Notes techniques

SÉCURITÉ DES MACHINES : LE « RISQUE CYBER » COMME RISQUE ÉMERGENT ?

Avec « l'industrie du futur » et la connexion des machines au réseau internet, le « risque cyber » est un risque émergent pour les salariés en poste au voisinage d'un équipement de travail vulnérable. Cet article propose de donner des éléments de contexte sur la cybersécurité et de montrer pourquoi il est nécessaire de se sensibiliser à ce risque et à sa prévention. La sécurité des machines, tant en matière de conception que d'utilisation, est concernée. Une analyse est proposée dans le cadre de la directive européenne « Machines » 2006/42/CE et de la protection des salariés. Elle vise à apporter des éléments méthodologiques pour prévenir le « risque cyber » et ses conséquences sur la santé et la sécurité des opérateurs.

PASCAL LAMY, INRS, département Ingénierie des équipements de travail

À l'origine, la cybersécurité s'est développée afin de garantir la non corruption des données traitées par les systèmes d'information. Le champ d'application se réduisait alors à ce qu'on appelle l'IT (*Informational Technology*). De par leur faible niveau (ou l'absence) de connexion aux réseaux ouverts, les systèmes industriels ont longtemps été plus ou moins épargnés et les industriels étaient moins préoccupés par ce risque. Toutefois, la situation évolue.

Tout d'abord, concernant les machines et équipements de travail, l'émergence récente du concept « d'industrie du futur » ou « Industrie 4.0 » [1] met en exergue et favorise la connexion des systèmes industriels mais aussi des produits et des opérateurs. Un accès, jusqu'au plus bas niveau des composants des machines (capteurs, actionneurs, composants de sécurité ou automates de sécurité) est ainsi rendu possible du fait de leur connexion au réseau du système d'information de l'entreprise, lui-même relié à l'extérieur par l'internet voire de leur connexion directe au réseau. Toutes ces évolutions facilitent des intrusions numériques.

Une autre évolution est perceptible : diverses attaques qui ont parfois été largement médiatisées ont déclenché une prise de conscience des acteurs autour de ce risque. Ainsi, en France, une réglementation [2] s'est mise en place sur ces risques, qui place l'Anssi[1] au cœur du dispositif. Cette agence propose sur son site de nombreux documents ou guides traitant de la cybersécurité.

Cette réglementation concerne les « Opérateurs d'importance vitale » (OIV), dont les activités sont indispensables au bon fonctionnement et à la survie de la nation et les Opérateurs de service essentiel (OSE ayant un impact essentiel pour l'économie et la société). Pour les OIV, cette réglementation requiert une réflexion sur l'impact de l'arrêt du processus industriel ou de la destruction de l'installation, notamment dans le cadre de la loi sur les risques industriels dite loi Bachelot [3] (transposition de la directive « Seveso » [4]). Le point de vue considéré est principalement celui de la disponibilité et de l'intégrité du système de production mais aussi celui de la confidentialité des données. La liste des OIV concernés par cette réglementation (et devant se déclarer auprès de l'Anssi) n'est pas disponible publiquement. Cependant, actuellement, on peut constater que pour les systèmes industriels, les entreprises qui mènent des actions sur ce sujet sont en général de grands groupes tels que la RATP, EDF, DGA (Direction générale de l'armement).

Cet article a pour objet d'apporter un éclairage sur le risque « cyber », du point de vue de la sécurité en lien avec le risque machine, pour le salarié au poste de travail utilisant ou supervisant des machines. Il peut concerner les concepteurs de machines et les utilisateurs/exploitants de tels équipements.

RÉSUMÉ

L'émergence du concept d'« industrie du futur » a mis en exergue la connexion des systèmes de production, soit au système d'information de l'entreprise soit directement via internet. Ceci facilite les intrusions voire les attaques numériques pouvant impacter la sécurité des systèmes industriels. Cet article a pour objectif de faire le point sur ce risque pour la sécurité des machines et donc des salariés. Il détaille le périmètre de la cybersécurité, qui recouvre des dispositions visant à se protéger d'incidents ou de malveillances puis discute de l'impact d'attaques numériques sur la sécurité des opérateurs intervenant auprès de ces machines. L'article aborde également la prévention du « cyber-risque », qui repose sur une évaluation des vulnérabilités de l'entreprise et des menaces auxquelles elle est exposée, évaluation qui permet d'identifier les événements pouvant remettre en cause la sûreté de fonctionnement des installations industrielles. Les étapes clés de cette analyse et les méthodes pour y parvenir sont détaillées dans l'article, ainsi que les mesures de prévention pouvant être mises en place.

Machine safety: the "cyber risk" as an emerging risk?

With "the industry of the future" and the connection of machines to the Internet, "cyber risk" is an emerging risk for employees working in the neighborhood of vulnerable work equipment. This article proposes to give elements of context on cybersecurity, and to show why it is necessary to be aware of this risk and its prevention. Machine safety, both in terms of design and of use in process, is concerned. An analysis is proposed in the context of the European Machinery Directive 2006/42 / EC and the protection of employees. It aims to provide methodological elements to prevent the "cyber risk" and its consequences on the health and safety of operators.

« Cybersécurité » : quel périmètre ?

Dans la littérature, la « cybersécurité » est principalement abordée selon le point de vue d'actes malveillants ou d'attaques, cadre qui sera retenu dans cet article. Avec le développement des réseaux numériques industriels et l'accès à internet des installations industrielles, la cybersécurité concerne à présent les équipements industriels, notamment dans le cadre de l'Industrie du futur. Pour les moyens de production, le champ d'application s'élargit à ce qu'on appellera l'OT (*Operational Technology*).

La cybersécurité désigne l'ensemble des dispositions visant à se protéger de tels actes par vecteur numérique (qu'il s'agisse pour l'attaquant, d'utiliser par exemple le réseau informatique/internet ou d'un autre support comme une clé USB contenant un malware), ciblant la disponibilité ou l'intégrité des systèmes [5]. On cherche alors à garantir la continuité de la production et au sens large, la sécurité du personnel voire des populations pour des installations à risque. Entrent également dans ce périmètre d'actes malveillants, des mesures permettant d'assurer la sécurité ou la confidentialité des données.

Remarque : Les négligences humaines, qui ne sont pas des actions volontaires ou malveillantes (les intervenants n'ayant pas la volonté de nuire) [6] mais qui peuvent toutefois rendre le système inopérant, ne sont pas abordées ici.

Le « risque cyber » pour les systèmes industriels : une réalité tangible

Chaque année, de nombreux incidents liés à des cyberattaques touchent les systèmes industriels. Aux Etats-Unis, le NCCIC comptabilise ainsi presque 300 incidents chaque année sur les systèmes de contrôle industriels. En France, l'Anssi évoque des actions de sabotage et une recrudescence de tentatives de déstabilisation. Elles se caractérisent par des attaques de plus en plus sophistiquées d'ampleur croissante. L'Anssi note une montée en compétences et en ressources des acteurs non-étatiques (organisation terroriste ou mafieuse par exemple).

Pour les systèmes industriels, le Clusif[2] a réalisé en avril 2017 un document de sensibilisation à la cybersécurité en environnement industriel [7]. Un historique des attaques sur les systèmes industriels est disponible dans [8]. Parmi les cyberattaques qui ont particulièrement attiré l'attention :

- en 2014, une campagne de mails infectés qui auront conduits à la prise de contrôle du système de production d'une aciérie ayant mené à un arrêt de production incontrôlé et de graves dommages matériels sur l'installation ;

→

- en 2015, le *malware BlackEnergy* avait entraîné une coupure électrique pour 80 000 foyers en Ukraine, avec une indisponibilité de 3 à 6 heures ;
- en 2017, des attaques par « rançongiciel » comme *WannaCry* ont touché de nombreux secteurs. Renault a ainsi subi des arrêts de production sur des chaînes de montage automobile. Une autre attaque de ce type (NotPetya) a eu des impacts chez Saint-Gobain avec une perte de chiffre d'affaire estimée à 250 M€ ;
- toujours en 2017, le *malware Triton* a été spécialement créé pour attaquer un système de sûreté industrielle (Triconex, automate programmable industriel de sécurité). Une usine pétrochimique était visée. Cette attaque n'a pas pu totalement aboutir, mais elle a mis en évidence la possibilité d'injecter un morceau de code interprétable par le processeur de l'automate programmable [9].

Le constat est que le « risque cyber » existe désormais pour les systèmes industriels. Il concerne souvent des secteurs comme l'énergie, l'industrie pétrolière ou gazière, l'eau, le transport et dans une moindre mesure, l'industrie manufacturière. Cependant, au vu des changements liés à l'industrie du futur et à la digitalisation de la plupart des activités, il devient un risque dont les impacts ne sont pas encore forcément pris en compte par les entreprises en termes de sécurité pour le salarié. Une récente étude [10] met en avant des impacts possibles pour la sécurité de l'opérateur intervenant auprès d'une installation robotisée.

« Risque cyber » et directive machines : malveillance *versus* défaillance

Dans le domaine des systèmes industriels, la sûreté de fonctionnement implique principalement quatre composantes (cf. Figure 1) qui sont :

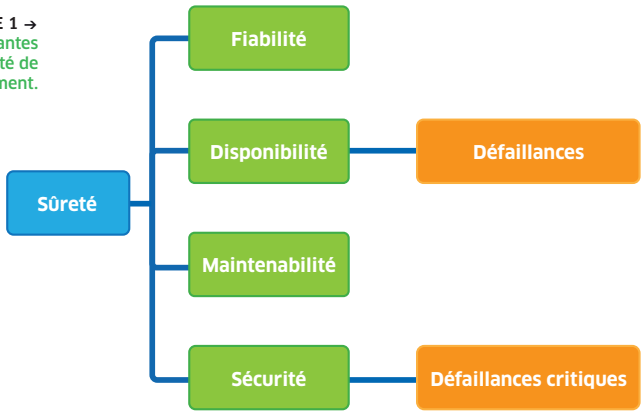
- la fiabilité (aptitude à accomplir la mission pendant une durée déterminée) ;
- la disponibilité (aptitude à accomplir la mission dans des conditions données et à un instant donné) ;
- la maintenabilité (aptitude d'une entité à être maintenue ou rétablie dans un état permettant de remplir la mission) ;
- et la sécurité (au sens anglophone de « *safety* » : capacité du système à ne pas conduire à des événements/accidents inacceptables pour les personnes, le système ou l'environnement).

La sûreté de fonctionnement, dans sa composante « sécurité », vise ainsi à déterminer l'impact des défaillances critiques (et techniques) du système alors que la cybersécurité prend en compte les actes malveillants. Ce point de vue étant différent, il mérite d'être souligné.

Cette notion de défaillance est ainsi celle que l'on retrouve, dans le référentiel pour la conception des machines tel que la Directive « Machines » n° 2006/42/CE, en ce qui concerne par exemple la sécurité et la fiabilité des systèmes de commande puisqu'une défaillance du matériel ou de logiciel du système de commande ne doit pas entraîner de situation dangereuse pour le salarié. De plus, cette directive ou la norme ISO 12100 [11], mentionnent qu'une machine doit être sûre dans des conditions normales d'utilisation (cf. Figure 2). Il est aussi demandé de prendre en compte les « mauvais usages raisonnablement prévisibles »). Pour l'INRS et la KAN (cf. *KAN-Brief* de février 2017 [12]) et comme explicité dans la directive Machines, la réglementation européenne couvre l'usage normal et tout mauvais usage raisonnablement prévisible de la part de l'utilisateur, mais pas un usage abusif résultant d'un acte criminel (acte malveillant, tel qu'une cyberattaque).

Il en résulte que les normes de conception machines ne prennent pas en compte la cybersécurité. En effet, la cybersécurité au sens acte malveillant est vue ainsi comme hors du périmètre de ces textes car elle n'est pas classée dans les mauvais usages raisonnablement prévisibles.

FIGURE 1 →
Les composantes de la sûreté de fonctionnement.



Vers la prise en compte du « risque cyber » dans les analyses de risque « sécurité machine » ?

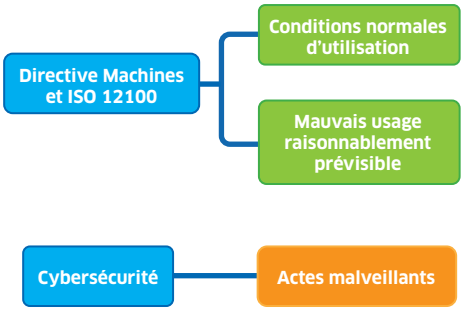
Bien que les actes cybercriminels ne soient pas aujourd'hui dans le giron de la directive machines et des normes associées, il est légitime de se poser la question de l'impact d'un acte malveillant par vecteur numérique : ces actes cybercriminels peuvent-ils présenter des risques pour le salarié et existe-t-il des règles de conception qui minimisent ce risque ? Une analyse de risques spécifique dédiée à la cybersécurité permettra d'évaluer si des conséquences existent en termes de sécurité pour le personnel utilisant ou évoluant à proximité d'une machine.

Une des conséquences potentielles serait une corruption d'une fonction de sécurité [3] (dès lors qu'elle utilise des systèmes électroniques programmables et ce qui est de plus en plus fréquent). Une autre

conséquence possible est celle d'une attaque provoquant soit un arrêt dangereux du processus de fabrication avec, par exemple, le déversement d'une matière dangereuse (matière chaude, nocive…), soit, au contraire, un démarrage ou redémarrage ou toute autre action intempestive du processus de production. Ainsi, au niveau normatif et pour les machines, même si les actes malveillants cybercriminels ne sont pas considérés comme étant dans le scope, le document ISO TR22100-4 [13] montre comment le « risque cyber » peut impacter les mesures de réduction du risque mises en œuvre par le concepteur (démarche en trois étapes de l'ISO 12100-1). Il propose ainsi une démarche et des recommandations générales, ainsi que des exemples de mesures de réduction du « risque cyber ». Ce document recommande de mener une analyse des risques classique (identification et réduction des phénomènes dangereux) selon l'ISO 12100 puis ensuite d'analyser ces mesures de réduction du risque (prévention intrinsèque, dispositifs de protection et autres mesures de réduction) au regard de la cybersécurité.
La Commission électronique internationale a conduit également des travaux sur ce sujet, avec la rédaction du document IEC/TR63074 [14] dédiée notamment à la sécurité fonctionnelle et à la perte de capacité à maintenir un fonctionnement sûr (des fonctions de sécurité mises en œuvre, au sens de la sûreté de fonctionnement, pouvant être compromises en cas de cyberattaque). Elle donne des exigences générales pour traiter ce « risque cyber ».

Existe-t-il des risques pour les salariés ?

Comme vu ci-dessus avec l'exemple de l'aciérie attaquée en 2014, des actions malveillantes sur des systèmes industriels peuvent mener à des dommages matériels qui pourraient alors avoir des conséquences pour les salariés. De même, même s'il n'y a pas eu encore, à notre connaissance, d'accident sur des salariés suite à une altération d'une fonction de sécurité d'un système de commande, rien ne permet actuellement d'assurer qu'une cyber-attaque ne pourrait pas corrompre une fonction de sécurité et être alors source d'un risque pour le salarié.
D'autre part, dans le cas où une attaque abouti sur des machines, installations automatisées, systèmes de production en général, elle va générer des interventions de maintenance pour remettre en service ces machines ou installations automatisées. De fait, il peut y avoir un risque indirect, dans la mesure où, à cause de l'urgence de la situation, une procédure formalisée d'intervention ne serait pas suivie.
En cas de dommages sur l'environnement (plutôt dans les industries de type process continu comme le traitement de l'eau, la pétrochimie), par effet de cascade, il pourrait alors y avoir, dans un second temps, un impact potentiel pour les salariés.
Enfin, on peut aussi penser aux risques psycho-sociaux pour les salariés qui seraient victimes de vol de données ou bien craindraient d'être mis au chômage technique voire accusés de négligence ou affectés par une dégradation de l'image ou notoriété de l'entreprise.



← **FIGURE 2**
Périmètre de la Directive « Machines » et de la norme ISO 12100 sur les conditions d'utilisation et périmètre de la cybersécurité.

Analyse de « risque cyber » et mesures de prévention de ce risque : état général des pratiques pour les systèmes industriels

Parmi les termes qui sont évoqués pour l'analyse du « risque cyber », on distingue :
- les menaces : il s'agit des circonstances ou événements ayant le potentiel d'affecter les installations et pouvant générer des dommages ; par exemple le sabotage informatique visant à rendre inopérant un système d'information ou l'espionnage/le piratage souvent à des fins économiques ou scientifiques ;
- les vulnérabilités : ce sont les faiblesses de sécurité (d'un point de vue cybernétique) qui peuvent être exploitées par une menace ; par exemple des failles de sécurité ou des outils non sécurisés de contrôle à distance.

Analyse et appréciation des « risques cyber »

Ici, il ne s'agit pas de rechercher une résistance à tout type d'événement cyber-malveillant (celle-ci serait chronophage et d'un coût important) mais d'identifier et d'apprécier les événements critiques pouvant remettre en cause le fonctionnement nominal et sûr de l'installation.
Les étapes clés de l'analyse et de l'appréciation des risques sont les suivantes (cf. Figure 3 page suivante) :
- *Décrire l'installation* : décrire ses objectifs métier, ses missions et ses fonctions, les interfaces avec l'extérieur. Il faudra expliciter sur quelles parties va porter l'analyse et déterminer ainsi quels composants techniques et fonctionnels seront à analyser, comment sont réalisées les fonctions, avec quels processus, à l'aide de quels moyens (techniques ou humains notamment d'un point de vue « informatique », centralisés, accessibles à distance), ainsi que les moyens de contrôle mis en œuvre.
- *Identifier les risques à l'aide des menaces potentielles, des vulnérabilités et des enjeux (éléments pouvant être impactés) :*

→

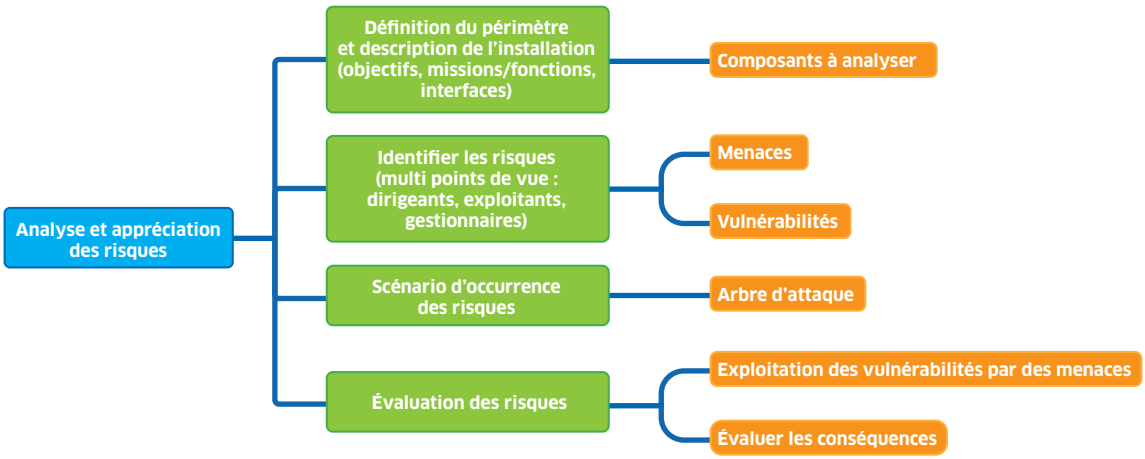
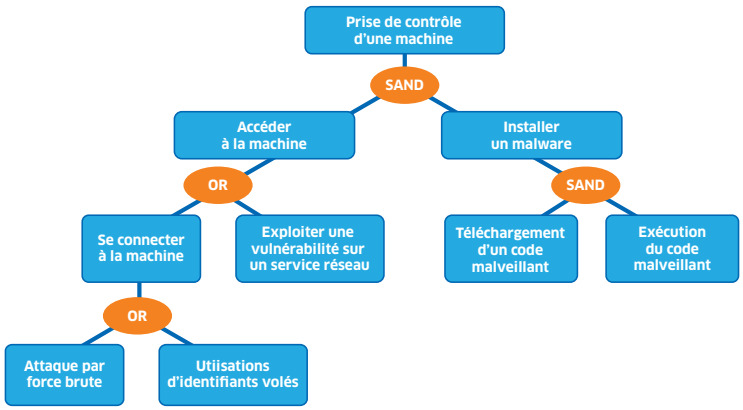


FIGURE 3 → Étapes clés de l'analyse et de l'appréciation des risques "cyber".

il s'agit de risques d'indisponibilité, voire de dommages pour l'installation et ceux liés à la sécurité des personnes. Cette identification sera à faire par les dirigeants, gestionnaires et exploitants en s'aidant des personnes compétentes en système d'information ou cybersécurité. Il s'agit d'identifier quels sont les éléments ou fonctions qui seraient perdus ou corrompus (par exemple une perte d'intégrité de données, une perte de la disponibilité ou de la sécurité de l'installation) par des événements malveillants. Pour mener cette étape, il importe de comprendre la logique et les motivations (par jeu, rançon, dommage économique, terrorisme, ...) de l'attaquant : imaginer, envisager et cerner sa logique permettra de savoir quels types de menace sont crédibles et en fonction de cela, d'adapter les mesures de prévention des risques à mettre en place. Il est aussi utile d'identifier ce qui peut faciliter une attaque ou au contraire ce qui pourra la compliquer.

- *Décrire les scénarios d'occurrence des risques* : à cette étape de l'analyse, il est d'usage d'utiliser des méthodes déductives qui partent d'un événement redouté pour identifier les causes possibles sous forme de combinaisons d'événements (exploitation des vulnérabilités par des menaces). Cette étape se déroule par itération. Une des représentations utilisées est l'arbre d'attaque (cf. figure 4), qui est similaire à l'arbre des défaillances utilisé en sûreté de fonctionnement. Il donne une représentation des scénarios sous une forme arborescente en reliant entre eux des événements.
  - *À noter* que l'utilisation de méthodes inductives (de type Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité – AMDEC) est délicate à ce niveau car partant d'un événement élémentaire pour en voir les impacts, elle demande un travail important et ne serait pas nécessairement efficace.
  - *À noter aussi* que cette étape est assez complexe et rendue optionnelle dans la dernière version d'*Ebios Risk manager* (la méthode générale d'analyse proposée par l'Anssi ; cf. Encadré 1).
- *Évaluer les risques* : à partir des scénarios ou des causes possibles d'un événement redouté, il s'agit d'évaluer les conséquences. Le niveau de risque est estimé en général à l'aide d'une matrice de risque combinant vraisemblance et gravité. Il sera nécessaire d'évaluer la sévérité des impacts d'une cyberattaque (par exemple remise en cause du fonctionnement de l'installation, modification des paramètres d'une installation comme la vitesse de déplacement d'un robot).



↓ FIGURE 4 Exemple d'arbre d'attaque [6]. *Note : SAND est un opérateur introduit pour les arbres d'attaque, il précise la notion de séquence entre les deux composantes du AND, celle de gauche devant être réalisée en premier. Ainsi, pour prendre contrôle, il faut d'abord accéder à la machine puis installer un malware.*

Mesures de prévention du « risque cyber »

D'une façon générale, les mesures de prévention (cf. Figure 5) doivent s'inscrire dans une une approche globale prenant en compte le personnel, le produit et la politique (et les procédures) de l'entreprise vis-à-vis de ce risque.

Un des concepts évoqué pour la cybersécurité est la défense en profondeur (voir par exemple l'ensemble des normes IEC 62443 [18] ou [8]), une approche générale de la sécurité visant à mettre en place des stratégies de défense complémentaires, autonomes, successives et indépendantes, pouvant être de natures différentes (technologiques, humaines, organisationnelles). Par exemple, cloisonner les réseaux informatiques à l'aide de pare-feu n'est pas suffisant.

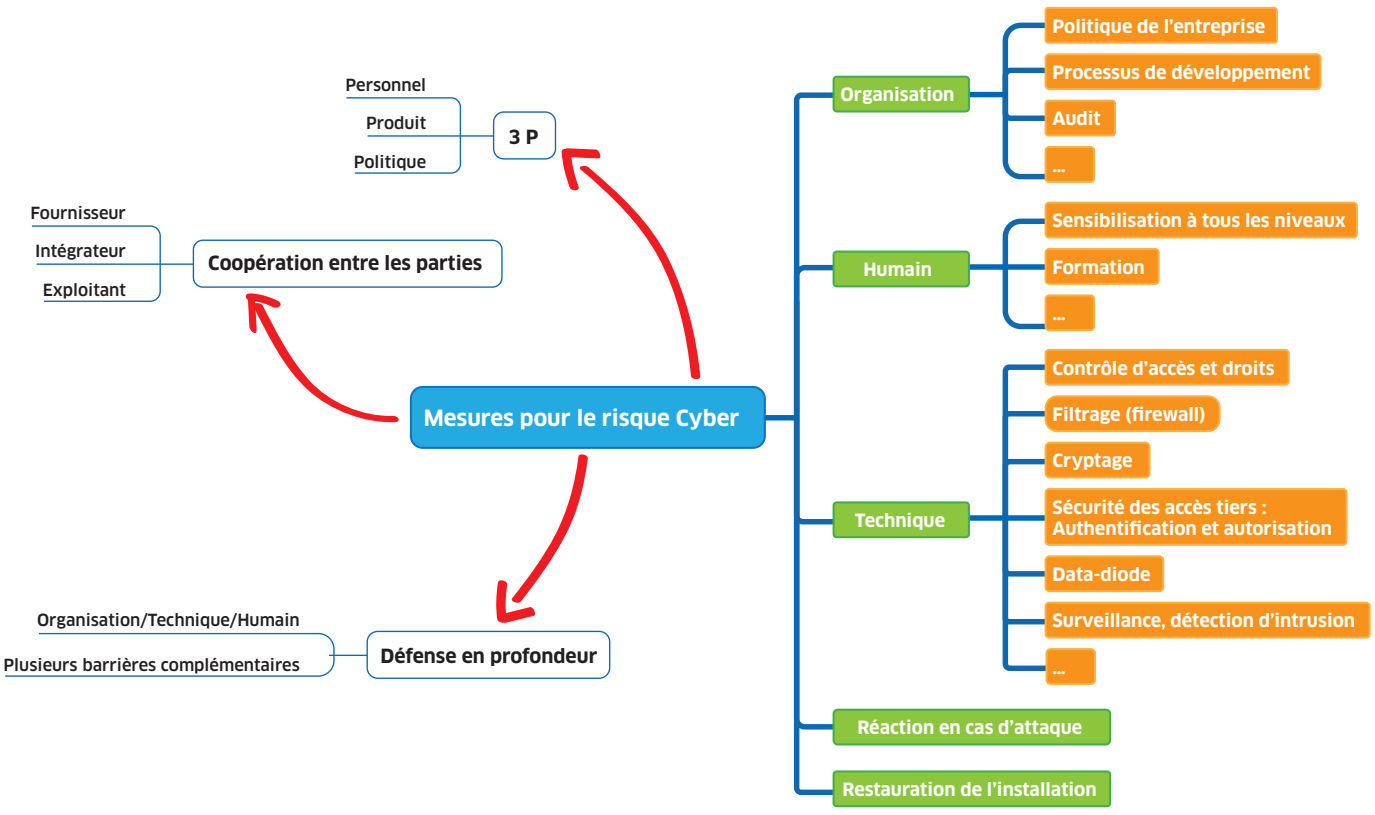
ENCADRÉ 1

QUELQUES PRÉCISIONS SUR LES ANALYSES DE « RISQUE CYBER »

La méthodologie est inductive [4] et met en avant des scénarios d'attaque par projection des menaces envisagées sur des vulnérabilités potentielles. Elle peut s'avérer fastidieuse pour une installation industrielle complexe, mais assure un rôle préventif adéquat.
La méthode Ebios Risk Manager (*Ebios : Expression des besoins et identification des objectifs de sécurité*) est une méthode de gestion des risques cyber, qui nécessite de prendre en compte les spécificités de l'installation industrielle. Les normes ISO 31000 [16] ou ISO 27005 [17] (qui est une déclinaison de l'ISO 31000 dans le domaine de la sécurité de l'information) permettent elles aussi, même si elles restent assez générales, d'obtenir des compléments d'informations et de méthodologie.
D'autres méthodes sont décrites dans l'ouvrage de J.M. Flaus [8]. L'analyse de risque cybersécurité est à faire vivre, à réviser car le « risque cyber » évolue vite (menace et capacité des attaquants, les technologies évoluent et les vulnérabilités évoluent aussi très vite) mais aussi afin de s'assurer que le contexte ou son contenu reste toujours valide.

De plus, il est nécessaire de mettre en place des mesures coordonnées entre les différentes parties prenantes : l'exploitant, l'intégrateur et le fournisseur, chacun apportant sa pierre à l'édifice. Pour l'exploitant, des exemples de mesures sont la sensibilisation du personnel à ce risque, à tous les niveaux de la hiérarchie, et des actions de formation. Ces mesures seront complétées, généralement par l'intégrateur, par exemple en segmentant l'architecture réseau. Ensuite, le fournisseur des composants élémentaires inclura, nativement dans ses produits, des mesures techniques tels des anti-virus, du cryptage de données, des accès par mots de passe, des restrictions concernant l'exécution de logiciel (liste figée de logiciels autorisés).

Une des spécificités liées à ce risque est la mise en place de mesures de prévention pour surveiller les installations et détecter les incidents ou intrusions ; ceci dans le but de limiter la propagation ou prévenir/anticiper les effets d'une attaque avant qu'elle ne devienne plus conséquente et porte atteinte à l'intégrité, la disponibilité, la sécurité de l'installation.
Ensuite, il importe de prévoir les réactions en cas d'attaque tant d'un point de vue fonctionnel, afin de stopper, contenir l'attaque, que d'un point de vue « organisationnel » : processus de gestion de crise, qui pourra contribuer à réduire les risques indirects pour les salariés intervenant sur l'installation (par exemple : planification adéquate des opérations de maintenance).



↓ FIGURE 5
Les mesures de prévention pour le « risque cyber » *(à droite)* avec le contexte général *(à gauche)*.

ENCADRÉ 2

SPÉCIFICITÉ DES SYSTÈMES INDUSTRIELS

Quelques spécificités, non exhaustives, sont à noter pour les systèmes industriels par rapport aux systèmes d'information. Ils peuvent générer des exigences contradictoires, entre la cybersécurité et la sûreté de fonctionnement, qui nécessiteront des compromis :

- en cybersécurité, il est important de mettre à jour les logiciels régulièrement. Pour une installation industrielle devant fonctionner en continu, ces mises à jour peuvent nécessiter un arrêt de l'installation qui n'est pas forcément compatible avec le processus de production ou difficile à planifier. De plus, dans les pratiques de sûreté, toute évolution/modification de l'installation doit mener à sa revalidation,
- le principe de la redondance, couramment utilisé pour assurer le maintien de la fonction de sécurité en cas de défaillance, peut être inefficace voire contre-productif pour le « risque cyber »,
- le temps de cycle des automates peut être contraint. Il peut devenir impossible d'y intégrer de nouvelles tâches gourmandes en temps comme le seraient le cryptage de données ou la gestion de logs, solutions techniques utilisées en cybersécurité.

La durée de vie des installations industrielles est un facteur pénalisant car les échelles de temps ne sont pas les mêmes que pour la cybersécurité. En effet, les évolutions liées à la cybersécurité sont rapides alors que les installations industrielles ont jusqu'à présent souvent été conçues pour 10, 20 voire 30 ans avec des évolutions plus difficiles à mettre en place. Certaines installations sont anciennes et les solutions actuelles pour traiter la cybersécurité peuvent être inadaptées ou nécessiter une refonte coûteuse.
L'hétérogénéité des produits (avec un empilement de technologies : marques différentes pour les capteurs, actionneurs, automates, ...) est aussi un facteur pouvant limiter la mise en œuvre de solutions techniques.
Les contraintes environnementales d'exploitation (température, poussière, humidité) sont aussi à prendre en compte dans le choix des solutions techniques de cybersécurité avec la difficulté à trouver l'équipement adéquat au monde industriel.

Enfin, il importe, si nécessaire, de restaurer l'installation altérée par l'attaque.

« Risque cyber » et risque professionnel pour les machines : cohabitation ou antagonisme ?

Pour les systèmes industriels, la communication autour du « risque cyber » pour les entreprises s'est intensifiée ces dernières années. L'impact pour les salariés y est rarement évoqué. D'une manière générale, après une phase de sensibilisation à ce risque cyber, les travaux sur ce sujet et sur la façon de prendre en compte ce risque, notamment son articulation avec la sûreté de fonctionnement, se poursuivent. En effet, pour les systèmes industriels, il est judicieux de comparer les analyses cybersécurité et les analyses plus classiques de sûreté de fonctionnement (notamment étude du comportement en cas de défaillances) afin de les compléter mutuellement si nécessaire, de définir les moyens pour les couvrir (certains pouvant être antagonistes entre les deux approches, un compromis sera alors nécessaire). Il est à noter que du point de vue de la démarche suivie, les analyses en cybersécurité sont plutôt qualitatives, alors que les analyses de type sûreté de fonctionnement sont quantitatives (estimation des probabilités de défaillance). De plus, les acteurs en sûreté de fonctionnement vont avoir un profil « métier » (automatisme, gestion de production, maintenance, sûreté de fonctionnement) alors que les acteurs de la cybersécurité sont issus généralement du monde des systèmes d'information. Il en résulte des points de vue qui peuvent être différents et la tendance est de proposer des méthodes qui combinent étude des défaillances et étude d'un point de vue cybersécurité [19].

Avec la connexion des machines au réseau Internet et comme évoqué au début de ce document, le « risque cyber » peut être considéré comme un risque émergent pour la sécurité des salariés. Il a été présenté plus haut dans le document l'état de l'art des pratiques en cybersécurité, ce qui pourra être utile pour les entreprises (utilisatrices ou concepteurs) voulant mener une analyse de risque professionnels prenant en compte le « risque cyber ». Il faut cependant rester objectif dans la perception de ce risque, notamment lors de la détermination des menaces et vulnérabilités. Une des premières difficultés consiste à caractériser la menace à sa juste valeur. De même, l'impact est à déterminer au plus près. Par exemple, dans le cas de « rançongiciel », est-ce que l'activité de l'entreprise est mise en péril et est-ce qu'il pourrait y avoir un impact pour la santé - sécurité du salarié ? Enfin, pour que cette analyse soit pérenne, il importe de mener une veille active et de réinterroger régulièrement ses dispositions de cybersécurité. Enfin, cette analyse est à mener en groupe pluridisciplinaire (notamment HSE, système d'information, métier pour les aspects systèmes industriels) afin de prendre en compte les différents points de vue et contraintes des uns et des autres.

Prise en compte de la cybersécurité à la conception des machines

Bien que les actes malveillants soient vus comme hors cadre de la Directive n° 2006/42/CE, le document ISO TR 22100-4 pourra servir de support à l'analyse des risques professionnels à la conception. Il recommande de mener une analyse des risques classique (identification et réduction des phénomènes dangereux) selon l'ISO 12100 puis ensuite d'analyser ces mesures de réduction du risque (prévention intrinsèque, dispositifs de protection

et autres mesures de réduction) au regard de la cybersécurité.

Prise en compte de la cybersécurité à l'utilisation : DU et EvRP

C'est l'évaluation des risques professionnels menée par les décideurs de l'entreprise qui déterminera si des mesures sont à prendre, au regard des impacts identifiés. En cas de risque avéré, il importe de mentionner ce « risque cyber » dans le document unique.

Quelles perspectives pour la sécurité des machines ?

Des situations restent à explorer et font l'objet de réflexions pour appréhender le « risque cyber » sur l'ensemble du champ de la santé et sécurité machine :

- la corruption d'une fonction de sécurité sur une machine qui ne remplirait plus son rôle en cas de cyberattaque où de nombreux éléments de protection sont instrumentés (programmables et connectés) ;
- l'utilisation de machines mobiles connectées et l'impact en termes de risque pour le salarié d'une prise en main à distance ;
- le cas particulier de la télé-opération (prise en main à distance et impact pour un salarié au poste de travail). ●

1. *Anssi : Agence nationale de la sécurité des systèmes d'information - https://www.ssi.gouv.fr/*
2. *Clusif : Club de la sécurité de l'information français.*
3. *Selon la norme ISO 12100 : fonction d'une machine dont la défaillance peut provoquer un accroissement immédiat du(des) risque(s).)*
4. *Il existe deux grandes classes de méthodologie d'identification de phénomènes dangereux :*
   - *logique inductive qui va à partir des causes, induire l'événement ou effet indésirable (approche de bas en haut) et*
   - *logique déductive qui va, à partir du danger, remonter ou en déduire les causes (approche de haut en bas) ; exemple : arbre des causes.*

Remerciements

L'auteur remercie Jean-Marie Flaus, professeur à l'Université de Grenoble (laboratoire G-SCOP), pour ses commentaires et sa relecture attentive.

BIBLIOGRAPHIE

[1] Décryptage – L'industrie du futur : de quoi parle-t-on ? *Hygiène et sécurité du travail,* décembre 2018, 253, pp. 6-10. *Accessible sur : www.hst.fr*

[2] Article 22 de la loi de programmation militaire (loi n°2013-1168 du 18 décembre 2013) **et décret n° 2015-351** pour les Opérateurs d'importance vitale ; **directive Network and Information System Security (NIS) du 6 juillet 2016 et décret n° 2018-384 du 23 mai 2018** pour les Opérateurs de services essentiels. *Accessibles sur : www.legifrance.gouv.fr*

[3] Loi n° 2003-699 du 30 juillet 2003 relative à la prévention des risques technologiques et naturels et à la réparation des dommages. *Accessible sur : www.legifrance.gouv.fr*

[4] Directive n° 2012/18/UE du parlement européen et du conseil du 4 juillet 2012 concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses. *Accessible sur : eur-lex.europa.eu/*

[5] Fourastier Y., Pietre-Cambacedes L. – *Cybersécurité des installations industrielles – Défendre ses systèmes numériques.* Cepadues Ed., 2015, 528 p.

[6] Anssi – Maîtriser la SSI pour les systèmes industriels – La cybersécurité des systèmes industriels. 2012, 40 p.

[7] Clusid – Fiches incidents Cyber SI industriels. 2017, 72 p.

[8] Flaus J. M. – Cybersécurité des systèmes industriels. ISTE Editions, 2019, 372 p.

[9] Federal Office for information Security – The state of IT Security in Germany *2018, 100 p. Accessible sur : https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2018.pdf?__blob=publicationFile&v=3*

[10] Quarta D., Pogliani M., Polino M., Maggi F., Zanchettin A.M., Zanero S. – *An experimental security analysis of an industrial robot controller.* In: 2017 IEEE Symposium on Security and Privacy (SP), 2017, pp. 268-286.

[11] NF EN ISO 12100 – *Sécurité des machines – Principes généraux de conception.* Paris, Afnor, décembre 2010.

[12] Kommission Arbeitsschutz und Normung – KAN-Brief n° 2/17. *Accessible sur https://www.kan.de/fileadmin/Redaktion/Dokumente/KAN-Brief/de-en-fr/17-2.pdf*

[13] ISO/TR 22100-4 – *Safety of machinery - relationship with ISO 12100 - Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects.* Genève, ISO, décembre 2018.

[14] IEC/TR 63074 – *Safety of machinery – Security aspects related to functional safety of safety- related control systems.* Genève, CEI, mai 2019.

[15] Godefroy E. – Définition et évaluation d'un mécanisme de génération de règles de corrélation liées à l'environnement. STIC Informatique / CentraleSupélec, 2016, 159 p.

[16] NF ISO 31000 – *Management du risque – Lignes directrices.* Paris, Afnor, juin 2018.

[17] NF ISO/IEC 27005 – *Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information.* Paris, Afnor, novembre 2018.

[18] IEC 62443 – *Security for industrial automation and control systems – Parts 1, 2, 3, 4.* Genève, CEI.

[19] 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 : 12e Congrès International Pluridisciplinaire en Qualité, Sûreté de fonctionnement et Développement durable (QUALITA 2017), août 2017, Bourges. Ineris-01863860.