NORMALISATION UNM

GUIDE CYBERSÉCURITÉ DES MACHINES

2025

Préambule

Le présent document a été mis au point par un groupe rassemblant des experts des commissions de normalisation UNM 45 « Sécurité des machines » et AFNOR UF 44 « Sécurité des machines - Aspects électrotechniques ».

Les sociétés suivantes ont contribué à sa rédaction :

- Cetim
- FIM
- Ineris
- INRS
- JDF Safety Management
- Rehlko
- Ministère du Travail
- Schneider Electric
- Wilo

Le lecteur est seul responsable de l'adéquation du contenu du document avec ses besoins spécifiques.

L'UNM et les organismes ayant contribué à l'élaboration de ce guide ne sauraient être tenus responsables des éventuels dommages directs ou indirects résultant de l'utilisation, de l'interprétation ou de la mise en œuvre des informations présentes dans ce document.

Compte tenu de l'évolution rapide de ces technologies, le présent guide contient l'état des connaissances des membres du groupe au moment de sa parution et est susceptible d'être révisé.

Les réglementations, référentiels et normes présentés dans ce guide ne constituent pas un ensemble exhaustif. Il s'agit d'une base minimale commune mais chaque entreprise doit analyser le cadre réglementaire et sectoriel de son activité car des normes, référentiels ou réglementations particulières peuvent exister et porter certaines exigences de cybersécurité.

Introduction

Le Règlement (UE) 2023/1230 relatif aux machines a été adopté par l'Union Européenne en juin 2023 et sera applicable en janvier 2027, remplaçant la Directive 2006/42/CE. Objectif : intégrer de nouvelles exigences relatives à la sécurité des machines notamment en traitant de nouveaux risques, par exemple liés aux cyberattaques.

Avec l'essor des systèmes connectés et autonomes, la cybersécurité devient une priorité. En effet, les enjeux de sécurité numérique sont associés aux préoccupations économiques, stratégiques ou encore d'image qui sont celles d'une entreprise.

La connectivité accrue des machines et leur interaction avec des réseaux, y compris l'Internet des objets (IoT), exposent ces équipements à des risques de cyberattaques. Les machines peuvent être vulnérables à des attaques malveillantes telles que le piratage, les ransomwares ou l'exploitation de failles dans les logiciels embarqués. Ces cybermenaces peuvent avoir des conséquences graves, allant de la perturbation de la production industrielle à des accidents de sécurité potentiellement mortels.

Le Règlement Machines 2023/1230 exige des fabricants qu'ils tiennent compte des risques liés à la cybersécurité lors de la conception des machines. Cela inclut l'intégration de mécanismes de protection contre les cyberattaques et la mise en place de processus de gestion des vulnérabilités. En contextualisant le besoin, en rappelant l'objectif poursuivi et en y répondant par la mesure concrète correspondante, des règles d'hygiène informatique doivent être suivies. Les machines doivent respecter des exigences strictes en matière de sécurité dès la conception et tout au long de leur cycle de vie, y compris lors de leur mise à jour logicielle.

Sommaire

1 Cible/scope

L'objectif de ce document est d'aider les bureaux d'études des entreprises de la mécanique à disposer d'une vision d'ensemble sur les aspects cybersécurité pour concevoir le système de commande des machines en toute sécurité et anticiper le contexte réglementaire à venir.

2 Contexte réglementaire

Le Règlement machines 2023/1230 s'adresse aux fabricants de machines.

Extrait du règlement :

1.1.9 Protection contre la corruption

La machine ou le produit connexe sont conçus et construits de telle sorte que le raccordement à ceux-ci d'un autre dispositif, par l'intermédiaire de toute caractéristique du dispositif connecté lui-même ou de tout dispositif distant qui communique avec la machine ou le produit connexe, ne crée pas de situation dangereuse.

Un composant matériel informatique de transmission de signaux ou de données, pertinent pour le raccordement ou l'accès au logiciel qui est essentiel pour la conformité de la machine ou du produit connexe aux exigences essentielles de santé et de sécurité pertinentes, est conçu de manière à être protégé de manière adéquate contre la corruption accidentelle ou intentionnelle. La machine ou le produit connexe recueillent la preuve d'une intervention légitime ou illégitime dans ce composant matériel informatique, quand cela est pertinent pour la connexion ou l'accès à un logiciel essentiel pour la conformité de la machine ou du produit connexe.

Les logiciels et les données essentiels pour la conformité de la machine ou du produit connexe aux exigences essentielles de santé et de sécurité pertinentes sont identifiés comme tels et sont protégés de manière adéquate contre la corruption accidentelle ou intentionnelle.

La machine ou le produit connexe identifient les logiciels installés sur ceux-ci dont ils ont besoin pour fonctionner en toute sécurité, et ils sont en mesure de fournir ces informations à tout moment sous une forme aisément accessible.

La machine ou le produit connexe recueillent la preuve d'une intervention légitime ou illégitime dans les logiciels ou d'une modification des logiciels installés sur ceux-ci ou de sa configuration.

1.2.1 Sécurité et fiabilité des systèmes de commande [1]

Les systèmes de commande sont conçus et construits de manière :
a) à pouvoir résister, lorsque les circonstances et les risques le justifient, aux contraintes d'exploitation prévues et aux influences extérieures volontaires et involontaires, y compris les tentatives malveillantes raisonnablement prévisibles de tiers conduisant à créer une situation dangereuse.

[1] Il s'agit du principal aspect lié à la cybersécurité dans cet article mais le 1.2.1 doit être lu dans son ensemble pour apprécier l'impact sur la cybersécurité.

En complément au Règlement Machines :

Le Cyber résilience Act (CRA) 2847/2024 est un règlement européen ayant pour objectif de définir des règles de cybersécurité minimum pour les produits composés d'un ou plusieurs éléments numériques vendus sur le marché de l'UE, considérés comme composants (matériel ou logiciel) du point de vue du fabricant de machine.

Il inclut des obligations relatives à la conception, à la gestion des vulnérabilités et à l'obligation d'information et de notification. Si un fabricant de machine intègre ces composants, il va pouvoir récupérer ces informations pour les exploiter dans le cadre de la conception de sa machine et dans le cadre de son obligation d'informer l'utilisateur de ses vulnérabilités.

Il est donc complémentaire à **la directive NIS 2 2022/2555** (concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'Union Européenne) qui traite d'opérateurs de services. De manière simplifiée, le CRA visera à sécuriser les produits numériques utilisés dans l'UE par les entreprises et le grand public alors que NIS 2 a pour objectif de sécuriser les moyens de production des entreprises et administrations de l'UE. Un fabricant de machines est soumis à NIS2 si sa propre activité rentre dans les 18 secteurs **d'activité concernés (voir annexes I et II de la directive, en particulier le secteur « fabrication »).** Mais, s'il vend des machines à des entreprises de l'un de ces 18 secteurs d'activité, des exigences par ricochet pourraient être répercutées par ses clients pour ces machines (dans un cadre contractuel en réponse à un cahier des charges).

De son côté, **la Directive RED 2014/53/UE** concerne la mise à disposition sur le marché d'équipements radioélectriques et s'adresse aux fabricants de composants (matériel ou logiciel). En complément du CRA, elle contient une exigence de ne pas perturber le réseau internet public.

3 Terminologie de base

Afin d'aider le lecteur novice sur le sujet et pour le familiariser avec le vocabulaire, nous proposons ci-dessous une liste non exhaustive de termes et acronymes employés dans le cadre de la cybersécurité. Pour compléter cette liste, le cyberdico peut aussi être consulté sur le site de l'ANSSI. **(CyberDico, Qu'est-ce que c'est ? | ANSSI)**.

Termes :

Note : les termes encadrés en vert sont issus du cyberdico.

Backdoor	Accès dissimulé, soit logiciel soit matériel, qui permet à un utilisateur de se connecter à une machine distante, de manière furtive.
Balayage de ports	Technique qui consiste à envoyer des paquets de données sur les différents ports d'une machine, puis à en déduire les états (la disponibilité) de ces ports en fonction de la réponse retournée, si elle existe.
Chemin d'attaque, scénario d'attaque-kill chain (pour la traduction et usage)	Suite d'événements distincts que la source de risque devra probablement générer pour atteindre son objectif.
Défense en profondeur	Mécanisme de défense basé sur la superposition de mesures.
Elévation de privilège	Obtention de privilège supérieur par exploitation d'une vulnérabilité. Par exemple, si un utilisateur local accède à des droits normalement réservés à l'administrateur, il y a élévation de privilège. Une élévation de privilège est souvent recherchée par une personne malveillante lorsqu'elle a réussi à s'introduire sur un système d'information en usurpant l'identité d'un utilisateur légitime.
Enregistreur de frappes, capteur clavier	Logiciel ou matériel employé par un utilisateur malveillant pour capturer ce qu'une personne frappe au clavier.
État de la menace	L'état de la menace caractérise, sur une période et un périmètre donnés, la nature et le niveau de risque atteints selon différentes variables telles que le type de menace, les acteurs concernés, les tendances observées, les modes opératoires à l'oeuvre, les objectifs visés ou encore les moyens disponibles. Pour dresser ce panorama, l'ANSSI s'appuie sur une typologie de la menace en quatre catégories : cybercriminalité, déstabilisation, espionnage, sabotage.

Termes :

Note : les termes encadrés en vert sont issus du cyberdico.

Faux positif	Qualification erronée d'un évènement en tant qu'évènement de sécurité d'origine cyber.
Force-brute	Technique d'attaque consistant à utiliser un nombre exhaustif d'authentifiant générés aléatoirement afin de deviner le bon mot de passe.
Hygiène informatique	Règles ou procédures que les individus et organisations mettent en place pour assurer la sécurité de leurs systèmes d'information (par ex utilisation de gestionnaire/coffre-fort de mots de passe).
Impact	Effet, conséquence d'un événement non souhaité (cyberattaque en l'occurrence) ; équivalent au dommage (selon ISO 12100). L'impact peut être catégorisé : impact financier, impact juridique, impact humain, impact environnemental. Il est qualifié par sa gravité.
Intégrité	Garantie que le système et l'information traitée ne sont modifiés que par une action volontaire et légitime.
Menace numérique	Terme générique utilisé pour désigner toute intention hostile de nuire dans le cyber espace. Une menace peut être ciblée ou non sur l'objet de l'étude.
Mitigation	Mesures destinées à supprimer ou réduire l'impact de cyberattaques.
Phishing ou Hameçonnage	Vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime. Les sites sont reproduits, après avoir été aspirés. L'utilisateur est souvent invité à visiter le site frauduleux par un courrier électronique.
Remédiation	La remédiation consiste en la reprise de contrôle d'un système d'information compromis et le rétablissement d'un état de fonctionnement suffisant du service suite à une attaque cyber.
Source de risque	Élement, personne, groupe de personnes ou organisation susceptible d'engendrer un risque.

Termes :

Note : les termes encadrés en vert sont issus du cyberdico.

Surface d'attaque	Ensemble des points faibles, des points d'entrée face à une attaque.
Test d'intrusion	Action qui consiste à essayer plusieurs codes d'exploitation sur un système d'information, afin de déterminer ceux qui donnent des résultats positifs. Remarque : il s'agit à la fois d'une intention défensive (mieux se protéger) et d'une action offensive (agresser son propre système d'information).
Vraisemblance	Probabilité d'occurrence de la cyberattaque – concept similaire à la probabilité d'occurrence du dommage (selon ISO 12100).
Vulnérabilité	Faille de sécurité pouvant affecter un logiciel, un système d'information ou encore un composant matériel. Elle peut servir de porte d'entrée pour des acteurs malveillants s'ils parviennent à l'exploiter. Les vulnérabilités sont généralement corrigées lors des mises à jour ou par des correctifs publiés par les éditeurs.
Vulnérabilité Jour 0 (Zero-day vulnerability)	Vulnérabilité n'ayant fait l'objet d'aucune publication ou n'ayant reçu aucun correctif.

Acronymes :

APT : Advanced Persistent Threat	Attaque prolongée et ciblée par des cybercriminels visant à accéder à un réseau et à rester non détectée pendant une longue période. Ce type d'attaque nécessite des moyens humains, financiers et repose sur une complexité des moyens utilisés.
CERT : Computer Emergency Response Team	Centre de réponse aux incident cyber.
CVE : Common Vulnerabilities and Exposure	Inventaire des vulnérabilités de sécurité (https://www.cve.org).
CVSS : Common Vulnerability Scoring System	Système de cotation des CVE pour en évaluer la criticité entre 0 et 10.

Acronymes :

Note : les termes encadrés en vert sont issus du cyberdico.

DoS : Denial of Service

Le déni de service est une action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu.

Comprendre et anticiper les attaques DDoS

Les attaques par déni de service distribué (Distributed Denial of Service ou DDoS) constituent une menace pour toute organisation disposant d'un système d'information connecté à Internet. Le guide de l'ANSSI « Comprendre et anticiper les attaques DDoS » présente les solutions existantes permettant d'anticiper cette menace, et de faire face à une attaque DDoS.
https://cyber.gouv.fr/publications/comprendre-et-anticiper-les-attaques-ddos

IGC : Infrastructure de gestion de clés

Ensemble organisé de composantes fournissant des services de gestion des clés cryptographiques et des certificats de clés publiques au profit d'une communauté d'utilisateurs.

OIV : Opérateur d'Importance Vitale

Organisation identifiée par l'état français comme ayant des activités indispensables à la survie de la nation ou dangereuses pour la population.

IDS : Système de détection d'intrusion

Un système de détection d'intrusion (Intrusion Detection System - IDS) est un dispositif logiciel ou matériel dont le rôle est de capter, puis d'analyser, l'activité d'un système numérique, dans le but de détecter les attaques ou les signes de compromission dont ce dernier est la cible. Un IDS se caractérise par la source de donnée utilisée pour capter l'activité d'un système (réseau, système, applicative) et par la méthode de détection employée pour distinguer les activités malveillantes des activités légitimes.

4 Les Guides ANSSI

En France, l'ANSSI, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cybersécurité. Même si ces documents n'ont pas été rédigés pour traiter de la conception des machines, les fabricants de machines peuvent les utiliser comme traduisant l'état de l'art en cybersécurité.

Le **Guide d'hygiène informatique** de l'ANSSI comporte 42 règles simples qui permettent la mise en place de plan d'actions prioritaires et renforcées à partir d'un état des lieux et d'un outil de suivi. Ces règles sont regroupées dans les rubriques suivantes :

Sensibiliser et former

Par exemple, chaque utilisateur, dès son arrivée dans l'entité, doit être informé des enjeux de sécurité, des règles à respecter et des bons comportements à adopter en matière de sécurité des systèmes d'information.

Connaître le système d'information

Par exemple, les données sensibles (propriété intellectuelle, savoir-faire, données personnelles, contrats, etc.) doivent être identifiées afin de pouvoir les protéger efficacement.

Authentifier et contrôler les accès

Par exemple, l'utilisation de comptes génériques (ex : admin, user) doit être marginale et ceux-ci doivent pouvoir être rattachés à un nombre limité de personnes physiques.

Sécuriser les postes

Par exemple, limiter les applications installées et modules optionnels des navigateurs web aux seuls nécessaires.

Sécuriser le réseau

Par exemple, segmenter le réseau et mettre en place un cloisonnement entre ces zones.

Sécuriser l'administration

Par exemple, utiliser un réseau dédié et cloisonné pour l'administration du système d'information.

Gérer le nomadisme

Par exemple, chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable.

Maintenir le système d'information à jour

Par exemple, définir une politique de mise à jour des composants du système d'information en s'informant de l'apparition de nouvelles vulnérabilités et appliquer les correctifs de sécurité dans le mois qui suit leurs publications. Il est possible de s'informer sur le site du CERT-FR (https://www.cert.ssi.gouv.fr) ou sur les sites Internet des constructeurs et éditeurs.

Superviser, auditer, réagir

Par exemple, activer et configurer les journaux des composants les plus importants.

Le guide **La cybersécurité pour les TPE/PME en treize questions** présente des mesures accessibles pour une protection globale de l'entreprise qui permettront d'accroître le niveau de sécurisation et de sensibiliser les équipes aux bons gestes à adopter.

Le guide **Méthode de classification et mesures principales** des systèmes industriels propose une méthode d'évaluation des niveaux d'exposition, de vraisemblance et des impacts permettant de déterminer une classe de risque. Des cas d'étude simplifiés illustrent l'utilisation de la méthode.

Le guide **Maîtriser la SSI pour les systèmes industriels** propose une démarche de sensibilisation et de mise en œuvre de bonnes pratiques pour accompagner les entreprises dans le déploiement de la sécurité permettant de protèger les investissements et la production de l'entreprise.

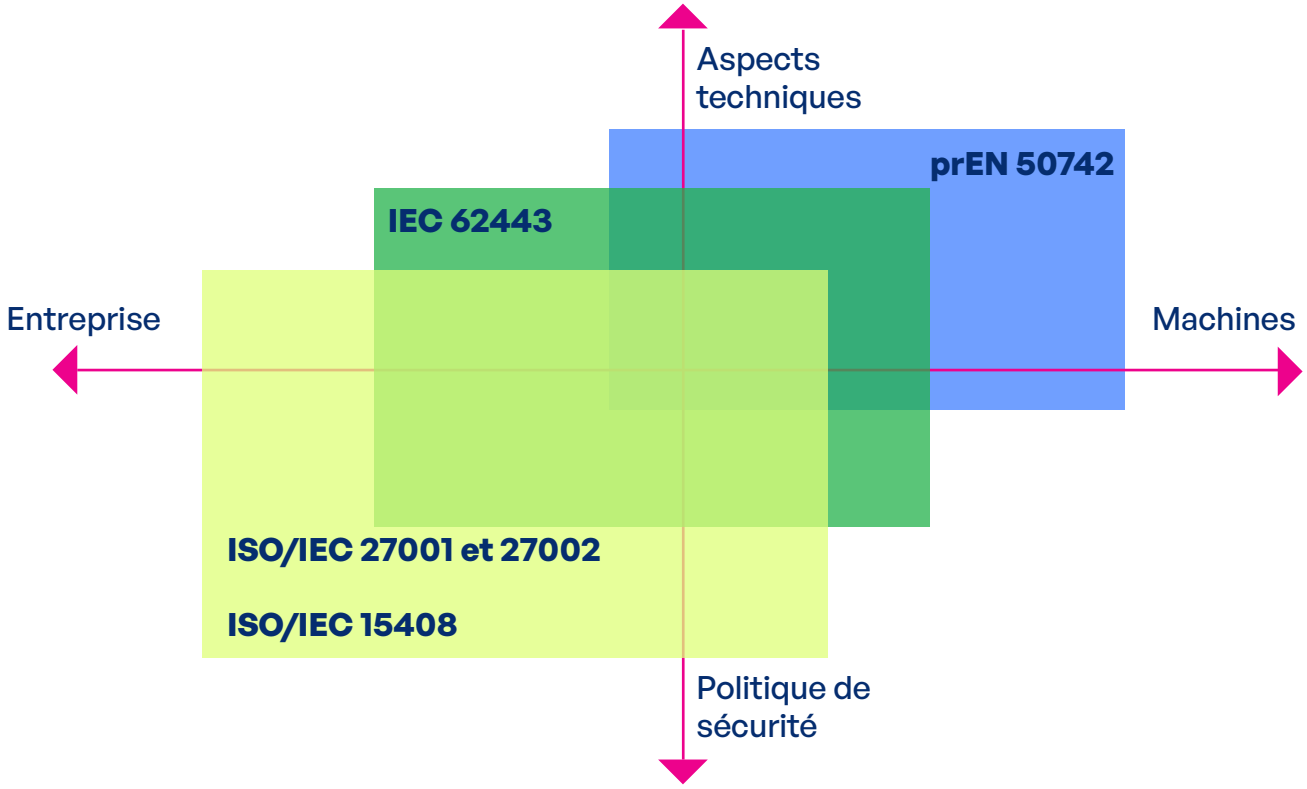
Le guide **Recommandations relatives à la sécurité des systèmes d'objets connectés** propose de faciliter la réalisation d'une analyse de sécurité, à partir de la prise en compte des scénarios d'attaques probables. Il propose enfin des recommandations techniques pour remédier quand cela est possible aux risques identifiés.

L'ANSSI publie aussi un ensemble de guides sur la **remédiation**, qui décrit les principes du pilotage et de la mise en œuvre d'une remédiation au sein d'une organisation affectée par un incident de sécurité.

Le **CyberDico** de L'ANSSI présente les définitions des mots, sigles et expressions de la cybersécurité en français et en anglais.

5 Les normes

Le corpus des normes internationales de la sécurité numérique peut être cartographié par la figure suivante.



La cybersécurité des systèmes d'information est traitée par la série des normes **ISO/IEC 27000**. Son évaluation est définie par l'**ISO/IEC 15408**. Ces normes horizontales s'appliquent en général aux systèmes d'information de l'entreprise.

La sécurité des systèmes d'automatisation et de commandes industriels est traitée par la série **IEC 62443** où les aspects liés à la gestion des processus industriels et la sécurité humaine sont pris en compte.

L'accroissement des échanges des données avec les systèmes industriels et les systèmes de traitement de l'information influence l'évolution de ces normes pour les rendre plus cohérentes et plus adaptables aux besoins.

Le projet de norme harmonisée **EN 50742** sur la protection contre la corruption selon le règlement européen sur les machines (UE) 2023/1230 est en cours de développement.

L'ISO/TR 22100-4

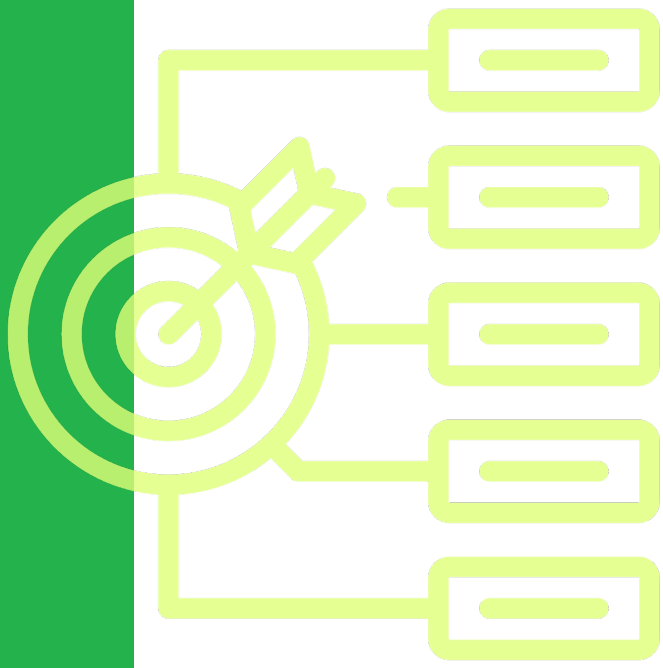
L'ISO/TR 22100-4 *Sécurité des machines — Relation avec l'ISO 12100 — Partie 4: Lignes directrices pour les fabricants de machines concernant les aspects liés à la sécurité informatique (cybersécurité)* donne aux fabricants de machines des indications pour identifier et traiter les menaces pour la sécurité informatique qui peuvent avoir une incidence sur la sécurité des machines.

Il commence par montrer la différence d'approche entre sécurité des machines (en anglais « safety ») et sécurité informatique (en anglais « security ») du point de vue de l'analyse des risques. Contrairement aux principes de base de sécurité des machines visant à traiter des risques raisonnablement prévisibles, les aspects cybersécurité couvrent les actes de malveillance intentionnelle.

L'ensemble des mesures d'élimination et d'atténuation des risques est analysé sous l'angle des vulnérabilités éventuelles à l'égard des menaces, sachant que la vulnérabilité est directement liée aux accès directs et indirects aux systèmes d'information de la machine. Le fabricant peut dans un premier temps se poser des questions vis-à-vis des accès : besoin de connexion, en continu, surveillée, configurable, en lecture seule...

5 étapes sont indiquées pour couvrir le risque cyber :

- Identifier les menaces et les vulnérabilités
- Protéger la machine
- Détecter les occurrences de cyber attaques
- Mener des actions si une attaque est détectée
- Maintenir les plans de résilience et restaurer les capacités et les services qui ont été altérés à la suite d'une attaque



L'ISO/TR 22100-4

Dans le TR /ISO 22100-4, un tableau fournit une liste de mesures de réduction des risques en fonction des aspects à protéger et donne les rôles des acteurs (fabricant de la machine, intégrateur, utilisateur final) pour chacune de ces mesures. Ces acteurs sont complémentaires et nécessaires pour assurer la cyberscurité de l'équipement, voire de l'entreprise. Par exemple, en cas de maintenance à distance, permettre d'activer ou désactiver une session de pilotage à distance.

Puis, les principes de base de conception de machine sont listés comme par exemple équiper la machine de pare-feux et d'antivirus, de système de demande d'autorisation (mots de passe), ...

Enfin, le document contient un ensemble de recommandations d'informations à transmettre aux acteurs par l'intermédiaire de la notice d'instruction.

Certaines normes ou projets dédiés à des équipements spécifiques intègrent des aspects cybersécurité, par exemple la série ISO 10218.

6 Les conseils pour initier la démarche sur les aspects cybersécurité dans la conception d'une machine

Quels sont les dangers ?	Quelle exposition prévue (accès physique, connectivité) ?	Quels impacts sur la sécurité humaine, sur les fonctions de sécurité ?	Comment éliminer ou protéger l'accès et enregistrer les interventions ?	Quelles sont les informations pour une utilisation sûre de la machine ?
1 S'appuyer sur l'ISO 12100	2 Définir les limites de l'environnement cyber pour établir la chaine de confiance	3 Définir les scenarii de menace	4 Éliminer les vulnérabilités connues	5 Définir les instructions

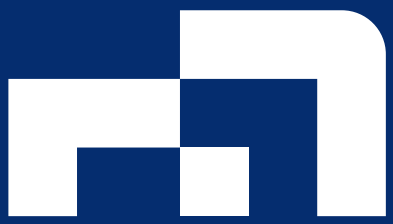
1 **S'appuyer sur les résultats** de l'analyse de risque **selon l'ISO 12100** et identifier les mesures de réduction du risque qui font appel à une technologie susceptible de subir des attaques.

2 **Définir les limites de l'environnement** dans lequel travaille la machine : qui a accès à quoi ? À quoi je connecte la machine ? Qu'est-ce que je dois connecter en permanence ?

3 **Définir des scénarii de menace** et leurs impacts (essentiellement liés à la sécurité humaine (impact éventuel sur une fonction de sécurité) mais pouvant avoir des impacts financiers ou sur l'image de l'entreprise utilisatrice de la machine en lien avec NIS2).

4 **Éliminer les vulnérabilités connues** (issues des informations délivrées par les fabricants de composants), désactiver les interfaces de communication inutiles ou les limiter au strict nécessaire, mettre en place des mécanismes d'enregistrement des interventions (par exemple pour détecter des tentatives d'accès, des modifications des données ou des modifications d'environnement physique). S'assurer de maintenir la machine en condition opérationnelle et en condition de sécurité dans la durée.

5 **Définir des instructions** spécifiques pour une utilisation sécurisée de la machine. Par exemple, le constructeur doit indiquer à l'intégrateur ou à l'utilisateur qu'il faut changer le mot de passe par défaut pour garantir une utilisation sécurisée de la machine. Ou encore, le constructeur doit indiquer que la machine ne doit pas rester connectée en permanence à une connexion distante de maintenance.



UNM

UNM - 45 rue Louis Blanc - 92400 Courbevoie
Contact : info@unm.fr
Tel : +33 (0)1 47 17 67 67
unm.fr