Mesures détaillées

La cybersécurité des systèmes industriels

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Table des matières

Chapitre 1

Introduction

1.1 Contexte

Le présent document est issu des réflexions du groupe de travail sur la cybersécurité des systèmes industriels piloté par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) [1]. L'objectif des travaux de ce groupe, constitué d'acteurs du domaine des systèmes automatisés de contrôle des procédés industriels et de spécialistes de la sécurité des systèmes d'information (SSI), est de proposer un ensemble de mesures pour améliorer le niveau de cybersécurité des systèmes industriels.

Ce document s'adresse à tous les acteurs (entités responsables, chefs de projets, acheteurs, équipementiers, intégrateurs, maîtres d'œuvre, etc.) participant à la conception, la réalisation, l'exploitation et la maintenance des systèmes industriels.

1.2 Champ d'application

Le groupe de travail ne s'est pas intéressé à un secteur d'activité en particulier et les éléments contenus dans ce document ont donc vocation à être applicables à tous les secteurs. Certains d'entre eux ont des spécificités qui n'ont peut-être pas été détaillées ou prises en compte dans le présent document. **En conséquence, une déclinaison sectorielle de ce document pourra être nécessaire dans certains cas afin de préciser les modalités d'application et prendre en compte les contraintes spécifiques.**

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

1. Les membres du groupe de travail sont les sociétés et organismes suivants : Actemium, Airbus Defence and Space, Arkoon-Netasq, A.R.C Informatique, Atos Worldgrid, Hirschmann, Cassidian Cybersecurity, CEA, CLUSIF, DCNS, DGA Maîtrise de l'information, Euro systems, EXERA, GDF SUEZ, Gimélec, INERIS, Itris Automation Square, Lexsi, Schneider Electric, Siemens, Sogeti, RATP, Solucom, Thales, Total.

Il est également 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 métier spécifiques, par exemple). Ces cas particuliers devront être étudiés spécifiquement et les mesures qui en découleront seront soumises pour approbation à l'autorité de cyberdéfense.

1.3 Structure du corpus documentaire

Les travaux du groupe de travail sont organisés en deux documents. Ce document contient les mesures techniques et organisationnelles détaillées à mettre en place sur les systèmes industriels en fonction des classes définies dans le guide de classification [13].

Il est donc important de commencer par lire attentivement le document cité précédemment qui constitue le socle de la démarche et contient la définition des termes utilisés dans la suite de ce document.

1.4 Avis aux lecteurs

Les mesures présentées dans le document sont des mesures de cybersécurité conventionnelles mais adaptées pour les systèmes industriels. L'objectif de ce document n'est en aucun cas de former les lecteurs à la cybersécurité pour les systèmes industriels. Il a donc été supposé que les lecteurs disposaient de connaissances élémentaires en matière de technologies de l'information et de la communication mais aussi de cybersécurité ou qu'ils pouvaient s'appuyer sur des personnes disposant de ces compétences. La bonne application de certaines mesures nécessitera certainement un travail d'équipe entre des « informaticiens » et des « automaticiens ».

Note

Les publications de l'ANSSI sont diffusées sur son site Internet : `http://www.ssi.gouv.fr/publications/`.
Toute remarque sur ce guide peut être adressée à systemes_industriels@ssi.gouv.fr.

Chapitre 2

Considérations relatives à la cybersécurité des installations industrielles

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 qui sont présentes dans ces systèmes 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 vulnérabilités rencontrées dans ces systèmes sont listées. Elles peuvent découler des contraintes listées dans la section précédente mais pas seulement. En particulier, on pourra retrouver dans cette section, des vulnérabilités couramment rencontrées dans les systèmes d'information de gestion.

2.1 Liste des contraintes

Les contraintes sont un ensemble de faits sur lesquels il ne va pas être possible d'agir et qui peuvent avoir un impact lourd sur la sécurité du système industriel concerné. Il sera très important de prendre en compte ces contraintes lors du choix des mesures de sécurité à mettre en œuvre.

Références	Thèmes	Contraintes
C1-MI	Maîtrise des installations	— Multitude d'intervenants sur une installation ce qui ne facilite pas la maîtrise des actions effectuées sur celle-ci. — 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 de l'installation peut être limitée. Ce qui entraîne une perte du savoir lors des départs de personnels et ne facilite pas le traitement des incidents. — Certains fournisseurs font de la télémaintenance depuis l'étranger. — Sur certaines installations cohabitent deux opérateurs différents, ce qui peut parfois poser des problèmes juridiques en cas de modification de l'installation. Par ailleurs, les systèmes qu'ils gèrent peuvent aussi constituer une menace entre eux. — Les installations sont souvent hétérogènes car venant de différents fournisseurs ou parce qu'elles ont évoluées au cours du temps. L'hétérogénéité peut être imposée pour des raisons de sûreté fonctionnelle.

Références	Thèmes	Contraintes
C2-CO	Contrats	— Les fournisseurs exigent d'avoir accès à leurs équipements en télémaintenance sous peine de ne pas les garantir. — La modification des systèmes sans accord préalable du fournisseur peut entrainer une perte de garantie. — Il peut être contractuellement interdit de modifier l'installation existante même pour implémenter des mesures de cybersécurité. — Certains clients exigent d'avoir accès à distance aux informations relatives (historisation) à la production du site. Pour des raisons de simplicité, le transfert de données se fait souvent sur un réseau public comme Internet.

Références	Thèmes	Contraintes
C3-REG	Réglementation	— Certaines réglementations imposent aux opérateurs d'exporter des données vers un tiers. Par exemple, les déchetteries doivent fournir un certain nombre de données à la DRIRE. — La traçabilité est une exigence forte dans certains domaines comme l'agro-alimentaire ou l'industrie pharmaceutique par exemple. — Remarque : les mesures de sécurité fonctionnelles imposées par la réglementation d'un secteur peuvent renforcer le niveau de sécurité de l'installation et offrir un niveau de risque résiduel acceptable. — La réglementation en matière de sûreté peut limiter la possibilité de modification des installations. En effet, la modification d'une installation peut entraîner la perte d'une homologation.
C4-GCH	Gestion des changements	— Il n'existe pas d'environnement de test permettant de s'assurer de la non-régression des installations. — Les interventions sur les installations ne peuvent être effectuées que lors des périodes de maintenances. — Les fournisseurs offrent peu de support pour aider les opérateurs à qualifier les impacts des mesures de sécurité sur les installations.

Références	Thèmes	Contraintes
C5-OPE	Opérations	— Certains environnements demandent une réactivité forte des opérateurs notamment en cas d'incident. Les mesures de sécurité ne doivent pas nuire à 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 opérateurs doivent souvent visualiser l'état de l'installation en temps réel et intervenir rapidement. De ce fait, ils ne peuvent pas verrouiller les postes qu'ils utilisent.
C6-CECO	Contraintes économiques	— Les mises à jour des systèmes existants et l'évolution des installations entraînent des coûts importants pour le client.

Références	Thèmes	Contraintes
C7-GOUV	Gouvernance de sécurité	— Lorsque la direction des systèmes d'information (DSI) se voit attribuer la mission de sécuriser les systèmes industriels, elle n'a pas de lien hiérarchique avec les équipes chargées de l'opération de ces derniers. Ceci complique ou ralentit la mise en œuvre de la cybersécurité. — Lorsque la sécurisation des systèmes industriels est confiée à une direction métier, la cybersécurité a souvent une priorité basse et la responsabilité de la gestion des interfaces entre les systèmes industriels et les systèmes de gestion est floue. — Il y a peu de personnel en charge de l'informatique industrielle sur un site industriel.

Références	Thèmes	Contraintes
C8-CTECH	Contraintes techniques	— Les équipements sont déployés pour 15 à 20 ans. L'obsolescence limite leurs possibilités de mise à jour ainsi que l'intégration de fonctions de sécurité. — Certains équipements (comme les automates) et protocoles offrent des fonctionnalités de sécurité limitées voire inexistantes. — Les fournisseurs offrent peu de solutions techniques permettant une gestion centralisée des fonctions de sécurité. Par exemple, il n'est souvent pas possible de changer un mot de passe sur plusieurs équipements dispersés géographiquement. — Sur certains systèmes, les besoins de performance exigent qu'il n'y ait pas de latence.
C9-CULT	Culture de la sécurité	— Dans les milieux où la sûreté de fonctionnement est très présente, il y a souvent un sentiment que celle-ci permet également de régler les problèmes de cybersécurité. — La sécurité des systèmes d'information n'est pas abordée lors des cursus de formation et en particulier ceux des automaticiens.

Références	Thèmes	Contraintes
C10-MAT	**Maturité des solutions techniques**	— Il existe peu de compétences en matière de cybersécurité des systèmes industriels. — Peu de fournisseurs intègrent la notion de cycle de développement sécurisé dans la réalisation de leurs produits.

2.2 Vulnérabilités

Les vulnérabilités des systèmes d'information industriels qui ont été identifiées par le groupe de travail sont listées ci-dessous.

Important

Les encadrés *Pourquoi est-ce une vulnérabilité ?* n'ont pas vocation à être exhaustifs et sont là uniquement pour illustrer la vulnérabilité en question.

2.2.1 Maîtrise des installations

Gestion des correctifs de sécurité

La gestion des vulnérabilités est complexe dans les systèmes industriels. Dans de nombreux cas, les mises à jour ne pourraient être faites que pendant les phases de maintenance et, parfois, leur application peut entrainer 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 de l'installation et, comme l'entité responsable dispose rarement d'une plateforme d'essai, elle ne peut pas effectuer de tests de non-régression sur les correctifs éventuellement publiés par les fournisseurs.

Toutes ces raisons font que la plupart des installations n'ont pas de procédures ou de mécanismes techniques pour l'application des mises à jour de sécurité. En particulier, les systèmes de mise à jour automatiques sont souvent incompatibles, notamment avec les anciennes installations.

Pourquoi est-ce une vulnérabilité ?

La présence de vulnérabilités connues non corrigées dans une installation augmente le risque d'une intrusion.
De nombreux codes malveillants génériques exploitent ce genre de vulnérabilités et le risque de contamination de l'installation est donc fortement augmenté par l'absence des mises à jour de sécurité.
Lors d'une attaque ciblée, l'attaquant commence souvent par la recherche de vulnérabilités connues non corrigées pour tenter de pénétrer dans le système. Une bonne politique d'application des mises à jour de sécurité permet d'éliminer ces vulnérabilités, ce qui complique fortement la tâche de l'attaquant.

Remarque

En 2013, de nombreux systèmes industriels sont encore vulnérables aux virus tels que Conficker apparu en 2009 et pour lequel le correctif est pourtant connu.

Pas de veille sur les vulnérabilités et les menaces

Les entités responsables de systèmes industriels mettent rarement en place une veille active sur les vulnérabilités des produits et technologies utilisés. Ceci est vrai malgré l'apparition de sources d'information spécialisées.

Aucune veille n'est faite non plus sur l'évolution de la menace ou des techniques d'attaque.

Pourquoi est-ce une vulnérabilité ?

L'absence de veille sur les vulnérabilités ou obsolescences de produits ou technologies utilisées empêche de réagir rapidement 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.

2.2.2 Défaut de contrôle d'accès logique

Défaut de la politique de gestion des mots de passe

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

- l'utilisation de mots de passe par défaut ;
- la faible fréquence de changement des mots de passe (par exemple due au manque d'outil pouvant mettre à jour les mots de passe d'un parc d'automates) ;
- l'utilisation de mots de passe faibles (parfois due à des limitations de l'équipement ou du logiciel).

Pourquoi est-ce une vulnérabilité ?

Une première étape pour un attaquant consiste souvent à tenter de compromettre le compte d'un utilisateur du système pour y avoir accès, au moins partiellement. Pour cela, une des techniques à sa disposition consiste à tenter de récupérer un mot de passe.
L'utilisation de mot passe par défaut lui permet donc d'avoir accès directement à des comptes présents par défaut sur l'installation, souvent avec des privilèges élevés. Lorsque les mots de passe ont été changés, l'attaquant peut essayer les attaques par dictionnaire pour tenter de découvrir un mot de passe et accéder ainsi au compte concerné. C'est pourquoi il est recommandé d'utiliser un mot de passe robuste et, dans la mesure du possible, de le changer régulièrement.

Pas 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, un ancien employé pourra conserver son compte longtemps après son départ.

Il est également courant de voir l'utilisation de comptes à privilèges. Ceci 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 ».

Pourquoi est-ce une vulnérabilité ?

L'utilisation de comptes génériques augmente considérablement les risques de compromission notamment du fait de la circulation du mot de passe. 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 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 visibilité sur le système industriel concerné (qui accède à quelles ressources ?). En cas de problème, il sera très difficile d'en retrouver l'origine.

2.2.3 Défaut de contrôle des interfaces de connexion

Sur certains systèmes industriels, on note régulièrement une absence de politique de gestion des interfaces de connexion. Par exemple, les ports USB ne sont pas bloqués ou les ports Ethernet non utilisés sont laissés actifs.

Pourquoi est-ce une vulnérabilité ?

Laisser des interfaces non maîtrisées augmente la surface d'attaque.
Par exemple, ne pas bloquer les ports USB peut favoriser l'introduction de virus dans le système ou la non-désactivation des ports Ethernet offre la possibilité de réaliser des branchements 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 WiFi par exemple).

2.2.4 Cartographie non maitrisée

La cartographie d'un système industriel n'est pas forcément maîtrisée. En particulier, on pourra noter :

— une prise en charge de l'installation du câblage réseau comme le câblage électrique, avec un manque de prise en compte des contraintes de documentation ;

- une insuffisance de la cartographie du système industriel et notamment :
  - des topologies réseau,
  - des matrices de flux,
  - des inventaires des équipements matériels et logiciels du parc industriel,
- pas de recensement des procédures d'exploitation ;
- une absence de vision des générations technologiques qui cohabitent et de leurs vulnérabilités intrinsèques.

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.

Pourquoi est-ce une vulnérabilité ?

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

2.2.5 Défaut de maîtrise de la configuration

Manque de contrôle d'intégrité ou d'authenticité

Il est très rare que des mécanismes de contrôle d'intégrité ou d'authenticité soient mis en place pour les firmwares, les logiciels, les programmes d'automates et applications SCADA.

Pourquoi est-ce une vulnérabilité ?

L'absence de mécanisme de contrôle d'intégrité ou d'authenticité permet à un attaquant de diffuser une mise à jour piégée.

Absence de sauvegarde

Les sauvegardes sont souvent partielles, inexistantes ou disponibles chez le fournisseur seulement. Lorsque des sauvegardes existent, le bon fonctionnement des procédures de restauration en cas d'incident est rarement testé.

Pourquoi est-ce une vulnérabilité ?

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

Modifications en ligne non maîtrisées

Il est possible de modifier à chaud, 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.

Pourquoi est-ce une vulnérabilité ?

L'absence d'authentification ou de journalisation permet à un attaquant de modifier de manière furtive le programme d'un automate. Cette modification pourra ne pas être détectable par les applications SCADA et les utilisateurs.

2.2.6 Utilisation d'équipements vulnérables

Les équipements développés pour les systèmes industriels intègrent souvent des contraintes de sûreté de fonctionnement fortes mais rarement des contraintes de cybersécurité. En particulier, les fonctions de sécurité sont souvent limitées voire inexistantes et les techniques de développement employées envisagent rarement la présence d'un attaquant sur le système comme une menace.

La configuration des équipements ou logiciels présents dans le réseau est rarement durcie. En particulier, les services inutilisés sont souvent laissés activés comme dans la configuration par défaut.

Pourquoi est-ce une vulnérabilité ?

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 ne sera pas vulnérable.

Remarque

N'installer que les éléments indispensables est un principe de sûreté de fonctionnement. Cela permet de réduire les risques de défaillance, simplifie la compréhension et la maintenabilité des installations

2.2.7 Utilisation de protocoles vulnérables

Les systèmes industriels font souvent usage de protocoles réseaux n'intégrant aucun mécanisme de sécurité. Ces protocoles peuvent être des protocoles classiques comme telnet mais peuvent également être des protocoles spécifiques aux systèmes industriels comme Modbus, Profibus, EtherNetIP, etc.

Remarque : EtherNetIp est le nom d'un protocole applicatif utilisé par certains équipements (automates industriels et logiciels SCADA par exemple).

Différentes technologies sans fil (WiFi, GSM, Zigbee) peuvent avoir été adaptées sans qu'une analyse de risque ait été menée ou sans que les mesures de protection adaptées n'aient été mises en place.

Pourquoi est-ce une vulnérabilité ?

L'utilisation de protocoles 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 identifiants de connexion circulant en clair sur le réseau.
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 de nombreux cas, les intervenants (mainteneurs, exploitants, etc) 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 dans d'autres endroits qui ne permettent pas la mise en place d'un contrôle d'accès physique efficace.

Pourquoi est-ce une vulnérabilité ?

L'absence de contrôle d'accès physique permet à un attaquant d'accéder directement à l'installation, contournant ainsi toutes les protections périmétriques qui pourraient avoir été mises en places.

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

Par ailleurs, il est très courant qu'il n'y ait pas de cloisonnement non plus au sein même des systèmes industriels ; entre ses différents sous-ensembles 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.

Pourquoi est-ce une vulnérabilité ?

L'absence de cloisonnement entre les systèmes facilite le travail d'un attaquant qui peut évoluer plus facilement dans le système pour accéder à son but.
Un cloisonnement efficace permettra aussi de limiter la propagation d'un virus.

Remarque

Le cloisonnement devrait être une bonne pratique en matière de sûreté de fonctionnement puisqu'il permet de limiter les effets d'un dysfonctionnement des systèmes sans même parler de cybersécurité.

2.2.10 Télémaintenance

La télémaintenance et la télégestion sont des pratiques de plus en plus courantes pour les systèmes industriels. Certains sont même connectés sur des réseaux publics comme Internet ou les réseaux 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 fabriquant ou l'intégrateur.

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

Pourquoi est-ce une vulnérabilité ?

L'utilisation d'accès à distance augmente considérablement la surface d'attaque d'un système. En effet, il est difficile de mettre en place des mesures de protection physique sur ce type d'accès.

2.2.11 Terminaux nomades non maîtrisés

Il est de plus en plus courant que les intervenants utilisent des terminaux mobiles comme des ordiphones ou des tablettes pour augmenter leur productivité en déplacement sur le terrain. Ceci est d'autant plus vrai pour des grandes installations distribuées.

La sécurité de ces terminaux n'est pas forcément maîtrisée et l'on commence à voir apparaître l'utilisation de matériel personnel pour remplir des missions professionnelles, ce que l'on appelle parfois le « Bring Your Own Device » (BYOD).

Pourquoi est-ce une vulnérabilité ?

L'utilisation de terminaux mobiles à la sécurité non-contrôlée augmente leur risque de compromission et offre ainsi une porte d'entrée potentielle à un attaquant.

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 sont de plus en plus standards. Ainsi, en termes de réseau, Ethernet et TCP/IP sont de plus en plus employés pour remplacer les technologies propriétaires qui étaient utilisées auparavant. Les outils de développement ou de maintenance font également de plus en plus appel à des briques génériques.

Pourquoi est-ce une vulnérabilité ?

L'utilisation de briques standards expose les systèmes à l'ensemble des vulnérabilités qu'elles contiennent. Les systèmes industriels sont alors vulnérables à des codes d'attaque génériques.
A contrario, l'utilisation de technologies propriétaires ou rares n'est pas une protection en soi mais augmente la complexité ou le coût d'une attaque du fait du besoin de développer soi-même les programmes malveillants.

2.2.13 Intervenants

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

Pourquoi est-ce une vulnérabilité ?

L'absence de sensibilisation à la SSI entraine 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 Supervision insuffisante des événements de cybersécurité

En cas d'incident sur une installation, les opérateurs et mainteneurs n'envisagent pas forcément une action malveillante comme cause possible. Les intervenants sont souvent peu qualifiés pour identifier les événements de cybersécurité.

La journalisation des événements de sécurité est souvent limitée et peu exploitée. Les dispositifs de détection d'incidents ou de dysfonctionnements sont rares.

Lorsqu'une supervision des événements de cybersécurité est effective, la multitude des paramètres et la complexité de l'environnement peuvent limiter l'analyse de l'incident.

Pourquoi est-ce une vulnérabilité ?

Ne pas superviser les événements de cybersécurité d'une installation 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 de mesure 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 ou les plans de reprise d'activité ne prennent pas forcément en compte les événements de cybersécurité. Les équipes opérationnelles disposent rarement de consignes pour réagir à un tel événement. La rédaction d'un plan de gestion de crise pour la perte du contrôle d'une installation due à un événement malveillant est rarement envisagée.

Pourquoi est-ce une vulnérabilité ?

La mise en place de consignes de réaction à des événements de sécurité permet de réduire le temps de réaction et de retour à une situation normale.

2.2.16 Non prise en compte de la cybersécurité dans les projets

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

Pourquoi est-ce une vulnérabilité ?

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 le cahier des charges. Augmenter le niveau de sécurité d'une installation existante est souvent plus compliqué et plus coûteux.

2.2.17 Absence de tests de cybersécurité

Les tests avant mise en service (FAT et SAT) 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.

Pourquoi est-ce une vulnérabilité ?

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

2.2.18 Absence de maîtrise des fournisseurs et prestataires

Dans les projets de système industriel, un audit du niveau de cybersécurité des fournisseurs et des prestataires est rarement envisagé. Aucune procédure d'échange sécurisé des informations n'est prévue non plus. La traçabilité des modifications lors des différentes phases du projet n'est pas prévue.

Pourquoi est-ce une vulnérabilité ?

Dans certains cas, il peut être plus aisé d'attaquer le fournisseur pour toucher le système industriel cible que d'attaquer le système cible directement.

2.2.19 Environnement de développement non sécurisé

Dans les projets de système industriel, l'environnement de développement est rarement dédié ou sécurisé, que ce soit en interne ou chez les fournisseurs. Par exemple, les machines de développement sont souvent également les machines de bureautique et sont donc connectées à Internet.

Pourquoi est-ce une vulnérabilité ?

L'utilisation d'un même environnement de travail pour des tâches d'exposition et de sensibilité différentes augmente les risques de compromission. Un environnement de développement non sécurisé, connecté à Internet par exemple, permettra à un attaquant ou un code malveillant de piéger les développements (firmware, programme automate, application SCADA, etc.)

2.2.20 Outils de développement présents

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 environnement de production et de développement. Mais cela peut également résulter de pratiques opérationnelles. Les stations d'ingénierie servent parfois de consoles de supervision en même temps.

Pourquoi est-ce une vulnérabilité ?

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 en apparence.

2.2.21 Non cloisonnement de l'administration

Les systèmes industriels ne présentent souvent pas de cloisonnement des machines d'administration. Souvent, ce sont les mêmes machines qui sont utilisées pour les applications SCADA et pour l'administration des équipements.

Pourquoi est-ce une vulnérabilité ?

Le défaut de cloisonnement 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 Définition des responsabilités

Les responsabilités en matière de cybersécurité sont souvent mal identifiées entre le fournisseur, l'intégrateur et l'entité responsable du système industriel. De même les responsabilités entre les directions métier et la DSI ne sont pas forcément claires non plus.

Pourquoi est-ce une vulnérabilité ?

Des responsabilités peu claires font courir le risque qu'une partie du système industriel ne soit sous la responsabilité de personne et ne reçoive donc pas les mesures de cybersécurité appropriées.

Chapitre 3

Mesures de sécurité organisationnelles

Les mesures organisationnelles présentées ci-dessous s'adressent à l'ensemble des acteurs impliqués sur les systèmes industriels (chefs de projet, acheteurs, automaticiens, intégrateurs, développeurs, équipes de maintenance, RSSI, etc.)

Important

Il revient à l'entité responsable de définir qui sera en charge de l'application des mesures de cybersécurité sur les installations.

Les mesures font référence aux chapitres de l'ISO 27002 [3] ainsi qu'aux recommandations du guide d'hygiène [14] et aux bonnes pratiques du guide sur la cybersécurité des systèmes industriels [10] publiées par l'ANSSI. Certaines mesures sont également abordées dans le guide de classification [13].

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

Références

Guide de classification : fait référence au guide de classification [13].
Vulnérabilité : fait référence aux vulnérabilités indiquées dans la section 2.2.
Guide SCADA : fait référence au guide sur les systèmes industriels [10].
Guide d'hygiène : fait référence au guide d'hygiène [14].
ISO 27002 : fait référence aux chapitres de l'ISO 27002 [3] abordant le sujet.

Les mesures sont indiquées en *recommandation* et notées **[R.x]** lorsqu'il s'agit d'un conseil. Elles sont indiquées en *directive* et notées **[D.x]** lorsqu'il s'agit d'une obligation. Les mesures sont cumulatives. Ainsi, une installation de classe 2 doit appliquer les mesures de classe 1 et une installation de classe 3 doit appliquer les mesures de classe 1 et de classe 2.

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 bonne défense, il est nécessaire d'avoir une connaissance très approfondie de son système, des risques encourus et des menaces à son encontre.

3.1.1 Rôles et responsabilités

Références

Guide de classification : 2.2.1
Vulnérabilité : 2.2.22
Guide SCADA : 2.3.1
ISO 27002 : 6.1.1

Classe 1

[R.1] Une chaîne de responsabilité de la cybersécurité devrait être mise en place. Elle devrait couvrir l'ensemble des systèmes.

[R.2] Les responsabilités pour la cybersécurité devraient être clairement définies pour chacune des parties prenantes quel que soit l'aspect concerné (développement, intégration, exploitation, maintenance, etc.).

Classe 2

[D.3] La recommandation R.1 devient une directive.

[D.4] La recommandation R.2 devient une directive.

Classe 3

[D.5] La directive D.3 est renforcée. L'identité et les coordonnées du responsable de la chaîne de responsabilité de la cybersécurité doivent être communiquées à l'autorité de cyberdéfense.

[D.6] La directive D.4 est renforcée. Les limites de responsabilité doivent être revues périodiquement et au moins une fois par an.

3.1.2 Cartographie

Références

Guide de classification : 2.2.3
Vulnérabilité : 2.2.4
Guide SCADA : BP09, BP02, 2.2.1
Guide d'hygiène : Règles 1 et 2
ISO 27002 : 8.1.1

Classe 1

[R.7] Il est recommandé de rédiger une cartographie :

- physique du système industriel ;
- logique du système industriel ;
- des applications (flux).

Classe 2

[D.8] Il est nécessaire d'établir une cartographie :

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

[R.9] La cartographie et la documentation du système industriel devraient être revues régulièrement, à chaque modification du système industriel et au moins une fois par an.

Classe 3

[D.10] La recommandation R.9 devient une directive.

Une description plus détaillée du contenu attendu pour une cartographie est disponible dans l'annexe A

Remarque

L'utilisation d'outils industriels comme les logiciels de Gestion de Maintenance Assistée par Ordinateur (GMAO) pour gérer les inventaires peut être utile. Cela permet de disposer de l'ensemble des informations dans une même base et de 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.

3.1.3 Analyse de risque

Références

Guide de classification : 2.2.2
Vulnérabilité : NA
Guide SCADA : 2.2.2
ISO 27002 : cf. ISO 27005

Remarque

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.

Classe 1

[R.11] Les systèmes industriels devraient faire l'objet d'une analyse de risque pour la cybersécurité, même succincte.

Classe 2

[D.12] Les systèmes industriels doivent faire l'objet d'une analyse de risque pour la cybersécurité suivant une méthode choisie par l'entité responsable.

Classe 3

[D.13] La directive D.12 est renforcée. L'analyse de risque devra être revue régulièrement, au moins une fois par an.

[R.14] L'analyse de risque devrait être réalisée en collaboration avec un prestataire labellisé.

3.1.4 Gestion des sauvegardes

Références

Vulnérabilité : 2.2.5
Guide SCADA : BP08
Guide d'hygiène : Règle 36
Ref ISO 27002 : 12.3

Classe 1

[R.15] Un plan de sauvegarde des données importantes devrait être mis en place afin de permettre leur restauration en cas d'incident.

[R.16] Les configurations devraient être sauvegardées avant et après toutes modifications, y compris lorsque celles-ci ont été apportées « à chaud ».

[R.17] Le processus de restauration des sauvegardes devrait être testé régulièrement. Il pourrait être testé sur un échantillon limité mais représentatif du système industriel dans son ensemble.

Périmètre d'application : Les données concernées sont toutes les données nécessaires à la reconstruction du système après un sinistre : les programmes, les fichiers de configuration, les firmwares, les paramètres de procédé (réglages d'asservissement par exemple), etc. Cela peut également concerner des données ayant un aspect réglementaire comme des exigences de traçabilité.

Classe 2

[D.18] Les recommandations R.15, R.16 et R.17 deviennent des directives.

Classe 3 Il n'y a pas d'exigence supplémentaire pour la classe 3.

3.1.5 Gestion de la documentation

Références

Vulnérabilité : 2.2.5
Guide SCADA : BP09
Ref ISO 27002 : 8.1.1

Classe 1

[R.19] Le niveau de sensibilité de la documentation devrait être défini et apparaître clairement sur les documents. Les documents devraient être traités en conséquence.

[R.20] L'ensemble des documents relatifs à la conception, à la configuration ou au fonctionnement du système industriel devraient être considérés comme sensibles.

[R.21] Les documents devraient être stockés dans un système d'information dont le niveau de sensibilité est adapté aux systèmes industriels.

> **Remarque**
>
> La documentation des systèmes industriels (analyses fonctionnelles, analyses organiques, plan d'adressage, etc.) est souvent stockée sur le système de gestion (bureautique) dont les exigences en matière de cybersécurité peuvent être plus faibles que pour les systèmes industriels. Les systèmes de gestion sont souvent la première cible des attaquants car ils permettent de collecter facilement de nombreuses informations en vue de préparer, par exemple, une attaque ciblée sur les systèmes industriels.

Classe 2

[R.22] La confidentialité de la documentation devrait être garantie.

[R.23] La documentation devrait être revue à intervalle régulier pour :

- s'assurer que les documents nécessaires existent bien,
- éliminer ceux qui ne servent plus.

Classe 3

[D.24] Les recommandations R.19, R.21 et R.22 deviennent des directives.

3.2 Maîtrise des intervenants

3.2.1 Gestion des intervenants

> **Références**
>
> Vulnérabilité : 2.2.2
> Guide SCADA : BP04
> Guide d'hygiène : Règle 3
> ISO 27002 : 15.1

Classe 1

[R.25] Des procédures de gestion des intervenants devraient être mises en place, notamment lors d'une arrivée ou d'un départ. Ces procédures devraient notamment traiter :

- la création et la destruction de comptes (cf 4.1),
- la gestion des accès aux locaux,
- la gestion des équipements mobiles (téléphones, tablettes, PC portables, etc),
- la gestion des documents sensibles.

[R.26] Un processus de gestion des compétences, afin de s'assurer que les intervenants disposent des compétences nécessaires pour leurs missions, devrait être mis en place. Ce processus devrait en particulier intégrer le transfert de compétences, en cas de départ ou de changement de poste, des personnes en charge des systèmes.

Classe 2

[D.27] Les recommandations R.25 et R.26 deviennent des directives.

Classe 3

[D.28] Une revue régulière des intervenants et de leurs comptes doit être effectuée, au minimum une fois par an.

Remarque

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

3.2.2 Sensibilisation et formation

Références

Guide de classification : 2.2.4
Vulnérabilité : 2.2.13
Guide SCADA : 2.2.1
Guide d'hygiène : Règle 39
ISO 27002 : 7.2.2

Classe 1

[R.29] Les intervenants devraient être habilités et formés à la cybersécurité.

[R.30] Une charte de bonne conduite devrait être mise en place et tous les intervenants devraient la signer lors de leur arrivée.

Classe 2

[D.31] Les recommandations R.29 et R.30 deviennent des directives.

Classe 3

[D.32] La directive D.31 est renforcée. La formation des intervenants est obligatoire **AVANT** toute intervention sur le système industriel.

[R.33] Les formations de cybersécurité devraient être dispensées par des prestataires labellisés.

[R.34] Les séances de formation et sensibilisation à la cybersécurité des systèmes industriels devraient être dispensées en même temps que les formations de sûreté et de sécurité du site.

3.2.3 Gestion des interventions

Références

Ref vulnérabilité : 2.2.6
Ref ISO 27002 : 12.1.2

Classe 1

[R.35] Une procédure de gestion des interventions devrait être mise en place afin de pouvoir identifier :

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

[R.36] L'ensemble des équipements matériels et logiciels utilisés pour les interventions sur les systèmes industriels devraient être recensés dans la gestion du parc afin d'être bien identifiés et maintenus à jour (cf R.7).

[R.37] L'autorisation d'intervention devrait être validée par l'entité responsable.

[R.38] Le processus d'intervention devrait être audité au minimum une fois par an afin de s'assurer du respect de la procédure.

> **Remarque**
>
> Ces éléments peuvent être intégrés aux permis de travail déjà en place et exigés pour certaines installations.

Classe 2

[D.39] Les recommandations R.35, R.36, R.37, et R.38 deviennent des directives.

[R.40] Pour les cas particuliers où l'intervenant apporte ses propres outils (des outils de diagnostic propres à l'équipementier par exemple), une procédure, même succincte, devrait être mise en place pour vérifier que les équipements de l'intervenant ont un niveau de sécurité satisfaisant.

Une telle situation ne devrait arriver qu'en cas d'absolue nécessité et doit rester exceptionnelle.

Classe 3

[D.41] L'utilisation d'outils particuliers hors d'un cadre prévu par la politique de sécurité du système industriel est interdite. La recommandation R.40 devient sans objet pour la classe 3.

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 une étape clé pour parvenir aux exigences attendues. Une attention particulière devra être portée à la cybersécurité lors des phases de conception du système industriel.

Il est conseillé de ne pas traiter le cybersécurité de manière isolée. Elle devrait 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 cahiers des charges

Références

Guide SCADA : 2.3.2 et 2.3.5
Vulnérabilité : 2.2.18
ISO 27002 : 15.1.2

Les projets peuvent être réalisés en interne ou être externalisés. Dans ce cas, il conviendra de préciser les exigences attendues dans les cahier des charges.

De manière plus générale, lorsqu'il est fait appel à une prestation extérieure, les exigences en matière de sécurité doivent être explicites et contractualisées.

Classe 1

[R.42] Les exigences identifiées lors de la phase de spécification devraient être intégrées au cahier des charges.

[R.43] Le cahier des charges devrait intégrer une clause exigeant la définition 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 (cf 3.1.1) ;
- la garantie du respect de la politique de cybersécurité ;
- la communication sur les divergences par rapport aux exigences et les autres non-conformités.

[R.44] Le cahier des charges devrait comprendre la liste des documents attendus avec notamment :

- une analyse de risque (cf 3.1.3) ;
- une analyse fonctionnelle ;
- une analyse organique ;
- un dossier d'exploitation et de maintenance ;
- une cartographie (cf 3.1.2).

[R.45] Le cahier des charges devrait contenir des clauses demandant des tests de cybersécurité, notamment lors des recettes usine et plateforme. La liste des tests demandés devrait suivre la recommandation R.71.

Classe 2

[D.46] Les recommandations R.42, R.43, R.44 et R.45 deviennent des directives.

[D.47] Le cahier des charges doit contenir une clause de confidentialité pour l'ensemble des informations du projet le nécessitant en précisant la durée de conservation des documents.

[R.48] Le cahier des charges devrait contenir une clause de révision régulière de l'analyse de risques. Le niveau de risque devrait être présenté régulièrement à l'entité responsable (par exemple pendant le comité de pilotage).

[R.49] Les documents de spécification fournis par le contractant devraient décrire de façon détaillée les moyens techniques, humains et organisationnels mobilisés afin de permettre leur traçabilité et de pouvoir vérifier leur niveau de cybersécurité.

[R.50] Le contractant devrait fournir un plan d'assurance sécurité décrivant toutes les mesures répondant aux exigences de cybersécurité demandées (cf [8]).

[R.51] Le contractant devrait utiliser un environnement de développement sécurisé (cf 4.3.6).

[R.52] Le contrat devrait intégrer une clause pour que l'entité responsable puisse auditer le contractant ou les fournisseurs afin de vérifier que l'ensemble des mesures de cybersécurité demandées sont bien appliquées.

Classe 3

[D.53] Les recommandations R.48, R.49, R.50, R.52 et R.51 deviennent des directives.

[R.54] Le cahier des charges devrait contenir une clause exigeant la fourniture d'équipements matériels et logiciels labellisés sur le plan de la cybersécurité.

[R.55] Le cahier des charges devrait exiger des concepteurs de logiciels une démonstration que leurs processus de développement emploient des méthodes d'ingénierie à l'état de l'art, des processus de contrôle qualité et des techniques de validation afin de réduire les défaillances logicielles et les vulnérabilités.

[R.56] Afin de faciliter l'application de la recommandation R.55, le contractant devrait être labellisé.

3.3.2 Intégration de la cybersécurité dans les phases de spécification

Références

Vulnérabilité : 2.2.16
Guide SCADA : 2.3.2
ISO 27002 : 14.1.1

Classe 1

[R.57] Les exigences techniques devraient intégrer l'ensemble des mesures techniques présentées dans le chapitre 4. À titre d'exemple, la conception devrait prendre en compte :

- la nécessité d'authentifier les intervenants (cf 4.1) ;
- la nécessité de définir une architecture sécurisée (cf 4.2) ;
- la nécessité de sécuriser les équipements (cf 4.3) ;
- la nécessité de pouvoir requalifier un système suite à des mises à jour de sécurité.

[R.58] Des procédures et des moyens techniques devraient être définis pour permettre des opérations de maintenance préventive et curative afin de maintenir le niveau de cybersécurité dans la durée.
Par exemple, des modes dégradés pourraient être prévus pour réaliser des mises à jour. On pourra, par exemple, configurer les sorties d'un automate pour qu'elles restent sur leurs derniers états, pendant la mise à jour de son firmware.

[R.59] La définition de la localisation des équipements devrait prendre en compte leur sécurité physique.

[R.60] Les spécifications du projet devraient exiger que les opérations non indispensables à la conduite du système industriel soient effectuées sur un autre système d'information. Les équipements et logiciels associés ne devraient pas être présents sur le système industriel. À titre d'exemple, des postes bureautiques non connectés au système industriel devraient être prévus pour permettre la consultation de la documentation, le remplissage de feuilles de suivi, etc.

Classe 2

[D.61] Les recommandations R.57, R.59 et R.60 deviennent des directives.

[R.62] La conception devrait intégrer des outils et mécanismes pour gérer la sécurité et faciliter les exigences telles que :

— la maîtrise de la configuration (cf 3.3.6) ;

— le durcissement des configurations (cf 4.3.1) ;

— la gestion des vulnérabilités (cf 4.3.2).

Classe 3

[D.63] La recommandation R.62 devient une directive.

3.3.3 Intégration de la cybersécurité dans les phases de conception

Références

Vulnérabilité : 2.2.16
Guide SCADA : 2.3.2
ISO 27002 : 14.1.1

Classe 1

[R.64] Lors de la conception, les interfaces et la complexité du système devraient être limitées au maximum afin de limiter l'introduction de vulnérabilités lors de l'implémentation.

[R.65] Les caractéristiques de cybersécurité des équipements (mécanismes d'authentification, ségrégation des droits, etc.) devraient être intégrées au processus de choix de ceux-ci.

[R.66] Des rôles devraient être définis pour les intervenants. Ces rôles devraient être intégrés dans la gestion des droits des comptes informatiques. Les rôles devraient correspondre strictement aux missions de chacun (politique des moindres privilèges). En particulier, les utilisateurs et les administrateurs devraient être distingués (cf 4.1.1).

Classe 2

[D.67] Les recommandations R.65 et R.66 deviennent des directives.

Classe 3 Il n'y a pas de mesure supplémentaire pour la classe 3.

3.3.4 Audits et tests de cybersécurité

Références

Guide classification : 2.2.5
Guide SCADA : 2.3.2
Vulnérabilité : 2.2.17
Guide d'hygiène : Régle 40
ISO 27002 : 12.7

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. Ceux-ci peuvent être intégrés aux phases de maintenance et de tests fonctionnels.

Classe 1

[R.68] Des audits devraient être mis en place régulièrement. Ces audits pourront être internes.

[R.69] L'audit doit être suivi d'un plan d'action validé et suivi par l'entité responsable.

Classe 2

[D.70] Les recommandations R.68 et R.69 deviennent des directives et sont renforcées par la recommandation R.71 ci-après.

[R.71] Un programme d'audit devrait être mis en place avec les éléments suivant :

- des tests aux limites ;
- des tests d'erreur des fonctions métier ;
- des tests de la vérification et de la gestion des exceptions ;
- le déroulement de scénarios de menace (tests de pénétration et tentatives de prise de contrôle) ;
- la vérification des mécanismes de sécurité (déploiement de correctifs, analyse de journaux d'événements, restauration de sauvegarde, etc.) ;
- l'évaluation des performances du système.

Important

Les tests de pénétration pouvant entraîner des défaillances, ils doivent être exécutés dans le cadre de maintenance ou avant la mise en production des systèmes.

[R.72] Les audits devraient être réalisés par des prestataires externes labellisés.

Classe 3

[D.73] La recommandation R.71 devient une directive.

[D.74] Les audits devront être effectués au moins une fois par an.

3.3.5 Transfert en exploitation

Références

Guide classification : 2.3
Guide SCADA : 2.3.2

Remarque

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

Classe 1

[R.75] Avant de mettre en exploitation un système il faudrait :

- établir un état des lieux exhaustif du niveau de cybersécurité du système ;
- s'assurer des moyens disponibles pour le maintenir à un niveau acceptable.

Classe 2

[D.76] Les systèmes industriels doivent être homologués par l'entité responsable.

Classe 3

[D.77] Les systèmes industriels doivent être homologués et requièrent une autorisation préalable de mise en service. L'homologation doit être faite par un organisme extérieur.

3.3.6 Gestion des modifications et évolutions

Références

Guide SCADA : BP07
ISO 27002 : 14.2.2

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

Classe 1

[R.78] Des outils devraient être utilisés pour contrôler rapidement les différences entre la version courante et la version à installer et s'assurer que seules les modifications nécessaires et demandées ont été appliquées.

[R.79] Les mises à jour et modifications apportées aux systèmes devraient être tracées.

Classe 2

[D.80] La recommandation R.79 devient une directive.

[R.81] Un processus de vérification des versions de programme en cours d'exécution par rapport à une version de référence devrait être mis en place. Cela permet de s'assurer que les configurations exécutées par le système industriel (les automates, les SCADA, etc.) sont bien les bonnes.

[R.82] Les modifications devraient être évaluées dans un environnement de test au préalable.

Classe 3

[D.83] La recommandation R.78 devient une directive. Les impacts des modifications doivent être validés par l'entité responsable avant mise en production.

[D.84] Les recommandations R.81 et R.82 deviennent des directives.

3.3.7 Processus de veille

Références

Guide de classification : 2.2.6
Vulnérabilité : 2.2.1
Guide SCADA : 2.2.6
ISO 27002 : 12.6

Classe 1

[R.85] Un processus de veille sur les menaces et vulnérabilités devrait être mis en place.

Remarque

Ce processus devrait notamment reposer sur les sources ouvertes disponibles telles que les CERT nationaux (CERT-FR, ICS-CERT), les CERT des équipementiers et des développeurs de logiciels.

Classe 2

[D.86] La recommandation R.85 devient une directive.

[R.87] La diffusion, par les fournisseurs, des bulletins de vulnérabilité pour l'ensemble des équipements matériels et logiciels utilisés dans le système industriel devrait être contractualisée.

[R.88] Un processus de veille sur l'évolution des techniques de protection devrait être mis en place. Il pourrait être basé également sur des sources ouvertes disponibles comme le site web de l'ANSSI.

Classe 3

[D.89] Les recommandations R.85, R.87 et R.88 deviennent des directives.

[D.90] Un processus de veille sur l'évolution des techniques d'attaque et sur l'évolution de la menace doit être mis en place. En cas d'évolution importante, une réévaluation de l'analyse de risque doit être engagée.

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 en phase d'obsolescence peuvent contenir de nom-

breuses vulnérabilités qui ne seront jamais corrigées. La gestion de l'obsolescence est un processus pouvant donc être utile et nécessaire pour la gestion des vulnérabilités.

Références

Vulnérabilité : 2.2.1

Classe 1

[R.91] Des clauses relatives à la gestion de l'obsolescence des équipements et logiciels, en indiquant par exemple la date à laquelle ils ne seront plus pris en charge, devraient être intégrées dans les contrats avec les fournisseurs.

[R.92] Un plan de gestion de l'obsolescence pour remplacer les équipements et applications obsolètes devrait être mis en place.

Classe 2

[D.93] La recommandation R.91 devient une directive.

Classe 3 Il n'y a pas de mesure complémentaire pour cette classe.

3.4 Sécurité physique et contrôle d'accès aux locaux

3.4.1 Accès aux locaux

Références

Vulnérabilité : 2.2.8
Guide d'hygiène : Règles 32 et 33
ISO 27002 : 11.1

Classe 1

[R.94] Une politique de contrôle d'accès physique devrait être définie. Cette politique devrait notamment prévoir de :

- récupérer les clés ou badges d'un employé à son départ (cf R.25) ;
- changer régulièrement les codes de l'alarme de l'entreprise ;

— ne jamais donner de clé ou de code d'alarme à des prestataires extérieurs sauf s'il est possible de tracer les accès et de les restreindre à des plages horaires données.

[R.95] Les accès aux locaux devraient être journalisés et auditables.

Classe 2

[D.96] La recommandation R.94 devient une directive.

[R.97] Les mécanismes de contrôle d'accès devraient être robustes. On pourra se reporter au guide de l'ANSSI sur le sujet [9].

[R.98] Les accès devraient être mis sous vidéoprotection.

[R.99] L'accès aux équipements devrait être strictement réservé aux personnes habilitées.

Classe 3

[D.100] Les recommandations R.95, R.97, R.98 et R.99 deviennent des directives.

[D.101] Un système de détection d'intrusion devra être mis en œuvre pour les zones vitales, en particulier celles non occupées 24 heures sur 24.

3.4.2 Accès aux équipements et aux câblages

Références

Vulnérabilité : 2.2.8
Guide d'hygiène : Règle 34
Guide SCADA : BP01
ISO 27002 : 11.2

Classe 1

[R.102] Les serveurs devraient être installés dans des locaux fermés sous contrôle d'accès (si possible dans des salles informatiques).

[R.103] Les unités centrales des stations, les équipements réseaux industriels et les automates devraient être placés dans des armoires fermées à clé.

[R.104] Des prises d'accès au système industriel ne devraient pas être accessibles dans les endroits ouverts au public.

Classe 2

[D.105] Les recommandations R.102, R.103 et R.104 deviennent des directives.

[D.106] La recommandation R.104 est renforcée par la directive suivante : les prises d'accès au système industriel ne doivent pas être accessibles dans les zones sans surveillance.

[R.107] L'intégrité physique des câbles devrait être protégée (par exemple : un capotage).

[R.108] Lorsqu'elles ne sont pas utilisées, les prises dédiées à la maintenance devraient être obturées (bouchons, plaques d'occultation...). Le retrait de l'obturateur suit une procédure bien définie et est soumis à autorisation préalable.

[R.109] Un dispositif de détection d'ouverture, avec remontée d'alarme, devrait être mis en place sur les armoires des équipements sensibles. A minima, sur les coffrets extérieurs contenant des composants sensibles, un moyen de contrôle visuel, comme la pose de scellés par exemple devrait être installé. Le retrait de ces moyens visuels devrait suivre une procédure bien définie et être soumis à autorisation préalable.

Classe 3

[D.110] Les recommandations R.104, R.108 et R.109 deviennent des directives.

3.5 Réaction en cas d'incident

3.5.1 Plan de reprise ou de continuité d'activité

Un plan de reprise ou de continuité d'activité permet de garantir la reprise ou la continuité du service suite à un sinistre, quelle qu'en soit l'origine. Ce plan de continuité d'activité, parfois déjà existant pour répondre à des sinistres d'origine autre que la cybersécurité devra 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, on pourra se reporter au guide édité par le SGDSN [2].

Références

Guide de classification : 2.2.7
Vulnérabilité : 2.2.15
Guide SCADA : 2.2.7
Guide d'hygiène : Règle 36
ISO 27002 : 17.1

Classe 1

[R.111] Un plan de sauvegarde des données sensibles devrait être mis en place afin de pouvoir reconstruire le système après sinistre (cf 3.1.4).

[R.112] Les plans de reprise et de continuité d'activité devraient intégrer les incidents de cybersécurité.

Classe 2

[R.113] Les plans de reprise et de continuité d'activité devraient être testés régulièrement et au moins une fois par an.

Classe 3

[D.114] Les recommandations R.111, R.112 et R.112 deviennent des directives.

3.5.2 Modes dégradés

Classe 1

[R.115] Les procédures d'intervention devraient intégrer un mode d'urgence (« procédure bris de glace ») pour pouvoir intervenir rapidement en cas de besoin sans dégrader significativement le niveau de cybersécurité du système industriel. En particulier, cette procédure d'urgence ne devrait pas affecter la traçabilité des interventions.

[R.116] Les systèmes devraient intégrer des modes dégradés leur permettant soit de s'arrêter sans provoquer de dégâts (materiel ou humain), soit de continuer à fonctionner par un pilotage en mode « manuel ».

Classe 2 Il n'y a pas de mesure supplémentaire pour cette classe.

Classe 3

[D.117] Les recommandations R.115 et R.116 deviennent des directives.

3.5.3 Gestion de crise

Références

Guide de classification : 3.5.3
Vulnérabilité : 2.2.15
Guide SCADA : 2.2.5
Guide d'hygiène : Règles 37 et 38
ISO 27002 : 17.1

Classe 1

[R.118] Un processus de gestion de crise devrait être mis en place. Celui-ci devrait permettre de déterminer :

- que faire lors de la détection d'un incident ;
- qui alerter ;
- qui est la personne qui doit coordonner les actions en cas de crise ;
- quelles sont les premières mesures à appliquer.

[R.119] Le processus de gestion de crise devrait également contenir une procédure d'escalade pour gérer les incidents au bon niveau de responsabilité et décider en conséquence :

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

[R.120] La gestion de crise devrait également 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.

Remarque

Une note de l'ANSSI décrit les bons réflexes en cas d'intrusion sur un système d'information [4].

Classe 2

[R.121] Les procédures de gestion de crise devraient être testées régulièrement et au moins une fois par an.

Classe 3

[D.122] Les recommandations R.118, R.119, R.120 et R.121 deviennent des directives.

Chapitre 4

Mesures de sécurité techniques

Ce chapitre regroupe l'ensemble des mesures techniques s'adressant à l'ensemble des acteurs impliqués sur les systèmes industriels (chefs de projet, acheteurs, automaticiens, intégrateurs, développeurs, équipes de maintenance, RSSI, etc.).

Important

Il revient à l'entité responsable de définir qui sera en charge de l'application des mesures sur les installations.

Les mesures sont indiquées en *recommandation* et notées **[R.x]** lorsqu'il s'agit d'un conseil. Elles sont indiquées en *directive* et notées **[D.x]** lorsqu'il s'agit d'une obligation. Les mesures sont cumulatives. Ainsi, une installation de classe 3 doit appliquer les mesures de classe 1 et de classe 2.

Les mesures font référence aux chapitres de l'ISO 27002 [3] ainsi qu'aux recommandations du guide d'hygiène [14] et aux bonnes pratiques du guide sur la cybersécurité des systèmes industriels [10] publiées par l'ANSSI. Certaines mesures sont également abordées dans le guide de classification [13].

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

Références

Guide de classification : fait référence au guide de classification [13].
Vulnérabilité : fait référence aux vulnérabilités indiquées dans la section 2.2.
Guide SCADA : fait référence au guide sur les systèmes industriels [10].
Guide d'hygiène : fait référence au guide d'hygiène [14].
ISO 27002 : fait référence aux chapitres de l'ISO 27002 [3] abordant le sujet.

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. Par défaut, le périmètre comprend les équipements suivants :

Les équipements sur lesquels peuvent porter les mesures sont :

- les serveurs, stations et postes de travail ;
- les stations d'ingénierie et consoles de programmation ;
- les équipements mobiles : ordinateurs portables, tablettes, ordiphones, etc. ;
- les logiciels et applications de supervision (SCADA) :
- les logiciels et applications de GPAO et de MES si existants ;
- les interfaces homme-machine (écrans tactiles) ;
- les automates et unités déportées (RTU) ;
- les équipements réseau (commutateurs, routeurs, pare-feu, bornes d'accès sans fil) ;
- les capteurs et actionneurs intelligents ;
- …

Cette liste est un exemple et doit être adaptée au contexte de chaque système.

Important

Certaines exigences font appel à des mécansimes cryptographiques (chiffrement, signature, authentification, etc.). Ces mécanismes devront être conformes aux annexes B du référentiel général de sécurité [6].

4.1 Authentification des intervenants : contrôle d'accès logique

4.1.1 Gestion des comptes

Références

Vulnérabilité : 2.2.2
Guide SCADA : BP04
Guide d'hygiène : Règles 8, 20 et 30
ISO 27002 : 9.1

Les comptes peuvent être de différents types :

— les comptes « de session » permettant l'accès aux machines Windows et Linux ;

— les comptes « applicatifs » permettant à un intervenant de se connecter à une application SCADA par exemple. Ces comptes sont souvent gérés par l'application elle-même ;

— les comptes « systèmes » utilisés pour qu'une application puisse s'exécuter et communiquer avec d'autres applications (exemple : compte de service). Ces comptes ne sont normalement pas utilisés par un intervenant.

Les comptes peuvent disposer de différents niveaux de privilèges. En particuliers, les comptes de niveau « administrateur » se découpent en deux catégories :

— les comptes de privilèges élevés « administrateur système » permettant l'administration informatique des équipements (serveurs, stations et équipements réseau par exemple) et des systèmes d'exploitation ;

— les comptes de privilège élevés « ingénieur de procédé » permettant d'accéder à des fonctions de configuration ou de programmation des applications SCADA et automates par exemple.

Remarque

Pour des questions de facilité, les comptes sont souvent mélangés alors qu'ils devraient être bien séparés. Un « ingénieur de procédé » n'a pourtant pas besoin d'être « administrateur système ». Il s'agit d'une mauvaise pratique.

Classe 1

[R.123] Chaque utilisateur devrait être identifié de manière unique.

[R.124] Tous les comptes disposant de privilèges importants comme les comptes administrateurs devraient être protégés par un mécanisme d'authentification comme un mot de passe par exemple. Les comptes utilisateurs et administrateurs devraient être strictement séparés.

[R.125] Les comptes génériques, en particulier ceux disposant de privilèges importants sont déconseillés.

Lorsqu'ils sont indispensables, leur utilisation devra être limitée à des usages très précis et être documentée.

[R.126] Des rôles devraient être définis, documentés et implémentés pour que les comptes des utilisateurs aient des privilèges correspondant exactement à leurs missions.

[R.127] Un audit des d'événements liés à l'utilisation des comptes devrait être mis en place.

[R.128] Les comptes appartenant à des personnels n'intervenant plus sur le système industriel devraient être supprimés ou, a minima, désactivés (cf R.25).

Classe 2

[D.129] Les recommandations R.123, R.124 et R.125 deviennent des directives. Les comptes par défaut et génériques ne doivent pas être utilisés sauf contrainte opérationnelle forte. Les comptes disposant de privilèges comme les comptes administrateurs ne doivent pas être des comptes génériques et doivent être distincts des comptes utilisateurs.

[D.130] La recommandation R.126 devient une directive. De plus, les comptes avec privilèges devront être validés par le responsable hiérarchique de l'utilisateur.

[D.131] La recommandation R.128 devient une directive et complète la directive D.27.

[R.132] Une revue annuelle des comptes utilisateurs devrait être mise en place. Elle pourrait notamment permettre de vérifier la bonne application des directives D.129 et D.130 et de la directive D.131. Cette revue devrait porter une attention particulière aux comptes d'administration.

[R.133] Lorsque cela est possible, un accès en lecture seule devrait être configuré pour les interventions de maintenance de premier niveau.

[R.134] Si la gestion des comptes est centralisée, la configuration de l'annuaire centralisé devra être auditée régulièrement et au moins une fois par an. Pour le cas de l'Active Directory, on pourra se reporter à l'article [1].

Important

Une solution centralisée (comme par exemple Active Directory, LDAP, etc.) peut faciliter la gestion des comptes et droits des intervenants. Ce type de solution peut également créer un point de vulnérabilité unique et doit donc être étudié avec le plus grand soin.

Classe 3

[D.135] Les recommandations R.127, R.132 et R.134 deviennent des directives.

4.1.2 Gestion de l'authentification

Références

Vulnérabilité : 2.2.2
Guide SCADA : BP04
Guide d'hygiène : Règles 9, 10, 11, 12 et 13.
ISO 27002 : 9.1

Classe 1

[R.136] Les différents composants (équipements et logiciels) ne doivent être accessibles qu'après une authentification avec identifiant et mot de passe. Lorsque cela est possible, la politique de mots de passe doit répondre a minima aux exigences suivantes :

— les mots de passe doivent être robustes (cf. [12]) ;

— les mots de passe par défaut doivent être changés.

[R.137] Une temporisation d'inhibition doit être privilégiée par rapport au blocage en cas d'échec d'authentification.

[R.138] Le mot de passe doit être protégé en confidentialité et en intégrité quand celui-ci est transmis sur le réseau.

[R.139] Dans le cas où une authentification ne peut pas être appliquée, du fait de contraintes opérationnelles notamment, des mesures compensatoires devraient être définies et documentées. A titre d'exemple, on pourra 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 ;

— etc.

Exemple

Dans une salle de contrôle opérationnelle en 24/7, les intervenants ont besoin de pouvoir agir vite sur les applications SCADA. Des comptes individuels peuvent être inadaptés. Il peut être envisageable dans ce cas 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.

[R.140] Les fichiers contenant les mots de passe ou leur empreinte devraient être conservés de manière à assurer leur confidentialité et leur intégrité.

[R.141] Une procédure sécurisée pour la réinitialisation des mots de passe en cas de perte devrait être définie.

Classe 2

[D.142] Les recommandations R.138, R.139 et R.140 deviennent des directives.

[R.143] Lorsque cela est possible, une authentification forte (carte à puce, OTP, etc.) devrait être mise en place sur les postes de travail et serveurs. Cette mesure peut être étendue aux équipements de terrain le permettant (automates, entrées/sorties déportées), etc.

[R.144] Lorsque la recommandation R.143 ne peut pas être appliquée, la politique de mots passe de la recommandation R.136 devrait être renforcée par :

- conservation de l'historique des mots de passe (par exemple les 5 derniers) ;
- la vérification technique de la complexité du mot de passe ;
- le renouvellement du mot de passe (par exemple au bout de 90 jours).

Remarque

Certains outils permettent de vérifier au moment de la définition d'un nouveau mot de passe s'il n'est pas trop proche des anciens. L'idée peut paraître séduisante car il est souvent aisé de deviner un mot de passe donné à partir de la connaissance des autres mots de passe de l'utilisateur. Cependant, cette technique nécessite de conserver un historique des mots de passe en clair, ce qui peut être dangereux. L'historisation simple peut être faite en ne conservant que les empreintes.

[R.145] La journalisation des événements de sécurité doit enregistrer les échecs d'authentification et les authentifications réussies des comptes à privilèges.

Classe 3

[D.146] Les recommandations R.136, R.144 et R.145 deviennent des directives.

[D.147] La recommandation R.143 devient une directive pour les équipements exposés (postes de travail, ordinateurs portables, stations d'ingénierie, consoles de programmation, pare-feu, VPN, etc.)

4.2 Sécurisation de l'architecture du système industriel

4.2.1 Cloisonnement des systèmes industriels

Références

Guide de classification : 2.2.10
Vulnérabilité : 2.2.9
Guide SCADA : BP02
Guide d'hygiène : Règles 21, 25 et 29
ISO 27002 : 13.1.3

Classe 1

[R.148] Les systèmes industriels devraient être découpés par zones fonctionnelles ou zones techniques cohérentes. Ces zones devraient être cloisonnées entre elles.

[R.149] Une politique de filtrages entre les zones devrait être mise en place. Pour définir une politique de filtrage, on pourra notamment se reporter au guide sur les pare-feu de l'ANSSI [11].

Pour les flux utilisant le protocole IP, on en rappelle néanmoins ici quelques grands principes :

- 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 rejetés doivent être journalisés et analysés ;

— tous les flux entrants ou sortants du système industriel doivent être journalisés.

Exemple

A titre d'exemple, on rappelle quelques exemples de protocoles et de ports utilisés par les protocoles industriels :

Modbus : TCP/502

S7 : TCP/102

EthernetIP : TCP/44818 et UDP/2222

OPCUA : TCP/4840

Profinet IO : TCP/UDP 34962, 34963, 34964

[R.150] Lorsque des flux non-IP doivent transiter entre deux zones distinctes, un filtrage devrait être effectué sur les identifiants source et destination. Par exemple, dans le cas d'Ethernet, on pourra effectuer le filtrage sur les adresses MAC source et destination.

Par ailleurs, on pourra faire un filtrage sur les protocoles autorisés.

[R.151] Autant que possible, un cloisonnement physique devrait être privilégié entre les zones fonctionnelles du système industriel. Indépendamment de la cybersécurité, le cloisonnement physique participe également à renforcer la disponibilité des systèmes.

[R.152] Lorsque une séparation physique n'est pas possible entre les zones fonctionnelles du système industriel, un cloisonnement logique devrait être mis en place. L'utilisation des VLAN est un exemple de cloisonnement logique possible.

[R.153] Le réseau d'administration des équipements devrait être cloisonné des autres réseaux, a minima de manière logique. Le périmètre porte sur les équipements d'informatique classique comme les commutateurs, passerelles, routeurs, pare-feu, etc.

[R.154] Les postes d'administration ne devraient pas avoir d'autre usage. Ils ne devraient pas être connectés à Internet ni à un réseau de gestion.

Remarque

Les VLAN n'ont pas été conçus comme un mécanisme de sécurité. Leur configuration devra être faite avec soin pour assurer le cloisonnement de manière effective.

Exemple

Voici un exemple de cloisonnement logique :

- 1 VLAN d'administration pour les composants réseau, les postes de travail d'administration et les serveurs d'administration ;
- 1 VLAN de serveurs ;
- 1 VLAN des postes de conduite ;
- 1 VLAN des postes de développement ;
- 1 VLAN par procédé contenant les automates et autres équipements associés (entrées/sorties déportées, etc.).

Classe 2

[D.155] Les recommandations R.148, R.149, R.150, et R.151 deviennent des directives.

[D.156] Les recommandation R.153 et R.154 deviennent des directives. Il est possible que certains équipements, notamment d'ancienne génération, ne permettent pas techniquement de réaliser un tel cloisonnement. Dans ce cas, une analyse spécifique devra être menée pour étudier les contre-mesures possibles et définir le niveau de risque résiduel.

[R.157] Les flux devraient être unidirectionnels entre les systèmes industriels de classe 2 et les systèmes industriels de classe 1. L'unidirectionnalité des flux pourra être assurée par un pare-feu.

[R.158] Les réseaux d'administration des équipements devraient être cloisonnés physiquement des autres réseaux. A minima, ils devraient être séparés logiquement à l'aide de tunnels VPN. L'utilisation de produits qualifiés pour l'établissement de ces tunnels est recommandée.

Classe 3

[D.159] Les flux doivent être unidirectionnels entre des zones de classe 3 et de classe inférieure. L'unidirectionnalité est assurée physiquement par une diode.

[R.160] La diode devrait être labellisée.

[D.161] Les systèmes industriels de classe 3 doivent être physiquement séparés des systèmes de classe inférieure. L'utilisation de cloisonnement logique est interdite.

Important

Des PLC sont parfois configurés avec deux coupleurs Ethernet différents pour séparer les flux, un pour les communications avec les SCADA et l'autre pour les communications avec les équipements de procédé par exemple. Cette mesure peut répondre à des besoins de sûreté de fonctionnement mais ne constitue pas une protection contre certaines attaques. En effet, l'étanchéité entre les deux coupleurs Ethernet n'est pas garantie.

4.2.2 Interconnexion avec le système d'information de gestion

Références

Guide de classification : 2.2.10
Vulnérabilité : 2.2.9
Guide SCADA : BP02
Guide d'hygiène : Règles 21, 29
ISO 27002 : 13.1

Le système d'information de gestion et ses réseaux sont considérés par défaut de classe 1.

Classe 1

[R.162] L'interconnexion devrait être protégée par un dispositif de filtrage (pare-feu).

[R.163] Les flux devraient être limités au strict minimum.

[R.164] Une politique de filtrage telle que celle décrite dans la recommandation R.149 devrait être mise en place.

Classe 2

[D.165] Les recommandations R.162, R.163 et R.164 deviennent des directives.

[R.166] Les flux sont unidirectionnels depuis le système industriel de classe 2 vers le système d'information de gestion. L'unidirectionnalité des flux pourra être assurée par un pare-feu.

Classe 3

[D.167] Les flux doivent être unidirectionnels entre les systèmes industriels et les systèmes de gestion. L'unidirectionnalité devra être assurée physiquement par une diode.

[R.168] La diode devrait être labellisée.

4.2.3 Accès Internet et interconnexions entre sites distants

Références

Guide de classification : 2.2.10
Vulnérabilité : 2.2.9
Guide SCADA : BP02
Guide d'hygiène : Règles 4, 24
ISO 27002 : 9.4

Classe 1

[R.169] Les accès vers Internet depuis le système industriel devraient être limités. En particulier, l'ensemble des postes de supervision et des équipements de terrain ne devraient pas avoir d'accès à Internet.

[R.170] Réciproquement, les accès depuis Internet vers le système industriel devraient être limités.

[R.171] Les interconnexions entre des systèmes répartis sur des localisations différentes devraient garantir la confidentialité, l'intégrité et l'authenticité des communications. On pourra utiliser un VPN IPsec par exemple.

[R.172] Un dispositif de filtrage (pare-feu) devrait être mis en place au niveau des passerelles d'interconnexion.

[R.173] Les passerelles d'interconnexion devraient être configurées de manière sécurisée. On pourra se reporter au guide de l'ANSSI [7].

Classe 2

[D.174] Les recommandations R.169, R.170, R.171, R.172 deviennent des directives.

[R.175] Les équipements utilisés pour l'interconnexion devraient être labellisés.

Classe 3

[D.176] Une interconnexion directe entre un système industriel de classe 3 et un réseau public ne doit pas être autorisée.

4.2.4 Accès distants

Références

Ref vulnérabilité : 2.2.10
Réf guide d'Hygiène : Règle 18
Ref ISO 27002 : 9.4

Télédiagnostic, télémaintenance et télégestion

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

La télémaintenance est l'action d'effectuer à distance, sous-entendu depuis l'extérieur des bâtiments dans lesquels se trouve le système industriel, en passant potentiellement par des réseaux non-maîtrisés, des tâches de maintenance sur des installations techniques. Cela implique de pouvoir faire des modifications de paramètres.

La télégestion consiste à prendre le contrôle à distance du système industriel et à pouvoir en faire la gestion complète. Si la télégestion est utilisée, les équipements utilisés pour ce faire doivent être intégrés au périmètre du système industriel. L'ensemble des mesures de sécurité doivent donc également s'appliquer à l'ensemble du système.

Classe 1

[R.177] Lorsque des opérations de télégestion, télémaintenance ou télédiagnostic sont nécessaires, les règles suivantes devraient être appliquées :

- les connexions devraient être faites à la demande de l'entité responsable ;
- l'équipement de connexion distant devrait être authentifié ;
- le mot de passe de connexion devrait être changé régulièrement ;
- la journalisation devrait être activée ;
- après un délai précis d'inactivité, la connexion devrait être fermée ;

— l'équipement devrait être cloisonné et seuls les flux requis devraient être autorisés entre l'équipement et le reste du système industriel ;

— les opération de télémaintenance ne devraient être faites qu'à l'aide de protocoles sécurisés, assurant notamment l'intégrité et l'authenticité des échanges.

[R.178] Dans le cas d'une connexion par modem n'offrant pas de système d'authentification robuste, a minima, un système de rappel (call-back) devrait être utilisé pour valider le numéro de téléphone appelant.

[R.179] L'équipement de connexion utilisé pour la télémaintenance devrait être labellisé.

Classe 2

[D.180] La solution de télémaintenance doit suivre les règles suivantes :

— elle doit assurer la confidentialité, l'intégrité et l'authenticité des communications (exemple : VPN IPsec) ;

— une authentification forte à deux facteurs doit être mise en place ;

— les équipements de connexion doivent être cloisonnés du reste du système industriel et seuls les flux indispensables à la télémaintenance doivent être autorisés ;

— la journalisation des événements de sécurité doit être activée.

[R.181] Une sonde de détection devrait être déployée au niveau de la passerelle de connexion pour pouvoir analyser l'ensemble du trafic entrant et sortant (cf R.279).

Classe 3

[D.182] La télémaintenance ne doit pas être autorisée. Si des opérations de télémaintenance étaient impérativement nécessaires, les équipements distants et la liaison doivent être intégrés au périmètre du système de classe 3. L'ensemble des mesures de classe 3 doivent leur être appliquées et en particulier celles de la section 4.2.5.

[D.183] Des solutions de télédiagnostic peuvent être mises en place. Dans ce cas, la solution doit mettre en place les mesures suivantes :

— la connexion distante ne se fera que sur un serveur cloisonné ;

— les données nécessaires au télédiagnostic seront poussées sur ce serveur au travers d'une diode. Cette diode devrait être labellisée.

4.2.5 Systèmes industriels distribués

Un système industriel est considéré comme distribué dès lors que des mesures de protection physique ne sont pas applicables à l'ensemble des équipements et liens le composant.

Classe 1

[R.184] L'ensemble des flux transitant par des réseaux non-protégés physiquement ou non-maîtrisés devraient utiliser des protocoles sécurisés. Ils devraient être protégés en confidentialité, en intégrité et authentifiés.

[R.185] Lorsque cela est possible des passerelles VPN devraient être déployées aux extrémités des liaisons pour protéger l'intégralité du trafic.

L'équipement devrait être positionné derrière un pare-feu ne laissant passer que les flux strictement indispensables. En particulier, le trafic externe au VPN devrait être bloqué.

[R.186] Pour les liaisons ayant des besoins de disponibilité, l'utilisation de réseaux publics comme Internet devrait être évitée. L'utilisation de liaisons louées avec des ressources dédiées devrait être privilégiée.

[R.187] Les équipements utilisés dans la recommandation R.185 devraient être labellisés.

Classe 2

[D.188] Les recommandations R.185 et R.186 deviennent des directives.

[R.189] 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. (cf R.279).

Classe 3

[D.190] L'utilisation de liaisons sur des réseaux publics ne doit pas être autorisée.

[D.191] La recommandation R.189 devient une directive.

4.2.6 Communications sans fil

Références

Vulnérabilité : 2.2.8
Guide d'hygiène : Règle 22
ISO 27002 : 13.1

Remarque

Dans certains cas, l'utilisation de réseau sans fil peut être un secours à l'utilisation des réseaux publics filaires.

Classe 1

[R.192] L'usage de technologies sans fil devrait être limité au strict nécessaire.

[R.193] En fonction de l'usage, les flux de données devraient être chiffrés et signés ou seulement signés.

[R.194] Les points d'accès sans fil devraient mettre en place les mécanismes suivants :

- l'authentification du point d'accès et du dispositif qui se connecte à l'infrastructure ;
- les fonctionnalités de contrôle d'accès réseau (ex : EAP) ;
- la journalisation des connexions.

[R.195] Les communications sans fil devraient être cloisonnées au maximum en isolant les périphériques sans fil dans un réseau physique ou logique séparé.

[R.196] Lorsque les événements de sécurité ne sont pas supervisés par un dispositif centralisé, il est recommandé que les événements générés par les équipements sans fil soient examinés régulièrement.

[R.197] La portée des émissions devrait être réduite au maximum en diminuant la puissance d'émission.

Important

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

Classe 2

[D.198] La recommandation R.196 devient une directive.

[D.199] Les correctifs de sécurité doivent être appliqués systématiquement sur les équipements des réseaux sans fil.

[R.200] Une sonde de détection d'intrusion devrait être déployée au niveau de l'interconnexion entre le réseau sans fil et les autres réseaux du système industriel.

Classe 3

[D.201] La recommandation R.200 devient une directive.

[D.202] L'usage des technologies sans fil est fortement déconseillé et doit être limité aux cas où il n'existe pas d'autre solution.

[D.203] L'utilisation de technologie sans fil doit être interdite sur toutes les liaisons ayant des besoins critiques de disponibilité.

[D.204] Les événements de sécurité générés par les équipements sans fil doivent être centralisés et supervisés en temps réel.

[R.205] L'ensemble des équipements utilisés dans des réseaux sans fil devraient être labellisés.

4.2.7 Sécurité des protocoles

Références

Vulnérabilité : 2.2.7
Guide SCADA : BP05
Guide d'hygiène : Régle 23
ISO 27002 : 13.2

Classe 1

[R.206] Les protocoles non sécurisés (http, telnet, ftp, etc.) devraient être désactivés au profit des protocoles sécurisés (https, ssh, sftp, etc.) pour assurer l'intégrité, la confidentialité, l'authenticité et l'absence de rejeu des flux.

Classe 2

[R.207] Pour les protocoles ne pouvant pas être sécurisés pour des raisons techniques et opérationnelles, des mesures compensatoires devraient être mises en place comme :

- mettre en place des protections périmétriques (pare-feu) ;
- encapsuler les flux dans un VPN pour en assurer l'intégrité et l'authenticité.

Classe 3

[D.208] Les recommandations R.206 et R.207 deviennent des directives.

Remarque

Les protocoles sécurisés ne doivent pas toujours chiffrer les flux. Si les flux, passent par des réseaux non-maîtrisés, le chiffrement est sans doute nécessaire. En revanche, sur un réseau maîtrisé, le chiffrement n'est pas toujours souhaitable car incompatible avec l'utilisation de sondes de détection. La signature des données peut être suffisante.
L'absence de chiffrement ne doit pas être incompatible avec la recommandation R.138 et la directive D.142.

Important

Certains protocoles intègrent des mécanismes de vérification d'intégrité des données basés sur des CRC. Cette mesure, efficace en sûreté de fonctionnement, ne constitue pas une protection face à des attaques dans le domaine de la cybersécurité.

4.3 Sécurisation des équipements

4.3.1 Durcissement des configurations

Références

Vulnérabilité : 2.2.7
Guide SCADA : BP05, BP07, BP10, BP12 et 2.2.3
ISO 27002 : 12.6

Désactivation des composants inutiles

Classe 1

[R.209] Sur les équipements, on devrait désactiver :

- les comptes par défaut ;
- les ports physiques inutilisés ;
- les supports amovibles, s'ils ne sont pas utilisés ;
- les services non indispensables (service web par exemple).

[R.210] Sur les postes de travail, ordinateurs portables et serveurs, on devrait également supprimer ou, au minimum, désactiver :

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

> **Remarque**
>
> Des lecteurs PDF et des logiciels de bureautique sont parfois installés sur des stations SCADA afin de pouvoir consulter des documents comme des modes opératoires. Il est préférable de mettre à disposition des utilisateurs d'autres postes que les stations SCADA pour utiliser les applications de bureautique et les lecteurs PDF (cf. R.60).

[R.211] Sur les automates et les applications SCADA,

- les fonctions de débogage (des intégrateurs et des équipementiers) devraient être désactivées ;
- les mnémoniques et commentaires ne devraient pas être chargés dans les équipements.

Classe 2

[D.212] La recommandation R.209 devient une directive.

Classe 3

[D.213] Les recommandations R.210 et R.211 deviennent des directives.

Renforcement des protections

Classe 1

[R.214] Les préconisations de durcissement des systèmes d'exploitation devraient être appliquées pour chaque équipement. Le site web de l'ANSSI [1] contient de nombreux guides et notes techniques sur ce sujet.

[R.215] Les applications doivent s'exécuter avec les privilèges strictement nécessaires à leur fonctionnement.

1. `http://www.ssi.gouv.fr`.

Classe 2

[D.216] La recommandation R.215 devient une directive.

[R.217] Des outils de défense en profondeur du poste de travail devraient être mis en place. En particulier, une liste blanche des applications ayant le droit de s'exécuter devrait être mise en place sur les équipements.

[R.218] Pour les automates, lorsque les équipements le permettent, les mécanismes suivants devraient être activés :

- la protection d'accès à la CPU et/ou au programme ;
- la restriction des adresses IP pouvant se connecter ;
- la désactivation du mode de programmation à distance.

Classe 3

[D.219] Les recommandations R.217 et R.218 deviennent des directives.

[R.220] Les outils devraient être labellisés.

Important

L'utilisation d'un dispositif de protection antivirale peut ne pas être adapté aux systèmes industriels pour les raisons suivantes :

- 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'utilisation d'un antivirus devrait sans doute se faire dans un poste ou un serveur dédié comme indiqué dans la recommandation R.235 et la directive D.241 mais elle n'est pas recommandée pour les autres composants du système industriel. Le durcissement des configurations, comme indiqué dans les recommandations R.217 et R.218, doit être privilégié.

Intégrité et authenticité

Classe 1

[R.221] Le processus de livraison de l'ensemble des logiciels, programmes et éléments de configuration ainsi que de leurs mises à jour devrait intégrer un mécanisme de vérification de l'intégrité et de l'authenticité (signature). Les éléments concernés sont en particulier :

- les firmwares ;
- les systèmes d'exploitation et logiciels standards ;
- les progiciels SCADA ;
- les programmes d'automates et de SCADA ;
- les fichiers de configuration des équipements réseau ;
- etc.

Classe 2

[D.222] La recommandation R.221 devient une directive.

[R.223] L'intégrité et l'authenticité des firmwares, logiciels et programmes applicatifs (automates, SCADA, etc.) devraient être vérifiées régulièrement. Idéalement, cette tâche devrait être automatisée et exécutée une fois par jour.

Classe 3

[D.224] La directive D.222 est renforcée de la manière suivante. Les éléments dont l'intégrité et l'authenticité doivent être vérifiées, doivent être signés par le fournisseur (équipementier, développeur, intégrateur,etc). La signature doit être vérifiée par l'entité responsable à la réception et par l'équipement au chargement.

[D.225] La recommandation R.223 devient une directive.

4.3.2 Gestion des vulnérabilités

Références

Vulnérabilité : 2.2.1
Guide SCADA : BP11
Guide d'hygiène : Règles 6, 7 et 16
ISO 27002 : 12.6

Classe 1

[R.226] Un processus de gestion des vulnérabilités doit être mis en œuvre afin de :

- rechercher les correctifs disponibles pour corriger ces vulnérabilités ;

— identifier les vulnérabilités connues et mesurer leurs impacts sur les systèmes ;
— déployer les correctifs en commençant par les plus importants ;
— 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).

> **Remarque**
>
> Appliquer des correctifs n'est pas une opération anodine. Il est important de s'assurer de leur compatibilité avec le fonctionnement des applications. Le déploiement des correctifs doit être intégré dans les plans de maintenance des installations. Il peut, en effet, être judicieux de mettre en place les correctifs lorsque l'installation est à l'arrêt pour une maintenance mécanique par exemple. Aujourd'hui, les correctifs concernent également les PLC et les équipements de terrain comme les capteurs et actionneurs intelligents.

[R.227] Les correctifs de sécurité doivent être appliqués en priorité sur les équipements les plus exposés (postes de travail, PC portables, stations d'ingénierie, consoles de programmation, pare-feu, VPN, etc.).

Classe 2

[D.228] Les vulnérabilités non corrigées doivent être clairement identifiées. Un suivi spécifique doit être mis en œuvre et des mesures palliatives doivent être appliquées pour diminuer l'exposition due à ces vulnérabilités.

[R.229] Les correctifs devraient être validés par les fournisseurs avant le déploiement.

[R.230] Une vérification de l'application effective des correctifs de sécurité devrait être effectuée. Cette vérification pourra constituer un indicateur de suivi de la cybersécurité du système industriel.

Classe 3

[D.231] Les recommandations R.226, R.227, R.229 et R.230 deviennent des directives.

[R.232] Un environnement de test représentatif des systèmes en production devrait être mis en œuvre afin de s'assurer de leur non-régression après l'application des correctifs.

4.3.3 Interfaces de connexion

Références

Vulnérabilité : 2.2.3
Guide SCADA : BP03
Guide d'hygiène : Règles 5, 15 et 34
ISO 27002 : 12.6

Gestion des médias amovibles

Classe 1

[R.233] Une politique d'utilisation des médias amovibles (clé USB, disquette, disque dur, etc.) devrait être définie.

[R.234] L'emploi des médias amovibles devrait être limité au strict minimum.

[R.235] Une station de décontamination devrait être installée afin d'analyser et décontaminer tous les périphériques amovibles avant de les utiliser sur le système industriel.

[R.236] La connexion des périphériques amovibles qui n'ont pas été vérifiés par la station de décontamination devrait être interdite.

[R.237] Des médias amovibles dédiés aux systèmes industriels devraient être mis à disposition des intervenants. L'utilisation de ces médias pour tout autre usage devrait être interdite. Réciproquement, l'utilisation de tout autre média devrait être interdite.

Classe 2

[D.238] Les recommandations R.233, R.234, R.235, R.236 et R.237 deviennent des directives.

[R.239] Les ports de médias amovibles devraient être désactivés lorsque leur utilisation n'est pas nécessaire. Si le blocage physique n'est pas possible, le port devrait être désactivé logiquement.

Par exemple, on pourrait envisager les mesures suivantes :

— le blocage des ports USB à l'aide de mécanismes de sécurité physiques ou logiques, comme les verrous USB physiques (avec clés) ou par un logiciel de sécurité capable de bloquer l'utilisation de clés USB et autres périphériques ;

— le retrait ou la déconnexion des lecteurs de médias amovibles.

Classe 3

[D.240] La recommandation R.239 devient une directive.

[D.241] Un sas doit être mis en place pour échanger des données avec les systèmes industriels. Il doit être placé dans une zone maîtrisée. Cet échange de données est une action ponctuelle qui doit être encadrée par une procédure.

[R.242] La solution de sas devraient être labellisée.

Gestion des points d'accès réseau

Classe 1

[R.243] Les points d'accès réseau devraient être clairement identifiés et recensés.

[R.244] Les points d'accès réseau non utilisés (commutateurs, hubs, baies de brassage, prises de maintenance sur les bus de terrain, etc.) devraient être désactivés.

Classe 2

[D.245] Les recommandations R.243 et R.244 deviennent des directives.

[D.246] En cas de tentative de connexion et de déconnexion sur des ports réseau, une alerte doit être remontée et traitée.

Classe 3

[D.247] Les points d'accès réseau ne doivent être accessibles que dans des locaux maîtrisés.

4.3.4 Équipements mobiles

Références

Vulnérabilité : 2.2.11
Guide d'hygiène : Règles 5, 17 et 19
ISO 27002 : 11.2.6

Classe 1

[R.248] L'usage des périphériques personnels quels qu'ils soient (ordiphones, tablettes, clés USB, appareils photos, etc.) devrait être interdit.

[R.249] Une charte d'utilisation des terminaux nomades et une signalétique pour rappeler cette exigence devraient être mis en place.

[R.250] Les équipements autorisés à se connecter aux systèmes devraient être clairement identifiés et validés.

[R.251] Lorsque l'équipement contient des données sensibles, sa mémoire de stockage devrait être chiffrée.

[R.252] Un processus d'attribution des terminaux mobiles devrait être mis en place. Il devrait permettre, a minima :

- de valider l'attribution du terminal par le responsable hiérarchique ;
- d'assurer la traçabilité entre le terminal et ses utilisateurs ;
- de sensibiliser l'utilisateur aux règles d'usage en vigueur.

Classe 2

[D.253] les recommandations R.248, R.249, R.251 et R.252 deviennent des directives.

[R.254] Les équipements utilisés devraient être dédiés au système industriel, y compris ceux utilisés par des prestataires extérieurs.

[R.255] Ces équipements ne devraient pas quitter le site.

Classe 3

[D.256] Les recommandations R.251, R.254 et R.255 deviennent des directives.

4.3.5 Sécurité des consoles de programmation, des stations d'ingénierie et des postes d'administration

Références

Vulnérabilité : 2.2.20
Guide SCADA : BP13
ISO 27002 : 11.2.6

Les consoles de programmation sont des équipements nomades et les stations d'ingénierie des stations de travail fixes. Dans les deux cas, il s'agit de postes dédiés à l'ingénierie des processus du système industriel. Il peut arriver que le terme « poste d'administration » soit utilisé ce qui peut prêter à confusion.

Les postes d'administration sont dédiés à l'administration des équipements d'infrastructure (commutateurs, serveurs, station, pare-feu, etc.) du système industriel.

Pour les mesures techniques sur le cloisonnement des fonctions d'administration, on pourra se reporter à la section 4.2.1.

Classe 1

[R.257] Les stations d'ingénierie devraient respecter les règles suivantes :

- être dédiées aux activités d'ingénierie ;
- ne pas être connectées à Internet ;
- être installées dans des locaux maîtrisés (sous contrôle d'accès) ;
- se voir appliquer les règles de durcissement des stations de travail ;
- être éteintes lorsqu'elles ne sont pas utilisées.

[R.258] Les consoles de programmation devraient :

- être dédiées aux activités de maintenance et d'exploitation ;
- ne pas être connectées à Internet ;
- ne pas être connectées à d'autres systèmes que le système industriel ;
- appliquer les règles pour les terminaux mobiles ;
- appliquer les règles de durcissement de configuration et de renforcement des protections ;
- être stockées dans un local sécurisé ;
- être facilement identifiables (marquage visuel par exemple).

[R.259] Les postes d'administration devraient :

- être dédiés à l'administration des équipements d'infrastructure ;
- ne pas être connectés à Internet ;
- appliquer les règles de durcissement de configuration et de renforcement des protections ;
- être installés dans des locaux maîtrisés (sous contrôle d'accès) ;
- être éteints lorsqu'ils ne sont pas utilisés.

[R.260] Les outils de développement ne doivent pas être installés sur les machines de production. Seuls les environnement de production (runtime) doivent être installés sur les serveurs et stations SCADA par exemple.

[R.261] La recommandation R.260 peut être difficile à appliquer dans le cas de l'utilisation de systèmes numériques de contrôle-commande (SNCC). Il conviendra alors d'étudier des solutions compensatoires pour isoler le système et réduire sa surface d'attaque.

Classe 2

[D.262] Les recommandations R.257, R.258, R.259, R.260 et R.261 deviennent des directives.

Classe 3

[R.263] Les postes d'administration ne devraient pas être utilisés pour la surveillance permanente des systèmes.

4.3.6 Développement sécurisé

Références

Vulnérabilité : 2.2.19
Ref ISO 27002 : 14.2

Classe 1

[R.264] Des règles de bonne pratique de programmation devraient être définies, appliquées et vérifiées. 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.

Remarque

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.

Remarque

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

Classe 2

[R.265] Un environnement de développement devrait être dédié au système industriel.

Remarque

L'environnement de développement peut être interne ou chez des fournisseurs. Dans ce cas il convient d'indiquer les exigences attendues dans le cahier des charges (cf. R.51).

[R.266] En plus de bonnes pratiques de développement évoquées dans la recommandation R.264, des règles de développement de sécurité (*secure coding*) devraient être mises en place et appliquées.

[R.267] Des outils d'analyse statique et des tests de robustesses devraient être utilisés systématiquement.

[R.268] Des audits de code devraient être effectués par des prestataires externes.

Classe 3

[D.269] Les recommandations R.265, R.266, R.267 et R.268 deviennent des directives.

[D.270] Le niveau de sécurité de l'environnement de développement doit être vérifié par des audits.

4.4 Surveillance du système industriel

Références

Guide de mesures : 2.2.12
Vulnérabilité : 2.2.14
Guide SCADA : BP06, 2.2.4
Guide d'hygiène : Règles 26 et 27
ISO 27002 : 12.4

4.4.1 Journaux d'événements

Classe 1

[R.271] Une politique de gestion des événements devrait être définie. Elle devrait permettre :

- de déterminer quels sont les événements pertinents à prendre en compte ;
- d'organiser leur stockage (volumétrie, durée de conservation, etc.) ;

— de définir les conditions d'analyse (en préventif, post-incident…) ;

— de définir quels sont les événements qui doivent générer des alertes. L'annexe B fournit une liste d'événements en exemple.

[R.272] Les fonctions de traçabilité devraient être activées si les équipements et logiciels le permettent (syslog, SNMPv3, Windows Event, etc.).

[R.273] Un système de gestion centralisée et sécurisée des journaux d'événements devrait être mis en place. Ce système devra en particulier assurer la sauvegarde, la confidentialité et l'intégrité des journaux d'événements. On pourra se reporter au guide de l'ANSSI [15].

[R.274] Les modifications des paramètres devraient être tracées et enregistrées pour les capteurs et actionneurs, fonctions d'asservissement et de régulation, etc.

> **Remarque**
>
> Une partie des changements de paramètres des processus peut, dans certains cas, être déjà enregistrée au niveau des applications de SCADA sous forme d'événements ou de courbes.

Classe 2

[D.275] Les recommandations R.271, R.273 et R.274 deviennent des directives.

[R.276] Les journaux devraient être analysés régulièrement.

Classe 3

[D.277] La recommandation R.276 devient une directive.

[R.278] Une solution de SIEM centralisant l'ensemble des journaux d'événements de sécurité devrait être mise en place. Elle devrait permettre de corréler les journaux en vue de détecter des incidents de sécurité. La solution de SIEM, pour ne pas être considérée de classe 3, devra être placée derrière une diode comme indiqué à la directive D.159.

Moyens de détection

Classe 1 Il n'y a pas de mesure pour cette classe.

Classe 2

[R.279] Des moyens de détection d'intrusion devraient être mis en place 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 (WiFi industriel par exemple) ;
- les stations sas ;
- le réseau fédérateur de postes de supervision industriel (SCADA) ;
- les réseaux d'automates jugés sensibles.

[R.280] Les moyens de détection mis en œuvre devraient être labellisés.

[R.281] Les événements collectés par les sondes devraient être centralisés.

[R.282] Un processus devrait clairement décrire comment les événements remontés par les sondes sont pris en compte.

Classe 3

[D.283] Les recommandations R.279, R.281, R.282 deviennent des directives.

Annexe A

Cartographie

Les équipes qui exploitent et maintiennent les systèmes industriels doivent pouvoir s'appuyer sur une documentation fiable et à jour. Nous proposons dans ce chapitre quatre types de cartographie à différents niveaux pour avoir une connaissance aussi précise que possible du système concerné. Chacune de ces cartographies consistera en une liste et en un schéma qui organise les éléments référencés.

A.1 Cartographie physique du système industriel

Le point de vue physique correspond à la répartition géographique des équipements au sein des différents sites. On pourra organiser cette cartographie sous la forme d'inventaires et d'un schéma.

A.1.1 Inventaire

Cet inventaire devra comporter notamment les éléments suivants :

la liste des équipements communicants du système industriel :

Cette liste comportera par exemple les automates, les entrées sorties déportées, les capteurs, les actionneurs, les variateurs de vitesse, les centrales de mesures, les disjoncteurs, les interrupteurs, les serveurs physiques, les postes de travail, les unités de stockage. Pour chaque élément, on précisera :

- le nom ;
- la marque ;
- le modèle ou la référence [1] ;
- la version du *firmware* (software version) embarqué et la version du produit (product version) si pertinent ;
- les caractéristiques matérielles si pertinent ;
- l'emplacement physique (bâtiment, pièce, armoire, baie) ;
- la liste des commutateurs reliés ;

1. Certains équipements (les automates modulaires, par exemple) contiennent plusieurs références.

la liste des équipements des réseaux de communication :

Cette liste comportera par exemple les commutateurs, les routeurs, les passerelles protocolaires, etc. Pour chaque équipement, on précisera :

— la marque ;

— le modèle et la référence ;

— la version du *firmware* embarqué.

— l'emplacement physique (bâtiment, pièce, armoire, baie).

Dans le cas de commutateurs Ethernet, on précisera également les numéros de VLAN pour chaque port du commutateur.

A.1.2 Schéma

Il s'agit de la représentation des différents sites géographiques, faisant apparaître :

— les commutateurs, les numéros de VLAN associés ;

— les liens entre équipements ;

— en cas d'installation inter-site, les identifiants d'interconnexion (MPLS, VPLS, numéros de téléphone) ;

— les équipements.

A.2 Cartographie logique des réseaux industriels

On s'intéresse ici à la topologie logique des réseaux (les plan d'adressage IP et non-IP, noms de sous-réseaux, liens logiques entre ceux-ci, principaux équipements actifs, etc.). Cette cartographie pourra également être organisée sous la forme d'inventaires et d'un schéma.

A.2.1 Inventaires

On propose de répertorier les éléments suivants :

les organisations :

avec pour chacune d'entre elles,

— le responsable.

la liste des plages d'adresses IP :

avec pour chacune,

— la liste des commutateurs en support ;

— la description fonctionnelle de la plage IP ;

— les interconnexions avec d'autres plages.

la liste des réseaux non-IP :

avec pour chaque réseau

— la liste des adresses MAC ou des adresses spécifiques à des protocoles industriels sur le réseau ;

— la liste des commutateurs en support ;

— la description fonctionnelle du réseau ;

— les équipements connectés à d'autres réseaux (automates).

la liste des points d'accès non Ethernet :

avec pour chacun d'entre eux,

— la liste des ports d'accès ;

— l'adressage en cas de protocole spécifique ;

— la liste des équipements connectés.

la liste des serveurs logiques et des postes de travail :

avec pour chacun d'entre eux, lorsque cela s'applique,

— l'adressage IP (réseau, masque, passerelle) ;

— la version du système d'exploitation ;

— le serveur physique en support ;

— les applications métier et leur version ;

— les services et versions.

la liste des automates et équipements de terrain communicants[2] **:**

avec pour chacun

— l'adressage IP (réseau, masque, passerelle), l'adressage MAC et réseau associé ou l'adressage spécifique le cas échéant ;

— les applications métier.

A.2.2 Schéma

Il s'agit de la représentation des ensembles IP (réseaux et sous-réseaux) et de leurs interconnexions, faisant apparaître :

— la description fonctionnelle de la plage IP ;

— les interconnexions avec les autres plages IP ;

— les routeurs, commutateurs et pare-feu ;

— les équipements informatiques de sécurité (relais filtrant, sondes, IDS, etc.).

Cette cartographie doit faire apparaître en particulier les points d'interconnexion avec des entités « extérieures » (partenaires, fournisseurs de services, etc.) et l'ensemble des interconnexions avec Internet.

2. entrées sorties déportées, capteurs/actionneurs intelligents, etc.

A.3 Cartographie des applications

Le point de vue applicatif correspond aux applications métier et aux flux de communication entre elles. Comme précédemment, on pourra organiser cette cartographie sous la forme d'inventaires et d'un schéma.

A.3.1 Inventaires

On pourra notamment lister les éléments suivants :

- le responsable ;
- le type d'application (application SCADA, programme automate, historique, etc.) ;
- le nombre d'utilisateurs ;
- les équipements (physiques ou logiques) supports ;
- les services en écoute sur le réseau et ports réseaux associés ;
- les flux applicatifs ;
- la version de l'application.

A.3.2 Schéma

Il s'agit d'une représentation des composants des applications et des flux entre elles :

- les programmes des automates ;
- les applications de SCADA ;
- les services d'infrastructure (DNS, NTP, passerelle Internet, etc.) ;
- les services d'administration (service d'inventaires, d'administration à distance, etc.)
- la matrice de flux associée à chaque application et service.

A.4 Cartographie de l'administration et de la surveillance du système d'information

Cette dernière cartographie ne s'applique que si une gestion centralisée des droits d'administration sur les équipements a été mise en place. Dans le cas où les droits sur les équipements ne sont gérés que par des comptes locaux, cette cartographie se réduira à une liste des comptes et des droits associés pour chaque équipement.

La cartographie devra contenir :

- les annuaires (voir plus bas) ;
- les infrastructures de gestion de clés ;
- les systèmes de mots de passe à usage unique ;
- les systèmes de gestion de journaux et d'événements de sécurité (collecteurs de journaux, SIEM) ;
- les système de supervision (alarmes réseau, sondes de détection, etc).

Le point de vue « domaines d'administration » représente le périmètre et le niveau de privilèges des administrateurs sur les ressources du parc informatique. Cette cartographie contiendra

- le cas échéant, un schéma « Active Directory » avec :
  - les domaines Active Directory et leur description,
  - les forêts Active Directory,
  - les relations d'approbation avec les domaines externes à chaque forêt,
  - les caractéristiques des relations d'approbation (bidirectionnelle, filtrée, etc.),
  - les serveurs support des Active Directory ;
- sinon, la représentation de l'architecture d'administration avec
  - les zones de responsabilité des différents administrateurs,
  - l'inventaire des secrets (mots de passe, clés, etc.) et droits associés à l'administration des ressources.

Ce point de vue permet, en cas de compromission d'un compte d'administration, d'identifier le niveau de privilège de l'attaquant et la portion du parc potentiellement affectée.

Annexe B

Journaux d'événements

Liste minimale (mais non exhaustive) des événements d'audit à configurer :

- tentatives d'authentification (réussite ou échec) ;
- actions des utilisateurs dans le système ;
- utilisation des comptes à privilèges ;
- défaillances des mécanismes de sécurité ;
- tentatives de connexions réseau ;
- démarrage et arrêt des fonctionnalités d'audit ;
- activation, désactivation et modification du comportement ou de paramètres des mécanismes de sécurité (authentification, génération d'audit, etc.) ;
- actions entreprises en raison d'une défaillance du stockage des audits ;
- toute tentative d'exportation d'informations ;
- utilisation de la fonction de gestion ;
- modification du groupe d'utilisateurs faisant partie d'un rôle ;
- détection d'une violation physique ;
- toute tentative d'établissement d'une session utilisateur ;
- tentatives de chargement, modification ou récupération de programme, micro-programme ou firmware ;
- modification de paramètres systèmes (heure, adresse IP ou non IP, temps de cycle, chien de garde,etc) ;
- modification ou forçage de données applicatives ;
- passage d'un équipement en mode stop, marche, stand-by, redémarrage.

Remarque

Les événements peuvent être centralisés sur un serveur de type syslog. De nombreux équipements permettent en effet de configurer un serveur syslog cible. Pour les journaux d'événements Microsoft il existe des utilitaires permettant, pour chaque nouvel événement enregistré, de l'envoyer vers un serveur syslog.

Pour plus d'information consulter la note d'information du CERTA [5] et la note technique relative aux recommandations de sécurité pour la mise en œuvre d'un système de journalisation [15].

Bibliographie

[1] Gerard De Drouas and Pierre Capillon. Audit des permissions en environnement Active Directory. In *SSTIC*, 2012.

[2] Secrétariat de la défense et de la sécurité nationale. Guide pour réaliser un plan de continuité d'activité. juin 2013.

[3] ISO. ISO27002 : Security techniques - Code of practice for security management. 2013.

[4] Agence nationale de la sécurité des systèmes d'information. Note d'information, les bons réflexes en cas d'intrusion. mai 2002.

[5] Agence nationale de la sécurité des systèmes d'information. Note d'information pour la gestion des journaux d'événement. mai 2008.

[6] Agence nationale de la sécurité des systèmes d'information. Référentiel général de sécurité. mai 2010.

[7] Agence nationale de la sécurité des systèmes d'information. Définition d'une architecture de passerelle d'interconnexion sécurisée. janvier 2012.

[8] Agence nationale de la sécurité des systèmes d'information. Guide de l'externalisation. mai 2012.

[9] Agence nationale de la sécurité des systèmes d'information. La sécurité des technologies sans contact pour le contrôle des accès physiques. novembre 2012.

[10] Agence nationale de la sécurité des systèmes d'information. Maitriser la SSI pour les systèmes industriels. juin 2012.

[11] Agence nationale de la sécurité des systèmes d'information. Note technique pour l'utilisation des pare-feu. mai 2012.

[12] Agence nationale de la sécurité des systèmes d'information. Recommandations de sécurité relatives aux mots de passe. mai 2012.

[13] Agence nationale de la sécurité des systèmes d'information. Cybersécurité pour les systèmes industriels : Classification et mesures principales. 2013.

[14] Agence nationale de la sécurité des systèmes d'information. Guide d'hygiène informatique. janvier 2013.

[15] Agence nationale de la sécurité des systèmes d'information. Recommandations de sécurité pour la mise en oeuvre d'un système de journalisation. décembre 2013.

Ce guide sur la cybersécurité des systèmes industriels a été réalisé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) avec le concours des sociétés et organismes suivants :

— Actemium,
— Airbus Defence and Space,
— Arkoon-Netasq,
— A.R.C. Informatique,
— Atos Worldgrid,
— Hirschmann,
— Cassidian Cybersecurity,
— CEA,
— CLUSIF,
— DCNS,
— DGA Maîtrise de l'information,
— Euro system,
— EXERA,
— GDF SUEZ,
— Gimélec,
— INERIS,
— Itris Automation Square,
— Lexsi,
— Schneider Electric,
— Siemens,
— Sogeti,
— RATP,
— Solucom,
— Thales,
— Total.

À propos de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009 sous la forme d'un service à compétence nationale.
En vertu du décret n° 2009-834 du 7 juillet 2009 modifié par le décret n° 2011-170 du 11 février 2011, l'agence assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.
Pour en savoir plus sur l'ANSSI et ses missions, rendez-vous sur www.ssi.gouv.fr.

Version 1.0 – Janvier 2014

Licence « information publique librement réutilisable » (LIP V1 2010.04.02)

Agence nationale de la sécurité des systèmes d'information
ANSSI - 51 boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
Sites internet : `www.ssi.gouv.fr` et `www.securite-informatique.gouv.fr`
Messagerie : communication [at] ssi.gouv.fr