figure 2. Factors of risk reduction by robot users.

When $Rr \geq Rd$, dealing with risk reduction by the robot user can be determined to have been implemented as expected by the robot designer. Incidentally, each coefficient is determined according to the combination of the factor of each coefficient as shown in Figure 2, but only the benefit of d within kt takes a value of 1 or more. As a coefficient of 1 or more, it is possible to include offset and relief measures.

4.2 An example of wearable walking assist device

Taking a walking assist device for people with paraplegia (“ReWalk” as shown in Figure 3(a)) as an example of collaborative application, each coefficient of Figure 2 is considered with respect to risk reduction for falls, which is a critical hazard source.

Firstly, the fall preventive functions provided by the robot designer include bending prevention for knees, safety stop (upright position resumption), alarm and vibration, all of which being devised not to make km smaller as much as possible. On the other hand, in order to stop avoiding falls from imbalanced walking state or resume the upright position, manipulation of a Lofstrand crutch held by the wearer or supporting act of a care providing therapist (See Figure 3(b)). For this reason, it is difficult to make ku larger, and it is necessary for the robot designer to provide specified practical lecture and training.

Having the above provided, the appropriate wearer can expect increase in kt considering benefits.



(a) Exoskeleton type - “ReWalk”. (b) Assist walking supported by therapist.

Figure 3. Example of wearable walking assist device.

5 CONCLUSION

For the residual risk evaluation of collaborative robots, the authors made a proposal of making an evaluation of the effect of residual risk reduction by the robot user after considering the trade-off for the safety. In the future, if the wearable robot user is not a physically unimpaired person, there will be an anticipated increase in residual risks which cannot be dealt with only by the robot designer, and, therefore, it will become important for the effect of residual risk reduction to be evaluated more comprehensively, not only from the viewpoint of stakeholders but also from the viewpoint of use environment and system and others.

6 REFERENCES

1. *ISO 12100: Safety of machinery - General principles for design – Risk assessment and risk reduction*, International Organization for Standardization, 2010.

Probabilistic Risk Analysis of Human-Robot Collaboration Using the Interference Theory

Kirschner R.-J.¹, Kim E.², Yamada Y.²

¹ Technical University of Chemnitz (TUC) – 62, Strasse der Nationen – 09111 Chemnitz – Germany

² University of Nagoya – Furo-cho – Chikusa-ku – 464 8601 - Japan

robin-jeanne.kirschner@s2013.tu-chemnitz.de

kim.eugene@a.mbox.nagoya-u.ac.jp

yoji.yamada@mae.nagoya-u.ac.jp

KEYWORDS: ISO/TS 15066, Human Robot Collaboration, Interference Theory, Speed and Separation Monitoring

ABSTRACT

This study proposes the use of the Interference Theory (IT) for a probabilistic analysis for the probability of harm occurrence within Human-Robot collaboration (HRC) relying on the Speed and Separation Monitoring (SSM) function introduced by ISO/TS 15066. An experimental battery assembly task is carried out by use of a motion capture system with a total of 10 participants each conducting 20 cycles of the task. The data of this experiment are evaluated by the IT as a statistical computation of the events where interference between the robot and a part of the human hand in the range of protective separation distance appears. A third dimension for the time zones is added to the graph of the IT to achieve accurate results. The productivity of the task is approximated. By applying analytical functions for the calculation with the IT the derived probability can be used for estimation of different parameters of HRC as the productivity.

1 INTRODUCTION

For guaranteeing safety, recently a safety standard supplementing basic requirements for collaborative robots has been launched [1]. The collaborative robots are generally designed to fulfil the given safety functions of Safety-rated monitor stops, Hand guiding and Power and force limiting. These applications of safety functions can be found all over the industry as for example the HC10 by Yaskawa, Panda by Franka Emika or the YuMi by ABB. An attempt of protecting the human from contact with the end effector by a mechanical barrier is shown by Weitschat et al. [2]. Meanwhile, Speed and Separation Monitoring (SSM) which requires the usage of sensors detecting the distance between robot and human is considered to change time consuming layouts of classic shared workspaces.

In the related literature to the SSM function, Sanderud et al. introduced a way of avoiding possible hazardous situations by estimating the probability of a human subject located at a certain space of interest within the workspace at a time. The probability density functions of a human body part taking up defined cells of the workspace were derived within around four cycles of a fictive assembly task [3]. Additionally, general SSM functionality such as specifications of input values and expectation of performance was investigated [3]. Belingardi et al. have examined the SSM function with an assembly task for the automotive industry by conducting a virtual environment simulation [5].

In this paper we present using the Interference theory (IT, hereafter) a strict solution to computing the probability of occurrence of harm. Furthermore, a statistical analysis for an experimental assembly task for which a participant and an industrial robot was used was carried out using a motion capture system to monitor their interference which considers a human hand intrusion as the most critical collision scenario. In contrast to previous studies, in this experiment 10 actual participants each conducted an assembly task consisting of 20 cycles modelled after a real task for battery assembly. Also by asking the participant to perform at different speeds a real life situation was modelled.

2 INTERFERENCE THEORY (IT)

In Reliability Engineering ways are being introduced in which the probability of failure of systems can be derived. Mainly those systems are hardware as for example mechanical or electrical parts. The IT is one of the theories. It uses empirically observed data about the stress (s) that is applied to a mechanical part and the strength (S) it can withstand under different conditions. These data are used to produce the probability density functions of both, depending on the distribution.

Probability density functions describe the density of the probability, therefore the area underneath the function is the probability of any event occurring and comes to be one. Due to this characteristic when having two probability density functions, F_S and f_s , the overlapping area between both resembles the likelihood of both events occurring. In case of Reliability Engineering this is the probability of stress exceeding strength, \bar{R} , and therefore the probability of failure. It is calculated by equation (1) with $y = S-s$ [6].

$$\bar{R} = 1 - \iint_0^{\infty} F_S(y + s) f_s(s) ds dy \quad (1)$$

Calculating this probability is necessary as the event of the stress exceeding the strength of a part might result in severe damage. In previous studies Huang and Jin have already found the usability of this theory for the conceptual Design-for-Reliability [7]. In this paper the idea of describing the probability of failure is transferred to the SSM function in HRC. For achieving realistic data an experiment has been conducted.

3 METHODOLOGY

In ISO/TS 15066 different safety functions are being introduced. Those can be required as a combination or single for securing the safety of a HRC. One of the is the Speed and Separation Monitoring. Herein it is obligatory that the distance between human and robot is being observed. Controlling the distance between human and robot is regulated by equation (2). With v_h , v_r and v_s being the velocities of human, robot and sensing system, integrated over time considering the reaction time, T_R , and stopping time, T_S . The parameter C , Z_d and Z_r are related to the performance of sensor systems and robots. Z_d and Z_r are the position uncertainties of the operator and the robot. C , the intrusion distance, is further defined in ISO 13855 and is calculated differently depending on the type of sensing devices [1], [8].

$$S_p = \int_{t_0}^{t_0+T_R+T_S} v_h(t)dt + \int_{t_0}^{t_0+T_R} v_h(t)dt + \int_{t_0+T_R}^{t_0+T_R+T_S} v_s(t)dt + C + Z_d + Z_r \quad (2)$$

The safety distance itself therefore does not cover the perspective of risk, which consists of the probability of occurrence and the severity of the occurring harm. In order to include this aspect to the calculation of the separation distance it is necessary to give a quantitative value to this probability. This is done by evaluating the probability within an experiment.

An assembly process for battery cells was used as a model task. The robotic task was the application of adhesive while the human was to assemble the parts and place them for the robot. Each participant was asked to complete 10 cycles in a row. This was repeated twice. The first time without time pressure, the second time the participant was asked to beat the first time by around 25%. This experiment was performed under agreement of the ethical committee with 10 participants, 6 males and 4 females aged between 20 and 40 years from different nations. The positions of the human hands and the end-effector was traced by a motion capture system. Velocities and distances were derived from this data. By using S_p for defining a potentially hazardous zone the necessary safety distance, S_p' , and the actual distance were compared. The hazardous area was defined as a distance between the end effector and operator and independent from the reliability parameters of the sensor. It is shown by equation (3).

$$S_p' = \int_{t_0}^{t_0+T_R+T_S} v_h(t)dt + \int_{t_0}^{t_0+T_R} v_h(t)dt + \int_{t_0+T_R}^{t_0+T_R+T_S} v_s(t)dt \quad (3)$$

In the experiment the robot was not stopped in order to improve the workflow and evaluate the likelihood of intrusion within a continuous process. In reality the starting and stopping of the robot would increase the time it takes to conduct a task and therefore lower the productivity. Previous research has taken the ratio of the time it

takes the robot to complete a task, $\hat{\tau}$, and the time it takes with the safety system running, τ_R , into account as the productivity of a robot system, P_R . It is calculated by equation (4) [9].

$$P_R = \frac{\hat{\tau}}{\tau_R} \quad (4)$$

4 EVALUATION

Using equation (1) the reliability of the safety within the experimental process is being evaluated. The probability of failure is in this case to be understood as the probability of the human hand intruding into the area defined by the safety distance as a potentially hazardous zone. Therefore \bar{R} is now called the probability of intrusion of the human hand, POI. Using the IT it is calculated by equation (5) shown in Figure 1.

$$POI = 1 - \iint_0^{\infty} F_{s_d}(y + s) f_{s_p'}(s) ds dy \quad (5)$$

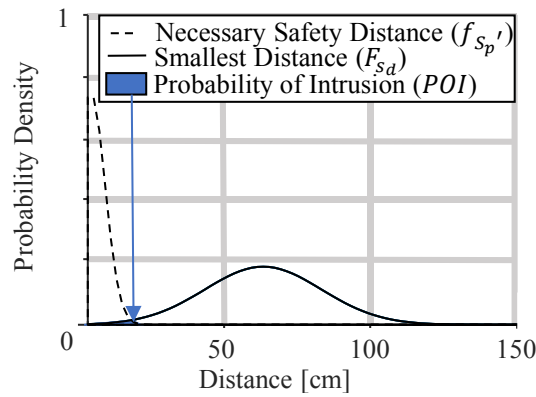


Figure 1. Concept of POI by model functions.

The distribution of the data does not match a common distribution. By using the probability density histograms instead of the probability density functions it is possible to calculate the overlapping area shown in Figure 2 for the interference probability, which leads to equation (6) and (7). Where Δs is the step size for the histograms, i is the step which is being considered, n the amount of steps and y_i the minimum of both values for the probability density at the considered interval.

$$POI = \sum_0^n y_i \Delta s \quad (6)$$

$$y_i = \text{MIN} \left(y_{s_p'}(i), y_{s_d}(i) \right) \quad (7)$$

For a comparison the POI can be calculated from the data set as the number of times intrusions appear divided by the number of measurements. The results are expected to differ slightly.

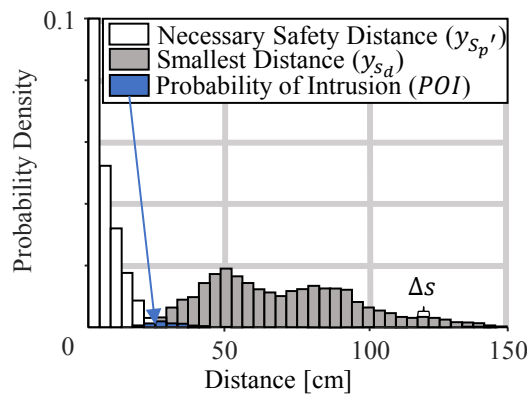


Figure 2. IT with histograms with n bars for the required and actual distance in the collaborative task.

5 RESULTS

5.1 Interference Theory for HRC

The evaluation of the experiment was performed by using the IT as shown in Figure 2. Changing the number of steps will result in an influence of the resolution of the calculation. The performance of the sensor will influence the results for the POI in real tasks. Therefore it is necessary to take different resolutions into account. This is shown by Figure 3. From around $n = 380$ steps, which relates to $\Delta s = 1.4$ mm, the result seems to be reasonably stable around $POI = 3.484\%$. The POI that can be calculated by counting the number of intrusions during the operation was $POI = 0.235\%$.

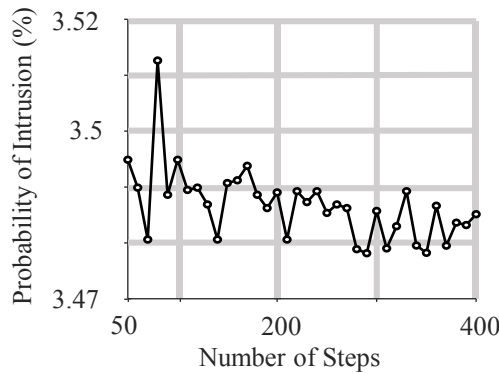


Figure 3. Variation of results for different amount of steps while creating the histogram.

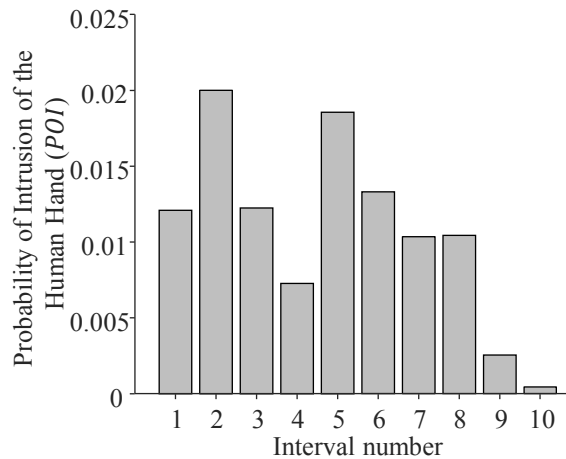


Figure 4. Results for POI within different time intervals.

Another calculation was performed where the POI was compared by using the data of short intervals. The entire record was split into 10 intervals so that the period of each interval was 45 s. The results for the different periods of the task are shown in Figure 4. The mean POI value across all the periods was 1.07%.

5.2 Productivity of the task

In the conducted experiment this ratio is calculated for all participants using the stopping performance and starting time of collaborative robots. This simulates the productivity of a collaborative task performed by different personalities, as it is expected to be in future work fields. Within the experiment a total of 1087 interferences into the assumed safety distance appeared. None of them were actual contacts. The total time taken without stops was 121 minutes. ISO/TS 15066 [1] allows the usage of a stop with category 2. Therefore assuming each of the intrusions would have caused a protective stop without cutting off power which is initiated and reset automatically after the human body part leaves the PSD. The time for stopping the motor and accelerating again plus the time for the human to react and leave the PSD is estimated by $t = 1.6$ s. This leads by usage of equation (4) to a productivity of $P_R = 85\%$.

6 DISCUSSIONS

In this research the IT was introduced into HRC. As a way of interpreting reliability it may be used for the prediction and prevention of accidents. It was observed that the POI calculated using the IT is greater than the probability derived from counting occasions of intrusion. This might be due to the lack of a time factor. Therefore the time factor was added by splitting the data into 10 time intervals. It shows that the POI_{10} is closer to the actual result by counting. When decreasing the size of the steps it might be possible to achieve a very correct result. The IT may be designed as a 3-dimensional calculation method for harm occurrence in HRC by adding a the time as another axis.

The estimated productivity was higher than in previous studies [9]. This allows the assumption that under improved conditions safe tasks are more productive. Therefore it is necessary to support the development of the reliability of implemented sensing devices. Further research should concentrate on adding another dimension to the IT and finding a way of successfully applying the POI to the safety functions for HRC.

7 CONCLUSIONS

In this paper we have presented a novel way of evaluating the probability of occurrence of harm within human-robot collaboration (HRC) named the probability of intrusion of the human hand (POI). We proposed to introduce the Interference Theory to statistically computing the events where interference between the robot and a part of the human subjects hand in the range of the protective separation distance was observed in HRC situation. An experiment performing an actual assembly task was conducted to find the necessity of adding the other dimension of period of task by dividing it in time zones to the original distance-probability graph representing the IT. The Introduction of the third 'period of task' dimension in the IT framework allowed us to compute the POI in the experiment more correctly. The productivity of the overall task was approximated and found to be 85%. We consider that the future work of the study will include estimation of productivity by applying an analytical function to consider the misconduct of hand intrusion in the IT framework.

8 REFERENCES

1. ISO/TS 15066., *Robots and robotic devices– Collaborative robots*, 2016.
2. Weitschat R., Vogel J., Lantermann S., Höppner H., *End-Effector Airbags to Accelerate Human-Robot Collaboration*, 2017 IEEE International Conference on Robotics and Automation (ICRA), Singapore, 2017, pp. 2279-2284.
3. Sanderud A.R., Niitsuma M., Thomessen T., *A Likelihood Analysis for a Risk Analysis for Safe Human Robot Collaboration*, 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), Luxembourg, 2015, pp. 1-6.
4. Marvel J. A., Norcross R., *Implementing speed and separation monitoring in collaborative robot workcells*. Robotics and computer-integrated manufacturing 44, 2017, pp. 144-155.
5. Belingardi G., Heydaryan S., Chiabert P., *Application of speed and separation monitoring method in human-robot collaboration: industrial case study*, 17th International Scientific Conference on Industrial Systems, 2017.
6. Kapur K.C., Lamberson L. R., *Reliability in Engineering Design*, John Wiley and Sons, 1977, p. 125.
7. Huang Z., Jin Y. *Extension of Stress and Strength Interference Theory for Conceptual Design-for-Reliability*, Journal of Mechanical Design, vol. 131, no. 7, pp.1-11, January 2009.
8. ISO 13855., *Safety of machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body*, 2010.
9. Marvel J. A., *Performance Metrics of Speed and Separation monitoring in Shared Workspaces*, IEEE Transactions on Automation Science and Engineering, vol. 10, no. 2 ,pp. 405-414, April 2013.

Work equipments' safe design: two complementary tools to take into account real working situations' variability

Daille-Lefèvre B.¹, Lux A.¹, Etienne A.², Siadat, A.²

¹ Institut national de recherche et de sécurité (INRS) - 1, rue du Morvan - CS 60027 - 54519 Vandœuvre Cedex - France

² Ecole Nationale Supérieure des Arts et Métiers (ENSAM) - 4, rue Augustin Fresnel - 57078 Metz Cedex - France

bruno.daille-lefevre@inrs.fr

aurelien.lux@inrs.fr

alain.etienne@ensam.eu

ali.siadat@ensam.eu

KEYWORDS: design, safety, NFA, FMEA

ABSTRACT

Work equipment's safe design principles are described in the machinery directive 2006/42/CE [1] and in the ISO EN 12100 standard. One of these principles is to take into account the machinery's use, whether normal or abnormal with respect to a standard process. To apply this concept of "integrated prevention", designers need to have a wide vision of future working situation. With a complete vision of working situation, designers could choose safety technical solutions adapted to the real worker's activities. By this way, designers could minimise workers bypass the prevention measure.

In this aim, INRS developed two complementary tools, based on the Need Functional Analysis (NFA) and the Process Failure Modes and Effects Analysis (P-FMEA).

The first tool, useful for working equipment's specification step, is based on the functional analysis. The aim of this tool is to support stakeholders in dynamic dialogue to define the information necessary for implementing safe design principles. To do this, during the functional specification of the work equipment, each function is completed by using the simple 5 W and H questions (Why, Who, What, Where, When and How). By this way, the stakeholders' answers describe not only the technical needs but also the use of the future machinery. A description of an industrial try will show the benefit of this tool to improve health and safety.

The second approach allows designers to take into account real working situations during P-FMEA activities. Usually, only quality and performance points of view are discussed in these meetings. After a short methodology explanation, an example will show how this tool can be helpful to bring occupational health and safety point of view at this design step: users' return of experience (REX) is collected and variability versus nominal process is identified. Then actions can be taken to reduce risks for operators.

With these two complementary tools, analysis scope is thus enlarged to review technical choices for each function, at each process step, in order to give to operators manoeuvre margins to cope with real situations' variability.

1 PROBLEM STATEMENT

In terms of health and safety at work, design gives a well-known prevention gap. The concept of "integrated prevention" has been widely shared by European countries since the 1990s. It consists of applying safe design principles as early as possible in the design process. The aim is to conduct a preliminary risk analysis in order to achieve a lower level of risk in the design of future work equipment by using inherently safe machinery design, taking the necessary protective measures in relation to risks that cannot be eliminated and inform users of the residual risks (Figure 1).

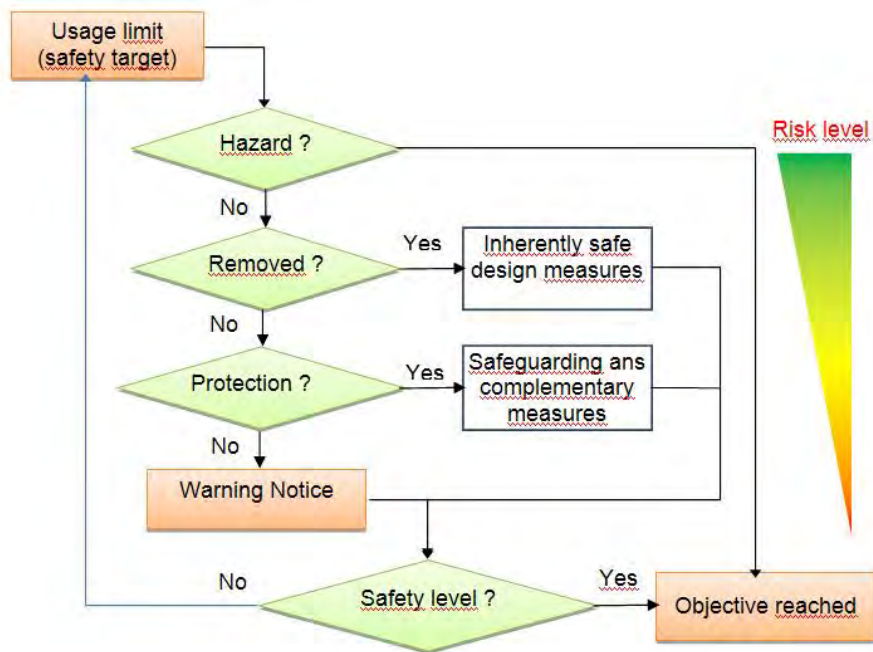


Figure 1. Risk reduction process [2].

In the past, health and safety requirements, relating to the design and construction of machinery, treated essentially mechanical hazard by using technical requirements. New principles of safety integration are multi-hazard and mainly based on users activities. Now, designers have to take into account not only normal use of the machinery but also taking into account any reasonably foreseeable misuse, based on similar machineries and users experience [3].

Designers work isn't only to make technical choice but also to have a wide vision of future working situation, including identifying variability versus nominal process.

Despite existing researches, knowledge and scientific methods [4-6], one of the problem statement is the lack of tools adapted to help designers work to take into account the future working situations [7].

For example, it's well known work activity analysis or workers involving could be helpful during design step, but they are often lacking. Designers mind that these elements increase demands (and give often opposed demands) and delays [7, 8]. So designers escape this "problem" and may imagine their own point of view, in place of worker, to choose the design solutions [9, 10].

Our proposal to solve this problem is to give to the designers a tool helping them to describe and taking into account the machinery uses by using two complementary ways (Figure 2).

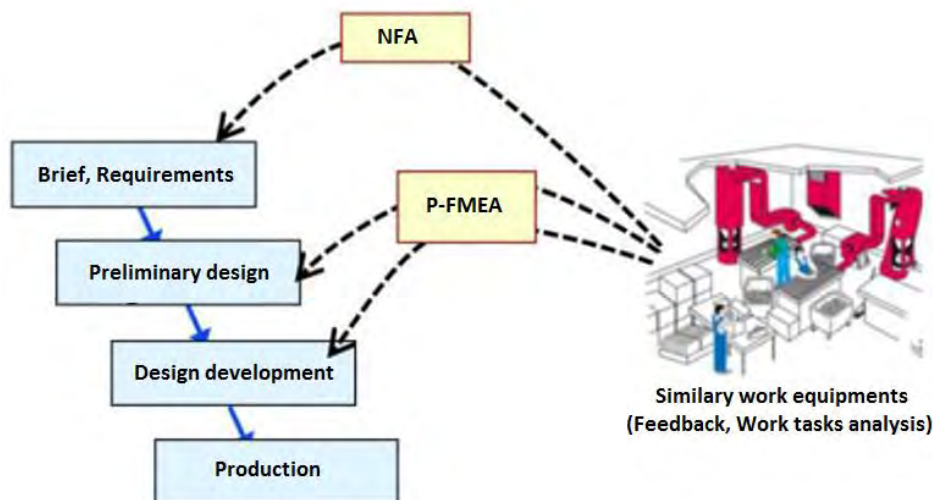


Figure 2. Links between the two proposals and the design process.

The first proposal concerns the initial design step: the specification step, also named brief or requirements sheet. The second proposal checks the technical choice during the following preliminary design and design development steps. In the aim to obtain useful tools, these two proposals are based on well-known tools: the Need Functional Analysis (NFA) and the Process Failure Modes and Effects Analysis (P-FMEA).

Before explaining these two proposals, the “working situation” concept must be described.

2 WORKING SITUATION CONCEPT

The “working situation” concept could be close with the “work system”, described in the EN 614-1 standard [11], which include “one or more workers and work equipment acting together to perform the system function, in the workspace, in the work environment, under the conditions imposed by the work tasks”.

Based on this definition and previous research work on safe design, we developed a working situation model (named MOSTRA, see figure 3) [12]. This model takes into account technical items (system, functions, technical choices...) and also human items (work team, work task...) and risk items (hazard, dangerous area, hazardous event...). But, by itself, this model couldn't lead the design process [13]. It must be used by design tools to follow the design process. In this case, the MOSTRA model ensures the data consistency.

So, for the early stage of the design process, known as “specification” step, we proposed to add MOSTRA to a methodological tool named “Functional analysis” (NFA).

Otherwise, the working situation concept is not static. It also takes into account variabilities linked to real working environment and unplanned events; for example deviations from procedures, adaptations to respond to technical or organizational problems or individual needs. This is what Rasmussen [14] calls the "space of possibilities". Inside, real activity migrates, often beyond the nominal framework initially established by designers: it is the notion of "boundary activity tolerated during use" [15]. Therefore, designing a "work situation" is designing an "adaptable", "plastic" system that gives to operators the necessary "maneuver margins" to carry out their work [9, 16]. This approach must be preferred to the notion of systems adapted to a unique prescribed (average) situation. Indeed, it has been considered for several years as significant axis to prevent musculoskeletal disorders [17-20] and a condition for keeping older operators at work [21]. For this, we propose an evolution of the Process FMEA tool, usually used to make the production lines more reliable.

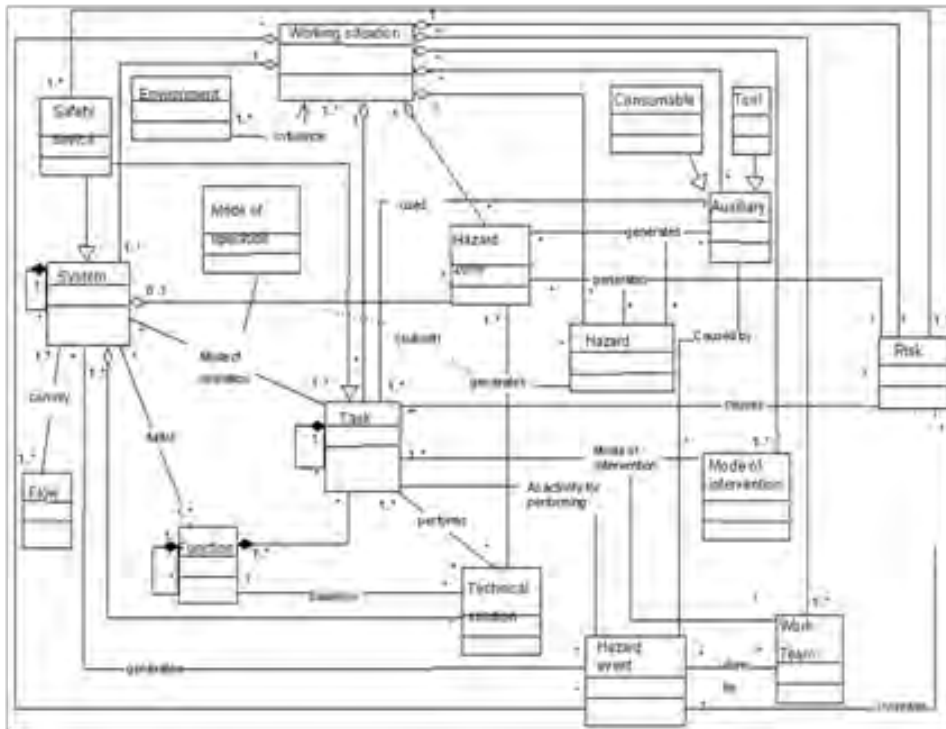


Figure 3. Overall view of the model MOSTRA (for reasons of clarity, not all of the objects are shown).

3 FUNCTIONAL ANALYSIS AND TASKS SPECIFICATION

The aim of the first design step, named “specifications” or requirements, is to identify and formalise the different needs for the future work equipment which will be designed. And, in these needs, we should fine some professional health and safety requirements. As said in lot of scientific papers, the work equipment specifications should contain the standards requirement and also be completed by analyse of similar work tasks or equipment. The aim is to describe the tasks and the constraints of future work situation [4, 7, 8, 22-24].

But designers have first interest in technical aspect. This fact is due to their studies and their diplomas, and also by the industrial’s constraints (level of technical performance required, quality aspects, cost, time...). So, we think that data about equipment’s use or work task analysis shouldn’t be described in a specific requirement chapter but must be developed in each technical function description. By this way, designers should choose safe solution in their design, step by step, and not at the end of their work when the work equipment is entirely designed.

In this aim, with the help of the CETIM (French research centre for mechanical industries), we propose a method based on the functional analysis and on the MOSTRA model described before.

The functional analysis must be made by a team composed by the actors of the future work equipment (designers, production team, service crew...) [25]. Functional analysis begins with the identification of all the functions required by the work equipment, in its different life steps. Next, each function must be defined by technical “measurable” and “controllable” criteria. At this step, we propose to add the “equipment usage” or “tasks” criteria. Firstly, we used the MOSTRA model items linked with the “function” item (see figure 4). But we try also, with the same success, the use of the well-known “5Ws and an H” questions [26]. So, with those entire requirements attached to each function, designers could define and design technical choices adapted to the technical performance level and also to the production/service uses required.

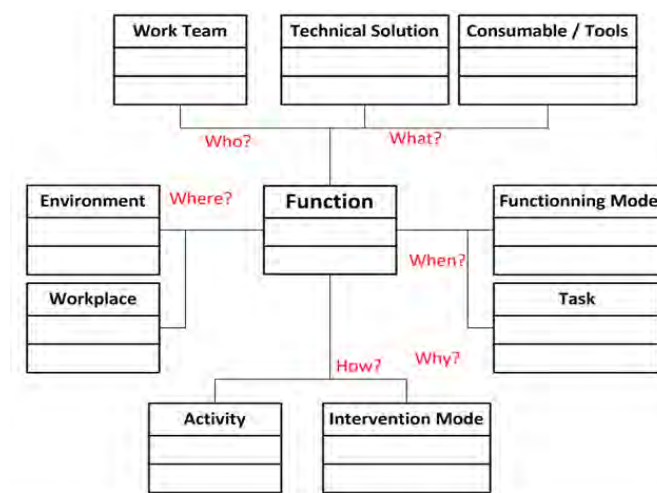


Figure 4. Mapping between MOSTRA and 5Ws and an H questions.

4 PROCESS FAILURE MODES AND EFFECTS ANALYSIS (P-FMEA) AND REAL USES' VARIABILITY

Usually, design projects are staked by project reviews. These meetings bring together the main actors involved (product design, process design, quality, management, production, etc.). The P-FMEA is then used to evaluate the potential failures of manufacturing processes that may have an impact on the quality of the finished product [27]. The production process is broken down into elementary steps and, for each of them, potential failures (causes, effects and detection means) are sought and then prioritized using a criticality index (RPN, Risk Priority Number). Beyond a certain threshold, a corrective action is required and a new quotation allows defining criticality of the corrected situation. The use of FMEA is illustrated here by an example (Figure 5): it is an operation of evacuation of a finishing cap on an assembly line. The failure mode treated is the risk of scratching. The planned corrective actions are the elimination of outstanding stocks (one piece flow) and the implementation of protections at the assembly station.

PROCESS STEP	FAILURE MODE	EFFECT	SEVERITY (S)	CAUSE	OCCURRENCE (O)	DETECTION	DETECTION (D)	RPN = S x O x D	ACTIONS	RESPON-SABILITY	DEADLINE	SEVERITY (S')	OCCURRENCE (O')	DETECTION (D')	RPN' = S' x O' x D'
Workstation 80 : evacuation of cap															
Evacuation of the cap, in box packaging	Scratched part	Customer unsatisfied	5	Part hurt during handling	3	Visual self-inspection	5	75	Workstation improvement (protections)+one piece flow	AL	Feb. 2019	5	1	5	25

Figure 5. Example of failure analysis in a Process FMEA.

However, traditional P-FMEA analysis remains technocentered: when the operator is evoked, he is most of the time considered as a potential cause of a failure (for example, "action forgotten by the operator", "procedure not respected", etc.). There is usually no in-depth analysis to determine the reasons for these "errors" or deviations from the standard task. In addition, action plans often result in the reinforcement of "barriers". These barriers can take several forms: material, functional, symbolic or immaterial [28]. By crossing them to adapt to the real work situations, the operators can expose themselves to risks that were not foreseen during the design.

While some authors [29] also propose using FMEA for the consideration of human factors on a production line (HF-FMEA, Human Factors-FMEA), the starting point of the analysis remains the quality issues. Work situations that do not lead to any quality risk are therefore excluded from the analysis. In order to integrate additional elements concerning the real work situations and to discuss them in a participative way, we propose an evolution of the P-FMEA that we have called "Working Situations FMEA", WS-FMEA (Figure 6). For the form, two options are possible according to companies' practices: either to insert the evolution in the usual table of P-FMEA, or to create a second table completed in parallel of the first one.

PROCESS STEP	REAL WORK SITUATIONS	CAUSES	EFFECTS, RISKS	SEVERITY (S)	PROBABILITY (P)	CRITICALITY (C = S x P)	ACTIONS	SEVERITY (S')	PROBABILITY (P')	CRITICALITY (C' = S' x P')			
Workstation 80 : evacuation of cap													
Evacuation of the cap, in box packaging	One piece flow not respected : 10 parts' buffer with parts on the floor	[X] Performance	Time saving, anticipation	[] Performance			[] Reject	Define a parts buffer (5 parts max). Implement a specific support, well located					
		[] Quality		[X] Quality	Scratched part	5	5		25	[] Validate	5	1	5
		[X] Working conditions	Organisation easier, fewer movements	[X] Working conditions	Falling, shock with forklift	10	3		30	[X] Manage	10	1	10

Figure 6. Example of work situation analysis using proposed table.

The first column (Process Step) is the same than for the classic P-FMEA. This condition is essential. It is indeed the starting point of the P-FMEA and WS-FMEA analysis, which can thus be conducted in parallel.

The second column allows the introduction of experience feedback, identifying work situations different from the nominal conditions. We thus find variability in its various forms described previously: abnormal predictable situations, migrations, boundary activities tolerated during use [15], etc. By taking over the assembly operation mentioned above as an example, the operator could set up an intermediate stock not planned at the exit of the assembly station (not respecting the procedure which imposes one piece flow).

It is important that the variability items are collectively validated by the operators. Their relevance to working conditions will therefore be legitimate. Different techniques based on the ergonomic approach (interviews, observations, questionnaires, self- or cross-confrontations, etc.) can be used for this, even the "5Ws and an H" type of questioning previously used jointly with the NFA.

The next two columns (Causes and Effects) provide a participatory analysis of the causes of the gaps and their potential effects on the work situation. From the literature [14, 28], three criteria were used to qualify them: performance, quality and working conditions. A cause or effect may fall under one or more of these criteria. Using the previous example, ergonomic analysis shows that parts' buffers are a way for operators to cope with tensions in a non-stabilized system [30]: in this case, we will identify causes "performance" and "working conditions". "Quality" and "working conditions" will be the main effects of this deviation from the prescribed procedure: buffers are indeed a potential source of defects, especially for fragile parts (scratches); they can also clutter the workstation or traffic lanes.

As with the classical P-FMEA, it is possible to calculate a criticality index for each failure mode, for example by relying on the BCD theoretical model of barriers' crossing [31]. This rating has not been developed here. We prefer to leave the choice to the working group involved in this analysis to develop their own evaluation criteria and scales.

Finally, for the "Actions" column, three types of decisions have been predefined depending on whether or not the "working conditions" aspects have been identified as causes or effects of a deviation:

- Refuse the gap: the "real" situation is unacceptable as it stands and corrective action is essential to return to the prescribed situation: for the purpose of prevention, it will be for example when the real situation has a negative effect on working conditions (for example, an operator will bypass a safety device to save time). However, it will not be possible to refuse a deviation if it is due to difficult working conditions of the prescribed situation.
- Validate the difference: the "real" situation is accepted as it is, because without negative consequences. This is for example the case where an operator would carry out an operation by hand instead of using the recommended tool, without degrading its performance or quality and without putting its health into play. On the other hand, and always in a prevention perspective, we will not be able to "validate" the gap if it has a negative impact on working conditions.
- Manage: the situation is acceptable provided that it is modified: it will be necessary, for example, to make modifications to ensure that the operation is carried out safely.

Thus, in the example, the project team cannot "refuse" the real situation; this would reinforce the "barriers" by setting up, for example, new procedures or an automatism guaranteeing an operation without "parasite" buffer. Operators would then be forced to follow a theoretical standard which does not allow them to cope with the instability of the work system. "Validate" the current situation is also not relevant: there is no planned location for the parts' buffer and this situation generates both quality risks and security risks.

The project team can therefore only "manage" the real situation by sizing the parts' buffer, based on feedback from the operators, and by arranging the position accordingly (location, support, etc.).

5 DISCUSSION

As said in the beginning of this paper, the concept of "integrated prevention" during work equipment design must be a global view (or systemic view) of work situations and, also, include the variability versus nominal process.

To answer to this question, we proposed two complementary approaches based on the Need Functional Analysis (NFA) and the Process Failure Modes and Effects Analysis (P-FMEA).

The first, attached to the initial design step and the definition of the work equipment requirements, offers some easy asks (Why, Who, When, Where, What and How) to help the customer and the designer to precise and define the operator use or the tasks linked to each technical function. Health and safety requirements are in this case not described in a specific chapter of the requirements sheet, but included in each future work equipment function: each function must be safe.

Two industrial cases, one with a designer [32] and one with the final work equipment user [33] showed this approach could easily be used by Small and Medium Enterprises / Industries (SME / SMI), with success for health and safety.

In fact, add to the well-known benefits of functional analysis to structure the work equipment requirements sheet, the proposed asks to define the technical function helped, in these industrial cases, the customers and the

designers to complete the requirements and add data coming from previous equipment or similar situation, based on their own experience, but not expressed in the first version of the requirements.

The definition of the work equipment uses, for each function, helped the designers to understand the customer needs, and by this way to identify early:

- Some functions which need a specific technical development to ensure the answer to the needed use.
- Some hazardous situations or area, helping the designer to evaluate and reduce the risk during the design task, as requested by the law in the machinery directive.

As an extension of the NFA, the P-FMEA can be used during the design phase of new production equipments, or as a corrective measure for their improvement. We therefore propose to rely on this tool to encourage designers to create or preserve the "maneuver margins" necessary to carry out the work of operators. However, this approach will be more suited to routine design cases, where production teams can use their experience on similar processes. Innovative designs or totally new teams are limits to our proposal.

This evolution consists in expanding the scope of analysis in order to question, for each function, the technical solutions envisaged with regard to real uses and their variability.

Although it contributes to this, the proposed FMEA "Work Situations" approach should not be confused with the risk assessment process, which is the responsibility of any designer of work equipment. There have already been attempts to use the FMEA formalism to make this phase of risk assessment more precise [34]. However there is a strong limitation due to the single-causal approach of this tool.

6 CONCLUSION AND PROSPECTS

By using well-known design tools (Need Functional Analysis (NFA) and the Process Failure Modes and Effects Analysis (P-FMEA)), two approaches were proposed to include to the design process the future operator use of a work equipment.

These approaches give a support to the designers to have a global view of the future work equipment and not only the technical view. If these supports are used by a team (customer, final users, designer...), they help them to explain, describe and complete the future work situations and their variability. As they are based on well-known design tools (NFA and P-FMEA), they don't require new tools for designers and don't increase their work tasks.

But requirement step and process failure analyse are not the only way to include working situations in the global process design. The other design steps need also a support to help the designers. This is the subject for future research on risk analysis or workers tasks simulation.

7 ACKNOWLEDGEMENTS

These research works were conducted with LCFC laboratory from ENSAM (French mechanical engineers school) and CETIM (French research centre for mechanical industries).

8 REFERENCES

1. Directive 2006/42/EC, Approximation of the laws of the Member States relating to machinery. Official Journal L 157, 09/06/2006.
2. NF EN ISO 12100, Safety of machinery. General principles for design. Risk assessment and risk reduction. AFNOR, 2010.
3. Fraser I., *Guide pour l'application de la Directive 2006/42/CE*, 2010 http://ec.europa.eu/enterprise/sectors/mechanical/files/machinery/guide-appl-2006-42-ec-2nd-201006_fr.pdf, 441 p.
4. Sagot J. C., Gouin V. and Gomes S., *Ergonomics in product design: safety factor*, Safety Science, Special issue « Safety in design », 41 (2-3), 2003, pp. 137-154.
5. Sun H., Houssin R., Gardoni M., de Bouvront F., *Integration of user behaviour and product behaviour during the design phase: Software for behavioural design approach*, International Journal of Industrial Ergonomics, Vol. 43, Issue 1, January 2013, pp. 100–114.
6. Neumann W. P., Ekman, M. and Jorgen, W., *Integrating ergonomics into production system development - The Volvo Powertrain case*. Applied Ergonomics 40(3), 2009, pp. 527-537.
7. Lamonde F., Richard J.G., Langlois L., Dallaire J. and Vinet A., *La prise en compte des situations de travail dans les projets de conception. La pratique des concepteurs et des opérations impliqués dans*

- un projet conjoint entre un donneur d'ouvrage et une firme de génie conseils. IRSST - Rapport de recherche R-636, 2010, 146 p.
8. Villatte R. and Dimerman S., *Ergonomiser les normes « zones d'atteintes » ou l'usage qui en est fait*. Actes du Congrès SELF, 2004, pp. 93-102.
 9. Béguin P., *Conception et santé : quelques remarques sur le statut de l'activité de travail dans la conception des systèmes de production*. PTO 14(4), 2008, pp. 369-384.
 10. Darses F. and Wolff M., *How do designers represent to themselves the users' needs?* Applied Ergonomics, 37(6), 2006, pp. 757-764.
 11. NF EN 614-1:2006+A1, *Sécurité des machines, principes ergonomiques de conception*. AFNOR, 2009, 7p.
 12. Hasan R., Bernard A., Ciccotelli J. and Martin P., *Integrating safety into the design process: elements and concepts relative to the working situation*. Safety Science, 41 (2-3), 2003, pp. 155-180.
 13. Daille-Lefèvre B. and Marsot J., *Intérêt des environnements PLM pour la mise en pratique des principes de conception sûre*. CPI 09, Fèz, Maroc, 2009, 9 p.
 14. Rasmussen J., *Risk Management in a dynamic society: a modeling problem*. Safety Science, 27 (2-3), 1997, pp. 183-213.
 15. Fadier E. and De La Garza C., *Towards a proactive safety approach in the design process: The case of printing machinery*. Safety Science 45, 2007, pp. 199-229.
 16. Daniellou F., *L'ergonomie dans la conduite de projets de conception de systèmes de travail*, In Falzon P. (Ed.) Ergonomie. Paris : PUF, 2004.
 17. Coutarel F., Daniellou F. and Dugue B., *Interroger l'organisation du travail au regard des marges de manœuvre en conception et en fonctionnement, La rotation est-elle une solution aux TMS ? Conception et organisation dans les abattoirs en France*, Pistes, vol 5 (2), 2003.
<http://www.pistes.uqam.ca/v5n2/articles/v5n2a2.htm>
 18. Douillet P. and Schweitzer J.M., *TMS, stress : gagner des marges de manœuvre*. In BTS, Le stress au travail, n° 19-20, 2002, pp. 64-66.
 19. Roquelaure Y., Malchaire J., Cock N., Martin Y.H., Piette A., Vergracht S., Chiron H. and Lenoulangier M.A., *Quantification de l'activité gestuelle au cours des tâches répétitives de production de masse*, DMT 85(102), INRS, Paris, 2001, pp. 167-176.
 20. Brunet M. and Riff, J., *L'analyse et l'exploitation de la variabilité gestuelle pour prévenir les TMS*, Pistes, vol. 11 (1), 2009, <http://www.pistes.uqam.ca/v11n1/articles/v11n1a7.htm>
 21. Gaudart C., *La baisse de la polyvalence avec l'âge : question de vieillissement, d'expérience, de génération ?*, Pistes, vol. 5 (2), 2003, <http://www.pistes.uqam.ca/v5n2/pdf/v5n2a4.pdf>
 22. Lemarchand C., *Cahier des charges du point de vue de l'activité de travail*, Techniques de l'Ingénieur, A 5093, 1998, 5 p.
 23. Fadier E. and De La Garza C., *Safety design: Towards a new philosophy*, Safety Science, 44, Issue 1, 2006, pp. 55-73.
 24. Daniellou F., *Des fonctions de la simulation de situations de travail en ergonomie*, Activités, vol. 4 (2), 2007, pp. 77-83.
 25. AFAV, *Exprimer le Besoin - Application de la démarche Fonctionnelle*, Paris, AFNOR, 1989, 372 p.
 26. Jang S. and Woo W., *Unified context representing user-centric context: Who, where, when, what, how and why*, International Workshop on ubiPCMM, CEUR Workshop Proceedings, 2005, pp. 26-34.
 27. NF EN 60812, *Techniques d'analyses de la fiabilité du système, procédure d'analyse des modes de défaillance et de leurs effets (AMDE)*, AFNOR, 2006, 46 p.
 28. Polet P., Vanderhaegen F. and Wieringa P.A., *Theory of Safety-Related Violations of system barriers*, Cognition Technology & Work, 4, 2002, pp. 171-179.
 29. Village J., Annett T., Lin E., Greig M. and Neumann P.W., *Adapting the failure modes effect analysis (FMEA) for early detection of human factors concerns*, Proceedings of the 42nd annual conference, association of Canadian ergonomists, 2011, pp. 18-20.
 30. Bourgeois F., *Que fait l'ergonomie que le lean ne sait / ne veut pas voir?*, Activités 9(2), 2012, pp. 38-147.
 31. Vanderhaegen F., Zieba S., Enjalbert S. and Polet P., *A Benefit/Cost/Deficit (BCD) model for learning from human errors*, Reliability Engineering and system safety, 96, 2011, pp. 757-766.
 32. Falconnet E., Fadier E., Daille-Lefèvre B., Marsot J. and Roignot R., *Conception des machines. Intégrer la sécurité et la santé dès la rédaction du cahier des charges*, Actes du 10e congrès Qualita, Compiègne, 2013, pp. 306-312.
 33. Daille-Lefèvre B., Roignot R., Marsot J., Falconnet E. and Fadier E., *Méthodologie d'aide à la rédaction d'un cahier des charges basé sur l'usage*, Communication acceptée au 19e congrès lamda mu, Dijon, 2014.
 34. Berthe F. and Vimeux J., *AMDEC Sécurité, 56è fiche*, Favi, 1997, www.favi.com

An Experimental Evaluation of Falling Down Damage Using Forearm Mimics

Okabe K., Saito T., Ikeda H.

National Institute of Occupational Safety and Health, JAPAN (JNIOSH) – Umezono 1-4-6, Kiyose, Tokyo 204-0024– Japan

okabe@s.jniosh.johas.go.jp

saitot@s.jniosh.johas.go.jp

ikeda@s.jniosh.johas.go.jp

KEYWORDS: falling accident, wearable device, forearm injury, bone fracture

ABSTRACT

Risks of falling down with wearable assist apparatus are discussed based on experimental evaluation using Japanese women forearm mimics. Wearable devices such as power assist suits are expected to increase activities and abilities in various industrial fields. Risks of falling in use of them, however, are not clarified yet. To understand risks caused by the falling, impact damage to break forearm or hand are examined in this paper. Affects of impact force are revealed in terms of kinetic energy. Forearm mimics were created to examine the damage of impact force. They are developed based on a 3D model calculated from Japanese women right forearm. Main parts of the mimics are artificial bones. The artificial bone consists of two components: cortical and cancellous as well as human bone. Load breaking test using mimics reveals affects of impact force. Bone fracture of the mimic is regarded as a criterion to show the damage of impact. Kinetic energy causing bone fracture is discussed in the breaking test.

1 INTRODUCTION

Wrist injury called Colle's fracture is famous for falling accidents. Workers sometimes get the fracture when they slipped and put their hands on ground to prevent falling. Three or more months are wasted to repair the injury in usual. Colle's fracture is quite severe injury in terms of occupational safety. Wearable devices such as power assist suite has a scarcity to increase the risk of getting the wrist injury. The mechanism of Colle's fracture, however, is not well known. It is still uncertain how to evaluate the risk of wrist injury due to wearable devices.

A new approach is proposed in this study to know risks of wrist injury by using human forearm mimics. Breaking loads of the mimics are examined in accordance with kinetic energy to indicate the damage of falling. Forearm mimics are created based on a 3D-CAD data formed from CT images of a Japanese woman right forearm. The size of the mimic parts and their geometries are correctly reproduced. To evaluate the tolerance of bone fracture, the mimics are composed from faithfully reproduced artificial bones. The artificial bone consists of two components: cortical and cancellous as well as human bone. They are made from resin and imitate the strength of human bone.

Damages of falling impact are discussed in terms of bone fracture in this paper. In other words, an outbreaking of bone fracture is regarded as a criterion of falling down risks. The magnitude of kinetic energy yielding bone fracture is examined in a breaking test. A weight falls on forearm mimics that are fixed on a base. Falling height is changed in accordance with target kinetic energy. The damages of kinetic energy 20J, 30J, 40J and 60J are evaluated. For example, a 5kg weight is set above 0.41m from top of forearm mimic for the test condition of energy 20J. In the cases of upper energy 30J, a 15kg weight falls down on a mimic from 0.2m height. The test showed that

- 1) Energy 20J is potential risk of bone fracture.
- 2) Energy 30J is a risk of bone fracture.
- 3) Energy 40J is certain risk of bone fracture.
- 4) Energy 60J is obvious risk of bone fracture.

2 FOREARM MIMICS FOR IMPACT LOAD TEST

To estimate forearm tolerance of impact due to falling down, forearm mimics were created based on a 3D-CAD data made from a Japanese forties' woman forearm. Three type mimics were developed to understand the effect by the presence of wrist. Wrist-less mimic is one of the types. Every mimic type has artificial bones imitating the strength of human bones. The artificial bones reproduce the human bone structure mainly constructed by cortical and cancellous. Joints of the bones are roughly reproduced. By the three type mimics, load impact test to evaluate falling damage was performed.

2.1 Specification of artificial bone

- Component: ulna, radius and finger bones.
- Structure: tow-layer structure by cortical and cancellous incorporating medullary cavity.
- Material: epoxy, silicone or polyurethane form. Strength are bellows;
 - Cortical;
 - ◇ Compression: over 150MPa, under 160MPa.
 - ◇ Tensile: over 90MPa, under 160MPa.
 - Cancellous;
 - ◇ Compression: over 15MPa, under 20MPa.
 - ◇ Tensile: over 10MPa, under 15MPa.

Biomechanical strength of artificial bones has already validated by 3-points bending test [1].

2.2 Forearm mimic CAD models

Three kinds of 3D-CAD data were newly designed based on the original CAD data in order to mold the 3 type mimics. Each image of CAD model was shown in Figure 1.

- A) Forearm model: ulna, radius and meat with skin. Ends of ulna and radius are uncovered. Approximately 5cm is out of skin.
- B) Carpus model: carpus bones are added to the forearm model. Carpus includes navicular, lunar, triquetral, trapezium, trapezoid, capitatum and hamatum.
- C) Metacarpus model: metacarpus bones are added to the carpus model. Metacarpus composes 1st metacarpal, 2nd metacarpal, 3rd metacarpal, 4th metacarpal and 5th metacarpal.

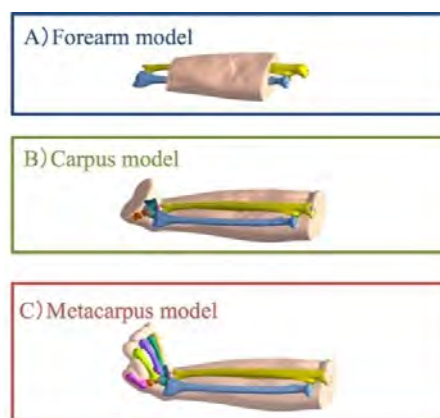


Figure 1. 3D-CAD mimic models.

2.3 Specification of materials

Meat with skin are made from silicone. The solidity is Shore A hardness. Skin and meat were integrally molded.

3 IMPACT LOAD TEST WITH FALLING-WEIGHT

3.1 Development of impact test devices

The newly created three models of forearm mimics based on CAD data are shown in Figure 2. One scene of load impact test is illustrated in Figure 3. Fixing jig was additionally equipped to adjust the posture of mimics so that angle of the crush area can be controlled.



Figure 2. The created three type mimics.



Figure 3. A scene of falling-weight impact test.

3.2 Results of impact test

3.2.1 Test condition for 20J

Impact load test was conducted with a falling-weight equipment. Forearm mimics got impact due to the weight. The weight of the impactor is 5kg. It was set to the position 0.41m height from the front of mimics. It falls down along sidebar-guides. The kinetic energy of the test condition is calculated 20J. Forearm mimics were fixed by epoxy into a metal cylindrical jig. Presence of bone fracture was check with eye after the collision.

3.2.2 Results of forearm model

A test result of forearm model is shown in Figure 4, 5. The Figure 5 shows bone conditions inside the mimic of Figure 4. Both bones: ulna and radius were broken. Unless meat or fat in hand absorbs impact damage, wrist will get severe injury. This result suggests a risk that kinetic energy 20J becomes potential damage to yield bone fracture.

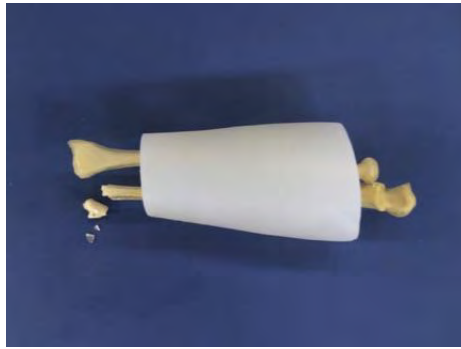


Figure 4. A result of type A) mimic after the test.



Figure 5. Bone fractures of type A) mimic.

3.2.3 Results of carpus and metacarpus model

Under the same condition of 20J energy, all artificial bones were not broken by the check with eyes in the tests for carpus and metacarpus models. To clarify the presence of bone fracture, the bones were confirmed by CT scan images. Sample of CT images and their 3D constructed images are shown in Figure 6 and Figure 7. Fracture was not detected in the images.

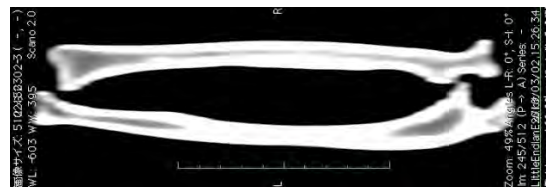


Figure 6. A CT image of the bones after the test.



Figure 7. The 3D reconstructed bone image.

3.2.4 Results of test for 60J

The weight 10kg was added to the impactor in the test for the condition of 60J energy, that is, falling-weight is 15kg. The height was same: 0.41m. Kinetic energy of impactor is counted as 60J in this condition. Test results of carpus model are shown in Figure 8 and Figure 9. As shown in Figure 8, the artificial forearm was crushed and bended by the impactor. Colle's fracture was not monitored. As shown in Figure 9, 10, the test of metacarpus model resulted in same as that of carpus model.

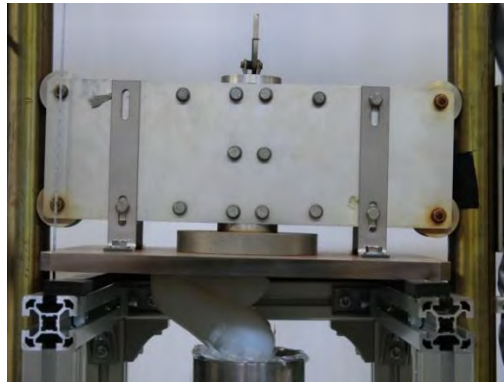


Figure 8. A result of type B) mimic after the test.

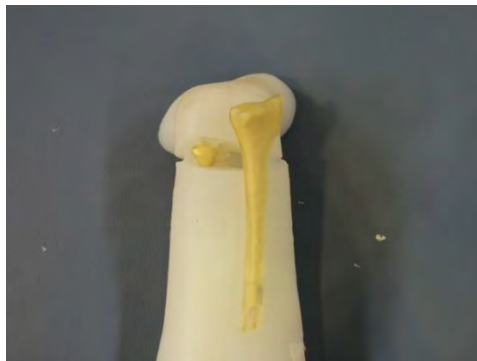


Figure 9. Bone fractures of type B) mimic.

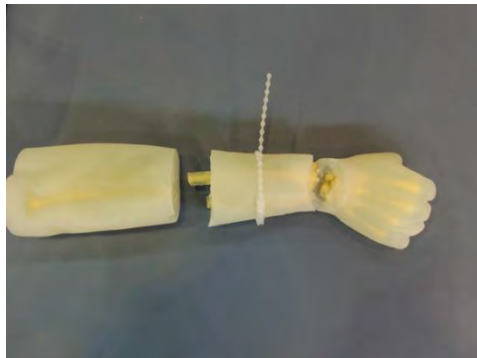


Figure 10. Bone fractures of type C) mimic.

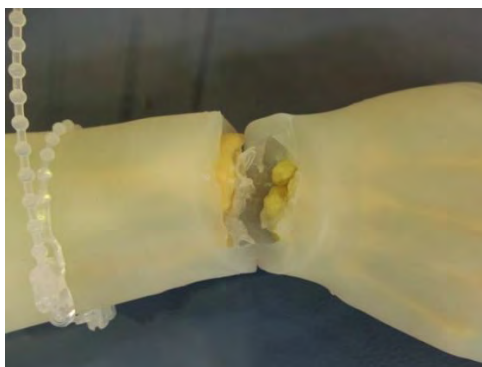


Figure 11. List of type C) mimic after the test.

4 REFERENCES

1. Yamaguchi. A., Okabe. K. and Ikeda. H., *Investigation of evaluation method for strength of artificial bones by using Finite Element Analysis*. Proc. of 8th International Conference Safety of Industrial Automated Systems (SIAS) 2015, pp. 240-242.

Investigation of evaluation method for bending strength of artificial bones simulated a woman's upper-limb bones by using Finite Element Analysis

Yamaguchi A., Saito T., Ikeda H., Okabe K.

National Institute of Occupational Safety and Health, JAPAN (JNIOSH) – 1-4-6 Umezono, Kiyose, Tokyo 204-0024 JAPAN

yamaguchi@s.jniosh.johas.go.jp

KEYWORDS: artificial bone, Finite Element Analysis, bending strength, simple modelling of artificial bone for testing

ABSTRACT

In the field of cooperative robots in Japan, it is required for establish of adequate safety criteria in order to avoid various accident due to cooperative robots, such as care robots. However, technologies and standards that satisfies both the required specifications of cooperative robots and the adequate safety of a cared person has not yet been established. A lot of kinds for artificial bone is developed and investigated in order to establish the technologies and criteria for safety in the field of cooperative robots. However, mechanical properties of developed artificial bones is not clarified because an evaluation test for strength of artificial bones or human bones has not been established. It is necessary to obtain the strength of artificial bone by a strength test in order to investigate the reproducibility and validity of the developed artificial bones.

In this study, the three-point bending test to evaluate the strength for artificial bones has been proposed. First, the bending strength of artificial radius and artificial ulna is obtained by bending test. The pieces of artificial radius and artificial ulna are 9 and 6, respectively. And then, Finite Element Analysis (FEA) is used to estimate the bending strength of artificial bones. The bending strength of 4-directions regarding the center axis direction of the artificial bones is obtained and it is shown that strength direction and weakness direction for load on each artificial bone. In the evaluation by FEA, it is shown that the cancellous bones does not contribute to strength of bones. Also, an availability and an evaluation method for strength of artificial bone by using FEA in field of cooperative robots is shown by comparing the strength of the artificial bone obtained by experimental with that obtained by using FEA. The difference between the both obtained bending strength has 23%. To make the matter worse, the analytical result was assessed as the dangerous side in this case.

1 INTRODUCTION

Cooperative robots are required to operate in close contact with a cared person. In additionally, cooperative robots are required a high power to supporting the activity of cared person. Technologies and standards that satisfies both the required specifications and the adequate safety has not yet been established in the field of cooperative robots in Japan. Therefore, it is necessary to clarify a relationship between the load caused by cooperative robots and the safety of human bone to establish technologies and standards for the field of cooperative robots.

Recently, a lot of kinds for artificial bone is developed and investigated in order to establish the technologies and standards for the field of cooperative robots, because it is difficult to use human bones due to problems on ethics. A developed artificial bone has simulated the physical properties of human tissue. However, mechanical properties of developed artificial bones is not clarified because an evaluation test for strength of artificial bones or human bones has not been established. It is necessary to obtain the strength of artificial bone by a strength test in order to investigate the reproducibility and validity of the developed artificial bones.

2 ARTIFICIAL BONE

The appearances of artificial radius and artificial ulna are shown by Figure 1. Both artificial bones are simulated the upper-limb bones of a Japanese woman. The length of artificial radius and artificial ulna are approximately 210 mm and 229 mm, respectively. The mechanical properties of both artificial bones are shown Table 1. The Young's modulus, yield strength and tensile strength of a part of cortical bone in both artificial bones, which are constructed of an epoxy resin, are 16,000 MPa, 95 MPa and 106 MPa, respectively. Then, The Young's modulus yield strength and tensile strength of a part of cancellous bone in both artificial bones, which are constructed of a

compressive foam, are 155 MPa, 6 MPa and 8 MPa, respectively. The mechanical properties of Both artificial bones are obtained by ASTM D 638[1] and ASTM D1621[2], respectively.



Figure 1. Appearance of artificial radius.

Table 1. Mechanical properties of an artificial bone.

Artificial born	Young's modulus (MPa)	Yield strength (MPa)	Tensile strength (MPa)
Cortical bone	16,000	95	106
Cancellous bone	155	6	8

3 BENDING TEST FOR ARTIFICIAL BONE

A three-point bending test was carried out in order to obtain the bending strength of both artificial radius and artificial ulna. The length of both supporting points is 120 mm as shown in Figure 2. Also, curvature radius of loading point and supporting points are 10 mm and 12 mm, respectively. Figure 3 shows lording direction in both artificial bones. The result of bending test is shown in Table 2, and the test for artificial radius and ulna are carried out 9 and 6 times, respectively. In artificial radius, the maximum failure load is 503.5 N, and the minimum failure load is 428.0 N and the average failure load is 471.9 N. Next, in artificial radius, the maximum failure load is 670.0 N, and the minimum failure load is 508.0 N and the average failure load is 612.7 N. Figure 4 shows the appearance of artificial ulna after the bending test. It is considered that artificial ulna was break due to a brittle failure, because a cracking and a deformation are not observed in artificial ulna after bending test.

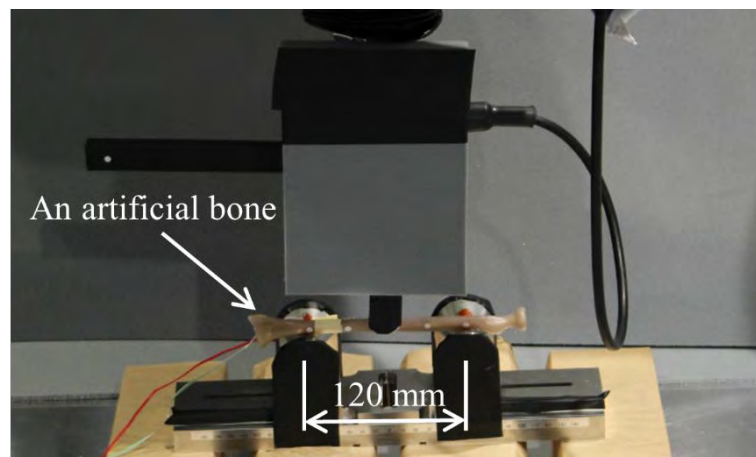


Figure 2. Situation of three-points bending test.

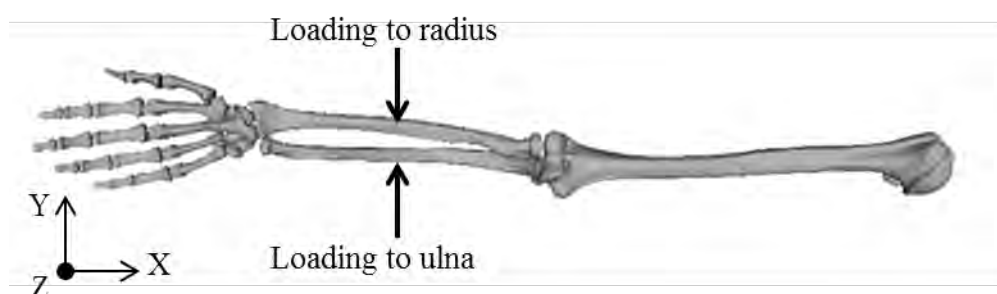
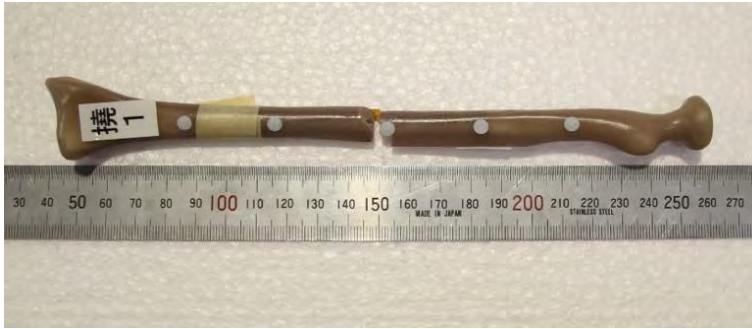


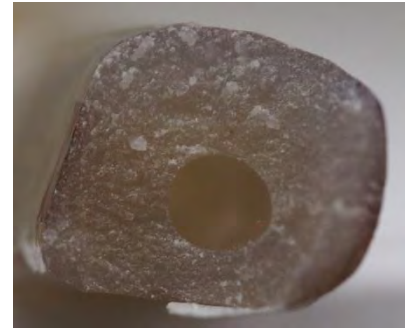
Figure 3. Loading directions.

Table 2. Failure load of artificial bones.

	Artificial radius	Artificial ulna
Number of specimens	9	6
Max (N)	503.5	670.0
MIN (N)	428.0	508.0
Average (N)	471.9	612.7



(a) Appearance of artificial ulna

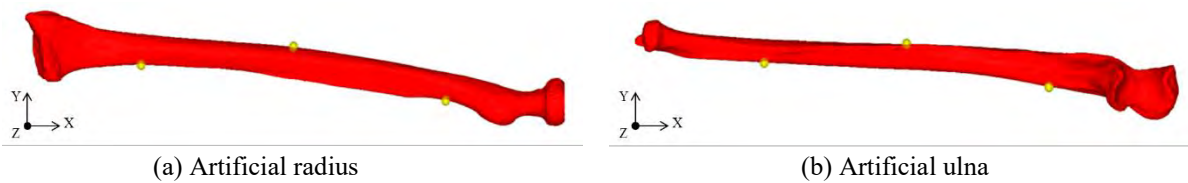


(b) A failure surface

Figure 4. Appearance of failed artificial radius.

4 FINITE ELEMENT ANALYSIS OF BENDING TEST FOR ARTIFICIAL BONE

Finite element analysis (FEA) is carried out in order to calculate the failure load by three-point bending test. Figure 5 shows the FE model of artificial radius and artificial ulna. FEA is carried out using ABAQUS 6.11. The FE model in artificial radius, which is a full-scale model of the artificial cortical bone, meshes 786,891 elements and 164,484 nodes. And the FE model in artificial ulna, which is a full-scale model of the artificial cortical bone, meshes 511,949 elements and 113,266 nodes. Both FE model is using three-dimensional elements (C3D4). The Young's modulus and Poisson's ratio of the artificial cortical bone are 16,000 MPa and 0.34, respectively. The true stress-true strain curve using FEA, as shown in Figure 6, was experimentally derived on the assumption that the specimen volume was constant up to the maximum load point. The true stress-strain relation is obtained based on result of ASTM D 638.



(a) Artificial radius

(b) Artificial ulna

Figure 5. FE models.

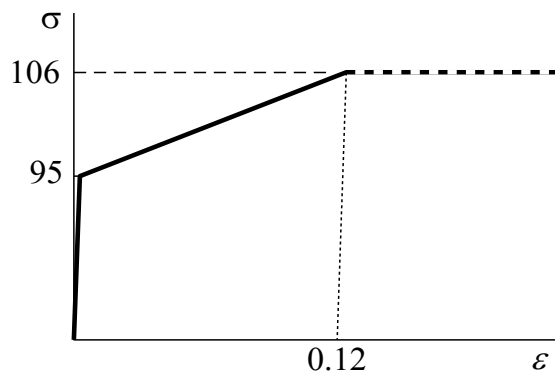


Figure 6. True stress-strain relation using FEA

4.1 Investigation for effect of strength of cancellous bone

The mechanical properties of artificial cancellous bone are lower than that of artificial cortical bone. It is considered that artificial cancellous bone does not contribute the strength of artificial ulna. Thus, it is investigated the effect of strength of cancellous bone by using FEA. In the present study, the failure load is used as an index for strength of artificial bone. Also, the failure load calculated by using FEA is defined as the load at which the strain does diverge. Figure 7 shows von Mises stress right before a break of the radius. Failure load of radius with and without cancellous bone are calculated by FEA is 654 N. The cancellous bone does not affect to strength of artificial bone. In other words, the strength of cancellous bone also does not affect to strength of human bone.

4.2 Evaluation of bending strength on 4-directions in radius and ulna

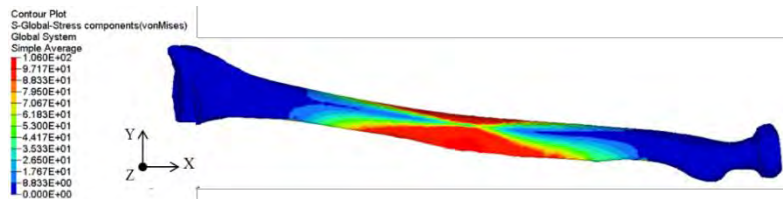


Figure 7. Stress distribution right before break on artificial radius.

The upper-limb bones have a multi-layer structure and a complicated shape. Thus, it is considered that bending strength of upper-limb bones is difference by loading direction. And, it is not clarified that bending strength from various directions. In the present study, the bending strength on 4-directions in radius and ulna is investigated by using FEA. 4-directions are, as shown by Figure 8, from thumb side, from little finger side, from back of hand side and from palm side. Table 3 shows the failure load on 4-directions in artificial radius and artificial ulna. The highest failure strength in artificial radius is 713 N from little finger side, and that in artificial ulna is 1010 N from back of hand side. It is clarified the resistant bending strength in radius and ulna by FEA. Then, it is considered that also most high strength direction of human radius and ulna is same direction in FE results, respectively.

4.3 Comparison of test result and FE result

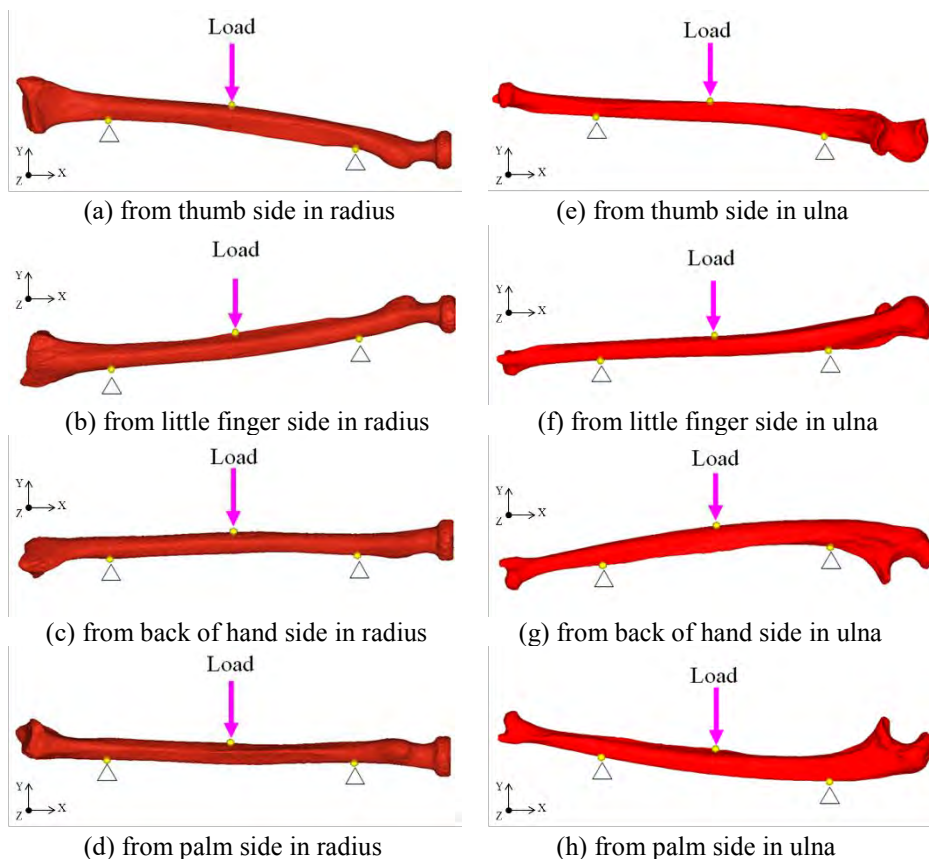


Figure 8. Boundary conditions on 4-directions in FEA.

In the radius, failure load of test result and that of analytical result are 503.5 N and 654 N, respectively. The

Table 3. Calculated failure load on 4-directions by using FEA.

	Calculated failure load (N)	
	Radius	Ulna
From thumb side	654	605
From little finger side	713	821
From back of hand side	593	1010
from palm side	462	558

difference between the both results has 23%. To make matter worse, the analytical result is assessed as the dangerous side in this case. it is considered the following reason as the cause which is generated the gap.

- 1) Difference of boundary conditions
- 2) Assessment by failure load
- 3) Without compressive strength

The contact point in bending test and that in analysis are 6 and 3, respectively. Then, failure load is defined by using failure load, but is not defined by using failure strain. Additionally, it is not used compressive stress-strain curve in analysis. In present study, the analysis conditions which are included boundary conditions, mechanical properties and etc. are set to simple compared with test conditions. Thus, it is estimated that the difference is caused due to multiple influences as shown by above conditions. A future task for the analysis is identifying the cause of the differences and reducing the differences. Also, if the safety factor is applied to the failure load in analysis, the analysis condition in this study is effective to decide the load by cooperative robots for a person.

5 CONCLUSIONS

- (1) A three-point bending test was carried out in order to obtain the bending strength of both artificial radius and artificial ulna. The bending test for artificial radius and ulna are carried out 9 and 6 times, respectively. In artificial radius, the maximum failure load is 503.5 N, and the minimum failure load is 428.0 N and the average failure load is 471.9 N. Next, in artificial ulna, the maximum failure load is 670.0 N, and the minimum failure load is 508.0 N and the average failure load is 612.7 N.
- (2) The bending strength on 4-directions in radius and ulna is investigated by using FEA. 4-directions are from thumb side, from little finger side, from back of hand side and from palm side, respectively. The highest failure strength in artificial radius is 713 N from little finger side, and that in artificial ulna is 1010 N from back of hand side. It is clarified the resistant bending strength in radius and ulna by FEA.
- (3) In the radius, failure load of test result and that of analytical result are 503.5 N and 654 N, respectively. The difference between the both obtained bending strength has 23%. To make the matter worse, the analytical result was assessed as the dangerous side in this case.

6 REFERENCES

1. ASTM D638-14, Standard Test Method for Tensile Properties of Plastics, ASTM international.
2. ASTM D1621-16, Standard Test Method for Compressive Properties of Rigid Cellular Plastics, ASTM international.

Analysis of Machinery Accidents in the Food Processing Industry During the Cleaning and Disinfection Phases

Giraud L.¹, Blaise J.-C.², Tissot C.³

¹ Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST) – 505, boul. De Maisonneuve Ouest – Montréal (Québec) – H3A 3C2 – Canada

² Institut national de recherche et de sécurité (INRS) – 1, rue du Morvan – CS 60027 – 54519 Vandœuvre Cedex – France

³ Institut national de recherche et de sécurité (INRS) – 65 Boulevard Richard Lenoir – 75011 Paris – France

giraud.laurent@irsst.qc.ca
jean-christophe.blaise@inrs.fr
claire.tissot@inrs.fr

KEYWORDS: cleaning, accident analysis, safety of machinery, food safety

ABSTRACT

In the food processing industry, the safety of production equipment is very important for public consumer safety. Increasingly stringent regulatory cleaning and hygiene requirements expose workers to machine hazards because they must work on or dismantle the equipment. Most of the time, guards and other protective devices are removed to allow better access to moving parts and more effective cleaning, disinfection, and post-disinfection inspection. The food industry thus faces a dilemma: allowing workers to access moving parts of machines to properly clean, disinfect and inspect them, thereby exposing them to hazards such as amputation, cuts and lacerations, and being struck by, crushed against or caught in equipment; or not allowing workers to access moving parts in order to ensure their safety, at the expense of health risks to consumers.

The overall objective of this research project is therefore to carry out an exploratory study of these risks and means of reducing them, and to identify possible ways of making the cleaning, disinfection and machine inspection phases safer, while satisfying the health requirements of the food processing industry.

As part of this research, data from the EPICEA database in France were analysed. The selection of data to target the machinery cleaning phases was done by coupling the variables “Activity of the victim” / “Object of the activity,” as well as the variables “Material factor at the origin of the harm” / “Relation victim” / “Material factor.” This resulted in the selection of 63 accidents.

1 INTRODUCTION

Machinery used in the food processing industry must comply with a wide range of machine safety and cleanliness requirements. To gain a better understanding of these sometimes conflicting constraints, a joint research project involving Quebec and France is being conducted [1]. The purpose is to identify possible ways to make the cleaning, disinfection and inspection stages safer for workers, while still meeting the cleanliness requirements of the food processing industry.

In Quebec, the degrees of risk of several food processing sectors [2, 3], for the years 2002 to 2011, are all considered to be high or extreme, according to CNESST [occupational standards, equity, and health and safety board] criteria, either for the entire sector or solely for small and medium-sized businesses. In France, too, food processing is a high-risk industry. According to France’s Caisse nationale de l’assurance maladie [national health insurance fund] [4], in the food processing industry, there were 18,303 accidents at work (AW) with at least 4 days of absence in 2014 and they led to a total of 1,155,612 days’ absence from work.

To perform the prewashing, thorough cleaning of all soiled surfaces of the machine, then the disinfection and rinsing that are required by hygiene and quality control officers, workers must be able to access all the soiled areas. The soiled areas of a machine generally also tend to be the hazard zones, that is, the areas where mechanical hazards exist. There are three standards that deal with the design of food processing machinery: standard ISO 14159:2002 [5], standard EN 1672-1 respecting safety requirements [6] and standard EN 1672-2 respecting hygiene requirements [7].

To document our research, we searched the INRS’s EPICEA database for information on the occurrence of accidents involving the cleaning or disinfection of food processing machinery.

2 METHOD

2.1 EPICEA database

Managed by the INRS, EPICEA is a national, anonymous database that, at the time of the search, contained records on 23,799 accidents at work. The accidents have occurred since the 1980s and involved employees covered by the French general social security system.

EPICEA does not document all accidents exhaustively, but rather all fatal or serious accidents and those significant for prevention. It is therefore not representative of all accidents at work covered by the general social security system in France. It is used for investigative, rather than statistical purposes.

The purpose of the EPICEA database is to learn about the causes and sequence of events leading to a given type of accident, without seeking to establish liability, and to provide illustrative cases for awareness, training and other initiatives.¹

2.2 Selection of accidents

The following parameters were used to select the accidents: food processing industry,² date of accident, accident with a machine (according to a filter), cleaning activity. To this end, we used information from the EPICEA database reserved for the INRS.

The dates selected were the years 1998 to 2018 inclusive. The accidents with a machine were obtained by setting the variable “Object of the activity” to “Machine, equipment.” Machines for planing metal, welding, grinding and generating power were removed from the search, as they were not relevant to the study.

The cleaning activity was obtained by combining four variables two by two using the following formula: “Activity of the victim” AND “Object of the activity” OR “Material factor at the origin of the harm” AND “Victim/Material factor relationship”

With

- Activity of the victim = *Maintain, clean, put away*
- Object of the activity = *Machine, equipment*
- Material factor at the origin of the harm = *Packaging-wrapping, manufacturing by assembly, manufacturing by division, manufacturing by printing, manufacturing by pressure, manufacturing by removal*
- Victim/Material factor relationship = *Cleaning*

A total of 320 accidents with machines in the food processing industry were identified, 104 of which were considered to be cleaning accidents on the basis of the formula given above. A reading of the case histories identified 63 accidents that concerned cleaning of a machine for hygiene reasons, that is, 19.7% of the initial 320 accidents. Cases of cleaning during repairs, maintenance or restart following a stop were removed.

3 DATA ANALYSIS

This paper presents only the most representative data associated with cleaning and disinfecting food processing equipment in the 63 accidents. We will focus first on the differences between cleaning and non-cleaning, then on the risk reduction features available on the machines or not.

3.1 Sectors concerned

Accidents occur more frequently during cleaning than during a non-cleaning activity in the following sectors: +8.9% 158VB (food industries not elsewhere classified), +8.2% 158AB (industrial production of bakery

¹ Source : <http://www.inrs.fr/publications/bdd/epicea.html>, for the public version which is an extraction of the version reserved for the INRS, 18 juillet 2018.

² Risk codes: 151AD, 151CA, 151EB, 152ZA, 153EC, 155CB, 157AB, 158AB, 158HC, 158KB, 158PB, 158VB, 159SB; codes NFA : 10.11Z, 10.12Z, 10.13A, 10.13B, 10.20Z, 10.31Z, 10.32Z, 10.39A, 10.39B, 10.41A, 10.41B, 10.42Z, 10.51A, 10.51B, 10.51C, 10.51D, 10.52Z, 10.61A, 10.61B, 10.62Z, 10.71A, 10.71B, 10.71C, 10.71D, 10.72Z, 10.73Z, 10.81Z, 10.82Z, 10.83Z, 10.84Z, 10.85Z, 10.86Z, 10.89Z, 10.91Z, 10.92Z.

Poster session

products, pastry and pizza), +4.8% 153EC (processing and conservation of vegetables and fruits), +4.6% 151EB and 10.13A (industrial preparation of meat-based products (including casings), +1.6% 158PB (production and processing of coffee and spices).

3.2 Machines concerned

The three machines involved in the most accidents during cleaning are 20.6% *Filling, packaging, packing, wrapping, nailing machines*; 19% *Cutting, slicing (other than saws), unwinding and defibring machines*; and 17.5% *Blending and mixing machines*.

The three biggest cleaning/non-cleaning differences between the types of machines are +11.1% *Cylindrical laminating, mixing, levelling, printing machines*; +7.3% *Pressing, moulding and injecting machines*; and +5% for *Cutting, slicing (other than saws), unwinding and defibring machines* and *Blending and mixing machines*.

3.3 Time and day of accident

Accident time varies significantly between the cleaning phases and the non-cleaning phases. The variations are due to the fact that machine cleaning is done between two production cycles, so primarily evenings and nights, or at the end of a shift.

The three biggest cleaning/non-cleaning differences with regard to accident time are +4.7% 7–8 p.m.; +4.3% 10–11 p.m., and +3.6% for 4–5 a.m., 11 a.m.–12 noon and 4–5 p.m..

Conversely, the three biggest time-of-day differences for an accident during a non-cleaning phase in relation to a cleaning phase are -8.7% 7–8 a.m., -4.3% 5–6 a.m., 6–7 a.m. and 10–11 a.m. and -2% 11 p.m.–12 midnight.

Accidents during a cleaning phase are more frequent on Thursdays, Fridays and Saturdays.

3.4 Victim's sex

There is little difference by victim's sex between the cleaning and non-cleaning phases, with men being associated with slightly more cleaning accidents. Note that women represent 6.8% of all accident victims in the EPICEA database, but 25.6% of the 320 accidents examined in this study.

3.5 Victim's job

The job that figures most frequently in all the accidents is "*Operators of food and related product manufacturing machinery*." It accounts for 52.4% of the accidents that occurred during cleaning and 43.6% of the non-cleaning accidents. The other two job titles most frequently associated with cleaning phase accidents are "handlers" (12.7%) and "other cleaners" (11.1%).

These job titles corroborate the work situations described in the accident summaries, which often indicate that machine users (machine operators) clean the machine at the end of their shifts: "Around 5 a.m., at the end of the shift (working hours: 9 p.m. to 5 a.m.), the victim—a 22-year-old assistant baker hired by the company 12 days earlier—was supposed to clean the belt of the continuous processor..."; "Toward the end of his shift, the victim, a 24-year-old deboner who had been on the job for a year and a half, began cleaning his machine..."; "Toward the end of the production run, in order to clean the dough sheeter ..."

3.6 Contributing factors

The three factors that contribute the most to accidents during the cleaning phase are 55.6% *Hazardous or inappropriate operating procedure*, 44% *Working on machine while it is running* and 31.7% *Inadequate training*.

The three factors that contribute the most to accidents during the non-cleaning phase are 54.5% *Hazardous or inappropriate operating procedure*, 40.9% *Working on machine while it is running* and 24.1% *Inherent design-related machine risk*.

The three biggest cleaning/non-cleaning differences with respect to contributing factors are +16.6% *Inadequate training*, +5.3% *Defective design/arrangement of workstation* and +3.6% *Working on machine while it is running*.

Poster session

A lack of guards is most frequently mentioned: 27% during cleaning and 30% in other work phases.

When present, the risk reduction features identified on the machines in question are virtually the same for the two phases, cleaning and non-cleaning. Fixed guards are mentioned in 17.5% and 18.7% of cases, respectively, movable guards without locking in 12.7% and 6.6% of cases, and movable guards with locking in 6.3% and 9.7% of cases.

The three causes for this technical barrier failing to operate are the same, but in a different order, depending on whether it's the cleaning phase or the non-cleaning phase. The guard is not implemented (15.9%/10.5%), the guard is switched off or has been disabled (14.3%/15.2%), and the guard is poorly designed in terms of size or strength (12.7%/11.3%).

Tables 1 and 2 summarize the results of the analyses conducted in an effort to understand, from a reading of the accident case histories, how access could be gained to the hazard zone when the machine was running (44 cases out of 63), as well as the causes of inadvertent start-up (17 cases out of 63). The two remaining cases concerned machines that tipped over during cleaning.

Table 1. Possibilities of gaining access to hazard zone – Machine running (in operation or inertia)

	Machine in operation				Machine inertia		
	Normal operation	Cleaning or no load	Operation mode not specified	Degraded mode	Step-by-step	Requested stop	□
Access next to guard	1	2	3			1	7
Access by product outlet	1	1	4				6
Unspecified possible access		1	4	1			6
Parts of dismantled machine			10		1		11
Guard without locking			1				1
Flawed design of locked guard			1				1
Safety switch failure			2				2
Safety switch disabled			2				2
Material projected outside machine			1				1
Tool drawn in			5				5
Guard open without failure					1	1	2
□	2	4	33	1	2	2	44

Table 2. Causes of inadvertent start-up of machine

	Other operator	Operator	Product	Technique	□
Machine control activated without worker's knowledge	4				4
Machine control activated with worker's knowledge	1				1
Machine sensor activated	1	5	1		7
Safety switch failure				2	2
Start-up control activated		2			2
Unexplained technical cause				1	1
□	6	7	1	3	17

4 DISCUSSION

The main factors that influence accidents with food processing machinery are virtually the same for the cleaning and non-cleaning phases. On the basis of EPICEA data, it can be stated that machine operating modes

Poster session

are not well thought out by designers, given that they are criticized in around 50% of cases for being inappropriate or hazardous; that workers work on the machine in 40% of cases when it is in operation; and that machine-associated risk is inherent in their design in 25% of cases.

The main risk reduction features mentioned when machines are operating are **fixed or movable guards**. However, three aspects reduce their effectiveness.

First of all, there were no guards in close to a third of cases, which is a significant proportion. Furthermore, the product outlet is one of the places where there are generally no guards. That access possibility ranks third in Table 1.

Second, the guards are poorly designed. They are either not the right size or do not prevent access to the hazard zone, which is the second-ranking access possibility according to Table 1. The choice of materials for the guards could be better, too, according to the assessments of prevention officers. Last, some movable guards are not associated with a locking device, which allows access to the hazard zone without a machine stop being initiated, which conflicts with ISO 14120 [8] and EN 1672-1 [6].

Finally, the guards are removed or disabled in close to a third of all cases when the worker performs the work. That indicates that a guard constitutes a constraint on cleaning work, and that this constraint is reduced when the guard is not used (15.9%) or is disabled (14.3%).

When machine components serve as fixed guards on food processing machinery, the question of how to clean the machine, which may require dismantling them, must systematically be asked. If that will occur, then the designer must manage possible access to the hazard zone. Yet this does not seem to happen, given that this cause is the top-ranked one in Table 1.

When the worker is in the hazard zone, the primary cause of inadvertent start-up of the machine is activation of a sensor by the operator, by another worker or by the product. That means that work on the machine is not being done in a safe shutdown mode [9].

It seems clear from the data that food processing machinery suffers from a **design problem**. Designers don't seem to take into consideration the specific operating mode associated with cleaning, disinfecting and inspecting these machines, in other words, an operating mode that would make it easier to meet cleanliness requirements.

5 CONCLUSION

The results obtained show that night-time hours, Saturdays, the cleaning and maintenance of certain specific machines and certain specific maintenance tasks are associated with cleaning accidents. Conversely, the absence of night work, Wednesdays and other factors are associated with non-cleaning accidents. In addition, in the case histories describing the accidents, it was possible to identify the primary causes of accessibility to the hazard zones of the machine. When the machine is in operation, it appears that the three main causes of accessibility are (i) dismantling of parts of the machine, (ii) access next to a guard and (iii) access through the material inlet or outlet openings of the machine. In the case of inadvertent/unexpected start-up, the main cause is an action inside the hazard zone that activates one of the machine sensors.

It should be noted that this paper is part of a broader research project and that we are going to attempt to confirm or refute these findings, particularly by means of plant visits and observations of actual cleaning and disinfection work on food processing machinery.

6 REFERENCES

1. Giraud L., Chinniah Y., Blaise J.-C., *Exploratory Study of Risks and Risk-reduction Measures during the Cleaning and Disinfection of Machines in the Agrifood Sector*, <http://www.irsst.qc.ca/en/ohs-research/research-projects/project/i/5329/n/etude-exploratoire-des-risques-et-des-moyens-de-reduction-des-risques-lors-des-phases-de-nettoyage-et-de-desinfection-des-machines-dans-le-domaine-agroalimentaire-2014-0031>.
2. Commission de la santé et de la sécurité du travail. "Analyse détaillée – CNESST", *Principaux risques de lésion par secteur d'activité – Abattage des animaux*, 2014. [En ligne] http://www.CNESST.qc.ca/prevention/risques/pages/analyse_detaillee.aspx?SCIAN=311611&vue=PME
3. Commission de la santé et de la sécurité du travail. "Analyse détaillée – CNESST", *Principaux risques de lésion par secteur d'activité – Coupe et dépeçage de viandes incluant la fonte des graisses et la*

transformation, 2014. [En ligne].

http://www.CNESST.qc.ca/prevention/risques/pages/analysedetaillee.aspx?SCIAN=REG017&vue=ENSEMBLE_SECTEUR.

4. Caisse nationale de l'assurance maladie des travailleurs salariés, Risque AT 2014 : *statistiques de sinistralité du CTN D par code NAF - Services, commerces et industries de l'alimentation*, Étude 2015-149-CTN D, novembre 2015.
5. Organisation internationale de normalisation (ISO). " Safety of machinery — Hygiene requirements for the design of machinery", ISO, ISO 14159, 2002.
6. Association française de normalisation, "Food Processing Machinery – Basic concepts —Part 1: Safety requirements", AFNOR, NF EN 1672-1, 2016.
7. Association française de normalisation, "Food Processing Machinery – Basic concepts —Part 2: Hygiene requirements", AFNOR, NF EN 1672-2+A1, 2009.
8. Organisation internationale de normalisation (ISO). "Safety of machinery — Guards — General requirements for the design and construction of fixed and movable guards", ISO, ISO 14120, 2015.
9. Institut national de recherche et de sécurité. ED 6038, « Interventions sur un équipement de travail – Réflexions pour la sécurité lors des arrêts », Paris, INRS, 2008.

Safety functions in pneumatic drive technology

Uppenkamp J.

Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA)
Alte Heerstrasse 111
53757 Sankt Augustin – Germany

juergen.uppenkamp@dguv.de

KEYWORDS: pneumatic safety sub function, pneumatic drive technology, STO (safe torque off), VDMA specification 24584, fault detection

ABSTRACT

Like other forms of machine drive, pneumatic drives must not endanger persons by causing unexpected movement of machine parts. Standardized safety functions for electrical drive controls, which are defined in IEC 61800-5-2 [1], have become established on the market and can be regarded as the state of the art. Before now, these safety functions for electrical drives have not been "converted" for application to pneumatic drives, and manufacturers and institutional users have not therefore enjoyed the benefit of a "common language" for them. Implementing the safety functions familiar from electrical drive technology in pneumatics is generally more resource-intensive. This article compares selected electrical safety sub-functions set out in IEC 61800-5-2 with pneumatic safety sub-functions. A detailed example describes the procedure for implementing the typical safety sub-function of STO (safe torque off) on a pneumatic drive. This example particularly shows the possible faults and failures for the safety sub-function of STO, and provides information on fault detection.

1 INTRODUCTION

ISO 12100 [2] considers a safety function to be a function of the machine whose failure can result in an immediate increase of the risk, by which a higher probability may arise of a hazard to the machine operator. ISO 13849-1 [3], which addresses safe machine controls independently of the technology used, considers the concept of safety functions in greater depth. Safety functions specifically for electrical drive controls, which are defined in IEC 61800-5-2, are now well established on the market and can be regarded as the state of the art. The drive manufacturer often provides the control system manufacturer with safety sub-functions such as STO or SS1 (safe stop 1) with a Performance Level PL and a Category to ISO 13849-1.

The safety functions in the current edition of IEC 61800-5-2 are defined as safety sub-functions that the machine manufacturer or designer can integrate into the machine-specific safety functions.

2 SAFETY FUNCTIONS

2.1 Typical safety functions on a machine

Examples of typical safety functions are:

- Protection against unexpected start-up of a drive from the rest position with the safety guard open
- Stopping of a hazardous movement when a light curtain is penetrated

Implementing the safety functions familiar from electrical drive technology in pneumatics generally entails more effort. In conjunction with manufacturers of pneumatic components and the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA), the FuSi (functional safety) working group in the Fluid Power Association of the German Engineering Federation (VDMA) has drawn up a specification that transfers the concepts from electrical drive technology to the sphere of pneumatic drive technology and mechanics. VDMA specification 24584, "Safety functions of regulated and unregulated (fluid) mechanical systems" [4], has been available since 2016. The specification includes descriptions of safety sub-functions familiar from IEC 61800-5-2, but for mechanical and pneumatic systems.

2.2 Characteristics of safety functions

The safety sub-functions described in the specification can be divided into active and passive safety sub-functions. Active safety sub-functions act for example upon drives, which induce force, velocity, location or

acceleration, by the application or removal of pressure or flow (energy). A valve can admit, vent or shut off the energy for a drive. A passive safety sub-function has the purpose of monitoring the observance of limit values for variables such as pressure, flow rate or position of the drive. In this context, IEC 61800-5-2 distinguishes between stopping functions and monitoring functions, which may be of active or passive design.

A safety function as defined in the standards governing functional safety typically comprises the elements of sensor (detection of triggering events), logic (interpretation of the input signals, execution of logic operations and generation of output signals; if applicable, fault detection functions) and actuator (power control elements for switching of the drive). The logic may be implemented by pneumatic components alone or in the form of an electrical sequential control. Valves piloted electrically or pneumatically serve as the actuators. A comprehensive introduction to "Definition of the safety functions: what is important?" can also be found in SISTEMA Cookbook 6 [5].

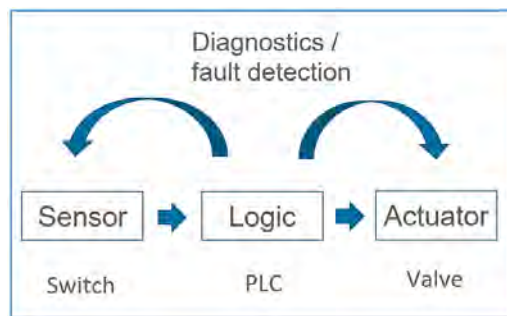


Figure 1. Elements of implementing a safety function.

2.3 Implementation of safety functions

In contrast to integrated electrical drive control systems, pneumatic control systems for the implementation of safety functions are frequently engineered using individual valves. Depending upon the control Category to ISO 13849-1, measures for fault detection may be required. The measures and processes required for fault detection must often also be integrated, developed separately, and implemented by the logic (hardware and associated software).

2.4 Description and selection of safety sub-functions

STO is one means of implementing the two typical safety functions described above. STO describes the safety sub-function of "safe torque off" for the power drive. On an electrical drive (electric motor), STO is initiated by disconnection of the electrical energy supply to the motor. On a pneumatic drive, STO is executed by venting of the piston chambers. For protection against unexpected start-up, this is generally easy to implement provided no external forces, caused for example by gravity, act upon the drive. If STO is also to be used to stop a movement, the overtravel occurring before the movement stops must be considered during the necessary risk assessment. If the overtravel is too great, SS1 or SS2 are alternative safety sub-functions (see Table 1). They are however not widely used in pneumatic control technology. In pneumatics, the SSC (safe stopping and closing) safety sub-function is suitable for rapid stopping.

Table 1 shows by way of example the possible implementation of individual safety sub-functions of IEC 61800-5-2 and the corresponding pneumatic safety sub-functions from the VDMA specification.

Table 1. Comparison of electrical and pneumatic safety sub-functions.

	Abbreviation	Possible implementation in accordance with:	
		IEC 61800-5-2	VDMA specification 24584
Safe torque off	STO	Disconnection of the supply of power to the power drive component (motor)	Venting of the piston chambers of the power drive component (cylinder)
Safe stop 1	SS1	Initiation of braking by pulse pattern and monitoring of the deceleration ramp by means of an angular or position measuring system, followed by STO	Implementation of the braking function for example by the use of valves to change the pressure in the power drive, followed by STO
Safe stop 2	SS2	Initiation of braking by pulse pattern and monitoring of the deceleration ramp by means of an angular or position measuring system, followed by SOS when the motor speed is below a specified limit	Implementation of the braking function for example by the use of proportional valves to change the pressure in the power drive, followed by SOS. Maintaining of the position in situations in which external forces act upon the power drive
Safe stopping and closing	SSC	---	By trapping of air in the piston chambers of the power drive (drive cylinder), without position monitoring and closed-loop position control
Safe operating stop	SOS	Monitoring and maintaining of the position in situations in which external forces act upon the power drive	
Safe cam	SCA	Monitoring whether the motor shaft is within a specified range	Safe position monitoring on the power drive (cylinder) with defined reaction in the event of departure from the position

In pneumatic drive technology, linear movements are encountered more frequently than rotary movements. On a drive installed horizontally and upon which no external forces act, STO is a suitable means of ensuring protection against unintended start-up or of stopping a movement. STO generally involves both piston chambers of the power drive being vented in order to prevent torque/force from continuing to act upon the drive.

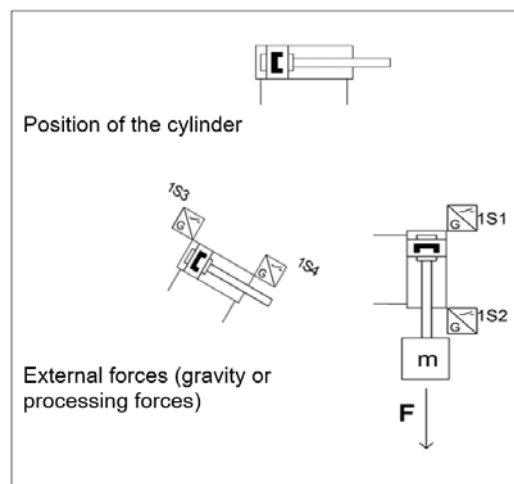


Figure 2. Cylinder orientation.

Conversely, a cylinder used in a vertical or inclined arrangement is always subject to external forces. These forces are generated by the weight of the piston rod and a load acting upon it. Should an STO be initiated during the movement by venting of both piston chambers, movement of the piston does not cease until the end position of the drive is reached, owing to the external forces. This could consequently present hazards to the operator, and is therefore not suitable in many applications. For such axes subject to the influence of gravity, the SSC (Safe

Stopping and Closing) safety sub-function is typically suitable for stopping. If the cylinder is already in the lower end position when the "protection against unexpected start-up" safety function is requested, an STO is able to implement this safety function. This requires reliable detection of the cylinder position. This is achieved by the SCA (safe cam) monitoring function, which can also be regarded as safe position monitoring.

3 EXAMPLE OF ELECTROPNEUMATIC CONTROL

An implementation of the STO safety sub-function, with possible faults and failures and their detection, is described in detail by way of example following.

3.1 Two-channel electropneumatic control for STO (Safe Torque Off)

On a cylinder arranged horizontally, the triggering of STO results in drive torque no longer being exerted upon the piston rod. Figure 3 shows a possible two-channel implementation in Category 3 to ISO 13849. Both piston chambers of the power drive (cylinder) must be reliably vented following a demand upon the STO safety sub-function, and the energy supply in the form of compressed air must be shut off. If STO is initiated during movement, overtravel occurs. On a cylinder not arranged horizontally, the drive does not stop until it reaches the lower end position, owing to the effect of gravity. Attainment of the end position can be queried by means of the SCA (Safe Cam, i.e. safe position monitoring) safety sub-function.

3.2 Functional description of the two-channel electropneumatic control for STO and SCA

Protection against unexpected start-up of a drive in either direction of the piston rod is implemented by means of the STO safety sub-function. If all the valves in Figure 3 are in the normal position, this ensures both redundant interruption of the energy supply (compressed air), and redundant venting of both piston chambers of the cylinder. STO can also be used to stop a hazardous movement when a possible overtravel would not be hazardous.

When the directional control valve 1V1 is in the spring-centred position, ports 2 and 4 are vented. The directional control valve 1V2 has the function of piloting the 3/2-way exhaust valves 1V3 and 1V4. The valves 1V3 and 1V4 must be engineered such that should the valve piston stick in any intermediate position, venting of port 2 to ports 1 and/or 3 is always ensured (underlap). When 1V3 and 1V4 are in the safety-related switching position (normal position), port 1 must always be reliably shut off (overlap).

Should an external force act upon the cylinder, for example because it is not situated horizontally, the SCA safety sub-function can be used to detect the extended end position of the piston rod redundantly by means of the two initiators 1S4 and 1S5. Once an extended end position has been detected by means of SCA, STO is executed.

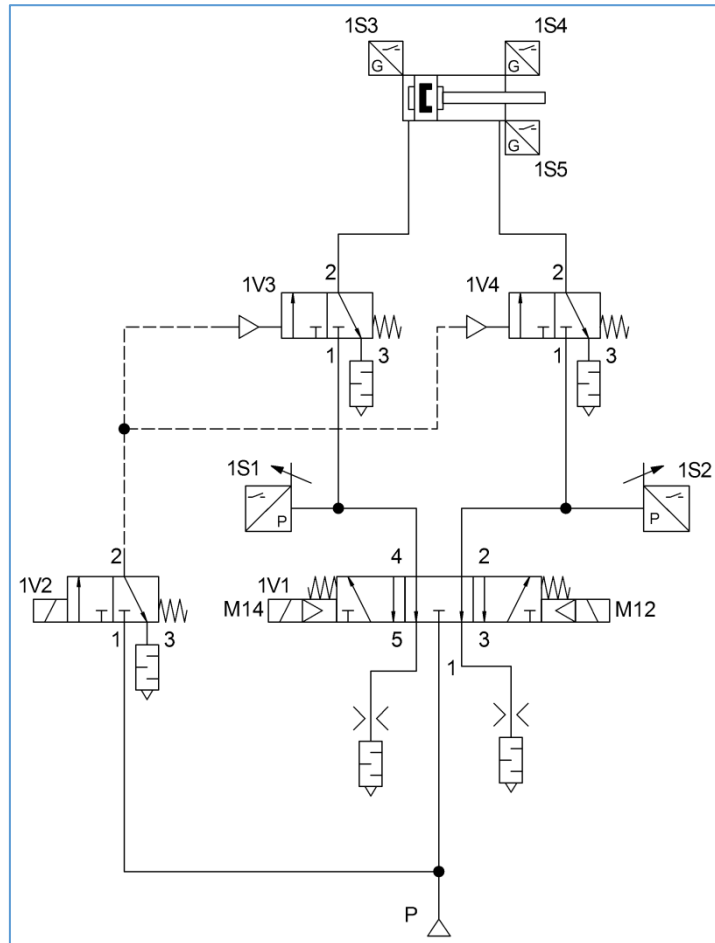


Figure 3. Example of a two-channel electro-pneumatic control for STO.

3.3 Safety-related block diagram for STO

In this circuit, a valve fault or failure does not lead to loss of the STO safety sub-function, since the circuit for venting and thus the STO is of redundant design. The safety-related block diagram shows the components of the pneumatic control involved in the STO safety sub-function. 1S1 to 1S4 are used solely for fault detection and are not involved in execution of the STO safety sub-function.

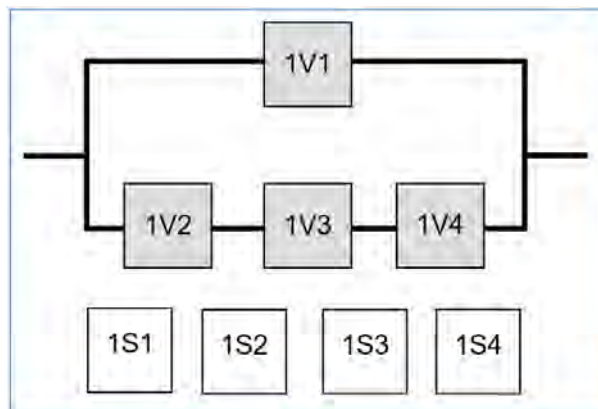


Figure 4. Safety-related block diagram for the example STO in Category 3.

For the SCA safety sub-function, the initiator 1S4 forms the first channel and 1S5 the second channel for the safety-related block diagram (not shown here).

3.4 Possible faults/failures

Measures for fault detection are required in order for the requirements of ISO 13849-1 for Category 3 to be satisfied. Where implementation is reasonably possible, a single fault must be detected at or prior to the next demand upon the safety function. For this purpose, **faults/failures** are assumed, and their impact upon the function of the cylinder is described in Table 2 below. The stationary position of standstill, in which all non-actuated valves are to remain in the normal position, and the stopping of a movement, in which the valves are to switch from the actuated position to the normal position when actuation ceases, are considered here.

Table 2. Possible faults/failures for the example of STO.

Operational situation	Fault assumption	Effect
Standstill	Switching of <u>one</u> of the valves from the normal to the actuated position	Owing to the redundant venting the piston chambers remain depressurized and a hazardous movement does not occur
	Internal leakage between the ports of <u>one</u> valve	
Stopping	Failure of 1V1 to switch back	Piston chambers vented via 1V3 and 1V4, the movement runs down
	Failure of 1V1 to switch back fully/sticking in an intermediate position	
	Failure of 1V2 to switch back	Piston chambers vented via 1V1, the movement runs down
	Failure of 1V2 to switch back fully/sticking in an intermediate position	
	Failure of 1V3 to switch back	Piston chambers vented via 1V4 and 1V1, the movement runs down
	Failure of 1V3 to switch back fully/sticking in an intermediate position (with underlap)	
	Failure of 1V4 to switch back	Piston chambers vented via 1V3 and 1V1, the movement runs down
	Failure of 1V4 to switch back fully/sticking in an intermediate position (with underlap)	

A range of solutions for fault-detection measures are available by which the assumed faults in the second column of the table are detected.

3.5 Fault-detection measures

Fault detection can be achieved for example by means of valves with direct position monitoring. During the operating cycle, the electrical control system performs a plausibility check between operation of the valves and the signal from the valves' position monitor. Should the electrical control system detect implausibility, continued operation of the machine must be prevented until the fault has been cleared.

When valves without position monitoring are used, the switching behaviour of 1V1 in the operating cycle can be used in conjunction with the pressure switches 1S1 and 1S2 for diagnostics. For this purpose, the pressure switches signal the safety-related centre position (normal position) of the valve 1V1 when it is not actuated. A test algorithm can be implemented for the valves 1V2 to 1V4 by means of the electrical control system. This enables faults on the valves to be detected in conjunction with the cylinder position sensors 1S3 and 1S4. Figure 5 uses a flow chart to describe an example test algorithm that indicates whether the valves 1V2 and 1V3 have assumed the normal position. In a similar way, testing is possible for whether the valve 1V4 has assumed the normal position.

Note:

The operating personnel must not be placed in danger whilst the test algorithm is running. The correct initial states of the pressure switches and initiators is queried at the start of the function test for 1V2 and 1V3. If 1S3 = 0 is also queried during the operating cycle, failure of 1S3 can be detected, which however is not among the requirements for the Category.

The measures for fault detection describe a diagnostic coverage (DC) for the relevant components in accordance with ISO 13849-1. If assumption of the centre position by 1V1 is checked in the operating cycle, this indirect monitoring yields a DC of 99% for 1V1. If the valves 1V2 to 1V4 are checked for example every eight hours by means of the fault detection described here, the indirect monitoring yields a DC of 90% (conservative estimate)

for each valve.

The function check of the initiators for the SCA safety sub-function, for detection of the extended end position, is performed cyclically by indirect monitoring comprising a plausibility check with comparison (signal change at attainment of and departure from the end position), which yields a DC of 99% for 1S4 and 1S5.

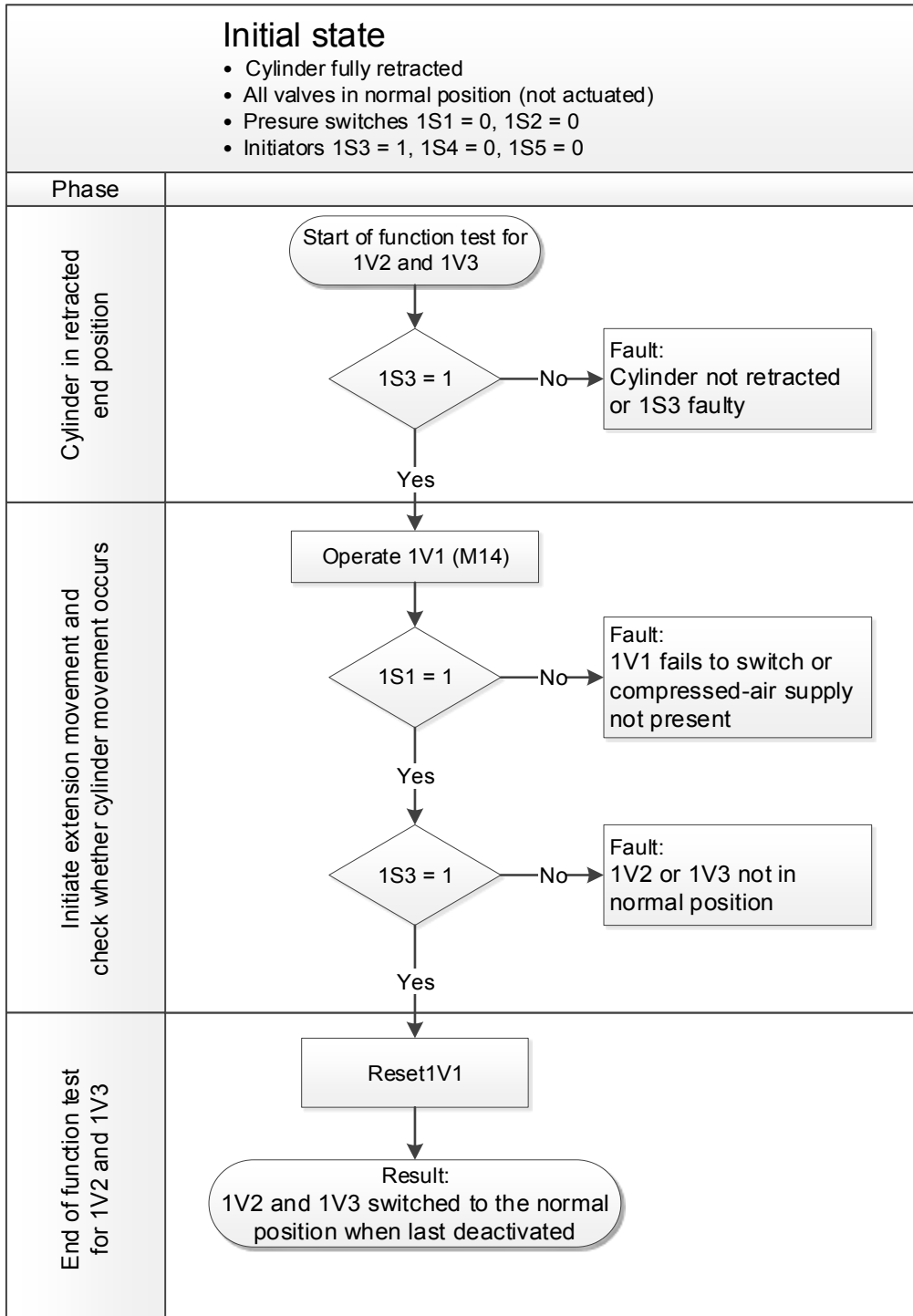


Figure 5. Flow chart for fault detection on valves for the example of STO.

3.6 Design features for the circuit

- Basic and well-tried safety principles to ISO 13849-2 [6] and the requirements of Category B are met for all components.
- The directional control valve 1V1 has a vented centre position with sufficient overlap and spring-centering. The directional control valve with spring-return 1V2 has sufficient overlap in the normal position.
- The valves 1V3 and 1V4 have sufficient overlap in the normal position and are not free of overlap (do not have underlap) in the intermediate position.
- Cessation of actuation causes the valves to adopt the safety-related switching position from any position.
- A stable arrangement for actuation of the initiators, which may take the form of cylinder position sensors, position switches or proximity switches, is ensured. The switching point and the hysteresis are selected such that departure from the end position of the cylinder is detected.
- The pneumatic switching point of the pressure switches, which leads to switching over of the electrical output signal, is selected such that the safety-related switching position (ports 2 and 4 vented) is detected by 1V1.
- The signals from the pressure switches and initiators are processed (for example) in relay logic/a PLC, or in a safety PLC in the case of the SCA safety sub-function. The requirements of ISO 13849-1 concerning safety-related software are met for the required PL.

3.7 Calculation of the probability of failure

With normal $MTTF_D$ and B_{10D} values, the diagnostic coverage values already described, observance of the basic and well-tried safety principles, and adequate measures against common-cause failure (CCF), the circuit satisfies as minimum Category 3. The IFA's SISTEMA [7] software application can be used to determine the probability of dangerous failure (PFH_D), as required by ISO 13849-1. The number of operations per year (n_{op}) of the components is also required for this purpose.

4 CONCLUSIONS

The article shows that the safety sub-functions described in the VDMA specification, which are already widely used in electrical drive technology, are now also described for pneumatic drive technology. The standardization and clarification of the requirements and descriptions that has been achieved by the specification makes the association between the required risk reduction on the machine and the performance criteria of the pneumatic control system employed more transparent. This is ultimately advantageous for occupational safety and health, as well as for the manufacturers and operators. The specification is undergoing further development with the inclusion of hydraulic control systems. Further information on the use of fluid power technology in safety technology can be found on the IFA's web page providing practical assistance with hydraulics and pneumatics at: <https://www.dguv.de/webcode/d1029520>. With reference to a further comprehensive example, this page shows how SSC can be used to place pneumatic drives in a safe state.

5 REFERENCES

1. IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional, (2016-04).
2. ISO 12100, Safety of machinery – General principles for design – Risk assessment and risk reduction, (2010-11).
3. ISO 13849-1, Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design, (2015-12).
4. VDMA specification 24584, Safety functions of regulated and unregulated (fluid) mechanical systems, Beuth, Berlin 2016.
5. Apfeld, R.; Hauke, M.; Otto, S.: The SISTEMA Cookbook 6. Definitions of safety functions: What is important? Published by: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin 2015, <https://www.dguv.de/webcode/e109249>
6. ISO 13849-2, Safety of machinery – Safety-related parts of control systems – Part 2: Validation, (2012-10).
7. SISTEMA download free of charge from: <https://www.dguv.de/webcode/e34183>

A Proposal to Solve Technical Issues on ISO 13855 – Positioning of Safeguards –

Saito T., Ikeda H.

National Institute of Occupational Safety and Health, Japan (JNIOSH) – 1-4-6 Umezono, Kiyose, Tokyo – 204-0024 – Japan

saitot@s.jniosh.johas.go.jp

ikeda@s.jniosh.johas.go.jp

KEYWORDS: international standard, ISO 13855, minimum distance, safeguard

ABSTRACT

ISO 13855 is a generic safety standard providing a basic methodology for determining the minimum distance to a hazard zone from a detection zone or an actuating device of safeguards. Formulas and parameters specified in this standard has been referred to in the requirements of many machine safety standards. However, the current ISO 13855 includes some technical ambiguities and discrepancies that could cause confusion for users of the standard. In this paper, four issues considered to be particularly significant are described: (1) ambiguousness of the direction of the minimum distance for the detection zone of electro-sensitive protective equipment (ESPE) angled to the direction of approach; (2) insufficiency of the intrusion distance applied to the detection zone of ESPE parallel to the approach; (3) a lower limit on the minimum distances for the detection zone of ESPE orthogonal to the approach and two-hand control devices; (4) insufficient explanation for the calculation procedure of the minimum distance for interlocking guards without guard locking. Then, modifications to solve them without largely changing the existing technical concept underlying ISO 13855 are proposed concretely. Our proposal is greatly expected to be considered and discussed in the next revision as it enhances the value and importance of ISO 13855.

1 INTRODUCTION

The effectiveness of certain types of safeguard to provide a trip function, such as light curtains and interlocking guards without guard locking, relies in part on appropriate positioning of the detection zone or the actuating device of safeguards in relation to an identified hazard zone. Because, in order to achieve the intended risk reduction, it is necessary to countervail the time required for the trip function to ensure safe condition of the machine and any intrusion by a part of the human body due to structural constraints on the used safeguard. In deciding on their positions adequately, ISO 13855 [1] is referred. It is a type-B1 standard providing a basic methodology for determining the minimum distance [1] and specifying key parameters based on approach speeds or dimensions of parts of the human body that are used in the calculations of minimum distances. The first edition of ISO 13855 was issued in 2002 based on EN 999. Afterward, its revision was decided through practical use experiences and its second edition was published in 2010 after about 5 years of deliberation. This revision added many new requirements including prevention of circumventing by reaching over the detection zone of vertically mounted electro-sensitive protective equipment (ESPE) and the minimum distance between the access point of interlocking guard without guard locking and the hazard zone.

However, the second edition of ISO 13855 includes some technical ambiguities and discrepancies that could cause confusion for the users of the standard. For example, regarding the detection zone of ESPE installed parallelly to the direction of approach of a person, it is stated in Subclause 6.3 that “when using the equipment as both a trip and presence sensing device, the distance between the end of the detection zone and the hazard zone shall not be less than the detection capability [1] of the equipment”, but this is technically incorrect. This paper points out four technical issues considered to be particularly significant and proposes concrete modifications to solve them.

2 TECHNICAL ISSUES IN ISO 13855

2.1 Direction of the minimum distance for angled detection zone

When a detection zone of ESPE using active optoelectronic protective devices (AOPDs) or active optoelectronic protective devices responsive to diffuse reflection that has a detection zone specified in two dimensions (AOPDDR-2D) is installed such that it is angled greater than 30° of the direction of approach of a person, it is

treated as the detection zone orthogonal to the approach. However, there is a discrepancy between the minimum distances for the angled detection zone described in ISO 13855 and IEC 62046 [2], which provides requirements and information on the application of protective equipment employing sensing devices. Figures 1(a) and 1(b) are explanatory drawings in ISO 13855 and IEC 62046 for the minimum distance in this case, respectively. In ISO 13855, the minimum distance is specified as a distance parallel to the direction of approach, regardless of the install angle of the light curtain. However, in IEC 62046, the minimum distance is explained as a distance perpendicular to the surface of the detection zone (plane) without considering the direction of approach.

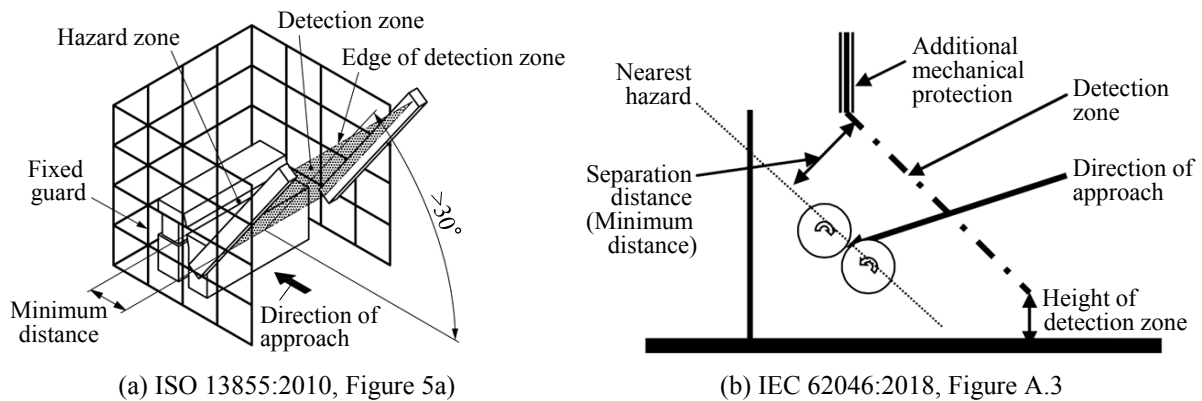


Figure 1. Explanatory drawings from ISO 13855 and IEC 62046 indicating the minimum distance for the angled detection zone which is treated as orthogonal to the direction of approach.

Using an example where an in-running nip created by a pair of counter-rotating rolls is identified as the hazard zone, the difference between the minimum distances in accordance with ISO 13855 and IEC 62046 is more clearly shown as Figure 2. The reason for this discordance is considered that the direction of the minimum distance is not adequately defined in both standards.

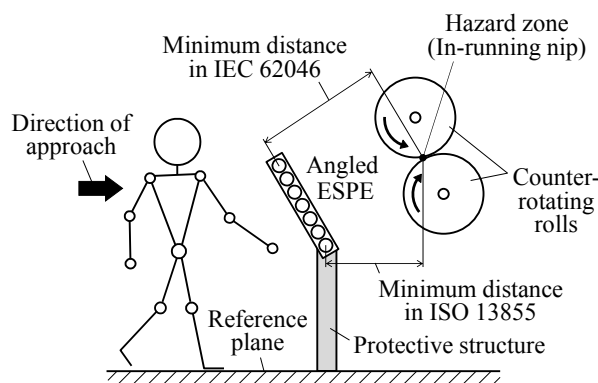


Figure 2. Minimum distances for the angled detection zone of ESPE in accordance with ISO 13855 and IEC 62046.

2.2 Intrusion distance for the detection zone parallel to the approach

Regarding the detection zone of an ESPE using AOPDs or AOPDDR-2D installed parallelly to the direction of approach, the intrusion distance [1] to be included in the minimum distance is given by Equation (7) of ISO 13855. If the height of the parallel detection zone above the reference plane is lower than 875 mm, then the intrusion distance varies depending on the height (as calculated by $1200 \text{ mm} - 0,4 \times H$, where H is the height in millimetres) and it is specified as 850 mm when the height is between 875 mm and 1000 mm because no intrusion distance less than 850 mm is permitted for the parallelly installed detection zone.

However, according to the values in Table 1 of ISO 13855, depending on the height of the hazard zone, there are some cases that the intrusion distance for prevention of access to the hazard zone by reaching over the detection zone of vertically mounted ESPE with the upper edge height between 900 mm and 1000 mm need to be longer than 850 mm. For example, the height of the hazard zone from the reference plane is assumed to be 1000 mm as shown in Figure 3. In a case that a light curtain is used to provide a detection zone orthogonal to the direction of approach (i.e., orthogonal approach) as shown in Figure 3(a), if the upper edge height of the detection zone is 900 mm, then the intrusion distance for prevention of circumventing by reaching over the orthogonal detection

zone needs to be 1200 mm according to Table 1. However, when the light curtain provides a detection zone parallel to the approach (i.e., parallel approach) at the same height as shown in Figure 3(b), the intrusion distance is specified as 850mm according to Equation (7). Similarly, when the height of both the hazard zone and the upper edge of the detection zone are 1000 mm, the intrusion distance for the orthogonal approach needs to be 1150 mm according to Table 1, but the intrusion distance according to Equation (7) is 850mm, equivalent to the previous example. These indicate that the intrusion distance specified in Equation (7) for the parallel detection zone might be insufficient to prevent the detection zone from being circumvented.

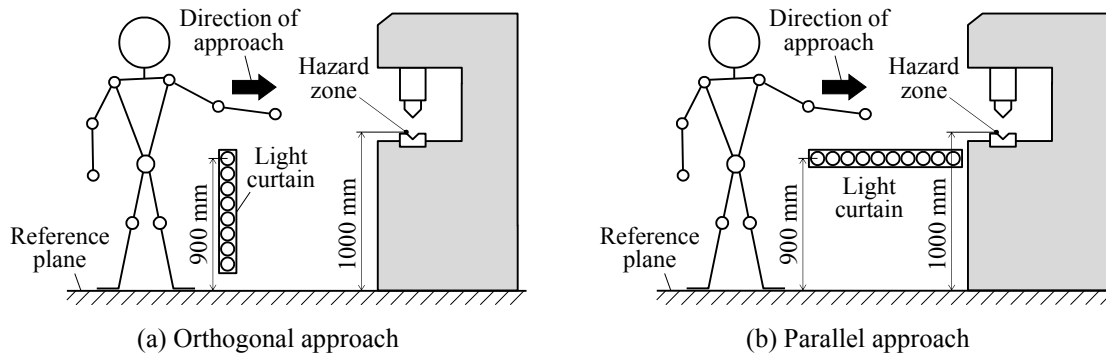


Figure 3. Application examples of ESPE mounted vertically and horizontally to the direction of approach.

2.3 Lower limit on the minimum distance

When a detection zone orthogonal to the direction of approach is provided by using an ESPE with a detection capability of 40 mm or less in diameter, the minimum distance is first calculated using Equation (3) of ISO 13855. However, there is a requirement that the minimum distance must be longer than 100 mm regardless of how small the parameters are (e.g., machine stopping time, system response time and the detection capability). This requirement is also imposed on two-hand control devices, especially those are designed so that the intrusion distance can be zero, i.e., the risk that the hazard zone can be reached by part of the hands while actuators of the device are being operated is adequately reduced, for example by shrouding.

As an example, assuming a light curtain with a detection capability of 14 mm is used to provide an orthogonal detection zone, if the overall system stopping performance [1] is determined to be 45 ms, then the minimum distance is calculated as 90 mm by using Equation (3). This result seems effective and any reason to increase the minimum distance to 100 mm cannot be found easily.

2.4 Reduction of overall system stopping performance of the interlocking guard without guard locking by its opening time

In the revision in 2010, the minimum distance for interlocking guards without guard locking was newly prescribed to ensure that the hazard zone cannot be reached before the termination of the hazardous machine function when the guard is opened. Also, in the minimum distance calculation under certain conditions (e.g., a power-operated guard which opens at a constant speed), it was allowed to reduce the overall system stopping performance by the opening time required for the guard to open to the extent that its opening size permits access of the relevant part of the human body.

However, any procedure of calculation taking into account this reduction is not explained concretely. In particular, although it is stated in Clause 9 of ISO 13855 that “the calculation shall start with the smallest part of the body that can reach the hazard zone in accordance with ISO 13857 [3]”, it is not always simple because the safety distances given in Tables 4 and 5 of ISO 13857 are discontinuous and no interpolation is permitted.

3 PROPOSAL TO RESOLVE THE DESCRIBED ISSUES

3.1 Definition of direction of the minimum distance

In order to eliminate the ambiguousness of the minimum distance for the angled detection zone of ESPE treated as orthogonal to the approach, we propose to modify the definition 3.1.9 “Minimum distance” so that its direction is expressly defined in relation to the direction of approach, as follows:

Definition 3.1.9 “Minimum distance S ”

calculated distance between the safeguard and the hazard zone in the direction of approach, which is necessary to prevent a person or part of a person reaching the hazard zone before the termination of the hazardous machine function

This modification is to insert the underlined words in the current definition and intended to address each minimum distance as a distance along the direction of approach. It also places the importance on maintaining the existing technical concept underlying ISO 13855 in which the approaches of persons are distinguished between orthogonal and parallel to the detection zone in order to let the equations and requirements provided in this standard remain functioning for the positioning of various safeguards.

Following the proposed definition, it is necessary to begin the procedure to determine the minimum distance by specifying the direction of approach. In practice, since different approaches may be foreseen by the risk assessment, different minimum distances would need to be calculated, and then the longest one would be adopted.

3.2 Clarification of restriction on the minimum distance calculated using Equation (7)

For all detection zones, it is indispensable to consider the prevention of circumvention. However, Table 1 of ISO 13855 cannot be simply applied to the parallel detection zones because values for those at heights below 900 mm are not provided. Actually, the values in Table 1 were obtained from experimental measurement using a light curtain mounted vertically on the floor [4] and intended to be applied to the detection zones of vertical ESPE as mentioned in its title.

It is desirable that values to prevent reaching over the parallel detection zones, especially for heights below 900 mm, should be specified based on ergonomic measurements, but it is difficult to accomplish in a short period. Therefore, as a practical alternative until appropriate values are obtained, we propose to clearly express that there is a restriction on the minimum distances calculated using Equation (7) of ISO 13855 that the distances cover only the access of persons who approach on foot with an upright attitude. Consequently, the implementation of risk assessment is always required to confirm the sufficiency of the calculated minimum distance for prevention of circumventing (reaching over) the detection zone. The concrete modification we propose is to add the following requirement and note after Equation (7):

$$S = (1600 \times T) + (1200 - 0,4 H) \tag{7}$$

The minimum distance S calculated using Equation (7) covers only access by persons who approach while walking upright. Therefore, the possibility of access to the hazard zone by circumventing the detection zone shall be taken into account in the risk assessment and additional protective measures applied if necessary.

NOTE Where the height of the edge of the detection zone furthest from the hazard zone is between 900 mm and 1000 mm, the values C_{RO} in Table 1 for prevention of reaching over the vertically installed detection zone may be referred for the risk assessment.

3.3 Removal of the lower limit on the minimum distance

The lower limit of 100 mm on the minimum distances for ESPE providing the orthogonal detection zone and two-hand control devices has been required since the first edition of ISO 13855, however, its purpose or reason was not mentioned. Although any operational problem caused by the lower limit still has not been known at present, it could become a constraint when applying such protective devices to various machines, e.g., small-sized machines having a short stopping time and machines controlling their working speed according to the distance to operator. Therefore, we propose to reconsider the lower limit and at least change to a recommendation.

3.4 Addition of calculation example of the minimum distance for the interlocking guard without guard locking

When the reduction of the overall system stopping performance by the opening time of interlocking guard is taken into account, the minimum distance calculation needs to be done iteratively for each opening size according to the order listed in Table 4 or 5 of ISO 13857, and then the most appropriate distance needs to be selected by comparing the results. In order to clearly show this calculation procedure in the standard, we propose to add the following example for a power-operated guard with a constant opening speed as an annex:

Annex XX (informative)

Calculation example of power-operated interlocking guard with constant opening speed

Calculate the minimum distance S for a power-operated interlocking guard without guard locking.

It is assumed that the overall system stopping performance T is determined to be 1 s, the power-operated guard opens with a constant speed v of 30mm/s, the values in ISO 13857:2008, Table 4 are applied as the safety distance for industrial applications, and no intrusion prior to the actuation of the interlocking device (i.e. while the guard is in closed position) is foreseeable.

If the overall system stopping performance T is not reduced by the opening time t_3 of the power-operated guard, the minimum distance S is calculated using Equation (2):

$$S = K \times T + C$$

where K is approach speed (= 1600 mm/s) and C is a safety distance (= 0 in this case). Then

$$S = 1600 \times 1 + 0 = 1600 \text{ mm}$$

Meanwhile, if T is reduced by t_3 , the calculation needs to be started with the smallest opening size e in ISO 13857:2008, Table 4, i.e., $e = 4$ mm. According to Equation (17), the opening time t_3 required to open the guard to 4 mm is calculated as (the values after the decimal point are rounded down):

$$t_3 = e / v = 4 / 30 = 0,133 \text{ s}$$

therefore the reduced overall system stopping performance T_{RE} is:

$$T_{RE} = T - t_3 = 0,867 \text{ s}$$

and the safety distance S_r for the slot opening of 4 mm to be added as C is 2 mm according to ISO 13857:2008, Table 4. Then

$$S = 1600 \times T_{RE} + C = 1600 \times 0,867 + 2 = 1389,2 \text{ mm}$$

The next smallest slot opening size e in ISO 13857:2008, Table 4 is 6 mm and the safety distance added as C is 10 mm. By the same procedure, the opening time t_3 and the minimum distance S are calculated as:

$$t_3 = e / v = 6 / 30 = 0,2 \text{ s}$$

$$S = 1600 \times (1 - 0,2) + 10 = 1290 \text{ mm}$$

Table XX.1 shows the opening times, the reduced overall system stopping performances and the minimum distances for other slot opening sizes calculated by the same procedure. By comparing the calculated minimum distances, the shortest one of 655 mm can be adopted as the minimum distance S for the power-operated interlocking guard unless it is less than the horizontal safety distance c determined from ISO 13857 to prevent access to the hazard zone by reaching over the guard. By taking the opening time t_3 into consideration, the minimum distance S is reduced by 945 mm in comparison with the case of simply applying the overall system stopping performance T of 1 s.

Table XX.1 - Minimum distances calculated with the reduced overall system stopping performance

Opening e	Opening time t_3^a	$T_{RE} = T - t_3$	Safety distance S_r^b	Minimum distance S^c
4 mm	133 ms	867 ms	2 mm	1390 mm
6 mm	200 ms	800 ms	10 mm	1290 mm
8 mm	266 ms	734 ms	20 mm	1195 mm
10 mm	333 ms	667 ms	80 mm	1148 mm
12 mm	400 ms	600 ms	100 mm	1060 mm
20 mm	666 ms	334 ms	120 mm	655 mm
30 mm	1000 ms	0 ms	850 mm	850 mm

^a Values after the decimal point are rounded down.

^b The safety distances are for slot openings given in ISO 13857:2008, Table 4.

^c Values after the decimal point are rounded up.

4 CONCLUSION

The methodology, formulas and parameters provided in ISO 13855 are normatively referenced in many type-C standards, however, the value of this standard can be more enhanced by appropriate modifications to clarify and correct technical ambiguities and discrepancies that could hinder its proper utilization. This paper pointed out the four issues which particularly need to be reviewed and proposed the modifications to solve them as follows:

- The direction of the minimum distance needs to be defined in relation to the direction of approach in order to eliminate the ambiguousness of the minimum distance for the angled detection zone;
- The restriction on the minimum distance calculated using Equation (7) needs to be clearly stated in order to warn of the insufficiency of the intrusion distance for detection zone parallel the approach;
- The purpose or the reason why the minimum distances for ESPE providing the orthogonal detection zone and two-hand control devices are required to be 100 mm or more should be elucidated and reconsidered if necessary;
- Examples to demonstrate the calculation procedure of the minimum distance for the interlocking guard considering the reduction of overall system stopping time should be added as an annex.

As the applying range of safety functions to detect the approach of persons or parts of the human body are expanding and protective devices based on new sensing technologies are actively developed, the role of type-B1 standard dealing with general requirements for the positioning of safeguards becomes increasingly important. Our proposal is greatly expected to be considered and discussed in the next revision of ISO 13855.

5 REFERENCES

1. *ISO 13855 Safety of machinery - Positioning of safeguards with respect to the approach speeds of parts of the human body (Second edition)*, International Organization for Standardization, Geneva, 2010.
2. *IEC 62046 (ed.1.0) Safety of machinery - Application of protective equipment to detect the presence of persons*, International Electrotechnical Commission, Geneva, 2018.
3. *ISO 13857 Safety of machinery - Safety distances to prevent hazard zones being reached by upper and lower limbs (First edition)*, International Organization for Standardization, Geneva, 2008.
4. BGM expert committee “Mechanical engineering, manufacturing systems, steel construction” (Fachausschuss Maschinenbau Fertigungssysteme Stahlbau), *Test description - Reaching over opto-electronic protective devices and indirect approach to points of hazard over obstacles with the whole body* -, Berufsgenossenschaft Metall Nord Süd, Mainz, 2008, pp. 5-6.

Online Human Activity Recognition for Ergonomics Assessment

Adrien Malaise, Pauline Maurice, Francis Colas and Serena Ivaldi

Universite de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France

adrien.malaise@inria.fr

We address the problem of recognizing the current activity performed by a human worker, providing an information useful for automatic ergonomic evaluation of workstations for industrial applications. Traditional ergonomic assessment methods rely on pen-and-paper worksheet, such as the Ergonomic Assessment Worksheet (EAWS). Nowadays, there exists no tool to automatically estimate the ergonomics score from sensors (external cameras or wearable sensors).

As the ergonomic evaluation depends of the activity that is being performed, the first step towards a fully automatic ergonomic assessment is to automatically identify the different activities within an industrial task. To address this problem, we propose a method based on wearable sensors and supervised learning based on Hidden Markov Model (HMM). The activity recognition module works in two steps. First, the parameters of the model are learned offline from observation based on both sensors, then in a second stage, the model can be used to recognize the activity offline and online.

We apply our method to recognize the current activity of a worker during a series of tasks typical of the manufacturing industry. We recorded 6 participants performing a sequence of tasks using wearable sensors. Two systems were used: the MVN Link suit from Xsens and the e-glove from Emphasis Telematics (See Fig. 1). The first consists of 17 wireless inertial sensors embedded in a lycra suit, and is used to track the whole-body motion. The second is a glove that includes pressure sensors on fingertips, and finger flexion sensors. The motion capture data are combined with the one from the glove and fed to our activity recognition model.

The tasks were designed to involve elements of EAWS such as load handling, screwing and manipulating objects while in different static postures. The data are labeled following the EAWS categories such as "standing bent forward", "overhead work" or "kneeling".

In terms of performances, the model is able to recognize the activities related to EAWS with 91% of precision by using a small subset of features such as the vertical position of the center of mass, the velocity of the center of mass and the angle of the L5S1 joint. We presented this work at ACHI 2018 (The Eleventh International Conference on Advances in Computer-Human Interactions).



Figure 1. Wearable sensors used in the experiment: (a) Xsens MVN suit; (b) e-glove from Emphasis Telematics.

REFERENCES

- [1] E. Schneider, X. Irastorza, M. Bakhuis Roozeboom, and I. Houtman, "Osh in figures: occupational safety and health in the transport sectoran overview", 2010.
- [2] G. Li and P. Buckle, "Current techniques for assessing physical exposure to work-related musculoskeletal risks, with emphasis on posture-based methods," *Ergonomics*, vol. 42, no. 5, pp. 674-695, 1999.
- [3] S. Ivaldi, L. Fritzsche, J. Babic, F. Stulp, M. Damsgaard, B. Graimann, G. Bellusci, and F. Nori, "Anticipatory models of human movements and dynamics: the roadmap of the andy project," in *Proc. International Conf. on Digital Human Models (DHM)*, 2017.
- [4] T. Bossomaier, A. G. Bruzzone, A. Cimino, F. Longo, and G. Mirabelli, "Scientific approaches for the industrial workstations ergonomic design: A review." in *ECMS*, 2010, pp. 189-199.
- [5] "e-glove - Emphasis Telematics," URL: <http://www.emphasisnet.gr/eglove/> [accessed: 2018-04-12-].
- [6] A. Bulling, U. Blanke and B. Schiele, "A tutorial on human activity recognition using body-worn inertial sensors". *ACM Computing Surveys (CSUR)*, 46(3), 33, 2014.
- [7] O. D. Lara and M. A. Labrador, "A Survey on Human Activity Recognition using Wearable Sensors", *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, 2013.
- [8] A. Malais, P. Maurice, F. Colas, F. Charpillat, S. Ivaldi, "Activity Recognition With Multiple Wearable Sensors for Industrial Applications", *Advances in Computer-Human Interactions*, Mar 2018, Rome, Italy. 2018.

Assessing and improving human movements using sensitivity analysis and digital human simulation

Pauline Maurice, Vincent Padois, Yvan Measson, Philippe Bidaud

Introduction

Enhancing the performance of technical postures or movements at work, in sports or in rehabilitation is of great concern for humans, and aims both at improving operational results and at reducing biomechanical demands on the body. Advances in human biomechanics and modeling tools allow to evaluate human performance with more and more details using digital human models [1]. However, the reliability of these force-related biomechanical measurements is questionable because most mappings of motion capture data onto a digital model do not ensure the dynamic consistency of the resulting motion [2]. Then, once an existing movement is evaluated, finding the right modifications to improve the performance is still addressed with extensive trial-and-error processes.

Methods

We propose a framework to easily and reliably assess the performance of a technical movement, and automatically provide recommendations to improve its performance. An optimization-based whole-body controller is used to track motion capture data in operational space while imposing dynamic and biomechanical constraints. Existing movements can thus be evaluated. Our method guarantees the dynamic consistency of the resulting motion (*i.e.* that the motion and force respect the laws of physics), without requiring the ground reaction force (GRF) measurement as an input. Digital human simulations are then automatically created and run (without motion capture) to estimate the performance when the movement is performed in many alternative ways. Sensitivity indices are thereby computed to quantify the influence of postural parameters on the performance. Critical parameters can thus be identified and tuned, using only little input data. Based on these results, recommendations for posture improvement are provided.

Results

The proposed method was validated on a drilling activity. 5 participants performed 10 trials of a drilling movement while their motion, drilling force and GRF were recorded. The tacking error of the replayed motion was smaller than 3 cm and the 6 components of the GRF computed in simulation closely matched their experimental counterparts (Pearson's correlation coefficient between 0.72 and 0.98).

9 postural parameters were varied to create 11601 different simulations of the drilling movement. The sensitivity analysis identified 3 parameters as crucial for the performance, and determined their optimal values. Compared to the original movement, the optimized movement significantly improved 5 performance indicators out of 6, while 1 was only slightly worsened.

Discussion

The good match between the experimental and replayed motion and GRF confirms the relevance of the dynamic replay method. Moreover, the significant increase in performance of the optimized movement shows the usefulness of the digital human simulation-based sensitivity analysis for quickly and easily identifying ways to improve a technical movement.

References

1. Demircan, E., *et al.* (2009), *Engineering in Medicine and Biology Society* p6534
2. Hicks J., *et al.*, (2015), *Journal of biomechanical engineering* 137(2)

Implementation, risk assessment and safety human/robot interaction of collaborative robot UR10

Menges B.^{1,2}, Sarrey M.¹, Henaff P.²

¹ Saint-Gobain PAM, Technocentre, Les Longues Raies, BP 109, 54704 PONT.A.MOUSSON Cedex, France

² Université de Lorraine, CNRS, LORIA, F-54000 Nancy, France

baptiste.menges@saint-gobain.com
Michael.SM.Sarrey@saint-gobain.com
patrick.henaff@loria.fr

Keywords: Collaborative robotic, human/robot interaction, industrial integration, function safety

Collaborative robotics is an increasingly emerging subject in industrial environments. This presentation concerns the integration of a collaborative robot (cobot) in a very hard steel environment, that very uncommon integration.

Saint-Gobain products ductile iron pipes for water conveyance by centrifugation process with a casting machine. Dust, high temperature, vibrations and high noise level are conditions qualifying this kind of the steel production environment that the robot must undergo to perform its tasks and helping the human operator.

In France, to integrate a cobot, we have no national recommendation, so it's necessary to refer to the European conformity (CE) and on the currently standards (ISO 10218:1 and ISO 15066) during the development, for setting the security laws (power and speed) and the other safety options.

The aim of the presented project is to reduce the musculoskeletal disorders of the operator by assigning to the cobot the tasks requiring strength, precision and repetition, and to free up more time for the operator to quality control and his added values.

Through the risks assessment, hazardous situations were evaluated and some safety adaptations were developed and added on the installation, especially about the cobot gripper with the INRS (French national institute of safety at work).

Owing to environment, some mechanical and workspace adaptations had to be integrated like fireproof cover to protect the cobot against the liquid iron splash and a ventilation to blown a fresh air inside the cover to protect the cobot motors against the heat sources of the plants.

First results are encouraging, the cobot working in the plant with the operator for 15 months (with several stops). Operators are enthusiasm to have a robot that help them and are delighted to participate to the integration of new technologies into "their old plant". Collaborative robot brings them ergonomic benefits, many risked postures of musculoskeletal disorders (MSD) are avoided.

Second main result is that fears of operators do not come from the collaborative robot but rather to work closer to the casting machine with hot ductile iron.

Despite a low maturity of human/robot collaboration in industrial applications in a hard environment, the final integration is successful, with several difficulties of integration (heat, conformity). Skills and experiences have been won through this project and it's a good step for the collaborative robotics.

Challenges of measuring physiological parameters as indicators of cognitive load in the context of human-machine interfaces

Żołnierczyk-Zreda D., Mockało Z., Nowak K., Szczepański G., Podgórski D. Bugajska J.¹, Czerniak-Wilmes J.²

¹ Central Institute for Labour Protection – National Research Institute (CIOP-PIB) – Poland

² Rheinisch-Westfälische Technische Hochschule Aachen (RWTHA) – Germany

dozol@ciop.pl

KEYWORDS: human-machine interface, physiological measurements, cognitive load, human factors

ABSTRACT

The rapid development of modern technologies allows for the improvement of the efficiency and speed in the production of high-quality products. High level of automation in manufacturing increased the productivity, however, the operation of modern machines often requires many complex activities for an efficient interaction with the interface. This results in a high cognitive demand, especially in relation to elderly, inexperienced or disabled operators. This may influence not only the worker efficiency but also health and well-being of employees. The aim of the INCLUSIVE project is to address this issue by developing a new concept of user-machine interactions, in which the behaviour of the automated systems adapts to human capabilities. The present study focused on the possibility of the assessment of cognitive load using various subjective (NASA-TLX scale), behavioural (error rate) and physiological measurements (heart rate, electrodermal activity, skin, temperature, electroencephalography). The task carried out in this study required solving mathematical problems at 5 difficulty levels. Although the results showed a significant increase of subjective workload, which was paralleled by an increasing error rate, we found significant differences only in one physiological parameter, i.e. the electrodermal activity was significantly higher in the most difficult condition (level 5) in comparison to the easiest one (level 1).

1 INTRODUCTION

The high level of automation in manufacturing increased the productivity, however the operation of modern machines often requires many complex activities for an efficient interaction with the interface. This results in a high cognitive demand, especially in relation to elderly, inexperienced or disabled operators. So far, signals from heart, eye, brain, muscles and skin have been investigated in relation to cognitive workload [1, 2]. A simple way of measuring that relationship is to look at heart rate or more precisely - heart rate variability (HRV), a non-invasive measurement of the interactions between the autonomic nervous system and the cardiovascular system, based on the study of oscillations of the interval between heartbeats [3]. Galvanic Skin Response, also referred to as electrodermal activity (EDA), is another low-cost, easily-captured, robust measurement [4]. In this method the electrical conductance of the skin is measured with one or two sensor(s) usually attached to a side of a hand or foot. Skin conductivity varies with changes in skin moisture level (sweating) and can reveal changes in sympathetic nervous system. Wearable and mobile devices that capture these data have the potential to identify risk factors of high stress levels caused by cognitive workload and to provide information to improve worker's well-being and performance. The aim of our study was to evaluate cognitive workload based on physiological indices using such wearable and mobile device and EEG, behavioural (the number of correct answers) and subjective (pen and pencil questionnaire).

2 METHODS

2.1 Subjects

21 healthy volunteers participated in the study: 12 females and 9 males aged 29-35 (Mean age = 30,05±3.38). Participants were informed about the aim of the study and written consents were obtained from the participants prior to the measurement session. The study had been approved by the Ethical Committee.

2.2 Physiological measurement of cognitive workload

Three physiological parameters were measured using the Empatica E4 [5] Electrodermal Activity (EDA), and Heart Rate (HR), and temperature. Additionally, HR was also measured using the Polar chest-band. EEG was measured with 32 Ag/AgCl Electrodes (256-channel g.Hlamp® biosignal amplifier).

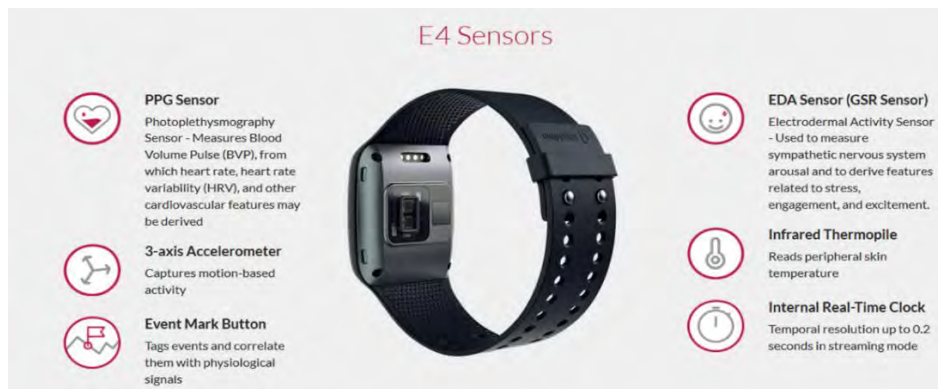


Figure 1. www.empatica.com/e4-wristband

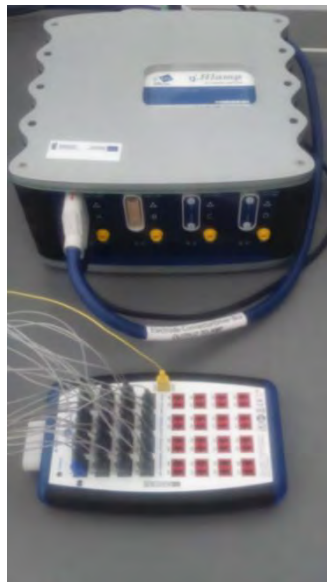


Figure 2. The 256-channel g.Hlamp Amplifier with a set of 32-active electrodes used in the experiment.

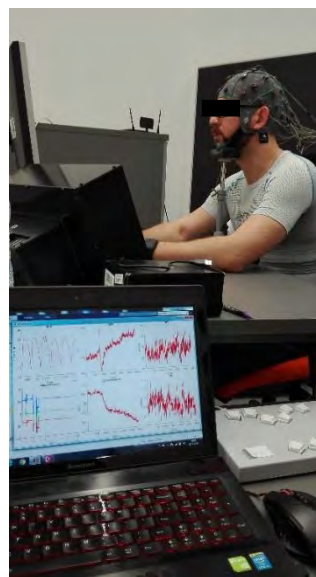


Figure 3. The set up of the experimental equipment.

2.3 Subjective measurement of cognitive workload

Subjective cognitive workload measurements were also conducted using the NASA-TLX (Nasa-Task Load Index) [6]. It consists of 6 scales: 1. Cognitive strain; 2. Physical strain; 3. Time Pressure; 4. Capacity; 5. Effort; 6. Frustration. The scales are grouped into pairs that the test participant selects an option from. When performing the task the test participant is asked to indicate within each pair the more perceptible or dominant category, as well as evaluate on a 20-point scale the scope of cognitive and physical strain experienced when performing the test task.

2.4 Behavioral measurement of cognitive workload

Behavioral measurement of cognitive workload was based on the number of errors made by a study participant during the arithmetic test.

2.5 The experimental task

To assess cognitive workload 5 sets of 22 arithmetic tasks (multiplication) corresponding to 5 levels of difficulty were used. In the beginning, each subject was given a set of instructions for the experiment, signed the consent form, and was seated comfortably about 50 cm from the computer screen in a noise-attenuated, shielded room. On the display screen there were being displayed mathematical multiplication tasks at various difficulty levels (ca 20 tasks per each difficulty level). The participant's task was to complete each calculation without helping himself/herself to a pen and paper and provide the score out loud. After providing each answer the correct score was displayed on the screen. The tasks were classified into 5 conditions (including base condition, serving as a task example) each condition corresponding to an increased difficulty level, and produced 5 experimental conditions. There was a time limit of 30 seconds for providing the answer. At the end of each task run, self-report assessments of task loading were obtained using the NASA–Task Load Index (TLX) rating scale.

2.6 Statistical analysis

A one-way Repeated Measures ANOVAs were conducted to compare the effect of 5 experimental conditions on heart rate, and EDA, as well as of subjective and behavioural cognitive workload measurement. Post hoc analyses using the Bonferroni post hoc test were performed to assess the differences between conditions.

3 RESULTS

Among physiological indices of cognitive load included in the study (HR, temperature, EEG and EDA) only EDA showed the significant differences between experimental conditions.

3.1 Physiological measurement of cognitive load: EDA

The entire data has been analysed using the Ledalab programme. The statistical analysis has been based on a data collected from 15 persons. The remaining persons have been disregarded due to signal issues. Repeated Measures ANOVA variance analysis was conducted, using a simplified contrast, whereby the μS phasic EDA average value constituted the interpersonal variable at every task level on a 1 (baseline) – 6 (hard) scale. Overall, the group differences test demonstrates an important, phasic EDA median discrepancy amongst selected test conditions, $F(2.937, 41.112) = 3.044, p < 0.04$.

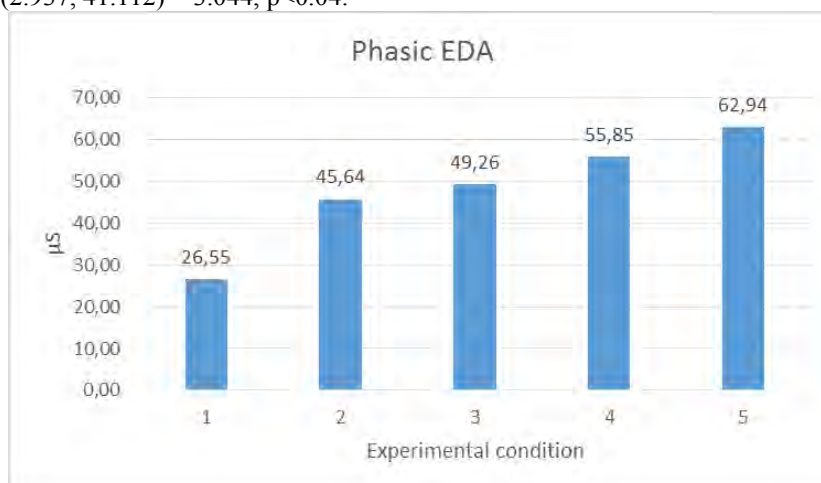


Figure 4. Mean EDA values in 5 experimental conditions (1 – very low cognitive load; 5 – very high cognitive load). $N = 17$

The simplified contrasts' analysis (comparing level 5 to each level) demonstrated differences between the highest level and the baseline level ($F(1, 14) = 5.722, p < 0.031$), as well as the level 1 ($F(1, 14) = 6.019, p < 0.028$). The dominant trend analysis indicates, however, a significant linearity $F(1, 14) = 6.234, p < 0.026$. Hence, the higher the difficulty level, the higher the expected phasic EDA level. Such a correlation permits to assume a potential phasic EDA use as a higher resolution cognitive workload indicator.

3.2 Subjective measurement of cognitive load: NASA-TLX

The results of a one-way Repeated Measures ANOVA show that there was a significant effect of experimental condition on the subjective workload, $F(4,64) = 23.72, p < 0.001$. The Bonferroni post hoc test showed a significant difference in subjective workload levels between most conditions, except for the difference between 1st and 2nd condition, 3rd and 4th condition, and between 4th and 5th condition. As shown in the Table 1, the more difficult experimental condition (higher error-rate), the higher subjective workload.

Table 1. The means (SD in brackets) of error-rate and subjective workload score (NASA TLX total score) in five conditions of the experimental task. The digit used in every condition denotes the difficulty level of the task (i.e. 1- the easiest, 2- the hardest).

	Condition 1	Condition 2	Condition 3	Condition 4	Condition 5
Error-rate	18%(±14%)	37%(±24%)	53%(±29%)	68%(±28%)	88%(±14%)
NASA-TLX	48.84 (±19.58)	55.95 (±18.37)	63.46 (±15.94)	71.32 (±19.69)	76.99 (±12.27)

3.3 Behavioral measurement of cognitive load: the number of errors

The results of a one-way Repeated Measures ANOVA show that there was a significant effect of experimental condition on the subjective workload, $F(4,64) = 81.40, p < 0.000$. The Bonferroni post hoc test showed a significant difference in errors between all of the 5 conditions. The direction of the workload conformed with the hypothesis, i.e. the more difficult experimental condition, the higher number of errors.

4 DISCUSSION

Although, the wearable and mobile tools to measure different physiological indices are increasingly used in both clinical and occupational settings, their validity is being rarely evaluated in the studies. Our findings showed that wearables, despite their advantage in terms of user comfort and real-time measurement functionality, are vulnerable to high artefact rate occurring as a result of body movements during experiment/work or other factors. However, in order to adapt working conditions to the worker's cognitive load, i.e. to the physiological parameters of cognitive load, data processing needs to be conducted in real-time. The challenge is to develop good algorithms for removing the artefacts. Another challenge is the large variability, both in cognitive skills (math skills) as well as the quality of the obtained signal (i.e. number and size of the motion, muscle artefacts, skin conduction). As these parameters were also measured, the future work will be concentrated on the analyses of the effect of individual differences on the obtained results.

Although the arithmetic test is an accepted procedure to measure the cognitive load, some other experimental procedures should also be tested for the cognitive load measurement performed with the help of wearable and mobile devices.

5 REFERENCES

1. Hill, S.G., Iavecchia, H.P., Byers, J.C., Bittner, A.C., Zaklad, A.L., & Christ, R.E. Comparison of four subjective workload rating scales. *Human Factors*, 1992; 34, 429–43
2. Ryu K, Myung R. Evaluation of cognitive workload with a combined measure based on physiological indices during a dual task of tracking and cognitive arithmetic. *International Journal of Industrial Ergonomics*. 2005; 35:991–1009.
3. Pumprla J, Howorka K, Groves D, Chester M, Nolan J. Functional assessment of heart rate variability: physiological basis and practical applications. *International Journal of Cardiology* 2002; 84: 1–14.
4. Nourbakhsh, N., Wang, Y., Chen, F., Calvo, R.A. Using Galvanic Skin Response for Cognitive workload Measurement in Arithmetic and Reading Tasks. *OZCHI'12*, 2012; Melbourne, Victoria, Australia.
5. Wristband E4 Wristband. Available online: <https://www.empatica.com/e4-wristband> (accessed on 21 November 2016).

Poster session

6. Hart, S. G., & Staveland, L. E. Development of NASA-TLX (Task Load Index): Results of empirical and theoretical research. In P. A. Hancock & N. Meshkati (Eds.), *Advances in psychology*, 52. Human cognitive workload (pp. 139-183). Oxford, England: North-Holland. 1988.

The research is carried out within the “Smart and adaptive interfaces for INCLUSIVE work environment” project funded by the European Union’s Horizon 2020 Research and Innovation Programme under grant agreement N. 723373.

Development of a VR based qualification module in trainings on risk assessment according to the EU Directive on Safety of Machinery

Gomoll K.¹, Nickel P.¹, Huis S.²

¹ Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA)
– Alte Heerstraße 111 – D-53757 Sankt Augustin – Germany

² German Social Accident Insurance Institution for the foodstuffs and catering industry (BGN)
– Dynamostraße 7-11 – D-68165 Mannheim – Germany

katrin.gomoll@dguv.de

peter.nickel@dguv.de

stephan.huis@bgn.de

KEYWORDS: Risk Assessment, Training, Structured Development, Virtual Reality, Machine Safety

ABSTRACT

According to the EU Directive on Safety of Machinery, it is mandatory to perform risk assessments before machinery is placed on the European market and is put into service. When varying or chaining up machines into production processes at operating sites, this may turn the operating company into a manufacturer of a new machine requiring new risk assessments. Thus, the demand on how to take into account OSH requirements for all scenarios with machinery use affects manufacturing as well as operating companies. A research project has been launched to investigate whether and how VR may be of benefit for risk assessment training in the given context.

The framework of structured development of virtual environments (SDVE) consists of an iterative process along project definition, requirement analyses, specifications, training concept, VR programming, implementation and evaluation. Translation of the SDVE into the current project is presented with initial results across the SDVE process. A draft model of a production environment has already been developed in virtual reality (VR). The model allows inspecting machinery in 1:1 scale and provides an insight into human-system interaction processes for risk assessment training; i.e. mounting emergency stop buttons, setting up light curtains, and placing a tunnel to prevent access to hazardous areas. The project is still in the process of the SDVE for VR-based support of risk assessment trainings, trainer needs and trainee activities during training. The SDVE framework offers a sound basis for planning and implementation of VR in projects on applications including human-system interaction.

1 INTRODUCTION

According to the EU Directive on Safety of Machinery [1] an iterative process of risk assessment including risk reduction should refer to scenarios with machinery use following consecutive stages of the machine life cycle. For manufacturers it is mandatory to perform risk assessments before placing machinery on the EU market and putting machinery into service. This aims at designing and manufacturing machines such that the essential health and safety requirements should be satisfied in order to ensure that machinery is safe. Performing prospective risk assessments early in the design process is seen most effective [2-4]. Modelling and simulation tools such as virtual reality (VR) techniques have the potential to support designers and those responsible for risk assessments early in machinery design while at the same time provide requirements for human-system interactions in the context of use. For this purpose, modelling and simulation applications should specifically be designed along the requirements of risk assessments and relevant work scenarios under inspection [5,6].

For operating companies, the above-mentioned process of risk assessment is important, because changing or chaining up machines into production processes may turn the company into the manufacturer of a new machine [1]. This poses a special challenge because of the broad range of requirements resulting from the EU Machinery Directive, among others with regard to ergonomics design, human-system interaction, safety distances and machine access [1]. Besides knowledge about suitable measures available with regard to the hierarchy of controls, experience with performance and documentation of professional risk assessments is required.

The German Social Accident Insurance Institution for the foodstuffs and catering industry (BGN) supports companies in the process of risk assessment by consultations and by education and training. Personnel associated with risk assessments in companies are given basic and advanced training on when and how to conduct risk assessments including risk reduction and documentation. At the shop-floor level, however, learning can improve, if training of basic knowledge is closely linked to practical work situations and thereby addresses procedural

knowledge. Among others, tapping human information processing and involving multiple senses is advantageous, such as hands-on experience, practice at solving problems, and understanding and experience of the limitations of a specific solution [6]. In the given context, VR is often used as a tool to support education and training requirements, e.g. to recreate work scenarios that otherwise cannot be recreated in reality due to lack of presence, due to costs, risk or the availability of resources [7]. Studies investigating the impact of different media to support risk assessment found virtual environments (VE), designed according to requirements of task goals and context of use, resulting in improved quality and quantity of assessments as compared to support by photo, video and documentation. This was due to a higher sense of presence in the VE and therefore points out, that VE design requires meeting the demands of the intended use and should follow procedures as suggested in work systems design [8-10,2]. Furthermore, existing training methods can be improved in terms of new qualification schemes, which are often not possible in the real world, and in terms of increased motivation and easy monitoring of trainees' activity [11,12]. An appropriate instructional design model is necessary to guide VR application design and development to fully exploit the potentials of virtual learning environments. Particular attention should be given to the framework used to guide the development, because VR as 3D visualisation attributes presence and immersion and while at the same time affects the quality and usefulness of the application [13].

In order to investigate whether and how VR may be of benefit for risk assessment training in the given context, the German Social Accident Insurance Institution for the foodstuffs and catering industry (BGN) launched a research project. The Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) developed and investigated a module for VR supported qualification in risk assessments according the EU Machinery Directive [1,14].

2 METHODS

In close cooperation with the BGN, a project group has been set up including members of the IFA Human-System-Interaction Group and students from the University of Applied Sciences Koblenz. The former managed the research project and adapted a module of an existing training concept of the BGN to integrate a VE for human-system interaction in a production setting referring to the framework for the structured development of VE (SDVE [15]). The latter were instructed to support the procedure by application of Unity (Unity Technologies ApS, USA) as a VR software system for the development of interactive and dynamic VR simulation models suitable to support the process of risk assessment in the training module.

Among the approaches for building virtual environments, there is no single correct approach. In practice, the chosen approach depends on what the VE is intended for, how well formalised the idea is, how specific the user's and task requirements are as well as the experience and programming style of the VE software programmers. For the current research project, it is important that the framework covers the stages of instructional design, namely analysis of learning problems, design, development and evaluation of instructional processes [13]. The iterative process of the SDVE provides appropriate feedback loops, allows therefore for VE design refinements and includes procedures for formative and summative evaluations. This allows the VE to be designed for the training task (top-down) and supporting effectively learning processes. However, at the same time, parts of the development are to serve performance requirements (bottom-up) referring to different user groups and their interactions (e.g. trainees, trainers, project managers, software developers) during VE development, VE integration in the training module and use during the training course. The SDVE follows a procedure with stages (see list) that will address different interrelated items (see brackets) and refer to different methods for information acquisition:

- Project definition (project description, stakeholders, priorities, limitations) using training documentation analysis and interviews
- Requirements analysis (user analysis, task analysis) using personas and hierarchical task analysis
- Specification (scenarios, storyboards) using interviews and training documentation analysis
- Concept Design (integration of VE in training concept related to formal knowledge, paper and pencil documentation, discussions, human system interaction in VE, scenario selection) using training documentation analysis and discussion
- VR development and programming (modelling, implementation of functionalities) using software development process and usability evaluations
- Implementation (test application of the VR model in the module and in the training course) using workshops and interviews
- Evaluation (investigation of learning effects) using questionnaires, interviews and workshops

The SDVE framework itself is an iterative process (i.e. structured development process), as is the risk assessment (i.e. risk assessment process) and as is the VE development process (i.e. preferably a user-centred

design process). In terms of stakeholders, project management and BGN are interested in all processes, while trainers concentrate on processes of risk assessment and VE development, and trainees are rather interested in a user-centred design process. The SDVE is a suitable approach for the development of VR-based training modules on risk assessment as it allows for breaking down and handing over the initial objective and context of use of the VE development (i.e. the project goal) into design and programming of the VE. As a consequence, the requirements for VE development will not only refer to work scenario design and human-system interaction requirements for specific stages in risk assessment (see implementation of functionalities), but include requirements to tap all stages of risk assessment (see task analysis) and include provision of learning environment to improve knowledge and skills (see limitations and training need analysis). Therefore, training need analysis is linked to the *goal* of the project, constraints, priorities and results from stakeholder analysis; with organizational goals such as occupational safety and health (OSH), strategic objectives such as risk assessment according to [1,14], and specific objectives such as qualification, development of knowledge and skills and including user's capabilities and limitations.

Educational studies in VE [e.g. 16-21] have highlighted the variety and flexibility of VR in instructional design and training. Benefits of using VR in education are related to the instructional design paradigm and the principles of constructivism [22] according to which knowledge is being actively constructed by the learner (i.e. teachers act as facilitators not as knowledge transmitters) and knowing is an adaptive process, which organises the learner's experiential world [23,24]. VR as a tool for modelling and simulation has the potential to serve these principles due to its ability to mediate world exploration and construction, its mapping of a user to any character and the provision of shared virtual worlds [25].

The aim of the training is to inform about the process of risk assessment and to support trainers and trainees in instructing and conducting assessments including risk reduction and documentation. This type of risk assessment follows a three-step procedure for risk reduction [1,14]; starting with risk analysis, followed by risk evaluation, and resulting in risk reduction according to OSH design requirements. Risk analysis includes determination of the limits of the machinery, hazard identification and risk estimation. This taken together with risk evaluation forms the risk assessment. Risk assessments as iterative processes should prospectively be performed for different stages of the machine life cycle (i.e. construction, modification), levels of maturity (i.e. mock-up, prototype) and degrees of detail (e.g. components, whole machinery). This type of risk assessment is recommended at the planning stage and is mandatory at final construction stages before putting machinery in operation [1].

3 RESULTS

The SDVE process as illustrated in Figure 1 will guide along initial results of the research project.



Figure 1. The framework of the SDVE with its main stages.

3.1 Project definition

The initial step of the SDVE is crucial as it defines the goal of the application in the context of use and addresses all stakeholders relevant in organising the structured development as well as providing and using the VE as a tool to support task performance. The *goal* of the research project is to investigate as well as integrate a dynamic and interactive VE into an existing concept for risk assessment training consisting of several modules. The project aims at improving risk assessment performance with support of VE. The training is one among different courses on OSH prevention provided by the BGN for interested, BGN insured companies. It aims at facilitating the development of risk assessment knowledge, rules and skills. One of the modules will be modified by implementation of a suitable VE to become a new qualification module. The support of the VE in the module is intended to promote learning on how to perform risk assessments of machinery (e.g. among others through exploration, situated action).

Several stakeholders of the qualification module need to be taken into account at different steps in the SDVE. Among them are occupational safety and health (OSH) experts of companies and of the BGN, members of plant management and maintenance departments in companies, manufacturers of machinery and equipment, machine operators, personnel involved in different operational stages of machinery operation. In addition and more closely related to the risk assessment support, members of departments for education and training of the BGN, risk assessment trainers and trainees as well as members of the research project team are among stakeholders.

3.2 Requirement Analysis

User analysis accounts for differentiation between trainer and trainees, i.e. individual analyses for each group. The analysis based on interviews and group discussions resulted in persona drafts, which should be validated before final integration of the module in training documentations.

Task analysis is required for the development of knowledge and skills in risk assessment including transformation of instructional information on risk assessment to procedural knowledge as well as the decomposition of risk assessment (e.g. the application task) into required stages and operations. The method applied is hierarchical task analysis referring to steps of the risk assessment process according to the standard on risk assessment [26]. Documentation of task analysis is organised in mind maps that illustrate parallel structures at project definition, requirements and specification levels.

3.3 Specification

Based on requirements derived from analyses for VE within the application context ‘risk assessment of machinery’, each step of the risk assessment process generates a specific *scenario*. Each scenario consists of (a) a virtual representation of the relevant environment in context of use (e.g. machinery with and without application of measures for risk reduction), (b) proposals for human-system interaction (e.g. allow for walking through the VE in 1:1 scale) and (c) functionalities for training needs (e.g. providing several good practice solutions for appropriate risk reductions). Specifications for scenarios serve project goals as well as user and task analysis rather than providing a testbed for technical capabilities or fancy technical functionalities. Scenarios refer to the stages in the process of risk assessment and to different tasks involved.

The *storyboard* displays for each scenario consecutive user operations and activities to be accomplished in the VE respective to fulfil tasks and sub-tasks and at higher levels to contribute to project goals. For example, in risk analysis and risk reduction scenarios, the user needs to measure distances, while in the function analysis scenario this operation is not necessary. Members of the project team have developed storyboards for each scenario as documentations based on group discussions.

3.4 Concept Design

With regard to training needs, risk assessment performance will follow a stepwise procedure in terms of performing the risk analysis for the machine as a whole rather than analysing individual risks that will subsequently be addressed in risk evaluation and risk reduction. This results in a modular structure of the training concept that requires the application of each scenario to be carefully matched with the other modules accounting for the respective step of the risk assessment process in terms of instruction, information and operations being provided. During the training course, teacher-centred instruction formally introduce each step of the risk assessment process. Then, knowledge gained by the trainees will be applied in the respective VE scenario to allow for developing rules and skills. Documentation of the process and intermediate as well as final results appear in paper or computer-based form. So far, the modular structure of the training concept has been outlined and the match and conjunction of the modular parts is almost completed. Adaption of the existing training material referring to others than the VE module, however, is still in progress.

3.5 VR development and programming

Though the SDVE process should usually be followed serially, some steps of VE development have been started in parallel. While modelling and simulation have reached conceptual design level (see Figure 2), some principal human-system interaction processes to support risk assessment training are already included, such as placing a tunnel at the machine entry for risk reduction. Further development will also address training needs with regard to presenting good practice solutions or specific training constellations, conservation of today’s training results for the next day and inclusion of control functionalities for starting, freezing and stopping VE scenarios.

3.6 Implementation

Although drafts of the VE are available for visualisation and formal testing and design reviews, implementation of the VE in the training module is work in progress.

3.7 Evaluation

The investigation of learning effects is not yet dealt with; however, criteria and measures relevant for evaluation have been discussed and gathered throughout the SDVE.



Figure 2. Virtual environment to support risk assessment of a production process with different machinery.

4 CONCLUSIONS

The research project aimed at developing and integrating a qualification module that allows a VE to support training on risk assessment [1,14]. The framework of the SDVE has successfully been used as an instructional model to organise the research and development process for the new training module. This process, however, is not yet completed and final steps of the framework are work in progress. The application of the SDVE supported the coordination of interwoven processes, i.e. the process of developing a VE could be informed by the process of risk assessment performance as well as by the framework process referring to the deduction of requirements from project goals through users and tasks to specifications with regard to training needs. In the present context, VE became a potential tool to support training on risk assessments by complying with requirements of the project, tasks and users. Outstanding evaluation studies will address the usability of the VE and effects on qualification through VR based risk assessments.

There are, however, methodological and technological issues to be considered in the application of VR modelling and simulation [6]. From a methodological point of view, scenario selection is rather limited to the production environment chosen in the given research project and cannot be a full representation of future work scenarios of relevance for risk assessments [1,14]. In addition, little is known about human factors to be considered in VE design that foster training transfer into practice, especially with regard to risk assessment performance. From a technological point of view, using VR is limited because it causes selection effects e.g. for those users who are very sensitive to simulation sickness or have impairments in depth perception.

Benefits and limitations for successful VE applications as demonstrated in the given research project, however, may also hold for other machinery and work systems in industry and services. This provides a sound basis for guiding similar projects along lessons learned and experiences gained in the study presented.

5 ACKNOWLEDGEMENTS

The authors are very grateful to the efforts of Mr. Christopher Braun und Mr. Nicolai Leuthner from the University of Applied Sciences Koblenz, RAC Remagen, for technical development of the dynamic VR model by using the cross-platform game engine Unity (Unity Technologies ApS, USA).

6 REFERENCES

1. EU Machinery Directive 2006/42/EC of the European Parliament and the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast), Off. J. Eur. Union L 157(2006), 24-86.
2. Kantowitz B.H., Sorkin R.D., *Human factors: Understanding people-system relationships*, New York, Wiley, 1983.
3. Merdian J., *Risikobeurteilung in Arbeitssystemen*, Die BG 10 (1995), 518-524.

4. EN ISO 6385, *Ergonomic Principles in the Design of Work Systems*, CEN, Brussels, 2016.
5. Nickel P., Janning M., Wachholz T., Pröger E., *Shaping Future Work Systems by OSH Risk Assessments Early On*, Advances in Intelligent Systems and Computing (AISC) 819 (2019), 247-256.
6. Hale K.S., Stanney, K.M. (eds.), *Handbook of virtual environments: Design, implementation, and applications*, CRC Press, Boca Raton, 2015.
7. Cobb S.C., Richir S., D'Cruz M., Klinger E., Day A., David P., Gardeux F., van den Broek E., van der Voort M.C., Meijer F., Izkara J.L., Mavrikios D., *How is VR used to support training in industry? The INTUITION network of excellence working group on education and training*, Proceedings of the 10th Virtual Reality International Conference (VRIC 2008) (75-83), Apr 9-13, 2008, Laval, France.
8. Perlman A., Sacks R., Barak R., *Hazard recognition and risk perception in construction*, Safety Science 64 (2013), 22-31.
9. Moreno R., Mayer R.E., *Learning science in virtual reality multimedia environments: Role of methods and media*, Journal of Educational Psychology, 94(2002) 3, 598-610.
10. Wichtl M., Nickel P., Kaufmann U., Bärenz P., Monica L., Radandt S., Bischoff H.-J., Nellutla M., *Improvements of Machinery and Systems Safety by Human Factors, Ergonomics and Safety in Human System Interaction*, Advances in Intelligent Systems and Computing (AISC) 819(2018), 257-267.
11. Rothbaum B.O., Hodges L.F., *The Use of Virtual Reality Exposure in the Treatment of Anxiety Disorders*, Behaviour Modification, 23(1999), 507-25.
12. Winn W., *Research into practice: Current trends in educational technology research: The study of learning environments*, Educational psychology review, 14(2002) 3, 331-351.
13. D'Cruz M., *Structured evaluation of training in virtual environments* (PhD thesis), Nottingham, University of Nottingham, 1999.
14. EN ISO 12100, *Safety of Machinery – General Principles for Design – Risk Assessment and Risk Reduction*, CEN, Brussels, 2010.
15. Eastgate R.M., Wilson J.R., D'Cruz, M., *Structured Development of Virtual Environments*, In Hale K.S., Stanney K.M., (eds.), *Handbook of virtual environments: Design, Implementation, and Applications* (353-390), Boca Raton: CRC Press, 2015.
16. Antonietti A., Cantoia M., *To see a painting versus to walk in a painting: an experiment on sense-making through virtual reality*, Computers & Education 34(2000) 3-4, 213-223.
17. Cobb S., Neale H., Crosier J., Wilson J.R., *Development and evaluation of virtual environments for education*. In Stanney K.M. (ed.), *Handbook of Virtual Environments: Design, Implementation, and Applications* (911-936), New Jersey: LEA, 2002.
18. Dede C. *Evolving from multimedia to virtual reality*. In Maurer H. (ed.), *Educational Multimedia and Hypermedia Annual* (123-130), Proceedings of ED-MEDIA 93, World Conference on Educational Media and Hypermedia, June 23-26, 1993, Orlando, USA.
19. Hamada M., *An example of virtual environment and web-based application in learning*, International Journal of Virtual Reality, 7(2008) 3, 1-8.
20. Helsel S. *Virtual Reality and education*, Educational Technology, 32(1992), 38-42.
21. Roussou M., *Learning by doing and learning through play: an exploration of interactivity in virtual environments for children*, ACM Computers in Entertainment, 2(2004) 1, 1-23.
22. Chen C.J., Teh, C.S., *An affordable virtual reality technology for constructivist learning environments*. Proceedings of the 4th Global Chinese Conference on Computers in Education (GCCCE 2000) (414-421), May 29-31, 2000, Singapore.
23. Chuah K.M., Chen C.J., *Unleashing the Potentials of Desktop Virtual Reality as an Educational Tool: A Look into the Design and Development Process of ViSTREET*, Proceedings of the 2nd International Malaysian Educational Technology Convention– Smart Education: Converging Technology, Pedagogy and Content (imetc 2008) (81-86), Nov 4-7, 2008, Kuantan, Pahang Darul Makmur, Malaysia.
24. Merrill M.D., *Constructivism and instructional design*, Educational Technology, 31(1991) 5, 45-53.
25. Burdea G.C., Coiffet, P., *Virtual reality technology*, New Jersey, Wiley, 2003.
26. Stanton N.A., *Hierarchical task analysis: developments, applications, and extensions*, Applied Ergonomics, 37(2006) 1, 55-79.

Conducting risk assessments early on serves multiple purposes

Nickel P.¹, Janning M.², Pröger E.³, Wachholz T.⁴, Lungfiel A.¹

¹ Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA)
– Alte Heerstraße 111 – D-53757 Sankt Augustin – Germany

² German Social Accident Insurance Institution of the Federal Government and for the railway services (UVB)
– Cheruskerring 11 – D-48147 Münster – Germany

³ Federal Waterways and Shipping Administration (GDWS)
– Mainzer Straße 20 – D-56068 Koblenz – Germany

⁴ Federal Waterways and Shipping Administration (GDWS)
– Am Waterlooplatz 5 – D-30169 Hannover – Germany

peter.nickel@dguv.de

KEYWORDS: Occupational Safety and Health, Risk Assessments, Modelling and Simulation, Prevention, Standardisation of Products

ABSTRACT

In future, new work systems become more interactive, dynamic, and flexible with the requirement that occupational safety and health (OSH) should call for prospective assessments of hazards and risks to facilitate prevention through design. German river locks for inland waterways will be composed of standardised objects representing a high level of OSH. A research project aimed at conducting risk assessments of river locks of the future; early in their planning stage, with standardised objects and referring to different EU Directives addressing safety and health at work. About 150 work scenarios across operational states and variations in river lock standardisation have been compiled and supplemented for instructing risk assessments. They also conveyed design requirements for setting up dynamic virtual reality (VR) planning models in future contexts of use. One out of three risk assessments has already been conducted. The assessment focused on OSH during maintenance operations with several operators involved. A draft documentation of the assessment revealed design flaws as well as hazards to be addressed with appropriate measures for risk reduction. Results will serve the remaining assessments and will be fed back to trigger different activities among project member organisations. Risk assessments will also facilitate prevention through design (PtD) and contribute to avoid detrimental consequences for operators before OSH impairments take effect, i.e. before standardisation for river locks goes into construction. The project motivates applications in similar contexts.

1 INTRODUCTION

Occupational safety and health (OSH) is becoming increasingly interested in prospective assessments of hazards and risks to enable improvements early in work systems design [1,2]; i.e. human-system interactions regarding work tasks, organisation, equipment, and environment. With its design strategies (e.g. task orientation) and principles (e.g. compatibility) human factors and ergonomics is well prepared for prospective design as it provides a broad range of recommendations to meet requirements in human centred design and OSH; already part of standards [e.g. 2,3] and legislation (e.g. [4,5,6]). In addition, the human factors and ergonomics literature offers procedures to support the design of interactive, dynamic and flexible work systems of the future.

In the German transport sector high priority is given to standardisation of river lock design since it has the potential to expand transport resources, reduce costs across the life cycle, and improve OSH [7]. The latter is seen most effective early in design, because re-design due to safety and health issues would be resource demanding, if not impossible, when river lock construction has already been completed. Improvements therefore should address potential hazards and risks in different operational stages of machinery and across a river lock life cycle. Design requirements to be addressed early in design should therefore go beyond those considered according to the EU Machinery Directive [5]. They should include all activities at river locks, especially hazards and risks during maintenance and repairs, as covered by the EU Framework Directive [4], as well as operations required at later stages of the technical system (e.g. when extending the building or cleaning facades) according to the Construction Site Directive [6].

With the aim to investigate potential OSH improvements for future standardisation of river locks, the German Social Accident Insurance Institution of the Federal Government and for the railway services (UVB) launched a research project. The Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA) has carried it out in close cooperation with the UVB, the German Federal Ministry of Transport and

Digital Infrastructure (BMVI), different departments of the Federal Waterways and Shipping Administration (GDWS) and the German Social Accident Insurance Institution for Transport and Traffic (BG Verkehr).

2 METHODS

2.1 Risk assessments

At work and across the life cycle of work systems, risk assessments serve to improve safety and health of employees at work and other forms of activity and include prevention of occupational accidents, occupational diseases and work-related health risks as well as human centred design of working conditions [8,7]. Risk assessments, often with different targets and procedures, are mandatory according to different European Directives transferred into member countries' legislation [4-6]. While hazards are intrinsic characteristics of objects or procedures such as work materials, equipment, procedures and practices with the potential to cause harm, risk is the likelihood that the potential harm will be attained under the conditions of use and/or exposure, and the possible extent of the harm [9]. Risk assessments should cover all risks arising out of working conditions, which are reasonably foreseeable and should also include reasonably foreseeable misuse. When referring to early stages of development or planning, risk assessments are sometimes attributed preventive and prospective [10], while for iterations in risk assessments or concluding assessments terms like amendatory or corrective are used.

In the context of the research project, risk assessments refer to three different EU Directives. Hazard and risk documentation requirements according to the EU Construction Site Directive [6,11] refer to safety and health plans and safety and health files to identify and prevent OSH risks during on-site construction as well as during subsequent construction work across the plant or facility life cycle. Safety and health of machine operators with regard to design requirements of machinery are of concern in the EU Machinery Directive [5]. With a view to EU Machinery Directive, the risk assessment mainly addresses scenarios referring to aft and head of the river lock and covers potential human interactions with mechanical and construction engineering parts of the machinery. Risk assessments according to the EU OSH Framework Directive [4] focuses on maintenance operations with several operators involved (e.g. draining of river lock and gate maintenance), the river lock superstructure and on ergonomics and human safety issues at the lock superstructure (e.g. guard railing, lightning repair).

Risk assessments usually are on-site investigations to determine the presence, type, severity, and location of hazards and provide suggested ways to control them. Assessments are often conducted by groups of inspectors having expertise in different domains for scenarios under investigation, i.e. OSH experts in cooperation with experts e.g. for the tasks at hand, machinery construction, production requirements. Conducting risk assessments in simulated environments is investigation and inspection work that relies on static and dynamic scenario design, with a broad range of typical scenarios in the context of use. While risk assessments in real life are conducted at different times and even several times across the river lock life cycle, in the research project, however, all will be performed early in design and therefore referring to the planning stage of a standardised river lock and variations according to the standard [12]. This is because potential hazards and risk across the life cycle should be considered to improve future standardisation for river lock design early on.

2.2 Development of scenarios

Assessing hazards and risks in static and dynamic work scenarios allows for analysis of human-system interactions during task performance in present and future contexts of use. The research project proposes a scenario approach, since scenarios cumulate situations of relevance for risk assessments and for improving OSH of working conditions at river locks. Although scenarios have neither the same impact nor the likelihood to achieve its goals, they serve as focal points representing a range of variations and possibilities. The different types of risk assessments at river lock sites determine scenario selection and development. Potentially relevant scenarios at river locks including further explanations about their integration in risk assessments were compiled based on different criteria [13-15]:

- typical work tasks conducted at river locks during normal operations; i.e. up-stream and downstream locking of different barges,
- typical work tasks conducted at river locks during operations deviating from normal operations; i.e. maintenance and repairs,
- work activities at different operational concepts and operating modes (e.g. automatic, manual and special),
- user requirements for operating the river lock and for shipping,
- accident prone situations or core hazardous situations with regard to river lock use or during operational states across the life cycle,
- scenarios usually taken into account at former risk assessments in reality, and
- scenarios showing standardised objects of river locks in contexts of use, to name but a few.

2.3 Development of a dynamic planning model and simulation

Risk assessment early in design requires modelling and simulation tools, which consider requirements for conducting different types of assessments and which introduce relevant work scenarios in the present and future context of use across the life cycle [16,17]. A dynamic virtual reality (VR) planning model in 1:1 scale has been developed based on 3D CAD planning information referring to drawings of ongoing implementation planning of the first river lock according to the new standard. The new standard comprises a kit of standardized objects covering river lock requirements for professional inland navigation in Germany (e.g. chamber construction, lock gates). The VR planning model comprises a river lock currently under planning as well as variations such as rise of water level (e.g. gates and chambers for 4 m to 25 m), length of river barges (e.g. for up to 135 m or even 185 m river barges), and type of water way (e.g. canal locks may have economizing basins).

3 RESULTS

3.1 Modelling and simulation

The research project required a dynamic VR planning model of use in terms of a tool suitable to support three different types of risk assessments in several work scenarios at future river locks with variations in standardisation. 3D CAD modelling referring to drawings of ongoing implementation planning of a river lock according to standardisation requirements served a basis for VR modelling. VR modelling and simulation was composed with the Vizard Virtual Reality Toolkit (WorldViz LLC, USA) to implement kinetics, apply environmental models (e.g. gravity, water, sky), animate moving parts of machinery (e.g. lock gates, water level), and include components necessary for contexts of use under investigation (e.g. river barges, mobile elevating work platforms).

Dynamic simulations of virtual work scenarios were projected on a 24 m² wall in the SUTAVE lab [www.dguv.de/ifa/sutave] in 1:1 scale. The scenarios were controlled by a Wii (Nintendo, USA) and by a graphical user interface on a desktop computer to allow for navigation in scenarios and to meet different purposes for assessment (e.g. 3D tape measurements, viewpoint selection, picture taking, adding comments). This interface also provided controls for dynamics of lock components (e.g. changing water level, driving barges, moving lock superstructure, dismantling gates using truck-mounted cranes) and for selection of alternative components (e.g. caverns covered or not, switching between ship arrester systems).

Prior to conducting risk assessments, project members performed a final design review [18], among others using cognitive walkthrough techniques. The review resulted in minor adjustments on functionalities; however, planning flaws identified were left untouched when verified by underlying sources for model development.

3.2 Scenarios for risk assessment

The collection of typical and relevant work scenarios among members of the project group and working groups in the Federal Waterways and Shipping Administration (GDWS) resulted in 150 work scenarios to be taken into account in one or more types of risk assessments (e.g. Figure 1). Scenario descriptions and explanations as well as a structure according to operational states (i.e. normal, maintenance, miscellaneous) and variations in standardisation of river locks (e.g. elastic ship impact protection devices independent of the gates, use of saving basins) served instructing risk assessments. Substructures were organised along standardised objects and work activities related to components of the river lock, such as

1. Normal operations
 - automatic operating mode,
 - manual operating mode,
 - special operating mode, etc.
2. Maintenance and repairs
 - chamber draining/flooding,
 - head/aft gate operations,
 - superstructure, etc.
3. Other operations
 - frost operations,
 - ship evacuation,
 - reasonable foreseeable misuse, etc.
4. Variations in standardisation
 - savings basins,
 - floating bollards,
 - elastic ship impact protection, etc.

3.3 Conducting risk assessments

Equipped with a collection of 150 work scenarios and the dynamic VR planning model in the SUTAVE lab of the IFA, so far one among three types of risk assessments have been conducted; i.e. the EU OSH Framework Directive [4]. Assessments according to the EU Construction Site Directive [6] and the EU Machinery Directive [5] will be carried out later this year. One inspector from an engineering consultancy and commissioned for conducting the risk assessment performed a two-day session risk assessment according to the EU Directive on the OSH Framework [4] (see Figure 1). Ten project members (from planning administration, maintenance managers, specialists for OSH, HFE, and VR) provided assistance during assessments. The assessment focused on OSH during maintenance operations with several operators involved (e.g. draining of river lock and gate maintenance) and with the usability of the lock superstructure (e.g. guard railing, lightning repair). A draft documentation of the assessment revealed design flaws (e.g. dismounting of head gate is blocked due to superstructure construction) as well as hazards to be addressed with appropriate measures for risk reduction (e.g. cavern access requires easy entry, guard rails at lock chamber causes crashing hazard when moving gate with guard rails attached).



Figure 1. Performing risk assessment according to EU OSH Framework Directive in the SUTAVE lab in the IFA.

Members of project group related to this type of risk assessment currently review the draft document of the risk assessments. Amendments and suggestions referring to individual notes taken during the assessment and for a complemented version will be discussed with the inspector from the engineering consultancy. Potential revisions will be organised with the inspector. A final documentation will be distributed among stakeholders for further use. Assessments will also feed risk assessments according to the EU Machinery Directive [5] and safety plan documentation according to the EU Construction Site Directive [6]. All results obtained during project preparations and assessments will serve the development of measures for risk reduction. Information will be fed back to the standardisation committee at GDWS to update construction and OSH requirements. Results will also go to planning organisations assigned to future river locks. In addition, template procedures available at GDWS and UVB for performing risk assessments and safety and health plans according to EU Directives [e.g. 4-6] will be developed and updated.

4 CONCLUSIONS

The research project investigated risk assessments being conducted early in the design process of river locks in future contexts of use with variations in standardisation. It could be demonstrated that identification of requirements for investigating work scenarios in the context of use and for performing risk assessments is a prerequisite for developing a suitable VR planning model. Risk assessments according to the EU OSH Framework Directive [4] are usually applied to improve OSH shortly before operational activities (e.g. normal operations, maintenance); however, in the current project it could successfully be applied to an early planning stage of a river lock. The assessments in a simulation environment revealed design flaws and measures for risk reduction relevant and transferable into OSH improvements in reality. This facilitates prevention through design

(PtD) and avoids detrimental consequences for operators before OSH impairments take effect, i.e. before standardisation for river locks goes into construction.

Conducting risk assessments early on serves multiple purposes:

- design improvements for river locks currently under planning,
- design improvements of standardised objects to better fit OSH requirements in standardisation of future inland river locks,
- improved templates and samples for conducting risk assessments according to [5],
- new templates and samples for risk assessments according to [4] and [6],
- basic information for operation instructions for technical components,
- basic information for working instructions for maintenance and repairs, and
- references for risk assessments to be conducted after successful construction and during operations.

There are, however, two methodological issues why care must be taken, when results related to simulations should be applied in practice. One refers to scenario selection, which cannot be a full representation of future work scenarios. The other refers to 3D CAD and VR as simulation techniques, which will always be simplifications and reductions due to complexity of reality. Nevertheless, both issues provide advantages such as that even those work scenarios can be investigated that do not yet exist and that simulation environments may to a certain extent represent and augment risk assessments as suggested above [19,20]. Risk assessments in work scenarios using modelling and simulation will neither replace final assessments in reality and in later stages of machinery design nor will they replace alternative means for support. However, as could be demonstrated, modelling and simulation serves risk assessments as beneficial complements and make risk assessments have the potential to shape OSH in future work systems early on.

5 ACKNOWLEDGEMENTS

The authors are very grateful to the efforts of Mr. Frank Schellberg and Mr. Andy Lungfiel for technical development of the 3D CAD and VR planning model.

6 REFERENCES

1. Kantowitz B.H., Sorkin R.D., *Human factors: Understanding people-system relationships*, Wiley, New York, 1983.
2. EN ISO 6385, *Ergonomic Principles in the Design of Work Systems*, CEN, Brussels, 2016.
3. EN 614-2, *Safety of machinery – Ergonomic design principles – Part 2: Interactions between the design of machinery and work tasks*, CEN, Brussels, 2008.
4. EU OSH Framework Directive 89/391/EEC of 12 June 1989 on *the introduction of measures to encourage improvements in the safety and health of workers at work* (with amendments 2008), Off. J. Eur. Union L 183(1989), 1-8.
5. EU Machinery Directive 2006/42/EC of the European Parliament and the Council of 17 May 2006 on *machinery, and amending Directive 95/16/EC* (recast), Off. J. Eur. Union L 157(2006), 24-86.
6. EU Construction Directive 92/57/EEC on *the implementation of minimum safety and health requirements at temporary or mobile construction sites*, Off. J. Eur. Union L 245(1992), 6-22.
7. Nickel P., *Extending the effective range of prevention through design by OSH applications in virtual reality*, Lecture Notes in Computer Science (LNCS), 9752 (2016), 325-336.
8. Lehto M.R., Cook B.T., *Occupational Health and Safety Management*, In: Salvendy, G. (ed.), *Handbook of Human Factors and Ergonomics* (701-733), Wiley, Hoboken, 2012.
9. European Commission, *Guidance on risk assessment at work*, ECSC-EC-EAEC, Luxemburg, 1996.
10. Merdian J., *Risikobeurteilung in Arbeitssystemen*, Die BG 10(1995), 518-524.
11. European Commission, *Non-binding guide to good practice for understanding and implementing Directive 92/57/EEC 'Construction Sites'*, Common, Frankfurt, 2010.
12. BMVI, *Standardisierung von Binnenschiffsschleusenanalgen bis zu 10 m Fallhöhe* (Erlass vom 20.12.2016 – WS 10/ 5212.4/1-2 (2576192)), BMVI, Bonn, 2016.
13. International commission for the study of locks, *Final Report of the International Commission for the Study of Locks*, PIANC, Brussels, 1996.
14. Dutch Ministry of Transport, Public Works and Water Management, *Design of Locks* (Report by the Civil Engineering Division), Bouwdienst Rijkswaterstaat, Utrecht, 2000.

Poster session

15. Nickel P., Kergel R., Wachholz T., Pröger E., Lungfiel A., *Setting-up a virtual reality simulation for improving OSH in standardisation of river locks*, Proceedings of the 8th International Conference on the Safety of Industrial Automated Systems (SIAS 2015) (223-228), Nov 18-20, 2015, Königswinter, Germany.
16. Eastgate R.M., Wilson J.R., D'Cruz, M., *Structured Development of Virtual Environments*, In Hale K.S., Stanney K.M., (eds.), *Handbook of virtual environments: Design, Implementation, and Applications* (353-390), Boca Raton: CRC Press, 2015.
17. Gomoll K., Nickel P., Huis S., *Development of a VR based qualification module in trainings on risk assessment according to the EU Directive on Safety of Machinery*, Proceedings of the 9th International Conference on the Safety of Industrial Automated Systems (SIAS 2018), Oct 10-12, 2018, Nancy, France.
18. EN IEC 61160, *Design review*, CEN, Brussels, 2005.
19. Nickel P., Nachreiner, F., *Evaluation arbeitspsychologischer Interventionsmaßnahmen*, In: Kleinbeck U., Schmidt K. (eds.), *Arbeitspsychologie (Enzyklopädie der Psychologie, D, III, 1)* (1003-1038), Hogrefe, Göttingen, 2010.
20. Meister D., *Simulation and modelling*, In: Wilson J.R., Corlett E.N. (eds.), *Evaluation of human work. A practical ergonomics methodology* (202-228), Taylor & Francis, London, 1999.

Practical application and experience: Tool for the safety of industrial machinery in reduced risk conditions

Aucourt B.¹, Chinniah Y.¹, Jocelyn S.², Bourbonnière R.³

¹ Department of Mathematical and Industrial Engineering, Polytechnique Montréal, 2500 chemin de Polytechnique, Montreal, Quebec, Canada H3T 1J4

² Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST), 505 de Maisonneuve Blvd. West, Montreal, Quebec, Canada H3A 3C2

³ Consultation Réal Bourbonnière, 58, rue de la Crête, Orford, Québec, J1X 0C5

barthelemy.aucourt@polymtl.ca

yuvn.chinniah@polymtl.ca

sabjoc@irsst.qc.ca

real@realbourbonniere.com

KEYWORDS: machinery, hazards, safe reduced speeds, safe contact pressures, safe energies

ABSTRACT

Industrial machines are known to possess many hazards such as mechanical, electrical, thermal, chemical, noise, vibration and ergonomics hazards. One machine safety design requirement found in the machinery directive in Europe, national or provincial legislation in North America, as well as national and international safety of machinery standards is the control mode for maintenance when guards or protective devices have to be displaced or removed. One of the conditions is that the control mode permits operation of the hazardous elements only in reduced risk conditions. These conditions present some challenges to designers and users alike. What are considered reduced risk conditions is open to interpretation. The objective of the tool presented in this paper is to help identify values for safe reduced speed, safe kinetic energy and safe contact pressure obtained from a previous study. In that study, values from the literature and from enterprises were obtained and the factors influencing the choice of values were investigated. The guide provides values for reduced speeds, force, energy, contact pressures, which varied widely. In the previous study, industrial visits showed that enterprises often use reduced speeds by switching to the reduced speed mode of operation without applying the other required conditions. Machines were modified to incorporate this mode of operation indicating some design problems. Some factors were identified which could guide the choice of values when the information is missing from standards or other documents. When a safety standard exists for a particular machine and values are specified in the standard, designers and users can use those values. However, if the machine has no safety standard, a risk assessment is needed before deciding which values to use. The tool will help designers and users of industrial machines for the safety of industrial machinery in reduced risk conditions.

1 INTRODUCTION

During maintenance, repair and adjustment activities, some workers may need to access the moving parts of industrial machinery by removing or disabling safeguards. Since the moving parts represent a hazard to the workers, various regulations and standards [1-4] provide requirements to secure those activities performed on machinery. For instance, the Machinery Directive [2], ISO 12100 [3] and CSA Z432 [4] require that moving parts, in such context, function under the following conditions:

“Where, for setting, teaching, process changeover, fault-finding, cleaning or maintenance of machinery, a guard has to be displaced or removed and/or a protective device has to be disabled, and where it is necessary for the purpose of these operations for the machinery or part of the machinery to be put into operation, the safety of the operator shall be achieved using a specific control mode which simultaneously

- a) disables all other control modes,
- b) permits operation of the hazardous elements only by continuous actuation of an enabling device, a two-hand control device or a hold-to-run control device,
- c) permits operation of the hazardous elements only in reduced risk conditions (for example, reduced speed, reduced power/force, step-by-step, for example, with a limited movement control device), and
- d) prevents any operation of hazardous functions by voluntary or involuntary action on the machine's sensors. [3]”.

Different sources such as type C standards (i.e. standards dedicated to a specific type of machine) dictate values, in addition to complementary measures, to help machine designers or users be compliant with the above requirements. Nevertheless, not all machines have a corresponding type C standard. Consequently, the designer or user can face difficulties when applying the wide variety of recommendations regarding reduced energy levels [5]. On top of that, since the values are sometimes contradictory from one source to another, they must be used in a specific context, i.e. based upon the machine type or with complementary measures. In the light of such variabilities and to facilitate the designers' and users' task, this paper presents a tool helping identify values and complementary measures to consider for safe reduced speed, safe kinetic energy and safe contact pressure for the design, the use or the modification of a machine.

2 RELEVANCE OF THE TOOL

In 2013 in the United States (US), 717 fatal work injuries resulted from a contact with objects and equipment [6]. Half of the accidents associated with moving parts of machines in the United Kingdom (UK) happened in printing presses and conveyors [7]. In 2005 in the US, 18% of workers fatally injured got harmed by contact with objects and equipment; that corresponds to over 1000 workers [8]. In the Netherlands annually, 400 accidents (21% of all accidents per year) occur due to contact with moving parts of machinery [9]. In Quebec (Canada), an analysis of 106 accidents related to moving parts of machinery revealed that many of them happened during maintenance (34,9%) and the handling of production disturbances (31,1 %) [10]. Some of the main causes were the easy access to moving parts of machinery, lack of safeguarding, bypassing safeguards and lack of risk assessment [10].

Risk is the combination of the probability of the harm and its severity [3]. The probability of the harm depends on 1) the exposure of person(s) to a hazard, 2) the occurrence of a hazardous event and 3) technical and human possibilities to avoid or limit the harm [3]. The reduced risk conditions allow for limiting the severity of harm and increasing the possibility of avoidance of harm. For instance, a slower speed gives more time to the worker to escape the moving part of a machine; if he cannot escape, the severity of the impact injury may be less. Unfortunately, reduced risk conditions present some challenges to designers and users [11]. Due to those challenges and the fact that many accidents happened while the workers were accessing some moving parts in a machine, a tool is needed to help the designers and users in their choices of reduced energy-related values.

3 METHOD

The following method has led to the tool:

- Collecting the recommended values for reduced risk conditions from the relevant literature (i.e. 55 standards, 14 guides, 11 scientific papers and two research reports);
- Visiting nine enterprises from various industrial sectors (manufacturing, pulp and paper, printing, horticulture and food processing) to:
 - ◇ understand and characterize the context surrounding the activities in reduced speed and energy mode,
 - ◇ note and measure, if possible, the values of reduced speed used,
 - ◇ understand the choices made and to identify the references used by enterprises and
 - ◇ determine the factors influencing the choice of values and the reasons for the use of those values [11].
- Writing a research report [5] detailing and analysing the outcome from the literature review as well as the visits;
- Extracting the essence of the report in the form a guide [12];
- Holding a consultation about the guide, with five engineers and one certified human resources professional, all coming from four partner organizations in the IRSST's network (www.irsst.qc.ca).

4 RESULTS: THE TOOL FOR REDUCED RISK CONDITIONS

The tool obtained is a decision assistance one, available in [12]. It consists of:

- a flowchart describing a procedure helping the designer or user choose a suitable value of speed, force, contact pressure or kinetic energy in a context of reduced risk conditions (Figure 1). That procedure is based on the comparison of the designer's or user's risk conditions with the one described in the standard corresponding to his machine. Considering those risk conditions in the decision making process is essential since a value cannot be used out of a precise context;
- benchmark-value tables listing the maximum thresholds regarding those values, as well as the other conditions required (complementary measures) for different types of industrial machines and sectors. The benchmark-value tables give simplified extracts from standards and other sources. Therefore, in order to capture the entire context of the complementary measures and further information surrounding the

benchmark values, one must look up the source where the information comes from. Tables 1 to 4 give some excerpts of the benchmark-value tables;

- some specifications about the following list of common factors to consider when determining if the reduced risk context to be designed or used is equivalent to that of the benchmark:
 - ◇ Contact surface, geometry of moving part (e.g., flat surface, edge)
 - ◇ Type of control (e.g., hold-to-run control, two-hand control, pulse control [automatic movement])
 - ◇ Guards within hazardous zone (e.g., nip point guards) or not
 - ◇ Sound/light signal at start-up or not
 - ◇ Accessibility of hazardous zone (e.g., impossible to reach or easy to get to)
 - ◇ Safe clearance or not
 - ◇ Relative position of movable/fixed parts (e.g., shearing areas)
 - ◇ Automatic reversal of movement in case of detection of part of worker's body
 - ◇ Emergency stop device nearby or not
 - ◇ Parts of body exposed.

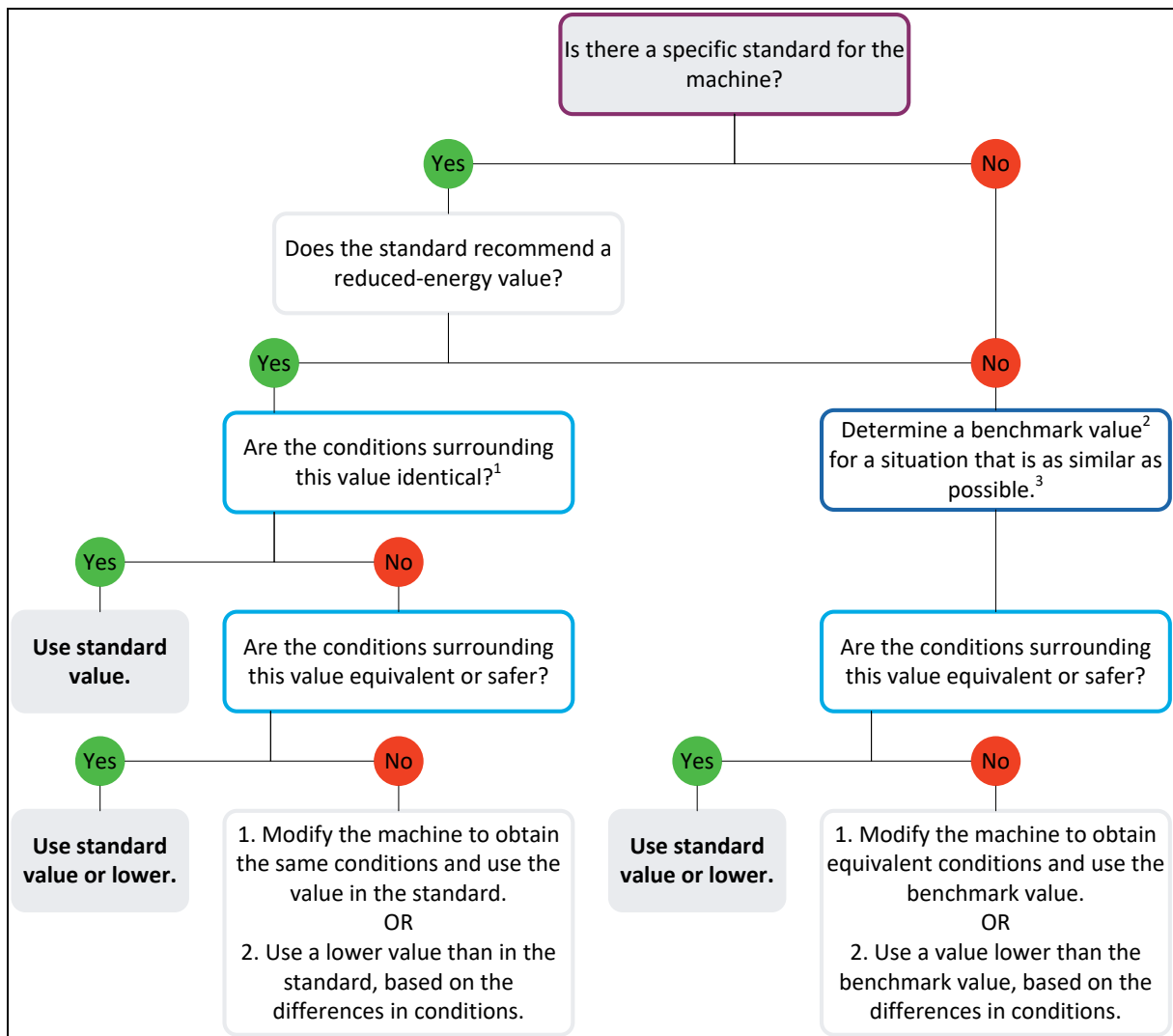


Figure 1. Flowchart of the proposed procedure for choosing the values in reduced risk conditions [12].

Legend:

¹ "An exhaustive, well-documented risk analysis makes it possible to closely compare the prescribed conditions around a value in relation to the conditions specific to the machine in question" [12].

² "The benchmark value may be taken from standards or other sources, such as technical guides" [12].

³ "Two situations are deemed similar when they involve the same hazard (type of danger) and when the other conditions are equivalent" [12].

The procedure in Figure 1 represents the core of the tool. The function of the benchmark-value tables as well as the specifications regarding the abovementioned common factors is to illustrate and precise the procedure. They do not intend to be used as is. Looking up the appropriate standards or other relevant documents is of paramount importance since those sources may contain critical information that exceeds the level of detail of the tool.

Table 1. Excerpt of the benchmark-value table for a reduced speed.


Industry/Machine	Hazard		Maximum speed	Other conditions required	Source
Manufacturing Machining centre	Impact, crushing, pinching/entrapment		33 mm/s	- Manual control with enabling switch	[13]

Table 2. Excerpt of the benchmark-value table for a reduced force.




Industry/Machine	Hazard		Maximum force	Other conditions required	Source
Printing Stapling machine Riveting machine	Crushing, shearing, cutting and severing		50 N	- Sensor to detect part of body (to apply force of work) - Control circuit reliability requirements	[14]

Table 3. Excerpt of the benchmark-value table for a reduced kinetic energy.

Industry/Machine	Hazard		Maximum kinetic energy*	Other conditions required	Source
General	Pinching/entrapment, crushing		4 J	- None	[15]
			10 J	- Automatic reversal of movement device	

*That energy is calculated at average speed of movement.

Table 4. Excerpt of the benchmark-value table for a reduced contact pressure.

Industry/Machine	Hazard		Maximum contact pressure	Other conditions required	Source
General General Packaging machine	Pinching/entrapment, crushing		25 N/cm ²	- None	[16-18]
			50 N/cm ²	- Automatic reversal of movement	

5 DISCUSSIONS AND CONCLUSION

The tool proposed for reduced risk conditions does not replace the standards to be compliant with nor a risk assessment. However, it is the life jacket of the designer or user in the ocean of values presented in the literature for reduced speed, force, kinetic energy and contact pressure conditions dedicated to machinery. Indeed, the guide helps the designer or user narrow his choice related to a given reduced speed, force, kinetic energy or contact pressure value. Thereafter, the designer or user must confirm that choice with the standard specific to the machine, based on a risk assessment comparing the risk conditions with the ones described in the standard. If that standard does not exist, performing a thorough risk assessment is even more important in that case.

6 REFERENCES

1. Publications du Québec, *Regulation respecting occupational health and safety*, Publications du Québec [Online] Available: <http://legisquebec.gouv.qc.ca/en/showdoc/cr/S-2.1,%20r.%2013>
2. EUR-Lex, *Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)* [Online] Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0042>
3. International Organization for Standardization (ISO), *Safety of machinery — General principles for design — Risk assessment and risk reduction*, ISO, ISO 12100:2010, Geneva, Swiss, 2010.
4. Association canadienne de normalisation (CSA), *Protection des machines*, CSA, CSA Z432-04, 2009.
5. Chinniah Y., Aucourt B., Bourbonnière R., *Study of Machine Safety for Reduced-Speed or Reduced-Force Work*, Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST), Montreal, Quebec, Canada, Research Report R-956, 2017 [Online] Available: <http://www.irsst.qc.ca/media/documents/PubIRSST/R-956.pdf?v=2018-07-18>
6. Bureau of Labor Statistics (BLS), *National Census of Fatal Occupational Injuries in 2013*, BLS, United States, 2014.
7. Health & Safety Executive (HSE), *Analysis of RIDDOR Machinery Accidents in the UK Printing and Publishing Industries, 2003–2004*, United Kingdom, Report HSL/2006/83, 2006.
8. Bulzacchelli M.T., Vernick J.S., Sorock G.S., Webster D.W., Lees P.S.J., *Circumstances of fatal lockout/tagout related injuries in manufacturing*, American Journal of Industrial Medicine, 51(2008), 728–734.
9. Bellamy L.J., Ale B.J.M., Geyer T.A.W., Goossens L.H.J., Hale A.R., Oh J., Mud M., Bloemhof A., Papazoglou I.A., Whiston J.Y., *Storybuilder – a tool for the analysis of accident reports*, Reliability Engineering and System Safety, 92(2007), 735–744.
10. Chinniah Y., *Analysis and prevention of serious and fatal accidents related to moving parts of machinery*, Safety Science, 75(2015), 163–173.
11. Chinniah Y., Aucourt B., Bourbonnière R., *Safety of industrial machinery in reduced risk conditions*, Safety Science, 93(2017), 152–161.
12. Aucourt B., Chinniah Y., *Machine safety and reduced-energy operating mode – Determining safe values*, Institut de recherche Robert-Sauvé en santé et en sécurité du travail (IRSST), Montreal, Quebec, Canada, Guide RG-1026, 2018 [Online] Available: <http://www.irsst.qc.ca/publications-et-outils/publication/i/100998/n/securete-machines-modes-fonctionnement-energie-reduite-choix-valeurs-securitaires>
13. Association française de normalisation (AFNOR), *Machines-outils : sécurité : centres d'usinage*, AFNOR, NF EN 12417+A2:2009, La Plaine Saint-Denis, France, 2009.
14. Association française de normalisation (AFNOR), *Sécurité des machines : prescriptions de sécurité pour la conception et la construction de machines d'impression et de transformation du papier. Partie 4, machines à relier les livres, machines de transformation et de finitions du papier*, AFNOR, NF EN 1010-4+A1:2010, La Plaine Saint-Denis, France, 2010.
15. Blaise J.C., Daillie-Lefèvre B., Lupin H., Marsot J., Wélitz G., *Sécurité des équipements de travail : prévention des risques mécaniques*, Institut national de recherche et de sécurité (INRS), Paris, France, 2012 [Online] Available: <http://www.inrs.fr/accueil/produits/mediatheque/doc/publications.html?refINRS=ED%206122>
16. International Organization for Standardization (ISO), *Safety of machinery – Guards – General requirements for the design and construction of fixed and movable guards*, ISO, ISO 14120:2002, Geneva, Swiss, 2002.
17. Association internationale de sécurité sociale (AISS), *Prévention des risques mécaniques : solutions pratiques*, AISS, Genève, Suisse, 1994.
18. Association française de normalisation (AFNOR), *Sécurité des machines d'emballage. Partie 7, machines de groupe et d'emballage secondaire*, AFNOR, NF EN 415-7+A1:2008, La Plaine Saint-Denis, France, 2008.

Normative surveillance for Occupational Safety and Health

Kieckbusch R.E.¹, Santos A.C.², Souza, L.W³

¹ National Confederation of Industry - Brazil (CNI) – SBN - Quadra 1 - Bloco C, Ed. Roberto Simonsen, Brasília – DF, CEP 70040-903 - Brazil

² Brasilia University (UnB) – Universidade de Brasília- UnB - Faculdade de Tecnologia - Laboratório Aberto de Brasília - Campus Darcy Ribeiro Asa Norte - Brasília DF, CEP 70904-970 - Brazil

³ Brasilia University (UnB) – Universidade de Brasília- UnB - Faculdade de Tecnologia – Laboratório Aberto de Brasília - Campus Darcy Ribeiro Asa Norte - Brasília DF, CEP 70904-970 - Brazil

rkieck@cni.com.br
andreasantos@unb.br
luandawaleska@gmail.com

Normative surveillance is to accompany the drafting and revision of legal standards and it's useful to companies intending to anticipate imminent changes in legislation. With the application of the environmental scanning, normative vigilance can lead to the gain of competitive advantage, because it allows the proper risk management. This practice is applicable to product planning, that is the initial stage of the product development. In this stage, which is subject to uncertainties, the legislation that determines the project must be considered, including Safety and Health at Work standards. So, an exploratory research was carried out, with bibliographical survey mostly virtual, in order to elucidate the regulation of Occupational Safety and Health in different countries and its use in the product planning. The countries were chosen according to the value of Gross Domestic Product. The information necessary for the development of this work was extracted from the database of the International Labor Organization and the official electronic websites of the countries enabled. Then, the normative procedures, the regulated risks and the ratified conventions regarding occupational safety for the countries analysed were explained and compared. The main data were available only for United States, Brazil, Canada and Mexico. Among these, Brazil is the country in which the time for adaptation to changes in labour regulatory norms is smaller and it is also the country in which more changes of such norms occurred in the last ten years.

A simulation-based approach for work system compatibility assessment using time allowances

El Mouayni I.1, Etienne A.1, Siadat A.1, Dantan J.-Y.1, Lux A.2

1 ENSAM, Ecole Nationale Supérieure des Arts et Métiers 4, rue Augustin Fresnel - 57078 Metz - Cedex 3, France

2 Institut national de recherche et de sécurité (INRS) – 1, rue du Morvan – CS 60027 – 54519 Vandœuvre Cedex – France

ismail.elmouayni@ensam.eu

KEYWORDS: work system compatibility, flow simulation, human factor, time allowances

ABSTRACT

Assessing the work system compatibility during its design phases is paramount for both, accurate productivity assessment and risk factors elicitation. These risks occur due to unbalanced work situations, where job demands exceed the worker's capacity causing incompatibility in work system. One of the reasons of this is the non-consideration variabilities during the work system design phases, mainly, workflow random variation and human factors. Accordingly, this paper proposes a new approach for work system compatibility assessment using the concept of time allowances. These allowances give operators the possibility to cope with variabilities leading to a better compatibility. Assuming that time allowances deficit is work system incompatibility indicator, this article details a simulation model that can be used to assess time allowances. To uphold the paper's proposal, the simulation model is used to investigate a production line configuration and assess the actual time allowances granted to human operators. Although simulation showed that the configuration subject of the study had positive allowances, these ones seem to be variable between workstations indicating partial system compatibility.

1 INTRODUCTION

Ensuring the work system compatibility, i.e. the technical sub-system and social sub-system adequacy is paramount to provide a sustainable productivity. Systems where this compatibility isn't investigated during the work system design phases may lead to unbalanced jobs where productivity is over estimated [1] and work demands exceeds the worker's capacity, leading to several risk factors [2].

In the past two decades, the macro-ergonomic approach has introduced the significance of nonphysical environment conditions such as organizational, social and technical factors [3]. These conditions are relevant to the work load and need to be considered. For example, the Balance Theory of Job Design, from the field of job stress research, maintains that balancing elements of the job (i.e. technology, task, environment, organization) leads to stress reduction [4]. This theory, however, did not demonstrate how the different elements of the job interact to produce the intended balance.

Instead of looking for perfect balance and by admitting that designing systems that are adapted to the future occupational activity of human operators, especially with consideration variabilities is hardly achievable, another approach consists in granting allowances or margins of maneuver to ensure the work system compatibility.

Developed in the field of French speaking ergonomics, the concept of margin of maneuver is recommended to ensure the job balance, by pointing the importance of considering variabilities in work situation, deterministic, random and non-random ones. It consists in giving the operators enough flexibility and freedom to develop different ways of working. This allows them to face variations in work situation and to meet the work demands without compromising their health [5]. This approach has been for several years a strong lever for preventing physical and psychological risk factors [2], [6].

In the other hand, allowances are a similar concept that was mainly introduced by industrial engineers as a substantial element of work standards. It concerns mainly time dimension. Time allowances are time intended to provide worker with the opportunity to recover from fatigue (relaxation allowances) and to cope with delays and abnormality (contingency allowances). The relation between the standard time (T_s), the normal time (T_n) and allowances (denoted A) is given by (1) [7]:

$$T_n = \frac{T_s}{1 + A} \quad (1)$$

Several empirical methods were proposed to determine the recovery allowances needed in a specific work situation by evaluating fatigue stressors in a job. The International Labour Office (ILO) [8] in his last

publication, proposed tables regarding twelve stress factors (force; posture; monotony; concentration; eye strain; vibration; noise; restrictive clothing; temperature; wet; dirt; cycle time) that can be used assess the level of these factors and accordingly, to determine the amount of time that must be granted for fatigue recovery.

In [9], the method proposed by Corman is presented. It represents a basic yardstick which consist in considering a set of then factors that affect fatigue (temperature; air supply; humidity; noise; duration of job; cycle repetitiveness; physical, mental and visual demand). The method consists on analysing a job and quantifying these factors. This is achieved by determining the degree which best characterizes the job on that factor. Corman gives a detailed description of each degree. The total points is then summed and converted into percentage of time for allowances using a conversion table. Another method which is somehow similar to Corman's is proposed by Page [9]. The method gives a list of allowance factors to be assessed. However, these factors lacks a clear definition making difficult its consistent application in workplaces [9].

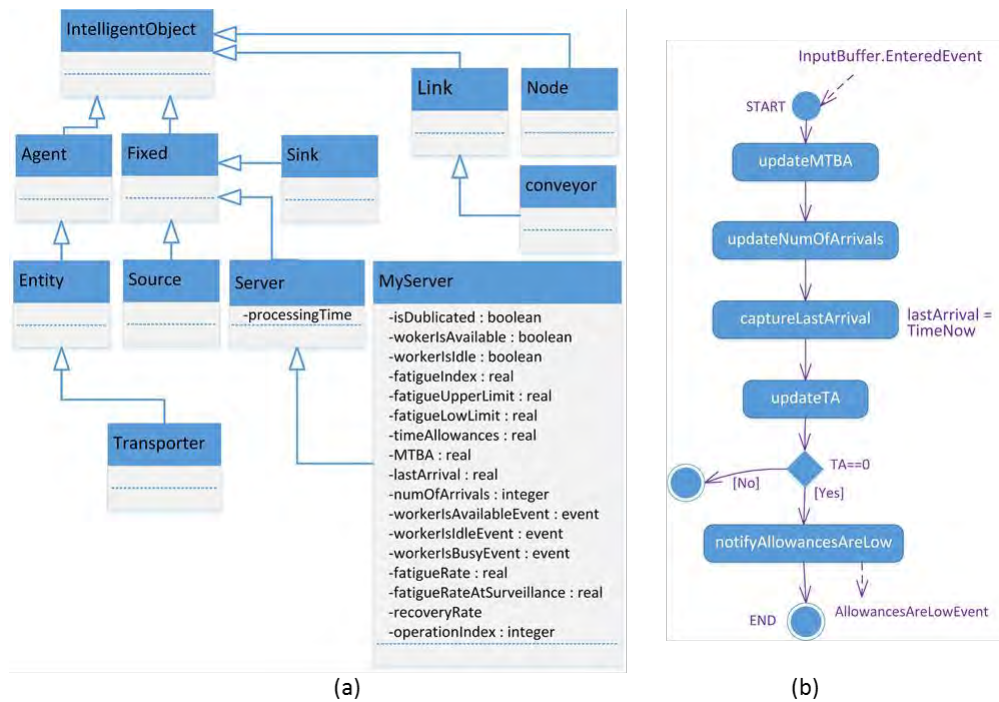


Figure 1. (a) Simulation structural modeling (UML class diagram). (b) Time allowances update process.

Nevertheless, these methods do not consider contingencies. Variable workflow up to a certain level may lead to allowances deficit. This implies unbalanced work situations where isn't enough time for fatigue recovery and temporal pression may lead to several risk factors. Accordingly, this article proposes a simulation-based method for allowances assessment by considering workflow variation. An allowances deficit is considered as incompatibility indicator. For this purpose, the section 2 presents the simulation model developed. Section 3 address a case study. The last section is about discussion, conclusions and future works.

2 PROPOSED METHOD

To achieve production system evaluation during design phases, as proposed in [10], simulation can be used. It is a commonly used technique for manufacturing system design and manufacturing operations management. It helps designers to overcome the system complexity and doesn't demand an explicit mathematical model to predict the system behaviour [11]. Simulations may be time consuming and expensive. Nevertheless, such techniques are often used for trial and error approach to design [12], [13] and help the designer to compare and evaluate several configurations during the design process.

Simulation consists in developing a conceptual model meant to be implemented into a simulation tool or code (called implemented model). The conceptual model is developed following the principal of a theory such as differential equations or discreet systems theories. These theories provide basic elements for system behaviour specification such as modelling elements (variables, equation, entities...) and behavioural description elements (equations, automata ...). The implemented model is then used to generate artificial behaviour using a simulation mechanism. Activities scan, events scheduling or processes interactions [13] are ones of the most used ones in the case of discreet systems. The simulated behaviour is then transposed to assess the actual system. The following section details the simulation model used to assess allowances in this paper.

2.1 Simulation conceptual modelling

To develop a simulation model, two views must be considered: structure views and behavioural views [14]. The structure view specifies the possible relations or interactions between the system entities. The behavioural view details entities behaviours. To conduct simulation, the software SIMIO is used [15]. As shown in Figure 1-a, SIMIO has a simulation model with predefined entities. There are four entities that can be used and instantiated to construct a simulation model: Agents, Fixed entities, Links and Nodes. To add relevant attributes to the problem tackled in this paper, a new entity called “MyServer” is added using heritage process. One of the attribute added to the predefined model is fatigueIndex. It is a state variable containing the worker’s fatigue level. The fatigue is modelled using an exponential variation as recommended in [16]. Its expression is given by (2):

$$F_{i+1} = \begin{cases} 1 - (1 - F_i) \cdot e^{-\lambda \cdot dt_i} & \text{if worker IsBusy} \\ F_i \cdot e^{-\mu \cdot dt_i} & \text{otherwise} \end{cases} \quad (2)$$

F denotes the fatigue index. The parameters λ and μ are respectively the fatigue and recovery rates. We considered two fatigues rates: a fatigue rate when performing a task and another rate when operator performs automatic operations supervision (fatigueAtSurveillance). The attribute timeAllowances (denoted TA) indicates the actual allowances in a given workstation. These allowances are computed using (3):

$$TA_n = (S_{\max} - S_n) \cdot MTBE_n \quad (3)$$

The parameter Smax designates the input buffer capacity of the server (InputBuffer.Capacity). The parameter Sn designates the number of parts or products contained in that buffer when processing the part n (InputBuffer.Content). MTBE designates the Mean Time Between job Arrival events computed dynamically using (4):

$$MTBA_n = \left(1 + \frac{1}{n}\right) \cdot MTBA_{n-1} + \frac{T_{A(n)} - T_{A(n-1)}}{n} \quad (4)$$

Where TA(n) is the nth part arrival date supplied by SIMIO model attribute TimeNow and TA(n-1) corresponds to the lastArrival attribute. Other attributes, especially events are also added and used for behavioral interactions which are described in the next section.

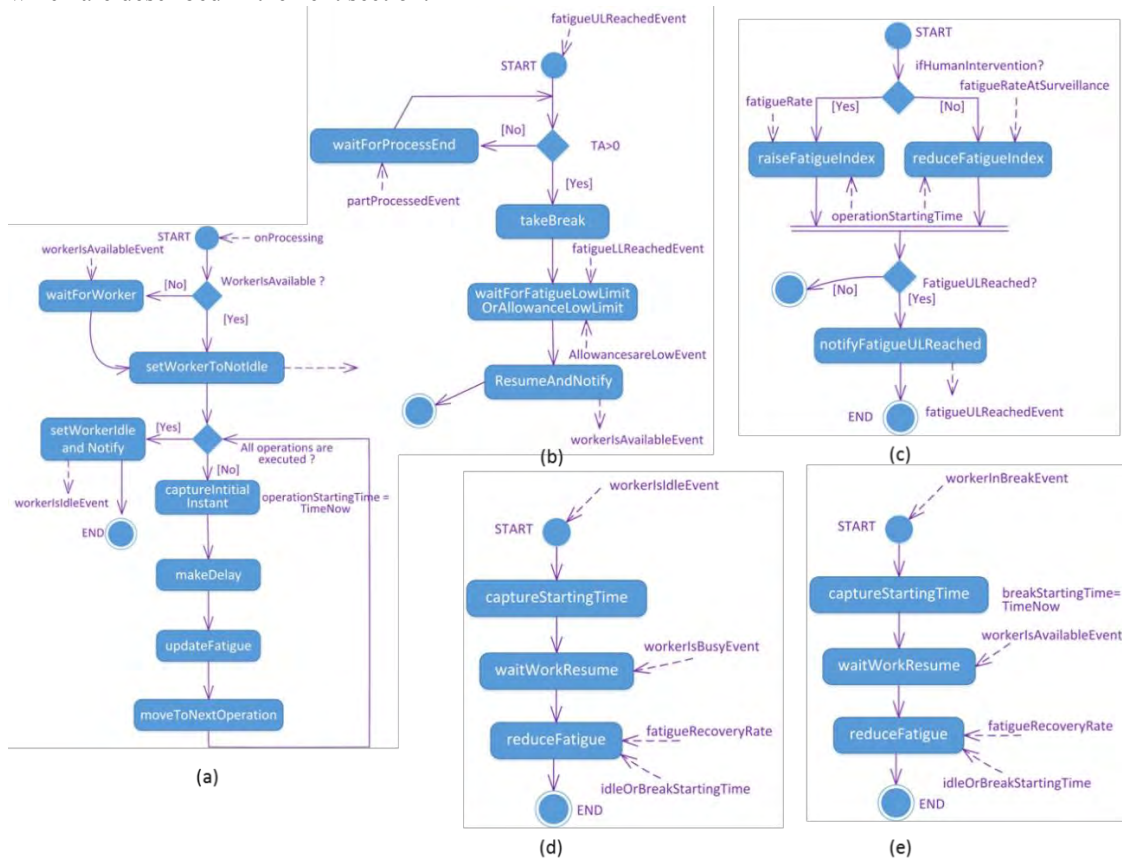


Figure 2. (a) Task processing model. (b) Time allowances use modelling. (c) Fatigue update under task processing. (d) Fatigue update under idle state. (e) Fatigue update under break state.

2.2 Simulation behavioural modelling

In this section, behavioural modelling used for simulation is detailed. SIMIO proposes process-based view to model the entities' behaviour. To achieve this, there are two ways: defining global processes under simulation model that can be used by all entities. These processes must be linked to predefined triggers through user interface. Example of such triggers are "on entered", "on processed" or "on exited" related to ModelEntity entering, being processed or exiting the server. ModelEntity is the mobile entity used to model parts in movement between workstations. The second approach consist in incorporating these processes under an entity and linking them to specific events, or to predefined processors using execute step. As the processes need to be modelled are only linked to "MyServer", to avoid inappropriate access, the second approach is adopted.

The first behaviour modelled aims to update time allowances when a part is received (Figure 1-b). When a "ModelEntity" enters the input buffer, this process recomputes MTBA, numOfArrivals and timeAllowances using (3) and (4). The Figure 3 details the task processing model. This process is activated when the predefined SIMIO event onProcessing is fired. It starts by checking the worker availability and wait for him if not the case. Then the worker's state "workerIsIdle" is set to false. A loop is then entered and serials delays corresponding to the operations' processing times are made. After each delay, the fatigue index is updated. When all operations are processed, workerIsIdleEvent is fired and the workerIsIdle state is set to true

This process shown in Figure 2-c is used to update fatigue when an operation is processed. It starts by checking if there is human intervention when processing an operation. Depending on the value of this attribute, a fatigue rate (fatigueRate or FatigueRateAtSurveillance) is used to update the fatigue index using (2). After updating the fatigue, the process checks if the fatigue upper limit is reached (the attribute fatigueUpperLimit). If it is the case, an event is fired to notify this.

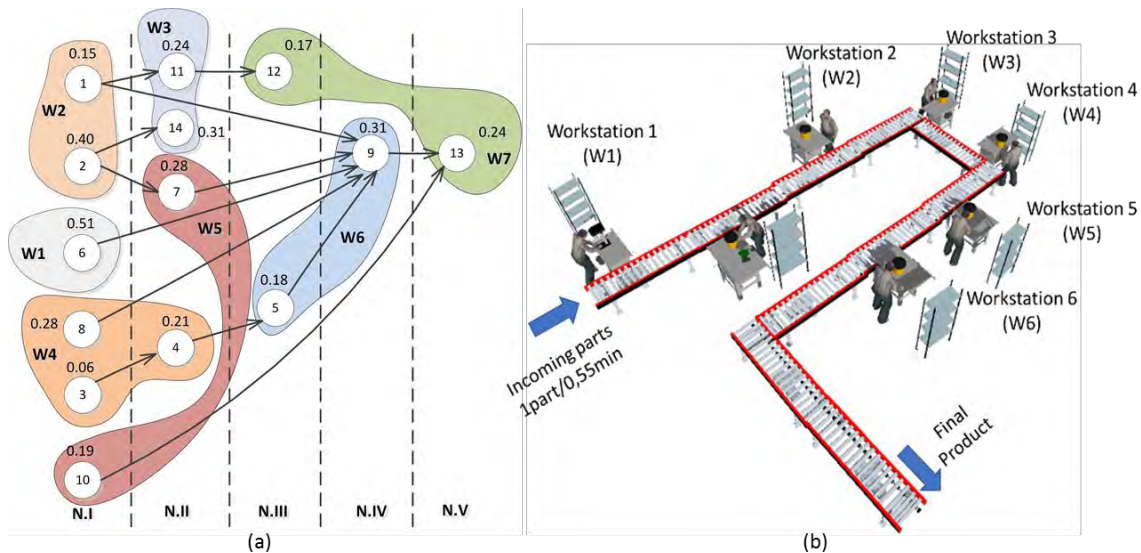


Figure 3. (a) Line balancing using Kilbridge & Wester method. (b) Production system physical configuration.

When fatigue reaches the upper limit, the process shown in Figure 2-b catches "fatigueULReachedEvent". This event activates this process. If the worker has allowances ($TA > 0$), then he can take a small unplanned break, otherwise, he will process the current task and try again in the next cycle if these allowances are improved. When fatigue index reaches a low level, or in the case of lacking time allowances to carry on the break, worker resumes his work and the process fires workerIsAvailableEvent.

The Figure 2-d and 2-e describes how fatigue is updated under idle and break states. Depending on the worker state, these two processes reduce fatigue until the appropriate event is fired. Under Idle state, the process is closed when worker get busy. Under break state, the event caught is worker is available, fired by allowance use process. The Simulation model detailed above is implemented in SIMIO and used to address the case study detailed in the next section.

3 CASE STUDY

The case study addressed in this section is about a blinder assembly. 14 operations are required to assemble one product. Their precedence constraints and processing time are given in Table 1. These processing times are assumed to follow a normal distribution with a standard deviation equal to 0.01. To achieve line balancing,

Kilbridge & Wester method is used. The cycle time required with consideration of line reliability is set to 0.55min.

Table 3. Operations' processing times.

Operation	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Precedency				3	4		2		1-5-6-7-8		1	11	9	2
Processing time (min)	0,2	0,4	0	0	0,18	0,51	0,28	0,28	0,31	0,2	0,24	0,14	0,26	0,17

The Kilbridge and Wester method consist in defining operations levels depending on the number of predecessors. Level 1 contains the operations with 0 predecessors, level 2 contains operations with one predecessor etc. For operations selection, operations with the lowest level and highest processing times have the priority. When operations gathering reached the maximum time less than the cycle time, a new workstation is opened. The Figure 3-a shows the line balancing obtained. Notice that the balancing efficiency is equal to $1 - E_b = 0.92\%$, where E_b is given by:

$$E_b = 1 - \frac{T_{wc}}{m \cdot T_{sl}} \tag{5}$$

Where T_{wc} is the work content. It is equal to the sum of the processing times. T_{sl} is the processing time at the slowest workstation and m is the number of workstations. The analyze of fatigue stressors in each workstation and the use of ILO [8] tables gives a score between 20pt and 22pt. Which implies relaxation allowances equal to 13%. Which means that 13% of standard time must be used for breaks. Accordingly, the work schedule is set as described in Table 2:

Table 4. Breaks scheduling.

8h-9h50	9h50-10h05	10h05-12h	12h-12h30	12h30-14h20	14h20-14h35	14h35-16h30
Work	Break	Work	Break	Work	Break	Work

The fatigue and recovery rates are determined using (6) and (7). Where T_{fb} is time to first break, A is the time allowances in %, and $1 - \delta_f$ is pseudo fatigued state and δ_r is pseudo-recovered state. These two parameters are introduced as the fatigue index can never reach 1 or 0. These equations are obtained using (2) and by considering that working T_{fb} continually leads to pseudo-fatigued state and resting $A \cdot T_{fb}$ leads to total recovery.

$$\lambda = \left(\frac{1 + A}{T_{fb}} \right) \cdot \ln \left(\frac{1}{\delta_f} \right) \tag{6}$$

$$\mu = \frac{1}{T_{fb}} \cdot \left(1 + \frac{1}{A} \right) \cdot \ln \left(\frac{1 + \delta_f}{\delta_r} \right) \tag{7}$$

For $T_{fb} = 120$ min, $\delta_f = \delta_r = 10 - 2$ it is found that $\lambda = 1.27 \cdot 10^{-2}$ min⁻¹ and $\mu = 0.209$ min⁻¹.

The Figure 3-b describes the physical design of the production line. To cope with flow variation and give operators allowances to cope with contingencies, an input buffer with a capacity of 3 at each workstation is considered. This gives allowances delay of 1.65 min. the conveyors speed is set to 2 m.s⁻¹.

Table 5. Time allowances obtained by simulation.

Workstation	W1	W2	W3	W4	W5	W6	W7	Average
Average time allowance (min)	0,36	0,33	0,66	1,21	1,22	1,23	1,23	0,89
standard deviation	0,38	0,44	0,55	0,1	0,13	0,17	0,21	0,28

The part arrivals follow a normal distribution with a mean equal to 0.55 min and a standard deviation equal to 0.01. Only random variations are considered (part arrivals and processing time variation). Abnormal variations such as machine breaks are not considered. The table 3 details the allowances in the production system estimated using simulation. It also gave the number of throughputs generated by the system (827).

4 DISSCUSSION AND CONCLUSIONS

The simulation results show that time allowances (table 3) in production line are greater than 0, giving operators the opportunity to cope with slight contingencies and extra time for relaxation. Nevertheless, these time

allowances vary among workstations. The two first workstations have lower allowances in comparison with the four others. This has a significant impact on fatigue. As shown on Figure 4, the fatigue index in W1 and W2 is higher than the fatigue index of the rest of the workstations. The time allowances being greater, the workers of these workstations could have unplanned small breaks to recover from fatigue. In the other hand. Being consumed by the workflow variation, the W1 and W2 didn't have enough allowances and worker couldn't have these breaks.

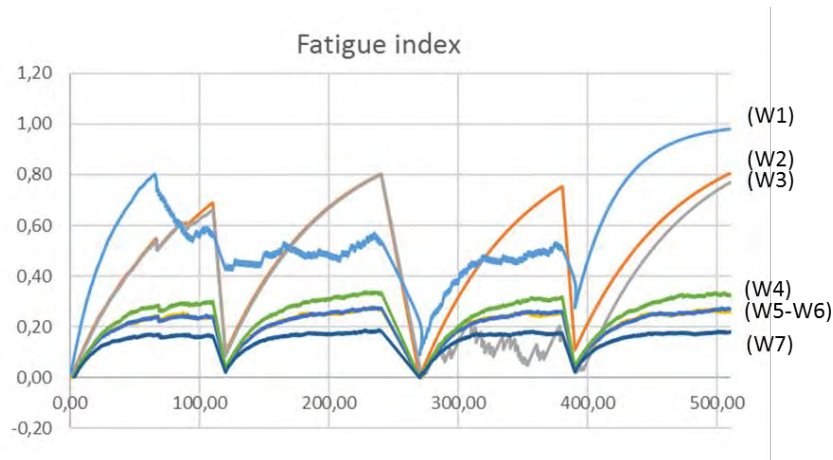


Figure 4. Fatigue index variation.

Hence, the simulation shows that balancing workload between workstations by considering nominal processing time is not enough to ensure efficient and effective balance. Variations such as randomness in processing times and job arrivals lead to unbalanced allowances distribution, causing disparity in workers fatigue and leading to work system partial incompatibility. Moreover, this disturbance may be more pronounced due to other variability aspects such as difference in workers capacities due to age, experience and physical abilities. Therefore, it is important to consider these variabilities when balancing a system. Beside using nominal processing times, random variations and human factors should be integrated. Simulation based methods and simulation-based optimization are adapted tools to consider these elements and particularly, when addressing simple line balancing problems.

5 REFERENCES

1. Baines, S. Mason, P.-O. Siebers, et J. Ladbrook, « Humans: the missing link in manufacturing simulation? », *Simul. Model. Pract. Theory*, vol. 12, no 7-8, p. 515-526, nov. 2004.
2. Lanfranchi, J. B. Duveau, A. « Explicative models of musculoskeletal disorders (MSD): biomechanical and psychosocial factors to clinical analysis of ergonomics », *Rev. Eur. Psychol. Appliquée*, vol. 58, p. 201-213, 2008.
3. Hendrick, H. W. « Future directions in macroergonomics », *Ergonomics*, vol. 38, no 8, p. 1617-1624, août 1995.
4. Smith, M. J. Sainfort, P. C. « A balance theory of job design for stress reduction », *Int. J. Ind. Ergon.*, vol. 4, no 1, p. 67-79, juill. 1989.
5. Durand, M. J. Vézina, N. Baril, R. Loisel, P. Richard, M. C. Ngomo, S. « Margin of Manoeuvre Indicators in the Workplace During the Rehabilitation Process: A Qualitative Analysis », *J. Occup. Rehabil.*, vol. 19, no 2, p. 194-202, juin 2009.
6. Coutarel, F. Daniellou, F. Dugué, B. « La prévention des troubles musculo-squelettiques: quelques enjeux épistémologiques », *Activités*, vol. 2, no 2-1, 2005.
7. Mital, A. Bishu, R. R. Manjunath, S. G. « Review and evaluation of techniques for determining fatigue allowances », *Int. J. Ind. Ergon.*, vol. 8, no 2, p. 165-178, 1991.
8. Kanawaty G. International Labour Office, *Introduction to work study*. Geneva: International Labour Office, 1992.
9. Lund J. Mericle, K. S. « Determining fatigue allowances for grocery order selectors », *Appl. Ergon.*, vol. 31, no 1, p. 15-24, janv. 2000.
10. Baines T. S. Kay, J. M. « Human performance modelling as an aid in the process of manufacturing system design: A pilot study », *Int. J. Prod. Res.*, vol. 40, no 10, p. 2321-2334, janv. 2002.
11. Negahban, A. Smith, J. S. « Simulation for manufacturing system design and operation: Literature review and analysis », *J. Manuf. Syst.*, vol. 33, no 2, p. 241-261, avr. 2014.
12. Banks, J. *Handbook of simulation principles methodology advances, application and practice*, 1998e éd. Engineering and Management Press EMP., 1998.

Poster session

13. Pidd, M. *Computer Simulation in Management Science*, 5 edition. Chichester, England ; Hoboken, NJ: Wiley, 2004.
14. Arbez G. Birta, L.G. « ABCmod: a conceptual modelling framework for discrete event dynamic systems », in *Proceedings of the 2007 Summer Computer Simulation Conference*, 2007, p. 987–995.
15. Simio, « Simio », 2018. [En ligne]. Disponible sur: <https://www.simio.com/index.php>. [Consulté le: 16-sept-2018].
16. Jaber, M.Y. Givi, Z. S. Neumann, W. P. « Incorporating human fatigue and recovery into the learning forgetting process », *Appl. Math. Model.*, vol. Vol. 37, no 12-13, p. 7287-7299, 2013.