RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LA CYBERSÉCURITÉ DES SYSTÈMES INDUSTRIELS - MÉTHODE DE CLASSIFICATION

GUIDE ANSSI

ANSSI-PA-107
10/03/2025

PUBLIC VISÉ :

Développeur | Administrateur | RSSI | DSI | Utilisateur

Informations

Attention

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

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

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
2.0	10/03/2025	Refonte du document

Table des matières

1
Introduction

1.1 Objectifs du guide

Les systèmes industriels s'appuyant sur la technologie opérationnelle (*Operational Technology*, OT), servent à conduire et surveiller des procédés qui ont une action physique directe et peuvent donc présenter des risques pour les personnes, les biens ou l'environnement.

Certains systèmes industriels utilisent les technologies de l'information (*Information Technology*, IT) mais n'ont pas été conçus pour faire face aux menaces qu'elles introduisent. De plus, les solutions de sécurisation utilisées dans le domaine de l'informatique de gestion ne sont pas toujours adaptées au fonctionnement des systèmes industriels.

En théorie, la sécurisation de l'OT doit se faire dès la phase de conception et nécessite parfois des solutions sur mesure. En pratique, les vulnérabilités propres aux composants d'un système industriel sont nombreuses (piles protocolaires sur les automates ou les serveurs par exemple). C'est pourquoi il est nécessaire d'intégrer ces éléments dans la réflexion générale sur la sécurité des systèmes d'information de l'entreprise.

Le présent guide a pour objectif de proposer une méthode de définition d'un socle de sécurité adapté aux systèmes industriels. Cette méthode s'appuie sur le découpage du périmètre industriel et sa classification en quatre niveaux. Pour chacun des niveaux appelés classes, le guide de mesures détaillées [6] propose un ensemble de mesures proportionnées au socle de sécurité.

Attention

Ce guide concerne exclusivement 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).

Information

Il s'agit d'une évolution des référentiels issus 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). Cette mise à jour tient compte du retour d'expérience du précédent guide, de la limitation imposée par la présence de trois classes de cybersécurité, et introduit les équivalences avec la norme IEC 62443 [9].

1.2 Organisation du guide

Chaque installation industrielle présente des particularités et des risques propres qu'il convient d'analyser pour déployer des solutions de sécurisation adaptées, en limitant les impacts sur l'activité de l'entreprise. Ce processus de sécurisation protège les investissements et la production de l'entreprise. C'est pourquoi il est important de définir les bons objectifs et de les adapter aux besoins, comme décrit au chapitre 5 du présent guide.

Les méthodes et recommandations de l'ANSSI sur la protection des systèmes industriels sont présentées dans deux documents. Le présent document contient les éléments structurant la méthodologie de classification. La démarche de sécurisation des systèmes industrielles est présentées au chapitre 3, les classes de cybersécurité sont présentées dans le chapitre 4 et l'évolution de la méthode de classification est présentée dans le chapitre 5. Une étude de cas proposant l'application des chapitres précédents est présentée au chapitre 6. Le guide des mesures détaillées [6] contient, quant à lui, l'ensemble des recommandations techniques et organisationnelles précises à appliquer en fonction des classes identifiées.

Les travaux présentés dans ce guide établissent des liens avec la norme ISA/IEC 62443 [9] utilisée dans le domaine des systèmes industriels.

1.3 Glossaire

AMDEC

Analyse des modes de défaillance, de leurs effets et de leur criticité. Il s'agit d'un outil de gestion de la qualité et de sûreté de fonctionnement.

API

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

Conduit

Groupement logique de voies de communication partageant des exigences de sécurité communes et connectant deux ou plusieurs zones (définition IEC 62443 [9]).

ERP

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

GMAO

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

IT

Information Technology. Ce sigle est utilisé dans le document pour désigner l'informatique dite « de gestion » pilotant les systèmes d'information d'entreprise. Dans le cas des systèmes industriels, l'IT est utilisée dans les niveaux 3.5, 4 et 5 du modèle de Purdue [1].

MES

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

OT

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

PLC

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

Poste de maintenance

Élément permettant d'interagir avec le système de conduite (SCADA) et l'ensemble des automates afin de réaliser des opérations de maintenance et éventuellement de modifier la configuration des automates.

SCADA

Supervisory Control And Data Acquisition. Ensemble de moyens informatiques permettant aux opérateurs et techniciens de la conduite de mettre en œuvre la supervision fonctionnelle et le contrôle, à distance ou local, des installations techniques d'un ou plusieurs sites.

Information

En dehors de l'Europe, le terme SCADA désigne un système étendu de pilotage d'une installation industrielle intégrant, entre autres, les automates, les capteurs et les actionneurs.

SIS

Safety Instrumented System ou « Système Instrumenté de Sécurité » en français. Il s'agit d'un composant automatisé assurant des fonctions de sécurité fonctionnelle pour la protection des biens et des personnes selon des critères de fiabilité, disponibilité, de maintenabilité et de sécurité (FDMS - il s'agit de la sécurité fonctionnelle introduite par la sûreté de fonctionnement, à ne pas confondre avec la sécurité informatique).

SL

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

SSI

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

Station d'ingénierie

Équipement permettant, entre autres fonctionnalités, la programmation du système de conduite (SCADA) et des automates programmables industriels (API).

SUC

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

Zone

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

2
Contexte et enjeux de la cybersécurité des systèmes industriels

Les systèmes industriels sont confrontés à un contexte de menaces en évolution permanente au gré des événements géopolitiques et de l'évolution de la cybercriminalité. La sécurisation de ces systèmes représente un enjeu important compte tenu du périmètre croissant et du risque inhérent aux procédés physiques qu'ils contrôlent. Il est important de disposer du contexte dans lequel évoluent les systèmes industriels pour comprendre les enjeux de leur sécurisation

Objectif

Présenter le panorama de la menace ciblant les systèmes industriels et leurs impacts potentiels.

2.1 Idées reçues et réalités des systèmes industriels

2.1.1 Réalités des SI de gestion et des systèmes industriels

Bien qu'utilisant de plus en plus des technologies standardisées issues de l'informatique d'entreprise ou de gestion, les systèmes industriels présentent des spécificités propres aux contextes dans lesquels ils sont utilisés. Ils se différencient des systèmes d'information d'entreprise par le fait qu'ils pilotent des installations physiques (unités et chaînes de production, unités de distribution d'eau, d'énergie, infrastructures routières, ferroviaires, etc.). Certains assurent en outre des fonctions de protection des biens et des personnes ou de l'environnement.

	SI de gestion	Systèmes industriels
Objectif des systèmes	Traiter des données	Piloter des installations physiques, réguler des procédés, acquérir et traiter des données
Aspects fonctionnels	Contraintes métier et contraintes de confidentialité et de protection de la vie privée, de charge du système	Contraintes métier et contraintes « temps réel », de sécurité fonctionnelle , de haute disponibilité 24/7
Profil des intervenants	Informaticiens	Automaticiens, instrumentistes électrotechniciens, spécialistes en génie du procédé
Environnement physique	Salle serveur climatisée, bureau voire domicile	Ateliers de production : poussière, température, vibrations, électromagnétisme, produits nocifs à proximité, environnement extérieur, etc.
Localisation géographique	Majoritairement dans des locaux fermés (bureau, domicile dans le cas du télétravail)	Dans des entrepôts, des usines, sur la voie publique, dans la campagne (stations de pompage, postes électriques, etc.), des lieux isolés, en mer, dans l'air et dans l'espace
Durée de vie	Environ 5 ans	Plus de 10 ans (parfois 30 ou 40 ans)
Gestion des incidents	Analyse post incident	La multitude de paramètres et la complexité de l'environnement rendent plus difficile la reproductibilité de l'incident
Composants	Des systèmes standards , des systèmes « durcis » face aux attaques informatiques	Des systèmes « temps réel » et robustes par rapport aux conditions difficiles des milieux industriels
Hétérogénéité des composants	La compatibilité des composants est une exigence technique (homogénéité et interopérabilité)	La grande durée de vie des installations conduit à une « superposition » des vagues technologiques successives sur un même site entraînant un phénomène d'obsolescence des matériels et logiciels

TABLE 1 – Dualité entre SI de gestion et systèmes industriels

2.1.2 Idées reçues concernant la cybersécurité des systèmes industriels

Il existe un certain nombre de Idées reçues relatifs aux systèmes industriels. Les plus communément admis sont examinés ci-après.

Idées reçues	Réalités
« Les réseaux industriels sont isolés, ils sont protégés. »	Les systèmes d'information industriels sont souvent connectés aux réseaux de gestion et parfois directement à Internet. Les clés USB et les consoles de maintenance sont par ailleurs des vecteurs majeurs de propagation de virus, y compris sur des systèmes isolés. Le besoin croissant de remontée de données vers le SI de gestion rend, à terme, l'isolation étanche des réseaux industriels utopique.
« Les protocoles et bases de données utilisés sont propriétaires, c'est un gage de protection. »	Les solutions propriétaires intéressent tout autant les attaquants que les standards ouverts, et elles ne sont pas par nature plus difficile à pirater. Elles peuvent comporter des vulnérabilités, voire n'avoir fait l'objet d'aucune analyse de sécurité. Par ailleurs, même les solutions propriétaires comportent des composants standards, pour des raisons d'interopérabilité (avec le système d'exploitation par exemple) et de moindre coût.
« L'intégration des mécanismes de sécurité (chiffrement, filtrage, authentification) est incompatible avec les contraintes de temps de réponse exigées. »	Les performances des composants ne sont plus un frein au déploiement de fonctions de sécurité. En revanche, des difficultés existent : systèmes « temps réel » ou la gestion de la durée des certificats (risque d'arrêt de la production en cas d'expiration).
« La SSI est incompatible avec la sûreté de fonctionnement (SdF). »	Au contraire la SSI et la SdF se rejoignent sur de nombreux points, voir le chapitre 3.
« Les mesures de SdF comme la redondance hétérogène protègent des attaques en disponibilité. »	Ce principe est de moins en moins employé car très coûteux. De plus, des produits de constructeurs différents s'appuient parfois sur les mêmes technologies et intègrent les mêmes composants matériels et logiciels. Ils contiennent dans ce cas des vulnérabilités identiques.
« La SSI coûte cher. »	La SSI doit être proportionnée aux enjeux. Elle coûtera d'autant moins cher qu'elle est prise en compte judicieusement dans les phases en amont des projets. Son coût reste généralement inférieur à l'ensemble des coûts liés à une cyberattaque comme par exemple la perte de chiffre d'affaires, le coût de la reconstruction du SI ou encore la perte de marchés.

Idées reçues	Réalités
« Une attaque du système industriel aura toujours moins d'impacts qu'un incident physique (vol de câbles, incendie, etc.) ou une attaque terroriste (explosion d'un réservoir de stockage de pétrole dans une raffinerie par exemple). »	Une cyberattaque peut causer des dommages directs sur des installations industrielles. Une attaque peut créer un dysfonctionnement global des installations plus difficile à identifier et plus pernicieux (sabotage industriel, ralentissement de la production) qu'une attaque physique pouvant entraîner un temps de rétablissement très long. Les dysfonctionnements provoqués peuvent devenir un facteur aggravant et provoquer une catastrophe industrielle, humaine ou écologique.
« La SSI empêchera de travailler efficacement. »	La SSI doit être centrée sur les enjeux critiques. Elle n'a pas pour objet de bloquer des comportements utiles, mais de prévenir les comportements dangereux (ce qui suppose de les identifier au préalable). La SSI impose parfois de formaliser des mesures de contournement des modes nominaux de fonctionnement (des modes dégradés d'opération).

TABLE 2 – Idées reçues relatifs aux systèmes industriels

2.2 Enjeux de la cybersécurité des systèmes industriels

2.2.1 Menaces et objectifs des attaquants

Les systèmes industriels sont de plus en plus la cible d'attaquants. Les problèmes de disponibilité (du simple ralentissement à l'interruption de service) peuvent avoir des conséquences lourdes tant humainement que financièrement. De plus, des attaques ciblées peuvent entraîner des accidents.

L'évolution des technologies, avec notamment l'avènement de l'industrie 4.0, amène les systèmes industriels intégrant des technologies opérationnelles à s'interconnecter avec des systèmes d'information d'entreprise, voire avec Internet. Cette interconnexion contribue à augmenter la surface d'attaque des systèmes de contrôle industriel, alors qu'ils étaient conçus pour fonctionner de manière isolée.

Les campagnes d'attaques à finalité d'espionnage sont une menace continue dans le temps. Plusieurs groupes d'attaquants, soutenus par des États, ont les capacités techniques de cibler les systèmes de contrôle industriel. Des campagnes visant à obtenir des données industrielles ou menant une reconnaissance sur des réseaux industriels (comme la taille du réseau, son organisation) ont été observées [13]. Le prépositionnement et la déstabilisation par sabotage informatique, affectant notamment des réseaux électriques et les unités de production, sont des menaces sérieuses qui s'inscrivent généralement dans le cadre de tensions internationales. Plusieurs États auraient déjà mis en pratique des actions de prépositionnement sur des réseaux électriques.

La transition vers l'industrie 4.0 présente plusieurs risques en cybersécurité :

- l'utilisation de protocoles non ou mal sécurisés offre à un attaquant la possibilité de modifier et injecter du trafic, ou de récupérer des identifiants de connexion circulant en clair sur le réseau ;
- l'augmentation du volume d'information transportable par les réseaux peut engendrer des difficultés à contrôler les valeurs acceptables et ainsi autoriser des attaques de type *buffer overflow* (débordement de tampon) ou déni de service distribué (DDoS) ;
- les technologies sans fil utilisées sans mesures de protection exposent davantage les systèmes industriels à des problèmes de disponibilité (brouillage de signaux) que les infrastructures filaires, et facilitent les compromissions (ex. : injection de trafic malveillant, modification de trames) ;
- les équipements et protocoles « historiques » qui étaient isolés physiquement (*air gap*) sont désormais accessibles par l'intermédiaire d'autres équipements connectés au réseau de l'entreprise (IT), directement ou via des passerelles de communication ;
- une plus importante automatisation d'actions en lien avec les procédés industriels peut d'une part amener des risques accrus en cas de mauvaise décision sans contrôle humain (cela peut intervenir avec un scénario dans lequel des données en provenance de l'extérieur du SI industriel sont directement injectées dans ce SI pour en piloter une partie du procédé), d'autre part entraîner sur le plus long terme une perte de maîtrise et de gouvernance de ce même procédé industriel par les équipes métier.

Les attaques informatiques majeures contre des systèmes industriels ont été exécutées en exploitant spécifiquement les protocoles ou solutions OT de l'entité victime, témoignant d'une phase de reconnaissance importante du système d'information de la cible choisie. Les attaques les plus visibles sur des systèmes industriels ont été motivées par une intention de sabotage. Mais les motivations d'espionnage et de vol de données sont de plus en plus fréquentes.

Les groupes cybercriminels et les rançongiciels constituent une menace additionnelle à l'encontre des systèmes industriels. Le besoin crucial de continuité d'activité des systèmes industriels est perçu par les attaquants comme un atout pour obtenir le paiement de la rançon. L'ANSSI a eu connaissance de plusieurs entités françaises ainsi ciblées ces dernières années [13].

Par ailleurs, la malveillance interne peut être considérée comme une menace limitée, mais pouvant avoir des effets importants sur le fonctionnement des systèmes industriels. Les capacités techniques des employés connaissant le fonctionnement des systèmes industriels dont ils sont chargés peuvent alors être exploitées à des fins malveillantes.

Afin de répondre au mieux à ces menaces, il est nécessaire pour les opérateurs de respecter des bonnes pratiques de sécurisation de leurs systèmes d'information d'entreprise et industriels pour assurer la pérennité de leur activité, mais aussi de renforcer leur mise en conformité avec les dispositions légales. Ainsi la protection et la sécurisation des systèmes industriels contre les cyberattaques doivent constituer une des priorités des acteurs économiques.

2.2.2 Négligences humaines

Les négligences ne sont pas le fruit d'actions malveillantes, mais leurs effets peuvent être similaires à ceux des attaques (par exemple le fait qu'un employé outrepasse volontairement des consignes de sécurité pour « se faciliter le travail »). Elles peuvent créer des vulnérabilités difficiles à détecter, qui pourront être exploitées par des attaquants ou simplement affecter la disponibilité des systèmes.

Par exemple, la modification involontaire de réglages d'asservissement ou la modification d'une alarme, peut avoir des conséquences désastreuses sur la qualité des produits et services délivrés, sur l'environnement, la santé ou la sécurité des personnes. Par exemple, l'utilisation d'une clé USB – qu'elle soit personnelle ou non – pour transférer des données entre des systèmes industriels isolés peut mener à une indisponibilité des systèmes si cette clé est porteuse d'un code malveillant.

Ces négligences peuvent avoir pour cause un manque de formation du personnel et d'information sur les enjeux de la SSI.

2.2.3 Vulnérabilités des systèmes d'information industriels

Les vulnérabilités peuvent être d'origines multiples et l'objet de ce guide n'est pas de les répertorier.
Les besoins croissants de consolidation des données de l'entreprise, de leur accès en temps réel depuis n'importe quel point de la planète, de réduction des coûts de développement et de possession, ainsi que les contraintes de délai ont précipité la convergence du domaine de l'informatique industrielle et de l'informatique d'entreprise.

Les outils de développement, de maintenance et télémaintenance sont aujourd'hui entièrement développés sur des briques génériques issues de l'informatique d'entreprise.
La standardisation des systèmes et les nouvelles fonctionnalités ont transmis aux systèmes industriels les vulnérabilités du monde de l'informatique d'entreprise. Les systèmes dits propriétaires, souvent pauvres en mécanismes de sécurité, ne sont pas à l'abri de vulnérabilités pouvant être exploitées par des attaquants motivés et organisés.
Alors que le monde de l'informatique d'entreprise parvient à corriger régulièrement les vulnérabilités, notamment par l'application de correctifs publiés par les constructeurs et les éditeurs de logiciels, le monde industriel, de par ses contraintes de sécurité fonctionnelle, ne peut pas adopter les mêmes protections dans les mêmes conditions (réactivité, procédure de qualification, processus de retour arrière, etc.). Cette différence de réactivité face aux vulnérabilités publiques est un des principaux risques des systèmes d'information industriels.
Le manque de formation des intervenants, les différences de cultures ou le manque de prise de conscience des risques liés à la SSI constituent d'autres sources majeures de vulnérabilités.

Information

Il est à noter que les systèmes industriels devant répondre à un niveau de sécurité fonctionnel élevé (par exemple de niveau SIL4 selon la norme IEC 61508 [10]) suivent des processus de développement et de validation (selon la norme IEC 24772 [11]) qui permettent de réduire l'impact de certaines attaques informatiques.

2.2.4 Impacts potentiels sur les systèmes industriels

De nombreux incidents sur les systèmes industriels surviennent chaque année. La plupart sont peu médiatisés, seuls certains font l'objet d'une attention plus importante. Ce fut par exemple le cas pour les incidents ciblant les centrales nucléaires au Royaume-Uni (lié au ver Conficker) et aux USA (lié au ver Slammer), pour la propagation généralisée du ver Stuxnet [1] en 2010, ou encore

pour le *malware* Triton qui ciblait les équipements SIS de la marque *Schneider Electric* en 2017. Leurs impacts peuvent être analysés selon différents axes, présentés dans le tableau 3.

Dommages matériels / corporels	La modification des configurations nominales des installations peut provoquer des dégradations physiques avec le plus souvent des conséquences matérielles – mais parfois aussi humaines.
Perte de chiffre d'affaires	L'interruption de la production génère des manques à gagner importants. La modification de paramètres de fabrication conduisant à des produits non conformes peut générer des pertes importantes.
Impact sur l'environnement	La défaillance du système suite à une prise de contrôle malveillante peut générer un dysfonctionnement des installations (ouverture de vannes de produits polluants) et provoquer une pollution du site et de son environnement.
Vol de données	Perte de secret de fabrication, contrefaçons, avantage pour la concurrence, menace hacktiviste avec l'atteinte à la réputation par divulgation d'informations sensibles.
Responsabilité civile / pénale - Image et notoriété	L'indisponibilité du service, comme la rupture de distribution d'électricité ou d'eau ainsi que la fourniture de produits défectueux mettant en danger le consommateur, peut aboutir à des poursuites pour les dommages occasionnés, ou simplement dégrader l'image de l'entreprise (la satisfaction du client et sa confiance).

TABLE 3 – Impacts potentiels concernant les systèmes industriels

1. Stuxnet est un code malveillant visant les systèmes industriels. Il exploite de multiples vulnérabilités présentes dans le système d'exploitation *Microsoft Windows* et le progiciel de SCADA *WinCC* de SIEMENS. Le code malveillant modifie le programme exécuté par certains automates industriels de la gamme *Simatic S7* de SIEMENS. Les modifications réalisées peuvent conduire au ralentissement de la production, mais aussi à la destruction physique des installations pilotées par l'automate.

3
Démarche SSI appliquée aux systèmes industriels

La démarche SSI doit être adaptée au contexte dans lequel elle s'inscrit. Dans le cas des systèmes industriels, celle-ci doit s'adapter aux spécificités sectorielles afin d'assurer une prise en compte de la SSI sans entraver la sûreté de fonctionnement.

Objectif

Présenter une démarche SSI adaptée au contexte des systèmes industriels.

3.1 Méthode de déploiement de la SSI

Parfois perçue uniquement comme une contrainte, la SSI contribue au contraire à améliorer la robustesse des installations et la productivité des entreprises. Le déploiement de la SSI dans les systèmes industriels consiste à étudier les menaces (aspects organisationnels, matériels et logiciels) et à mettre en place des mécanismes et des procédures (aspects humains) dans le cadre de politiques de sécurité permettant d'assurer la continuité des fonctions métiers à un niveau acceptable.

Le déploiement de la SSI peut être organisé autour des thématiques suivantes :

- **Sensibilisation** : Une part importante des incidents est liée à une méconnaissance des risques sur l'installation. La sensibilisation aux règles d'« hygiène informatique » [2] contribue fortement à réduire les vulnérabilités et les opportunités d'attaques. Cette sensibilisation doit être régulière car les risques et les intervenants évoluent en permanence.
- **Cartographie** : Un inventaire, extrait de la cartographie, précisera les installations matérielles, les systèmes et les applications critiques. C'est un pré-requis incontournable à la mise en place de la sécurité des SI dans les installations industrielles. Cet inventaire, première étape de l'analyse de risques, permettra de définir les différents niveaux de criticité, de sécurité fonctionnelle, de disponibilité ou d'intégrité attendus pour les éléments cartographiés.

Information

Un guide d'élaboration d'une cartographie en 5 étapes est disponible sur le site de l'ANSSI [3].

- **Analyse de risque** : Tout projet doit comprendre une analyse de risque afin d'identifier les éléments critiques du système, les évènements redoutés et les objectifs de sécurité face aux menaces retenues. Ces objectifs sont alors déclinés en exigences de sécurité, qui porteront sur le système lui-même (robustesse intrinsèque), sur son environnement de conception, de construction et d'exploitation. Ces exigences sont ensuite traduites en mesures techniques, physiques, et organisationnelles.

Information

Un guide d'élaboration d'une analyse de risque en 5 ateliers (méthode EBIOS **Risk Manager**) est disponible sur le site de l'ANSSI [5].

- **Défense en profondeur** : La défense en profondeur consiste à protéger les installations en les entourant de plusieurs barrières de protection, indépendantes les unes des autres, de façon à ce que la défaillance de l'une d'entre elles puisse être compensée par une autre. Elles peuvent être technologiques ou liées à des procédures organisationnelles. Adopter une démarche de défense en profondeur permet de se protéger contre des menaces qui ne sont pas encore connues, de diminuer le périmètre dans lequel une menace est exercée ou d'en atténuer l'impact. La stratégie de défense en profondeur doit intégrer non seulement une démarche de mesures préventives, mais aussi des mesures de surveillance, de détection et de réaction.
- **Détection d'incidents** : Dans un environnement industriel, il peut être complexe, voire impossible, de déployer certaines barrières de protection sans impacter l'activité de l'entreprise. Les contre-mesures devraient inclure des mécanismes de surveillance des installations et de détection des incidents. La collecte des informations au moyen des journaux d'alarmes et d'événements est indispensable à la détection des attaques mais aussi aux analyses ultérieures en cas d'incident. Bien configurés, ces journaux peuvent apporter des éléments utiles, voire des preuves dans le cadre d'une enquête judiciaire.

Attention

Ces mesures n'empêcheront pas un incident mais permettront de le détecter, d'en limiter autant que possible les effets et d'aider à l'identification d'une menace.

Information

Pour plus d'information, il est recommandé de se référer à la doctrine de détection des systèmes industriels [4].

- **Traitement des incidents, chaîne d'alerte** : Un dispositif de détection n'a de sens qu'associé à la mise en place d'une organisation et de procédures pour traiter les incidents. Il convient de déterminer les bonnes actions à mener lors de la détection d'un incident de sécurité. Un processus d'escalade doit être défini pour gérer les incidents au bon niveau de responsabilité et décider en conséquence s'il faut déclencher un plan de réponse à incident (PRI), un plan de continuité d'activité (PCA) puis un plan de reprise d'activité (PRA), et si une action judiciaire est nécessaire. La gestion des incidents doit également intégrer une phase d'analyse post incident qui permettra d'améliorer l'efficacité des mesures de SSI déployées initialement.

Information

L'ANSSI a publié trois guides pour aider les entreprises à mettre en œuvre et piloter la remédiation [12].

- **Plan de continuité (PCA) et de reprise d'activité (PRA)** : Se préparer à faire face aux événements redoutés permet de minimiser leurs impacts et le temps de redémarrage de l'activité. Les PCA et PRA de l'entreprise doivent impérativement intégrer les systèmes industriels en identifiant les moyens et les procédures nécessaires pour un maintien et une reprise d'activité nominale en cas d'incident.

Information

Les PCA et PRA doivent être adaptés aux contraintes imposées par les systèmes industriels. Ils doivent être mis à jour et testés lors des périodes de maintenance opérationnelle afin de ne pas risquer une perturbation du système en production.

- **Veille sur les menaces et les vulnérabilités** : Se tenir informé de l'évolution des menaces et des vulnérabilités ainsi que de leurs effets potentiels constitue une mesure fondamentale de défense. Les mises à jour des micrologiciels des équipements industriels, les correctifs des systèmes d'exploitation et des applications font l'objet d'alertes et d'avis de sécurité disponibles sur le site du CERT-FR [2]. Les vulnérabilités propres aux systèmes industriels sont actuellement classées dans la catégorie SCADA.

Information

Les fournisseurs d'équipements industriels publient régulièrement, via leurs propres canaux de communication, des bulletins de sécurité donnant des informations spécifiques sur la mise en place des correctifs propres à leurs équipements.

3.2 Une approche globale IT/OT

La SSI ne peut pas se traiter correctement dans l'urgence, de façon ponctuelle ou isolée. Il s'agit d'une démarche qui se planifie et qui demande la participation de ressources et compétences multiples, ainsi qu'un engagement fort au plus haut niveau de la hiérarchie.

3.2.1 Une volonté à tous les niveaux

Dans les systèmes industriels, les mondes IT et OT cohabitent avec chacun leurs spécificités et leurs contraintes. Néanmoins, la démarche SSI doit être globale. Elle peut s'appuyer sur les standards de la sécurité des systèmes d'information existants, en prenant en compte les contraintes spécifiques aux systèmes industriels. Les systèmes d'information industriels doivent être intégrés dans

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

les politiques de sécurité de l'entreprise, comme tout système d'information, et ceci dès la genèse du projet.

Attention

Bien que de nombreuses problématiques de sécurité soient communes entre IT et OT, la mise en œuvre des solutions dans l'OT demande à ce qu'elles soient ajustées au contexte industriel et à ses contraintes.

Le projet de déploiement de la sécurité sur les systèmes industriels ne peut pas réussir sans l'implication de la direction au plus haut niveau de l'entreprise.

3.2.2 Prise en compte de la SSI dans les projets

La sécurité du système doit être envisagée dès le début du projet par le propriétaire de l'installation (ou l'exploitant s'il s'agit par exemple d'une délégation de service public) qui doit exprimer ses besoins en matière de cybersécurité. Pour les différentes phases d'un projet, plusieurs recommandations sont formulées dans le guide de l'ANSSI relatif aux mesures détaillées pour la cybersécurité des systèmes industriels [6].

Information

Plus la cybersécurité est prise en amont du projet et intégrée comme une composante initiale du besoin métier et moins elle coûte au projet.

4
Classes de SI industriels

Tous les systèmes industriels n'ont pas la même criticité. Si certains assurent des fonctions dont la moindre défaillance peut entraîner des conséquences sur des vies humaines, d'autres, sur le même site, pourront tout au plus nuire au confort des intervenants. Il convient donc d'adapter les efforts consentis à leur sécurisation en fonction des impacts potentiels d'une attaque. Pour cela, il est proposé de définir des classes de cybersécurité, en fonction de la criticité des systèmes, auxquelles seront associées des recommandations.

Objectif

Définir quatre classes de cybersécurité pour les systèmes industriels, puis la méthode permettant de déterminer la classe d'un système industriel en fonction de son impact potentiel maximal.

4.1 Classes de cybersécurité des systèmes industriels

Il est proposé de répertorier les systèmes industriels en quatre classes exprimant leurs besoins de sécurité. Ce besoin est directement lié aux impacts maximaux qu'un dysfonctionnement majeur pourrait entraîner.

Classe de cybersécurité

Une classe de cybersécurité est définie en fonction de la gravité des conséquences pour la Nation selon les impacts sur la population, l'économie et l'environnement. L'impact maximal envisagé est la somme des conséquences théoriques les plus pessimistes pouvant résulter d'un acte de malveillance informatique. Il correspond aux événements redoutés des référentiels de sûreté (sécurité fonctionnelle) du domaine industriel, limités à ceux qui sont la conséquence directe ou indirecte d'une attaque informatique. Ainsi les enceintes de confinement et les automates de sûreté purement électromécaniques, par exemple, permettent de diminuer l'impact à considérer pour les cyberattaques. La classe est déterminée avant la mise en place de contre-mesures, ou de palliatifs permettant de limiter les conséquences.

4.1.1 Présentation de la classification

La méthode de classification reprend des termes et concepts que l'on retrouve dans les premières étapes des méthodes d'analyse de risque. Par exemple, dans la méthode EBIOS RM [5], l'atelier 1

« Cadrage et socle de sécurité » demande d'identifier les événements redoutés et la gravité de leurs impacts. Dans la suite du chapitre, des tableaux permettant d'estimer les impacts sont présentés. C'est en fonction de ces impacts que la classification industrielle est déterminée.

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 4.2.1. Il appartient à chaque entité responsable de définir le périmètre précis du système industriel concerné.

La version 1.0 de ce guide proposait trois classes, déterminées en fonction d'un impact et d'une vraisemblance. La vraisemblance est une probabilité subjective d'occurrence qui est déterminée à partir de formules empiriques faisant intervenir la menace (interne et externe) et l'exposition du système industriel. Toutefois, avec cette précédente méthode, il résultait trop souvent une définition des systèmes en classe 3.
L'une des raisons est qu'il y avait un phénomène de bouclage par la vraisemblance : au fur et à mesure que l'architecture du système industriel intégrait des mesures de sécurisation informatique, la vraisemblance d'une attaque diminuait, abaissant (par rebond) la classification du système. Pour éviter ce rebouclage, il était usuel de maintenir la vraisemblance à un niveau constant (alors que ce dernier évolue en fonction du contexte). Or, il est préférable que la classe d'un système industriel, dont les fonctions n'évoluent pas, reste stable afin que le référentiel de mesures de sécurité à lui appliquer soit clairement déterminé. D'autre part, la vraisemblance est trop fluctuante dans le temps alors que la classification proposée ici vise à déterminer des mécanismes de sécurité sur le long terme.

Il n'y a pas d'équivalence directe entre les 4 classes du présent guide et les niveaux de sécurité (*SL*) de la norme IEC 62443 [9]. En effet, cette dernière positionne les niveaux de sécurité en fonction du niveau de menace (opportuniste, criminelle ou étatique), tandis que les classes de cybersécurité correspondent à la criticité des impacts. Toutefois, les impacts dus à des attaques cyber sont envisagés comme des menaces latentes, et les mesures détaillées pour chaque classe font le lien avec les exigences de la norme IEC 62443. Le mesures des classes 1 ou 2 mettent l'accent sur la résilience, c'est-à-dire la capacité à surmonter une panne ou une cyberattaque, à restaurer et à redémarrer l'installation ; tandis que celles des classes 3 ou 4 mettent l'accent sur la nécessité de survivre à une attaque pour les systèmes les plus critiques.

Information

La politique de sécurité appliquée sur un site industriel se fonde sur une analyse de risques mise à jour régulièrement pour tenir compte de l'état de la menace. En effet, le risque d'occurrence d'un événement redouté (R) dépend de la gravité de son impact (G) et de sa vraisemblance (V) : $R = I \times V$. La vraisemblance est mise à jour par l'analyse de risque du moment, en fonction de la menace (contextes politique et géopolitique, perception de la menace cyber) et de l'exposition (surface d'attaque, vulnérabilités non corrigées, etc.).
Ainsi, dans la perspective de la politique de sécurité, la vraisemblance, non prise en compte dans la présente classification, reste un critère déterminant de l'analyse de risque, en particulier si cette dernière contient des scénarios d'attaque.

Attention

Une politique de sécurité adaptée doit permettre de passer rapidement (en quelques heures) d'une situation nominale à une situation d'alerte avec vérifications renforcées, lorsque l'état de la menace et le degré d'exposition du SI industriel l'exigent.

4.1.2 Definition des classes de cybersécurité

Définies par l'ANSSI, les quatre classes de cybersécurité des systèmes opérationnels de conduite et d'exploitation de procédés industriels sont les suivantes :

Classe 1 : Il s'agit des systèmes industriels pour lesquels l'impact d'une attaque est faible.

Classe 2 : Il s'agit des systèmes industriels pour lesquels l'impact d'une attaque est modéré. Il n'y a pas de contrôle étatique pour ces systèmes, 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 l'impact d'une attaque est fort. Dans cette classe, les mesures de sécurité détaillées sont renforcées et il est recommandé de faire vérifier la conformité de ces systèmes industriels par un organisme qualifié.

Classe 4 : Il s'agit des systèmes industriels pour lesquels l'impact d'une attaque est catastrophique. Dans cette classe, les mesures de sécurité détaillées sont les plus fortes et il est recommandé de faire vérifier la conformité de ces systèmes industriels par un organisme qualifié.

Chaque nouvelle classe renforce les mesures de la ou des classes inférieures, sauf exceptions.

Attention

Toutes les modifications fonctionnelles ou techniques apportées à un système industriel, hors des mesures spécifiquement liées à la sécurisation elle-même, nécessitent une revue de l'estimation de la classe de cybersécurité.

4.2 Détermination de la classe

4.2.1 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. Le périmètre doit être choisi de manière cohérente en fonction du risque et de l'architecture des systèmes analysés.

Attention

S'il est décidé de découper une infrastructure en plusieurs systèmes industriels, une analyse de risque globale doit 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. Toutefois, il conviendra de les mettre à jour en tenant compte en particulier des modes communs propres aux cyberattaques. En effet, du fait de sa nature non physique, une cyberattaque sur un équipement peut facilement être répliquée à l'ensemble des équipements qui possèdent la même vulnérabilité, par exemple parce qu'ils partagent un même composant logiciel. Ainsi, deux systèmes en redondance physique doivent être considérés comme attaqués en même temps, au contraire d'une redondance fonctionnelle.

La méthode est appliquée de manière séquentielle :

- 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 l'architecture fonctionnelle établie, la méthode est appliquée sur des sous-ensembles plus restreints. Ces sous-ensembles sont parfois appelés «zones» dans la littérature et en particulier dans la norme IEC 62443 [9].

Compte tenu de l'impact potentiel de certaines mesures, il est important de déterminer de manière précise le périmètre étudié. Une mauvaise définition du périmètre pourrait conduire, par exemple, à imposer des mesures de classe 3 à des systèmes industriels de classe 2.

Information

Par exemple, un site de type SEVESO seuil haut sera globalement de classe 3 (voire 4). 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. Certains systèmes de production pourront être seulement de classe 2.

4.2.2 Evaluation de la criticité

Dans l'évaluation de la criticité d'un système industriel, seuls deux critères de sécurité sont principalement retenus - à savoir la disponibilité et l'intégrité - qui ont un lien fort avec la sûreté de fonctionnement. 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 ce guide.

La classe du système industriel est déterminée par le plus grand impact du pire événement redouté. La gravité d'un impact s'évalue sur une échelle d'impact (ei) à 4 niveaux : mineur, modéré, majeur et catastrophique. Plusieurs échelles sont nécessaires pour mesurer la gravité de l'impact d'un événement redouté (er). Les impacts considérés sont les suivants : humains, environnementaux,

macroéconomiques et éventuellement économiques. Les niveaux sont donnés par les tableaux 4, 5, 6 et 7.

Information

La décision d'avoir un nombre pair de niveaux de gravité oblige à prendre position et évite le piège de la « zone refuge » d'indécision, au milieu.

Le choix de la classe, qui peut se comprendre intuitivement par le niveau d'impact maximal des événements redoutés, s'écrit de façon formelle :

$$\text{Classe} = \max_{\forall ei, \forall er} \text{Niveau}_{ei}(er)$$

Où ei est une échelle de niveau d'impact parmi l'ensemble des échelles d'impact proposées, et er un événement redouté, parmi l'ensemble des événements considérés dans l'étude de risques. Le $\text{Niveau}_{ei}(er)$ est déterminé au moyen de la table d'échelle d'impact ei, en se basant sur une évaluation de l'impact de l'événement er.

Dans certains secteurs industriels, les analyses de sécurité ou de sûreté de fonctionnement permettent de démontrer l'indépendance des événements redoutés. Ainsi, l'attaque physique d'une installation industrielle peut être considérée indépendante des attaques d'autres installations de même type à partir d'une distance déterminée. Ces hypothèses ne tiennent plus en cas d'attaque informatique d'installations en réseau ayant des interfaces identiques : l'attaque de l'une d'entre elles est généralisée à l'attaque de toutes les installations en même temps par le même scénario opérationnel. Ce cas est illustré par l'étude de cas à la section 6.4.

Attention

Les impacts doivent tenir compte des modes communs propres aux attaques informatiques : dans le cas de systèmes industriels distribués avec des interfaces standardisées, l'impact d'une attaque depuis un réseau informatique est celui résultant de l'attaque de tous les systèmes équivalents, vulnérables de la même façon. **Cela conduit à nettement renforcer la classe des petites installations largement réparties sur le territoire.** Ce point est illustré à la section 6.4.

4.3 Échelles de gravité

Les tableaux ci-dessous présentent les échelles de gravité des impacts humains, environnementaux et d'indisponibilité pour la collectivité.

Information

Selon le secteur d'activité, il est possible d'ajouter une échelle supplémentaire pour les impacts sur le chiffre d'affaire de l'entreprise.

L'échelle d'impact économique est laissée à la discrétion du propriétaire ou de l'exploitant de l'installation. Elle pourra refléter le contexte économique de l'installation industrielle. Les conséquences doivent être décrites avec des valeurs chiffrées (en euros, en dollars, en % du chiffre d'affaire, etc.) et prendre en compte notamment :

- les pertes matérielles, le remplacement, la réparation ou la destruction d'équipements ;
- le manque à gagner ;
- les sanctions économiques.

Les impacts dépendent très largement du secteur concerné. Ainsi, les échelles doivent être adaptées et précisées pour chaque secteur d'activité. Pour les secteurs d'importance vitale, l'article L1332-3 du code de la défense (voir le document [7]) définit des critères complémentaires. Un secteur jugé stratégique pourra avoir une échelle d'impact économique renforcée. Par ailleurs, l'article L511-1 du code de l'environnement (voir le document [8]) précise également des impacts. Enfin, si une analyse de type AMDEC a été réalisée, il est recommandé d'utiliser les échelles de gravité qui y ont été définies.

Attention

L'adaptation des échelles de gravité des impacts au secteur concerné ne doit pas dégrader significativement les niveaux esquissés ici. En effet, cela conduirait à sous-estimer la classe, et donc les mesures de sécurité à mettre en œuvre.

Gravité	Qualificatif	Conséquences humaines
1	Mineur	Accident déclaré avec arrêt ou traitement médical.
2	Modéré	Invalidité permanente.
3	Majeur	Un décès.
4	Catastrophique	Plusieurs décès.

TABLE 4 – Gravité des impacts humains

Gravité	Qualificatif	Conséquences sur l'environnement
1	Mineur	Dépassement d'une norme de rejet exigeant déclaration aux autorités mais sans conséquence pour l'environnement.
2	Modéré	Pollution modérée limitée au site.
3	Majeur	Pollution significative ou externe au site. Évacuation de personnes.
4	Catastrophique	Pollution majeure avec conséquences environnementales durables externes au site.

TABLE 5 – Gravité des impacts environnementaux

Gravité	Qualificatif	Conséquences macroéconomiques
1	Mineur	Impacts lourds sur 10 000 personnes. Perturbation de l'économie locale.
2	Modéré	Impacts lourds sur 100 000 personnes. Perturbation de l'économie régionale. Perte temporaire d'infrastructure majeure.
3	Majeur	Impacts lourds sur 1 000 000 personnes. Perturbation de l'économie nationale. Perte temporaire d'une infrastructure critique. Perte définitive d'une infrastructure majeure.
4	Catastrophique	Impacts lourds sur 10 000 000 personnes. Perte définitive d'une infrastructure critique.

TABLE 6 – Gravité des impacts macroéconomiques consécutifs à l'indisponibilité du service rendu

Gravité	Qualificatif	Conséquences économiques
1	Mineur	Impact inférieur à ***XX XXX*** euros.
2	Modéré	Impacts économiques d'au moins ***XXX XXX*** euros.
3	Majeur	Impacts économiques d'au moins ***X XXX XXX*** euros.
4	Catastrophique	Impacts économiques d'au moins ***XX XXX XXX*** euros ou entraînant la cessation d'activité.

TABLE 7 – Gravité des impacts économiques pour le propriétaire de l'installation industrielle

5
Méthode de classification

La présente méthode de classification nécessite d'intégrer divers éléments. Afin de faciliter sa mise en œuvre, le cheminement et les procédures associées sont décrits ci-après.

Objectif

Le présent chapitre a pour objectif de présenter la méthode de classification d'un système d'information industriel permettant de déterminer une classe de cybersécurité afin de définir un socle de mesures de sécurité. Cette méthode s'appuie sur une étude qui doit être réalisée préalablement pour identifier, entre autres, les évènements redoutés.

La présente méthode de classification est harmonisée avec la méthode EBIOS RM pour permettre la maîtrise des risques sur l'ensemble du système industriel. La méthode de classification étant autonome, d'autres méthodes permettant d'identifier des évènements redoutés peuvent être utilisées.

Pour rappel, les ateliers EBIOS RM sont :

1. **Atelier 1** - Cadrage et socle de sécurité
   - Étapes
     a. définir le cadre de l'étude ;
     b. définir le périmètre métier et technique de l'objet étudié et les biens supports ;
     c. identifier les événements redoutés et estimer leur niveau de gravité ;
     e. déterminer le socle de sécurité et en évaluer la conformité.
   - Sorties
     a. les éléments de cadrage : objectifs de l'étude, rôles et responsabilités, cadre temporel ;
     b. le périmètre métier et technique : missions, valeurs métier, biens supports ;
     c. les événements redoutés et leur niveau de gravité ;
     d. le socle de sécurité : liste des référentiels applicables, état d'application, identification et justification des écarts.
2. **Atelier 2** - Source de risques (SR) / objectifs visés (OV)
3. **Atelier 3** - Scénarios stratégiques
4. **Atelier 4** - Scénarios opérationnels

5. **Atelier 5** - Traitement du risque

Information

Les activités de la méthode de classification s'insèrent dans l'atelier 1 de la méthode EBIOS RM.

« tel que défini dans »

Ce terme signifie que l'activité EBIOS RM référencée peut être réalisée sans modification dans le cadre de la méthode de classification.

« en s'appuyant sur »

Ce terme signifie que des instructions complémentaires doivent être prises en compte lors de la réalisation de l'activité EBIOS RM dans le cadre de la méthode de classification.

Les activités à réaliser pour la méthode de classification sont :

1. **Activité 1.** Définir le cadre de l'étude en s'appuyant sur EBIOS RM - Atelier 1.a et Atelier 1.b (section 5.1) ;
2. **Activité 2.** Établir des zones au sein du périmètre (section 5.3) ;
3. **Activité 3.** Identifier les événements redoutés (section 4.3), en s'appuyant sur EBIOS RM - Atelier 1.c et en déduire les classes.

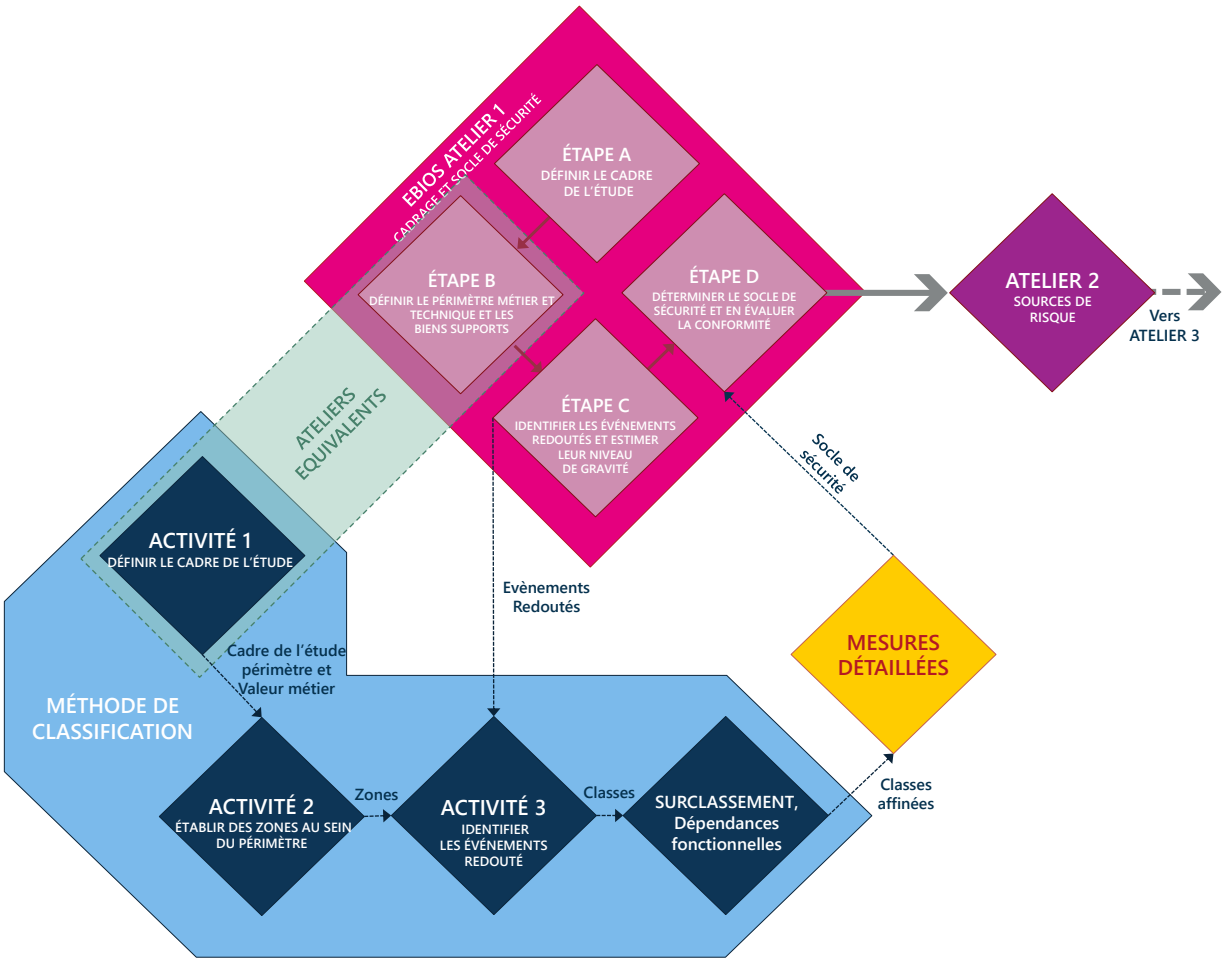

FIGURE 1 – Méthode de classification associée à la démarche EBIOS RM

5.1 Activité 1 - Définir le cadre de l'étude

5.1.1 Objectif

L'objectif de cette activité est d'identifier le périmètre du SI d'une installation industrielle et son découpage en zones pour lesquelles la gravité des impacts sera évaluée dans l'activité suivante de la méthode.

Information

À titre d'exemple, la norme IEC 62443 [9] propose la définition d'un périmètre appelé *System Under Consideration* (SUC) qui est décrit dans le fascicule 3-2 du référentiel normatif. Un SUC se compose d'une ou plusieurs zones et des conduits correspondants (voir la définition des zones et des conduits selon la norme IEC 62443 dans le glossaire du présent guide à la section 1.3).

5.1.2 Renvoi à EBIOS RM

Cette activité s'appuie sur EBIOS RM - Atelier 1.a et Atelier 1.b. Dans un premier temps, dérouler les activités telles que proposées dans EBIOS RM. Les indications supplémentaires, spécifiques aux systèmes industriels sont précisées dans la section 5.1.4.

5.1.3 Données de sorties

Les données élaborées à l'issue de cette activité sont les suivantes :

- le cadre de l'étude ;
- le périmètre de l'étude ;
- les missions et les valeurs métiers.

5.1.4 Procédure

5.1.4.1 Définissez les objectifs et hypothèses

- Présentez l'objectif principal de l'étude, à savoir établir le socle de sécurité pour le système industriel, ainsi que les objectifs secondaires. Les objectifs secondaires peuvent inclure par exemple la mise en place d'un processus de management du risque cyber dans l'organisme, la délivrance d'une autorisation de mise en service d'un système d'information ou encore l'identification du niveau de sécurité à atteindre pour obtenir la conformité à une réglementation.
- Selon l'objectif défini, il en est déduit le niveau de granularité de l'étude et les ateliers à conduire.
- Posez les différentes hypothèses et contraintes qui devront être prises en compte dans l'analyse.

5.1.4.2 Délimitez les périmètres métier et technique

Dans un deuxième temps, vous allez recenser les missions, valeurs métier (VM) et biens supports (BS) relatifs à l'objet de l'étude.
Les questions qui pourront être posées sont :

- À quoi sert le système industriel ? Quelles sont ses missions principales, ses finalités, ses raisons d'être ?
- Quelles sont les fonctions et les informations majeures permettant au système industriel étudié de réaliser ses missions ?
- Quels sont les services numériques (applications, réseaux informatiques, structures organisationnelles, ressources humaines, locaux, etc.) qui permettent de mener à bien ces fonctions ou de traiter ces informations ?

Attention

Veillez à bien respecter le niveau de granularité choisi pour l'étude, en particulier lors de l'identification des missions et des valeurs métier.

Commencez par lister **l'ensemble des missions** du système industriel, c'est-à-dire les finalités et raisons d'être majeures de ce dernier. Selon le niveau de granularité de l'étude, les missions à identifier peuvent parfois être intrinsèques au système industriel mais sont généralement celles de l'organisme dans lequel l'objet s'inscrit.
Par exemple :

- ce que le système produit (fabrication de papier, production d'électricité, etc.) ;
- le service qu'il rend (transport de voyageurs, transport d'électricité, sécurité des biens et des personnes, etc.).

De la même manière, recensez ensuite l'ensemble des valeurs métier (VM) associées au système industriel, à savoir les informations ou fonctions jugées importantes dans le cadre de l'étude et qu'il convient de protéger. Les valeurs métier représentent le patrimoine informationnel important pour l'organisation qu'une source de risque aurait intérêt à attaquer pour atteindre ses objectifs (par exemple, la protection des biens et des personnes, la production de vapeur, le niveau de charge du réseau de transport de fluide, etc.).

L'objectif est d'identifier les valeurs métiers associées au système industriel. Contrairement à EBIOS RM qui ne recherche pas l'exhaustivité et veille à limiter le nombre de valeurs métier pour ne garder que celles identifiées comme essentielles ou sensibles, cette méthode de classification requiert d'identifier toutes les fonctions et informations du système industriel en respectant le niveau de granularité choisi pour l'étude.

A titre indicatif, un système industriel correspond à une mission et trois à cinq valeurs métier telles que la production, la supervision, la sécurité des biens et des personnes, etc.

- À ce stade, identifiez, pour chacune des valeurs métier, les équipements associés (périmètre technique). Pour réaliser cela, il est possible d'identifier, pour chacune des valeurs métier, les boucles d'asservissement et les données concernées.
- Identifiez le chemin de la donnée dans vos systèmes d'information, et, en particulier, tous les systèmes (sur site ou externalisés) qui traitent ou stockent la donnée : ces systèmes font partie du périmètre technique du système industriel.

Attention

Dans le cas d'un système géographiquement réparti, veillez à inclure dans le périmètre l'ensemble des sites ou des infrastructures participant au procédé industriel.

5.2 Activité 2 - Établir des zones au sein du périmètre

5.2.1 Objectif

L'objectif de cette activité est de créer des zones cohérentes pour votre organisation à l'intérieur du périmètre technique identifié précédemment. Ce découpage n'est pas nécessairement issu des valeurs métier précédemment identifiées.

Information

À titre d'exemple, la norme IEC 62443 [9] précise les caractéristiques des zones et des conduits dans le fascicule 3-2 du référentiel normatif.

5.2.2 Renvoi à EBIOS RM

Cette activité n'est pas issue de la méthode EBIOS RM.

5.2.3 Données de sorties

Les données élaborées à l'issue de cette activité sont les suivantes :

- les critères permettant de créer les zones ;
- le découpage du périmètre en zones.

5.2.4 Procédure

Établissez les critères permettant d'établir les zones. Pour réaliser cela, identifiez les missions du système industriel ainsi que ses caractéristiques.

À titre d'exemple, pour définir ces critères, les questions suivantes peuvent être posées :

- Que produit le système industriel ?
- Quelles sont les actions du système industriel sur le procédé industriel ?
- Quelles sont les fonctions assurées par le système industriel ?
- Quels sont les lieux d'implantation du système industriel ?
- Quelles sont les populations intervenant sur le système industriel ?
- Quelles sont les fonctions essentielles au bon déroulement du procédé industriel ?
- Existe-t-il déjà une division (naturelle ou organisationnelle) du périmètre ?
  Les divisions peuvent être dues :
  - au niveau de classification de sécurité fonctionnelle (par exemple le niveau de SIL [3]) des équipements (automate de sécurité ou relais de sécurité) ;
  - à l'usage (par exemple, par type de produit issu de l'installation industrielle) ;
  - à l'architecture du réseau existant ;
  - au constructeur (par exemple, un ensemble de lots fournis et maintenus par un même fournisseur) ;
  - à la situation géographique, notamment dans le cas de systèmes géographiquement répartis ;
  - à la population intervenant sur les systèmes (par exemple, les machines sous la responsabilité d'un corps de métier ou d'un prestataire).

Pour compléter, identifiez ensuite les populations administrant les ressources de l'usine, notamment :

- les populations en charge de la configuration des automates (administration métier) et des applicatifs industriels (souvent désignés comme l'ingénierie) ;
- les populations en charge du maintien en condition opérationnelle et de sécurité du matériel informatique de l'usine (postes de travail, serveurs, équipements réseau, etc.).

À ce stade, un ensemble de critères permettant l'établissement de zones doit apparaître. Affinez ces critères pour obtenir des zones constituées de ressources homogènes et administrées par une même population.

5.3 Activité 3 - Identifier les événements redoutés et en déduire la classe

5.3.1 Objectif

L'objectif de cette activité est d'identifier les événements redoutés portant sur le système industriel et d'en déduire la classe des zones.

5.3.2 Renvoi à EBIOS RM

Cette activité s'appuie sur EBIOS RM - Atelier 1.c : Identifiez les événements redoutés et estimez leur niveau de gravité.
Dans une analyse EBIOS RM, le degré de préjudice ou d'impact sur les événements redoutés est estimé selon une échelle de gravité permettant la hiérarchisation de ces derniers. Ce n'est pas le cas dans la méthode de classification. L'évaluation du niveau d'impact sur les événements redoutés doit permettre la comparaison des événements redoutés entre deux systèmes industriels.

5.3.3 Données de sorties

Les données élaborées à l'issue de cette activité sont les suivantes :

- les événements redoutés et leur gravité ;
- le niveau d'implication du numérique pour chacun des événements redoutés ;
- la classe de chaque zone.

5.3.4 Procédure

Dans la méthode de classification, les événements redoutés sont associés aux valeurs métier et traduisent les effets préjudiciables d'une altération de la qualité de service et des performances auxquelles la valeur métier doit répondre.

3. *Safety Integrity Level*. Niveau de sécurité d'un produit ou système (défini dans la norme CEI 61508).

Afin de faire émerger les événements redoutés, vous pouvez, pour chaque valeur métier recensée dans l'activité précédente, identifier :

- les événements redoutés directement issus des études de sûreté de fonctionnement et des processus qualité de votre organisation. Ces événements redoutés ont généralement comme source un événement accidentel et non une source malveillante ;
- les effets néfastes d'une atteinte en disponibilité de la valeur métier (par exemple, production impossible, service non rendu) ;
- les effets néfastes à une atteinte en intégrité de la valeur métier (par exemple, produit non conforme, dysfonctionnement du procédé) ;
- les effets néfastes d'une atteinte en confidentialité (par exemple, la divulgation d'une expertise à l'origine d'un avantage concurrentiel) ;
- les effets préjudiciables d'une atteinte en traçabilité (par exemple, perte du numéro de lot d'un produit) ;
- les effets préjudiciables d'une altération de la qualité de service et des performances auxquelles la valeur métier doit répondre.

Information

- Un événement redouté est décrit sous la forme d'une expression courte ou d'un scénario permettant une compréhension facile du préjudice lié à l'atteinte de la valeur métier concernée.
- Pour les événements redoutés portant atteinte à la disponibilité, il est recommandé de préciser au-delà de quelle perte de service le niveau de gravité mentionné est atteint (par exemple, indisponibilité du service pendant une durée supérieure à 2 heures, impossibilité de diffuser des flux de données supérieurs à 1 Mbps, etc.). Cette approche vous permettra notamment d'ancrer dans votre appréciation du risque la notion de mode de fonctionnement dégradé.
- À ce stade, les événements redoutés sont identifiés du point de vue de l'organisation, en dehors de tout scénario d'attaque. Leur gravité est estimée indépendamment des capacités d'un attaquant à les réaliser.

Il est ensuite nécessaire d'estimer la gravité de chaque événement redouté selon la méthode proposée en section 4.1.

Information

Il est important de vous accorder sur l'usage et la définition de l'échelle d'impact économique conformément au tableau 7. Cette échelle doit être adaptée à votre activité et à votre entité.

Pour chaque événement redouté, identifiez le niveau d'implication du numérique. Les questions qui pourront être posées sont :

- Cet événement peut-il être déclenché par ou depuis un équipement informatique ou un équipement d'informatique industrielle, tel qu'un automate ?

- Cet événement peut-il être facilité par l'usage d'un équipement informatique ou un équipement d'informatique industrielle, tel qu'un automate ?

Pour chaque zone, identifiez l'évènement redouté ayant la gravité maximale. Cette gravité correspond à la classe de la zone.

L'intégration de la vraisemblance est réalisée au travers des scénarios stratégiques définis par la méthode EBIOS RM conformément à la section 5.4 et à l'étude de cas proposée à l'annexe B.

Information

Si vous souhaitez effectuer des regroupements entre zones, la classe d'un ensemble de zones est égale à la classe la plus élevée de ces zones.

5.3.5 Surclassement

Selon la définition initiale du périmètre, il est possible de surclasser une zone.

Pour chacune des zones, étudiez la pertinence du surclassement, notamment :

- Dans le cas d'installations géographiquement réparties, l'impact d'un événement pour un site peut être faible. Cependant, l'occurrence de cet événement simultanément sur un ensemble de sites peut avoir un impact significatif. Dans ce cas, il est recommandé de surclasser chaque site pour prendre en compte l'impact maximal de l'événement à l'échelle de l'ensemble des sites comme présenté à la section 6.4.1
- Si deux zones de classes distinctes ne peuvent pas être cloisonnées au niveau recommandé (voir recommandations dans le guide de mesures détaillées [6]), il est recommandé de surclasser vers la classe la plus élevée (par exemple dans le cas d'automates de sécurité fonctionnelle - SIS - et standards ne pouvant être cloisonnés entre eux).

5.3.6 Dépendances fonctionnelles

Une dépendance fonctionnelle apparaît lorsqu'une communication doit s'établir entre entre deux zones. C'est le cas lorsque, pour réaliser une fonction, une zone dépend d'une donnée provenant d'une autre zone.
La sécurité de l'interconnexion est assurée selon deux scénarios :

- Si la communication est établie entre deux zones de même classe, alors, on peut considérer que le risque induit est acceptable.
- Sinon, l'interconnexion doit être sécurisée tel que décrit dans le guide des mesures détaillées.

Information

Un principe équivalent est décrit dans le fascicule 3-2 de la norme IEC 62443 [9] :

- Dans une zone, un équipement interconnecté à un ou plusieurs équipements hérite du niveau sécurité (SL) le plus élevé du ou des bien(s) connecté(s).
- Un conduit entre deux ou plusieurs zones distinctes hérite du niveau de sécurité (SL) le plus élevé des zones connectées.

5.4 Réaliser une analyse EBIOS RM après la méthode de classification

Les éléments ci-après permettent d'associer les deux méthodes :

- Alimentation du socle de sécurité

  Lorsque les classes ont été déterminées, l'ensemble des mesures applicables correspondantes (voir guide de mesures détaillées [6]) doit être versé au socle de sécurité EBIOS RM.

- Scénarios opérationnels

  Lors des ateliers 3 et 4, vous établissez des scénarios de risque sur la base des couples « Sources de Risques (SR) » et « Objectifs Visés (OV) ». Si vous souhaitez réaliser une analyse de risque allégée, vous pouvez considérer que ces modes opératoires usuels sont partiellement couverts par le socle de sécurité et vous concentrer sur les scénarios exploitant des particularités du système industriel étudié.

6
Étude de cas

La précédente version de la méthode de classification était mise en pratique au moyen de l'étude de cas d'un tunnel routier. Dans le cadre de la mise à jour de cette méthode, une nouvelle étude de cas, sur un réseau d'assainissement de l'eau, est intégrée au présent guide et vise à illustrer les chapitres 4 et 5.

Objectif

Ce chapitre constitue une étude de cas et a pour but de contextualiser la méthode de classification en l'appliquant au cadre de la sécurisation d'un réseau d'assainissement d'eaux usées et pluviales géré par l'entité fictive Assaineaux. Afin de ne pas surcharger le chapitre, les résultats de certains ateliers EBIOS RM ne sont volontairement pas présentés.

6.1 Contexte

6.1.1 Présentation de l'entité Assaineaux

Le réseau d'assainissement est exploité en régie par une collectivité territoriale. Pour cela, une société d'économie mixte du nom d'Assaineaux a été créée.

Le réseau d'assainissement existant est en cours de rénovation. Dans ce cadre, la société souhaite sécuriser le système d'information industriel des différents sites qu'elle exploite.

6.1.2 Organisation du réseau d'assainissement

Le réseau d'assainissement est un système fictif composé de plusieurs stations d'épuration des eaux usées et pluviales (STEP) et de pluviomètres. Ces sites sont distribués géographiquement sur un périmètre de 20 kilomètres et collectent les eaux usées et pluviales d'un bassin de population d'environ 100 000 habitants. Ce système est supervisé localement, mais aussi depuis un poste de contrôle distant. Dans le cadre de cette étude, le poste de contrôle n'est pas redondé sur un autre site. La figure 2 présente l'architecture de ce réseau.

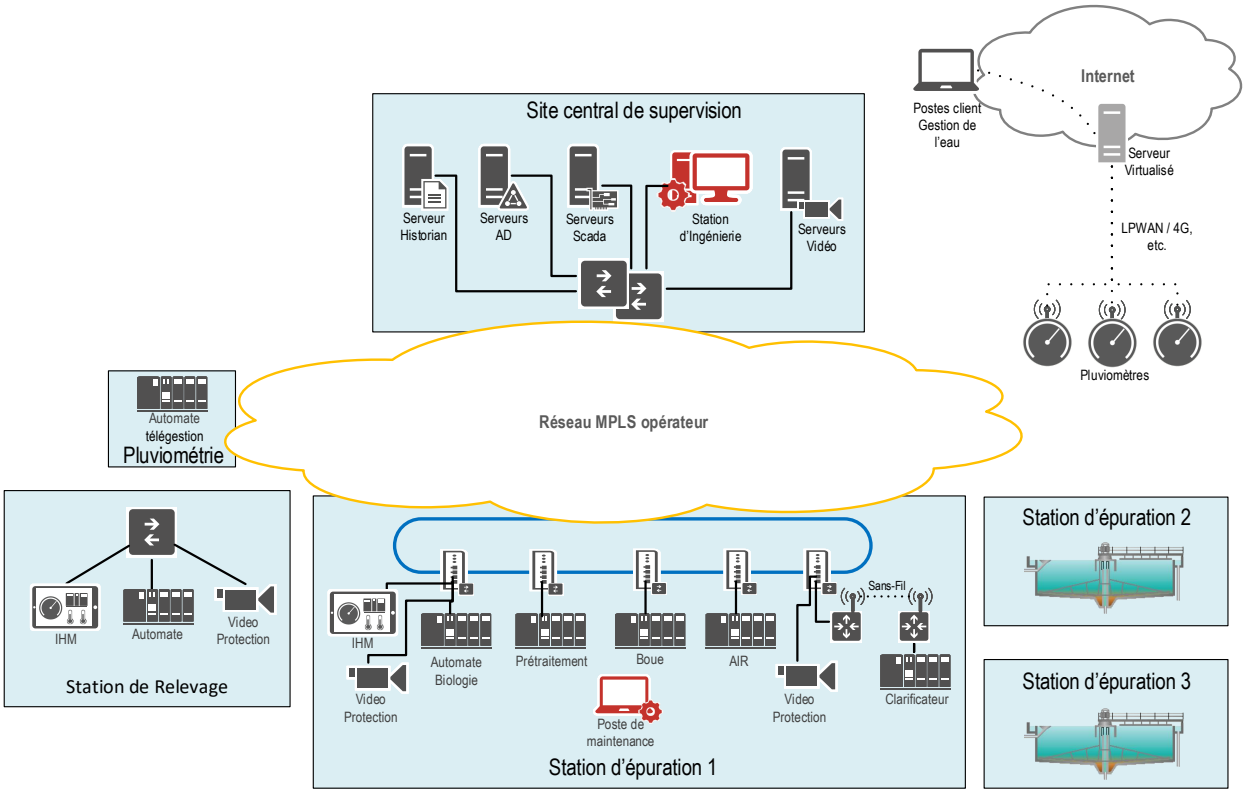

FIGURE 2 – Architecture du réseau d'assainissement - 1re approche technique avant classification

6.1.3 Définition du périmètre du réseau d'assainissement

Pour commencer cette étude, il convient de réaliser un inventaire des différentes zones du réseau d'assainissement conformément à la section 5.3 (ateliers 1.a et 1.b). Ces éléments ont été établis à partir des questions présentées à la sous-section 5.2.4.

Les zones correspondent aux fonctions suivantes :

- **le relevage** : il s'agit d'un système actif de pompage de l'eau pour permettre la poursuite de l'écoulement gravitaire de l'eau lorsque la collecte est en contre-bas de la station d'épuration ;
- **le prétraitement** : il s'agit du premier traitement de l'usine. Ce procédé permet de protéger les ouvrages (tuyaux et machines en aval par exemple) contre l'arrivée de matériaux ou de matière volumineuse (dessablage, dégraissage, etc.) ;
- **l'oxygénation** (traitement biologique) : il s'agit d'un procédé de production d'air dans l'eau permettant le développement de biomasse bactérienne. Ces bactéries aérobies dégradent les composés organiques qui peuvent contaminer l'eau (il en résulte des boues secondaires) ;
- **la clarification** (clarificateur ou décanteur secondaire) : il s'agit de la dernière étape de l'assainissement. L'objectif est d'extraire les boues des micro-organismes de l'eau traitée de manière à produire un effluent clarifié conforme aux normes de rejet ;
- **la récupération des boues** : après l'étape de clarification, les boues sont ensuite valorisées pour des applications diverses comme l'épandage, le compostage, la méthanisation ou l'incinération (après séchage) ;

- **la désodorisation** (traitement de l'air) : il s'agit d'un système permettant de réduire les odeurs émises par la station d'épuration (non traité dans le présent guide comme précisé à la section 6.2.1);
- **la pluviométrie** : il permet, lors de fortes pluies, le déversement dans un bassin de stockage ou dans un déversoir d'orage. Des pluviomètres sont également installés afin de transmettre uniquement des informations du niveau de pluie à la collectivité territoriale. Cette dernière s'y connecte au travers d'un service nuagique sur lequel sont raccordés les pluviomètres (système non traité dans le présent guide comme précisé à la section 6.2.1);
- **la supervision** : la supervision est la conduite des stations d'épuration, des ouvrages du réseau d'assainissement et des pluviomètres;
- **la vidéosurveillance** : il s'agit d'un système composé d'un poste central et de plusieurs caméras permettant de contrôler les éventuelles intrusions sur les sites du réseau d'assainissement.

6.2 Intégration des éléments de l'atelier 1 - EBIOS RM

Le cadre de l'étude a été défini à la section 6.1.3 . Suivant la méthode présentée au chapitre 5, les analyses de risque et l'application de l'atelier 1 de la méthode EBIOS RM ont permis d'identifier, entre autres, les événements redoutés (ER), les valeurs métier (VM) et les biens supports (BS). Ces éléments sont décrits dans la présente section.

6.2.1 Valeurs métier (VM)

Les valeurs métier (VM) retenues dans cette étude sont les suivantes :

- relèvement de l'eau des points bas vers des points hauts;
- traitements des eaux (prétraitement / traitement primaire);
- traitement des boues (séchage et incinération des boues et des graisses).

Information

Les valeurs métier *valorisation des déchets*, *transport* (collecte et transfert des eaux de pluie vers le milieu naturel, etc.) et *désodorisation* (traitement de l'air) n'ont pas été retenues par souci de simplification [4] de l'étude et dans certains cas parce qu'aucun système d'information n'est présent et qu'il s'agit essentiellement d'équipements physiques (collecteurs, bus, etc.).

6.2.2 Biens supports de la valeur métier

D'un point de vue technique, chaque fonction peut impliquer un nombre plus ou moins important de composants. Sans tenir compte de la mutualisation possible de certains équipements (dont les automates et les consoles IHM), la liste des fonctions et des composants associés est résumée dans le tableau 8.

4. Une indisponibilité ou une malveillance sur ces éléments n'ont pas d'incidence sur les événements redoutés.

Valeurs métier (VM)	Fonctions de la VM	Biens supports
Relèvement de l'eau des points bas vers des points hauts	**Relevage**	Automate IHM locale Pompe et sonde de mesure de niveau
Traitements des eaux	**Prétraitement**	Automate IHM locale Pompe d'aspiration des particules, moteur du pont racleur, sonde de mesure de niveau, électrovannes, débitmètre, etc.
	Oxygénation	Automate IHM locale Injecteurs de réactifs, compresseur ou surpresseur d'air, électrovannes, agitateur, sonde de mesure de niveau, sonde de mesure O_2 turbine de surface, ballon tampon, manomètre (qui pilote le démarrage du compresseur lorsque la pression passe sous un seuil défini), etc.
	Clarification	Automate IHM locale Moteur du pont racleur Pompes de recirculation et d'évacuation des boues, etc.
	Vidéosurveillance du site	Serveur de gestion de la vidéosurveillance (VMS) Caméras Console de vidéosurveillance Enregistreur
	Supervision	Serveurs du système de contrôle/commande Poste opérateur du contrôle/commande
Traitement des boues	**Récupération des boues**	Automate IHM locale Pompes, débitmètre, sonde de mesure de niveau, motoréducteur, air-comprimé, capteur de pression, électrovanne, agitateur, etc.

TABLE 8 – Fonctions des valeurs métier

6.2.3 Événements redoutés

Dans le cadre de l'étude de sûreté de fonctionnement, la société Assaineaux a notamment mené diverses analyses, dont :

- une analyse et une modélisation fonctionnelles ;
- une analyse préliminaire de risques (APR) ou de dangers (APD) ;

- une analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC) ;
- un arbre de défaillances.

Ces différentes analyses, et plus particulièrement l'arbre de défaillance et l'AMDEC système (ou AMDEC fonctionnelle), ont fait émerger les modes de défaillance fonctionnelle : fonction intempestive, absence de fonction, fonction erronée, non arrêt de la fonction, etc. Elles ont ainsi permis d'identifier et de caractériser la criticité des événements redoutés liés aux défaillances des fonctions du système.

À partir de l'analyse de sûreté de fonctionnement, complétée par l'atelier 1.c de la méthode EBIOS RM, il est possible de dégager une liste d'événements redoutés regroupés dans le tableau 9.

Valeurs métier	Evénements redoutés
[VM1] Relèvement de l'eau des points bas vers des points hauts	**[ER1]** Destruction de biens matériels
[VM2] Traitement des eaux	**[ER1]** Destruction de biens matériels
	[ER2] Destruction des micro-organismes de la biologie
	[ER3] Arrêt de la fourniture du service
	[ER4] Sabotage des équipements avec un rançongiciel
[VM3] Traitement des boues	**[ER1]** Destruction de biens matériels

TABLE 9 – Liste des événements redoutés associés aux VM

6.3 Classification

Information

Le maintien de la vie aquatique nécessite de conserver un niveau suffisant d'oxygène dans le milieu naturel (cours d'eau, fleuve, mer, etc.). Les matières organiques rejetées alimentent des micro-organismes. Ces micro-organismes consomment de l'oxygène pour se développer et dégrader cette pollution, réduisant ainsi le niveau d'oxygène présent dans le milieu naturel. En vue de maîtriser les risques environnementaux causés par les eaux usées, plusieurs paramètres sont contrôlés :

- la demande chimique en oxygène (DCO). Il s'agit de mesurer les substances consommatrices d'oxygène. Cette mesure permet de déterminer l'effet d'un effluent sur le milieu récepteur ;
- la demande biochimique en oxygène (DBO). Il s'agit de la dégradation des charges organiques polluantes par les micro-organismes. Cette mesure permet de déterminer l'effet d'un effluent sur le milieu naturel ;
- la matière en suspension (MES). La présence trop importante de MES peut colmater les branchies des poissons.

Relevage : Un défaut de cette unité peut entraîner une inondation totale ou partielle des installations ou une détérioration significative des équipements en aval (défaut de pompe ou perte de l'électrovanne en aval). A partir des échelles de gravité présentées à la section 4.3, il en résulte les niveaux suivants :

Impact humain : 1 Impact environnemental : 2 Impact macroéconomique : 1

Prétraitement :
Un défaut sur ce système peut provoquer les événements suivants :

- un risque de débordement conduisant à un colmatage des évacuations ;
- un dégagement toxique de biogaz au niveau du poste de réception des graisses ;
- des risques sanitaires, eau potable polluée avec des points de captage de l'eau à proximité (production d'eau) ;
- une pollution du milieu naturel lors du rejet au niveau de l'effluent ;
- une mauvaise image de la collectivité territoriale ;
- un risque de destruction des équipements en aval si l'eau contient trop de sable ou de graisse ;
- une atteinte à la fonction du traitement biologique.

Impact humain : 1 Impact environnemental : 2 Impact macroéconomique : 1

Oxygénation : Un défaut de cette unité peut entraîner une non conformité de l'eau rejetée (risque de pollution) due à la dégradation de l'unité de traitement biologique (panne d'un composant de l'unité d'oxygénation).

Impact humain : 1 Impact environnemental : 2 Impact macroéconomique : 1

Clarification : Un défaut de cette unité peut entraîner une non conformité de l'eau rejetée (risque de pollution) due à la dégradation de l'unité de traitement biologique (panne d'un composant de l'unité de clarification ou obstruction de l'évacuation des éléments flottants).

Impact humain : 1 Impact environnemental : 2 Impact macroéconomique : 1

Information

Le rejet d'eaux usées non traitées peut entraîner des risques sanitaires pour les humains comme pour les animaux si une nappe phréatique est à proximité. Dans cette étude, aucune station d'épuration ni de collecteur d'eaux usées ne sont à proximité d'une nappe phréatique ou d'un puits de forage pour la production d'eau potable.

Vidéosurveillance : Le système de vidéosurveillance n'intervient pas dans le procédé industriel ni dans la prise de décisions des exploitants pour la commande de l'installation et est utilisé pour

détecter les intrusions dans les sites du réseau d'assainissement. En revanche, un intrus pourrait endommager la biomasse, voire même effectuer un arrêt électrique du site concerné.

Impact humain : 1 Impact environnemental : 2 Impact macroéconomique : 2

Supervision :
La liste des événements qui ne seraient plus visibles au centre de supervision en cas de défaut de ce dernier est la suivante :

- alarmes de défaut de surpresseurs ou de compresseurs ;
- alarmes de défaut du pont de brosse, d'agitateurs ou de capteurs ;
- alarmes de défaut du pont racleur et du seuil du couple appliqué sur le moteur du pont racleur ;
- alarmes de niveau bas dans les bassins ;
- alarmes de débits intempestifs ;
- alarmes de défaut de pompe ;
- visualisation et action sur le fonctionnement des différentes unités de traitement (états des pompes, des électrovannes, des niveaux des réservoirs, débits, le niveau de turbidité [5], etc.).

L'impact d'une panne du site central de supervision est plus élevé si elle est conjuguée avec une panne sur une unité fonctionnelle. Dans le cas contraire, le fonctionnement du procédé reste opérant. De plus, certains sites sont équipés d'une supervision locale. Il en résulte les éléments ci-dessous.

Impact humain : 1 Impact environnemental : 1 Impact macroéconomique : 1

Récupération des boues :
Un défaut de ce système peut provoquer les événements suivants :

- un retard dans l'incinération des déchets ;
- des opérateurs blessés ou intoxiqués ;
- une mauvaise image de la métropole (ou de la collectivité territoriale) ;
- une incapacité à déterminer la qualité des fumées rejetées.

Impact humain : 2 Impact environnemental : 2 Impact macroéconomique : 1

Information

Le critère économique de l'entreprise n'a pas été ajouté dans cette étude de cas.

5. La turbidité est un des paramètres qui caractérise la qualité d'une eau. Il s'agit de désigner ici le trouble de l'eau par la matière en suspension.

En se référant au chapitre 4 et en tenant compte des critères mentionnés à la section 4.3, les éléments suivants ont été retenus (conformément à l'activité 3 5.3) :

Fonctions	Impact Humain	Impact environnemental	impact macroéconomique
Relevage	1	**2**	1
Prétraitement	1	**2**	1
Oxygénation	1	**2**	1
Clarification	1	**2**	1
Videosurveillance	1	**2**	1
Supervision	1	1	1
Récupération des boues	**2**	**2**	1

TABLE 10 – Impacts par fonction

En tenant compte des éléments précédents, la répartition des classes est présentée dans le tableau 11. Cette classification des fonctions sera utilisée pour la suite de l'analyse.

Classes	Fonctions
Classe 1	Supervision
Classe 2	Vidéosurveillance, Relevage, Prétraitement, Oxygénation, Clarification et Récupération des boues
Classe 3	Aucune
Classe 4	Aucune

TABLE 11 – Classification des fonctions

6.4 Raffinement et regroupement de classes

6.4.1 Prise en compte du périmètre (surclassement)

Comme précisé à la section 4.2.1, le périmètre doit être choisi afin de contenir l'ensemble des installations critiques d'un site ou d'une infrastructure. Ainsi, dans cette étude de cas, **il est nécessaire d'intégrer l'ensemble des stations d'épuration**. Le bassin d'habitants est donc plus peuplé qu'avec une seule station d'épuration (ce qui induit un surclassement pour le périmètre concerné). En effet, en intégrant l'ensemble des stations d'épuration gérées par la collectivité territoriale, la population à considérer est la totalité du bassin de vie (plus de 100 000 habitants). L'impact environnemental pour la pollution de l'eau s'élève donc à 3 et les l'impacts macroéconomiques à 2 comme précisé à dans le tableau 12.

Information

La fonction « Vidéosurveillance » n'est pas concernée par cette réévaluation car une attaque sur l'ensemble des sites ne provoquerait pas directement un évènement redouté. Il faudrait que des intrusions aient lieu au même moment sur l'ensemble des sites du réseau d'assainissement. Il s'agit d'une mesure de sécurité pour protéger un système ayant des valeurs métiers importantes pour l'entité.

Fonctions	Impact humain	Impact environnemental	impact macroéconomique
Relevage	1	**3**	2
Prétraitement	1	**3**	2
Oxygénation	1	**3**	2
Clarification	1	**3**	2
Videosurveillance	1	2	2
Supervision	1	1	1
Récupération des boues	**2**	**2**	1

TABLE 12 – Impacts par fonction après surclassement

En tenant compte du périmètre de l'ensemble des stations d'épuration, la répartition des classes est présentée dans le tableau suivant :

Classes	Fonctions
Classe 1	Supervision
Classe 2	Récupération des boues et Vidéosurveillance
Classe 3	Relevage, Prétraitement, Oxygénation et Clarification
Classe 4	Aucune

TABLE 13 – Classification des fonctions avec l'ensemble du périmètre

6.4.2 Dépendances fonctionnelles des classes

Au-delà de la classification des fonctions de manière unitaire, et comme précisé à la section 5.3.6, il convient de compléter l'analyse par l'étude des relations entre ces fonctions (les dépendances fonctionnelles de la présente étude sont présentées à l'annexe A).

Ainsi, l'analyse des dépendances fonctionnelles impose de reclasser les fonctions « Supervision » et « Récupération des boues » en classe 3 conformément à la figure 4 présentée à l'annexe A. Un récapitulatif est présenté dans le tableau ci-dessous :

Classes	Fonctions
Classe 1	Aucune
Classe 2	Vidéosurveillance
Classe 3	Supervision, Relevage, Prétraitement, Oxygénation, Clarification et Récupération des boues
Classe 4	Aucune

TABLE 14 – Classification des fonctions avec dépendances fonctionnelles

6.5 Intégration de la menace

6.5.1 Scénarios stratégiques - atelier 3

Suivant la méthode présentée au chapitre 5, l'application de l'atelier 2 de la méthode EBIOS RM a permis d'identifier et de caractériser un couple (SR/OV). Les analyses réalisées dans le cadre de l'atelier 3 de la méthode EBIOS RM, à partir des couples SR/OV, ont permis de bâtir les scénarios stratégiques suivants :

- arrêt du service ;
- perte des données d'exploitation.

6.5.2 Scénarios opérationnels - atelier 4

À l'issue de l'analyse des scénarios opérationnels (atelier 4 de la méthode EBIOS RM) et du traitement du risque (atelier 5 de la méthode EBIOS RM) présentés à l'annexe B, il est possible de préciser les mesures à appliquer selon les valeurs métier et les biens supports concernés (voir le tableau 8).
Les scénarios de risques opérationnels **R1**, **R2**, **R3** et **R4** du scénario stratégique « Arrêt du service » présentent un risque élevé.
Ces scénarios sont liés aux événements redoutés **ER1** et **ER2** conformément au tableau 9.
Ces événements redoutés sont associés aux valeurs métier **VM1**, **VM2** et **VM3**.

Information

Ces valeurs métier étant portées par des biens supports, il est important d'agir sur ces biens supports afin de réduire les risques liés à la malveillance. Les mesures détaillées sont décrites dans l'étude de cas du guide de mesures détaillées [6]. Une première étape peut consister en la séparation physique du réseau de vidéosurveillance afin de rendre ce réseau totalement indépendant de ceux des stations d'épuration.

Annexe A
Dépendances fonctionnelles

Les relations entre les fonctions peuvent se résumer à celles de la figure 3. Les relations sont toutes bidirectionnelles vers le centre de supervision métier ou le PC sécurité. Des communications inter-sites entre fonctions sont également présentes (variables non émises par le centre de supervision ou pour transmettre des états locaux).

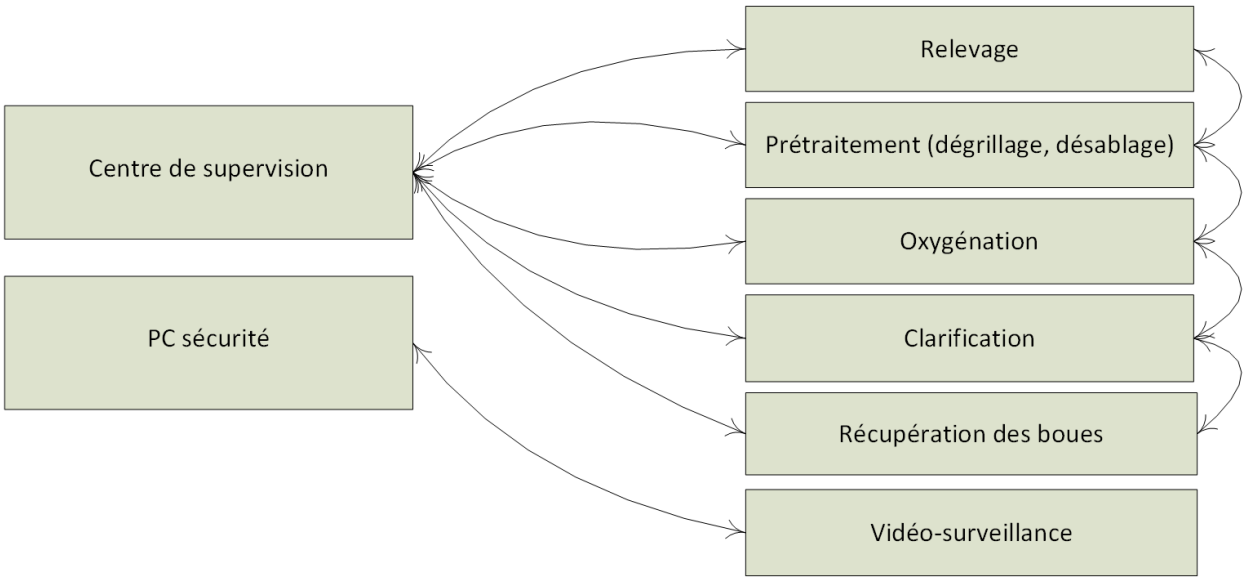

FIGURE 3 – Étude de cas - Graphe des dépendances fonctionnelles

Le site central de supervision communique avec l'ensemble des fonctions. Les dépendances fonctionnelles nécessitent de relever le niveau de classification des fonctions « Supervision » et « Récupération des boues ».

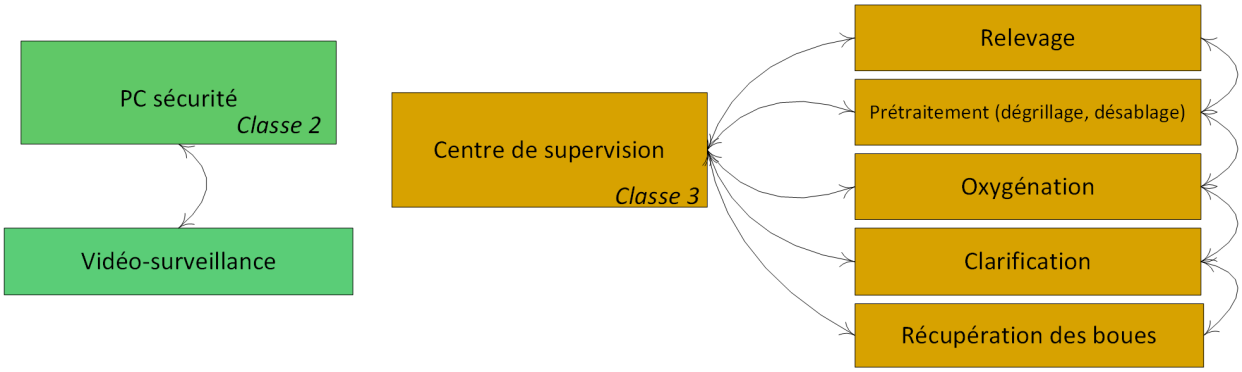

FIGURE 4 – Étude de cas - Graphe après analyse des dépendances fonctionnelles

Annexe B
Étude du risque

Ce chapitre présente le traitement du risque selon les différents scénarios opérationnels qui peuvent mener à chacun des événements redoutés listés à la section 6.2.3.

B.1 Cartographie des risques relatifs au scénario stratégique « Arrêt du service »

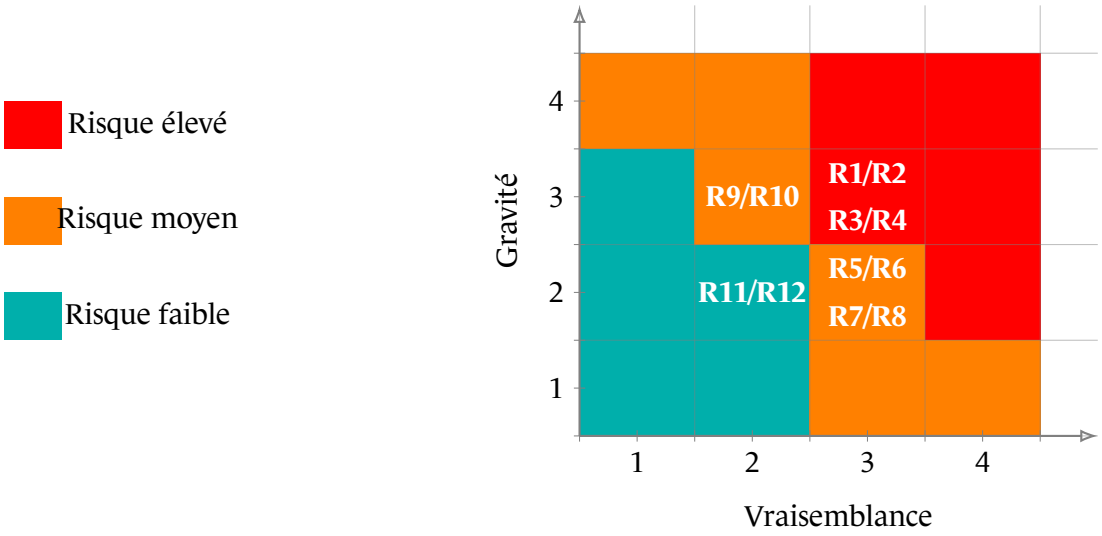

FIGURE 5 – Cartographie « Arrêt du service »

Les scénarios opérationnels sont les suivants :
R1 : Compromission d'un compte légitime entraînant la destruction de matériels
R2 : Exploitation de vulnérabilités entraînant la destruction de matériels.
R3 : Compromission d'un compte légitime entraînant la destruction de la biomasse.
R4 : Exploitation de vulnérabilités entraînant la destruction de la biomasse.
R5 : Compromission d'un compte légitime entraînant l'arrêt du service (via chiffrement par rançongiciel).
R6 : Exploitation de vulnérabilités entraînant l'arrêt du service (via chiffrement par rançongiciel).
R7 : Compromission d'un compte légitime entraînant l'arrêt du service (via le sabotage des équipements).
R8 : Exploitation de vulnérabilités entraînant l'arrêt du service (via le sabotage des équipements).
R9 : Propagation d'une attaque au travers d'un tiers entraînant la destruction du matériel.
R10 : Propagation d'une attaque au travers d'un tiers entraînant la destruction de la biomasse.
R11 : Propagation d'une attaque au travers d'un tiers entraînant l'arrêt du service (via chiffrement

par rançongiciel).
R12 : Propagation d'une attaque au travers d'un tiers entraînant l'arrêt du service (via le sabotage des équipements).

B.2 Cartographie des risques relatifs au scénario stratégique « Perte des données d'exploitation »

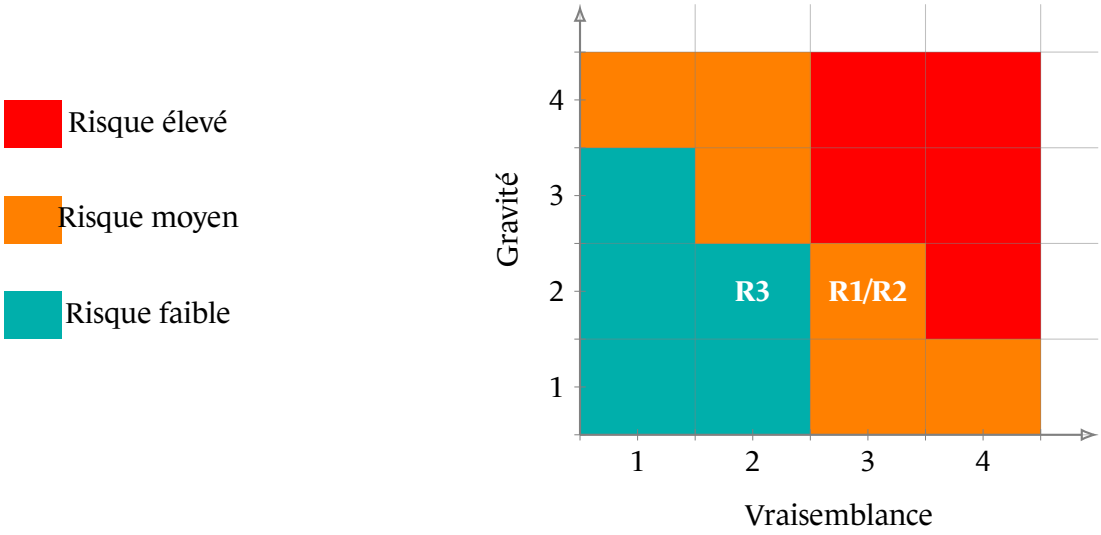

FIGURE 6 – Cartographie « Perte des données d'exploitation »

Les scénarios opérationnels sont les suivants :
R1 : Compromission d'un compte légitime entraînant la perte de données d'exploitation.
R2 : Exploitation de vulnérabilités entraînant la perte de données d'exploitation.
R3 : Propagation d'une attaque au travers d'un tiers entraînant la perte de données d'exploitation.

Bibliographie

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

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

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

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

[5] *La méthode EBIOS Risk Manager - Le Guide*.
Guide ANSSI-PA-048 v1.5, ANSSI, mars 2024.
https://cyber.gouv.fr/ebios-rm.

[6] *La cybersécurité des systèmes industriels - Mesures détaillées*.
Guide Version 2.0, ANSSI, A paraître 2025.
https://cyber.gouv.fr/publications/la-cybersecurite-des-systemes-industriels.

[7] *Service public de la diffusion du droit*.
Code, Legifrance.
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006901449.

[8] *Service public de la diffusion du droit*.
Code, Legifrance.
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043978078.

[9] *ISA/IEC 62443 : série de normes ISA/IEC 62443, « Sécurité des automatismes industriels et des systèmes de contrôle »*.
Document normatif, ISA, juillet 2009 à 2024 selon les parties.
Ce document résulte de développements conjoints entre l'IEC et l'ISA.
https://www.boutique.afnor.org/fr-fr/resultats?Keywords=IEC+62443
https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

[10] *IEC 61508 : Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité.*
Document normatif, IEC, 2010.
https://www.boutique.afnor.org/fr-fr/norme/iec-6150812010/securite-fonctionnelle-des-systemes-electriques-electroniques-electroniques/xs121824/244493.

[11] *IEC 24772 : Langages de programmation. Conduite pour éviter les vulnérabilités dans les langages de programmation.*
Document normatif, IEC, 2024.
https://www.boutique.afnor.org/fr-fr/norme/bs-iso-iec-2477212024/langages-de-programmation-conduite-pour-eviter-les-vulnerabilites-dans-les-/eu188126/427410.

[12] *Piloter la remédiation d'un incident cyber*.
Guides, ANSSI, 2024.
https://cyber.gouv.fr/piloter-la-remediation-dun-incident-cyber.

[13] *Le panorama de la menace*.
Etude, ANSSI, Publiée chaque année.
https://cyber.gouv.fr/le-panorama-de-la-cybermenace.

Version 2.0 - 10/03/2025- ANSSI-PA-107
Licence ouverte / Open Licence (Étalab - v2.0)
ISBN : 978-2-11-167186-7 (papier)
ISBN : 978-2-11-167187-4 (numérique)
Dépôt légal : mars 2025

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité