Méthode de classification et mesures principales

La cybersécurité des systèmes industriels

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Table des matières

1 Introduction **5**

1.1 Contexte 5

1.2 Champ d'application 6

1.3 Structure du corpus documentaire 6

1.4 Vocabulaire 7

2 Classes de cybersécurité et mesures associées **9**

2.1 Classes de cybersécurité des systèmes industriels 9

2.2 Mesures 11

2.3 Homologation 20

3 Méthode de classification **23**

3.1 Contexte 23

3.2 Critères de sécurité 25

3.3 Échelles 25

3.4 Biens essentiels 28

3.5 Biens supports 29

3.6 Détermination de la classe 39

A Cas d'étude simplifiés **43**

A.1 Installation d'adduction d'eau 43

A.2 Industrie manufacturière 44

A.3 Industrie de procédé continu 44

A.4 Poste de manœuvre informatisé 46

Liste des acronymes **49**

Glossaire **51**

Bibliographie **59**

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.

Ces propositions seront utilisées pour définir les modalités d'application des mesures évoquées dans le cadre de la loi n° 2013-1168 du 18 décembre 2013, dite loi de programmation militaire (LPM).

L'objectif est d'homologuer l'ensemble des nouveaux systèmes industriels critiques afin de s'assurer que leur niveau de cybersécurité est acceptable compte tenu de l'état de la menace actuelle et de ses évolutions potentielles.

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. 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.

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 s'appliquer à tous les secteurs. Certains d'entre eux ont des spécificités qui n'ont pas été détaillées ou prises en compte dans le présent document. **En conséquence, une déclinaison sectorielle de ce document, avec les ministères coordinateurs, 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.

Il est également possible que dans certaines situations (pour des raisons de compatibilité avec des systèmes industriels existants ou à cause de contraintes métier spécifiques, par exemple) certaines mesures ne puissent s'appliquer sans adaptation. Ces cas particuliers devront être étudiés spécifiquement et les mesures qui en découleront seront soumises pour approbation à l'autorité de cyberdéfense.

Ces travaux s'intéressant exclusivement à la cybersécurité des systèmes industriels, la définition de la stratégie globale de la SSI des organismes ne rentre pas dans ce cadre. Il revient donc à chaque entité responsable d'intégrer les systèmes industriels et leurs contraintes spécifiques dans leur politique de sécurité des systèmes d'information (PSSI). Sur ce sujet, on pourra se reporter au guide [6].

1.3 Structure du corpus documentaire

Les travaux du groupe de travail sont organisés en deux documents. Ce document constitue le socle et contient les éléments structurants. Les classes de cybersécurité et les mesures principales sont présentées dans le chapitre 2 et la méthode de classification est présentée dans le chapitre 3.

Le guide des mesures [9] contient, quant à lui, l'ensemble des mesures techniques et organisationnelles précises à mettre en place en fonction des classes identifiées.

1.4 Vocabulaire

Dans l'ensemble des documents, le terme *système automatisé de contrôle des procédés industriels* (ou, plus brièvement, *système industriel*) désigne un ensemble de moyens humains et matériels ayant pour finalité de contrôler ou commander des installations techniques (composées d'un ensemble de capteurs et d'actionneurs). Cela englobe bien évidemment les systèmes de contrôle-commande que nous retrouvons dans de nombreux secteurs d'activité (énergie, transport, traitement de l'eau, industrie, etc.) mais également la gestion technique de bâtiment (GTB). Dans la littérature, nous rencontrons souvent le terme d'ICS [2].

Les systèmes de gestion sont exclus du périmètre de ce document. Seules leurs interfaces avec les systèmes industriels sont abordées. Pour plus d'information sur la distinction entre ces systèmes, on pourra se reporter au guide de l'ANSSI [8].

Le terme *cybersécurité* sera utilisé dans le document afin d'éviter tout risque de confusion avec le terme «sécurité» qui, dans le monde industriel, peut avoir d'autres significations que celles liées à la sécurité des systèmes d'information comme la sécurité des biens et des personnes par exemple.

Dans toute la suite de ce document, l'entité responsable désigne la personne morale ou physique qui a la responsabilité légale de la mise en place des mesures de cybersécurité pour le système industriel concerné. Selon les cas, il ne s'agit pas toujours de la même personne ou du même organisme. Par ailleurs, le vocabulaire peut varier en fonction des secteurs d'activité.

Exemple

Dans le secteur de la pétrochimie, l'*opérateur* est l'entité qui exploite l'installation et qui sera responsable de la mise en œuvre des mesures de cybersécurité des systèmes industriels. Au contraire, le terme *exploitant* désigne le personnel intervenant sur l'installation. Dans d'autres secteurs, ces termes peuvent être inversés.

Les termes techniques utilisés dans ce document ont été définis dans le glossaire. En particulier, les termes relatifs à la sécurité des systèmes d'information sont issus de la série des normes ISO 27000 [5] et de l'IGI 1300 [3].

2. Industrial Control System.

Avertissement

Les recommandations et directives contenues dans ce document sont livrées en l'état et adaptées aux menaces connues au jour de la publication de ce document. Au regard de la diversité des systèmes industriels, il ne peut être garanti que ces informations puissent être reprises sans adaptation aux systèmes cibles. Une analyse préalable doit être réalisée par l'entité responsable avant toute mise en œuvre des mesures indiquées.

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

Classes de cybersécurité et mesures associées

L'objectif de ce chapitre est de présenter les classes de cybersécurité et de donner les mesures (techniques et organisationnelles) applicables à chacune d'entre elles. Certaines mesures sont de simples recommandations, d'autres sont des directives.

2.1 Classes de cybersécurité des systèmes industriels

Il existe des référentiels proposant de classer les systèmes industriels en 4 ou 5 niveaux. Le constat est que les premiers niveaux de ces référentiels relèvent bien souvent de la sûreté de fonctionnement et apportent peu d'éléments du point de vue de la cybersécurité. Il a été considéré que les aspects de sûreté de fonctionnement étaient déjà pris en compte et n'étaient pas l'objet de ce document.

Remarque

Les risques liés à la négligence humaine sont pris en compte par la sûreté de fonctionnement alors que ceux liés à la malveillance sont traités par la cybersécurité. Néanmoins, les mesures de cybersécurité permettent de couvrir certains risques liés à la négligence.

Il est donc proposé ici de répertorier simplement les systèmes industriels en trois classes en fonction de leurs besoins de sécurité. Cette classification peut être appliquée à un site dans son ensemble, à une partie plus spécifique, ou à un système industriel réparti sur plusieurs sites. Ceci sera détaillé dans la description du périmètre à la section 3.1.1. Il appartient à chaque entité responsable de définir le périmètre précis du système industriel concerné.

Important

Les niveaux de cybersécurité sont définis en fonction des conséquences pour la Nation et non en fonction des conséquences propres aux entités responsables.

Chaque classe intègre nécessairement les mesures de la classe inférieure. Voici une description succincte des trois classes de cybersécurité des systèmes industriels :

Classe 1 : Il s'agit des systèmes industriels pour lesquels le risque ou l'impact d'une attaque est faible. L'ensemble des mesures préconisées pour cette classe doivent pouvoir être appliquées en complète autonomie. Ce niveau correspond principalement aux règles d'hygiène informatique énoncées dans le guide de l'ANSSI [10].

Classe 2 : Il s'agit des systèmes industriels pour lesquels le risque ou l'impact d'une attaque est significatif. Il n'y a pas de contrôle étatique pour cette classe de système industriel mais l'entité responsable doit pouvoir apporter la preuve de la mise en place des mesures adéquates en cas de contrôle ou d'incident.

Classe 3 : Il s'agit des systèmes industriels pour lesquels le risque ou l'impact d'une attaque est critique. Dans cette classe, les obligations sont plus fortes et la conformité de ces systèmes industriels est vérifiée par l'autorité étatique ou un organisme accrédité.

Les classes de cybersécurité sont estimées en fonction de la méthodologie détaillée dans le chapitre 3. La prochaine section décrit les mesures *structurantes* qui doivent être appliquées en fonction des trois classes. La liste exhaustive des mesures est décrite dans le guide de mesures [9]. Pour chaque mesure présentée dans la suite de cette section, les sections correspondantes de ce guide sont indiquées.

Important

Toutes les modifications fonctionnelles et techniques apportées aux systèmes industriels nécessiteront une revue de l'estimation du niveau de cybersécurité. En effet, une modification peut remettre en cause la classe qui avait été préalablement estimée. À titre d'exemple, on pourra se reporter au cas d'étude A.3 dans l'annexe.

2.2 Mesures

2.2.1 Rôles et responsabilités

Les rôles et responsabilités en matière de cybersécurité doivent être clairement établis.

Classe 1 : Une chaîne de responsabilité de la cybersécurité devrait être mise en place et couvrir l'ensemble des systèmes industriels.

Classe 2 : Une chaîne de responsabilité de la cybersécurité doit être mise en place et couvrir l'ensemble des systèmes industriels.

Classe 3 : Une chaîne de responsabilité de la cybersécurité doit être mise en place et couvrir l'ensemble des systèmes industriels. L'identité et les coordonnées du responsable de cette chaîne doivent être communiquées à l'autorité de cyber-défense.

Les mesures détaillées correspondantes se trouvent dans la section 3.1.1 du guide des mesures [9].

2.2.2 Analyse de risque

L'analyse de risque constitue le cœur des mesures organisationnelles. Elle est le point de départ de toute démarche de cybersécurité et beaucoup d'autres mesures vont dépendre directement de celle-ci.

Classe 1 : Les systèmes industriels devraient faire l'objet d'une analyse de risque pour la cybersécurité, même succincte.

Classe 2 : Les systèmes industriels doivent faire l'objet d'une analyse de risques suivant une méthode choisie par l'entité responsable.

Classe 3 : Les systèmes industriels doivent faire l'objet d'une analyse de risques détaillée suivant une méthode choisie par l'entité responsable. L'analyse de risque devra être revue régulièrement, au moins une fois par an. Elle devrait être réalisée en collaboration avec un prestataire labellisé.

Les mesures détaillées correspondantes se trouvent dans la section 3.1.3 du guide des mesures [9].

2.2.3 Cartographie

Une cartographie complète du système industriel est un élément indispensable pour une bonne politique de cybersécurité car cela offre une connaissance fine du système et de son environnement. À titre d'exemple, cela permet d'évaluer rapidement l'impact d'une vulnérabilité découverte dans un produit ou de mesurer l'étendue d'une compromission. Une cartographie des systèmes industriels permettra également de résoudre les incidents plus rapidement. Une explication succincte sur les cartographies est donnée dans l'annexe A du guide des mesures [9].

Classe 1 : Une cartographie physique, logique et des applications du système industriel devrait être rédigée.

Classe 2 : Une cartographie physique, logique et des applications du système industriel doit être rédigée.

La cartographie doit être revue régulièrement (la fréquence sera définie par l'entité responsable) et à minima à chaque modification apportée au système industriel.

Classe 3 : Une cartographie physique, logique et des applications du système industriel doit être rédigée.

La cartographie doit être revue régulièrement et au moins une fois par an.

Les mesures détaillées correspondantes se trouvent dans la section 3.1.2 du guide des mesures [9].

2.2.4 Formation, contrôle et habilitation des intervenants

La formation des intervenants sur un système industriel est un élément indispensable pour en assurer la cybersécurité. La formation devra contenir les éléments de sensibilisation aux risques induits par les technologies de l'information et de la communication ainsi qu'une présentation de la PSSI. Elle devra être formalisée et reconnue par l'entité responsable.

Dans la suite de ce document, nous considérons qu'une personne est **habilitée** dès lors qu'elle a reçu une formation spécifique à son rôle sur le système industriel concernée et qu'elle a été sensibilisée à la sécurité des systèmes d'information. Cette formation devra avoir été actée par l'entité responsable du système industriel. Par ailleurs, nous considérons qu'une personne est **contrôlée** si elle a été autorisée explicitement à intervenir et si ses actions peuvent être tracées.

Classe 1 : L'ensemble des intervenants devrait être habilité.

Classe 2 : L'ensemble des intervenants doit être habilité.

Classe 3 : L'ensemble des intervenants doit être habilité et contrôlé.
La formation à la cybersécurité comprise dans l'habilitation devrait être assurée par des prestataires labellisés.

Les mesures détaillées correspondantes se trouvent dans la section 3.2.2 du guide des mesures [9].

2.2.5 Audits

Les audits permettent de vérifier, avant la mise en service, lors des recettes plateforme (SAT [1]) et usine (FAT [2]), puis régulièrement lors du cycle de vie, le niveau effectif de cybersécurité du système industriel. L'audit doit porter sur les aspects techniques mais aussi organisationnels afin de vérifier l'application des mesures listées dans le présent document ainsi que dans le guide des mesures [9]. Des tests d'intrusion sont également à prévoir. Le processus d'audit doit intégrer les fournisseurs (équipementiers, intégrateurs, etc.).

Classe 1 : Des audits réguliers devraient être mis en place. Ces audits pourraient être internes.

Classe 2 : Des audits réguliers doivent être mis en place. Ces audits devraient être réalisés par des prestataires externes.

Classe 3 : Des audits réguliers doivent être mis en place et être effectués au moins une fois par an. Ces audits devraient être réalisés par des prestataires indépendants labellisés.

Les mesures détaillées correspondantes se trouvent dans la section 3.3.4 du guide des mesures [9].

2.2.6 Processus de veille

Un processus de veille permet de se tenir informé du niveau de la menace et des vulnérabilités. En fonction de la classe de cybersécurité, le processus de veille pourra être plus ou moins évolué.

Classe 1 : Une veille sur les vulnérabilités des produits utilisés, pour pouvoir les mettre à jour en cas de faille critique, devrait être mise en place.

Classe 2 : Un processus de veille devrait être mis en place afin de :

1. Site Acceptance Test.
2. Factory Acceptance Test.

— se tenir informé des vulnérabilités identifiées sur les produits et technologies mis en œuvre dans les systèmes industriels ;

— se tenir informé de l'évolution des mécanismes de protection.

Classe 3 : Un processus de veille doit être mis en place afin de :

— se tenir informé de l'évolution de la menace ;

— se tenir informé des vulnérabilités identifiées sur les produits et technologies mis en œuvre sur les systèmes industriels ;

— se tenir informé de l'évolution des techniques d'attaque ;

— se tenir informé de l'évolution des mécanismes de protection.

Les mesures détaillées correspondantes se trouvent dans la section 3.3.7 du guide des mesures [9].

2.2.7 Plans de reprise et de continuité d'activité

Un plan de continuité d'activité (PCA) et un plan de reprise d'activité (PRA) permettent de garantir la continuité ou la reprise du service suite à un sinistre, quelle qu'en soit l'origine. Ces plans, parfois déjà existants pour répondre à d'autres sinistres, devraient répondre à l'ensemble des scénarios d'incident entraînant un arrêt ou une dégradation 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 secrétariat de la défense et de la sécurité nationale (SGDSN) [2].

Classe 1 : Un PCA ou un PRA, même succinct, devrait être mis en place.

Classe 2 : Un PCA ou un PRA devrait être mis en place. Son efficacité devrait être testée de manière régulière.

Classe 3 : Un PCA ou un PRA doit être mis en place. Ce plan doit répondre à l'ensemble des scénarios d'incident menant à un arrêt du service rendu ayant un impact lourd. Son efficacité doit être testée de manière régulière et au moins une fois par an. Un plan de continuité, ayant une portée plus large que la cybersécurité, pourra être demandé par les ministères coordinateurs.

Les mesures détaillées correspondantes se trouvent dans la section 3.5.1 du guide des mesures [9].

2.2.8 Modes d'urgence

Les mesures prises pour améliorer la cybersécurité ne doivent bien évidemment pas abaisser le niveau de sûreté des systèmes industriels. Il peut être nécessaire de mettre en place des procédures de type « bris de glace » pour permettre une intervention rapide suite à un incident métier.

L'analogie suivante illustrera le propos. En cas d'incendie dans un bâtiment, les portes sous contrôle d'accès s'ouvrent automatiquement. Les personnes ne sont ainsi pas obligées de « badger » pour évacuer. Il s'agit d'un mode d'urgence.

Classe 1 : Les modes d'urgence devraient être mis en place et bien encadrés pour qu'ils ne constituent pas une vulnérabilité exploitable. Ils devraient être intégrés à l'analyse de risque et les procédures associées devraient être explicitées dans la PSSI. En particulier, la traçabilité des opérations devrait être préservée.

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

Classe 3 : Les modes d'urgence doivent être mis en place et bien encadrés pour qu'ils ne constituent pas une vulnérabilité supplémentaire pour le système. Ils doivent être pris en compte dans l'analyse de risque et les procédures associées doivent être explicitées dans la PSSI. En particulier, la traçabilité des opérations doit être préservée.

Les mesures détaillées correspondantes se trouvent dans la section 3.5.2 du guide des mesures [9].

2.2.9 Processus d'alerte et de gestion de crise

Un processus d'alerte et de gestion de crise permet de mettre en place les procédures de réaction aux scénarios d'incident qui ont été identifiés à l'aide de l'analyse de risque.

Classe 1 : Un processus d'alerte même minimal devrait être mis en place.

Classe 2 : Un processus de gestion de crise devrait être mis en place. Il devrait être testé régulièrement pour vérifier son efficacité.

Classe 3 : Un processus d'alerte et de gestion de crise doit être défini. Il doit être testé régulièrement, et au minimum une fois par an, pour vérifier son efficacité. La chaîne de traitement opérationnelle doit être communiquée à l'autorité de cyberdéfense.

Les mesures détaillées correspondantes se trouvent dans la section 3.5.3 du guide des mesures [9].

2.2.10 Interconnexions réseau

Les interconnexions sont une source forte de vulnérabilités et il est nécessaire de considérer soigneusement les risques avant d'interconnecter deux réseaux.

Il est nécessaire de cloisonner au maximum les réseaux. En particulier, nous veillerons soigneusement aux interconnexions entre un système industriel et un réseau public (téléphone, internet), entre un système industriel et un système d'information de gestion ainsi qu'entre des systèmes industriels de classes de cybersécurité différentes.

Classe 1 : Voici les recommandations selon les différents types d'interconnexion.

Systèmes industriels : Les systèmes industriels de classe 1 devraient être cloisonnés entre eux à l'aide de pare-feu. Un équipement labellisé devrait être utilisé pour réaliser l'interconnexion.

Système d'information de gestion : Le système industriel doit être cloisonné du système d'information de gestion à l'aide d'un pare-feu. Un équipement labellisé devrait être utilisé pour réaliser l'interconnexion.

Réseau public : Les systèmes industriels qui ne le justifient pas impérativement ne devraient pas être exposés sur Internet. Le cas échéant, des mesures devraient être prises afin de s'assurer qu'ils ne sont accessibles qu'aux personnes autorisées. Les risques engendrés par une telle solution devraient être identifiés clairement.

Classe 2 : Systèmes industriels : Les systèmes industriels de classe 2 devraient être cloisonnés entre eux à l'aide de pare-feu. Un équipement labellisé devrait être utilisé pour réaliser l'interconnexion. L'interconnexion d'un système industriel de classe 2 et d'un système industriel de classe 1 devrait être unidirectionnelle vers le système de classe 1. Un équipement labellisé devrait être utilisé pour réaliser l'interconnexion.

Système d'information de gestion : L'interconnexion devrait être à sens unique depuis le système industriel vers le système d'information de gestion. Dans le cas contraire, l'ensemble des flux vers le système industriel de classe 2 devraient être clairement définis et limités. Les risques associés devraient être identifiés et évalués.

L'interconnexion doit être réalisée avec un équipement de sécurité comme un pare-feu. Celui-ci devrait être labellisé.

Réseau public : Les systèmes industriels qui ne le justifient pas impérativement par un besoin opérationnel ne doivent pas être connectés à un réseau public. Le cas échéant, ils ne devraient pas être exposés sans protection et les risques engendrés par une telle solution devraient être identifiés clairement. L'interconnexion devrait être unidirectionnelle vers le réseau public. Un équipement labellisé devrait être utilisé pour réaliser l'interconnexion.

Classe 3 : Systèmes industriels : Les systèmes industriels de classe 3 doivent être cloisonnés entre eux à l'aide de pare-feu. Il est fortement recommandé d'utiliser un équipement labellisé pour réaliser l'interconnexion.

L'interconnexion d'un système industriel de classe 3 et d'un système industriel de classe inférieure doit être unidirectionnelle vers le système de classe inférieure. L'unidirectionnalité doit être garantie physiquement (avec une diode, par exemple). Un équipement labellisé devrait être utilisé pour réaliser l'interconnexion.

Système d'information de gestion : L'interconnexion doit être unidirectionnelle vers le système d'information de gestion. L'unidirectionnalité doit être garantie physiquement (avec une diode, par exemple). Un équipement labellisé devrait être utilisé pour réaliser l'interconnexion.

Réseau public : Un système industriel de classe 3 ne doit pas être connecté à un réseau public.

Remarque

Une infrastructure louée auprès d'un opérateur de télécommunication avec des ressources dédiées (comme un MPLS) n'est pas considérée comme un réseau public dès lors que les ressources sont cloisonnées logiquement du reste du trafic (par exemple avec des labels MPLS) et que l'opérateur offre des garanties de service.
On pourra noter que ce type de solution ne garantit pas nécessairement la confidentitalité ou l'intégrité des flux et ne dispense en aucun cas l'entité responsable d'appliquer les mesures adaptées (comme un VPN) pour assurer l'authenticité, l'intégrité voire la confidentialité des flux.

Les mesures détaillées correspondantes se trouvent dans la section 4.2.1 du guide des mesures [9].

2.2.11 Télédiagnostic, télémaintenance et télégestion

Classe 1 : Des procédures claires devraient être définies et des moyens de protection devraient être mis en place pour encadrer les opérations de télédiagnostic, télémaintenance et télégestion.

Pour les opérations de télédiagnostic comme pour les opérations de télémaintenance, il est recommandé d'utiliser des produits labellisés.

Classe 2 : Les opérations de télémaintenance ou de télégestion sont fortement déconseillées. Le cas échéant, l'équipement utilisé devrait garantir l'authenticité et l'intégrité de la communication. Cet équipement devrait être labellisé.

Classe 3 : Les opérations de télémaintenance ou de télégestion ne doivent pas être autorisées.

Les opérations de télédiagnostic sont possibles à l'aide d'équipements garantissant physiquement l'impossibilité d'interagir avec le réseau de classe 3. Des produits labellisés devraient être utilisés.

Remarque

Lorsque les besoins opérationnels le justifient impérativement, la télémaintenance et la télégestion pourront être autorisées pour les systèmes industriels de classe 3.
Mais dans ce cas, elles devront être effectuées depuis un site qui sera également de classe 3 et qui devra être inclus dans l'analyse de risque du système industriel. En particulier, les mesures portant sur l'interconnexion présentées dans la section 2.2.10 s'appliquent.

Les mesures détaillées correspondantes se trouvent dans la section 4.2.4 du guide des mesures [9].

2.2.12 Surveillance et moyens de détection

La mise en place de moyens de surveillance et de détection augmente la visibilité sur le système industriel concerné et augmente la vitesse de réaction en cas d'attaque, permettant d'en limiter les conséquences.

Classe 1 : Un système de gestion des journaux d'événements des différents équipements présents dans le réseau devrait être mis en place. Une politique de gestion des événements devrait également être définie.

Classe 2 : Des moyens de détection d'intrusion devraient être déployés en périphérie des systèmes industriels et sur les points identifiés comme critiques qui comprennent notamment :

- les interconnexions avec Internet (y compris la télémaintenance) ;
- les interconnexions avec le système d'information de gestion ;
- les points de connexion spécifiques vers l'extérieur (WiFi industriel par exemple) ;
- sur les réseaux d'automates jugés sensibles.

Les moyens de détection utilisés devraient être labellisés.

Classe 3 : Des moyens de détection d'intrusion doivent être mis en place en périphérie des systèmes industriels et sur les points identifiés comme critiques qui comprennent notamment :

- les interconnexions des équipements de télégestion ;
- les interconnexions entre les systèmes d'information de gestion et systèmes industriels ;

— les points de connexion spécifiques vers l'extérieur (WiFi industriel par exemple) ;

— les stations sas ou les stations blanches ;

— le réseau fédérateur des postes de supervision industriel (SCADA [3]) ;

— les réseaux d'automates jugés sensibles.

Les moyens de détection utilisés devraient être labellisés.

Remarque

Le déploiement de moyens de détection suppose également la mise en place d'outils de centralisation et d'analyse afin de traiter les événements collectés.

Les mesures détaillées correspondantes se trouvent dans la section 4.4 du guide des mesures [9].

2.3 Homologation

L'homologation est le processus de vérification du niveau de cybersécurité qui accompagne la mise en route d'un nouveau système industriel. Le dossier d'homologation doit contenir la réponse à l'ensemble des mesures listées dans le présent document. Le processus d'homologation consiste essentiellement à vérifier que l'analyse de risque du système industriel a été faite correctement ; que les mesures issues de celle-ci ont été mises en place et que les risques résiduels sont acceptables. Lors de l'homologation, l'autorité de cyberdéfense donne une autorisation préalable de mise en service et l'entité responsable accepte les risques résiduels.

Classe 1 : Il est recommandé de traiter les risques relevés lors de l'analyse de risque jusqu'à ce que l'entité responsable estime les risques résiduels acceptables.

Classe 2 : Les systèmes industriels doivent être homologués par l'entité responsable. L'homologation, dans ce cas, relève d'un principe déclaratif.

Classe 3 : Les systèmes industriels doivent être homologués et requièrent une autorisation préalable de mise en service. L'homologation doit être faite par un organisme extérieur accrédité.

3. Supervisory Control And Data Acquisition.

Remarque

Afin de ne pas multiplier les procédures, l'homologation de cybersécurité peut s'intégrer dans les procédures d'homologation déjà existantes dans certains secteurs.

Chapitre 3

Méthode de classification

3.1 Contexte

L'objectif de ce chapitre est de décrire la méthode de classification des systèmes industriels. Les classes de cybersécurité sont déterminées en fonction d'un impact et d'une vraisemblance. La méthode reprend des termes et concepts que l'on retrouve dans des méthodes d'analyse de risque (comme la méthode EBIOS [1] [7] par exemple) sans être une analyse de risque complète. Le cheminement de la méthode est résumé sur la figure 3.1. Les impacts peuvent s'estimer simplement à partir de grilles. En revanche, l'estimation de la vraisemblance demande plusieurs étapes intermédiaires.

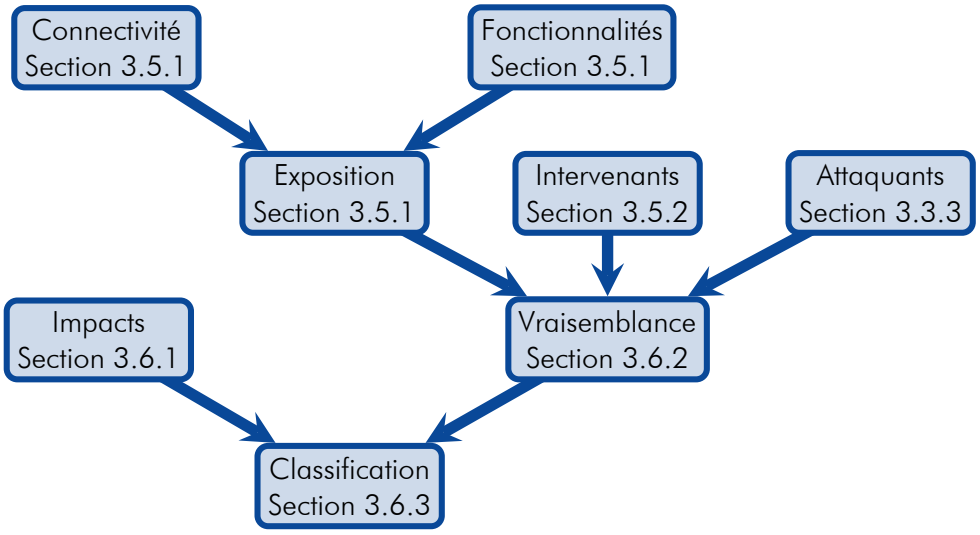

Figure 3.1 – Schéma de la méthode de classification

1. Expression des besoins et identification des objectifs de sécurité.

3.1.1 Périmètre

Le périmètre doit être choisi afin de contenir l'ensemble des installations critiques d'un site ou d'une infrastructure (réseaux, transport, électricité, etc.). Inversement, il est possible de découper un site en plusieurs systèmes industriels qui auront potentiellement des niveaux de criticité différents.

S'il est décidé de découper une infrastructure en plusieurs systèmes industriels, une analyse de risque de l'ensemble complet devra être menée pour vérifier que toutes les menaces ont bien été prises en compte, y compris celles qui pourraient résulter de l'infrastructure prise dans son ensemble.

Les analyses de sûreté de fonctionnement, bien souvent déjà effectuées par les entités responsables, peuvent servir de base de travail. En effet, le découpage des systèmes et les processus qu'ils supportent sont déjà définis.

Exemple

Le périmètre doit être choisi de manière cohérente en fonction du risque et de l'architecture des systèmes analysés.
Ainsi, il peut être cohérent d'effectuer une analyse pour les installations de gestion technique d'un tunnel routier (aération, éclairage, prévention des incendies…) indépendamment du reste des systèmes présents au bord de la route (signalisation, téléphones de secours…). Néanmoins, pour que cette séparation soit possible et cohérente, il est nécessaire que la limite entre les deux systèmes soit clairement identifiable. Dans le cas contraire, l'analyse doit être menée pour l'ensemble.

La méthode peut être appliquée de manière itérative :
Dans un premier temps, elle est appliquée à l'ensemble d'une infrastructure ou d'un site afin d'identifier le niveau de classe le plus élevé auquel il faudra répondre. Dans un second temps, une fois la cartographie fonctionnelle établie, la méthode pourra être appliquée sur des sous-ensembles plus restreints. Ces sous-ensembles sont parfois appelés «zones» dans la littérature.

Important

Compte tenu de l'impact potentiel de certaines mesures présentées précédemment, il est important de déterminer de manière précise le périmètre étudié. Plus les systèmes industriels seront précis, plus les mesures applicables seront limitées au strict nécessaire.
Une mauvaise définition du périmètre pourrait conduire à imposer des mesures de classe 3 par exemple à des systèmes industriels de classe 2 seulement.

Exemple

Un site de type SEVESO seuil haut sera globalement de classe 3. En affinant le découpage des systèmes industriels, il apparaîtra sans doute que seuls les systèmes de protection des biens et des personnes doivent être de classe 3. Les systèmes de production seront, eux, sans doute de classe 1 ou 2.

3.2 Critères de sécurité

Pour les critères de sécurité, ne sont retenus que les deux principaux qui sont les plus souvent rencontrés dans les systèmes industriels, de par leur lien fort avec la sûreté de fonctionnement : la disponibilité et l'intégrité.

Remarque

En fonction des secteurs, il sera possible d'ajouter d'autres critères de sécurité comme la confidentialité, la traçabilité ou l'imputabilité mais ils ne sont pas pris en compte dans cette étude.

3.3 Échelles

Plusieurs échelles sont nécessaires pour mesurer l'impact et la vraisemblance d'une attaque.

3.3.1 Gravité

Pour la gravité, une échelle de 1 à 5 a été retenue avec les niveaux suivants : insignifiant, mineur, modéré, majeur, catastrophique. La gravité est mesurée en fonction des différents impacts qui sont considérés : humains, environnementaux, économiques. Des déclinaisons sont données à titre d'exemple dans les trois tableaux suivants ; elles devront être adaptées et précisées pour chaque secteur d'activité. Pour les secteurs d'importance vitale par exemple, l'article L1332-3 du code de la défense définit des critères complémentaires. Par ailleurs, l'article L511-1 du code de l'environnement, précise également des impacts.

	Niveau	Qualificatif	Description des conséquences
Impacts humains	1	Insignifiant	Accident déclaré sans arrêt ni traitement médical.
	2	Mineur	Accident déclaré avec arrêt ou traitement médical.
	3	Modéré	Invalidité permanente.
	4	Majeur	Un décès.
	5	Catastrophique	Plusieurs décès.

	Niveau	Qualificatif	Description des conséquences
Impacts environnementaux	1	Insignifiant	Dépassement limité et passager d'une norme de rejet sans exigence légale de déclaration aux autorités
	2	Mineur	Dépassement d'une norme de rejet exigeant déclaration aux autorités mais sans conséquence pour l'environnement.
	3	Modéré	Pollution modérée limitée au site.
	4	Majeur	Pollution significative ou externe au site. Évacuation de personnes.
	5	Catastrophique	Pollution majeure avec conséquences environnementales durables externes au site.

	Niveau	Qualificatif	Description des conséquences
Impacts consécutifs à l'arrêt du service rendu	1	Insignifiant	Impacts lourds sur 1 000 personnes.
	2	Mineur	Impacts lourds sur 10 000 personnes. Perturbation de l'économie locale.
	3	Modéré	Impacts lourds sur 100 000 personnes. Perturbation de l'économie régionale. Perte temporaire d'infrastructure majeure.
	4	Majeur	Impacts lourds sur 1 000 000 de personnes. Perturbation de l'économie nationale. Perte temporaire d'une infrastructure critique. Perte définitive d'une infrastructure majeure.
	5	Catastrophique	Impacts lourds sur 10 000 000 de personnes. Perte définitive d'une infrastructure critique.

Remarque

Les impacts dépendent très largement du secteur concerné. C'est pourquoi il pourra être nécessaire de préciser les grilles par secteur. Des critères complémentaires propres à un secteur ou à un organisme pourront être ajoutés.

3.3.2 Vraisemblance

La vraisemblance, quant à elle, peut être obtenue en appliquant la méthode proposée au paragraphe 3.6.2. Du fait de la difficulté d'estimer la fréquence d'occurrence d'une attaque, cette échelle n'est pas quantitative.

	Niveau	Qualificatif
Vraisemblance	1	Très faible
	2	Faible
	3	Moyenne
	4	Forte

3.3.3 Niveau de l'attaquant

Cette grille est nécessaire pour l'évaluation de la vraisemblance. La classification suivante est proposée pour le niveau de l'attaquant.

	Niveau	Qualificatif	Description/Exemples
Attaquant	1	Non ciblé	Virus, robots…
	2	Hobbyiste	Personnes avec des moyens très limités, pas nécessairement de volonté de nuire.
	3	Attaquant isolé	Personne ou organisme avec des moyens limités mais avec une certaine détermination (employé licencié, par exemple).
	4	Organisation privée	Organisme aux moyens conséquents (terrorisme, concurrence déloyale, par exemple).
	5	Organisation étatique	Organisme aux moyens illimités et à la détermination très forte.

Étant donné que les systèmes industriels ont une durée de vie très longue, il paraît peu probable qu'aucune personne déterminée avec des moyens limités ne veuille porter atteinte au système industriel dans l'intervalle. Il est donc proposé de fixer le niveau de l'attaquant au minimum à 3. Le niveau de l'attaquant devra également être décliné par secteur d'activité. Il pourra éventuellement être personnalisé pour un organisme donné, mais uniquement pour être aggravé par rapport à la référence du secteur.

3.4 Biens essentiels

Selon la définition utilisée dans la méthode EBIOS, les biens essentiels sont les informations et les processus jugés importants pour l'organisme. Dans le cas présent, les biens essentiels sont les processus portés par le système industriel étudié dont l'affectation pourrait impliquer des dommages pour les personnes, l'environnement ou le fonctionnement du pays. Ce travail d'analyse des processus (parfois appelé fonctionnalités ou services) a souvent déjà était fait dans les analyses de risque de sûreté de fonctionnement, analyses de risque financier, etc.

Exemple

Dans le cas d'un tunnel routier, les biens essentiels seront constitués, par exemple, des fonctions de recyclage de l'air, de la gestion de l'éclairage, de la gestion des moyens de secours et de protection contre les incendies. En effet, une atteinte à l'une de ces fonctions peut avoir un impact sur la sécurité des usagers ou sur le bon écoulement du trafic routier dans le tunnel.

3.5 Biens supports

Les biens supports sont les composants, les sous-systèmes du système étudié.

Exemple

Dans le cas d'un tunnel routier, les biens supports comprennent notamment les postes utilisateurs, automates, serveurs, capteurs, détecteurs (opacimètres, anénomètres, analyseurs CO), caméras.

3.5.1 Architectures types

La surface d'attaque d'un système industriel dépend en grande partie de son architecture. Afin d'évaluer simplement les risques liés à cette dernière, il est proposé d'évaluer un système industriel en fonction de deux échelles : son niveau de fonctionnalité et sa connectivité avec l'extérieur.

Fonctionnalités d'un système industriel

En ce qui concerne le niveau de fonctionnalité, la classification obtenue coïncide essentiellement avec les différentes couches habituellement utilisées dans le modèle de «production intégrée par ordinateur» (CIM [2]) et qui sont rappelés ici pour mémoire :

CIM 0 capteurs et actionneurs non communicants,

CIM 1 automates (PLC [3]) et analyseurs,

CIM 2 supervision (SCADA),

CIM 3 système d'exécution des fabrications (MES [4]),

2. Computer Integrated Manufacturing.
3. Programmable Logic Controller.
4. Manufacturing Execution System.

CIM 4 planification, gestion des ressources (ERP [5]).

Il faut noter qu'un système industriel ne contenant que des éléments au niveau CIM 0 a peu de chances d'exister. C'est pourquoi ce niveau n'est pas conservé dans la classification. Par ailleurs, il apparait que le niveau CIM 4 n'apporte pas de vulnérabilités additionnelles par rapport au niveau CIM 3. Ces deux niveaux sont donc considérés conjointement.

> **Remarque**
>
> Il a été décidé d'accorder un traitement spécial aux consoles de programmation et stations d'ingénierie qui apportent des outils additionnels importants à un attaquant. Leur présence permanente dans le système industriel suffit à justifier un niveau maximal.

C'est ainsi que nous obtenons les niveaux de fonctionnalité suivants, représentés sur la figure 3.2.

Fonctionnalité 1 : Systèmes minimaux. Cette catégorie contient les systèmes industriels avec uniquement des éléments de niveau CIM 0 et 1 (contrôle-commande) à l'exclusion des consoles de programmation, à savoir :

- capteurs/actionneurs,
- entrées/sorties déportées,
- automates,
- pupitres,
- systèmes embarqués,
- analyseurs.

Fonctionnalité 2 : Systèmes complexes. Cette catégorie contient les systèmes industriels ne contenant que des éléments de niveau CIM 0 à 2 (contrôle-commande et SCADA). Ainsi, s'ajoutent aux éléments de la catégorie précédente :

- stations de supervision,
- serveurs d'historique local (Historian),
- bases de données locales.

5. Enterprise Resource Planning.

Fonctionnalité 3 : Systèmes très complexes. Cette catégorie contient tous les systèmes industriels ne rentrant pas dans les deux premières catégories. En particulier, y sont contenus tous les systèmes industriels avec des consoles de programmation ou des stations d'ingénierie connectées en permanence ou bien les systèmes qui sont connectés à un système d'exécution des fabrications ou encore des systèmes industriels comportant des bases de données d'historiques centralisées.

Remarque

Les systèmes numériques de contrôle-commande (SNCC) comportent nativement des fonctionnalités comme les stations d'ingénierie pouvant être optionnelles dans d'autres systèmes. Sauf cas particulier, les SNCC seront considérés en niveau de fonctionnalité 3.

Remarque

Les historiques ont été séparés en deux niveaux de fonctionnalités différents. Les historiques locaux sont à proximité du SCADA, et parfois intégrés dans celui-ci et la durée de rétention des données est courte. Les historiques centralisés peuvent contenir les données de plusieurs SCADA et la durée de rétention est plus importante.

Connectivité d'un système industriel

Connectivité 1 : Système industriel isolé. Cette catégorie correspond à tous les réseaux de production complètement fermés.

Connectivité 2 : Système industriel connecté à un système d'information de gestion. Cette catégorie correspond à tous les réseaux de production qui sont reliés au système d'information de gestion de l'entreprise mais sans que des opérations depuis l'extérieur du système d'information de gestion ne soient autorisées.

Connectivité 3 : Système industriel utilisant de la technologie sans fil. Cette catégorie contient tous les systèmes industriels faisant usage de technologie sans fil.

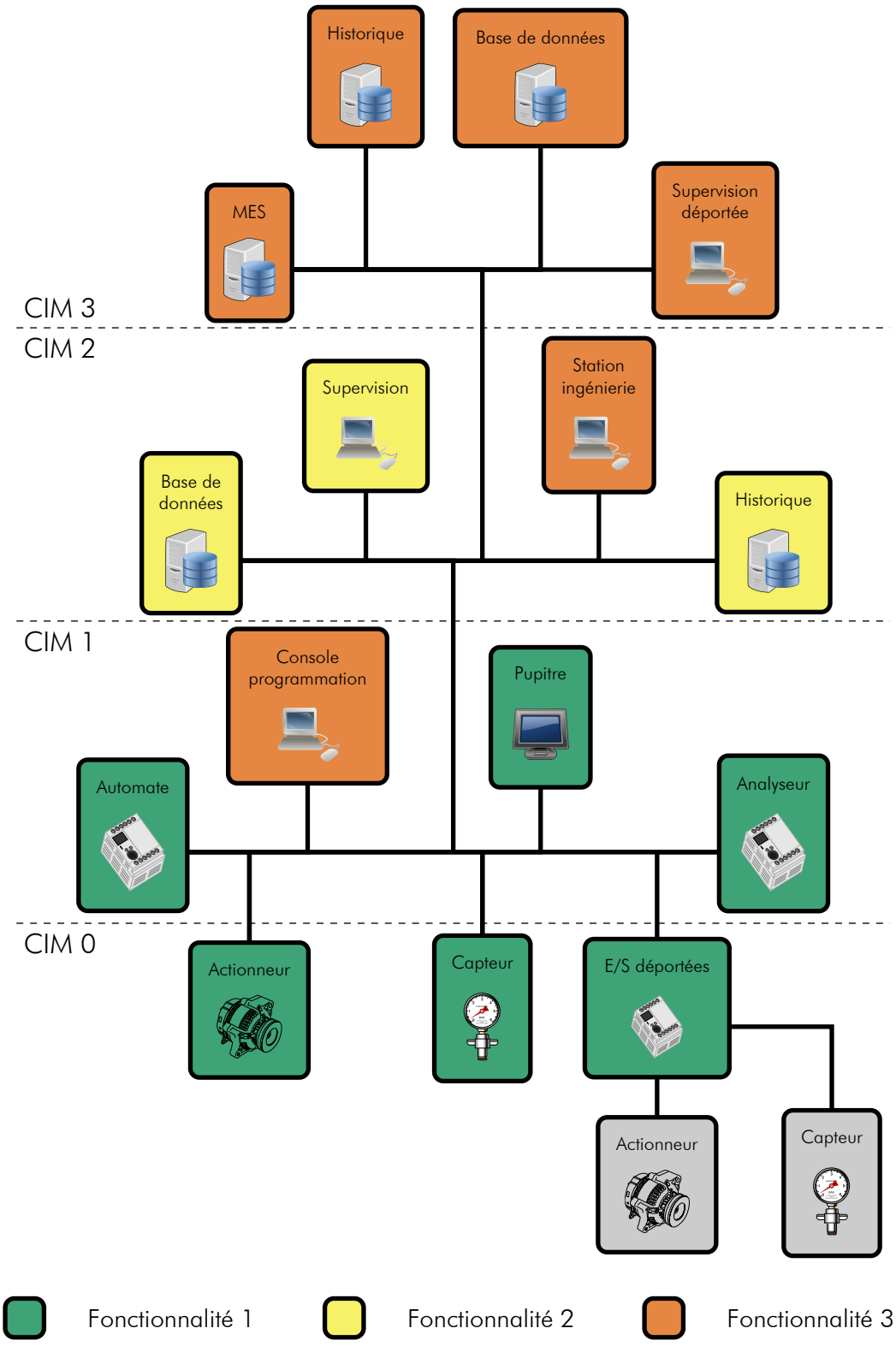

Figure 3.2 – Niveaux de fonctionnalité.

Connectivité 4 : Système industriel distribué avec infrastructure privée ou permettant des opérations depuis l'extérieur. Cette catégorie correspond à un système distribué où les différents sites communiquent entre eux par le biais d'une infrastructure privée. Celle-ci pourra être complètement privée ou être louée auprès d'un opérateur de télécommunications.

Rentrent également dans cette catégorie tous les systèmes industriels permettant de faire des opérations depuis l'extérieur du site ou depuis un réseau de gestion (par exemple télédiagnostic et télémaintenance).

Connectivité 5 : Système industriel distribué avec infrastructure publique. Cette catégorie correspond à la catégorie précédente, sauf que l'infrastructure utilisée est publique, comme celle d'un opérateur de télécommunications. Ce cas correspond typiquement à une infrastructure de distribution d'eau, par exemple.

Les différentes catégories décrites précédemment sont résumées sur les schémas suivants. Sur la figure 3.3, nous pouvons voir un système industriel de connectivité 1. Le système industriel est complètement déconnecté et se trouve sur un seul site fermé.

Dans cette catégorie, la surface d'attaque est limitée mais non nulle. En effet, les vecteurs d'entrée existent malgré tout, du fait des supports amovibles, des machines des opérateurs de maintenance ou de la malveillance interne.

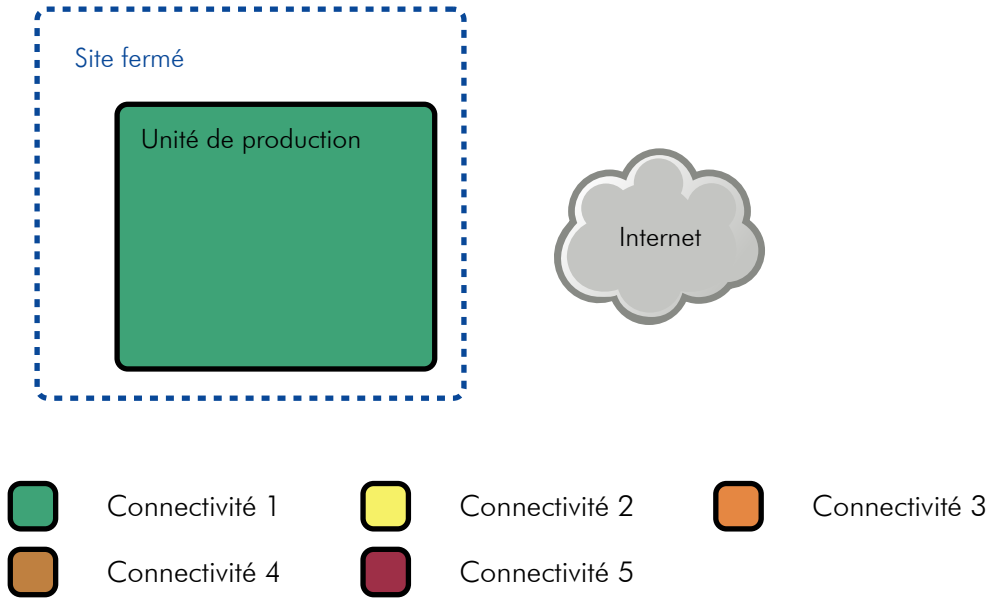

Figure 3.3 – Système industriel de connectivité 1.

Sur la figure 3.4, le système industriel est de connectivité 2 ; il est toujours sur un seul site fermé mais est désormais relié à un réseau de gestion. Il n'y a pas d'hypothèse particulière sur le réseau de gestion qui peut être relié à un réseau public comme Internet ou même distribué sur plusieurs sites.

Dans cette catégorie, la surface d'attaque comprend tout ce qui a été envisagé dans la catégorie 1 avec, en plus, les attaques depuis le système d'information de gestion.

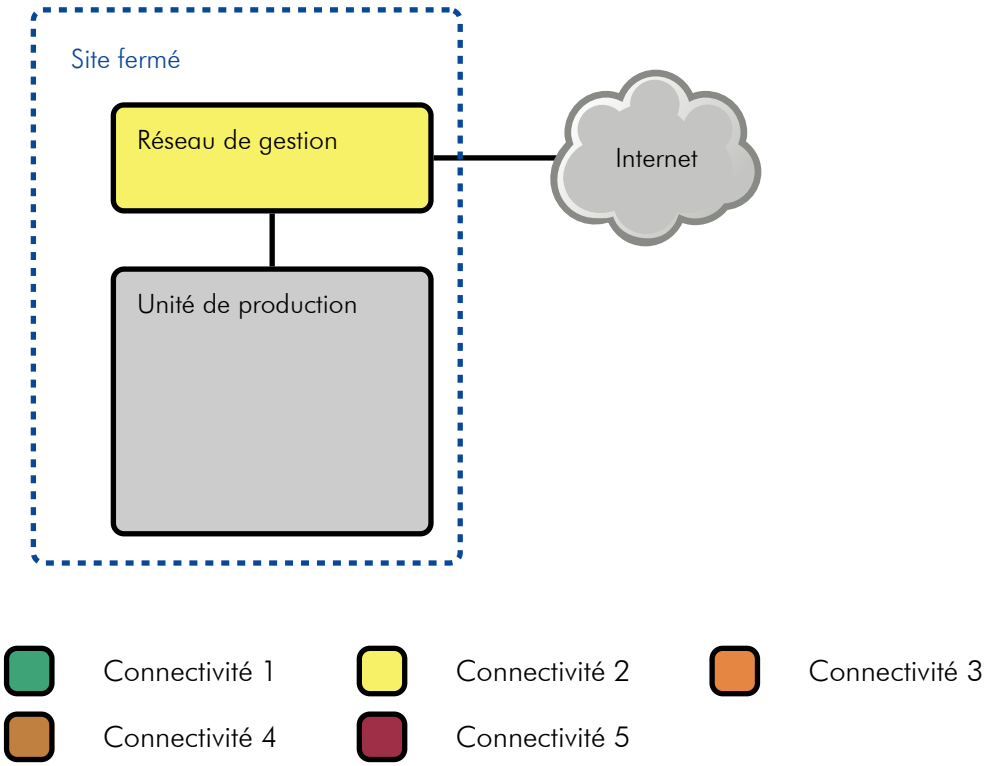

Figure 3.4 – Système industriel de connectivité 2.

Sur la figure 3.5, le système industriel est de connectivité 3 ; il y est fait usage de technologie sans-fil.

Dans cette catégorie, la surface d'attaque comprend toutes les vulnérabilités inhérentes au sans-fil. En particulier, il existe des attaques en disponibilité contre lesquelles il n'est pas possible de se prémunir facilement.

La figure 3.6 représente un système industriel de connectivité 4 avec la même nomenclature que précédemment. Les deux points essentiels sont l'utilisation d'une infrastructure privée de communication et la présence de systèmes de télémaintenance.

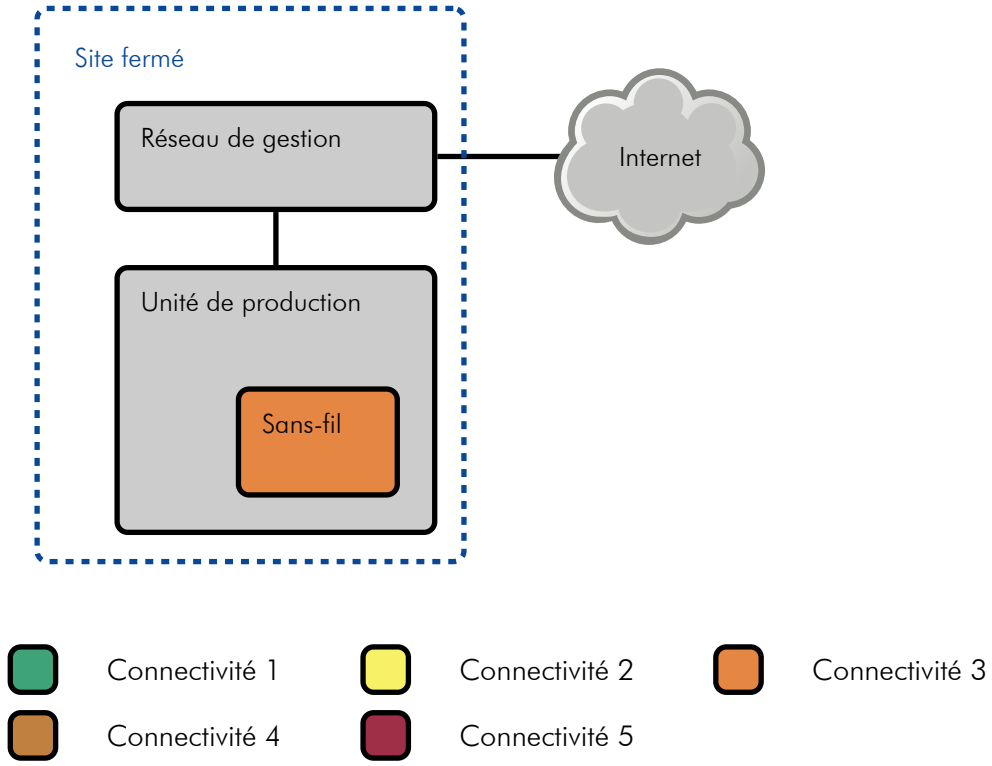

Figure 3.5 – Système industriel de connectivité 3.

On appelle infrastructure privée tout réseau qui serait entièrement sous le contrôle de l'entité responsable du système industriel mais également tout système d'un opérateur de télécommunications dont une part des ressources est dédiée au système industriel en question et qui ne permet pas simplement à des extérieurs d'interférer avec le système. Des infrastructures telles que des APN [6] privés ou un VPN [7] de type MPLS [8] entrent dans cette catégorie. Dans tous les cas, des mesures de protection doivent être prises pour assurer l'intégrité, voire la confidentialité, sur un tel réseau. Néanmoins, les vulnérabilités sont moindres que dans le cas d'une infrastructure publique.

Dans cette catégorie, la surface d'attaque contient tous les cas précédents avec de nouvelles vulnérabilités potentielles liées à la présence d'une infrastructure qu'il est très difficile, voire impossible de surveiller/contrôler dans son intégralité notamment du point de vue des accès physiques. Sont également présentes toutes les vulnérabilités liées aux opérations de télémaintenance.

6. Access Point Name.
7. Virtual Private Network.
8. Multiprotocol Label Switching.

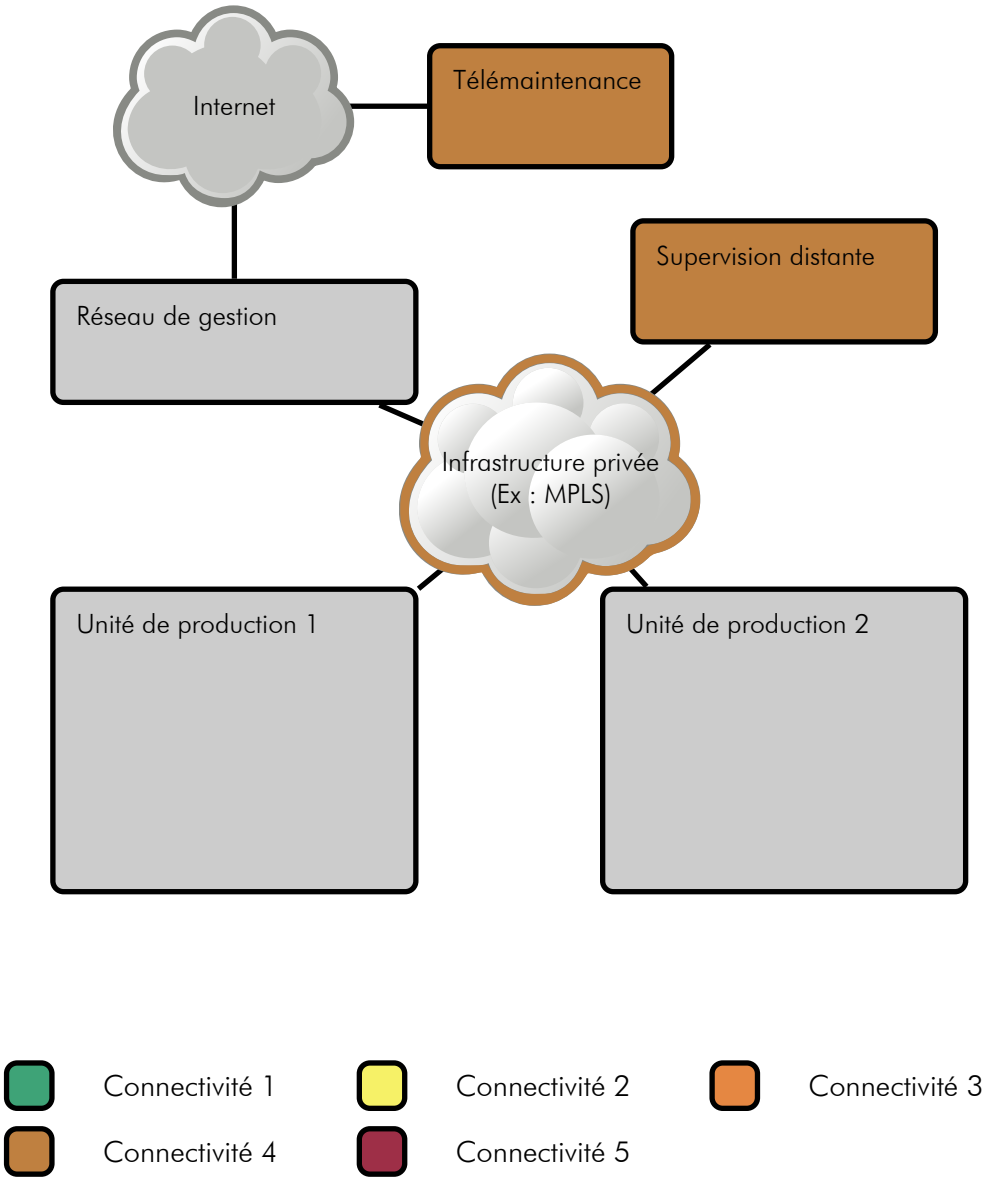

Figure 3.6 – Système industriel de connectivité 4.

Enfin, la figure 3.7 représente une système industriel de connectivité 5. Dans ce cas, la connectivité entre les différents éléments du système industriel est assurée par une infrastructure publique telle que le réseau téléphonique ou Internet. En particulier, un attaquant pourra accéder sans entrave aux différents points d'entrée du système industriel et il sera donc nécessaire d'appliquer des mesures de protection supplémentaires. Par ailleurs, aucune ressource n'est dédiée au système industriel et ce dernier pourra être une victime collatérale d'une utilisation anormalement élevée du réseau.

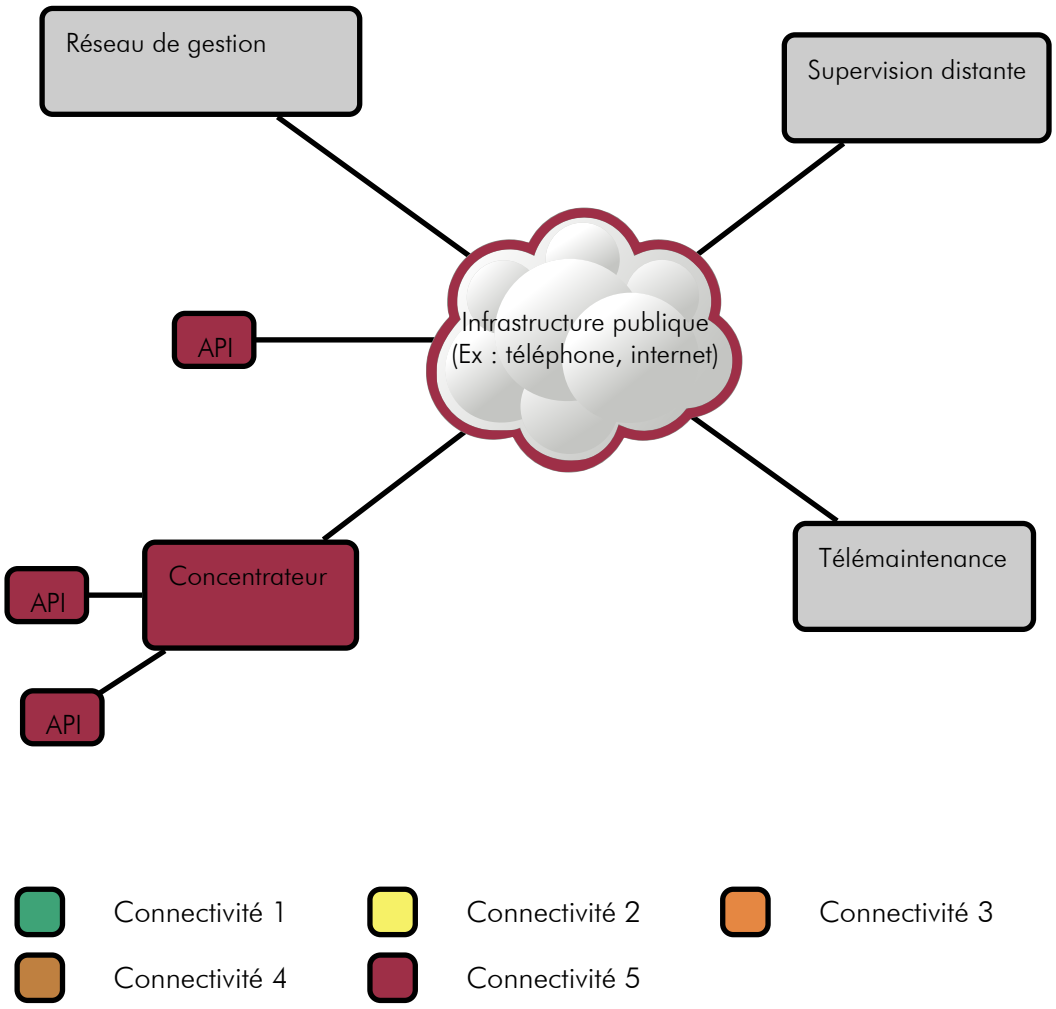

Figure 3.7 – Système industriel de connectivité 5.

Exposition du système industriel

L'exposition du système industriel résulte de ses niveaux de fonctionnalité et de connectivité. Nous proposons 5 niveaux d'exposition allant de 1 (le moins exposé) à 5 (le plus exposé).

Le niveau d'exposition est obtenu de la façon suivante :

F3	Exposition 3	Exposition 3	Exposition 4	Exposition 4	Exposition 5
F2	Exposition 2	Exposition 2	Exposition 3	Exposition 4	Exposition 5
F1	Exposition 1	Exposition 2	Exposition 3	Exposition 4	Exposition 5
Fonct./Conn.	**C1**	**C2**	**C3**	**C4**	**C5**

On pourra noter que les niveaux de fonctionnalité et de connectivité n'évoluent pas de façon indépendante. Il y a donc certaines cases du tableau précédent qui peuvent ne correspondre à aucun système industriel réel.

Remarque

Beaucoup d'autres facteurs auraient pu être pris en compte dans l'analyse et ont été laissés de côté pour des raisons de simplicité. Parmi ceux-ci, se trouvent la taille du système industriel (le nombre d'équipements qui le composent) et l'hétérogénéité des équipements utilisés.
Dans le cadre d'une analyse de risque complète, il est nécessaire de prendre en compte ces facteurs.

3.5.2 Accessibilité du système industriel

Le personnel intervenant sur un système industriel est un vecteur important de vulnérabilités. Il a été décidé de classer les intervenants en deux catégories. Les intervenants légitimes sont toutes les personnes ayant le droit d'interagir avec le système industriel de manière contrôlée. Ces intervenants peuvent être les opérateurs qui veillent au bon fonctionnement du système au quotidien mais également le personnel responsable de sa maintenance ou de son évolution. Les intervenants illégitimes sont toutes les personnes qui peuvent être amenées à interagir avec le système industriel sans être contrôlées, que cette interaction soit volontaire ou non.

Remarque

La formation et la sensibilisation évoquées pour une personne habilitée n'ont pas forcément besoin d'être reconnues par un organisme de formation ; il peut s'agir d'une formation interne.
Néanmoins, il est demandé à ce qu'elles soient clairement définies par l'entité responsable et cette dernière devra s'assurer que les intervenants les ont bien suivies.

Intervenants 1 : autorisés, habilités et contrôlés L'ensemble des intervenants autorisés sont habilités et contrôlés. Une intervention non-autorisée n'est pas possible.

Intervenants 2 : autorisés et habilités L'ensemble des intervenants autorisés sont habilités mais au moins une partie des opérations possibles n'est pas tracée. Une intervention non-autorisée n'est pas possible.

Intervenants 3 : autorisés Il n'y a pas d'exigence particulière sur les intervenants autorisés mais une intervention non-autorisée n'est pas possible.

Intervenants 4 : non-autorisés Cette catégorie contient tous les systèmes industriels dans lesquels une intervention non-autorisée est possible.

Exemple

Un système industriel dont l'ensemble des équipements sont protégés par un système avec contrôle d'accès strict, dont l'accès logique aux équipements est protégé par une authentification et où les actions des intervenants sont journalisées est dans la catégorie 1.
En revanche, un système industriel dont les équipements sont protégés par contrôle d'accès mais dont certains équipements ne nécessitent pas d'authentification est en catégorie 2.
Un système industriel dont les équipements ne sont pas (ou mal) protégés et donc accessibles au public ou à du personnel non concerné (personnel d'entretien des locaux non-habilité, par exemple) est en catégorie 4.

3.6 Détermination de la classe

3.6.1 Estimation de l'impact

On rappelle que, pour chaque bien essentiel, les critères de sécurité pris en compte sont l'intégrité et la disponibilité.

A l'aide de la liste des biens essentiels qui a été établie, l'entité responsable peut énumérer les événements redoutés et estimer leur impact selon les échelles données à la section 3.3.

L'événement redouté ayant l'impact le plus grave est conservé pour déterminer la classe du système industriel.

Exemple

La perte de disponibilité du système de ventilation d'un tunnel peut conduire à un impact humain de gravité 3, un impact sur l'environnement de 1 et un impact consécutif à l'arrêt du service rendu (le tunnel est fermé à la circulation) de 1. La perte de l'intégrité du même système ne conduit pas à des impacts plus importants. La gravité retenue sera de 3.
En revanche, la perte de disponibilité du système de traitement des produits toxiques d'une usine conduit à un impact humain de 1, un impact environnemental de 2 et un impact consécutif à l'arrêt du service rendu de 1 alors que la perte d'intégrité de ce même système conduit à un impact humain de 4, un impact environnemental de 3, et un impact consécutif à l'arrêt du service rendu de 1. La gravité retenue sera de 4.

3.6.2 Estimation de la vraisemblance

Pour le calcul de la vraisemblance, nous nous appuyons sur l'exposition qui a été calculée au 3.5.1. Les échelles *Intervenants* et *Attaquant* sont alors utilisées comme des facteurs aggravants pour le calcul de la vraisemblance selon la formule suivante :

$$V = E + \left\lceil \frac{A + I - 2}{2} \right\rceil$$

où V est la vraisemblance, E l'exposition, I les intervenants et A le niveau de l'attaquant. L'opérateur mathématique $\lceil . \rceil$ dénote la partie entière supérieure.

3.6.3 Classification

Les événements redoutés et les scénarios de menace conduisent à des risques. Ceux-ci sont positionnés dans le tableau suivant qui permet de déterminer la classe d'un système industriel. Comme expliqué précédemment, le plus grave parmi les impacts humain, environnemental et d'arrêt du service rendu est retenu.

5+	Classe 2	Classe 2	Classe 3	Classe 3
4	Classe 2	Classe 2	Classe 2	Classe 3
3	Classe 1	Classe 2	Classe 2	Classe 2
2	Classe 1	Classe 1	Classe 2	Classe 2
1	Classe 1	Classe 1	Classe 1	Classe 1
Impact/Vraisemblance	1	2	3	4+

Annexe A

Cas d'étude simplifiés

Les exemples ci-dessous illustrent l'application de la démarche de classification des systèmes industriels pour différents secteurs d'activité. Les résultats donnés ici ne préjugent en rien de la classification de systèmes réels similaires.

A.1 Installation d'adduction d'eau

L'installation considérée est un système industriel de télégestion pour l'adduction d'eau d'une agglomération de 500 000 habitants.

Le système industriel est géographiquement réparti sur plusieurs sites (réservoirs, surpresseurs, pompes). Les sites distants communiquent avec le site central via des lignes RTC [1] ou des liaisons GPRS [2]. Le système industriel comporte de nombreux équipements de télégestion (RTU [3]) et des stations de supervision (SCADA). Les techniciens peuvent, depuis chez eux, se connecter au système en cas de problème. Le niveau de fonctionnalité est donc de 2 et le niveau de connectivité de 5. D'après la matrice proposée, le niveau d'exposition est 5.

Les intervenants sont peu nombreux. En théorie, seuls des intervenants autorisés peuvent accéder au système industriel. De plus, chaque site dispose d'un système de contrôle d'accès et de vidéoprotection. La catégorie des intervenants est donc 3.

En ce qui concerne les attaquants, il semble peu probable que des puissances étrangères ou des entreprises concurrentes veuillent porter atteinte au système car l'entreprise a essentiellement un rayonnement national. Le niveau de l'attaquant est donc fixé à 3.

Les impacts se limitent à l'interruption de la distribution d'eau pour plusieurs heures. D'après la matrice des arrêts de service cela correspond à un impact modéré. La gravité est donc 3.

1. Réseau téléphonique commuté.
2. General Packet Radio Service.
3. Remote Terminal Unit.

L'impact maximum est 3. En utilisant la formule fournie, on obtient une vraisemblance de 7. D'après la matrice de classification, le système industriel est en classe 2.

A.2 Industrie manufacturière

Le site considéré est une chaîne d'assemblage de produits électroménagers pour une entreprise de rayonnement essentiellement national.

Pour information, l'entreprise a déjà subi un incident de sécurité lorsqu'un employé de l'équipe de nuit a introduit une clé USB contenant un virus sur un poste de supervision. La chaîne de production a été arrêtée pendant trois jours.

Le système industriel est limité à un site unique. Il comporte un MES et des stations d'ingénierie connectées en permanence. Les techniciens et les opérateurs utilisent des tablettes et des douchettes sans fil pour scanner des codes barres. Le niveau de fonctionnalité est donc de 3 et le niveau de connectivité de 3. D'après la matrice proposée, le niveau d'exposition est 3.

Les intervenants sont nombreux mais, en théorie, seuls des intervenants autorisés peuvent accéder aux machines. La catégorie des intervenants est donc de 3.

En ce qui concerne les attaquants, il semble peu probable que des puissances étrangères ou des entreprises concurrentes veuillent porter atteinte au système car l'entreprise a essentiellement un rayonnement national. Le niveau de l'attaquant est donc fixé à 3.

Les impacts se limitent à des pertes de production, ce qui peut être gênant pour l'entreprise mais n'aura qu'un impact faible sur l'économie locale. Il est proposé de fixer l'impact à 1.

En utilisant la formule fournie, on obtient une vraisemblance de 5. D'après la matrice de classification, le système industriel est en classe 1.

A.3 Industrie de procédé continu

Le système industriel considéré est une installation de production de produits chimiques toxiques. Le site est classé SEVESO.

Les scénarios les plus graves sont :

— une introduction d'un programme malveillant dans le système industriel,

— une intrusion sur le système industriel.

Cette action malveillante peut être le fait d'une personne sur site ou à distance via le système d'information de gestion ou depuis un poste compromis sur le système industriel.

Le scénario aboutit soit à la perte d'un ou de plusieurs pupitres de conduite (écrans noirs ou figés, informations affichées erronées, etc.) soit à l'envoi de consignes destinées à provoquer un dysfonctionnement d'une unité.

Cet incident serait détecté

- soit par un opérateur de conduite,
- soit par la remontée d'alarmes (de seuil dépassé par exemple),
- soit par la mise en sécurité des unités concernées par le système instrumenté de sécurité, complètement isolé du système de conduite, à la suite de la détection de conditions de fonctionnement anormales ou d'une action manuelle d'un opérateur.

Il en résulterait un arrêt de production d'une partie des unités pendant une durée type d'un à trois jours le temps de diagnostiquer le problème, de restaurer les configurations. Le système pourra fonctionner temporairement en mode dégradé le temps de corriger complètement.

Il n'y a pas d'impact humain résultant de ce scénario. L'impact environnemental est estimé à 2. L'impact sur le service rendu peut aller de 1 à 3 en fonction du temps avant remise en service. L'impact retenu est donc 3.

Le système industriel comporte des historiques centralisés, des stations d'ingénierie ou de programmation connectées en permanence. Les réseaux industriels sont connectés au système d'information de gestion du site. Les réseaux sans fils ne sont pas encore déployés sur le périmètre industriel. Le niveau de fonctionnalité est donc estimé à 3 et celui de connectivité à 2. En utilisant la matrice proposée, l'exposition est donc de 3.

Étant sur un site SEVESO, les intervenants sont tous habilités et contrôlés et le niveau correspondant est 1.

Ce site industriel sensible est susceptible d'attirer l'attention d'«hacktivistes» et le niveau de l'attaquant est donc fixé à 4.

En utilisant la formule fournie, nous obtenons que le niveau de vraisemblance est 5. Combiné avec l'impact de gravité 3, il en résulte que le système industriel est de classe 2.

Remarque

Si les systèmes instrumentés de sécurité (des biens et des personnes) n'étaient pas isolés du système de pilotage de l'unité de production, il pourrait être envisagé qu'un virus ou la prise de contrôle du système industriel perturbe les fonctions de sécurité. De ce fait, les impacts ne seraient plus uniquement des arrêts de service rendu mais potentiellement des impacts humains majeurs (gravité 4).
D'après la matrice, le système industriel basculerait alors en classe 3.

A.4 Poste de manœuvre informatisé

Dans un réseau de transport ferré, un poste de manœuvre informatisé (MEI) permet de gérer les affectations de voies, de contrôler les aiguillages et les équipements de signalisation.

Le système est composé des éléments suivants :

— un module informatisé d'enclenchement (i.e. un automate) lié à des aiguillages sur les voies de chemin de fer (i.e. un actionneur). Le module contient les graphes de circulation paramétrables, préalablement formellement validés ;

— des postes de configuration (PC) situés sur un réseau privé, dédié au système de transport. Les équipements de ce réseau sont situés dans des emprises physiques privées, donc protégées contre les accès intempestifs. Les PC servent à des fonctions de diagnostic et au paramétrage des graphes de circulation ;

— un poste de maintenance hors réseau qui est connecté physiquement au module pour mettre en place un nouveau schéma lorsque nécessaire. Cette connexion est ponctuelle.

On identifie immédiatement deux événements redoutés :

— un accident si le MEI applique un schéma non valide et donne des ordres dangereux à un aiguillage ;

— la perte de l'exploitation de la ligne (ou tout au moins d'une portion) si le MEI cesse de fonctionner ou s'il envoie des paramétrages de circulation restrictifs.

Donc l'impact est de 5 puisqu'un dysfonctionnement dangereux du système peut provoquer un accident avec plusieurs morts.

Compte tenu des équipements, la fonctionnalité est de 2. Le réseau de télécommunication utilisé par le MEI est distribué mais privé. La connectivité est donc de 4. L'exposition est donc de 4.

Les intervenants sur le MEI sont des mainteneurs habilités et leurs interventions contrôlées conformément aux exigences de sûreté de fonctionnement. Par conséquent, l'intervenant est évalué à 1.

On retient la source de menace maximale car le système peut provoquer des accidents mortels et est donc susceptible d'attirer l'attention de personnes malveillantes, de plus le scénario consistant à provoquer le déraillement d'un train est régulièrement cité dans des scénarios de cyberattaque. L'adversaire est donc évalué à 5.

En conclusion, la vraisemblance est supérieure à 4 et le système est de classe 3.

Liste des acronymes

ANSSI Agence nationale de la sécurité des systèmes d'information. 5
APN Access Point Name. 35

CIM Computer Integrated Manufacturing. 29

EBIOS Expression des besoins et identification des objectifs de sécurité. 23, 28
ERP Enterprise Resource Planning. 30

FAT Factory Acceptance Test. 13

GPRS General Packet Radio Service. 43
GTB Gestion technique de bâtiment. 7

ICS Industrial Control System. 7

LPM Loi de programmation militaire. 5

MES Manufacturing Execution System. 29, 44
MPLS Multiprotocol Label Switching. 18, 35

PCA Plan de continuité d'activité. 14
PLC Programmable Logic Controller. 29
PRA Plan de reprise d'activité. 14
PSSI Politique de sécurité des systèmes d'information. 6, 12, 15

RTC Réseau téléphonique commuté. 43
RTU Remote Terminal Unit. 43

SAT Site Acceptance Test. 13
SCADA Supervisory Control And Data Acquisition. 20, 29, 30
SGDSN Secrétariat général de la Défense et de la Sécurité nationale. 14
SNCC Système numérique de contrôle commande (DCS). 31
SSI Sécurité des systèmes d'information. 5, 6

VPN Virtual Private Network. 35

Glossaire

Attaque Tentative d'atteinte à des systèmes d'information réalisée dans un but malveillant. Elle peut avoir pour objectif de voler des données (secrets militaires, diplomatiques ou industriels, données personnelles bancaires, etc.), de détruire, endommager ou altérer le fonctionnement normal de systèmes d'information (dont les systèmes industriels). 10, 14, 25, 27, 28, 30

Authenticité Propriété d'une information ou d'un traitement qui garantit son identité, son origine et éventuellement sa destination.
Traduction anglaise : authenticity. 18

Automate Automate programmable industriel.
Traduction anglaise : Programmable Logic Controller. 19, 20, 29, 30

Autorité de cyberdéfense Autorité nationale en charge de la défense des systèmes d'information, qui, dans le cadre des orientations fixées par le Premier ministre, décide des mesures que l'État met en œuvre pour répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des autorités publiques et des opérateurs d'importance vitale [1]. 6, 11, 16, 20

Besoin de sécurité Définition précise et non ambiguë du niveau d'exigences opérationnelles relatives à un bien essentiel pour un critère de sécurité donné (disponibilité, confidentialité, intégrité,...).
Exemples : doit être disponible dans la journée, doit être connu du groupe projet.
Traduction anglaise : sensitivity. 9

Bien Toute ressource qui a de la valeur pour l'organisme et qui est nécessaire à la réalisation de ses objectifs. [4] On distingue notamment les biens essentiels et les biens supports.
Traduction anglaise : asset. 28, 29

Bien essentiel Information ou processus jugé comme important pour l'organisme. On appréciera ses besoins de sécurité mais pas ses vulnérabilités.
Traduction anglaise : primary asset. 28

Bien support Bien sur lequel reposent des biens essentiels. On distingue notamment les systèmes informatiques, les organisations et les locaux. On appréciera ses vulnérabilités mais pas ses besoins de sécurité.
Exemples : société d'intégration, atelier de production, automaticien, réseau Ethernet, système d'exploitation.
Traduction anglaise : supporting asset. 29

Compromission Prise de connaissance, certaine ou probable, d'une information ou d'un support protégé par une ou plusieurs personnes non-autorisées [3].
Pour un système d'information, voir *Intrusion*. 12

Concentrateur Automate ou autre équipement informatique collectant des données d'équipements de terrain et les mettant à disposition d'un système tiers. 37

Confidentialité Caractère réservé d'une information ou d'un traitement dont l'accès est limité aux seules personnes admises à la (le) connaître pour les besoins du service, ou aux entités ou processus autorisés [3].
Traduction anglaise : confidentiality. 18, 25, 35

Console de programmation Poste contenant les outils permettant de programmer, de configurer et de réaliser des opérations d'administration sur un automate industriel. 30

Critère de sécurité Caractéristique d'un bien essentiel permettant d'apprécier ses différents besoins de sécurité.
Exemples : disponibilité, intégrité, confidentialité, traçabilité.
Traduction anglaise : security criterion. 25

Cyberdéfense Ensemble des mesures techniques et non techniques permettant à un État de défendre les systèmes d'information jugés essentiels. 6

Cybersécurité État recherché pour un système d'information lui permettant de résister à des événements d'origine malveillante susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services rendus par ce système. 7

Diode Équipement de cloisonnement visant à permettre la circulation des informations dans un seul sens. L'unidirectionnalité est assurée de manière physique. 17

Disponibilité Propriété permettant de rendre le service attendu en temps voulu et dans les conditions d'usage prévues.
Traduction anglaise : Availability. 25, 39, 40

Entité responsable Personne morale ou physique qui a la responsabilité légale de la mise en place des mesures appropriées de cybersécurité pour le système concerné. 7

Événement redouté Scénario générique représentant une situation crainte par l'organisme. Il s'exprime par la combinaison des sources de menaces susceptibles d'en être à l'origine, d'un bien essentiel, d'un critère de sécurité, du besoin de sécurité concerné et des impacts potentiels.
Exemple : une personne mal intentionnée (journaliste, concurrent) parvient à obtenir le budget prévisionnel de l'organisme, jugé confidentiel et publie l'information dans les médias.
Traduction anglaise : Feared event. 40

Faille Vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient. 13

Gestion technique de bâtiment Système industriel permettant la gestion de l'ensemble des installation techniques d'un bâtiment (électricité, climatisation, aération, ascenseurs, contrôle d'accès, vidéoprotection…).
Traduction anglaise : Building management system. 7

Gravité Quantification des conséquences d'un événement redouté ou d'un risque.
Exemples : Cf. 3.3.
Traduction anglaise : Consequences. 26

Historique Base de données contenant les historiques des alarmes et des valeurs du processus collectées par le logiciel de supervision (SCADA). Ces historiques sont souvent locaux ou centralisés.
traduction anglaise : Historian. 31

Historique centralisé Historique centralisant les informations de plusieurs consoles de supervision (SCADA). La durée de rétention des informations est souvent longue avec cependant une granularité moins fine que dans un historique local.
Cet historique peut être utilisé par des responsables pour de l'analyse de données, des statistiques, etc pour une unité de production complète. . . 31

Historique local Historique situé à proximité des équipements industriels dont il enregistre les données. La durée de rétention des informations est souvent limitée dans le temps avec cependant une granularité très fine.
Cet historique permet aux opérateurs de réaliser des analyses fines lors d'incidents de production. 31

Homologation de sécurité Déclaration par l'autorité d'homologation, au vu du dossier d'homologation, que le système d'information considéré est apte à remplir sa mission conformément aux objectifs de sécurité visés, et que les risques de sécurité résiduels sont acceptés et maîtrisés.
L'homologation de sécurité reste valide tant que le système d'information opère dans les conditions approuvées par l'autorité d'homologation. . . 20

Impact Conséquence directe ou indirecte de la non-réalisation des besoins de sécurité sur l'organisme et/ou sur son environnement.
Exemples : sur la mission, sur la sécurité des personnes, financiers, juridiques, sur l'image, sur l'environnement. 23, 25–27, 39–41

Imputabilité Capacité d'attribuer la responsabilité juridique d'une action à une personne physique ou morale. 25

Incident de sécurité Un ou plusieurs événements indésirables ou inattendus, liés à la sécurité de l'information, présentant une forte probabilité de compromettre les opérations liées à l'activité de l'organisation et de menacer la sécurité de l'information. [5] 10, 12, 14–16

Intervenant Toute personne étant amenée à intervenir sur un système d'information. Ceci comprend le personnel chargé de l'opération du système mais également les intégrateurs, les mainteneurs. 12, 13, 38, 39

Intervenant habilité Tout intervenant sur un système d'information ayant reçu une formation spécifique à son rôle sur l'installation concernée ainsi qu'une sensibilisation à la sécurité des systèmes d'information. La formation devra avoir été actée par l'entité responsable du système. 12, 13, 39

Intrusion Prise de contrôle, certaine ou probable, d'un système d'information ou de l'un de ses constituants par une ou plusieurs personnes non-autorisées. 19

Test d'intrusion Test de la sécurité d'un système d'information consistant généralement à simuler le comportement d'un utilisateur ou d'un logiciel malveillant.
Traduction anglaise : Penetration test. 13

Intégrité Propriété de protection de l'exactitude et de la complétude des actifs.
Traduction anglaise : Integrity. 18, 25, 35, 39, 40

Menace Cause potentielle d'un incident indésirable, qui peut nuire à un système ou à une organisation [5].
Exemples : vol de supports ou de documents, piégeage de logiciel, écoute passive…
Traduction anglaise : Threat. 5, 8, 13, 14, 24, 40

Mesure de sécurité Moyen de traiter un risque de sécurité de l'information. La nature et le niveau de détail de la description d'une mesure de sécurité peuvent être très variables.
Traduction anglaise : Control. 11

Pare-feu Équipement permettant d'appliquer la politique de cloisonnement entre plusieurs réseaux en filtrant les flux de données entre ceux-ci.
Traduction anglaise : Firewall. 16, 17

Pupitre Interface homme-machine permettant à un intervenant d'interagir et de contrôler le pilotage d'un système industriel.
Traduction anglaise : HMI. 30

Recette Plateforme Ensemble de tests permettant de vérifier la conformité d'un équipement et de sa configuration par rapport à l'usage qui en est attendu. Ces tests sont généralement effectués sur le lieu d'installation par l'intégrateur ou l'utilisateur final.
Traduction anglaise : Site Acceptance Test. 13

Recette Usine Ensemble de tests permettant de vérifier la conformité d'un équipement à ses spécifications. Ces tests sont généralement effectués en usine par le constructeur.
Traduction anglaise : Factory Acceptance Test. 13

Risque Scénario, avec un niveau donné, combinant un événement redouté et un ou plusieurs scénarios de menaces. Son niveau correspond à l'estimation de sa gravité et de sa vraisemblance. *Traduction anglaise* : Information security risk. 39

Sas Dispositif sécurisé permettant d'échanger des données avec des médias amovibles.
Un sas est généralement une station dédiée sur laquelle figurent des mécanismes de sécurité pour limiter une éventuelle propagation de virus, vérifier l'authenticité des données, etc. 20

Scénario de Menace Scénario, avec un niveau donné, décrivant des modes opératoires. Il combine les sources de menaces susceptibles d'en être à l'origine, un bien support, un critère de sécurité, des menaces et les vulnérabilités exploitables pour qu'elles se réalisent. Son niveau correspond à l'estimation de sa vraisemblance.
Exemples : vol de supports ou de documents du fait de la facilité de pénétrer dans les bureaux ; piégeage du logiciel du fait de la naïveté des utilisateurs. 14, 16, 40

Station Blanche Station permettant de vérifier, avant leur utilisation sur les installations, que les médias amovibles ne contiennent pas de virus. Parfois appelée station de dépollution. 20

Station d'ingénierie Équipement informatique disposant des progiciels de paramètrage, de conception, de programmation, d'administration des équipements industriels comme les automates et les SCADA. Cet équipement est connecté sur le réseau industriel et mis à disposition des équipes de maintenance, d'ingénierie, de support, etc. 30, 31

Surface d'attaque Ensemble des ressources vulnérables d'un système donné, exposées à des attaques par des sources de menace extérieures via les différentes interfaces entre ce système et son environnement. 29, 33–35

Système d'information Ensemble des moyens humains et matériels ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire l'information [3].
Traduction anglaise : Information system. 7

Système automatisé de contrôle des procédés industriels (Système industriel) Ensemble des moyens humains et matériels ayant pour finalité de contrôler ou de commander un ensemble de capteurs et d'actionneurs.
Traduction anglaise : Industrial Control System..... 7

Système d'information de Gestion Système d'information comprenant les services et applications destinés à la gestion (bureautique, ressources humaines, relation clients…)..... 7

Système d'information distribué Système d'information ou système industriel interconnectant plusieurs sites. Un système entre dans cette catégorie dès lors qu'il n'est pas possible de mettre en place une enceinte fermée avec contrôle d'accès autour de l'ensemble du système. Ceci s'applique en particulier aux câbles et fibres optiques du réseau sous-jacent. 33

Système de contrôle-commande Système assurant de manière automatique le pilotage et la protection d'un procédé industriel.
Les systèmes de contrôle commande sont fréquemment constitués de capteurs, d'actionneurs et d'automates programmables industriels.
7

Système de supervision industrielle Système permettant d'acquérir et de traiter un grand nombre de données (télémesures, télésignalisations et télé-alarmes) et de contrôler des équipements industriels (automates, capteurs, actionneurs…) en leur envoyant des télécommandes et téléréglages.
Traduction anglaise : Supervisory Control and Data Acquisition (SCADA). .. 29, 30

Sécurité des systèmes d'information Ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des évènements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. 5

Sûreté de fonctionnement Étude des défaillances et des pannes d'un système visant à s'assurer de l'aptitude de celui-ci à accomplir des fonctions, dans des conditions définies et durant un intervalle de temps donnés.
La sûreté de fonctionnement traite en particulier les propriétés de fiabilité, maintenabilité, disponibilite et sécurité (FMDS). La sécurité est entendu ici au sens des biens et des personnes.
L'Analyse des Modes de Défaillance, de leurs Effets et de leurs Criticité (AMDEC) est une méthode fréquemment employée en sûreté de fonctionnement
Traduction anglaise : Dependability. 7

Traçabilité Propriété permettant d'identifier l'origine et de reconstituer le parcours d'un bien essentiel depuis sa production jusqu'à son utilisation. ... 15, 25

Télédiagnostic Action d'effectuer à distance, sous-entendu depuis l'extérieur des systèmes d'information de l'entité responsable, un diagnostic d'installation technique. Ceci n'inclut pas de modification de paramétrage (lecture seule). 18

Télégestion Action de prendre le contrôle à distance, sous-entendu depuis l'extérieur des systèmes d'information de l'entité responsables, d'installations techniques géographiquement réparties (lecture/écriture). 18, 19

Télémaintenance Action d'effectuer à distance, sous-entendu depuis l'extérieur des systèmes d'information de l'entité responsable, des tâches de maintenance sur des installations techniques. Ceci implique notamment de pouvoir faire des modifications de paramètres ou de programmes (lecture/écriture). 18, 19

Vraisemblance Estimation de la possibilité qu'un scénario de menace ou un risque, se produise. Elle représente sa force d'occurrence. *Exemple :* Cf 3.3.
Traduction anglaise : Likelihood. 23, 25, 27, 28, 40

Vulnérabilité Caractéristique d'un bien support qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information.
Exemples : Crédulité du personnel, facilité de pénétrer sur un site, possibilité de créer ou modifier des commandes systèmes.
Traduction anglaise : Vulnerability. 12–16, 30, 35, 38

Bibliographie

[1] Décret n° 2011-170. février 2011.

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

[3] Secrétariat général de la défense nationale. Instruction générale interministérielle sur la protection du secret de la défense nationale. août 2003.

[4] ISO. ISO27001 : Information Security Management System (ISMS) standard. 2005.

[5] ISO. ISO27000 : Information security management systems — Overview and vocabulary. 2013.

[6] Agence nationale de la sécurité des systèmes d'information. Guide d'élaboration de politiques de sécurité des systèmes d'information. 2004.

[7] Agence nationale de la sécurité des systèmes d'information. EBIOS-2010 - Expression des besoins et identification des objets de sécurité. 2010.

[8] Agence nationale de la sécurité des systèmes d'information. Maîtriser la ssi pour les systèmes industriels. juin 2012.

[9] Agence nationale de la sécurité des systèmes d'information. Cybersécurité pour les systèmes industriels : Mesures détaillées. 2013.

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

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