Décryptage

COMPRENDRE L'ANALYSE DU « RISQUE CYBER » DANS LE CONTEXTE DE LA SÉCURITÉ DES MACHINES

La cybersécurité (capacité d'un système à résister aux cyberattaques et aux pannes survenant dans le cyberespace) est devenue, depuis près d'une quinzaine d'années, une préoccupation pour de nombreuses entreprises. Du point de vue de la santé et la sécurité au travail (SST), cette prise en compte du « risque cyber » va être renforcée dans le cadre de la conception des machines, avec la mise en application du règlement européen 2023/1230, prévue pour le 20 janvier 2027.
Cet article s'adresse aux préventeurs machines et vise à donner une première approche du processus de l'analyse du risque cyber et à le comparer avec l'analyse du risque physique machine.

UNDERSTANDING 'CYBER RISK' ASSESSMENT IN THE CONTEXT OF MACHINE SAFETY –
Over the past fifteen years, cybersecurity (i.e. a system's ability to withstand cyberattacks and failures occurring in cyberspace) has become a major concern for many companies. From an occupational health and safety (OHS) perspective, the consideration of 'cyber risk' in machine design is set to become even more important following the implementation of European Regulation 2023/1230, which is due to come into force on 20 January 2027. This article is intended for machine safety professionals and provides an introductory overview of the cyber risk assessment process.
It also compares this process with the conventional physical risk assessment of machines.

PASCAL LAMY,
NISRINE GHADBAN
INRS, département Ingénierie des équipements de travail

ALEXANDRE DEPRIESTER
INRS, département Informatique et système d'information

Présentation générale et contexte

Le numérique étend son emprise sur les machines et les installations industrielles depuis plusieurs années, et cette tendance s'est accélérée dans le contexte de l'industrie 4.0. Les machines, anciennes ou récentes, sont ainsi de plus en plus connectées à des réseaux, notamment Internet. Les machines industrielles en service de conception ancienne, n'ont pas été conçues pour faire face aux cyberattaques, ou bien sont utilisées dans des environnements et des contextes d'exploitation qui rendent difficile la mise en place de mesures de sécurité informatique. Qu'elles soient récentes ou anciennes, les machines industrielles peuvent donc être exposées au « risque cyber », ce qui peut mener à un dommage physique pour l'opérateur, par exemple en cas de modification du fonctionnement de la machine ou de prise de commande à distance de la machine.

Dans le secteur industriel, la cybersécurité (définie par l'Agence nationale de la sécurité des systèmes d'information comme « *un état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles* »[1]) est devenue une préoccupation pour de nombreuses entreprises industrielles (retentissement médiatique suite à des cyberattaques, obligations réglementaires selon les secteurs d'activité, sensibilisation accrue au risque de cyberattaque). Avec la mise en application du règlement européen « Machines » 2023/1230, à partir du 20 janvier 2027 [1], de nouvelles exigences essentielles de santé et de sécurité (EESS: *Cf. Annexe III, section 1.1.9 et 1.2.1)* relatives,

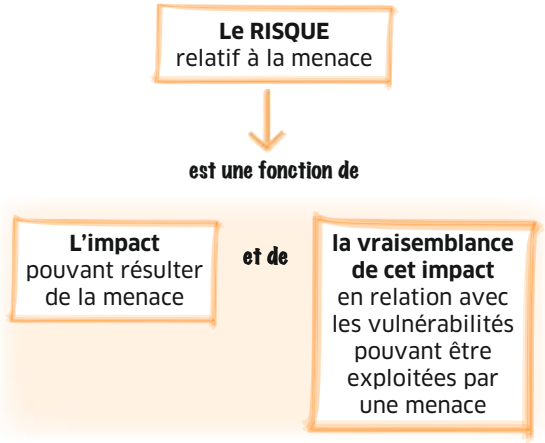


FIGURE 1 →
Définition du risque cyber *(issue du document ISO TR 22100-4 [3]).*

part, à la protection contre la corruption (de données) et, d'autre part, au comportement du système de commande en cas de tentatives malveillantes sont introduites.
Comme dans tout processus de prévention des risques, avant de mettre en place des mesures de prévention, il faut commencer par une analyse du risque. Cet article a comme objectif de se focaliser sur le processus de l'analyse du risque cyber. Il propose d'expliciter et de vulgariser le « jargon » employé en cybersécurité, dans le contexte de la santé et de la sécurité au travail (SST) pour les machines industrielles.

Le risque numérique ou « risque cyber »

Dans le domaine de la SST, pour la conception des machines, le référentiel en support à l'analyse de risque professionnel est la norme NF EN ISO 12100 [2]. Cette analyse y est organisée en trois étapes : la détermination des limites de la machine, l'identification des phénomènes dangereux et l'estimation du risque.
Ce référentiel est complété, pour les aspects de cybersécurité, par le document ISO TR 22100-4 [3]. Ce rapport technique propose de définir le « risque cyber » comme une combinaison de l'impact et de la vraisemblance de cet impact *(Cf. Figure 1)*. Ces notions sont elles-mêmes reliées à celles de menace et vulnérabilité, précisées plus loin dans l'article *(Cf. § « Menace et vulnérabilités » p. 8)*.
Sur la base de cette définition, cet article se concentre sur les impacts pour la SST (dommage physique par exemple), incluant ceux affectant potentiellement une mesure de prévention, et non pas sur les impacts financiers, juridiques liés à une cyberattaque. En cas de cyberattaque, une compromission de l'intégrité d'un système ou de ses commandes peut mener à un dommage pour le salarié : par exemple, la corruption du fonctionnement d'un robot mobile ou la prise de contrôle de ses commandes peuvent entraîner une collision avec le salarié *(Cf. Figure 2)*. Une cyberattaque peut aussi générer un stress lié à l'attaque et à ses conséquences, comme la perte de données, l'indisponibilité prolongée de l'outil de production, voire la perte d'emploi. Pour une description plus générale, voir la note technique [4] parue dans un numéro précédent de la revue.

Les étapes d'une cyberattaque

Avant de détailler l'analyse du risque cyber, il est important de comprendre par quel processus général un attaquant mène son opération, car cela sera utile dans une des étapes du processus de cette

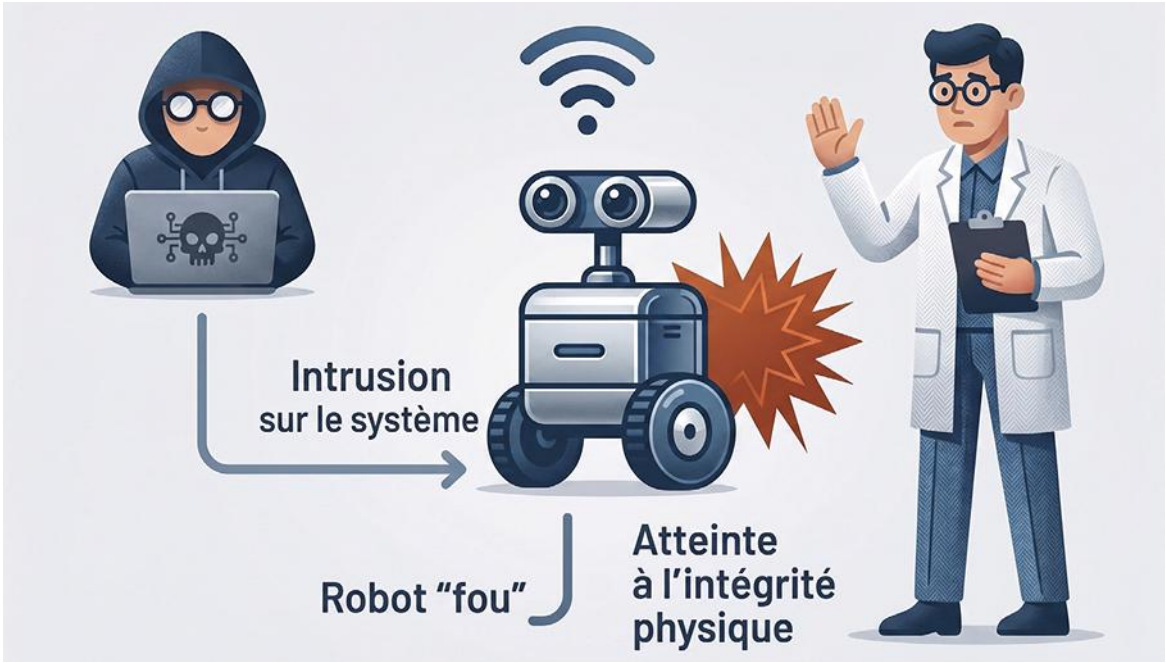


FIGURE 2 →
Corruption d'un robot mobile par la prise de contrôle de ses commandes menant à une possibilité de heurt avec un salarié.

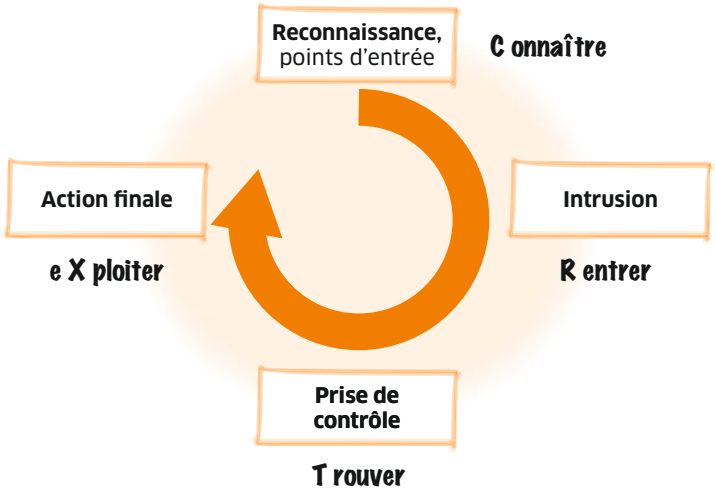
© INRS/Image générée avec une IA

analyse. On parle de chemin ou de scénario d'attaque (en anglais, *kill chain)*. Différentes représentations de chemin d'attaque existent. La *Figure 3* présente celle qui est utilisée dans la méthode EBIOS-RM (Expression des besoins et identification des objectifs de sécurité – *Risk manager)* [5], méthode française développée par l'Anssi (Agence nationale de la sécurité des systèmes d'information). Le chemin d'attaque est composé de quatre étapes : « Connaître, Rentrer, Trouver et eXploiter ». On parle alors de la *kill chain* C-R-T-X.

Connaître

La première étape consiste pour l'attaquant à recueillir toutes les informations disponibles par rapport à la cible visée. Ce peut être par exemple *via* la recherche d'information en source ouverte et disponible, telle que les adresses mails des employés lorsque celles-ci sont mentionnées sur le site de l'entreprise, ou en exploitant des bases d'adresses accessibles, de manière légale ou non. L'attaquant peut également chercher les points d'accès lui permettant de rentrer dans le système d'information de l'entreprise. Il peut notamment essayer d'effectuer un scan du réseau et déterminer les accès à des services ouverts ou potentiellement vulnérables à une intrusion. Il peut aussi observer les pratiques concernant les accès physique ou logique, tels que l'absence de contrôle ou une résistance insuffisante aux attaques, et ainsi profiter des faiblesses dans ces accès.

En fonction de son profil *(Cf. Tableau 1)*, l'attaquant peut également observer ou chercher, parmi les prestataires ou les intervenants extérieurs, un moyen détourné d'entrer dans le système d'information ; il peut recueillir des informations sur les façons de faire de l'entreprise, voire soudoyer un prestataire.



↑FIGURE 3
Illustration des quatre étapes d'un chemin d'attaque.

↓TABLEAU 1
Liste de profils d'attaquants proposée dans la méthode EBIOS-RM *(Source : Anssi [5]).*

PROFIL D'ATTAQUANT	EXEMPLES ET MODES OPÉRATOIRES HABITUELS
Étatique	*État, agence de renseignement :* Attaques généralement conduites par des professionnels, respectant un calendrier et un mode opératoire prédéfinis. Ce profil est caractérisé par sa capacité à mener une attaque sur un temps long (ressources stables), à déployer des moyens et des compétences importants, à adapter ses outils et ses méthodes en fonction de la cible. Possibilité d'exploiter des vulnérabilités non connues.
Crime organisé	*Organisation cybercriminelle :* Arnaque en ligne, demande de rançon (attaque par rançongiciel). Ces cybercriminels mènent des attaques de plus en plus sophistiquées. Certains peuvent exploiter des vulnérabilités non connues.
Terroriste	*Cyberterroriste, cybermilice :* Attaques généralement peu sophistiquées mais menées avec détermination, à des fins de déstabilisation et de destruction : indisponibilité, arrêt intempestif, défiguration de site Internet.
Activiste idéologique	*Cyber-activiste (hacktiviste), groupement d'intérêt, secte :* Profil équivalent au terroriste dans la façon et la capacité de procéder mais motivé par des intentions moins destructrices. Ce peut être pour véhiculer une idéologie, un message, etc.
Officine spécialisée	*« Cybermercenaire » avec un but lucratif :* Capacités techniques généralement élevées, agissant par défi et pour la quête de reconnaissance. Peut s'organiser en officine spécialisée proposant des services de piratage ou peut concevoir des outils d'attaques et les mettre à disposition sur Internet.
Amateur	*Attaquant doté de connaissances informatiques,* motivé par la reconnaissance sociale, l'amusement ou le défi. Peut utiliser des outils d'attaque disponibles en ligne.
Vengeur	*Attaquant motivé par un esprit de vengeance ou un sentiment d'injustice,* comme un salarié ou un prestataire mécontent. Caractérisé par une détermination et une connaissance interne des systèmes et de l'entreprise.
Malveillant pathologique	*Motivation d'ordre pathologique ou opportuniste, parfois par appât du gain* Assaillant de compétences diverses : peut mener l'attaque seul, ou en s'aidant de solutions accessibles ; ou en sous-traitant l'attaque à une officine spécialisée, peut soudoyer un salarié, un prestataire.

→

Il s'agit donc dans cette étape, pour l'attaquant, d'obtenir le maximum d'informations exploitables, et généralement il privilégiera les informations les plus faciles à obtenir et les plus pertinentes pour la suite du scénario.

Rentrer

La deuxième étape consiste pour l'attaquant à pénétrer dans le système d'information de l'entreprise, et à accéder au réseau informatique/numérique par quelque moyen que ce soit, en s'appuyant sur les informations exploitables recueillies dans l'étape « Connaître ». Il emploie pour cela des techniques profitant de failles ou points d'entrée vulnérables. Il peut par exemple :

- envoyer un mail piégé à un salarié, contenant un *malware* (code malveillant) lui permettant de s'introduire dans le système ;
- envoyer un lien vers un site Internet frauduleux ;
- contourner les sécurités des services d'accès à distance, en profitant de l'existence d'un mot de passe faible.

Trouver

Une fois entré dans le système, l'attaquant l'explore, s'y déplace, parcourt les différents équipements et services accessibles en réseaux, exploite ceux qui se révèlent les plus vulnérables et qui pourront être utilisés pour la suite. Il peut aussi augmenter ses privilèges (droits d'accès, par exemple, pour passer d'un utilisateur normal à un utilisateur administrateur). Il cherche ainsi à atteindre sa cible finale. Cette troisième étape peut durer plusieurs mois, à partir du moment où l'attaquant n'est pas détecté. Il reste pour cela le plus discret possible.

eXploiter

Cette dernière étape est la concrétisation de l'attaque. L'attaquant exploite ce qu'il a trouvé au cours des étapes précédentes et mène son action finale. Ce peut être, par exemple, un déni de service (rendre l'équipement indisponible), la prise de contrôle à des fins malveillantes, ou encore la modification (indésirable et/ou malveillante) altérant le fonctionnement attendu de l'équipement (changer la vitesse de déplacement d'un élément mobile).

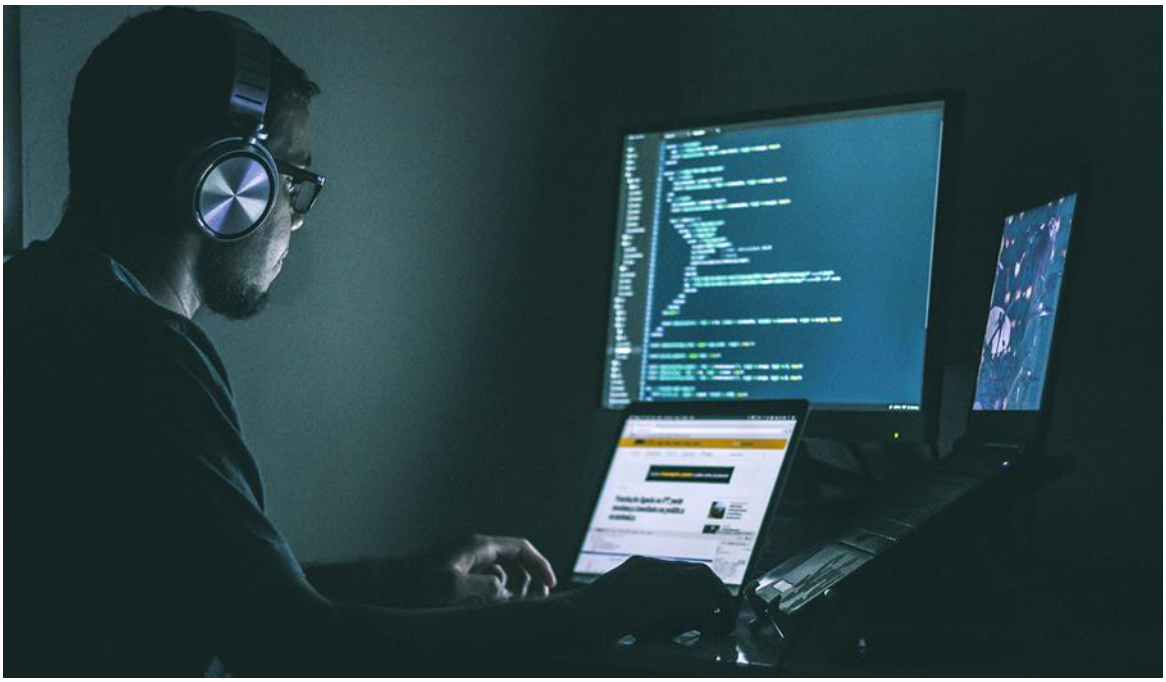
Il est important d'avoir en tête ces étapes pour pouvoir imaginer des scénarios d'attaque, en fonction des menaces et vulnérabilités.

Menace et vulnérabilités

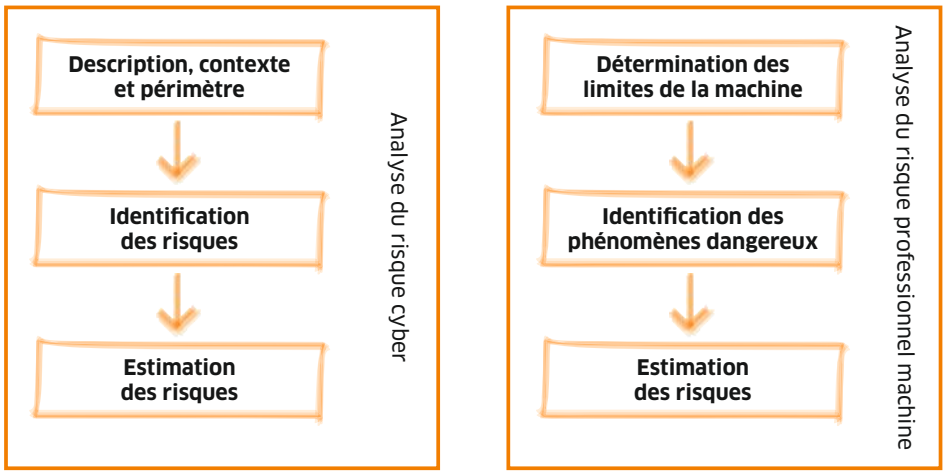
Menace et source de risque

La menace est un terme générique pour désigner toute intention, malveillante ou involontaire, susceptible de provoquer un risque ; par exemple, une cyberattaque ou une mise à jour légitime provoquant un incident de sécurité grave.

Ici, nous nous concentrons sur les menaces malveillantes. L'Anssi propose chaque année un panorama de la cybermenace [6] permettant de comprendre les évolutions et les tendances relatives aux techniques d'attaque, de mieux comprendre l'objectif des attaquants et leur origine. Une bonne connaissance des contextes de menace générale, mais aussi locaux (domaine d'activité, environnement géopolitique, exposition de l'activité, etc.) apparaît comme fondamentale pour mener l'analyse de risque, notamment pour estimer la vraisemblance de ces menaces. Il importe de mener une veille sur le sujet afin d'être en



© Jefferson Santos/Unsplash



←FIGURE 4
Les étapes de l'analyse du risque cyber *(à gauche)*, similaires à l'analyse du risque professionnel machine de la norme NF EN ISO 12100 *(à droite)*.

capacité de se protéger au plus vite et au mieux.
Il faut identifier la menace et l'estimer sereinement, sans exagération et en fonction du contexte géopolitique notamment. Par exemple, en période de conflits, des secteurs tels que l'aéronautique, la défense ou l'énergie peuvent être plus ciblés que d'autres.
Pour qu'une menace se concrétise, il faut déterminer son initiateur, appelé « source de risque » ou « source de menace ». Une source de risque malveillante communément désignée « attaquant » correspond à tout élément, personne, groupe de personnes ou organisation susceptible d'engendrer un risque ; elle est caractérisée par sa motivation, ses ressources, ses compétences, ses modes privilégiés pour opérer (attaquer). Il importe, lors d'une analyse du risque de cyberattaque, de se questionner : « *Qui peut m'attaquer ? Pourquoi ? Quels sont ses intérêts ? Quels sont ses objectifs : la déstabilisation par atteinte à l'image ou déni de service ; le préjudice financier, avec demande de rançon ou en portant atteinte à la capacité de production ; la corruption ou l'exfiltration de données sensibles ou de savoir-faire ; etc. ?* ». Dans les fiches méthodes associées à la méthode EBIOS-RM, l'Anssi propose une liste de profils d'attaquants *(cf. Tableau 1)*.

Vulnérabilités

Les vulnérabilités sont des failles de sécurité numérique qui peuvent être exploitées par un attaquant pour mener son attaque. Elles se divisent en trois catégories : techniques, organisationnelles, et liées au comportement humain. Les vulnérabilités sont clairement définies, quantifiées et caractérisées ; par exemple, l'absence d'antivirus sur un poste informatique, ou un mot de passe « faible ». Pour les équipements (ordinateurs, automates programmables industriels…) et logiciels, il existe des bases de données de vulnérabilités techniques, telles que celles du Cert [7] ou du Mitre [8].

Pour les machines, des exemples de vulnérabilités techniques peuvent être un accès physique ou logique non contrôlé, l'utilisation de protocoles de communication vulnérables entre les équipements industriels, comme le protocole non chiffré Modbus, l'absence de mot de passe pour se connecter à un équipement, etc. Les vulnérabilités liées aux erreurs humaines (par exemple liées à un manque de formation ou à une fatigue de l'humain) peuvent impliquer la connexion, non sécurisée ou non maîtrisée sur le réseau, de PC portables ou smartphones, l'absence de verrouillage du poste de travail en quittant ce dernier (ordinateur, interface de pilotage, console de programmation industrielle…), l'utilisation de matériel non protégé, une imprudence liée à l'ouverture de pièces jointes à un mail ou l'accès à un site Internet clairement frauduleux. L'absence de politique de sécurité des systèmes d'information constitue généralement une vulnérabilité organisationnelle reflétant une gouvernance faible du risque cyber.
Dans la suite de cet article, le processus d'analyse du risque cyber est présenté à travers ses similitudes avec l'analyse du risque professionnel lié à la conception des machines, en pointant les différences dans les termes employés. Ceci permettra au lecteur de mieux s'approprier les notions relatives à l'analyse du risque cyber.

Parallèle entre l'analyse du risque cyber et l'analyse du risque professionnel machine

Portée de l'analyse du risque cyber

Dans le cadre de l'analyse du risque professionnel lié aux machines et comme présenté dans la norme NF EN ISO 12100 [2], la mise en place des mesures de prévention ne fait pas partie de la phase d'analyse du risque mais de la phase de réduction du risque. Le référentiel normatif NF EN ISO/IEC 27005 [9] sur la sécurité de l'information propose le même processus : appréciation du risque (incluant l'analyse du risque) suivie de la

→

ENCADRÉ

CONSÉQUENCES D'UNE CYBERATTAQUE SUR UNE MACHINE

Pour une machine, une cyberattaque intervient dans le processus de survenue d'un dommage en tant qu'événement dangereux – par exemple, un mouvement non voulu d'un élément mobile de la machine. Une cyberattaque peut également corrompre une mesure de protection d'un risque mécanique mise en œuvre dans le plan de gestion des risques au sens de la norme NF EN ISO 12100 [2]. Ainsi, une cyberattaque sur un robot mobile présentant un risque lié à sa chute (phénomène dangereux dû à son énergie potentielle) peut contribuer au processus menant au dommage, en déclenchant sa chute.
Une cyberattaque ne crée pas de nouveaux phénomènes dangereux mais intervient en tant qu'événement dangereux, qui peut conduire à un dommage, en fonction du scénario opérationnel envisagé.
Comme évoqué précédemment dans cet article *(Cf. § « Le risque cyber » p. 6)* ainsi que dans la note technique déjà parue [4], une cyberattaque peut également générer du stress, facteur de risques psychosociaux chez les salariés.

↓TABLEAU 2
Parallèle entre les termes de l'analyse du risque cyber et de l'analyse du risque professionnel machine.

ANALYSE DU RISQUE CYBER	ANALYSE DU RISQUE PROFESSIONNEL MACHINE
Détermination du contexte de l'analyse : • fonctions, processus, données critiques, activités ; • description des usages ; • contexte de l'entreprise.	Fonction de la machine – Périmètre et contexte de l'analyse – Informations pour l'appréciation du risque. Détermination des limites de la machine : • limites spatiales (exemple : interactions humaines) ; • limites d'utilisation (exemple : mode de fonctionnement).
Phase d'identification des sources de risque (menaces) et des vulnérabilités.	Phase d'identification des phénomènes dangereux (énergies…).
Scénario macroscopique et événements principaux préjudiciables. Estimation de l'impact de l'événement.	Analyse préliminaire de risque. Dommages possibles. Estimation du ou des dommages : gravité.
Action finale de la cyberattaque (« eXploiter ») et atteinte à la cybersécurité.	Événement dangereux.
Scénario opérationnel (le comment : *kill chain*) ➜ Vraisemblance.	Processus d'apparition du dommage ➜ Probabilité d'occurrence du dommage.
Risque = fonction de la gravité de l'impact et de la vraisemblance de l'attaque.	Risque = fonction de la gravité du dommage et de la probabilité d'occurrence du dommage.

phase de traitement du risque, notion équivalente à la réduction du risque. La méthode EBIOS-RM [5] propose également ces deux phases. Seule la phase d'analyse du « risque cyber » est présentée dans cet article.

Parallèle entre les analyses du risque cyber et du risque professionnel machine

Pour faire un parallèle avec l'analyse du risque professionnel machine de la norme NF EN ISO 12100, qui est constituée de trois étapes – détermination des limites de la machine, identification des phénomènes dangereux et estimation du risque –, l'analyse du risque cyber peut également être décomposée en trois étapes *(Cf. Figure 4)* :
• la description du système à étudier, le périmètre de l'analyse et le contexte ;
• l'identification des risques ;
• l'estimation des risques.

La première étape consiste à borner le périmètre de l'analyse (une machine, par exemple), à décrire le système analysé, puis à recueillir les informations sur le contexte de l'entreprise, comme son domaine d'activité. Ces éléments permettront d'identifier les risques et de contribuer à leur estimation *(Cf. Encadré)*.
La deuxième étape est l'identification des risques : elle vise à préciser, à l'aide du contexte et de la description du système objet de l'analyse, la menace, les vulnérabilités, ainsi que les événements préjudiciables pour l'entreprise.
La troisième étape consiste à estimer les risques, en s'appuyant sur la cotation de la vraisemblance de l'attaque et sur la cotation de son impact.
Pour décrire plus finement cette analogie dans les étapes de l'analyse du risque (risque cyber ou risque professionnel machine), le *Tableau 2* présente les correspondances des termes employés dans le cadre de ces deux démarches d'analyse.
Le terme de « vraisemblance » mérite une attention particulière. L'estimation de la vraisemblance consiste à se positionner sur le fait que l'attaque réussisse ou non. Le *Tableau 3* explicite les paramètres qui permettent d'estimer la vraisemblance, et montre le parallèle avec la probabilité d'occurrence du dommage pour le risque professionnel.

L'analyse du risque cyber pour les machines

Sur la base des éléments précédents, une représentation graphique du processus de l'analyse du risque cyber pour les machines, des éléments constituant cette analyse et de leur articulation est proposée dans la *Figure 5*.
Dans cet article, c'est l'impact humain et les possibles dommages causés aux salariés qui nous intéressent. Pour déterminer cet impact, on l'évalue sur la base de scénarios « de haut niveau » (macroscopiques), qui ne nécessitent pas une

ESTIMATION DE LA VRAISEMBLANCE (RISQUE CYBER)	PROBABILITÉ D'OCCURRENCE DU DOMMAGE (RISQUE MACHINE)
Pas de déclinaison normative pour la vraisemblance, mais elle peut s'estimer grâce à : • la probabilité de survenue de l'incident ; • la fréquence des incidents (si connue) ; • la facilité d'exploitation des vulnérabilités ; • le degré de motivation de la menace (coût/bénéfice de l'attaque) et les capacités de la menace ; • la difficulté technique du scénario ; • la vulnérabilité intrinsèque au nouveau produit (projet/matériel récent peu éprouvé) ; • les vulnérabilités observées sur le système étudié ou l'organisation (précédents audits ou contrôles) ; • l'exposition et la visibilité de l'entreprise vis-à-vis de l'extérieur (un grand groupe, un secteur d'activité stratégique peuvent être plus visés) ; • une sécurité numérique du système lacunaire (par exemple : mesures de sécurité prévues non appliquées) ; • etc.	**Combinaison de :** • l'exposition au phénomène dangereux (source potentielle de dommage comme l'énergie cinétique, des éléments mobiles en mouvement, un fluide sous pression) ; • la probabilité d'occurrence d'un événement dangereux (probabilité de survenue de l'événement susceptible de causer un dommage tel que l'éclatement d'un outil, le contact avec des parties en mouvement) ; • la possibilité d'éviter ou de limiter le dommage (par exemple, vitesse de déplacement réduite).

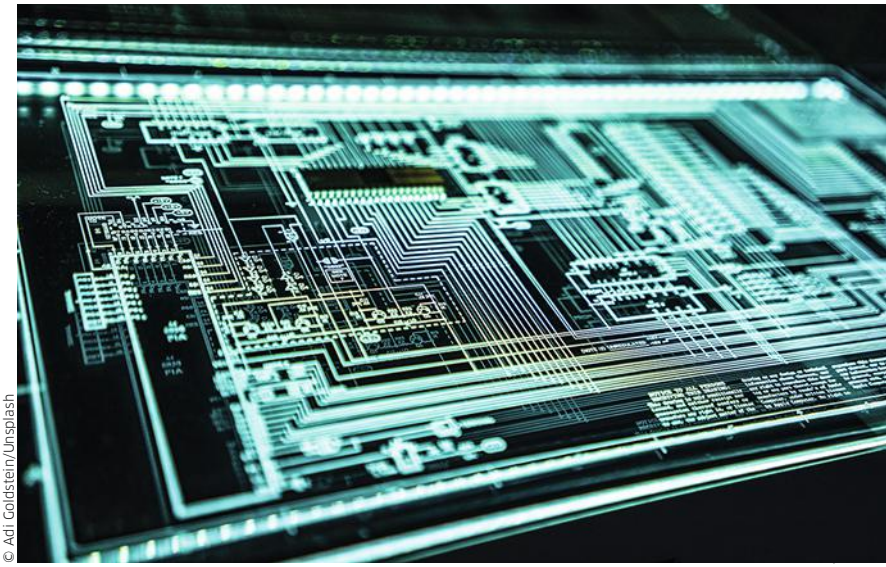
←TABLEAU 3
Paramètres pouvant servir à l'estimation de la vraisemblance et parallèle avec la probabilité d'occurrence du dommage.

connaissance fine de l'installation, mais une vue fonctionnelle qui tient compte du contexte de l'entreprise. Ces scénarios de haut niveau servent à déterminer les événements principaux susceptibles d'être préjudiciables à la santé ou à la sécurité des salariés. Il faut imaginer en quoi une cyberattaque pourrait impacter les fonctions, les processus, les activités et les données critiques pour l'intégrité des salariés.

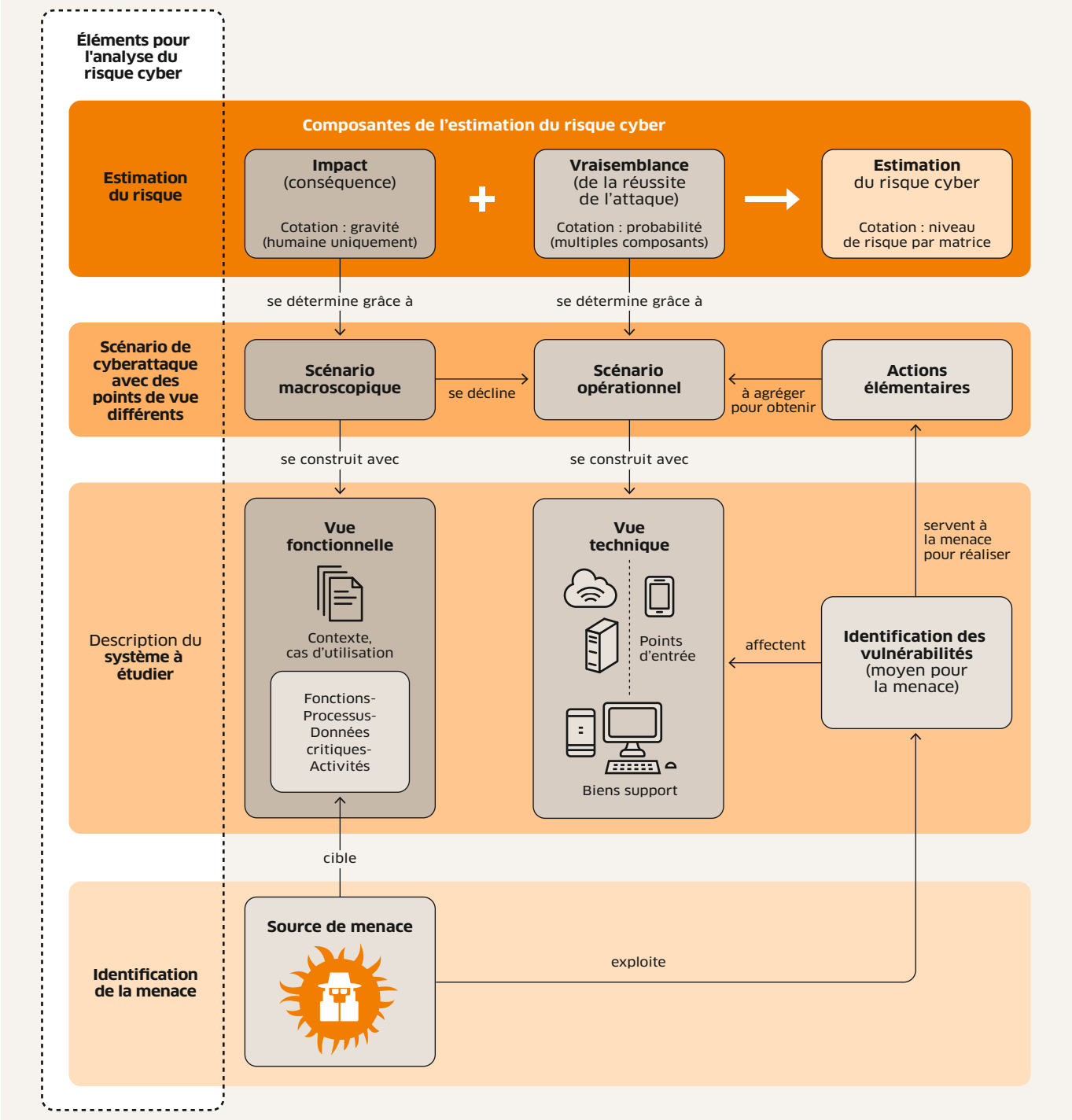
La vraisemblance permet d'estimer la probabilité de réussite de l'attaque. Pour la déterminer, les scénarios de haut niveau sont déclinés en scénarios opérationnels, élaborés avec une vue technique de la machine, afin d'expliciter comment l'attaquant (la source de la menace) peut atteindre son objectif. Ce sont les scénarios d'attaque, chemins d'attaque ou *kill chain* C-R-T-X, tels que présentés précédemment. Exprimé autrement, il convient d'identifier les fonctions, les processus, les données et les activités ciblés par la source de la menace et les vulnérabilités qu'elle exploiterait pour imaginer un ou plusieurs scénarios opérationnels ; ces vulnérabilités sont un moyen pour que la menace effectue différentes actions élémentaires telles que le *phishing* (captation de données sensibles ou confidentielles), le déplacement dans le système pour atteindre la cible, la finalisation de l'attaque telle qu'un déni de service. Les vulnérabilités affectent généralement des éléments techniques (matériel ou logiciel) et tout ce qui peut servir de support à la réalisation des fonctions, des processus et des activités. On parle ainsi de « biens supports ». Ce sont eux qui peuvent être directement ciblés par la menace et « attaqués » par l'intermédiaire de points d'entrée, comme un port USB, une connexion au réseau, ou tout autre moyen d'échange de données avec la cible.

La *Figure 5* présente ainsi une décomposition plus fine de l'analyse du risque cyber pour les machines, avec ses principaux éléments : l'identification de la menace, la description du système, les scénarios de cyberattaque avec des points de vue différents (en premier une vue macroscopique, haut niveau pour les scénarios macroscopiques, et une vue plus détaillée avec les scénarios opérationnels), et enfin l'estimation du risque. L'identification de la menace et le scénario de cyberattaque correspondent à l'étape d'identification des risques de la *Figure 4*. Chaque scénario va être coté avec un niveau de risque.

→



© Adi Goldstein/Unsplash



↑FIGURE 5
Représentation de la démarche d'analyse du risque cyber pour les machines.
À gauche, éléments constituant l'analyse : identification de la menace, description du système, scénarios de cyberattaque avec des points de vue différents.

Conclusion

Si le vocabulaire employé pour décrire la cybersécurité est spécifique, les principes de prévention des risques restent similaires à ceux utilisés dans le domaine des risques professionnels associés aux machines ; on y retrouve globalement les mêmes étapes dans le processus d'analyse du risque. La spécificité intervient dans les composantes du risque avec, pour le risque cyber, la notion d'impact qui est plus large que le dommage pour le salarié, et la notion de vraisemblance. Le langage employé est généralement d'un style militaire (attaque, défense, charge…), du fait que les secteurs stratégiques de la nation ont été les premiers à prendre en charge ce risque, notamment ceux de la défense et du renseignement.

L'INRS poursuit ses travaux sur l'analyse du risque cyber pour les machines, en la transposant au contexte des machines industrielles, et en examinant comment elle peut s'articuler avec l'analyse des risques professionnels, ou en réexploiter des éléments.

GLOSSAIRE

- **Attaquant :** une personne, un groupe, une organisation, un état, qui exécute une attaque.
- **Chemin d'attaque (ou *cyber kill chain*) :** les différentes étapes qu'un attaquant suit ou qu'il envisage de suivre pour exécuter son attaque.
- **Code malveillant :** un programme développé dans le but de causer un dommage à un système numérique.
- **Cyberattaque :** attaque qui vise les systèmes numériques (par exemple informatiques ou automatismes programmables industriels) dans le but de satisfaire des intentions malveillantes.
- **Cybersécurité :** état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace, susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.
- **Impact-s :** conséquence-s d'une attaque.
- **Intrusion :** acte d'une personne ou d'un objet entrant dans un espace défini (physique, logique) où sa présence n'est pas souhaitée.
- **Malware :** logiciel qui compromet le fonctionnement d'un système en réalisant un process ou une fonction non autorisée.
- **Menace :** terme générique utilisé pour désigner toute intention, malveillante ou involontaire, susceptible de provoquer un risque.
- **Vraisemblance :** probabilité de réussite de l'attaque (s'estime qualitativement).
- **Vulnérabilité :** faille de sécurité qui affecte un produit logiciel, un système numérique ou un composant matériel. Elle peut servir de point d'entrée pour des actions malveillantes d'un attaquant s'il décide de les exploiter. Les vulnérabilités logicielles sont corrigées par des mises à jour publiées par les éditeurs de logiciels.

Pour des aspects méthodologiques plus développés sur l'analyse du risque cyber, le lecteur peut se reporter à une récente publication dans une revue internationale [10].
Cette publication est une première proposition pour des systèmes industriels ; les travaux actuels visent à proposer une approche encore plus dédiée et outillée pour les machines industrielles du secteur manufacturier. ●

1. Voir le référentiel proposé par l'Anssi concernant les expressions et sigles du domaine de la cybersécurité, accessible sur : https://cyber.gouv.fr/cyberdico. Les termes les plus utilisés se rapportant au risque cyber sont explicités dans le glossaire en fin d'article.

BIBLIOGRAPHIE

[1] RÈGLEMENT (UE) 2023/1230 du Parlement européen et du Conseil du 14 juin 2023 sur les machines, abrogeant la directive 2006/42/CE et la directive 73/361/CEE. *JOUE* du 29 juin 2023. Accessible sur : https://eur-lex.europa.eu/

[2] NORME NF EN ISO 12100 – *Sécurité des machines – Principes généraux de conception. Appréciation du risque et réduction du risque.* Iso/Afnor, décembre 2010. Accessible sur : https://www.boutique.afnor.org (site payant).

[3] RAPPORT TECHNIQUE 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.* Afnor, décembre 2018. Accessible sur : https://www.boutique.afnor.org (site payant).

[4] LAMY P. – Sécurité des machines : « le risque cyber » comme risque émergent ? *Hygiène & sécurité du travail,* 2019, 256, NT 76, pp. 72-79. Accessible sur : https://www.inrs.fr/media.html?refINRS=NT%2076

[5] ANSSI – EBIOS-RM – *Expression des besoins et identification des objectifs de sécurité – Risk manager.* Accessible sur : https://cyber.gouv.fr/la-methode-ebios-risk-manager

[6] ANSSI – *Le Panorama de la cybermenace.* Accessible sur : https://cyber.gouv.fr/le-panorama-de-la-cybermenace

[7] CERT-FRANCE (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) – *Alertes de sécurité.* Accessible sur le site : https://www.cert.ssi.gouv.fr/

[8] MITRE – *Common vulnerabilities and exposures (CVE).* Accessible sur : https://cve.mitre.org

[9] NORME NF EN ISO/IEC 27005 – *Sécurité de l'information, cybersécurité et protection de la vie privée – Préconisations pour la gestion des risques liés à la sécurité de l'information.* Iso/Afnor, août 2024. Accessible sur : https://www.boutique.afnor.org (site payant).

[10] LAMY P., FLAUS J.M. – A method of cyber risk assessment for occupational risk in machinery. *International journal of occupational safety and ergonomics,* mars 2026. Accessible sur : https://doi.org/10.1080/10803548.2025.2595860