RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

LA CYBERSÉCURITÉ DES SYSTÈMES INDUSTRIELS – MESURES DÉTAILLÉES

GUIDE ANSSI

ANSSI-PA-108
27/11/2025

PUBLIC VISÉ :

Développeur Administrateur RSSI DSI Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI s'intitule **« La cybersécurité des systèmes industriels – Mesures détaillées »**. Il est téléchargeable sur le site `cyber.gouv.fr`.

Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence Ouverte v2.0 » publiée par la mission Etalab.

Conformément à la Licence Ouverte v2.0, le document peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.

Sauf disposition réglementaire contraire, les recommandations n'ont pas de caractère normatif ; elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	01/01/2014	Version initiale
2.0	27/11/2025	Refonte du document

Table des matières

1 Introduction

1.1 Objectifs du guide

L'objectif de ce document est de proposer un socle minimal de sécurité pour les installations industrielles. Les recommandations du socle sont réparties sur 4 classes [1]de niveau de sécurité croissant.

La méthode et les recommandations de l'ANSSI sur la protection des systèmes industriels sont présentées au travers de deux documents. Le premier guide [41] présente une méthode de définition d'un socle de sécurité adapté aux systèmes industriels. Cette méthode s'appuie sur le découpage du périmètre industriel et sa classification en quatre niveaux. Il est conseillé d'en prendre connaissance avant de lire le présent document. Le second guide, ce document, présente les mesures techniques et organisationnelles détaillées à mettre en place sur les systèmes industriels en fonction des classes définies dans le premier document.

De plus, les mesures de sécurité décrites dans le présent guide ne sont pas suffisantes pour les systèmes industriels présentant un niveau de criticité élevé.

Chaque installation industrielle présente des particularités et des risques propres qu'il convient d'analyser pour déployer des mesures de sécurisation adaptées. Ce processus de sécurisation protège les investissements et la production de l'entreprise. C'est pourquoi il est important de définir les bons objectifs et de les adapter aux besoins, comme décrit dans le guide de méthode de classification des systèmes industriels [41].

Information

La mise à jour du guide tient compte du retour d'expérience sur sa précédente version, et introduit les équivalences avec la norme IEC 62443 [53].

1.2 Champ d'application

Les éléments contenus dans ce document ont vocation à être applicables à tous les secteurs. Cependant, certains d'entre eux ont des spécificités qui n'y seront peut-être pas détaillées ou prises en compte. **En conséquence, une déclinaison sectorielle pourra être nécessaire dans certains cas, afin de préciser les modalités d'application et prendre en compte les contraintes spécifiques.**

1. La notion de classe est définie dans la méthode de classification [41]

L'ensemble des mesures présentées ont été pensées pour des systèmes industriels récemment installés. Il est tout à fait possible que les mesures ne puissent pas s'appliquer directement à des systèmes industriels existants. Il conviendra donc d'évaluer de manière exhaustive les impacts avant toute mise en œuvre de ces mesures.

Il est possible que, dans certaines situations, des mesures ne puissent s'appliquer sans adaptation pour des raisons de compatibilité avec des systèmes industriels existants ou des contraintes opérationnelles (par exemple des contraintes de sûreté et de performance) appelées « fonctionnalités essentielles » dans la norme [53]. Les mesures qui ne peuvent pas être appliquées doivent être revues dans le cadre d'une procédure de gestion des exceptions. Toute exception doit être intégrée dans un registre des risques et revue de manière périodique.

1.3 Organisation du guide

Le présent guide contient l'ensemble des recommandations organisationnelles et techniques à appliquer en fonction des classes identifiées. Pour chacune des recommandations, une correspondance avec celles de la norme IEC 62443 [53] est indiquée (lorsqu'elle existe).

Ce guide est un outil qui peut fournir des éléments pour constituer le dossier d'homologation de sécurité d'un système industriel.

1.4 Conventions de lecture

Pour chacune des recommandations de ce guide, l'utilisation du verbe *devoir* est volontairement plus prescriptive que la formulation *il est recommandé*.

Pour certaines recommandations, il est proposé plusieurs solutions que le lecteur choisit en fonction de la menace qu'il cherche à couvrir, de son contexte et des objectifs de sécurité à atteindre.

Les recommandations de ce guide sont données en fonction de la classe déterminée selon le guide [41], comme précisé dans le tableau 1.

Classes	Description
C1	Recommandation à appliquer pour les systèmes de **classe 1**, de **classe 2**, de **classe 3** et de **classe 4**.
C2	Recommandation à appliquer pour les systèmes de **classe 2**, de **classe 3** et de **classe 4**.
C3	Recommandation à appliquer pour les systèmes de **classe 3** et de **classe 4**.
C4	Recommandation à appliquer pour les systèmes de **classe 4**.

TABLE 1 – Grille de lecture de recommandation selon les classes

Ainsi, les recommandations sont présentées de la manière suivante (liste non exhaustive) :

R

C1 Recommandation à l'état de l'art

Cette recommandation permet de mettre en œuvre un niveau de sécurité à l'état de l'art et est applicable pour les systèmes de **classe 1**, **classe 2**, **classe 3** et **classe 4**.

R

C3 Recommandation à l'état de l'art

Cette recommandation permet de mettre en œuvre un niveau de sécurité à l'état de l'art et est applicable pour les systèmes de **classe 3** et **classe 4**.

R

C1 Recommandation à l'état de l'art avec exigence(s) IEC 62443

Cette recommandation inclut une ou plusieurs exigences issues de la norme IEC 62443 (pastilles oranges) pour les systèmes de **classe 1**, **classe 2**, **classe 3** et **classe 4**.

SR 2.1 **CR 2.1**

R -

C1 Recommandation alternative de premier niveau

Cette recommandation permet de mettre en œuvre une première alternative d'un niveau de sécurité moindre que la recommandation R, et est applicable pour les systèmes de **classe 1**, **classe 2**, **classe 3** et **classe 4**.

R +

C1 Recommandation renforcée complémentaire

Cette recommandation complémentaire permet de mettre en œuvre un niveau de sécurité renforcé et est applicable pour les systèmes de **classe 1**, **classe 2**, **classe 3** et **classe 4**.
Elle est destinée en priorité aux entités matures en sécurité des systèmes d'information.

Information

Les exigences de l'IEC 62443 sont issues des parties 2-1, 2-4, 3-2, 3-3, 4-1 et 4-2 et sont reprises à l'annexe A du présent guide.

Dans une démarche permanente de gestion du risque numérique et d'amélioration continue de la sécurité des systèmes d'information[2], la pertinence de mise en œuvre des recommandations décrites dans ce document doit être périodiquement réévaluée.

2. Se reporter au guide ANSSI relatif à la maîtrise du risque numérique [23].

Recommandations

Mesures organisationnelles et techniques proposées par la doctrine de sécurité de l'ANSSI.

Exigences

Mesures obligatoires dans le cadre d'une certification IEC 62443 [53].

La liste récapitulative des recommandations est disponible en page 109.

1.5 Liste des sigles et acronymes

API
: Automate Programmable Industriel. Il s'agit d'un équipement disposant d'un ensemble d'entrées/sorties, sur lequel sont raccordés des capteurs et actionneurs, et qui exécute un programme de façon cyclique afin de piloter un procédé industriel.

BPCS
: *Basic Process Control System*. Système permettant le contrôle et le pilotage d'une installation industrielle standard. Ce système gère des éléments non soumis à des contraintes élevées de sûreté de fonctionnement contrairement à un système SIS.

Conduit
: Groupement logique de voies de communication partageant des exigences de sécurité communes et connectant deux ou plusieurs zones (définition IEC 62443 [53]).

EMS
: *Energy Management System*. Système permettant de surveiller, contrôler et optimiser la consommation d'énergie dans les bâtiments tertiaires, les usines, etc. : suivi de facturation et compteurs d'énergie, plan de comptage, amélioration de la performance énergétique selon la norme ISO 50001, etc.

ERP
: *Enterprise Resource Planning*. Système informatique permettant la gestion du procédé de planification, le suivi des fabrications, la gestion des stocks, etc.

FAT
: *Factory Acceptance Test*. Essais effectués en usine sur un équipement ou un système avant envoi sur site.

GMAO
: Gestion de la Maintenance Assistée par Ordinateur. Logiciel de maintenance industrielle permettant la gestion des opérations de maintenance (préventive ou corrective) des équipements, la gestion des stocks, etc.

IT
: *Information Technology*. Cette abréviation est utilisée dans le document pour désigner l'informatique dite « de gestion » pilotant les systèmes d'information d'entreprise.

MES

Manufacturing Execution System ou GPAO en français (Gestion de la production assistée par ordinateur). Système informatique permettant l'acquisition de données de production, la gestion des ressources, le contrôle de la qualité, la gestion de la maintenance, le cheminement des produits et des lots, la traçabilité du produit, etc.

OT

Operational Technology. Cette abréviation est utilisée dans le document pour désigner la technologie utilisée entre autres, du niveau 0 au niveau 3 du modèle de Purdue [1]. Cette technologie permet de contrôler et commander des systèmes physiques (par exemple dans les domaines du transport de l'énergie, du transport de personne ou de marchandises, de l'industrie de manufacture, de la gestion technique de bâtiment, de l'assainissement des eaux).

PLC

Programmable Logic Controller. Il s'agit du terme anglais désignant un automate programmable industriel (API).

SAT

Site Acceptance Test. Essais effectués sur un équipement ou un système après le déploiement sur site.

SCADA

Supervisory Control And Data Acquisition. Ensemble de moyens informatiques permettant aux opérateurs et techniciens de la conduite de réaliser la supervision fonctionnelle et le contrôle, à distance ou local, des installations techniques d'un ou plusieurs sites.
En dehors de l'Europe, le terme SCADA désigne un système étendu de pilotage d'une installation industrielle intégrant, entre autres, les automates, les capteurs et les actionneurs.

SIS

Safety Instrumented System ou « Système Instrumenté de Sécurité » en français. Il s'agit d'un automate assurant des fonctions de sécurité fonctionnelle pour la protection des biens et des personnes. Se référer à la norme [2] pour plus de précisions.

SL

Security Level. Selon la définition de la norme IEC 62443, le SL est un indicateur caractérisant un ensemble de mesures qui concourent à la réduction du niveau des risques relatifs à un système (SUC), une zone de sécurité ou un conduit.

SNCC

Système numérique de contrôle-commande ou *Distributed Control System - DCS* en anglais. Ce système qui est en général utilisé pour les procédés nécessitant un niveau de sécurité fonctionnelle (ou *safety*) élevé comme par exemple les centrales électriques ou les usines de pétrochimie, il est constitué de BPCS et de SIS.

SSI

Sécurité des Systèmes d'Information. Ensemble des moyens techniques et organisationnelles de protection permettant à un système d'information d'assurer la disponibilité, l'intégrité et la confidentialité des données, traitées ou transmises, et des services connexes que ces systèmes rendent accessibles.

Station d'ingénierie

Équipement permettant, entre autres fonctionnalités, de réaliser des opérations de maintenance et la programmation du système de conduite (SCADA) et des automates programmables industriels (API). La station d'ingénierie permet d'effectuer des opérations de configuration et de programmation des automates, c'est donc un poste d'administration. Plus de précisions sont apportées à la sous-section 4.3.5.

SUC

System Under Consideration. Système étudié. Selon la définition de la norme IEC 62443, il s'agit d'un ensemble d'actifs du système industriel, nécessaire pour fournir une solution d'automatisation complète, y compris tout élément pertinent de l'infrastructure de réseau.

WMS

Warehouse Management System. Système permettant d'organiser la gestion des stocks, le suivi des flux de marchandises et leur emplacement optimal dans un entrepôt. Ce système permet également l'optimisation des tâches de préparation, de manutention et d'expédition. Il est en interface avec d'autres outils de la chaîne logistique (scanners, ERP, etc).

Zone

Selon la définition de la norme IEC 62443, une zone est un ensemble de sous-systèmes ou de composants partageant les mêmes exigences en matière de sécurité. Il s'agit donc d'un ensemble d'actifs logiques ou physiques qui représentent la division d'un système à l'étude (SUC) à partir de leurs exigences communes en matière de sécurité, de leur criticité (par exemple, impact financier élevé, impact sur la santé, la sécurité ou l'environnement), leurs fonctionnalités et leurs relations logiques et physiques (y compris leur emplacement).

2
Considérations relatives à la cybersécurité des systèmes industriels

L'objectif de ce chapitre est de dresser un état des lieux succinct de la cybersécurité des systèmes industriels. Pour ce faire, une liste des contraintes inhérentes aux systèmes industriels est établie dans la section 2.1. Ces contraintes sont un des éléments qui distingue les systèmes industriels des systèmes d'information de gestion. Il est important de les identifier afin de proposer des mesures adaptées.

Dans la section 2.2, les principales faiblesses et risques rencontrés dans ces systèmes sont listés. Ils peuvent découler des contraintes listées dans la section précédente, mais pas seulement. En particulier, on retrouve dans cette section les faiblesses et risques couramment rencontrés dans les systèmes d'information de gestion. Ces faiblesses et risques sont évoqués dans les publications [3], [5] et [8] de l'ANSSI traitant des états de la menace relatifs aux systèmes industriels.

2.1 Liste des contraintes dans les installations industrielles

Les contraintes sont des faits sur lesquels il peut être difficile d'agir et qui peuvent avoir un impact significatif sur la sécurité du système industriel concerné. Il est très important de prendre en compte ces contraintes lors du choix des mesures de sécurité à mettre en œuvre. Le tableau ci-dessous présente quelques contraintes observées.

Thèmes	Contraintes
Maîtrise des systèmes	■ Il y a une multitude d'intervenants (ayant parfois une méconnaissance du système) sur un système, ce qui ne facilite pas la maîtrise des actions effectuées sur celui-ci. ■ Il y a une multitude de sites isolés, notamment dans les secteurs du transport, de la distribution d'eau ou de l'énergie, bénéficiant d'une protection physique limitée. ■ La documentation technique (fournie par le constructeur ou un intégrateur ou des documents d'exploitation internes) du système peut être incomplète. Ceci peut entraîner une perte du savoir lors des départs de personnels et ne facilite pas le traitement des incidents. ■ Certains systèmes peuvent dépendre de deux entités différentes. Ceci peut poser des problèmes juridiques en cas de modification du système (par exemple lorsque les limites de responsabilité entre ces entités ne sont pas définies ou mal définies). ■ Les systèmes sont souvent hétérogènes car venant de différents fournisseurs ou parce qu'ils ont évolué au cours du temps. L'hétérogénéité peut être imposée pour des raisons de sûreté fonctionnelle. ■ Sur certains sites, aucun personnel n'est présent physiquement (ex. : barrages, parcs éoliens, châteaux d'eau).
Contrats	■ Les fournisseurs ou intégrateurs exigent d'avoir accès en télémaintenance aux équipements sous leur responsabilité sous peine de ne pas les garantir ou de ne pas respecter les contrats de maintenance. ■ La modification des systèmes sans accord préalable du fournisseur peut entraîner une perte de garantie. ■ Il peut être contractuellement interdit de modifier le système existant, y compris pour implémenter des mesures de cybersécurité (par exemple la mise à jour d'un SNCC sans participation du constructeur).

Thèmes	Contraintes
Réglementation	■ Certaines réglementations imposent aux opérateurs d'exporter des données vers un tiers. Par exemple, les déchèteries doivent transmettre des données à la DREAL [3]. ■ Opportunité : les mesures de sécurité fonctionnelles imposées par la réglementation d'un secteur peuvent renforcer le niveau de sécurité du système et offrir un niveau de risque résiduel acceptable. ■ La réglementation en matière de sûreté peut limiter la possibilité de modification des systèmes. En effet, la modification d'un système peut entraîner la perte d'une homologation fonctionnelle [4].
Gestion des modifications	■ Peu d'environnements de test sont utilisés afin de s'assurer de la non-régression des systèmes. ■ La majorité des interventions sur les systèmes sont effectuées lors des périodes de maintenance. ■ Les fournisseurs offrent peu de support pour aider les opérateurs à qualifier les impacts des mesures de sécurité sur les systèmes.
Opérations	■ Certains environnements nécessitent une réactivité forte des opérateurs notamment en cas d'incident. Les mesures de sécurité ne doivent pas entraver cette réactivité. ■ Les opérateurs partagent souvent des équipements, ce qui peut avoir un impact significatif sur la traçabilité (utilisation de comptes génériques par exemple). ■ Les éléments de protection individuelle (EPI) peuvent entraver la saisie d'identifiants ou de mots de passe sur un écran tactile. ■ Les opérateurs doivent souvent visualiser l'état du système en temps réel et intervenir rapidement, comme par exemple lors des changements d'équipes d'exploitation. Ainsi, les postes d'exploitation pourraient ne pas être verrouillés. ■ Une pratique culturelle répandue consiste à ne rien modifier tant que le système fonctionne.
Contraintes économiques	■ Les mises à jour et les évolutions des systèmes existants entraînent des coûts importants pour le client.

3. Directions régionales de l'environnement, de l'aménagement et du logement.
4. À ne pas confondre avec l'homologation de cybersécurité.

Thèmes	Contraintes
Gouvernance de sécurité	■ Bien qu'une gouvernance ait été mise en place depuis quelques années, la cybersécurité des systèmes industriels n'est pas totalement intégrée à l'organisation de l'entreprise et peut manquer de soutien et de moyens de la part de la direction. Ceci peut compliquer ou ralentir la mise en œuvre de la cybersécurité. ■ Lorsque la sécurisation des systèmes industriels est confiée à une direction métier, la responsabilité de la gestion des interfaces entre les systèmes industriels et les systèmes de gestion est peu définie.
Contraintes techniques	■ Les équipements sont généralement déployés pour au moins 20 ans. L'obsolescence limite leurs possibilités de mise à jour ainsi que l'intégration de fonctions de sécurité après leur mise en service. ■ Certains équipements et protocoles offrent des fonctionnalités de sécurité insuffisantes. ■ Sur certains systèmes, les besoins de performance exigent qu'il n'y ait pas de latence.
Culture de la sécurité	■ Dans les milieux où la sûreté de fonctionnement est très présente, il peut y avoir le sentiment que celle-ci permet également de régler les problèmes de cybersécurité. ■ La cybersécurité n'est pas abordée lors des cursus de formation, et en particulier ceux des automaticiens.
Maturité des solutions techniques	■ L'expertise relative à la cybersécurité des systèmes industriels reste rare car elle se positionne au croisement des métiers de l'industrie et de la cybersécurité. ■ La croyance que l'isolation d'un site industriel est possible ou suffisante pour assurer sa sécurité a pour conséquence un niveau de sécurité insuffisant compte tenu des modes opératoires d'attaquants actuels. ■ Les systèmes en exploitation sont parfois très complexes ; ainsi peu de personnes ont la connaissance globale IT, OT et cybersécurité.
Priorisation des besoins métier	■ La cybersécurité est souvent faiblement priorisée par rapport aux besoins fonctionnels métier. Ces dépriorisations ont des conséquences fortes qui engendrent des reports d'applications de correctifs par exemple.

2.2 Faiblesses de sécurité et risques dans les installations industrielles

Information

Les encadrés *Tactiques, techniques et procédures (TTP)* de la **présente section** n'ont pas vocation à être exhaustifs et sont là uniquement pour illustrer les faiblesses et risques concernés.

2.2.1 Gestion des correctifs de sécurité

La gestion des vulnérabilités diffère entre les systèmes industriels et les systèmes d'information de gestion. Dans de nombreux cas, les correctifs ne peuvent être installés que pendant les phases de maintenance et, parfois, leur application peut entraîner la nécessité de requalifier le système industriel du point de vue de la sûreté de fonctionnement.

La priorité est donnée à l'intégrité et à la disponibilité du système et, comme l'entité responsable dispose rarement d'une plate-forme d'essai, elle ne peut pas effectuer de tests de non-régression sur les correctifs publiés par les fournisseurs.

AInsi, la plupart des systèmes n'ont pas de procédure ou de mécanisme technique pour l'application des correctifs de sécurité. En particulier, les systèmes de mises à jour automatiques sont souvent incompatibles, notamment avec les anciens systèmes.

Tactiques, techniques et procédures (TTP)

La présence de vulnérabilités connues non corrigées dans un système augmente le risque d'une intrusion, la fuite ou le vol de données sensibles, les attaques par rançongiciel, l'injection de maliciels, une atteinte à l'intégrité des systèmes et de potentielles interruptions du système industriel.
L'absence de mise en œuvre des correctifs de sécurité permettant de réduire - voire de supprimer - les vulnérabilités connues dans un système augmente le risque de compromission. Que l'attaque soit ciblée ou générique. Une politique permettant l'application des correctifs de sécurité complique fortement la tâche de l'attaquant [5].

5. Pour davantage de précisions, se reporter à la matrice du Mitre relative aux systèmes industriels : https://attack.mitre.org/matrices/ics/.

2.2.2 Veille sur les vulnérabilités et les menaces

Les activités de veille active de vulnérabilités et d'analyse de la menace ne sont pas encore suffisamment intégrées dans les procédures des industriels malgré l'apparition de sources d'information spécialisées. De plus, les résultats de ces activités ne sont pas suffisamment mis à profit pour l'amélioration du niveau de cybersécurité des systèmes industriels.

Information

L'absence de veille sur les vulnérabilités ou obsolescences de produits ou technologies utilisées empêche de réagir lors de la publication de l'une d'entre elles.
Une veille active sur les techniques d'attaque ou sur l'évolution de la menace permet d'améliorer la pertinence de l'analyse de risque du système industriel. Elle permet également d'adapter les mesures de protection et de réduire le temps d'exposition du système aux vulnérabilités.

2.2.3 Défaut de contrôle d'accès logique

2.2.3.1 Défaut de la politique de gestion des mots de passe

Il est fréquent que les politiques de mots de passe soient insuffisantes voire incomplètes. Ceci peut impliquer les problèmes suivants :

- l'utilisation de mots de passe par défaut ;
- l'utilisation de mots de passe faibles (parfois due à des limitations de l'équipement ou du logiciel) ;
- le stockage de mot de passe « en clair » sur un support papier ;
- la réutilisation de mêmes mots de passe pour des systèmes de sensibilité différente dans un objectif de simplifier l'accès des utilisateurs.

Tactiques, techniques et procédures (TTP)

Une première étape pour un attaquant consiste souvent à tenter de compromettre le compte d'un utilisateur du système pour l'utiliser. Pour cela, une des techniques à sa disposition consiste à récupérer un mot de passe.
L'utilisation de mots de passe par défaut ou codés « en dur » dans un équipement lui permet donc d'utiliser directement des comptes présents par défaut sur le système, souvent avec des privilèges élevés. Lorsque les mots de passe par défaut ont été changés, l'attaquant peut essayer les attaques par dictionnaire pour tenter de découvrir un mot de passe et utiliser ainsi le compte concerné. C'est pourquoi il est recommandé d'utiliser un mot de passe robuste et de le modifier en cas de suspicion de compromission conformément aux recommandations de l'ANSSI sur l'authentification [50].

2.2.3.2 Défaut de gestion des comptes

Il est fréquent que la politique de gestion des comptes d'un système industriel soit inadaptée ou inexistante.

Afin de faciliter les opérations, du fait du roulement des opérateurs ou de la multitude de sites à gérer pour les équipes de maintenance, des comptes génériques peuvent être utilisés.

Il est fréquent qu'il n'y ait pas de procédure de gestion des départs et des arrivées. En particulier, le compte d'un ancien employé peut ne pas être désactivé ou supprimé après son départ.

Il est également courant de voir l'utilisation non justifiée de comptes à privilèges. Cela peut être dû à une recherche de facilité de gestion des comptes utilisateurs ou à des limitations techniques d'un produit utilisé. De nombreuses applications, par exemple, ne s'exécutent qu'avec des comptes de niveau « administrateur ».

Tactiques, techniques et procédures (TTP)

L'utilisation de comptes génériques augmente considérablement les risques de compromission, notamment du fait de la circulation du mot de passe partagé. En pratique, les mots de passe utilisés pour les comptes génériques sont souvent trop faibles ou notés sur des papiers faciles à égarer. Ne pas désactiver ou supprimer un compte après le départ de son titulaire offre une possibilité d'action à un ancien employé mécontent. D'autre part, l'absence de politique de gestion des comptes diminue la traçabilité sur le système industriel concerné (qui accède à quelles ressources ?). Dès lors, il est difficile, en cas de problème, d'en retrouver l'origine.

2.2.4 Défaut de contrôle des interfaces de connexion

L'absence de contrôle des interfaces de connexion (par exemple : ports USB non bloqués ou ports Ethernet non utilisés mais ouverts, accès au réseau sans fil non contrôlé) peut simplifier le travail d'un attaquant.

Tactiques, techniques et procédures (TTP)

Laisser des interfaces ouvertes augmente la surface d'attaque.
Par exemple, ne pas bloquer les ports USB peut favoriser l'introduction de virus dans le système ou ne pas désactiver des ports Ethernet offre la possibilité de réaliser des connexions sauvages pouvant perturber le fonctionnement du système. Cela peut également être utilisé pour lancer ultérieurement une attaque depuis l'extérieur du site (en connectant un équipement Wi-Fi par exemple).

2.2.5 Défaut de cartographie

De manière générale, les entités ne réalisent que rarement la cartographie de leur système d'information. Elles ne le font pas davantage pour leurs systèmes industriels. En particulier, on peut noter :

- l'absence, notamment :
  - des topologies réseau ;
  - des matrices de flux ;
  - des inventaires des équipements matériels et logiciels du parc industriel ;
- l'absence recensement des procédures d'exploitation ;
- la méconnaissance des générations technologiques qui cohabitent et de leurs vulnérabilités intrinsèques ;
- une connaissance insuffisante de l'obsolescence des équipements et de la disponibilité de leur support par les constructeurs.

De plus, lorsqu'une cartographie existe, les procédures ou les outils qui pourraient permettre de la maintenir à jour ne sont pas forcément mis en œuvre.

Information

La cartographie d'un système est un élément fondamental de la sécurité des systèmes d'information.
La bonne connaissance de son système permet notamment d'évaluer très rapidement l'impact potentiel d'une vulnérabilité, de faire une analyse de risque ou de déterminer rapidement et efficacement l'étendue d'une compromission en cas d'incident.

2.2.6 Défaut de maîtrise des configurations

2.2.6.1 Manque de contrôle d'intégrité ou d'authenticité

Il est peu fréquent que des mécanismes de contrôle d'intégrité ou d'authenticité soient mis en place pour les micrologiciels (*firmware*), les logiciels, les programmes d'automates et applications SCADA.

Tactiques, techniques et procédures (TTP)

L'absence de mécanisme de contrôle d'intégrité ou d'authenticité permet à un attaquant de diffuser une mise à jour piégée (par exemple l'utilisation de la technique `https://attack.mitre.org/techniques/T1553/002/` qui a été utilisée pour corrompre la solution Orion de la société Solarwinds).

2.2.6.2 Absence de sauvegarde

Les sauvegardes sont souvent partielles, inexistantes ou uniquement disponibles chez un tiers. Lorsque des sauvegardes existent, le bon fonctionnement des procédures de restauration est rarement testé.

Information

En cas de compromission du système, les sauvegardes peuvent permettre de restaurer la configuration du système dans un état antérieur sain.

2.2.6.3 Défaut de maîtrise des modifications en ligne

Il est souvent possible de modifier en ligne (c'est-à-dire de manière connectée sans redémarrage de l'équipement), sans mécanisme d'authentification ou de journalisation, des programmes d'automates ou des applications SCADA. Cette fonctionnalité, très utile lorsque les systèmes fonctionnent en 24/7, présente souvent très peu de mécanismes de cybersécurité.

Tactiques, techniques et procédures (TTP)

L'absence d'authentification ou de journalisation permet à un attaquant de modifier de manière furtive le programme d'un automate (comme par exemple le malware Triton ciblant des automates de sécurité dont le protocole ne dispose pas de mécanismes d'authentification, `https://evals.mitre.org/ics/triton`). Cette modification pourrait ne pas être détectable par les applications SCADA et les utilisateurs.

2.2.6.4 Utilisation des configurations par défaut

Il existe encore en production des équipements développés à une époque où étaient intégrées des contraintes de sûreté de fonctionnement fortes mais peu de contraintes de cybersécurité. En particulier, les techniques de développement employées envisageaient rarement comme vraisemblable la présence d'un attaquant sur le système.

Les configurations des équipements ou logiciels constituant les réseaux de communication sont rarement durcies. En particulier, les services inutilisés sont souvent laissés activés comme ils l'étaient, par exemple, dans une configuration par défaut.

Information

Les équipements qui ont été développés sans objectif de cybersécurité sont plus susceptibles de présenter des vulnérabilités qui pourront être exploitées par un attaquant.
Afin de minimiser la surface d'attaque, il est nécessaire de désactiver ou de désinstaller les services et logiciels inutilisés. Ainsi, si une vulnérabilité est découverte dans un de ces composants, le système industriel sera moins vulnérable.

2.2.7 Utilisation de protocoles réseau vulnérables

Les systèmes industriels font souvent usage de protocoles réseau n'intégrant aucun mécanisme de sécurité (ex. : absence de chiffrement ou d'authentification). Ces protocoles peuvent être des protocoles classiques comme Telnet, mais peuvent également être des protocoles spécifiques aux systèmes industriels comme Modbus TCP, Profinet, EtherNetIP [6], etc.

Tactiques, techniques et procédures (TTP)

L'utilisation de protocoles réseau non sécurisés peut permettre à un attaquant de modifier les trames à la volée ou de forger des trames, perturbant ainsi le fonctionnement du système industriel. Cela peut également permettre de récupérer des authentifiants de connexion circulant en clair sur le réseau.
De la même manière, l'utilisation de protocole non sécurisé de prise en main à distance augmente la capacité de latéralisation de l'attaquant au sein du système.
L'utilisation de technologies sans fil expose le système à des problèmes de disponibilité car il est facile de brouiller, volontairement ou non, un signal. Par ailleurs, lorsque l'installation sans fil n'est pas sécurisée correctement, l'attaquant peut éventuellement modifier le trafic légitime ou injecter du trafic illégitime plus aisément que dans le cas d'une infrastructure filaire.

2.2.8 Défaut de contrôle d'accès physique

Dans certains cas de figure, les intervenants (ex. : mainteneurs, exploitants) ont besoin de pouvoir accéder physiquement aux installations.

Selon le domaine d'activité, le système industriel ou ses composants pourraient être localisés dans des usines, sur la voie publique ou sur d'autres sites qui ne permettent pas la mise en place d'un contrôle d'accès physique efficace.

Tactiques, techniques et procédures (TTP)

L'absence de contrôle d'accès physique permet à un attaquant d'accéder directement à tout ou partie du système (par exemple sur un système distribué), contournant ainsi les protections périmétriques logicielles qui pourraient avoir été mises en place.

2.2.9 Défaut de cloisonnement

Il est courant qu'il n'y ait pas de cloisonnement effectif entre un système industriel et le système d'information de gestion. Cette ouverture des réseaux industriels vers le système d'information de

6. EtherNetIP ou EIP est le nom d'un protocole industriel ouvert fonctionnant sous TCP ou UDP et utilisé par certains équipements industriels (par exemple : automates industriels, organes terrain) dans les architectures de systèmes avec des contraintes de fonctionnement en temps réel ou déterministes.

gestion ou vers un réseau public comme Internet peut être justifiée par des raisons opérationnelles comme des contraintes de planning ou de mutualisation d'outils ou par des raisons de réduction de coûts pour simplifier la remontée d'informations du système industriel vers le système d'information de gestion.

Par ailleurs, il est très courant qu'il n'y ait pas non plus de cloisonnement au sein même des systèmes industriels ; entre ses différents sous-systèmes par exemple. Ceci peut également être dû à des besoins de réduction de coûts ou à une méconnaissance de la nécessité de cloisonner les systèmes.

Tactiques, techniques et procédures (TTP)

L'absence de cloisonnement entre les sous-systèmes facilite le travail d'un attaquant pour se latéraliser dans le système et accéder à son but.
La présence d'un cloisonnement efficace permet également de limiter la propagation de codes malveillants (par exemple rançongiciel).

2.2.10 Télémaintenance et télégestion

La télémaintenance et la télégestion sont des pratiques courantes pour les systèmes industriels, qui consistent à réaliser des opérations, parfois sensibles, sur le système et à distance (c'est-à-dire en dehors du périmètre maîtrisé du site hébergeant le système). Les infrastructures de télégestion ou de télémaintenance peuvent utiliser des réseaux publics comme Internet (via un réseau filaire ou un réseau de téléphonie mobile). Ces accès à distance peuvent avoir été mis en place pour des besoins internes, mais également pour permettre des opérations de maintenance par le fournisseur ou l'intégrateur.

Les solutions techniques employées pour la télégestion ou la télémaintenance offrent dans de nombreux cas un niveau de sécurité faible.

Tactiques, techniques et procédures (TTP)

L'utilisation d'accès à distance augmente considérablement la surface d'attaque d'un système. En effet, les équipements de bordure sont des cibles très prisées des attaquants comme l'illustre le *Panorama de la menace* [8].

2.2.11 Défaut de maîtrise des terminaux nomades

Il est de plus en plus courant que les intervenants utilisent des terminaux mobiles comme des smartphones ou des tablettes pour augmenter leur productivité en déplacement sur le terrain. Ceci est d'autant plus vrai pour de grands systèmes distribués.

La sécurité de ces terminaux n'est pas toujours maîtrisée et certains utilisent du matériel personnel pour remplir des missions professionnelles (BYOD - *Bring Your Own Device*). Dès lors, leur connexion au système pose un problème de sécurité.

Tactiques, techniques et procédures (TTP)

L'utilisation de terminaux mobiles à la sécurité non contrôlée augmente leur risque de compromission. S'ils sont connectés au système, cela offre une porte d'entrée potentielle à un attaquant (se référer à l'état de la menace relative aux téléphones mobiles [6]).

2.2.12 Utilisation de technologies standards

Pour des raisons de coût et d'interopérabilité des systèmes industriels avec les systèmes d'information de gestion, les technologies utilisées pour les premiers ont été standardisées. Ainsi, concernant le réseau, Ethernet et TCP/IP sont de plus en plus employés pour remplacer les technologies propriétaires utilisées auparavant. Les outils de développement ou de maintenance font également de plus en plus appel à des briques logicielles génériques utilisées par l'informatique de gestion.

Cette standardisation est globalement bénéfique pour l'industrie, notamment en facilitant :

- la maîtrise, le maintien en condition opérationnelle et de sécurité des protocoles ;
- le remplacement du matériel, pour des modèles ou des fournisseurs différents.

2.2.13 Formation et sensibilisation

Les intervenants sur un système industriel ne sont pas toujours formés et sensibilisés à la sécurité des systèmes d'information et ne connaissent pas nécessairement la politique de sécurité des systèmes d'information (PSSI) du système sur lequel ils interviennent.

Attention

L'absence de sensibilisation à la SSI entraîne la multiplication des comportements à risque pouvant faciliter une compromission du système cible. De nombreux incidents, provenant d'un manque de sensibilisation et d'application de bonnes pratiques, sont régulièrement constatés.

2.2.14 Insuffisance de la supervision des événements de cybersécurité

L'analyse des événements de cybersécurité est souvent limitée et donc peu exploitée en cas d'incident sur un système. Les dispositifs de détection d'événements ou de dysfonctionnements se limitent à des scénarios non malveillants de sûreté de fonctionnement.

Information

Ne pas superviser les événements de cybersécurité d'un système limite fortement la capacité de détection et, *a fortiori*, de réaction en cas d'incident. Une intervention rapide peut permettre de limiter les impacts d'un incident. De plus, dans certains cas, lorsque pour des contraintes métiers ou techniques il n'est pas possible de déployer des mesures de protection, la supervision est la seule mesure de sécurité possible.

2.2.15 Absence de plan de continuité d'activité

Les plans de continuité d'activité (PCA) ou les plans de reprise d'activité (PRA) ne prennent pas systématiquement en compte les incidents de cybersécurité. Les équipes opérationnelles disposent rarement de consignes pour réagir à un tel événement (par exemple en cas de compromission par rançongiciel). La rédaction d'un plan de gestion de crise pour la perte du contrôle d'un système due à un événement malveillant est rarement envisagée.

2.2.16 Absence de prise en compte de la cybersécurité dans les projets

Lors des phases de spécification et de conception d'un système industriel, les documents n'intègrent généralement aucune exigence en matière de cybersécurité.

Information

Pour mettre en place des mécanismes de défense efficaces, il est nécessaire de prendre en compte la cybersécurité dès les phases initiales des projets, et en particulier dès la rédaction du cahier des charges. Augmenter le niveau de sécurité d'un système existant est souvent plus compliqué et plus coûteux.

2.2.17 Absence de tests de cybersécurité

Les tests avant mise en service (FAT et SAT - voir les définitions à la section 1.5) contiennent rarement des tests portant sur la cybersécurité. Lors des opérations de maintenance, des tests de sûreté ou de conformité du système d'information sont souvent prévus, mais pas d'audits de cybersécurité.

Information

Pour que la cybersécurité d'un système industriel reste à un niveau acceptable, il est nécessaire de tester les mécanismes de protection mis en place tout au long de la vie du système.

2.2.18 Absence de maîtrise des fournisseurs et prestataires

Dans les projets de systèmes industriels, un audit de cybersécurité des fournisseurs et des prestataires n'est pas toujours envisagé. Des procédures d'échanges sécurisés des informations ne sont pas toujours prévues.

Tactiques, techniques et procédures (TTP)

Dans certains cas, il peut être plus aisé ou discret d'attaquer le fournisseur pour toucher le système industriel cible que d'attaquer le système cible directement comme l'attaque visant la société Solarwinds en 2017 (attaque de la chaîne d'approvisionnement, traduction du terme anglais *supply chain attack* couramment employé).

Information

L'ANSSI qualifie des prestataires d'administration et de maintenance sécurisées (PAMS)[7] qui attestent d'un niveau de sécurité et de confiance. En particulier, la maintenance de systèmes industriels est un cas d'usage ciblé par le référentiel de qualification.

2.2.19 Défaut de sécurisation des environnements de développement

Dans les projets de systèmes industriels, l'environnement de développement est rarement dédié ou sécurisé, que ce soit en interne ou chez les fournisseurs. Par exemple, les postes de développement sont parfois également les postes de bureautique et ont donc accès à Internet.

Tactiques, techniques et procédures (TTP)

L'utilisation d'un même environnement de travail pour des tâches de natures différentes (par exemple, activité d'ingénierie et activité opérationnelle) augmente les risques de compromission. Un environnement de développement non sécurisé, connecté à Internet par exemple, augmente le risque qu'un attaquant déploie un code malveillant ou piége les développements (par exemple : micrologiciel, programme automate, application SCADA)

2.2.20 Accès libre aux outils de développement

Dans de nombreux systèmes industriels, les outils de développement sont présents sur le réseau. Cela peut être dû au fait que certains produits ne distinguent pas les environnements de production et de développement. Cela peut également résulter de pratiques opérationnelles. Les stations d'ingénierie servent parfois de consoles de supervision.

Tactiques, techniques et procédures (TTP)

La présence des outils de développement sur le réseau facilite la tâche de l'attaquant qui pourra les détourner pour modifier le comportement du système industriel, de manière légitime mais malveillante.

2.2.21 Défaut de cloisonnement des moyens d'administration

La séparation des pratiques d'exploitation et d'administration au sein des systèmes industriels n'est pas suffisante. Souvent, ce sont les mêmes postes qui sont utilisés pour les mises à jour, le développement et l'exploitation des applications SCADA.

7. https://cyber.gouv.fr/pams

Tactiques, techniques et procédures (TTP)

Le défaut de cloisonnement des moyens d'administration facilite la tâche de l'attaquant qui pourra avoir accès à l'administration des équipements depuis les postes de supervision SCADA, potentiellement très exposés.

2.2.22 Défaut de définition des responsabilités

Les responsabilités en matière de cybersécurité sont souvent mal identifiées entre le fournisseur, l'intégrateur et l'entité responsable d'un système industriel. De même, les responsabilités entre les directions métier et la direction informatique ne sont souvent pas précisées.

Attention

Des responsabilités peu claires font courir le risque qu'une partie du système industriel soit dépourvue d'un responsable et ne reçoive donc pas les mesures de cybersécurité appropriées.

3
Mesures organisationnelles de sécurité

Les mesures organisationnelles présentées dans ce chapitre s'adressent à l'ensemble des acteurs impliqués dans les systèmes industriels (par exemple : chefs de projet, acheteurs, automaticiens, intégrateurs, développeurs, équipes de maintenance, RSSI).

Attention

Il revient à l'entité responsable de définir la personne ou les personnes qui seront en charge de l'application des mesures de cybersécurité sur les systèmes.

Les mesures font référence aux chapitres de l'ISO 27002 [55] ainsi qu'aux recommandations du guide d'hygiène informatique [17] publié par l'ANSSI.

Ces références sont indiquées dans un encadré comme celui présenté ci-dessous :

Références

- **TTP :** fait référence aux tactiques, techniques et procédures indiquées dans la section 2.2.
- **Guide d'hygiène :** fait référence au guide d'hygiène informatique [17].
- **ISO 27002 :** fait référence aux chapitres de l'ISO 27002 [55] abordant le sujet.

Attention

Les mesures sont cumulatives. Ainsi, un système de classe 2 doit appliquer les mesures de classe 1 et de classe 2, et un système de classe 4 doit appliquer les mesures de classe 1, de classe 2, de classe 3 et de classe 4.

3.1 Connaissance du système industriel

Cette section regroupe l'ensemble des mesures qui permettent d'accroître la connaissance du système industriel et de son environnement. Afin d'assurer une défense permettant de répondre aux menaces, il est nécessaire d'avoir une connaissance très approfondie de son système, des risques encourus, des événements métier redoutés et des menaces à son encontre.

3.1.1 Rôles et responsabilités

Références

- **TTP :** 2.2.22
- **Guide d'hygiène :** règle n° 39
- **ISO 27002 :** 5.2

R1

C1 Mettre en place un cadre de gouvernance

Il est recommandé de mettre en place un cadre de gouvernance de la cybersécurité des systèmes industriels, en cohérence avec celui de l'informatique de gestion, par exemple au travers d'une PSSI.

ORG 1.1

R2

C1 Identifier les rôles et responsabilités

Il est recommandé d'identifier les rôles et responsabilités de cybersécurité pour chaque partie prenante pour l'ensemble du cycle de vie du système (par exemple : développement, intégration, exploitation, maintenance, désengagement).

ORG 1.3 SM-2 SP01.05 SP01.06BR SP01.07BR

R3

C2 Revoir périodiquement les limites de responsabilité

Il est recommandé de revoir périodiquement la bonne mise en œuvre de la recommandation R2.

3.1.2 Cartographie

Références

- **TTP :** 2.2.5
- **Guide d'hygiène :** règle n° 4
- **ISO 27002 :** 5.9

R4

C1 Etablir et maintenir à jour une cartographie de l'écosystème

Il est recommandé de définir et de maintenir à jour une cartographie de l'écosystème dans lequel les systèmes industriels sont mis en œuvre et contenant, au minimum, les informations suivantes :

- la liste des prestataires et fournisseurs (de matériels et/ou de logiciels) contribuant à la réalisation des activités ou des services de l'entité ;
- la liste des interconnexions avec les systèmes d'information des prestataires et fournisseurs.

CM 1.1 **SR 7.8** **CR 7.8** **SP01.02RE1** **SP06.02BR**

R5

C1 Établir une cartographie du système

Il est recommandé d'établir une cartographie du système industriel, contenant les vues :

- physique du système industriel ;
- logique du système industriel ;
- des applications ;
- de l'administration et de la maintenance du système.

CM 1.2 **SR 7.8** **CR 7.8** **SP01.02RE1** **SP06.02BR**

Information

Les outils industriels comme les logiciels de gestion de maintenance assistée par ordinateur (GMAO) peuvent gérer les inventaires. Ces outils disposent de l'ensemble des informations dans une même base et sont utilisés pour les partager avec les équipes métier.
De plus, la GMAO contient déjà bien souvent un inventaire des composants matériels comme les automates, les interfaces homme-machine (IHM), capteurs et actionneurs intelligents par exemple.

R6

C2 Maintenir à jour une cartographie

Il est recommandé de maintenir à jour une cartographie du système industriel en s'appuyant sur le guide de cartographie d'un système d'information [22].

CM 1.2 **SR 7.8** **CR 7.8** **SP01.02RE1** **SP06.02BR**

3.1.3 Analyse de risque

Références

- **TTP :** néant
- **Guide d'hygiène :** règle n° 41
- **ISO 27002 :** se référer à la norme ISO 27005

R7

C2 Réaliser une analyse de risque

Il est recommandé de réaliser une analyse de risque de cybersécurité sur le système industriel concerné en suivant une méthode choisie par l'entité responsable (pour une analyse selon la méthode EBIOS *Risk Manager*, il est possible de se référer au guide [41] de l'ANSSI).
Le niveau de profondeur de l'analyse de risque est à adapter selon la classe du système. Par exemple, à partir des niveaux précisés dans EBIOS RM [44], la classe 2 correspond à la démarche d'homologation *simplifiée* selon le guide de l'homologation de sécurité des systèmes d'information [20].

ORG 2.1 **SP03.01** **SP02.01BR**

Attention

Il est recommandé que l'analyse de risque pour la cybersécurité du système industriel soit intégrée à l'analyse de risque globale du système pouvant traiter par exemple des aspects de sûreté de fonctionnement.

3.1.4 Gestion des sauvegardes

Références

- **TTP :** 2.2.6
- **Guide d'hygiène :** règle n° 37
- **ISO 27002 :** 8.13

Les données à sauvegarder sont celles nécessaires à la reconstruction du système après un sinistre : par exemple, les programmes, les fichiers de configuration, les micrologiciels, les paramètres de

procédé (réglages d'asservissement par exemple). Cela peut également concerner des données ayant un aspect réglementaire comme des preuves de traçabilité.

R8

C1 Sauvegarder les données

Il est recommandé de définir et de mettre en œuvre un plan de sauvegarde des données afin de restaurer le système en cas d'incident. Il est nécessaire de prendre compte des besoins des métiers (délai d'indisponibilité maximal admissible et perte de données maximale admissible).
Il est recommandé de s'appuyer sur les référentiels [16] et [37] afin de réaliser une sauvegarde à l'état de l'art.
La sauvegarde doit inclure notamment les micrologiciels des automates, les logiciels applicatifs SCADA, les fichiers de configuration des automates, etc.

AVAIL 2.1 **SP12.01BR** **SP12.05BR** **SP12.06BR** **SP12.08BR**

R9

C1 Sauvegarder les configurations

Il est recommandé de sauvegarder les configurations avant et après toute modification, y compris lorsque celles-ci ont été apportées « à chaud ».

SR 7.3 **CR 7.3** **SP12.07BR**

R10

C1 Tester le processus de restauration des sauvegardes

Il est recommandé de tester régulièrement le processus de restauration des sauvegardes. Ce processus peut être testé sur un échantillon représentatif du système industriel ou dans son ensemble.

SR 7.3 RE1 **CR 7.3 RE1** **AVAIL 2.3** **SP12.04BR**

R11

C1 Mettre hors de portée d'un attaquant les données sauvegardées

Conformément au fondamentaux relatifs à la sauvegarde des systèmes d'information [16], il est recommandé d'appliquer la règle « 3 – 2 – 1 » : 3 copies distinctes des données, c'est-à-dire, les données en production et 2 sauvegardes stockées sur des supports différents, dont 1 hors ligne.

3.1.5 Gestion de la documentation

Références

- **TTP :** 2.2.6.2
- **Guide d'hygiène :** néant
- **ISO 27002 :** 5.12

R12

C2 Définir le niveau de sensibilité de la documentation

Il est recommandé de définir le niveau de sensibilité de la documentation et de le marquer clairement sur les documents, en s'appuyant éventuellement sur le référentiel [40].

ZCR 5.13

R13

C2 Adapter le stockage et la diffusion des documents

Il est recommandé d'adapter le stockage et la diffusion des documents relatifs à la conception, à la configuration ou au fonctionnement du système industriel, par exemple en adoptant la politique de partage et d'utilisation des informations de l'ANSSI [8](reposant sur le *Traffic Light Protocol* et le *Permissible Actions Protocol*).

CR 3.9 **DATA 1.1**

Attention

La documentation des systèmes industriels (par exemple : analyses fonctionnelles, analyses organiques, plan d'adressage, cartographie) est souvent stockée sur le système de gestion (bureautique), qui est plus exposé que le système industriel. Les systèmes de gestion sont souvent la première cible des attaquants car ils permettent de collecter de nombreuses informations en vue de préparer, par exemple, une attaque ciblée sur les systèmes industriels.

R14

C3 Revoir la documentation à intervalles réguliers

Il est recommandé d'effectuer une revue de la documentation au moins une fois par an, pour s'assurer que les documents nécessaires existent bien et correspondent à

8. https://www.cert.ssi.gouv.fr/csirt/politique-partage/

la dernière version du système, et pour supprimer ceux qui ne sont plus utilisés ou obsolète.

SR-5 SG-7

3.2 Maîtrise des intervenants

Cette section regroupe les mesures de sécurité nécessaires à la gestion du personnel ayant un accès physique ou logique au système industriel. Afin de limiter les risques d'erreurs de manipulation ou de configuration, il est nécessaire d'appliquer des règles permettant de garantir la maîtrise des interventions sur le système industriel.

3.2.1 Gestion des intervenants

Références

- **TTP :** 2.2.3
- **Guide d'hygiène :** règle n° 3
- **ISO 27002 :** 5.19

R15

C1 Mettre en œuvre un processus de gestion des compétences

Il est recommandé de mettre en œuvre un processus de gestion des compétences afin de s'assurer que les intervenants disposent des compétences nécessaires pour leurs missions Ce processus doit en particulier intégrer le transfert de compétences, en cas de départ ou de changement de poste, des personnes en charge des systèmes industriels.

ORG 1.5 SM-4 SP01.01 SP01.02 SP01.03

R16

C2 Mettre en place des procédures de gestion des intervenants

Il est recommandé de mettre en place des procédures de gestion des intervenants, en particulier lors d'une arrivée ou d'un départ. Ces procédures doivent notamment contenir les éléments suivants [9] :

- la création et la suppression de comptes (voir la section 4.1) ;
- la gestion des accès aux locaux ;
- la gestion des équipements mobiles (par exemple : téléphones, tablettes, PC portables) ;

- la gestion des documents sensibles ;
- la mise en place d'une procédure pour la gestion des intervenants de courte durée tels que les intervenants ponctuels et les intérimaires.

ORG 1.3 **SP01.05** **SP01.06** **SP01.07**

R17

C2 Effectuer une revue régulière des intervenants et de leurs comptes

Il est recommandé d'effectuer une revue régulière (au minimum une fois par an) des intervenants et de leurs comptes.

Information

Suivant les réglementations applicables aux systèmes industriels, une enquête de sécurité sur les intervenants pourra être demandée.

3.2.2 Sensibilisation et formation

Références

- **TTP :** 2.2.13
- **Guide d'hygiène :** règles n° 1 et n° 2
- **ISO 27002 :** 6.3

R18

C2 Sensibiliser les intervenants à la cybersécurité

Il est recommandé de sensibiliser les intervenants à la cybersécurité.

ORG 1.5 **SP01.01** **SP01.02** **SP01.03**

R19

C3 Habiliter et former les intervenants à la cybersécurité

Il est recommandé d'habiliter (habilitation interne ou au secret de la défense nationale selon le niveau de sensibilité, se référer au document [51]) tout intervenant à l'utilisation sécurisée du système d'information de l'usine et de veiller à ce que chacun reçoive une formation adaptée à la cybersécurité.

ORG 1.5 **SP01.01** **SP01.02** **SP01.03**

9. L'attribution des rôles est définie dans la recommandation R42.

R20

C3 Former obligatoirement les intervenants avant toute intervention sur le système industriel

Il est recommandé de former obligatoirement les intervenants **avant** toute intervention sur le système industriel.

ORG 1.5 **SP01.01** **SP01.02** **SP01.03**

R21

C3 Choisir des prestataires labellisés

Il est recommandé de choisir des prestataires labellisés pour dispenser les formations de cybersécurité (par exemple une entreprise disposant du label « ExpertCyber » [10]).

R22

C3 Dispenser des séances de formation de cybersécurité en plus des formations de sûreté

Il est recommandé de dispenser les séances de formation à la cybersécurité des systèmes industriels en plus des formations de sûreté et de sécurité du site.

ORG 1.4

3.2.3 Gestion des interventions

Références

- **TTP :** néant
- **Guide d'hygiène :** néant
- **ISO 27002 :** 8.3.2

R23

C2 Définir une procédure de gestion des interventions

Afin de valider les interventions, il est recommandé de mettre en place une procédure de gestion des interventions prévoyant, à chaque intervention, les éléments suivants :

- la personne qui exécute le travail et son donneur d'ordre ;
- la date et l'heure de l'intervention ;
- le périmètre sur lequel le travail est exécuté ;

10. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/label-expertcyber/decouvrir-le-label-expertcyber

- les actions réalisées ;
- la liste des équipements déposés ou remplacés (y compris, le cas échéant, les numéros d'identification) ;
- les modifications apportées et leur impact.

SR 2.8 **SR 2.12** **CR 2.8** **CR 2.12**

R24

C2 Intégrer le processus d'intervention dans la démarche d'amélioration continue

Il est recommandé d'intégrer le processus d'intervention dans la démarche d'amélioration continue de l'entreprise (en tenant compte des différents retours d'expérience) afin de s'assurer du respect de la procédure et éventuellement de la faire évoluer.

SM-13

R25

C2 Mettre en place une procédure d'encadrement lorsqu'un intervenant utilise ses propres outils

Il est recommandé de mettre en place une procédure d'encadrement (signature d'une charte informatique, encadrement par un employé, transmission des références du poste de l'intervenant en amont de l'intervention, etc.) pour les cas exceptionnels où l'intervenant apporte ses propres outils (des outils de diagnostic propres à l'équipementier par exemple). **Dans la phase opérationnelle, il est recommandé de limiter ces interventions à des situations exceptionnelles (par exemple, avarie du système).**

R26

C3 Recenser l'ensemble des matériels et logiciels utilisés pour les interventions

Il est recommandé de recenser, dans la gestion du parc, l'ensemble des équipements matériels et logiciels utilisés pour les interventions sur les systèmes industriels afin qu'ils soient bien identifiés (conformément à la recommandation R6) et maintenus à jour.

SR 7.8 **CR 7.8** **CM 1.1** **SP01.02RE1** **SP06.02BR**

3.3 Intégration de la cybersécurité dans le cycle de vie du système industriel

L'intégration de la cybersécurité dans le cycle de vie des systèmes industriels est important pour parvenir aux exigences attendues. Une attention particulière doit être portée à la cybersécurité lors de la phase de conception du système industriel.

Il est conseillé de ne pas traiter la cybersécurité de manière isolée. Elle doit être intégrée dans le projet comme un métier, au même titre que l'électricité, la mécanique, etc.

3.3.1 Exigences dans les contrats et les cahiers des charges

Références

- **TTP :** 2.2.18
- **Guide d'hygiène :** néant
- **ISO 27002 :** 5.20

Les projets d'installation de systèmes industriels peuvent être réalisés en interne ou en externe. Dans ce cas, il convient de préciser les exigences de cybersécurité dans le cahier des charges. Ces exigences doivent être explicites, mesurables (contrôle de leur mise en place par exemple) et contractualisées.

Le référentiel [48] propose des exigences relatives aux prestataires d'intégration et de maintenance de systèmes industriels. Ces éléments peuvent être intégrés, par exemple, dans un cahier des charges.

R27

C1 Intégrer au cahier des charges les exigences de cybersécurité identifiées lors de la phase de spécification

Il est recommandé d'intégrer au cahier des charges les exigences de cybersécurité identifiées lors de la phase de spécification, en particulier les exigences réglementaires (par exemple celles relatives au *Cyber Resilience Act* – CRA).

R28

C1 Exiger la définition d'un point de contact pour la cybersécurité

Il est recommandé d'intégrer au cahier des charges une clause exigeant l'identification d'un point de contact pour la cybersécurité du projet. Celui-ci devrait être chargé de :

- la liaison avec la chaîne de responsabilité de l'entité responsable (voir la section 3.1.1) ;

- la garantie du respect de la politique de cybersécurité ;
- la communication sur les écarts par rapport aux exigences et les autres non-conformités.

R29

C1 Intégrer dans le cahier des charges la liste des documents à fournir

Il est recommandé d'inclure, dans le cahier des charges, la liste des documents à fournir par le prestataire concernant le système industriel, dont :

- une analyse de risque (voir la section 3.1.3) ;
- une analyse fonctionnelle ;
- une analyse organique [11] ;
- un dossier d'exploitation et de maintenance ;
- une cartographie (voir la section 3.1.2).

ORG 2.1 SP02.01BR SP03.01

R30

C2 Exiger du prestataire un plan d'assurance sécurité

Il est recommandé d'exiger un plan d'assurance sécurité décrivant toutes les mesures répondant aux exigences de cybersécurité demandées (voir le guide relatif à la maîtrise de l'externalisation [18]).

SR-3

R31

C2 Faire figurer des tests de cybersécurité dans le cahier des charges

Il est recommandé de préciser, dans le cahier des charges, des clauses exigeant des tests de cybersécurité, notamment lors des FAT et SAT. La liste des essais demandés doit suivre la recommandation R45.

SVV-1 SVV-3

11. Décomposition d'un système en organes permettant d'assurer les fonctions identifiées lors de l'analyse fonctionnelle (se référer à la norme « NF X50-151 »).

R32

C3 Prévoir une révision de l'analyse de risque pour chaque étape du projet

Il est recommandé d'effectuer une révision de l'analyse de risque à chaque jalon de phases du projet (par exemple : spécification, conception, intégration, validation), mais aussi lors de chaque modification jugée majeure.

R33

C3 S'assurer de l'utilisation d'un environnement de développement sécurisé

Il est recommandé d'utiliser un environnement de développement sécurisé conformément à la section 4.3.6.

ORG 2.3 **SD-1**

R34

C3 Préciser une liste des équipements matériels et logiciels exigeant un Visa de sécurité

Il est recommande de préciser, dans le cahier des charges, une liste des équipements matériels et logiciels exigeant un Visa de sécurité. Cette liste a pour but de mettre en évidence les équipements jugés sensibles et nécessitant une évaluation de sécurité.

R35

C3 Exiger la visibilité du processus de contrôle qualité

Il est recommandé d'exiger, dans le cahier des charges, la visibilité du processus de contrôle qualité afin de réduire les défaillances logicielles et les vulnérabilités. Ces éléments doivent être présents dans le plan d'assurance sécurité (PAS) pour assurer la sécurité de l'information durant les phases projet.

SM-1

3.3.2 Intégration de la cybersécurité dans les phases de spécification

Références

- **TTP :** 2.2.16
- **Guide d'hygiène :** néant
- **ISO 27002 :** 5.8

R36

C1 Intégrer les mesures correspondant à la classe de cybersécurité

Il est recommandé d'intégrer les mesures correspondant à la classe de cybersécurité présentées dans le chapitre 4. À titre d'exemple :

- authentifier les intervenants (voir la section 4.1) ;
- définir une architecture sécurisée (voir la section 4.2) ;
- sécuriser les équipements (voir la section 4.3) ;
- gérer les vulnérabilités (voir la section 4.3.2).

SUM-1

R37

C1 Prendre en compte la sécurité physique

Il est recommandé de prendre en compte la sécurité physique lors de la définition de la localisation des équipements (par exemple le positionnement d'un automate dans un coffret sécurisé ou un local fermé protégé par un contrôle d'accès) selon le guide de sécurisation des systèmes de contrôle d'accès physique et vidéoprotection [35].

ORG 3.1

R38

C1 Intégrer uniquement des outils nécessaires à la conduite et la gestion de l'installation

Il est recommandé d'intégrer uniquement des outils nécessaires à la conduite et la gestion de l'installation industrielle. À titre d'exemple, des postes bureautiques non connectés au système industriel doivent être prévus pour permettre la consultation de la documentation et le remplissage de feuilles de suivi.

R39

C2 Exiger du prestataire des procédures et des moyens techniques pour le maintien en condition de sécurité

Il est recommandé d'exiger du prestataire des procédures et des moyens techniques pour le maintien en condition de sécurité (MCS) des composants du système industriel et faciliter les exigences telles que :

- la maîtrise de la configuration (voir la section 3.3.6) ;
- le durcissement des configurations (voir la section 4.3.1) ;
- la gestion des vulnérabilités (voir la section 4.3.2).

Prévoir des états de variable(s) lors des modes dégradés. Par exemple, le positionnement à un état sûr des variables à chaque redémarrage d'un automate.

SR 3.6 SR 7.6 CR 3.6 CR 7.6 CM 1.3 CM 1.4
DATA 1.4 DM-5 SP06.03

3.3.3 Intégration de la cybersécurité dans les phases de conception

Références

- **TTP :** 2.2.16
- **Guide d'hygiène :** néant
- **ISO 27002 :** 5.8

R40

C1 Limiter au maximum les interfaces et la complexité du système

Il est recommandé, lors de la conception, de limiter au maximum les interfaces et la complexité du système afin d'en réduire la surface d'attaque.

R41

C1 Sélectionner les équipements selon leurs caractéristiques de cybersécurité

Il est recommandé, à fonctionnalités équivalentes, de sélectionner les équipements selon leurs caractéristiques de cybersécurité (par exemple : mécanismes d'authentification, ségrégation des droits, chiffrement).

SR 1.1 SR 1.2 SR 1.3 SR 1.4 SR 1.5 SR 1.6 RE1
CR 1.1 CR 1.2 CR 1.3 CR 1.4 CR 1.5 NDR1.6RE1
SP03.08RE1 SP09.01BR SP09.02

R42

C1 Définir des rôles pour les intervenants

Il est recommandé de définir des rôles pour les intervenants (internes et externes) et de les intégrer dans la gestion des droits des comptes informatiques. Ces rôles correspondent aux missions de chacun (principe du moindre privilège) en distinguant, en particulier, les utilisateurs et les administrateurs (comme précisé à la section 4.1.1).

CR 2.1 RE2 USER 1.5 SP03.08BR

3.3.4 Audits et tests de cybersécurité

Références

- **TTP :** 2.2.17
- **Guide d'hygiène :** règles n° 38 et n° 42
- **ISO 27002 :** 8.34

Afin de s'assurer que le niveau de sécurité ne se dégrade pas au cours du temps, il est nécessaire d'effectuer régulièrement des tests ou des audits de cybersécurité qui doivent être encadrés par des procédures spécifiques. Ces audits peuvent être intégrés aux phases de maintenance et de tests fonctionnels.

La sécurité d'une installation industrielle est dépendante de tous les systèmes qui la composent. Il est donc nécessaire d'auditer l'installation dans son ensemble. Dans la pratique, un séquencement des audits pourra être mis en œuvre de sorte à auditer d'abord les systèmes identifiés comme les plus critiques, conformément à l'analyse de risque réalisée au préalable.

R43

C2 Conduire des audits triennaux

Il est recommandé de réaliser des audits triennaux et lors de modifications substantielles de l'installation. Ces audits peuvent être réalisés par du personnel interne ou externe à l'entité.

R44

C2 Poursuivre les audits par un plan d'actions

Il est recommandé de mettre en place un plan d'actions et de suivi de l'audit validé et contrôlé par l'entité responsable.

R45

C3 Concevoir un programme d'audit

Il est recommandé de réaliser un programme d'audit intégrant les éléments suivants :

- un audit d'architecture ;
- un audit de configuration ;
- un audit organisationnel et physique ;
- des tests d'intrusion physique et logique.

SVV-4

Attention

Les tests d'intrusion logique pouvant entraîner des défaillances : ils doivent être exécutés dans le cadre d'une maintenance, avant la mise en production des systèmes ou sur une plateforme représentative de ce qui est déployé (dans ce cas, le système doit être remis dans sa configuration initiale après l'audit).

R46

C4 Confier les audits à un prestataire qualifié

Il est recommandé de confier l'audit à un prestataire qualifié d'audit de la sécurité des systèmes d'information (PASSI) conformément au référentiel PASSI [47].

R47

C4 Effectuer les audits au moins une fois par an

Il est recommandé d'effectuer les audits au moins une fois par an.

3.3.5 Mise en exploitation

L'entité en charge de l'exploitation peut ne pas être le propriétaire du système industriel, et donc ne pas avoir été impliquée dans son projet de réalisation. Cela peut concerner les cas de délégation de service public, de concession d'exploitation ou de contrat d'exploitation avec obligation de résultat par exemple.

R48

C2 Établir un état des lieux avant la mise en exploitation

Il est recommandé d'établir un état des lieux du niveau de cybersécurité du système avant sa mise en exploitation (par exemple au moyen d'audits internes ou externes).

R49

C3 Faire homologuer les systèmes industriels par l'entité responsable

Il est recommandé de faire homologuer (c'est-à-dire de faire accepter formellement les risques résiduels) les systèmes industriels par l'entité responsable de l'installation.

ZCR 7.1

3.3.6 Gestion des modifications et des évolutions

Références

- **TTP :** néant
- **Guide d'hygiène :** néant
- **ISO 27002 :** 8.32

La gestion des modifications concerne les programmes des automates, les applications SCADA, les fichiers de configurations des différents équipements (par exemple : équipements réseaux, capteurs et actionneurs intelligents).

R50

C1 Tracer les mises à jour et les modifications apportées aux systèmes

Il est recommandé de tracer les mises à jour et les modifications apportées aux systèmes industriels.

R51

C3 Vérifier que seules les modifications nécessaires ont été appliquées

Il est recommandé de vérifier que seules les modifications nécessaires et demandées ont été appliquées aux configurations entre la version courante et la version à installer.

SR 3.4 CR 3.4 CM 1.4 SP03.05BR

R52

C3 Évaluer les modifications dans un environnement de test

Il est recommandé d'évaluer les modifications prévues dans un environnement de test avant leurs mises en production.

R53

C3 Faire valider les impacts des modifications par l'entité responsable

Il est recommandé de faire valider les impacts des modifications par l'entité responsable avant la mise en production.

R54

C4 Mettre en place un processus de vérification des versions de programme en cours d'exécution

Il est recommandé de mettre en place un processus de vérification des versions de programme en cours d'exécution par rapport à une version de référence. Cela permet de s'assurer que les processus exécutés par le système industriel (par exemple les automates, les logiciels SCADA) sont ceux qui doivent être utilisés.

CR 3.4

3.3.7 Processus de veille

Références

- **TTP :** 2.2.2
- **Guide d'hygiène :** règle n° 34
- **ISO 27002 :** 8.8

R55

C2 Se tenir informé des vulnérabilités critiques et des correctifs associés

Il est recommandé de se tenir informé des vulnérabilités critiques et des correctifs relatifs aux équipements matériels et logiciels utilisés dans le système industriel.

COMP 3.3 **EVENT 1.9** **DM-1** **SP03.03BR** **SP11.06RE3**

Information

Ce processus devrait notamment reposer sur les sources ouvertes disponibles telles que les CSIRT nationaux (par exemple CERT-FR [12], ICS-CERT), les PSIRT des équipementiers et des éditeurs de logiciels.

R56

C2 Mettre en place un processus de veille sur l'évolution des techniques d'attaque et de défense

Il est recommandé de mettre en place un processus de veille sur l'évolution des techniques d'attaque et de défense.

12. https://www.cert.ssi.gouv.fr/

R57

C3 Contractualiser la diffusion des bulletins de vulnérabilités

Il est recommandé de contractualiser la diffusion, auprès des fournisseurs, des bulletins de vulnérabilités pour l'ensemble des équipements matériels et logiciels utilisés au sein du système industriel.

DM-5

3.3.8 Gestion de l'obsolescence

La gestion de l'obsolescence n'est pas directement une mesure de cybersécurité mais elle y contribue. Les équipements obsolètes peuvent contenir de nombreuses vulnérabilités qui ne seront jamais corrigées. La gestion de l'obsolescence est donc un processus utile et nécessaire pour la gestion des vulnérabilités.

Références

- **TTP :** 2.2.2
- **Guide d'hygiène :** règles n° 34 et n° 35
- **ISO 27002 :** néant

R58

C1 Intégrer des clauses relatives à la gestion de l'obsolescence

Il est recommandé d'intégrer des clauses relatives à la gestion de l'obsolescence des équipements et logiciels en indiquant, par exemple, la date à laquelle le support ne sera plus assuré par les fournisseurs, la date jusqu'à laquelle il y a un souhait de maintien en condition opérationnelle.

R59

C2 Mettre en œuvre un plan de gestion de l'obsolescence

Il est recommandé de mettre en œuvre un plan de gestion de l'obsolescence pour remplacer les équipements et applications obsolètes.

3.4 Sécurité physique et contrôle d'accès aux locaux

Cette section décrit les mesures de sécurité physique adaptées à la classe du système concerné afin de réduire les risques d'accès non autorisés au système industriel.

3.4.1 Accès aux locaux

Références

- **TTP :** 2.2.8
- **Guide d'hygiène :** règle n° 26
- **ISO 27002 :** 7.2 et 7.4

R60

C1 Définir une politique de contrôle d'accès physique

Il est recommandé de définir une politique de contrôle d'accès physique conformément aux recommandations de sécurité relatives au contrôle d'accès et à la vidéoprotection [35].

ORG 3.1

R61

C1 S'assurer que les accès aux locaux sont journalisés et auditables

Il est recommandé de s'assurer que les accès aux locaux sont journalisés et auditables.

SR 2.8 RE1 CR 6.1 RE1 EVENT 1.6 SP08.02RE1

R62

C2 S'assurer de la robustesse des mécanismes de contrôle d'accès

Il est recommandé de s'assurer de la robustesse des mécanismes de contrôle d'accès, en se reportant notamment aux recommandations de sécurité relatives au contrôle d'accès et à la vidéoprotection [35].

R63

C2 Réserver aux seules personnes autorisées l'accès aux équipements

L'accès physique aux équipements doit être strictement réservé aux personnes autorisées.

R64

C3 Mettre en œuvre un système de détection d'intrusion pour les zones sensibles

Il est recommandé de mettre en œuvre un système de détection d'intrusion pour les zones sensibles (ou contrôlées au sens du guide [35]), en particulier celles non occupées 24 heures sur 24.

R65

C3 Placer les accès sous vidéoprotection ou vidéosurveillance

Il est recommandé de placer les accès sous vidéoprotection (sites publics) ou vidéosurveillance (sites privés). Ces derniers doivent se conformer, respectivement, au code de la sécurité intérieure et au RGPD [13].

3.4.2 Accès aux équipements et aux câblages

Références

- **TTP :** 2.2.8
- **Guide d'hygiène :** règle n° 26
- **ISO 27002 :** 7.8 et 7.12

R66

C1 Installer les serveurs dans des locaux fermés

Il est recommandé d'installer les serveurs SCADA dans des locaux fermés et avec un contrôle d'accès.

R67

C1 Réduire le nombre de prises d'accès au réseau dans les endroits ouverts au public

Il est recommandé de réduire le nombre de prises d'accès au réseau du système industriel lorsqu'il est situé dans des endroits ouverts au public.

EDR 3.11 NDR 3.11 HDR 3.11

13. https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000025505424/

R68

C2 Installer les équipements dans des armoires avec accès contrôlés

Il est recommandé d'installer les unités centrales des stations, les équipements réseaux industriels et les automates dans des armoires avec accès contrôlés.

R69

C2 Réduire le nombre de prises d'accès au réseau dans les zones sans surveillance

Il est recommandé de réduire le nombre de prises d'accès au réseau au réseau du système industriel dans les zones sans surveillance.

EDR 3.11 NDR 3.11 HDR 3.11

R70

C2 Protéger l'intégrité physique des câbles

L'intégrité physique des câbles doit être protégée (par exemple par un capotage).

R71

C2 Obturer les prises réseau dédiées à la maintenance lorsqu'elles ne sont pas utilisées

Si les ports d'accès au réseau du système industriel ne peuvent être fermés logiquement comme énoncé à la recommandation R156, il est recommandé d'obturer les prises réseau dédiées à la maintenance lorsqu'elles ne sont pas utilisées (par exemple à l'aide de bouchons ou de plaques d'occultation).

R72

C3 Déployer un dispositif de détection d'ouverture avec remontée d'alarme

Il est recommandé de déployer un dispositif de détection d'ouverture, avec remontée d'alarme, sur les armoires des équipements sensibles. Au minimum, il est recommandé d'installer sur les coffrets extérieurs contenant des composants sensibles un moyen de contrôle visuel, comme la pose de scellés par exemple. Le retrait de ces moyens visuels doit suivre une procédure et doit être soumis à autorisation préalable.

3.5 Anticipation et réaction en cas d'incident

3.5.1 Plan de reprise ou de continuité d'activité

Les plans de reprise ou de continuité d'activité (PRA et PCA) permettent de garantir la reprise ou la continuité du service suite à un sinistre, quelle qu'en soit l'origine. Le plan de continuité d'activité, parfois déjà existant pour répondre à des sinistres d'origine autre que la cybersécurité, doit

répondre à l'ensemble des événements redoutés entraînant un arrêt du service rendu, tels qu'ils ont été identifiés dans l'analyse de risque pour la cybersécurité. Pour plus de détails, se reporter au guide édité par le SGDSN [57].

Références

- **TTP :** 2.2.15
- **Guide d'hygiène :** règle n° 37
- **ISO 27002 :** 5.29 et 5.30

R73

C1 Mettre en place un plan de sauvegarde et de restauration

Il est recommandé de mettre en œuvre un plan de sauvegarde et de restauration afin de pouvoir reconstruire le système après un incident de cybersécurité (voir le chapitre 3.1.4). Pour plus d'informations, se reporter aux Fondamentaux relatifs à la sauvegarde des systèmes d'information [16].

SR 7.3 RE2 | SR 7.4 | CR 7.4 | AVAIL 2.1 | AVAIL 2.5 | SP12.01BR | SP12.02BR | SP12.05BR | SP12.06BR | SP12.08BR

R74

C1 Inclure les incidents de cybersécurité dans les PRA et PCA

Il est recommandé d'inclure les incidents de cybersécurité au sein des plans de reprise et de continuité d'activité.

AVAIL 1.1 | SP12.09

R75

C2 Tester régulièrement les PRA et PCA

Il est recommandé de tester régulièrement les plans de reprise et de continuité d'activité, et au moins une fois par an sur les applications critiques pour les processus métier.

R76

C1 Définir un ordre de reconstruction des sites industriels avec la direction

Il est recommandé de définir un ordre de reconstruction des systèmes industriels avec la direction. Plusieurs sites peuvent être simultanément impactés par une cyberattaque. Certains sites peuvent présenter un niveau de criticité plus élevé que d'autres, il est essentiel de définir et valider en amont, avec les métiers, un ordre de priorité pour la remise en service des installations industrielles. Cette priorisation doit également inclure les applications les plus critiques pour les processus métier.

3.5.2 Modes dégradés

R77

C1 S'assurer que les mesures de cybersécurité ne portent pas atteinte au bon fonctionnement des modes dégradés

Il est recommandé de s'assurer que les mesures de cybersécurité ne portent pas atteinte au bon fonctionnement des modes dégradés du système, en particulier ceux permettant de garantir la sécurité des biens et personnes.

COMP 3.4 **SP11.06RE1**

R78

C2 Intégrer un mode d'urgence dans les procédures

Il est recommandé d'intégrer un mode d'urgence (par exemple avec la mise en place d'un compte « bris de glace »[14]) dans les procédures. Il s'agit typiquement des secrets d'authentification relatifs à des comptes de séquestre sensibles, qui visent notamment à permettre la reconstruction de systèmes en cas d'incident majeur, comme par exemple les mots de passe DSRM (voir le guide [9]) pour pouvoir intervenir rapidement en cas de besoin sans dégrader significativement le niveau de cybersécurité du système industriel. En particulier, cette procédure d'urgence doit être documentée.

SR 1.1 **CR 1.1** **NDR 1.6** **USER 1.8**

14. Un compte « bris de glace » est un compte à privilège dont le mot de passe est conservé dans un coffre et dont l'usage est réservé à la résolution d'incident exceptionnel. Après usage, le mot de passe est modifié et remis dans le coffre. Généralement, l'authentification de ce compte repose sur la seule utilisation d'un mot de passe très complexe.

3.5.3 Gestion de crise

Références

- **TTP :** 2.2.15
- **Guide d'hygiène :** règles n° 40
- **ISO 27002 :** 5.29 et 5.30

R79

C1 Mettre en place une procédure de gestion de crise

Il est recommandé de mettre en place une procédure de gestion de crise conformément aux publications de l'ANSSI [31].

R80

C1 Inclure une procédure d'escalade

Il est recommandé d'inclure une procédure d'escalade dans le processus de gestion de crise pour gérer les incidents au bon niveau de responsabilité et décider en conséquence (conformément au guide [31]) :

- s'il faut déclencher un plan de reprise d'activité ;
- si une action judiciaire est nécessaire.

R81

C1 Définir une phase d'analyse post incident

Il est recommandé de définir une phase d'analyse post incident dans le but de déterminer l'origine de l'incident et d'améliorer la cybersécurité du système industriel (conformément au guide [31]).

R82

C2 Réaliser des exercices de gestion de crise

Il est recommandé de réaliser des exercices de gestion de crise, et au moins une fois par an (se reporter au guide [25] pour plus de détail).

4
Mesures techniques de sécurité

Ce chapitre regroupe l'ensemble des mesures techniques s'adressant à l'ensemble des acteurs impliqués dans les systèmes industriels (par exemple : chefs de projet, acheteurs, automaticiens, intégrateurs, développeurs, équipementiers, mainteneurs, RSSI).

Information

Il revient à l'entité responsable de définir quelle personne sera en charge de l'application des mesures sur les systèmes.

Les mesures font référence aux chapitres de l'ISO 27002 [55] ainsi qu'aux recommandations du guide d'hygiène informatique [17] publié par l'ANSSI.

Ces références sont indiquées dans un encadré comme celui présenté ci-dessous :

Références

- **TTP :** fait référence aux TTP indiqués dans la section 2.2.
- **Guide d'hygiène :** fait référence au guide d'hygiène [17].
- **ISO 27002 :** fait référence aux chapitres de l'ISO 27002 [55] abordant le sujet.

Attention

Les mesures sont cumulatives. Ainsi, un système de classe 2 doit appliquer les mesures de classe 1 et de classe 2 et un système de classe 4 doit appliquer les mesures de classe 1, de classe 2, de classe 3 et de classe 4.

Le périmètre d'application est précisé pour chaque famille de mesures, voire chaque mesure. Sans précision complémentaire, il est le même pour toutes les mesures d'une famille.

Les équipements sur lesquels peuvent porter les mesures sont :

- les serveurs, stations et postes de travail ;
- les stations d'ingénierie (console de programmation et poste de maintenance) ;
- les équipements mobiles (ordinateurs portables, tablettes, smartphones) ;

- les logiciels et applications de supervision (SCADA) ;
- les logiciels et applications MES, EMS, WMS, etc., si existants ;
- les interfaces homme-machine tactiles ;
- les automates et unités déportées (RTU - *Remote Terminal Unit*) ;
- les modules d'entrées/sorties déportés des automates ;
- les équipements réseau (commutateurs, routeurs, pare-feux, bornes d'accès sans fil) ;
- les capteurs et actionneurs intelligents ;
- les passerelles protocolaires.

Cette liste est un exemple et doit être adaptée à l'environnement de chaque système.

4.1 Authentification et contrôle d'accès logique

4.1.1 Gestion des comptes

Références

- **TTP :** 2.2.3
- **Guide d'hygiène :** règles n° 5, n° 6, n° 8 et n° 12
- **ISO 27002 :** 5.15

Les comptes peuvent être de différents types :

- les comptes « de session » permettant l'accès aux stations, postes de travail (bureautique, d'exploitation, de maintenance, etc.) et serveurs ;
- les comptes « applicatifs » permettant à un intervenant de se connecter à une application SCADA par exemple ; ces comptes peuvent être gérés par l'application elle-même ;
- les comptes « systèmes » sont utilisés pour qu'une application puisse s'exécuter et communiquer avec d'autres applications (ex. : compte de service) ; ces comptes ne sont normalement pas utilisés par un opérateur.

Les comptes peuvent disposer de différents niveaux de privilèges. En particulier, les comptes avec un niveau de privilèges élevé se découpent en deux catégories :

- les comptes à privilèges élevés « administrateur système » permettant l'administration informatique des équipements (serveurs, stations et équipements réseau par exemple) et des systèmes d'exploitation ;
- les comptes à privilèges élevés « ingénieur de procédé » permettant d'accéder à des fonctions de configuration ou de programmation des applications SCADA et automates par exemple.

Information

Les comptes avec un niveau de privilèges élevé cités précédemment doivent appartenir à des groupes d'utilisateurs distincts.

R83

C1 Identifier chaque utilisateur à privilèges de manière individuelle

Il est recommandé d'identifier chaque utilisateur à privilèges de manière nominative.

SR 1.1 RE1 | SR 1.3 | SR 1.4 | CR 1.1 | CR 1.3 | CR 1.4 | NDR 1.6 | USER 1.8 | USER 2.2

R83 +

C1 Identifier chaque utilisateur de manière individuelle

Il est recommandé d'identifier chaque utilisateur de manière nominative, y compris les utilisateurs non privilégiés.

SR 1.1 RE1 | SR 1.3 | SR 1.4 | CR 1.1 | CR 1.3 | CR 1.4 | NDR 1.6 | USER 1.8

Information

Des cas particuliers peuvent imposer la création de comptes partagés, empêchant ainsi la stricte imputabilité de chaque opération effectuée. Il peut s'agir d'équipements qui n'intègrent pas de mécanisme de gestion de comptes ou de systèmes qui doivent maintenir dans la durée une même session active. Dans ce cas, les utilisateurs ne peuvent pas recourir à des sessions différentes, ouvertes avec leurs comptes individuels respectifs. C'est le cas, par exemple, des postes de conduite d'une installation industrielle. L'entité responsable doit ainsi mettre en place des mesures permettant d'atteindre un niveau d'imputabilité équivalent à celui assuré par l'utilisation d'un compte individuel (par exemple : un cahier d'enregistrement, un système de contrôle d'accès et de vidéoprotection des locaux).

R83 -

C1 Appliquer des mesures palliatives d'imputabilité

Lorsque l'utilisation de comptes individuels n'est pas possible, il est recommandé de mettre en œuvre des mesures permettant d'atteindre un niveau d'imputabilité équivalent (par exemple dans un cahier à l'entrée de la salle).

Exemple

Dans une salle de contrôle opérationnelle en 24/7, les intervenants ont besoin d'agir rapidement sur l'installation industrielle depuis l'application SCADA. Des comptes individuels peuvent être inadaptés. Il peut être envisageable dans ce cas, en tant que mesure palliative, de ne pas exiger d'identifiant et de mot de passe individuel, car l'accès à la salle de contrôle est possible uniquement à des intervenants habilités, les accès physiques sont tracés, et la salle de contrôle est occupée en permanence.

R84

C1 Éviter d'utiliser des comptes génériques

Il est recommandé de ne pas utiliser de comptes génériques, en particulier ceux disposant de privilèges. Lorsqu'ils sont indispensables, leur utilisation doit être limitée à des usages très précis, être documentée et un propriétaire du compte générique doit être désigné.

SR 1.1 RE1 | SR 1.3 | SR 1.4 | CR 1.1 | CR 1.3 | CR 1.4 | NDR 1.6 | USER 1.8

Attention

Lorsque des comptes génériques sont utilisés pour des raisons d'exploitation de l'installation, il est nécessaire d'appliquer la recommandation R83-.

R85

C1 Définir et documenter l'ensemble des droits attribués

Il est recommandé de définir et documenter, pour chacun des profils utilisateurs, l'ensemble des droits attribués. Leur mise en œuvre peut s'appuyer sur des mécanismes de type RBAC (*Role-Based Access Control*).

SR 2.1 | CR 2.1 | USER 2.1 | SP03.07BR

R86

C1 Supprimer les comptes appartenant à des personnels n'intervenant plus sur le système industriel

Il est recommandé de supprimer ou, au minimum, désactiver les comptes appartenant à des personnes n'intervenant plus sur le système industriel (conformément à la recommandation R16).

ORG 1.3 | SM-2 | SP01.05BR | SP01.06BR | SP01.07BR

R87

C1 Modifier tous les authentifiants par défaut

Il est recommandé de modifier tous les authentifiants (par exemple, certificat, mot de passe) par défaut (par exemple, implémentés par le constructeur, l'intégrateur).

SR 1.3 SR 1.5 CR 1.3 CR 1.5

R88

C2 Auditer les événements liés à l'utilisation des comptes

Il est recommandé de mettre en place un audit des événements liés à l'utilisation des comptes (une liste minimale des événements à journaliser est présentée à l'annexe C du guide).

SR 2.8 CR 2.8 EVENT 1.1 SP08.01BR SP08.03BR

R89

C2 Faire valider les comptes à privilèges par un responsable

Il est recommandé de faire valider les comptes à privilèges par un responsable de l'utilisateur.

R90

C2 Conduire une revue annuelle des comptes

Il est recommandé de revoir annuellement les comptes des utilisateurs internes et externes à l'organisation afin de vérifier la bonne application des recommandations R86 et R89. Cette revue doit porter une attention particulière aux comptes à privilèges. Afin de faciliter sa mise en œuvre périodique, il est recommandé de l'automatiser. Par exemple, pour un serveur *Active Directory Domain Services*, il est possible de lister les comptes actifs avec une date de dernière connexion pouvant présumer que l'utilisateur ne fait plus partie de l'organisation. Le script liste et désactive les comptes concernés et transfère les états par mail. Le gestionnaire peut ensuite décider dans un second temps, après vérification, de supprimer ces comptes.

R91

C2 Configurer un accès par défaut en lecture seule aux équipements

Lorsque les équipements le permettent, un accès en lecture seule doit être configuré par défaut.

R92

C3 Auditer la configuration de l'annuaire

Il est recommandé d'auditer régulièrement, et au moins une fois par an, la configuration de l'annuaire (par exemple, OpenLDAP, Active Directory) si la gestion des

comptes est centralisée (pour les entités réglementées, on pourra se reporter au service ADS [56]).

Attention

Une solution centralisée (comme par exemple OpenLDAP, Active Directory) peut faciliter la gestion des comptes et droits des intervenants. Dans ce cas, il faut favoriser une solution centralisée dédiée aux environnements industriels (séparation IT/OT).

4.1.2 Gestion de l'authentification

Références

- **TTP :** 2.2.3
- **Guide d'hygiène :** règles n° 9, n° 10, n° 11, n° 12 et n° 13
- **ISO 27002 :** 5.15

R93

C1 Authentifier les utilisateurs avec identifiant et mot de passe

Les utilisateurs doivent s'authentifier avec au moins un identifiant et un mot de passe. Lorsque cela est possible, la politique de mots de passe doit répondre aux exigences suivantes :

- les mots de passe doivent être robustes (conformément au guide relatif à l'authentification multifacteur et aux mots de passe [50]) ;
- les mots de passe définis initialement par le service informatique doivent être modifiés par l'utilisateur à la première connexion.

SR 1.1 **SR 1.5** **SR 1.7** **CR 1.1** **CR 1.5** **CR 1.7**
USER 1.11 **SP09.05** **SP09.06** **SP09.07** **SP09.08**

R93 -

C1 Définir et documenter des mesures compensatoires en cas d'impossibilité d'authentifier

Il est recommandé de définir et documenter des mesures compensatoires dans le cas où une authentification ne peut pas être appliquée, du fait de contraintes opérationnelles notamment. À titre d'exemple, on peut envisager :

- d'appliquer un contrôle d'accès physique ;
- de limiter les fonctionnalités accessibles (consultation sans modification, par exemple) ;

- de mettre en place une authentification par carte à puce sans code ;
- de cloisonner plus fortement l'équipement.

R94

C1 Privilégier un verrouillage temporaire de compte en cas d'échec d'authentification

Il est recommandé de privilégier un verrrouillage temporaire par rapport au blocage d'un compte en cas d'échecs répétés d'authentification.

CR 1.11 SR 1.11 EVENT 1.1 USER 1.14

R95

C1 Protéger les mots de passe en confidentialité et en intégrité

Il est recommandé de protéger les mots de passe en confidentialité et en intégrité quand ces derniers sont transmis sur le réseau.

R96

C1 Stocker les secrets de manière sécurisée

Il est recommandé de stocker de manière sécurisée (par exemple dans un HSM, une carte à puce) les secrets (par exemple, clefs privées, empreintes de mot de passe) afin d'assurer leur confidentialité et leur intégrité.

SR 4.1 CR 1.14 CR 4.1 DATA 1.2 SP03.08RE2

R97

C1 Définir une procédure sécurisée pour la réinitialisation des mots de passe

Il est recommandé de définir une procédure qui garantit la confidentialité et l'intégrité des authentifiants lors de la réinitialisation des mots de passe.

SR 1.5 CR 1.5

R98

C1 Journaliser les événements de sécurité liés à l'authentification des comptes à privilèges

La journalisation des événements de sécurité doit enregistrer les échecs d'authentification et les authentifications réussies des comptes à privilèges.

R98 +

C1 Journaliser les événements de sécurité liés à l'authentification des comptes utilisateur

Il est recommandé de journaliser les échecs et les réussites d'authentification des comptes utilisateur.

R99

C2 Mettre en œuvre une authentification multifacteur

Sauf contrainte opérationnelle justifiée, il est recommandé de mettre en œuvre une authentification multifacteur (par exemple, avec une carte à puce ou un OTP comme second facteur) sur les postes de travail et serveurs dont les accès sont critiques (par exemple une station d'ingénierie).

SR 1.1 | CR 1.1 RE2 | USER 1.9 | SP03.07RE1

R99 +

C2 Mettre en œuvre une authentification forte

Conformément au guide relatif à l'authentification multifacteur et aux mots de passe [50], il est recommandé de mettre en œuvre une authentification forte (par exemple, FIDO2, protocole OTP, Kerberos) *a minima* sur les postes de travail et serveurs dont les accès sont critiques (par exemple une station d'ingénierie).

SR 1.1 | CR 1.1 RE2 | USER 1.9 | SP03.07RE1

R100

C2 Renforcer la politique de mots de passe

Lorsque la recommandation R99 ne peut pas être appliquée, la politique de mots passe de la recommandation R93 devrait être renforcée par :

- la conservation de l'historique des mots de passe (par exemple les 5 derniers) pour éviter leur réutilisation ;
- la vérification technique de la complexité du mot de passe ;
- la définition d'une politique de renouvellement du mot de passe [15].

4.2 Sécurisation de l'architecture du système industriel

4.2.1 Principe d'interconnexion entre classes

Dans certains cas de figure et selon le découpage des zones, il peut être nécessaire de transmettre des informations vers des zones de classe inférieure (par exemple depuis un sous système vers son

15. Un renouvellement de mots de passe trop fréquent pourrait inciter les utilisateurs à noter les mots de passe sur une feuille. Cette dernière ne sera pas nécessairement conservée en lieu sûr.

DCS). Pour cela, il est recommandé de mettre en œuvre une passerelle d'interconnexion sécurisée industrielle conformément à la section 4.2.2.

Les fonctions de sécurité portées par une telle passerelle ont pour but :

- de protéger en intégrité les classes hautes ;
- de protéger en confidentialité des données exportées depuis ces mêmes classes ;
- de limiter la capacité de latéralisation d'un attaquant entre les zones, indépendemment de leur casse.

Les fonctions de sécurité associées à la passerelle sont listées dans le tableau 3 et décrites ci-dessous :

- **Uni** : fonction d'unidirectionnalité du transfert de données entre deux zones qui permet :
  - d'assurer que les données soient exclusivement ou écrites ou lues depuis une seule des deux zones, garantissant que le flux d'information est strictement à sens unique entre ces zones.
  - de limiter la capacité de latéralisation entre les deux zones.

Information

Cette fonction est préférablement positionnée au plus proche de la classe de moindre sécurité pour les propriétés d'isolation qu'elle confère à l'interconnexion, de préférence avec un pare-feu. Les solutions techniques compatibles pour mettre en œuvre cette fonction sont, notamment, un pare-feu *à états*, une passerelle d'interconnexion ou une diode (selon la classe, définie dans le tableau 3).

- **Aut (IT)** : fonction de contrôle de la source de la donnée à partir d'une liste de sources de données autorisées (type liste d'autorisations) afin de s'assurer de la provenance légitime des données émises. Cette fonction de contrôle peut être mise en œuvre, par exemple, avec un pare-feu *à états* autorisant une adresse IP source qui peut être complétée par une authentification.
- **Rup** : fonction de rupture protocolaire et de transformation de la donnée, par exemple avec une passerelle protocolaire Modbus/BACnet.
- **Aut (OT)** : fonction de contrôle de la destination des données à partir d'une liste de tuples autorisés (type liste d'autorisations) afin d'assurer que la donnée transmise peut être écrite dans la classe de destination. Ceci peut être mis en œuvre, par exemple, avec un pare-feu disposant de la fonctionnalité *Deep Packet Inspection* sur la base des règles suivantes :
  - `IP Source, IP Destination, Protocole: Modbus, IPS : write single register (code 6) : adresse du registre;`
  - `IP Source, IP Destination, Protocole: OPC UA, IPS : write (Id 673 et 676);`
  - `IP Source, IP Destination, Protocole: IEC 60870-5-104, IPS : type P_ME_NA_1 (Id 110) : valeur à transmettre.`
- **Inno (IT)** : fonction de vérification antivirale des données transmises pour s'assurer qu'elles ne sont pas vectrices de code malveillant. Ce contrôle d'innocuité bénéficie idéalement des mêmes politiques antivirales et de supervision de sécurité que l'OT.

Le tableau 3 synthétise les différentes fonctions de sécurité nécessaires à l'interconnexion entre systèmes de classes différentes conformément à la section 4.2.2.

Les fonctions de sécurité de la passerelle peuvent être mises en œuvre au sein de multiples architectures composées d'un ou plusieurs produits. Le choix de mise en œuvre de ces fonctions est dépendant du contexte de l'interconnexion. De plus, les fonctions doivent être mises en œuvre avec un niveau de sécurité adapté au regard du risque.

Information

Le choix de décrire les passerelles d'interconnexion d'un point de vue fonctionnel, par opposition à une description orientée solutions (par exemple : pare-feu, diode, ACL dans un équipement de télécommunication), vise à permettre une plus grande liberté de mise en œuvre de ces fonctions afin de les adapter à une grande variété de systèmes industriels et, en particulier, pour les interconnexions non IP.
Les fonctions décrites s'appuient sur celles définies dans les recommandations pour les architectures des interconnexions multiniveaux [39]. Elles sont adaptées à la protection en intégrité des classes hautes et en confidentialité des données exportées. L'iconographie a été choisie en cohérence avec ce guide. En particulier, le symbole de la diode fait référence à la fonction d'unidirectionnalité des données.

Pour des éléments supplémentaires relatifs aux passerelles d'interconnexions IT/OT, il est possible de se référer à l'article *Approche SSI pour l'Internet des objets industriels* [52].

		Classes				
	vers	IT	C1	C2	C3	C4
Classes	IT		Uni + Aut (IT)	Uni + Aut (IT) + Rup + Inno (IT) + Aut (OT) + Inno (OT)	Uni + Aut (IT) + Rup + Inno (IT) + Aut (OT) + Inno (OT)	***À proscrire***
	C1	Uni + Aut (IT)	Uni + Aut (IT)	Uni + Aut (IT)	Uni + Aut (IT) + Rup + Aut (OT)	Uni + Aut (IT) + Rup + Aut (OT) + Inno (OT)
	C2	Uni + Aut (IT) + Rup	Uni + Aut (IT) + Rup	Uni + Aut (IT)	Uni + Aut (IT) + Rup + Aut (OT)	Uni + Aut (IT) + Rup + Aut (OT) + Inno (OT)
	C3	Uni + Aut (IT) + Rup	Uni + Aut (IT) + Rup	Uni + Aut (IT) + Rup	Uni + Aut (IT)	Uni + Aut (IT) + Aut (OT) + Inno (OT)
	C4	Uni + Aut (IT) + Rup ***ou*** Diode (voir R115)	Uni + Aut (IT) + Rup ***ou*** Diode (voir R115)	Uni + Aut (IT) + Rup ***ou*** Diode (voir R115)	Uni + Aut (IT) + Rup ***ou*** Diode (voir R115)	Uni + Aut (IT) ***ou*** Diode (voir R115)

TABLE 3 – Fonctions de sécurité entre classes – Ce tableau permet d'identifier les fonctions de sécurité minimales à mettre en œuvre lors d'une interconnexion d'une classe source (lignes) vers une classe destination (colonnes). Exemple de lecture : les communications entre IT et une classe 4 sont à proscrire. Entre une classe 1 et IT, les fonctions Uni et Auth(IT) sont à mettre en œuvre.

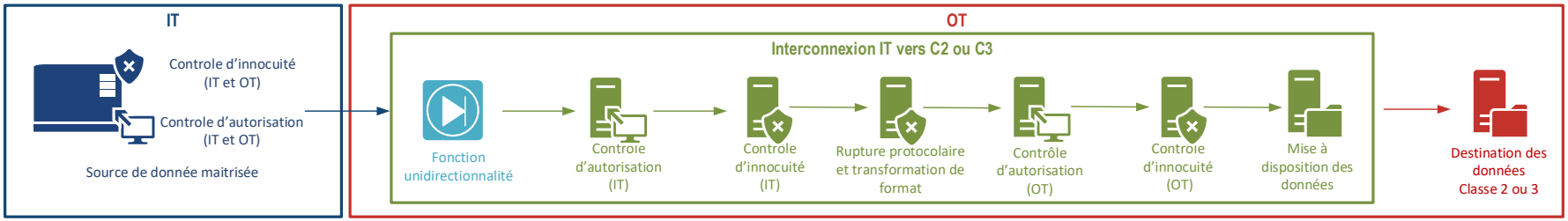

FIGURE 1 – Proposition de passerelle IT vers OT (classe 2 ou classe 3)

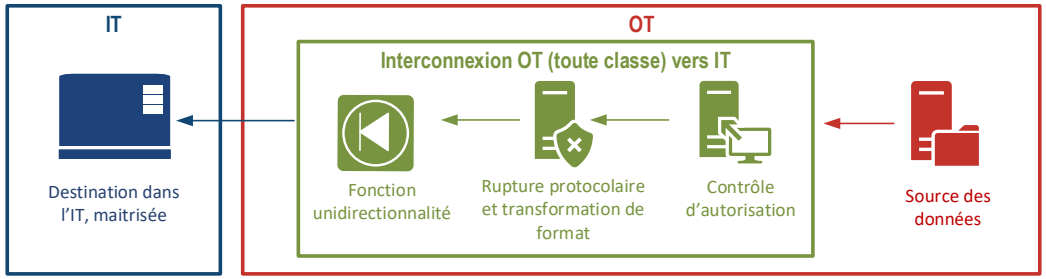

FIGURE 2 – Proposition de passerelle OT vers IT

4.2.2 Cloisonnement des systèmes industriels

Références

- **TTP :** 2.2.10
- **Guide d'hygiène :** règles n° 19, n° 27, n° 28 et n° 42
- **ISO 27002 :** 8.22

R101

C1 Segmenter les systèmes industriels en zones cohérentes

Il est recommandé de segmenter les systèmes industriels en zones cohérentes selon la méthode proposée dans le guide méthode de classification [41]. Ces zones doivent être cloisonnées entre elles.

ZCR 3.2

R102

C1 Mettre en œuvre une politique de filtrage entre les zones

Il est recommandé de mettre en œuvre une politique de filtrage entre les zones. Pour définir cette politique de filtrage, il est notamment possible de se reporter au guide relatif à la définition d'une politique de pare-feu [19].
Pour les flux utilisant le protocole IP, quelques grands principes sont rappelés ici :

- un flux est identifié par l'adresse IP source, l'adresse IP destination, le protocole (par exemple UDP ou TCP) et, le cas échéant, les numéros de port source et destination ;
- les flux sont refusés par défaut ;
- seuls les flux nécessaires au fonctionnement du système industriel sont autorisés ;
- les flux refusés peuvent être journalisés et analysés conformément à la stratégie de sécurité établie en R203 (une liste minimale des événements à journaliser est présentée à l'annexe C du présent guide).

SR 5.2 CR 5.2 NET 1.1

Exemple

À titre d'exemples, quelques protocoles et ports standards utilisés dans les systèmes industriels :

- Modbus : TCP/502
- S7Comm : TCP/102

- EtherNet/IP : TCP/44818, UDP/44818 et UDP/2222
- BACnet/IP : UDP/47808
- BACnet/SC : TCP/47808
- OPCUA : TCP/4840 (parfois TCP/4841)
- Profinet IO : TCP/UDP 34962 (RT Unicast), 34963 (RT Multicast), 34964 (Context Manager)

R103

C1 Sécuriser les interconnexions entre les zones

Il est recommandé de sécuriser les interconnexions en utilisant les fonctions de sécurité décrites dans le tableau 3.

SR 5.1 **CR 5.1**

R104

C1 Cloisonner le réseau d'administration

Il est recommandé d'utiliser un réseau d'administration dédié. Ce réseau doit être cloisonné des équipements des autres réseaux, physiquement ou à défaut logiquement. Pour de plus amples informations, se reporter au guide d'administration sécurisée [33].

ZCR 3.2 **SR 5.1** **SR 5.2** **CR 5.1** **CR 5.2** **NDR 5.2**
NDR 5.13 **NET 1.1** **SP03.02** **SP03.03RE1** **SP03.07BR**

Information

Le poste d'administration est décrit au chapitre 4.3.5 du présent guide.

R105

C2 Réserver les postes d'administration à ce seul usage

Il est recommandé de réserver les postes d'administration à ce seul usage. Ils ne doivent pas être connectés à Internet, ni à un autre réseau informatique que celui utilisé pour l'administration (conformément au guide d'administration sécurisée [33]).

ZCR 3.6

R106

C2 Privilégier un cloisonnement physique entre les zones fonctionnelles

Il est recommandé de privilégier un cloisonnement physique entre les zones fonctionnelles du système industriel. Indépendamment de la cybersécurité, le cloisonnement physique participe à renforcer la disponibilité de l'installation industrielle.

SR 5.1 RE3 **NET 1.1** **SP03.02BR**

R106 -

C2 Mettre en place un cloisonnement logique entre les zones fonctionnelles

Il est recommandé de mettre en place un cloisonnement logique lorsqu'une séparation physique n'est pas possible entre les zones fonctionnelles du système industriel. Le cloisonnement à réaliser s'entend aux niveaux : calcul (par exemple un système d'exploitation), réseau (par exemple VLAN) et stockage (par exemple VSAN).

SR 5.1 RE3 **NET 1.1** **SP03.02BR**

Exemple

Voici un exemple de cloisonnement logique de composants industriels au niveau réseau :

- un VLAN d'administration pour les composants réseau, l'administration des serveurs, les postes d'administration et les serveurs d'administration (se référer à la recommandation R104 pour les équipements d'administration) ;
- un VLAN pour le réseau de supervision des serveurs SCADA et des postes de conduite ;
- un VLAN pour le réseau des serveurs SCADA et le ou les serveurs métier (MES et ERP par exemple) ;
- un VLAN pour les stations d'ingénierie (se référer à la recommandation R104 pour les équipements d'administration) ;
- un VLAN par procédé contenant les automates et autres équipements associés (par exemple, entrées/sorties déportées).

R107

C2 Identifier les équipements obsolètes et les cloisonner de manière appropriée

Il est recommandé d'identifier les équipements obsolètes, notamment d'ancienne génération, qui ne permettent pas techniquement de réaliser le cloisonnement proposé à la recommandation R106-, puis de mener une analyse spécifique pour étudier

les contre-mesures possibles et définir le cloisonnement approprié et le niveau de risque résiduel.

R108

C2 Cloisonner physiquement le réseau d'administration

Il est recommandé de cloisonner physiquement le réseau d'administration des équipements des autres réseaux.

ZCR 3.2 SR 5.1 SR 5.2 CR 5.1 CR 5.2 NDR 5.2
NDR 5.13 NET 1.1 SP03.02 SP03.03RE1 SP03.07BR

R108 -

C2 Cloisonner par le chiffre le réseau d'administration

Il est recommandé de cloisonner le réseau d'administration des équipements des autres réseaux à l'aide de tunnels VPN (se référer au guide [21]). L'utilisation de produits qualifiés pour l'établissement de ces tunnels est recommandée. Pour de plus amples informations, se reporter au guide d'administration sécurisée [33].

ZCR 3.2 SR 5.1 SR 5.2 CR 5.1 CR 5.2 NDR 5.2
NDR 5.13 NET 1.1 SP03.02 SP03.03RE1 SP03.07BR

R109

C2 Utiliser des flux unidirectionnels entre les systèmes industriels de classe 2 et les systèmes industriels de classe 1

Il est recommandé de mettre en œuvre des flux unidirectionnels entre les systèmes industriels de classe 2 et les systèmes industriels de classe 1 conformément au tableau 3. L'unidirectionnalité des flux peut être assurée par un pare-feu.

R110

C2 Mettre en œuvre des postes d'administration dédiés par classe

Il est recommandé de mettre en œuvre des postes d'administration dédiés à une seule classe. Il faut envisager, au minimum :

- un même poste d'administration pour les équipements de classes 1 et 2 ;
- un poste d'administration pour les équipements de classe 3 ;
- un poste d'administration pour les équipements de classe 4.

ZCR 3.6

R111

C3 Utiliser des flux unidirectionnels entre les systèmes industriels de classe 3 et les systèmes industriels de classes inférieures

Il est recommandé de mettre en œuvre des flux unidirectionnels entre les systèmes industriels de classe 3 et les systèmes industriels de classes inférieures (comme précisé dans le guide méthode de classification [41] et dans le tableau 3). L'unidirectionnalité des flux doit être assurée par une passerelle unidirectionnelle (par exemple un équipement constitué d'un guichet haut et d'un guichet bas pour le transfert de donnée entre deux zones) .

R112

C3 Privilégier un cloisonnement physique entre les automates de sécurité fonctionnelle (SIS) et les automates standards (BPCS)

Il est recommandé de privilégier un cloisonnement physique entre les automates de sécurité fonctionnelle (SIS) et les automates standards (BPCS). Indépendamment de la cybersécurité, le cloisonnement physique participe à renforcer la disponibilité de l'installation industrielle.

SR 5.1 RE3 NET 1.1 SP03.02BR

R112 -

C3 Mettre en place un cloisonnement logique entre les automates de sécurité fonctionnelle (SIS) et les automates standards (BPCS)

Il est recommandé de mettre en place un cloisonnement logique lorsqu'une séparation physique n'est pas possible entre les automates de sécurité fonctionnelle (SIS) et les automates standards (BPCS). L'utilisation des VLAN est un exemple de cloisonnement logique possible.

SR 5.1 RE3 NET 1.1 SP03.02BR

R113

C3 Effectuer un filtrage MAC pour les flux non IP

Il est recommandé d'effectuer un filtrage sur les adresses MAC source et destination, ainsi que sur les protocoles autorisés lorsque des flux non IP doivent transiter entre deux zones distinctes. Compte-tenu du filtrage effectué sur le niveau 2 du modèle OSI, il est important de prévoir des solutions et outillage en cas d'intervention sur mode dégradé de l'installation (adresses MAC des postes et équipement de remplacement intégré dans le filtrage par exemple).

R114

C4 Cloisonner physiquement les systèmes industriels de classe 4 des systèmes de classes inférieures

Il est recommandé de cloisonner physiquement les systèmes industriels de classe 4 des systèmes de classes inférieures. L'utilisation de cloisonnement logique est fortement déconseillée.

R115

C4 Utiliser des flux unidirectionnels entre les systèmes industriels de classe 4 et les systèmes industriels de classes inférieures

Il est recommandé de mettre en œuvre des flux unidirectionnels entre les systèmes industriels de classe 4 et les systèmes industriels de classes inférieures (comme précisé dans le guide méthode de classification [41] et dans le tableau 3). L'unidirectionnalité peut être assurée physiquement par une diode qualifiée par l'ANSSI [16].

SR 5.1 **CR 5.1**

4.2.3 Interconnexion avec le système d'information de gestion

Références

- **TTP :** 2.2.10
- **Guide d'hygiène :** règle n° 42
- **ISO 27002 :** 8.20

R116

C1 Protéger l'interconnexion par un dispositif de filtrage réseau

Il est recommandé de protéger l'interconnexion par un dispositif de filtrage réseau (pare-feu).

SR 5.2 **CR 5.2** **NET 1.1**

16. La liste des produits qualifiés est disponible à l'adresse suivante : https://cyber.gouv.fr/decouvrir-les-solutions-qualifiees.

R116 +

C1 Protéger l'interconnexion par deux dispositifs de filtrage réseau

Il est recommandé de protéger l'interconnexion par deux dispositifs de filtrage réseau (pare-feu), conformément au guide [27].

SR 5.2 CR 5.2 NET 1.1

R117

C1 Limiter les flux au strict nécessaire

Il est recommandé de limiter les flux au strict nécessaire pour l'opérationnel.

SR 7.1 CR 7.1 SP08.04BR

R118

C1 Filtrer les flux avec le système informatique de gestion

Il est recommandé de filtrer les flux avec le système d'informatique de gestion en complément de la recommandation R102.

R119

C2 Autoriser les flux unidirectionnels depuis le système industriel de classe 2 vers le système d'information de gestion

Il est recommandé d'autoriser les flux unidirectionnels depuis le système industriel de classe 2 vers le système d'information de gestion. L'unidirectionnalité des flux doit au minimum être contrôlée par un pare-feu.

SR 5.1 E1 CR 5.1

R120

C3 Autoriser les flux unidirectionnels depuis le système industriel de classe 3 vers le système d'information de gestion

Il est recommandé d'autoriser les flux unidirectionnels depuis le système industriel de classe 3 vers le système d'information de gestion. L'unidirectionnalité des flux doit au minimum être contrôlée par une passerelle unidirectionnelle.

SR 5.1 RE1 CR 5.1

R121

C4 Autoriser les flux unidirectionnels depuis le système industriel de classe 4 vers le système d'information de gestion

Il est recommandé d'autoriser les flux unidirectionnels depuis le système industriel de classe 4 vers le système d'information de gestion. L'unidirectionnalité des flux peut être contrôlée par une diode qualifiée par l'ANSSI.

SR 5.1 RE1 **CR 5.1**

4.2.4 Accès Internet et interconnexions entre sites distants

Références

- **TTP :** 2.2.10
- **Guide d'hygiène :** règles n° 4, n° 24 et n° 42
- **ISO 27002 :** 8.22

R122

C1 Interdire les accès directs vers Internet depuis le système industriel

Il est recommandé d'interdire les accès directs vers Internet depuis le système industriel. En particulier, l'ensemble des postes de supervision et des équipements de terrain ne devraient pas avoir d'accès à Internet.

SR 5.1 RE1

R123

C1 Interdire les accès directs depuis Internet vers le système industriel

Il est recommandé d'interdire réciproquement les accès directs depuis Internet vers le système industriel. Dans le cas d'interconnexion d'une usine 4.0, il est recommandé de se référer à l'article *Approche SSI pour l'Internet des objets industriels* [4].

ZCR 3.2 **SR 5.1** **SR 5.2** **CR 5.1** **CR 5.2** **NDR 5.2**
NDR 5.13 **NET 1.1** **SP03.02** **SP03.03RE1** **SP03.07BR**

R124

C1 Garantir la confidentialité l'intégrité et l'authenticité des flux des interconnexions

Il est recommandé de garantir la confidentialité, l'intégrité et l'authenticité des flux entre des systèmes répartis sur des localisations différentes avec des protocoles configurés à l'état de l'art. On peut utiliser un tunnel VPN IPsec par exemple [21].

SR 3.1 | CR 3.1 | NET 3.2 | SP07.02BR | SP07.03BR | SP07.04

R125

C1 Déployer un pare-feu au niveau des passerelles d'interconnexion

Il est recommandé de déployer un pare-feu au niveau des passerelles d'interconnexion conformément au guide de l'ANSSI [27].

ZCR 3.2 | SR 5.1 | SR 5.2 | CR 5.1 | CR 5.2 | CM 1.2
NET 1.1 | SP03.02 | SP03.03RE1 | SP03.07BR

R126

C3 Disposer d'équipements certifiés pour l'interconnexion

Il est recommandé de s'assurer que les équipements utilisés pour l'interconnexion disposent d'un certificat de sécurité de premier niveau (CSPN) de l'ANSSI [17] ou équivalent (par exemple Critère Commun intégrant AVA_VAN.3).

R127

C3 Déployer un pare-feu distinct du concentrateur VPN pour les interconnexions

Il est recommandé de déployer un pare-feu distinct du concentrateur VPN au niveau des passerelles d'interconnexion, conformément au guide de l'ANSSI [27].

ZCR 3.2 | SR 5.1 | SR 5.2 | CR 5.1 | CR 5.2 | CM 1.2
NET 1.1 | SP03.02 | SP03.03RE1 | SP03.07BR

R128

C4 Disposer d'équipements qualifiés pour l'interconnexion

Il est recommandé de s'assurer que les équipements utilisés pour l'interconnexion disposent d'une qualification de l'ANSSI [18].

17. La liste des produits certifiés est disponible à l'adresse suivante : `https://cyber.gouv.fr/produits-certifies`.

4.2.5 Accès distants

Références

- **TTP :** 2.2.10
- **Guide d'hygiène :** règles n° 18, n° 32 et n° 42
- **ISO 27002 :** 8.16 et 8.22

4.2.5.1 Télédiagnostic, télémaintenance et télégestion

Le télédiagnostic est l'action d'effectuer, à distance (c'est-à-dire depuis l'extérieur des bâtiments dans lesquels se trouve le système industriel), un diagnostic de l'installation technique en passant potentiellement par des réseaux non-maîtrisés. Cela n'inclut pas de modification de paramétrage.

La télémaintenance est l'action d'effectuer, à distance (c'est-à-dire depuis l'extérieur des bâtiments dans lesquels se trouve le système industriel), des tâches de maintenance sur une installation technique en passant potentiellement par des réseaux non maîtrisés. Cela implique de pouvoir faire des modifications de paramètres, voire de programmes.

La télégestion consiste à prendre le contrôle à distance du système industriel (supervision et modification de paramétrage). Si la télégestion est utilisée, les équipements utilisés pour cet usage doivent être intégrés au périmètre du système industriel. L'ensemble des mesures de sécurité doivent donc également s'appliquer à l'ensemble du système.

R129

C1 Sécuriser les opérations de télédiagnostic et de télémaintenance

Il est recommandé d'appliquer les règles suivantes lorsque des opérations de télédiagnostic, de télémaintenance ou de télégestion sont nécessaires :

- établir les connexions à la demande pour une durée définie (par exemple 4h) ;
- authentifier l'équipement de connexion distant ;
- disposer d'un mot de passe robuste (conformément au chapitre 4.1.2) ;
- activer la journalisation des authentifications ;
- fermer la connexion après un délai d'inactivité fixé en respectant les contraintes opérationnelles ;
- cloisonner l'équipement accédé et autoriser uniquement les flux requis entre l'équipement et le reste du système industriel ;
- réaliser les opérations de télémaintenance à partir de protocoles sécurisés assurant notamment l'intégrité et l'authenticité des échanges (conformément au guide d'administration sécurisée [33]).

SR 3.1 | CR 3.1 | NET 3.2 | SP07.02BR | SP07.03BR | SP07.04

R130

C2 Appliquer des règles de sécurisation pour la solution de télémaintenance

Il est recommandé de suivre les règles suivantes pour la solution de télémaintenance :

- la solution doit assurer la confidentialité, l'intégrité et l'authenticité des communications (par exemple avec un tunnel VPN IPsec) avec des protocoles configurés à l'état de l'art ;
- mettre en œuvre une authentification multifacteur ;
- cloisonner les équipements de connexion du reste du système industriel et autoriser uniquement les flux indispensables à la télémaintenance ;
- activer la journalisation des événements de sécurité.

SR 1.1 | SR 1.5 | SR 3.1 | CR 1.1 | CR 1.5 | CR 3.1

USER 1.9 | NET 3.2 | SP07.02BR | SP07.03BR | SP07.04 | SP03.07RE1

R131

C3 Déployer une sonde de détection au niveau de la passerelle de connexion

Il est recommandé de déployer une sonde de détection au niveau de la passerelle de connexion pour pouvoir analyser l'ensemble du trafic entrant et sortant (conformément à la recommandation R211).

SR 6.2 | CR 6.2 | EVENT 1.1 | SP08.01BR | SP08.03BR

R132

C4 Mettre en œuvre si besoin une solution de télédiagnostic

Il est recommandé de mettre en œuvre (si besoin) uniquement des solutions de télédiagnostic. Dans ce cas, la solution doit intégrer les mesures suivantes (conformément au chapitre 4.2.1) :

- la connexion distante est réalisée sur un serveur cloisonné ;
- les données nécessaires au télédiagnostic sont transférées sur ce serveur au travers d'une diode. Cette diode doit être qualifiée par l'ANSSI.

R133

C4 Proscrire la télémaintenance

La télémaintenance n'est pas recommandée. Si des opérations de télémaintenance sont impérativement nécessaires, les équipements distants et la liaison doivent être intégrés au périmètre du système de classe 4. L'ensemble des mesures de classe 4 doivent leur être appliquées, et en particulier celles de la section 4.2.6 et celles du guide d'administration sécurisée [33].

4.2.6 Systèmes industriels distribués

Un système industriel distribué désigne un ensemble d'actifs matériels et logiciels interconnectés qui agissent comme une entité unifiée pour exécuter des fonctions d'automatisation ou de contrôle industriel tout en étant géographiquement répartis.

R134

C1 Utiliser des protocoles sécurisés pour les flux transitant par des réseaux non protégés physiquement

Il est recommandé d'utiliser des protocoles sécurisés sur l'ensemble des flux transitant par des réseaux non protégés physiquement (accessibles dans un lieu public) ou non maîtrisés. Ils doivent être au minimum protégés en intégrité et authentifiés.

SR 3.1 **SR 4.1** **CR 3.1** **CR 4.1** **DATA 1.2**

R135

C1 Déployer des concentrateurs VPN aux extrémités des liaisons

Il est recommandé de déployer des concentrateurs VPN aux extrémités des liaisons pour protéger l'intégralité du trafic entre les deux extrémités.

NET 3.2 **SP07.02BR** **SP07.03BR** **SP07.04**

R136

C2 Privilégier des liaisons maîtrisées

Pour la communication entre sites distants, il est recommandé de privilégier des liaisons maîtrisées, par opposition à un raccordement au travers d'Internet ou d'un réseau opérateur. Cela a pour but de limiter l'exposition des systèmes aux acteurs malveillants.

R137

C3 Disposer de concentrateurs VPN certifiées

Il est recommandé de s'assurer que les équipements utilisés dans la recommandation R138 disposent d'un certificat de sécurité de premier niveau (CSPN) de l'ANSSI [19] ou équivalent (par exemple Critère Commun intégrant AVA_VAN.3).

19. La liste des produits certifiés est disponible à l'adresse suivante : `https://cyber.gouv.fr/produits-certifies`.

R138

C3 Déployer des concentrateurs VPN et un pare-feu aux extrémités des liaisons

Il est recommandé de déployer des concentrateurs VPN aux extrémités des liaisons pour protéger l'intégralité du trafic. L'équipement doit alors être positionné derrière un pare-feu ne laissant passer que les flux strictement indispensables.

NET 3.2 **SP07.02BR** **SP07.03BR** **SP07.04**

R139

C3 Déployer des sondes de détection au niveau des passerelles d'interconnexion

Il est recommandé de déployer des sondes de détection au niveau des passerelles d'interconnexion pour pouvoir analyser l'ensemble du trafic circulant entre les sites (conformément à la recommandation R211).

SR 6.2 **CR 6.2** **EVENT 1.1** **SP08.01BR** **SP08.03BR**

R140

C3 Proscrire l'utilisation de liaisons inter-sites sur des réseaux publics

L'utilisation de réseau public pour réaliser des communications inter-sites est proscrite.

R141

C4 Disposer de concentrateurs VPN qualifiés

Il est recommandé de s'assurer que les équipements utilisés dans la recommandation R138 disposent d'une qualification de l'ANSSI [20].

4.2.7 Communications sans-fil

Références

- **TTP :** 2.2.8
- **Guide d'hygiène :** règles n° 7 et n° 20
- **ISO 27002 :** 8.1 et 8.22

Dans certains cas, l'utilisation de réseaux sans-fil (par exemple, Wi-Fi, 4G/5G et LoRaWAN) peut être une solution de secours à l'utilisation des réseaux publics ou privés filaires.

20. La liste des produits qualifiés est disponible à l'adresse suivante : https://cyber.gouv.fr/produits-services-qualifies.

L'utilisation d'un réseau sans fil implique la perte de protection physique et facilite l'intrusion d'un tiers sur le réseau. La sécurité repose ainsi sur la qualité cryptographique du protocole sous-jacent. D'autre part, la disponibilité du réseau-sans fil peut être dégradée par l'emploi d'équipements de brouillage radio.

R142

C1 Limiter l'usage de technologies sans-fil au strict nécessaire

Il est recommandé de limiter l'usage de technologies sans-fil au strict nécessaire.

SR 2.2 RE1 **CR 2.2** **NET 2.2** **SP04.02**

R143

C2 Consulter régulièrement les événements générés par les équipements sans-fil

Il est recommandé de consulter régulièrement les événements générés par les équipements sans-fil lorsque les événements de sécurité ne sont pas supervisés par un dispositif centralisé. Les événements peuvent être par exemple des connexions d'équipements, le brouillage radio (par exemple, des déconnexions d'équipements et une variation de la qualité du signal).

R144

C3 Éviter d'utiliser des technologies sans-fil

Il est recommandé de ne pas utiliser des technologies sans-fil, et d'en limiter l'usage aux situations où il n'existe pas d'autre solution de communication.

R145

C3 Sélectionner une technologie permettant de sécuriser les données sur le réseau sans-fil

Dans le cas d'utilisation de réseau sans-fil, il est recommandé de sélectionner une technologie permettant la protection en intégrité et en authenticité des données, conformément aux recommandations de l'ANSSI [30].

SR 3.1 **SR 4.1** **CR 3.1** **CR 4.1** **DATA 1.2** **SP03.08RE2** **SP03.10**

Information

Dans le cas d'utilisation de réseaux sans-fil, les recommandations R146 à R149 doivent être appliquées.

R146

C3 Activer des fonctions de sécurité pour les points d'accès sans-fil

Il est recommandé de mettre en œuvre les mécanismes suivants pour les points d'accès sans-fil :

- l'authentification du point d'accès et du dispositif qui se connecte à l'infrastructure ;
- les fonctionnalités de contrôle d'accès au réseau (par exemple EAP-TLS), conformément au guide relatif au déploiement du protocole 802.1X pour le contrôle d'accès à des réseaux locaux [12] ;
- la journalisation des connexions.

SR 1.13 **SR 1.6** **SR 2.2 RE1** **CR 1.6** **CR 2.2** **NDR 1.6** **NDR 1.13**

R147

C3 Cloisonner les périphériques sans-fil dans un réseau séparé

Il est recommandé de cloisonner au maximum les communications sans fil en isolant les périphériques sans fil dans un réseau physique ou logique séparé.

SR 1.6 **SR 2.2 RE1** **CR 1.13** **CR 2.2** **CR 5.1** **NDR 1.13** **NET 2.2** **SP04.02BR**

R148

C3 Réduire autant que possible la puissance des émissions

Il est recommandé de réduire autant que possible la portée des communications en diminuant la puissance d'émission.

CR 2.2 **CR 3.1**

Attention

Même avec une puissance réduite, il est possible de capter des émissions d'un réseau sans-fil à grande distance en utilisant des dispositifs adaptés.

R149

C3 Déployer une sonde de détection entre le réseau sans-fil et les autres réseaux

Il est recommandé de déployer une sonde de détection d'intrusion au niveau de l'interconnexion entre le réseau sans-fil et les autres réseaux du système industriel afin de détecter un accès non autorisé depuis le réseau sans-fil.

SR 6.2 **CR 6.2** **EVENT 1.1** **SP08.01BR** **SP08.03BR**

R150

C3 Proscrire l'utilisation de technologie sans-fil pour les liaisons ayant des besoins critiques de disponibilité

Il est recommandé de proscrire l'utilisation de technologie sans-fil pour toutes les liaisons ayant des besoins critiques de disponibilité.

R151

C3 Superviser les événements de sécurité générés par les équipements sans-fil

Il est recommandé de centraliser et de superviser en temps réel les événements de sécurité générés par les équipements sans-fil.

SR 2.8 RE1 **CR 2.8** **EVENT 1.6** **SP08.02RE1**

R152

C4 Sécuriser les protocoles applicatifs transitant par un réseau sans-fil

Si le protocole radio ne permet pas de garantir un niveau de sécurité satisfaisant, il est recommandé d'utiliser un protocole applicatif sécurisé supplémentaire, conformément à la section 4.2.8.

4.2.8 Sécurité des protocoles

Références

- **TTP :** 2.2.7
- **Guide d'hygiène :** règle n° 21
- **ISO 27002 :** 8.7

R153

C1 Désactiver les protocoles non sécurisés

Il est recommandé de désactiver les protocoles IT non sécurisés (http, telnet, ftp, SNMPv1 et v2, etc.) au profit de protocoles plus sécurisés (https, ssh, sftp, SNMPv3 etc.) pour assurer l'intégrité, la confidentialité, l'authenticité et l'absence de rejeu des flux.

SR 7.7 **CR 7.7** **COMP 1.1** **SP02.03** **SP03.05**

Attention

Certains protocoles disposent de mécanismes de vérification d'intégrité des données reposant sur des CRC (contrôle de redondance cyclique ou *cyclic redundancy check*). Cette mesure, efficace en sûreté de fonctionnement, ne constitue pas une protection face à des attaques dans le domaine de la cybersécurité.

R154

C3 Mettre en œuvre des mesures compensatoires pour les protocoles ne pouvant être sécurisés

Pour les protocoles ne disposant pas de sécurité intrinsèque (protocoles d'administration propriétaires, protocoles de sécurité fonctionnelle ou protocoles d'exploitation tels que Modbus, S7comm, BACnet, EIP/CIP, etc.), il est recommandé de :

- mettre en œuvre une sécurisation au moyen d'un tunnel VPN (se reporter aux guides de l'ANSSI [26], [21] et [32]) pour en assurer l'intégrité et l'authenticité ;
- mettre en place des mesures de filtrage applicatif. Ce filtrage doit permettre de limiter l'usage de commandes non souhaitées supportées par des protocoles non sécurisés. Seules les fonctions strictement utiles doivent être acceptées.

SR 5.2 **CR 5.2** **NET 1.1** **NET 3.2** **SP07.02BR** **SP07.03BR** **SP07.04**

Information

Si les flux transitent par des réseaux non maîtrisés, le chiffrement est nécessaire (se référer à la recommandation R134). En revanche, sur un réseau maîtrisé, le chiffrement n'est pas toujours souhaitable car incompatible avec l'utilisation de système de détection. L'intégrité et l'authenticité des données sont suffisantes.
L'absence de chiffrement ne doit pas être incompatible avec la recommandation R95.

R155

C3 Privilégier l'usage de protocoles sécurisés et interopérables

Il est recommandé de privilégier l'usage de technologies standardisées, sécurisées et interopérables (par exemple OPC UA [21]).

4.3 Sécurisation des équipements

4.3.1 Durcissement des configurations

Références

- **TTP :** 2.2.7
- **Guide d'hygiène :** règle n° 42
- **ISO 27002 :** 8.7 et 8.19

4.3.1.1 Réduction de la surface d'attaque

R156

C1 Désactiver certains composants sur les équipements

Il est recommandé de désactiver sur les équipements :

- les comptes par défaut ;
- les ports physiques inutilisés (ports USB, réseau, etc.) ;
- les accès aux supports amovibles, s'ils ne sont pas utilisés ;
- les services non indispensables (serveur WEB par exemple).

SR 7.7 **CR 7.7** **COMP 1.1** **SD-4** **SP02.03** **SP03.05**

R157

C1 Supprimer ou désactiver les fonctions de développement

Il est recommandé de supprimer ou, au minimum, désactiver sur les postes de travail, ordinateurs portables et serveurs :

- les outils de débogage et de développement des systèmes en production ;
- les données et fonctions de test, ainsi que les comptes associés ;
- l'ensemble des programmes non indispensables.

SR 7.7 **CR 7.7**

21. Se reporter aux spécifications OPC UA disponibles sur le site de la fondation OPC UA (`https://opcfoundation.org/`) et au standard [54].

Information

Des lecteurs PDF et des logiciels de bureautique sont parfois installés sur des stations de supervision SCADA afin de pouvoir consulter des documents (procédure ou manuel de maintenance par exemple). Il est préférable de mettre à disposition des utilisateurs d'autres postes que les stations de supervision SCADA pour utiliser les applications de bureautique, dont les lecteurs PDF (cf. R38).

R158

C1 Désactiver les fonctions de débogage

Il est recommandé de désactiver, sur les applications de supervision SCADA, les fonctions de débogage (des intégrateurs et des équipementiers) et de ne pas charger les mnémoniques et commentaires dans les équipements.

SR 7.7 | CR 7.7 | EDR 2.13 | SD-4

4.3.1.2 Renforcement des protections

R159

C1 Durcir les systèmes d'exploitation et les équipements réseau

Il est recommandé d'appliquer des mesures de durcissement des systèmes d'exploitation et des équipements réseau suivantes :

- Pour les routeurs et les commutateurs, il est possible de s'appuyer sur les recommandations données dans les guides ANSSI [10], [13] et [14]. **Il est important d'appliquer ces recommandations, notamment la mise en œuvre de durcissement comme les règles d'administration sécurisées des commutateurs et pare-feux (par exemple, restriction d'adresses IP).**
- Le guide ANSSI [15] fournit des recommandations concernant la configuration matérielle et logicielle d'un environnement Linux afin d'obtenir un système d'exploitation sûr.
- Une note technique concernant la mise en œuvre de restrictions logicielles sous Windows [11] ainsi que des Essentiels relatifs à la mise en œuvre sécurisée de serveurs Windows [42] sont disponibles sur le site de l'ANSSI.

R160

C1 Limiter les privilèges d'exécution des applications

Il est recommandé d'exécuter les applications avec les privilèges strictement nécessaires à leur fonctionnement.

SR 1.1 | SR 1.2 | SR 2.1 RE1 | USER 1.5 | SP03.08BR

21. https://cyber.gouv.fr/windows-restrictions-logicielles/

R161

C2 Concevoir une liste des applications autorisées

Il est recommandé de mettre en œuvre une liste des applications autorisées ayant le droit de s'exécuter sur les équipements.

SR 3.2 SR 5.2 COMP 2.2 SD-4 SG-3 SP10.03 SP10.04

R162

C2 Activer les mécanismes de sécurité de l'automate

En plus de la réduction de la surface d'attaque (comme présentée au travers des recommandations R156 et R153) et lorsque les équipements le permettent, il est recommandé d'utiliser les mécanismes suivants pour les automates :

- la protection (par authentification) d'accès à la CPU et aux blocs de programme ;
- la protection (par authentification) de la mise à jour de l'équipement ;
- la restriction des adresses IP pouvant se connecter ;
- la fermeture des ports réseau non utilisés ;
- la désactivation du mode de programmation à distance.

NDR 1.13

R163

C3 Disposer d'un automate certifié

Il est recommandé de s'assurer que les automates utilisés disposent d'une certification de sécurité de premier niveau (CSPN)[22] ou équivalent (par exemple Critère Commun intégrant AVA_VAN.3).

R164

C4 Disposer d'un automate qualifié

Il est recommandé de s'assurer que les automates utilisés disposent d'une qualification de sécurité délivrée par l'ANSSI[23].

Attention

Un dispositif de protection antivirale peut ne pas être adapté à certains systèmes industriels pour les raisons suivantes :

22. La liste des produits certifiés est disponible à l'adresse suivante : https://cyber.gouv.fr/produits-certifies.
23. La liste des produits qualifiés est disponible à l'adresse suivante : https://cyber.gouv.fr/decouvrir-les-solutions-qualifiees.

- les mécanismes de mise à jour des signatures peuvent apporter des vulnérabilités et nécessiter des connexions vers des systèmes d'information externes qui n'existaient pas jusqu'alors ;
- un dispositif de protection antivirale peut être incompatible avec les principes et exigences de sûreté de fonctionnement.

L'installation d'un antivirus ou d'un EDR doit être réalisée sur un poste ou un serveur dédié, comme indiqué dans les recommandations R176 et R179, mais elle n'est pas recommandée pour les autres composants du système industriel. Le durcissement des configurations, comme indiqué dans les recommandations R153, R156, R161 et R162, doit être privilégié.

4.3.1.3 Intégrité et authenticité

R165

C1 Intégrer au processus de livraison logicielle un mécanisme de vérification de l'intégrité et de l'authenticité

Il est recommandé d'intégrer au processus de livraison de l'ensemble des logiciels, programmes et éléments de configuration (ainsi que de leurs mises à jour) un mécanisme de vérification de l'intégrité et de l'authenticité (par exemple, une signature). Les éléments concernés sont :

- les micrologiciels (*firmware*) ;
- les systèmes d'exploitation et logiciels standards ;
- les logiciels et applications de supervision SCADA ;
- les logiciels de programmation des différents constituants ;
- les programmes d'automates ;
- les fichiers de configuration des équipements réseau.

SR 3.4 **CR 3.4** **EDR 3.10** **HDR 3.10** **NDR 3.10** **SM-6** **SUM-1**

R166

C3 Vérifier régulièrement l'intégrité des logiciels et programmes

Il est recommandé de vérifier régulièrement l'intégrité des micrologiciels (*firmware*), logiciels et programmes applicatifs (par exemple : logiciel d'ingénierie, programme automate, SCADA). Cette tâche doit être automatisée et journalisée. Par exemple, pour vérifier l'intégrité d'un automate, il est recommandé de :

- intégrer un compteur permettant de définir la durée d'un cycle du procédé industriel et de vérifier s'il n'y a pas une déviation du temps de réalisation ;

- ajouter un bloc de programme permettant de surveiller le temps de cycle de l'automate ;
- vérifier l'espace mémoire utilisé par l'automate.

SR 3.6 CR 3.6 SI-2

R167

C3 Vérifier le condensat et la signature du logiciel de l'équipement

Il est recommandé de vérifier l'intégrité et l'authenticité d'un logiciel (voir la recommandation R166) :

- le condensat doit être vérifié par l'entité responsable lors de la réception du logiciel (comparaison du condensat réel avec celui transmis par le fournisseur) ;
- la signature du logiciel doit être vérifiée par l'équipement avant son exécution.

4.3.2 Gestion des vulnérabilités

Références

- **TTP :** 2.2.1
- **Guide d'hygiène :** règle n° 34
- **ISO 27002 :** 8.8

R168

C1 Disposer d'un processus de gestion des vulnérabilités

Il est recommandé de disposer d'un processus de gestion des vulnérabilités afin de :

- rechercher les correctifs de sécurité disponibles correspondant aux matériels et logiciels utilisés ;
- identifier les vulnérabilités connues et mesurer leurs impacts sur les systèmes ;
- déployer les correctifs en commençant par les plus critiques (selon l'analyse de risque associée) ;
- recenser les vulnérabilités qui n'ont pas pu être corrigées (soit par manque de correctifs, soit parce que le correctif n'a pas pu être appliqué en raison de contraintes opérationnelles) pour acceptation du risque et traitement si un correctif est publié.

COMP 3.3 EVENT 1.9 ORG 2.2 SVV-3 SP02.02 SP03.03BR SP11.06

Information

Il est important de s'assurer de la compatibilité des correctifs avec le fonctionnement des applications (en effectuant des essais sur une installation représentative de ce qui est installé sur site par exemple). Le déploiement des correctifs doit être intégré dans les plans de maintenance des systèmes. Les correctifs peuvent être appliqués lors de maintenances programmées ou lorsque le système est à l'arrêt. Les correctifs concernent également les automates et les équipements de terrain comme les capteurs et actionneurs intelligents.

R169

C1 Appliquer les correctifs de sécurité en priorité sur les équipements les plus exposés

Il est recommandé d'appliquer les correctifs de sécurité en priorité sur les équipements les plus exposés à des menaces (par exemple, un attaquant depuis le réseau de gestion, un utilisateur malveillant accédant à un poste de travail).

R170

C2 Identifier les vulnérabilités non corrigées

Il est recommandé d'identifier de façon exhaustive les vulnérabilités non corrigées (soit par manque de correctifs, soit parce que le correctif n'a pas pu être appliqué en raison de contraintes opérationnelles). Dans le cas de vulnérabilité ne disposant d'aucun correctif applicable, cet élément doit apparaître dans l'analyse de risque afin de mettre en œuvre des mesures compensatoires adéquates ou de l'accepter au regard des risques résiduels.

COMP 3.5 ORG 2.2 DM-4 SP11.02RE2

R171

C2 Faire valider les correctifs de sécurité

Il est recommandé de faire valider les correctifs de sécurité par les fournisseurs d'application industrielle avant leur déploiement afin d'éviter les régressions fonctionnelles.

R172

C3 Vérifier l'application effective des correctifs de sécurité

Il est recommandé de vérifier l'application effective des correctifs de sécurité (s'assurer par exemple de la prise en compte de la version dans les logiciels ou équipements comme les automates). Cette vérification peut constituer un indicateur de suivi de la cybersécurité du système industriel.

COMP 3.3 SP11.01RE1 SP11.06RE3

R173

C4 Mettre en œuvre un environnement de test représentatif

Il est recommandé de mettre en œuvre un environnement de test représentatif des systèmes en production afin de s'assurer de l'absence de régression de ceux-ci après l'application des correctifs ou de mises à jour avant leur déploiement généralisé.

SUM-1

Information

L'application de correctif de sécurité, comme tout autre modification de l'installation, peut nécessiter une nouvelle qualification de l'installation industrielle d'un point de vue sûreté de fonctionnement.

4.3.3 Interfaces de connexion

Références

- **TTP :** 2.2.4
- **Guide d'hygiène :** règles n° 15 et n° 26
- **ISO 27002 :** 7.10 et 8.20

4.3.3.1 Gestion des médias amovibles

R174

C1 Limiter l'usage des médias amovibles

Il est recommandé de définir une politique d'utilisation des médias amovibles et d'en limiter l'usage au strict minimum.

SR 2.1 COMP 1.2 SP10.05RE1

R175

C1 Mettre à disposition des intervenants des médias amovibles dédiés

Il est recommandé de mettre à disposition des intervenants des médias amovibles dédiés aux systèmes industriels et dont l'utilisation pour tout autre usage est proscrite. Réciproquement, l'utilisation de tout autre média amovible non identifié comme spécifique aux systèmes industriels est fortement déconseillée.

ZCR 3.4 COMP 1.2 SP10.05RE1

R176

C2 Utiliser une station de décontamination

Il est recommandé d'utiliser une station de décontamination afin de rechercher les codes malveillants, et décontaminer le cas échéant, tous les périphériques amovibles avant de les connecter sur les équipements du système industriel.

R177

C2 Interdire la connexion des périphériques amovibles non vérifiés

Il est recommandé d'interdire aux intervenants la connexion des périphériques amovibles non vérifiés par la station de décontamination.

R178

C2 Désactiver les ports de médias amovibles

Il est recommandé de désactiver les ports de médias amovibles lorsque leur utilisation n'est pas nécessaire. Si le blocage physique n'est pas possible, il est recommandé de désactiver logiquement le port.
Par exemple, les mesures suivantes sont envisageables :

- le blocage des ports USB à l'aide de mécanismes de sécurité physiques ou logiques, comme les verrous USB physiques (avec clés), via un logiciel de sécurité capable de bloquer l'utilisation de clés USB et autres périphériques, ou à travers la configuration UEFI au démarrage du poste ;
- le retrait ou la déconnexion physique des lecteurs de médias amovibles.

SR 7.7 **CR 7.7** **COMP 1.1** **SD-4** **SP02.03** **SP03.05**

R179

C3 Utiliser un sas ou une station blanche pour échanger des données avec un média amovible

Il est recommandé d'utiliser un sas ou une station blanche pour échanger des données entre un média amovible et certains composants du système industriel. Ce sas ou cette station blanche doit respecter les exigences décrites dans le profil de fonctionnalités et de sécurité de l'ANSSI [49]. Cet échange de données est une action ponctuelle qui doit être encadrée par une procédure.

R180

C3 Disposer d'un Visa de sécurité pour le sas ou la station blanche

Il est recommandé de s'assurer que les équipements de type sas ou station blanche disposent d'un Visa de sécurité de l'ANSSI (certification ou qualification).

4.3.3.2 Gestion des points d'accès réseau

R181

C1 Identifier et recenser les points d'accès réseau

Il est recommandé d'identifier et de recenser les points d'accès réseau conformément à la recommandation R6.

R182

C1 Désactiver les ports des points d'accès réseau non utilisés

Il est recommandé de désactiver les ports des points d'accès réseau non utilisés (par exemple, commutateurs, routeurs, automates, prises de maintenance sur les bus de terrain) conformément aux guides ANSSI [10], [13] et [14].

COMP 1.1 **SP02.03** **SP03.05** **SP03.10RE4**

R183

C2 Intégrer les alertes de connexion/déconnexion au réseau

Il est recommandé de remonter et de traiter les alertes en cas de tentatives de connexion et de déconnexion sur des ports réseau.

SR 6.2 **CR 6.2** **EVENT 1.3** **SP08.01RE1** **SP08.02RE1** **SP08.03RE1**

R184

C2 Rendre accessibles les points d'accès réseau uniquement dans des locaux maîtrisés

Il est recommandé de rendre accessibles les points d'accès réseau uniquement dans des locaux maîtrisés (sous contrôle d'accès).

ZCR 1.1 **ORG 3.1**

4.3.4 Équipements mobiles

Références

- **TTP :** 2.2.11
- **Guide d'hygiène :** règles n° 31
- **ISO 27002 :** 7.9

R185

C1 Durcir le poste nomade

Conformément au guide sur le nomadisme numérique [36], il est recommandé de mettre en œuvre, pour les postes nomades, les éléments de durcissement suivants :

- les mesures de la recommandation R159 ;
- l'utilisation d'une solution de chiffrement de disque ;
- la mise en place d'une politique des supports amovibles, en refusant par exemple l'exécution de code directement depuis le support ;
- l'emploi d'un filtre de confidentialité.

SR 3.1 SR 4.1 CR 3.1 CR 4.1 EDR 3.14 HDR 3.14 NDR 3.14 DATA 1.1 DATA 1.2 SP03.08RE2 SP03.10

Information

Conformément au guide sur le nomadisme numérique [36], il est recommandé de chiffrer le disque dur du poste nomade avec des mécanismes cryptographiques robustes, et donc conforme au référentiel général de sécurité (RGS) annexes B1 [46] et B2 [45].

R186

C1 Proscrire le raccordement de périphériques personnels

Conformément au guide sur le nomadisme numérique [36], il est recommandé de proscrire le raccordement au système industriel de périphériques personnels quels qu'ils soient (par exemple, smartphones, tablettes, clés USB, appareils photos).

SR 2.3 SR 5.3

R187

C1 Concevoir une charte d'utilisation des postes nomades

Il est recommandé de mettre en œuvre une charte d'utilisation des postes nomades.

COMP 1.2 SP10.05RE1

R188

C1 Identifier et valider les équipements autorisés à se connecter aux installations

Il est recommandé d'identifier et de valider (au travers par exemple d'une procédure de tests) les équipements autorisés à se connecter aux installations.

CR 1.2 NET 1.7

R189

C2 Dédier les équipements mobiles au système industriel

Les équipements mobiles connectés au système industriel doivent être dédiés à cet usage (et ne pas être déplacés hors du site), y compris ceux utilisés par des prestataires extérieurs.

ZCR 3.2 COMP 1.2 SP10.05RE1

4.3.5 Sécurité des stations d'ingénierie et des postes d'administration

Références

- **TTP :** 2.2.20
- **Guide d'hygiène :** règles n° 27, n° 28 et n° 29
- **ISO 27002 :** 7.9

Les stations d'ingénierie regroupent au moins deux fonctionnalités :

- la programmation du procédé industriel ;
- la maintenance des équipements industriels (par exemple, automates, SCADA, RTU).

Lorsque la station d'ingénierie est utilisée en tant que console de programmation, il s'agit généralement de postes de travail fixes. Les stations d'ingénierie utilisées en tant que poste de maintenance sont généralement des équipements mobiles. Dans les deux cas, il s'agit de postes dédiés à l'ingénierie des processus du système industriel.

Pour les mesures techniques sur le cloisonnement des fonctions d'administration, on pourra se reporter à la section 4.2.2.

R190

C1 Respecter les règles relatives à la fonction de console de programmation

Il est recommandé de respecter les règles suivantes relatives à la fonction de console de programmation :

- dédier le poste aux activités de développement ;
- ne pas connecter le poste à Internet (les mises à jour doivent être effectuées hors ligne) ;
- ne pas connecter le poste à d'autres systèmes que le système industriel ;
- installer le poste dans des locaux maîtrisés (sous contrôle d'accès) ;
- appliquer les règles de durcissement de configuration et de renforcement des protections (voir la section 4.3.1) ;
- éteindre le poste lorsqu'il n'est pas utilisé ;
- identifier toutes les consoles de programmation pouvant être raccordées au réseau industriel et appliquer sur le réseau les règles de filtrage associées (voir la recommandation R102) ;
- identifier physiquement le poste (marquage visuel par exemple).

ZCR 3.2

R191

C1 Respecter les exigences relatives à la fonction de poste de maintenance

Il est recommandé de respecter les règles relatives à la fonction de poste de maintenance suivantes :

- dédier le poste aux activités de maintenance ;
- ne pas connecter le poste à Internet (les mises à jour doivent être effectuées hors ligne) ;
- appliquer les règles pour les équipements mobiles du guide (voir la section 4.3.4) ;
- stocker le poste dans un local sécurisé ;
- ne pas utiliser le poste d'un prestataire et lui fournir un poste dédié ;
- appliquer les règles de durcissement de configuration et de renforcement des protections (voir la section 4.3.1) ;
- identifier tous les postes de maintenance pouvant être raccordés au réseau industriel et appliquer sur le réseau les règles de filtrage associées (voir la recommandation R102) ;
- identifier physiquement le poste (marquage visuel par exemple).

ZCR 3.2

R192

C1 Ne pas installer d'outils de développement sur les postes et serveurs de production

Il est recommandé de ne pas installer ou de supprimer les outils de développement sur les postes et serveurs de production. Seuls les environnements d'exécution (*run-time*) doivent être installés sur les serveurs et stations SCADA par exemple.

SR 7.7 SP03.05

Information

La recommandation R192 peut être difficile à appliquer dans le cas de l'utilisation de SNCC. Il conviendra alors d'étudier des solutions compensatoires pour isoler le système et réduire sa surface d'attaque.

R193

C2 Respecter les exigences relatives au poste d'administration

Les stations d'ingénierie étant considérées comme des postes d'administration, il est recommandé d'appliquer les recommandations afférentes issues du guide relatif à l'administration sécurisée des SI [33].

SR 7.7 CR 7.7 COMP 1.1 USER 2.2 SP02.03 SP03.05 SP03.08BR SP09.01

4.3.6 Développement sécurisé

Références

- **TTP :** 2.2.19
- **Guide d'hygiène :** néant
- **ISO 27002 :** 8.25, 8.27, 8.28 et 8.29

R194

C1 Appliquer des règles de développement sécurisé

Il est recommandé d'appliquer des règles de développement sécurisé comme précisé dans les Essentiels de l'ANSSI sur le DevSecOps [38].

SR 3.6 | CR 3.6 | SI-2 | SVV-3.5 | SVV-3.6

R195

C2 Dédier un environnement de développement au système industriel

Il est recommandé de dédier un environnement de développement (configuration et programmation des automates par exemple) au système industriel.

SM-7

Information

L'environnement de développement peut être interne ou chez des éditeurs, équipementiers ou intégrateurs. Dans ce cas, il convient d'indiquer les exigences attendues dans le cahier des charges (conformément à la recommandation R33).

R196

C2 Ajouter des contrôles au niveau de la logique fonctionnelle de l'automate

Il est recommandé d'ajouter, au niveau de la logique fonctionnelle de l'automate, les éléments suivants :

- un contrôle des compteurs et des horloges (*timer*) ;
- une vérification de la cohérence des variables du procédé industriel, par exemple le mode de fonctionnement de l'automate (*Start* <> *Stop*) ou la position d'une vanne (ne peut pas être ouverte et fermée en même temps) ;
- la limitation d'une plage de fonctionnement ou l'ajout d'un contrôle croisé avec différents points de mesures installés sur site.

SR 3.5 | SR 3.6 | CR 3.5 | CR 3.6 | SI-1 | SI-2

R197

C2 Programmer la logique de l'automate de façon modulaire

Il est recommandé de programmer la logique de l'automate de façon modulaire et non en un unique bloc de programmation. Cela facilite la détection des nouvelles portions de code non légitimes et potentiellement malveillantes.

SR 3.4 | CR 3.4 | SI-2

R198

C2 Privilégier la mise en œuvre de la logique fonctionnelle dans l'automate

Il est recommandé de privilégier l'implémentation de la logique fonctionnelle dans l'automate plutôt que dans un composant tiers. Par exemple, la vérification qu'une consigne rentre dans des limites autorisées doit être réalisée au niveau de l'automate et non par une IHM. En effet, la programmation d'une IHM dispose d'un contrôle des modifications moins rigoureux que celui d'un automate. D'une part, les modifications au niveau de l'IHM sont plus difficiles à détecter. D'autre part, il est plus facile pour un attaquant de manipuler des éléments calculés au niveau de l'IHM que s'ils sont répartis sur plusieurs automates.

SR 3.6 **CR 3.6** **SI-2** **SVV-1**

R199

C3 Effectuer un audit de code

Il est recommandé d'effectuer un audit de code par une entité indépendante (interne ou externe à l'entreprise). Cet audit peut être réalisé en priorité sur les fonctions critiques de l'installation.

SVV-5

R200

C3 Appliquer et vérifier les règles de bonnes pratiques de programmation

Il est recommandé d'appliquer et de vérifier les règles de bonnes pratiques de programmation. Pour cela, on pourra par exemple utiliser les options avancées de certains compilateurs ou des outils dédiés à la vérification des bonnes pratiques de programmation comme précisé dans les guides de l'ANSSI [28] et [29].

SI-2 **SI-3.5** **SI-3.6**

Information

Certains compilateurs, ateliers de développement de SCADA et d'automates disposent de nombreuses options pour remonter des avertissements supplémentaires à l'utilisateur. Ces options ne sont souvent pas activées par défaut. Elles permettent pourtant d'éviter de nombreuses erreurs de programmation et bogues pouvant induire des vulnérabilités.

Attention

L'application et la vérification des bonnes pratiques de programmation ne permettent pas d'éviter tous les bogues pouvant mener à des vulnérabilités.

R201

C3 Utiliser de manière systématique des outils d'analyse statique

Il est recommandé d'utiliser de manière systématique des outils d'analyse statique et d'effectuer des tests de robustesse.

SI-2 SVV-1 SVV-3.5 SVV-3.6

R202

C3 Vérifier le niveau de sécurité de l'environnement de développement

Il est recommandé de vérifier, par le biais d'un audit, le niveau de sécurité de l'environnement de développement.

4.4 Supervision de sécurité du système industriel

Références

- **TTP :** 2.2.14
- **Guide d'hygiène :** Règles n° 36 et n° 42
- **ISO 27002 :** 8.15 et 8.16

Une collection de guides de l'ANSSI sur la supervision de sécurité décrit les clés de décision nécessaires pour fixer des objectifs de supervision et passer à l'action [7].

Au coeur de la réflexion sur la stratégie de supervision se trouve le lien entre des familles de données de supervision (par exemple, des journaux système, de l'activité réseau) et des points de collecte pertinents (par exemple, en bordure du SI, au sein d'une zone spécifique).

R203

C1 Définir une stratégie de supervision de sécurité

Il est recommandé de définir une stratégie de supervision de sécurité en s'appuyant sur la stratégie de supervision de l'entité et sur la collection de guides de l'ANSSI [7].

R204

C2 Activer les fonctions de journalisation locale

Il est recommandé d'activer les fonctions de journalisation locale, conformément à la stratégie de sécurité établie en R203, si les équipements et logiciels le permettent (se référer aux guides [34] et [43]).

SR 6.1 RE1 CR 6.1 RE1 EVENT 1.6 SP08.02RE1

R205

C2 Définir une politique de gestion des événements

Il est recommandé de définir une politique de gestion des événements (se référer aux guides [34] et [43]), conformément à la stratégie de sécurité établie en R203. Elle doit permettre :

- de déterminer quels sont les événements pertinents à prendre en compte ;
- d'organiser leur stockage (par exemple, volumétrie, durée de conservation) ;
- de définir les conditions d'analyse (en préventif, post-incident) ;
- de définir quels sont les événements qui doivent générer des alertes. L'annexe C fournit une liste d'événements en exemple.

SR 2.8 **SR 2.9** **CR 2.8** **CR 2.9** **EVENT 1.4** **EVENT 1.5**

Information

Les analystes de supervision, majoritairement formés dans des environnements IT, n'ont *a priori* pas la capacité de qualifier un événement de sécurité en environnement OT. Cette capacité est portée par le personnel en charge du système industriel. Il est donc important de mettre en place un processus de qualification des incidents de sécurité OT qui implique ces deux profils.

R206

C2 Journaliser les modifications de paramètres

Il est recommandé, conformément à la stratégie de sécurité établie en R203, de journaliser les éléments suivants :

- les modifications du mode de fonctionnement de l'automate (Start/Stop) ;
- la durée de fonctionnement de l'automate ;
- les modifications des paramètres de capteurs et actionneurs, des fonctions d'asservissement et de régulation.

SR 2.8 RE1 **SP08.03BR**

R207

C2 S'assurer de la conservation des événements de sécurité

Il est recommandé de s'assurer que les événements de sécurité et les journaux sont conservés pour une durée d'au moins trois mois, conformément à la stratégie de sécurité établie en R203.

EVENT 1.4

R208

C3 Mettre en œuvre un système de gestion centralisée

Il est recommandé de mettre en œuvre un système de gestion centralisée et sécurisée des journaux d'événements, conformément à la stratégie de sécurité établie en R203. Pour cela, il est recommandé d'appliquer les recommandations de sécurité pour l'architecture d'un système de journalisation [34].

SR 2.8 RE1 **SR 6.2** **CR 6.2**

R209

C3 Activer les fonctions de journalisation distante

Il est recommandé d'activer les fonctions de journalisation distante (Syslog TLS, SNMPv3, Windows Event, etc.), conformément à la stratégie de sécurité établie en R203, si les équipements et logiciels le permettent (se référer aux guides [34] et [43]).

SR 6.1 RE1 **CR 6.1 RE1** **EVENT 1.6** **SP08.02RE1**

R210

C3 Mettre en œuvre une solution de corrélation des journaux

Il est recommandé de mettre en œuvre une solution de type SIEM (*Security Information and Event Management*) centralisant l'ensemble des journaux d'événements de sécurité, conformément à la stratégie de sécurité établie en R203. Elle doit permettre de corréler les journaux en vue de détecter des incidents de sécurité. La solution de SIEM connectée à un système de classe 4, pour ne pas être considérée de classe 4, doit être placée derrière une diode comme indiqué à la recommandation R115 et dans le tableau 3.

SR 2.8 RE1 **SR 6.2** **CR 6.2**

R211

C3 Mettre en œuvre des moyens de détection d'intrusion

Conformément à la doctrine de détection des systèmes industriels [24], il est recommandé de mettre en œuvre des moyens détection d'intrusion en périphérie des systèmes *ET* sur les points identifiés comme critiques, qui comprennent notamment :

- les interconnexions entre des systèmes distants ;
- les interconnexions des systèmes de télégestion ;
- les interconnexions entre le SI de gestion et le SI industriel ;
- les points de connexion spécifiques vers l'extérieur (Wi-Fi industriel par exemple) ;
- les sas ou stations blanches ;

- le réseau fédérateur de postes de supervision industriel (SCADA) ;
- les réseaux d'automates jugés sensibles (en se servant de l'analyse de risque).

ZCR 3.2 **SR 6.2**

R212

C3 Centraliser les éléments collectés par les systèmes de détection d'intrusion

Il est recommandé de centraliser les journaux et événements collectés par le système de détection d'intrusion, conformément à la stratégie de sécurité établie en R203.

SR 2.8 RE1

R213

C3 Disposer d'un système de détection certifié

Il est recommandé de s'assurer que le système de détection disposent d'un certificat de sécurité de premier niveau de l'ANSSI (CSPN) [24]ou équivalent (par exemple Critère Commun intégrant AVA_VAN.3).

R214

C4 Disposer d'un système de détection qualifié

Il est recommandé de s'assurer que le système de détection dispose d'une qualification de l'ANSSI [25].

24. La liste des produits certifiés est disponible à l'adresse suivante : https://cyber.gouv.fr/produits-certifies.
25. La liste des produits qualifiés est disponible à l'adresse suivante : https://cyber.gouv.fr/decouvrir-les-solutions-qualifiees.

Annexe A
Liste des exigences IEC 62443 couvertes par le présent guide

62443-2-1			
AVAIL 1.1	R74	NET 2.2	R142 R147
AVAIL 2.1	R8 R73	NET 3.2	R124 R129 R130 R138 R138 R154
AVAIL 2.3	R10	ORG 1.1	R1
AVAIL 2.5	R73	ORG 1.3	R2 R16 R86
CM 1.1	R4 R26	ORG 1.4	R22
CM 1.2	R5 R6 R125 R127	ORG 1.5	R15 R18 R19 R20
CM 1.3	R39	ORG 2.1	R7 R29
CM 1.4	R39 R51	ORG 2.2	R168 R170
COMP 1.1	R153 R156 R178 R182 R193	ORG 2.3	R33
COMP 1.2	R174 R175 R187 R189	ORG 3.1	R37 R60 R184
COMP 2.2	R161	USER 1.5	R42 R160
COMP 3.3	R55 R168 R172	USER 1.8	R78 R83 R84
COMP 3.4	R77	USER 1.9	R99 R130
COMP 3.5	R170	USER 1.11	R93
DATA 1.1	R13 R185	USER 1.14	R94
DATA 1.2	R96 R134 R145 R185	USER 2.1	R89
DATA 1.4	R39	USER 2.2	R83 R193
EVENT 1.1	R88 R94 R131 R139 R149		
EVENT 1.3	R183		
EVENT 1.4	R205 R207		
EVENT 1.5	R205		
EVENT 1.6	R61 R151 R204 R209		
EVENT 1.9	R55 R168		
NET 1.1	R102 R104 R106 R108 R112 R116 R123 R125 R127 R154		
NET 1.7	R188		

62443-2-4			
SP01.01	R15 R18 R19 R20	SP07.03BR	R129 R130 R138 R138 R154
SP01.02	R15 R18 R19 R20	SP07.04	R124 R129 R130 R138 R138 R154 R124
SP01.02RE1	R4 R5 R6 R26	SP08.01BR	R88 R131 R139 R149
SP01.03	R15 R18 R19 R20	SP08.01RE1	R183
SP01.05	R2 R16	SP08.02RE1	R61 R151 R183 R204 R209
SP01.05BR	R86	SP08.03BR	R88 R131 R139 R149 R206
SP01.06	R16	SP08.03RE1	R183
SP01.06BR	R2 R86	SP08.04BR	R117
SP01.07	R16	SP09.01	R193
SP01.07BR	R2 R86	SP09.01BR	R41
SP02.01BR	R7 R29	SP09.02	R41
SP02.02	R168	SP09.05	R93
SP02.03	R153 R156 R178 R182 R193	SP09.06	R93
SP03.01	R7 R29	SP09.07	R93
SP03.02	R104 R108 R123 R125 R127	SP09.08	R93
SP03.02BR	R106 R112	SP10.03	R161
SP03.03BR	R55 R168	SP10.04	R161
SP03.03RE1	R104 R108 R123 R125 R127	SP10.05RE1	R174 R175 R187 R189
SP03.05	R153 R156 R178 R182 R192 R193	SP11.01RE1	R172
SP03.05BR	R51	SP11.02RE2	R170
SP03.07BR	R89 R104 R108 R123 R125 R127	SP11.06	R168
SP03.07RE1	R99 R130	SP11.06RE1	R77
SP03.08BR	R42 R160 R193	SP11.06RE3	R55 R172
SP03.08RE1	R41	SP12.01BR	R8 R73
SP03.08RE2	R96 R145 R185	SP12.02BR	R73
SP03.10	R145 R185	SP12.04BR	R10
SP03.10RE4	R182	SP12.05BR	R8 R73
SP04.02	R142	SP12.06BR	R8 R73
SP04.02BR	R147	SP12.07BR	R9
SP06.02BR	R4 R5 R6 R26	SP12.08BR	R8 R73
SP06.03	R39	SP12.09	R74
SP07.02BR	R124 R129 R130 R138 R138 R154		

62443-3-2	
ZCR 1.1	R184
ZCR 3.2	R101 R104 R108 R123 R125 R127 R189 R190 R191 R211
ZCR 3.4	R175
ZCR 3.6	R110 R110
ZCR 5.13	R12
ZCR 7.1	R49

62443-3-3	
SR 1.1	R41 R78 R93 R99 R130 R160
SR 1.1 RE1	R84 R83
SR 1.11	R94
SR 1.13	R146
SR 1.2	R41 R160
SR 1.3	R41 R83 R84 R87
SR 1.4	R41 R83 R84
SR 1.5	R41 R87 R93 R97 R130
SR 1.6	R146 R147
SR 1.6 RE1	R41 R83+
SR 1.7	R93
SR 2.1	R89 R174
SR 2.1 RE1	R160
SR 2.2 RE1	R142 R146 R147
SR 2.3	R186
SR 2.8	R23 R88 R205
SR 2.8 RE1	R151 R206 R208 R210 R212
SR 2.8 RE1	R61
SR 2.12	R23
SR 2.9	R205
SR 3.1	R124 R129 R130 R134 R145 R185
SR 3.2	R161
SR 3.4	R51 R165 R197
SR 3.5	R196
SR 3.6	R39 R166 R194 R196 R198
SR 4.1	R96 R134 R145 R185
SR 5.1	R103 R104 R108 R115 R123 R125 R127
SR 5.1 RE1	R120 R121 R119 R122
SR 5.1 RE3	R106 R112
SR 5.2	R102 R104 R108 R116 R123 R125 R127 R154 R161
SR 5.3	R186
SR 6.1 RE1	R204 R209
SR 6.2	R131 R139 R149 R183 R208 R210 R211
SR 7.1	R117
SR 7.3	R9
SR 7.3 RE1	R10
SR 7.3 RE2	R73
SR 7.4	R73
SR 7.6	R39
SR 7.7	R153 R156 R157 R158 R178 R192 R193
SR 7.8	R4 R5 R6 R26

	62443-4-1
DM-1	R55
DM-4	R170
DM-5	R39 R57
SD-1	R33
SD-4	R156 R158 R161 R178
SG-3	R161
SG-7	R14
SI-1	R196
SI-2	R166 R194 R196 R197 R198 R200 R201
SI-3.5	R200
SI-3.6	R200
SM-1	R35
SM-2	R2 R86
SM-4	R15
SM-6	R165
SM-7	R195
SM-13	R24
SR-3	R30
SR-5	R14
SUM-1	R36 R165 R173
SVV-1	R31 R198 R201
SVV-3	R31 R168
SVV-3.5	R194 R201
SVV-3.6	R194 R201
SVV-4	R45
SVV-5	R199

62443-4-2	
CR 1.1	R41 R78 R83 R84 R93 R130
CR 1.1 RE2	R99 R99+
CR 1.2	R41 R188
CR 1.3	R41 R83 R84 R87
CR 1.4	R41 R83 R84
CR 1.5	R41 R87 R93 R97 R130
CR 1.6	R146
CR 1.7	R93
CR 1.11	R94
CR 1.13	R147
CR 1.14	R96
CR 2.1	R89
CR 2.1 RE2	R42
CR 2.2	R142 R146 R147 R148
CR 2.8	R23 R88 R151 R205
CR 2.9	R205
CR 2.12	R23
CR 3.1	R124 R129 R130 R134 R145 R148 R185
CR 3.4	R51 R54 R165 R197
CR 3.5	R196
CR 3.6	R39 R166 R194 R196 R198
CR 3.9	R13
CR 4.1	R96 R134 R145 R185
CR 5.1	R103 R104 R108 R115 R119 R120 R121 R123 R125 R127 R147
CR 5.2	R102 R104 R108 R116 R116+ R123 R125 R127 R154
CR 6.1 RE1	R204 R209 R61
CR 6.2	R131 R139 R149 R183 R208 R210
CR 7.1	R117
CR 7.3	R9
CR 7.3 RE1	R10
CR 7.4	R73
CR 7.6	R39
CR 7.7	R153 R156 R157 R158 R178 R193
CR 7.8	R4 R5 R6 R26
EDR 2.13	R158
EDR 3.10	R165
EDR 3.11	R67 R69
EDR 3.14	R185
HDR 3.10	R165
HDR 3.11	R67 R69
HDR 3.14	R185

62443-4-2 (suite)	
NDR 1.13	R146 R147 R162
NDR 1.6	R78 R83 R84 R146
NDR1.6RE1	R41
NDR 3.10	R165
NDR 3.11	R67 R69
NDR 3.14	R185
NDR 5.2	R104 R108 R123
NDR 5.13	R104 R108 R123

Annexe B
Correspondance des recommandations entre les deux versions du guide

Guide V2	Guide V1
R1	R.1
R2	R.2
R5	D.8
R6	R.7
R3	D.6
R7	R.11
R8	R.15
R9	R.16
R10	R.17
R12	R.19
R13	R.20
R14	R.23
R15	R.26
R16	R.25
R17	D.28
R19	R.29
R20	D.32
R21	R.33
R22	R.34
R23	R.35
R24	R.38
R26	R.36
R25	R.40
R27	R.42
R28	R.43
R29	R.44
R30	R.50
R31	R.45
R32	R.48
R33	R.51
R34	R.54
R35	R.55

Guide V2	Guide V1
R36	R.57
R37	R.59
R38	R.60
R39	R.58
R40	R.64
R41	R.65
R42	R.66
R43	R.68
R44	R.69
R45	R.71
R46	R.72
R47	D.74
R48	R.75
R49	R.76
R50	R.79
R51	R.78
R52	R.82
R53	D.83
R54	R.81
R55	R.85
R56	R.88
R57	R.87
R58	R.91
R59	R.92
R60	R.94
R61	R.95
R62	R.97
R65	R.98
R63	R.99
R64	D.101
R66	R.102
R67	R.104

Guide V2	Guide V1
R68	R.103
R69	D.106
R70	R.107
R71	R.108
R72	R.109
R73	R.111
R74	R.112
R77	R.116
R75	R.113
R79	R.118
R80	R.119
R82	R.121
R83	R.124
R83+	R.123
R84	R.125
R86	R.128
R87	D.129
R88	R.127
R89	R.126
R90	R.132
R91	R.133
R92	R.134
R93	R.136
R94	R.137
R95	R.138
R93-	R.139
R96	R.140
R97	R.141
R98	R.145
R98+	R.145
R99	R.143
R100	R.144

Guide V2	Guide V1
R101	R.148
R102	R.149
R110	R.154
R106	R.151
R106-	R.152
R107	D.156
R108	R.153
R109	R.157
R113	R.150
R115	R.160
R116	R.162
R116+	R.162
R117	R.163
R118	R.164
R119	R.166
R121	D.167
R122	R.169
R123	R.170
R124	R.171
R126	R.175
R128	R.175
R127	R.172
R133	D.182
R132	D.183
R134	R.184
R138	R.185
R136	R.186
R137	R.187
R139	R.189
R140	D.190
R140	R.202
R141	R.187
R142	R.192
R143	R.196
R146	R.193
R146	R.194
R147	R.195
R148	R.197
R149	R.200
R151	D.204
R153	R.206

Guide V2	Guide V1
R154	R.207
R156	R.209
R157	R.210
R158	R.211
R159	R.214
R160	R.215
R161	R.217
R162	R.218
R163	R.220
R164	R.220
R165	R.221
R166	R.223
R167	D.224
R168	R.226
R169	R.227
R170	D.228
R172	R.230
R173	R.232
R174	R.233
R174	R.234
R175	R.237
R176	R.235
R177	R.236
R178	R.239
R179	D.241
R180	R.242
R181	R.243
R182	R.244
R183	D.246
R184	D.247
R186	R.248
R187	R.249
R188	R.250
R189	R.254
R190	R.257
R191	R.258
R193	R.259
R192	R.260
R195	R.265
R194	R.266
R199	R.268

Guide V2	Guide V1
R200	R.264
R201	R.267
R202	D.270
R205	R.271
R209	R.272
R208	R.273
R206	R.274
R207	R.276
R210	R.278
R211	R.279
R212	R.281
R213	R.280
R214	R.280

Annexe C
Liste minimale des événements à journaliser

La liste minimale (mais non exhaustive) des événements à journaliser est composée des :

- tentatives d'authentification (réussite ou échec) ;
- actions des utilisateurs dans le système ;
- utilisations des comptes à privilèges ;
- défaillances des mécanismes de sécurité ;
- tentatives de connexions réseau ;
- démarrage et arrêt des fonctionnalités de journalisation ;
- activation, désactivation et modification du comportement ou de paramètres des mécanismes de sécurité (authentification, génération de journaux, etc.) ;
- actions entreprises en raison d'une défaillance du stockage des journaux ;
- tentatives d'exportation d'informations ;
- modifications du groupe d'utilisateurs faisant partie d'un rôle ;
- détections d'une violation physique ;
- tentatives d'établissement d'une session utilisateur ;
- tentatives de chargement, modification ou récupération de programme, micrologiciel ;
- modifications de paramètres systèmes (heure, adresse IP ou MAC, temps de cycle, chien de garde, etc.) ;
- modifications ou forçages de données applicatives ;
- modifications du mode de fonctionnement d'un automate ou RTU (démarrage, arrêt, redémarrage).

Liste des recommandations

Bibliographie

[1] *Purdue Reference Model (ISA95)*.
Page web, PERA, Juin 1990.
https://www.pera.net.

[2] *Systèmes instrumentés de sécurité pour l'industrie de transformation*.
Norme, ISA, février 2016.
Ce document résulte de développements conjoints entre l'IEC et l'ISA.
https://www.boutique.afnor.org/fr-fr/resultats?Keywords=IEC+61511
https://www.isa.org/standards-and-publications/isa-standards/isa-84-standards.

[3] *Secteur de l'eau : état de la menace informatique*.
Rapport, ANSSI, 28 novembre 2024.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-011/.

[4] *Approche SSI pour l'Internet des objets industriels*.
Article Version 1.0, ANSSI, juin 2025.
https://cyber.gouv.fr/article-iiot.

[5] *Etat de la menace informatique sur le secteur des transports urbains*.
Rapport, ANSSI, 11 mars 2025.
https://cyber.gouv.fr/actualites/etat-de-la-menace-informatique-sur-le-secteur-des-transports-urbains.

[6] *Etat de la menace informatique sur les équipements mobiles*.
Rapport, ANSSI, 26 novembre 2025.
https://cyber.gouv.fr/actualites/etat-de-la-menace-informatique-sur-les-equipements-mobiles.

[7] *La supervision de sécurité*.
Guides, ANSSI, 26 août 2025.
https://cyber.gouv.fr/la-supervision-de-securite.

[8] *Panorama de la cybermenace 2024*.
Rapport, ANSSI, 17 avril 2025.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-011/.

[9] *Recommandations de sécurité relatives à Active Directory*.
Note technique DAT-NT-017/ANSSI/SDE/NP v1.1, ANSSI, septembre 2014.
https://cyber.gouv.fr/publications/recommandations-de-securite-relatives-active-directory.

[10] *Recommandations pour la sécurisation d'un commutateur de desserte*.
Note technique DAT-NT-025/ANSSI/SDE/NP v1.0, ANSSI, juin 2016.
https://cyber.gouv.fr/guide-commutateurs.

[11] *Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows*.
Note technique DAT-NT-013/ANSSI/SDE/NP v2.0, ANSSI, janvier 2017.
https://cyber.gouv.fr/guide-windows-restrictions-logicielles.

[12] *Recommandations de déploiement du protocole 802.1X pour le contrôle d'accès à des réseaux locaux*.
Guide ANSSI-BP-043 v1.0, ANSSI, août 2018.
https://cyber.gouv.fr/guide-802-1x.

[13] *Recommandations de configuration des commutateurs et pare-feux Hirschmann*.
Guide ANSSI-BP-033 v1.3, ANSSI, février 2022.
https://cyber.gouv.fr/guide-commutateurs-hirschmann.

[14] *Recommandations de configuration des commutateurs et pare-feux Siemens Scalance*.
Guide ANSSI-BP-094 v1.0, ANSSI, février 2022.
https://cyber.gouv.fr/guide-commutateurs-siemens.

[15] *Recommandations de sécurité relatives à un système GNU/Linux*.
Guide ANSSI-BP-028 v2.0, ANSSI, octobre 2022.
https://cyber.gouv.fr/guide-linux.

[16] *Sauvegarde des systèmes d'information*.
Fondamentaux ANSSI-BP-100 v1.0, ANSSI, octobre 2023.
https://cyber.gouv.fr/publications/fondamentaux-sauvegarde-systemes-dinformation.

[17] *Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures*.
Guide ANSSI-GP-042 v2.0, ANSSI, septembre 2017.
https://cyber.gouv.fr/hygiene-informatique.

[18] *Externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques*.
Page Web Version 1.0, ANSSI, décembre 2010.

[19] *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*.
Note technique DAT-NT-006/ANSSI/SDE/NP v1.0, ANSSI, mars 2013.
https://cyber.gouv.fr/guide-politique-filtrage-pare-feu.

[20] *L'homologation de sécurité en neuf étapes simples*.
Guide ANSSI-PA-096 v1.0, ANSSI, août 2014.
https://cyber.gouv.fr/guide-homologation-securite.

[21] *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau*.
Note technique DAT-NT-003/ANSSI/SDE/NP v1.1, ANSSI, août 2015.
https://cyber.gouv.fr/guide-ipsec.

[22] *Cartographie du système d'information*.
Guide ANSSI-PA-046 v1.0, ANSSI, octobre 2018.
https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation.

[23] *Maîtrise du risque numérique - l'atout confiance*.
Guide ANSSI-PA-070 v1.0, ANSSI, novembre 2019.
https://cyber.gouv.fr/publications/maitrise-du-risque-numerique-latout-confiance.

[24] *Doctrine de détection pour les systèmes industriels*.
Guide ANSSI-PA-084 v1.0, ANSSI, décembre 2020.
https://cyber.gouv.fr/doctrine-detection-si-indus.

[25] *Organiser un exercice de gestion de crise cyber*.
Guide ANSSI-PA-081 v1.0, ANSSI, octobre 2020.
https://cyber.gouv.fr/publications/organiser-un-exercice-de-gestion-de-crise-cyber.

[26] *Recommandations de sécurité relatives à TLS*.
Guide ANSSI-PA-035 v1.2, ANSSI, mars 2020.
https://cyber.gouv.fr/guide-tls.

[27] *Recommandations relatives à l'interconnexion d'un système d'information à Internet*.
Guide ANSSI-PA-066 v3.0, ANSSI, juin 2020.
https://cyber.gouv.fr/guide-interconnexion-si-internet.

[28] *Règles de programmation pour le développement d'applications sécurisées en Rust*.
Guide ANSSI-PA-074 v1.0, ANSSI, juin 2020.
https://cyber.gouv.fr/publications/regles-de-programmation-pour-le-developpement-dapplications-securisees-en-rust.

[29] *Règles de programmation pour le développement sécurisé de logiciels en langage C*.
Guide ANSSI-PA-073 v1.2, ANSSI, juillet 2020.
https://cyber.gouv.fr/publications/regles-de-programmation-pour-le-developpement-securise-de-logiciels-en-langage-c.

[30] *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques*.
Guide ANSSI-PG-083 v2.0, ANSSI, janvier 2020.
https://cyber.gouv.fr/publications/mecanismes-cryptographiques.

[31] *Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique*.
Guide ANSSI-PA-089 v1.0, ANSSI, décembre 2021.
https://cyber.gouv.fr/publications/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique.

[32] *Guide de sélection d'algorithmes cryptographiques*.
Guide ANSSI-PA-079 v1.0, ANSSI, mars 2021.
https://cyber.gouv.fr/publications/mecanismes-cryptographiques.

[33] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v3.0, ANSSI, mai 2021.
https://cyber.gouv.fr/guide-admin-si.

[34] *Recommandations de sécurité pour l'architecture d'un système de journalisation*.
Guide DAT-PA-012 v2.0, ANSSI, janvier 2022.
https://cyber.gouv.fr/guide-journalisation.

[35] *Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection*.
Guide ANSSI-PA-072 v2.1, ANSSI, novembre 2023.
https://cyber.gouv.fr/guide-controle-acces-videoprotection.

[36] *Recommandations sur le nomadisme numérique*.
Guide ANSSI-PA-054 v2.0, ANSSI, novembre 2023.
https://cyber.gouv.fr/guide-nomadisme-numerique.

[37] *Sauvegarde des systèmes d'information*.
Essentiels Version 1.1, ANSSI, décembre 2023.
https://cyber.gouv.fr/publications/sauvegarde-des-systemes-dinformation.

[38] *DevSecOps*.
Essentiels Version 1.0, ANSSI, février 2024.
https://cyber.gouv.fr/publications/devsecops.

[39] *Recommandations pour les architectures des interconnexions multiniveaux*.
Guide ANSSI-PA-101 v1.0, ANSSI, octobre 2024.
https://cyber.gouv.fr/guide-archi-interco-mn.

[40] *Données et traitements sensibles*.
Essentiels Version 1.0, ANSSI, mars 2025.
https://cyber.gouv.fr/publications/donnees-traitements-sensibles.

[41] *La cybersécurité des systèmes industriels - Méthode de classification*.
Guide ANSSI-PA-107 v1.0, ANSSI, mai 2025.
https://cyber.gouv.fr/publications/la-cybersecurite-des-systemes-industriels.

[42] *Mise en œuvre sécurisée d'un serveur Windows*.
Essentiels Version 1.0, ANSSI, octobre 2025.
https://cyber.gouv.fr/publications/mise-en-oeuvre-securisee-dun-serveur-windows.

[43] *Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory*.
Guide ANSSI-PB-090 v1.0, ANSSI, janvier 2022.
https://cyber.gouv.fr/guide-journalisation-windows.

[44] *Expression des besoins et identification des objectifs de sécurité*.
Guide Version 1.1, ANSSI, janvier 2010.

[45] *RGS Annexe B2 : Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques*.
Référentiel Version 2.0, ANSSI, juin 2012.
https://cyber.gouv.fr/rgs.

[46] *RGS Annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques*.
Référentiel Version 2.03, ANSSI, février 2014.
https://cyber.gouv.fr/rgs.

[47] *Prestataires d'audit de la sécurité des systèmes d'information. Référentiel d'exigences*.
Référentiel Version 2.1, ANSSI, octobre 2015.
https://cyber.gouv.fr/referentiels-dexigences-pour-la-qualification.

[48] *Référentiel de cybersécurité pour les prestataires d'intégration et de maintenance de systèmes industriels*.
Guide Version 1.0, ANSSI, mars 2016.
https://cyber.gouv.fr/publications/referentiel-dexigences-de-securite-pour-les-prestataires-dintegration-et-de.

[49] *Profil de fonctionnalités et de sécurité - Sas et station blanche (réseaux non classifiés)*.
Guide ANSSI-PG-076 v1.0, ANSSI, juillet 2020.
https://cyber.gouv.fr/publications/profil-de-fonctionnalites-et-de-securite-sas-et-station-blanche-reseaux-non-classifies.

[50] *Authentification multifacteurs et mots de passe*.
Guide ANSSI-PG-078 v1.0, ANSSI, octobre 2021.
https://cyber.gouv.fr/guide-authentification.

[51] *Instruction générale interministérielle n°1300*.
Référentiel, SGDSN, août 2021.
https://cyber.gouv.fr/igi1300.

[52] *Approche SSI pour l'Internet des objets industriels*.
fondamentaux ANSSI-PG-109 v1.0, ANSSI, 2025.
https://cyber.gouv.fr/publications/approche-ssi-pour-linternet-des-objets-industriels.

[53] *ISA/IEC 62443 - Control Systems Cybersecurity Standards*.
Document normatif, ISA, 2009 à 2024 selon les parties.
https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

[54] *IEC 62541 - Architecture unifiée OPC*.
Document normatif, OPC FOUNDATION, 2015 à 2021 selon les parties.
https://www.boutique.afnor.org/.

[55] *ISO 27002 : Security techniques - Code of practice for security management.*
Document normatif, ISA, 2022.
https://www.iso.org/fr/standard/75652.html.

[56] *Service ADS*.
Service, ANSSI, 2025.
https://cyber.gouv.fr/actualites/le-service-active-directory-security-ads-accompagner-la-securisation-des-annuaires.

[57] *Guide pour réaliser un plan de continuité d'activités*.
Guide, SGDSN, 2013.
https://www.sgdsn.gouv.fr/files/files/Nos_missions/guide-pca-sgdsn-110613-normal.pdf.

Version 2.0 - 27/11/2025- ANSSI-PA-108
Licence ouverte / Open Licence (Étalab - v2.0)
Dépôt légal : Novembre 2025

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité