INDUSTRIE

DOSSIER TECHNIQUE

GUIDE DE LA CYBERSÉCURITÉ DES **SYSTÈMES INDUSTRIELS**

1 Tous publics **2 Avancé** 3 Expert

Septembre 2025

Découvrir et comprendre
les enjeux, mettre en place
les mesures de sécurité

CLUSIF

Table des matières

Remerciements

Le Clusif tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

L'animateur du groupe de travail :

Mohammed Ayoub	**KARA-ALI**	Wavestone

Les précédents animateurs du groupe de travail :

Etienne	**CHARBONNIER**	Wavestone
René	**KOUM**	Eclairion

Les contributeurs à la seconde édition du guide :

Guillaume	**CHAUSSIN**	Cisco
Antony	**GONCALVES**	Nutrition & Santé
Richard	**IMPERIAL**	IN VIVO GROUP
Guillaume	**JICQUEL**	Veolia
Stéphanie	**JOUVE**	Médiane Système
Guillaume	**LE HEGARET**	SETEC
Nicolas	**LEFEVRE**	Nijkerk
Jean-Yves	**LEMARCHAND**	GRTGaz
Olivier	**LEVY**	Kyron
Vincent	**NICAISE**	Stormshield
Thierry	**PERTUS**	CONIX
Nathan	**VOISIN**	Schneider Electric
Laurent	**CRUZ-MERMY**	ELCEM-COM

Les contributeurs à la première édition du guide :

Patrice	**BOCK**	Bock Conseil
Jean	**CAIRE**	RATP
Guillaume	**CHAUSSIN**	Cisco
David	**DIALLO**	ANSSI
Guillaume	**LE HEGARET**	Setec ITS
Frédéric	**LENOIR**	RTE
Frédéric	**MIRAULT**	Suez
Thierry	**PERTUS**	CONIX

Le **Clusif** remercie également les membres du **GT Cybersécurité des systèmes industriels et les adhérents** ayant participé à la construction et à la relecture.

1 À propos du groupe de travail Cybersécurité des systèmes industriels

Le groupe de travail Cybersécurité des systèmes industriels est un groupe d'échange et de partage entre les acteurs de la sécurité informatique du monde industriel. Il regroupe notamment des RSSI, des architectes, des éditeurs et des consultants.

Les objectifs du groupe sont d'échanger sur les pratiques en matière de cybersécurité des systèmes industriels, d'analyser les tendances actuelles et les évolutions réglementaires.

Le groupe, créé en 2013, a mené plusieurs travaux qui ont abouti, entre autres, à la publication, en 2017, de Fiches incidents cyber SI industriels[1] ainsi qu'au Panorama des référentiels de sécurité[2], dont la dernière mise à jour a été publiée en 2019.

Le groupe a par la suite été remplacé par l'Espace Cybersécurité Industrielle en 2025.

[1] https://clusif.fr/publications/fiches-incidents-cyber-industriels-2017/

[2] https://clusif.fr/publications/panorama-des-referentiels-2eme-edition-2/

2 Introduction

En 2019, le groupe de travail (GT) Cybersécurité des systèmes industriels a publié la mise à jour de son Panorama des référentiels de sécurité des systèmes industriels. Le panorama, unique document en son genre, inclut une analyse des référentiels de sécurité traitant de la cybersécurité des systèmes industriels. L'analyse du groupe de travail a permis de noter la présence d'une littérature abondante, avec une tendance à citer finalement les mêmes exigences et mesures de sécurité issues des principaux référentiels de sécurité (NIST, IEC 62443, ISO, ANSSI). Cependant, le groupe de travail a noté que le traitement, par les référentiels, de certaines thématiques, ne permettait pas une mise en application concrète et pratique.

En effet, la littérature traite parfois vaguement de certaines thématiques en reprenant les concepts issus de la sécurité des systèmes d'information bureautique avec une contextualisation limitée pour le milieu industriel ou, parfois même, sans vulgarisation pour les populations qui n'y sont pas familières. Ceci complexifie l'application des mesures de sécurité en milieu industriel et se traduit donc par une non-compréhension de leur intérêt, et, parfois même, par leur pur et simple abandon.

2.1 Objectifs du guide

L'objectif de ce document est d'expliquer, pour certaines thématiques de sécurité, les enjeux liés à la sécurité des systèmes industriels, ainsi que la préconisation des mesures afférentes qui peuvent être implémentées de façon pratique sur le terrain. Les mesures indiquées dans ce guide pourront néanmoins nécessiter une adaptation en fonction du contexte (sectoriel, entreprise).

Ce document n'a pas vocation à être un référentiel de sécurité des systèmes industriels. En effet, comme indiqué dans le panorama, il existe un grand nombre de documents de ce type, dans lesquels il est possible de retrouver les principales mesures de sécurité. Ce guide a plus spécifiquement pour objectif de vulgariser certains concepts, ainsi que de fournir aux lecteurs des mesures pratiques applicables en milieux industriels, grâce aux retours d'expériences des experts membres du groupe de travail.

Le Guide de la cybersécurité des systèmes industriels est à destination de l'ensemble des acteurs amenés à sécuriser un système industriel existant ou à venir. Le groupe de travail a voulu que les préconisations soient applicables pour des systèmes existants, obsolètes ou non, ainsi que pour la conception de nouveaux systèmes industriels. Les acteurs visés par ce document peuvent être issus du monde de l'informatique bureautique avec des connaissances limitées sur le contexte industriel, mais également des personnes issues du monde de l'automatisme avec des connaissances limitées sur la sécurité des systèmes d'information.

2.2 Organisation du document

Le groupe de travail a établi une liste de thématiques de sécurité qui méritent des explications complémentaires. La volonté des auteurs est également de couvrir le plus grand nombre d'étapes du cycle de vie d'un système industriel : de la conception au décommissionnement, en passant par l'exploitation et la maintenance de ces systèmes. À ce titre, sont abordées dans ce document les thématiques suivantes :

- Gouvernance de la sécurité des systèmes industriels ;
- Inventaire et cartographie des systèmes industriels ;
- Appréciation des risques cyber ;
- Architecture sécurisée ;
- Sécurisation des flux ;
- Intégration et recette de sécurité ;
- Gestion de la sous-traitance ;
- Maintien en conditions de sécurité ;
- Résilience et réponse à incident ;
- Audit cybersécurité ;
- Surveillance de la sécurité des systèmes industriels.

D'autres points d'intérêt ont été identifiés et pourront faire l'objet d'une mise à jour du guide.

Chacune des thématiques a été traitée en suivant un plan identique :

- Que signifie la thématique ?
- Quel est l'intérêt de la traiter ?
- Quel est le périmètre à couvrir par la thématique ?
- Quand est-il recommandé de la traiter ?
- Quel est le coût de la thématique ?
- Comment la traiter ?
- Quelle est la personne responsable de ce traitement ?

Ce plan permet de couvrir les principaux points liés à chacune des thématiques abordées. En ce qui concerne le coût de leur traitement, il est important de préciser que le guide n'a pas vocation à fournir des valeurs, puisque celles-ci dépendent fortement du contexte. Le document permet en revanche d'identifier les paramètres impactant ce coût.

Enfin, il n'est pas recommandé d'utiliser à l'identique les métriques de l'informatique bureautique afin d'évaluer les coûts de traitement des thématiques en milieu industriel. En effet, les spécificités du milieu industriel (notamment la diversité des acteurs, des systèmes, les notions de requalification des systèmes, les difficultés géographiques de réalisation, l'obsolescence, etc.) rendent les coûts différents de l'informatique bureautique.

2.3 Hypothèses de travail

La cible des préconisations concerne les systèmes industriels existants ou à concevoir. Plusieurs hypothèses ont été émises afin que les mesures soient applicables dans la majorité des cas d'usage

2.3.1 Cycle de développement d'un système industriel

La conception d'un système industriel doit suivre un cycle en « V », qui reste la norme. Bien que des méthodologies agiles existent en milieu industriel, elles sont peu répandues en raison des fortes contraintes de qualification des systèmes.

Ces contraintes font qu'un développement agile en milieu industriel peut être assimilé à plusieurs cycles de développement en « V » avec des durées de développement plus courtes. Les préconisations de ce guide restent donc valables pour des développements en mode agile.

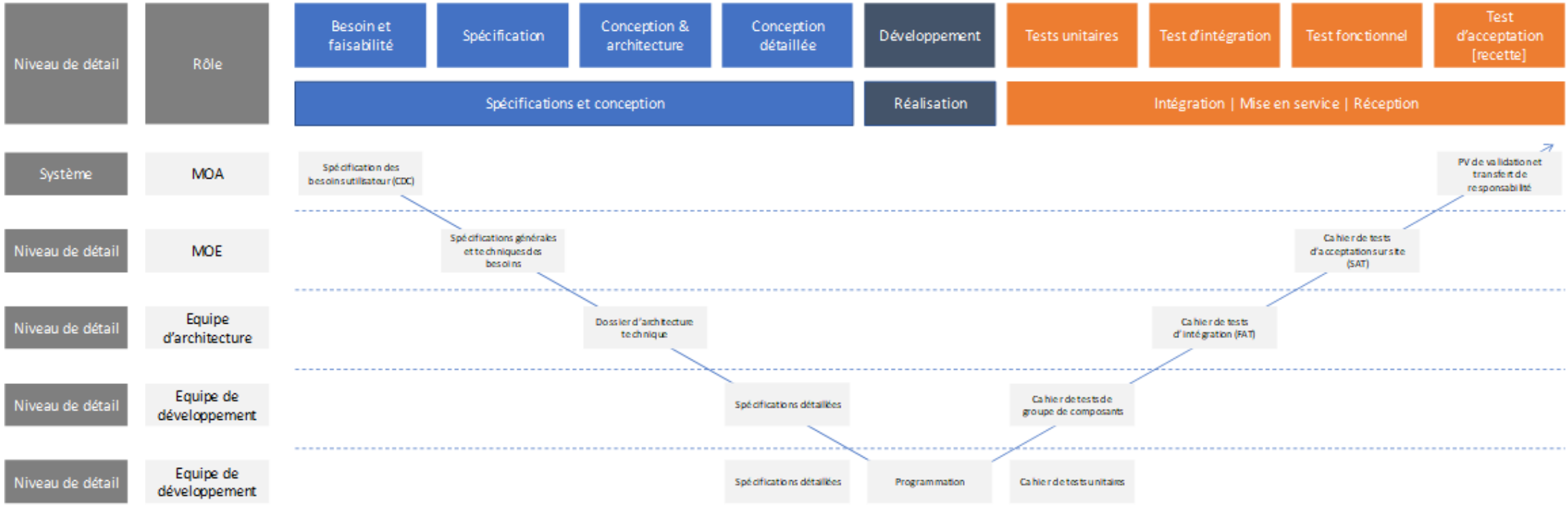


Figure 1. Étapes et principaux livrables d'un développement en cycle en « V »

Les préconisations de ce guide peuvent s'appliquer à un simple automate, une ligne de production, un site ou un ensemble de sites.

L'ensemble des secteurs (énergie, eau, assainissement, transport, etc.) sont couverts par ce document. Un système industriel de production couvre l'ensemble des cas d'usage : production d'énergie, compression de gaz, palettisation, etc.

2.3.2 Sûreté et sécurité de fonctionnement

En milieu industriel, la « sûreté de fonctionnement » et la « sécurité industrielle » sont des composantes importantes prises en compte dans le développement de la plupart des systèmes. La sûreté de fonctionnement permet au système de fonctionner en mode nominal et en mode dégradé selon les conditions de fiabilité, disponibilité, maintenabilité et sécurité définies par les exigences de conception. Afin d'évaluer la sûreté de fonctionnement de systèmes, plusieurs composantes (FMDS) sont étudiées, dont :

- La fiabilité ;
- La maintenabilité ;
- La disponibilité ;
- La sécurité.

La sécurité de fonctionnement est l'ensemble des pratiques, procédures et technologies mises en œuvre pour prévenir les accidents, minimiser les risques et protéger les travailleurs, l'environnement et les installations industrielles contre les incidents et les dangers.

La définition et la mise en œuvre des mesures visant à réduire le risque du point de vue de la sûreté et de la sécurité de fonctionnement reposent sur un processus structuré selon les étapes et les documents détaillés ci-dessous (la liste des documents n'est pas exhaustive).

- **Besoin et faisabilité** :
    - Définition des objectifs de sécurité, organisation de la sécurité.
- **Conception et architecture** :
    - Analyse préliminaire des risques ;
- **Préparation** :
    - Plan d'assurance sécurité ;
- **Études générales** :
    - Analyse élémentaire des dangers ;
    - Analyse fonctionnelle et matérielle ;
    - Analyse des modes de défaillance, de leur effet et de leur criticité (AMDEC) ;
    - Analyse des combinaisons de défaillances ;
    - Registre des situations dangereuses ;
    - Liste des pièces ou composants de sécurité ;
    - Dossier de sécurité pour la conception.
- **Études détaillées** :
    - Exigences de sécurité exportées vers les autres sous-systèmes ;
    - Exigences de sécurité exportées vers l'exploitation et la maintenance ;
    - Analyse de risques aux interfaces ;
    - Registre des situations dangereuses (mise à jour) ;
    - Liste des pièces ou composants de sécurité (mise à jour) ;
    - Dossier d'autorisation pour les tests et essais ;
    - Dossier de sécurité pour la réalisation ;
    - Cahiers de recette.
- **Recette** :
    - Tests et essais de sécurité ;
    - Analyse des risques en opération ;
    - Registre des situations dangereuses (mise à jour).

- **Mise en service** :
    - Règlement de sécurité de l'exploitation ;
    - Procédures d'exploitation et de maintenance ;
    - Plan d'intervention des secours ;
    - Registre des situations dangereuses (clôture).
- **Vie du système** :
    - Visites de contrôle de l'autorité ;
    - Diagnostic de la sécurité par un organisme indépendant ;
    - Rapports d'accident ;
    - Rapport annuel sur la sécurité (accidentologie, contrôles internes, évolution du système, plan d'action pour maintenir la sécurité).

Certaines installations industrielles mettent en œuvre des composants ayant pour objectif de garantir la sécurité industrielle des procédés. Ces composants, appelés Safety instrumented systems (SIS) peuvent être des systèmes isolés ou en réseau parallèle au réseau de production industrielle.

Afin d'éviter toute confusion entre la « sécurité informatique industrielle » et la « sécurité industrielle » (comme composante de la sécurité de fonctionnement), il a été convenu de désigner la « sécurité industrielle » par safety dans la suite du document.

3 Sécurité des systèmes d'information

La sécurité des systèmes d'information consiste en l'étude des vulnérabilités impactant un système, afin de définir et de déployer des mesures organisationnelles et techniques permettant d'assurer un niveau de service acceptable des systèmes. La sécurité des systèmes d'information repose sur plusieurs critères, dont, a minima :

- La disponibilité ;
- L'intégrité ;
- La confidentialité.
- La traçabilité.

Le champ d'application de la sécurité des systèmes d'information est large et couvre, entre autres, les sujets suivants :

- La sécurité des développements ;
- La sécurité physique ;
- La continuité et reprise d'activité ;
- La sécurité dans les processus de ressources humaines ;
- etc.

La définition et la mise en œuvre des mesures de sécurité visant à réduire le risque informatique industriel reposent sur l'établissement d'une base documentaire concluant chaque étape du développement, dont une ébauche est présentée ci-dessous.

- **Spécification des besoins utilisateurs (MOA)** : la rédaction de la spécification des besoins utilisateurs doit être réalisée à partir, a minima, des documents de référence ci-dessous :
  - Politique de sécurité des systèmes d'information, plan d'assurance sécurité[3] de l'opérateur ;
  - Identification des règles et exigences de cybersécurité spécifiques au métier ;
  - Réglementation applicable (LPM, NIS, RGPD, etc.) ;
  - Réalisation d'une analyse de risques métier (ex. : EBIOS) ;
  - Identification des risques de cybersécurité associés au système à mettre en œuvre.
- **Spécifications générales et techniques des besoins (MOE)** : la rédaction des spécifications générales des mesures techniques des besoins doit être réalisée après la conduite, a minima, des actions suivantes :
  - Identification des mesures spécifiques à mettre en œuvre au cours de la phase de développement du système (NDA, etc.) ;
  - Définition des principes d'authentification des utilisateurs et des équipements ;
  - Identification des systèmes spécifiques à déployer et connecter (surveillance des événements et alarmes : SIEM, SOC, IDS, etc.).
- **Dossier d'architecture technique (équipe architecturale)** : la rédaction du dossier d'architecture technique doit inclure a minima les thématiques suivantes :
  - Cloisonnement des réseaux par métier et/ou fonction ;
  - Identification de la politique d'accès ;
  - Serveurs et réseau d'administration ;
  - Infrastructure de déploiement des mises à jour ;

[3] Le Guide d'externalisation de l'ANSSI présente les éléments clés à figurer au sein du plan d'assurance sécurité : https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf

    - Architecture sécurisée pour les accès distants.
- **Dossier de spécifications détaillées** : ce dossier doit inclure a minima les spécifications des équipements réseau et de sécurité de type :
    - Pare-feux ;
    - Commutateurs réseau ;
    - Sondes réseau ; etc.
- **Règles de programmation sécurisée** : une politique de développement sécurisé regroupant l'ensemble des règles de programmation sécurisée est à privilégier.
- **Cahier de tests unitaires** : le cahier de tests unitaires vise à vérifier la configuration de chaque équipement (commutateurs, équipements d'automatisme, IoT, sondes, etc.).
- **Cahier de tests des groupes de composants** : le cahier de tests des groupes de composants a pour objectif la vérification des systèmes composés de plusieurs équipements (IDS, système d'identification et d'authentification, etc.).
- **Cahier de tests d'intégration FAT** : le cahier de tests d'intégration FAT a pour objectif la vérification du bon fonctionnement de l'ensemble des équipements sur plateforme d'essais (connexion du système d'identification et d'authentification, flux de communication, serveur de rebond, etc.).
- **Cahier de tests SAT** : le cahier de tests SAT a pour objectif la vérification du bon fonctionnement de l'ensemble des équipements sur site, en lieu et place de leur utilisation (flux et fonctionnalités liés aux systèmes existants).
- **Procès-verbal de validation et transfert de responsabilité** : le document a pour objectif de s'assurer de la conformité du système livré par rapport aux spécifications définies à la suite des différents tests.

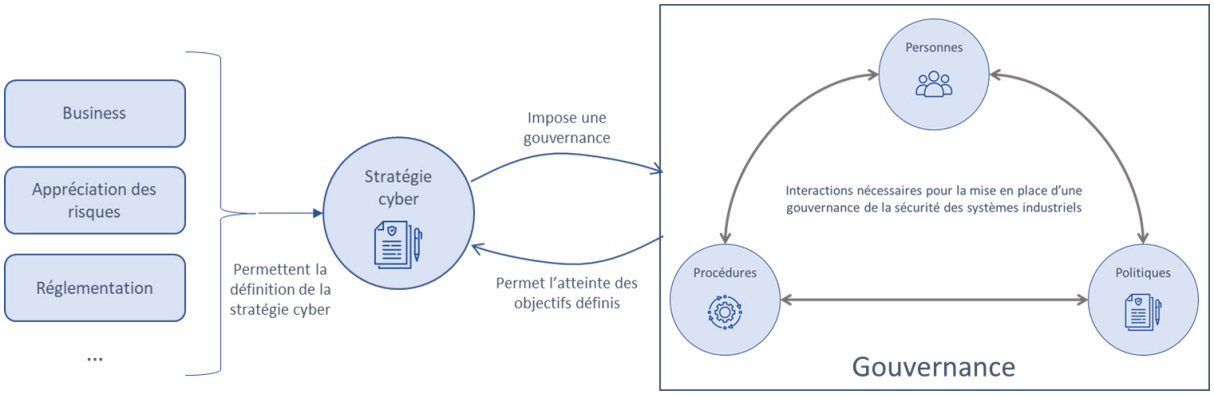
Une attention particulière devra être portée aux documents cités plus haut, mais également à ceux dont la production est recommandée par le présent guide. En effet, ces documents peuvent divulguer des informations pouvant aider des attaquants à la compromission des systèmes industriels. La protection de ces documents doit prendre en compte la sensibilité des informations qu'elles contiennent ainsi que la réglementation en vigueur. L'appréciation des risques permettra d'identifier le niveau de sécurité adéquat.

4 Gouvernance

4.1 Qu'est-ce qu'une gouvernance de la sécurité des systèmes industriels ?

La gouvernance de la sécurité des systèmes industriels consiste en l'organisation des acteurs jouant un rôle dans la sécurité de ces systèmes, afin d'atteindre les objectifs par la stratégie de cybersécurité des systèmes industriels. Cette stratégie est définie par un ensemble de facteurs dont, notamment, les besoins métiers, les risques de cybersécurité ou encore les exigences définies par les réglementations.

Dans le cadre d'une stratégie de sécurité des systèmes industriels, l'organisation de la sécurité des systèmes industriels s'articule autour de la définition de politiques, procédures et acteurs.



Interactions nécessaires pour la mise en place d'une gouvernance de la sécurité des systèmes industriels

4.2 Quel est l'intérêt de mettre en place une gouvernance à la sécurité des systèmes industriels ?

La sécurité des systèmes d'information évolue au cours du temps, selon l'évolution de la menace, des systèmes et de leur niveau de sécurité.

Ainsi, les résultats d'une appréciation des risques effectuée à la conception d'un système ne seront pas identiques lors de la mise en exploitation du système ni au cours de sa durée de vie. Il est important de mettre en place une gouvernance de la sécurité des systèmes d'information afin de garantir une bonne gestion de la sécurité des systèmes.

Les systèmes industriels intègrent de plus en plus des systèmes issus de l'informatique bureautique, mais doivent également répondre à de nouveaux besoins (suivi à distance, interactions multisites, etc.), ce qui augmente leur exposition et les sources de risques. De ce fait, leur sécurité évolue également au cours du temps, et cela, même si les systèmes évoluent peu au cours du temps.

De plus, les systèmes industriels mobilisent différents intervenants qui n'ont pas tous des connaissances en informatique. Les profils des intervenants évoluent également au cours du temps, les acteurs mobilisés lors de la conception de systèmes n'étant pas les mêmes que ceux chargés de leur exploitation.

Il est ainsi nécessaire de mettre en place une gouvernance de la sécurité des systèmes

industriels qui peut s'adapter aux particularités de ces systèmes.

L'objectif d'une gouvernance de la sécurité des systèmes industriels est de :

- Définir une stratégie de la sécurité des systèmes industriels qui sera validée par le management pour, ensuite, assurer son pilotage avec des moyens techniques, organisationnels et humains ;
- Coordonner l'ensemble des parties prenantes afin de :
  - Identifier les risques ;
  - Protéger les systèmes industriels ;
  - Maintenir les risques à un niveau acceptable ;
  - Détecter les incidents ;
  - Répondre et reconstruire les systèmes en cas d'incident.

4.3 Quel est le périmètre à couvrir par une gouvernance de la sécurité des systèmes industriels ?

La sécurité des systèmes industriels doit s'inscrire au sein d'une gouvernance globale qui couvre l'ensemble des ressources matérielles et humaines des systèmes industriels durant toute leur durée de vie.

La gouvernance doit également couvrir les aspects techniques de la sécurité :

- Les composants matériels ;
- Les composants logiciels.

Mais la gouvernance devra aussi couvrir les personnes et équipes en interaction avec ces systèmes :

- Les équipes informatiques internes ou externes ;
- Les équipes chargées de la sûreté ;
- Les équipes chargées de la maintenance ;
- Les ressources humaines, etc.

L'organisation mise en place devrait aussi intégrer l'évolution des systèmes. La gouvernance devra s'appliquer durant toute la durée de vie des systèmes et des projets (projets de développements de systèmes industriels) : spécification, conception, validation, mise en service, opération, maintenance et fin de vie, en intégrant toutes les évolutions qui peuvent modifier le système durant sa vie.

4.4 Quand faut-il mettre en place une gouvernance de la sécurité des systèmes industriels ?

Comme recommandé par l'ensemble des référentiels d'exigences et guides de bonnes pratiques de sécurité, il est primordial de mettre en place une gouvernance dès la mise en place d'un système industriel. Si le système industriel est en cours d'exploitation mais qu'aucune gouvernance de la sécurité des systèmes industriels n'est mise en place, il est nécessaire de la mettre en place le plus tôt possible.

Il est à noter que la gouvernance évoluera au cours du temps, notamment lorsqu'un nouveau système doit être conçu. Dans ce cas, plusieurs gouvernances devraient cohabiter :

- Une organisation mise en place par le(s) fournisseur(s) afin d'intégrer la sécurité dans le programme de développement (intégration de la sécurité dans la réponse technique et dans la conception) ;
- Une organisation mise en place par le client afin d'établir des exigences de sécurité et préparer l'exploitation sécurisée des systèmes.

4.5 Combien coûte la mise en place d'une gouvernance de la sécurité des systèmes industriels ?

La définition des coûts va naturellement dépendre du contexte (complexité de l'organisation de l'entreprise, du système, maturité, etc.). Sources de dépense pour la mise en place de la gouvernance :

- Recrutement ou formation de personnels ;
- Rédaction des politiques et procédures ;
- Outillage (pilotage projets, KPI, etc.) ;
- Obtention d'une certification si nécessaire ;
- Accompagnement par des prestataires externes dans la mise en œuvre de cette gouvernance.

Il est également nécessaire de définir un budget pour la mise en œuvre de cette gouvernance et des plans d'action qui en découlent :

- Coûts d'investissement ;
- Coûts d'exploitation ou opérationnels (coûts récurrents).

Le budget sera à définir de façon régulière (annuellement, par exemple) et en fonction des contrôles à mettre en place (besoins en audit interne, audit par des prestataires qualifiés, etc.).

4.6 Comment mettre en place une gouvernance de la sécurité des systèmes industriels ?

La mise en place d'une gouvernance de la sécurité des systèmes industriels commence par l'identification d'un sponsor qui nommera un responsable de la sécurité des systèmes industriels.

Le responsable devra comprendre le(s) métier(s) et identifier l'ensemble des réglementations ou normes qui s'appliquent dans le contexte (par exemple : loi de programmation militaire, exigences GxP, décret d'homologation des véhicules automatisés, etc.).

Il sera nécessaire de capitaliser sur la connaissance du métier, afin d'identifier le niveau de criticité des systèmes (identifier leur importance en termes d'impact sur les missions, impacts humains, financiers, environnementaux, etc.). Il est recommandé de compléter ce travail avec une appréciation des risques pour décliner un plan d'action.

Le responsable de la sécurité des systèmes industriels devra par la suite identifier les acteurs intervenants sur les systèmes industriels, les principales parties prenantes internes ou externes (responsable de maintenance, responsable de site, responsable de risques industriels, etc.), les responsables budgétaires et les responsables achat. L'objectif de cette étape est d'assimiler l'organisation actuelle et les rôles et responsabilités de chacun afin de mettre en place une organisation de la sécurité qui s'intègre au mieux dans l'organisation et les processus actuels.

Dès lors que le responsable a saisi le contexte et identifié les parties prenantes, il peut être possible, pour les plus petites structures, de lancer une gouvernance de la sécurité. Par exemple, pour les plus petits sites industriels, le responsable pourrait de façon régulière (semestrielle, annuelle) évoquer le sujet de la sécurité des systèmes industriels avec les parties prenantes et identifier les éléments déjà mis en place ou ce qui pourrait être réalisé. La maturité de cette gouvernance évoluera et pourra intégrer les éléments évoqués dans la suite de cette thématique.

Il est recommandé que le responsable définisse ou adapte les politiques et procédures afin d'y intégrer la cybersécurité des systèmes. Afin d'identifier les procédures et politiques à mettre en œuvre, il est recommandé de se reposer sur les référentiels de sécurité, dont, notamment, ceux du NIST, l'IEC 62443, l'ANSSI et l'ISO 27001. Parmi les politiques et procédures qui peuvent être mises en œuvre, il faut évoquer :

- Politique de la sécurité des systèmes d'information (PSSI) ;
- Procédure de maintien en condition de sécurité ;
- Procédure d'intégration de la sécurité dans les projets ;
- Plan d'assurance sécurité ;
- Politique d'exploitation sécurité ;
- etc.

À l'issue, le responsable aura ainsi :

- Saisi le contexte métier et réglementaire dans lequel se trouve le système industriel ;
- Identifié les principales parties prenantes sur le fonctionnement des systèmes ;
- Initié la définition des politiques et procédures.

Comme indiqué dans la partie 1, une gouvernance de la sécurité est l'association d'acteurs, de politiques et de procédures. Le responsable de la sécurité des systèmes est chargé de la mise en marche de cet ensemble. Cependant, il est primordial que le responsable ne soit qu'une partie prenante parmi les autres, et non le seul animateur et responsable de cette gouvernance. En effet, afin que cette gouvernance soit durable, les rôles et responsabilités devront être répartis entre les différentes parties prenantes. Ainsi, il est nécessaire de définir un RACI (Responsable, Acteurs, Consultés et Informés) pour l'ensemble des processus, ainsi que pour le plan d'action de la sécurité des systèmes industriels.

Le choix du sponsor est ici primordial, car c'est lui qui donnera le poids nécessaire au responsable et permettra la bonne implication de l'ensemble des parties prenantes.

En fonction du contexte (typologie et taille du système industriel), les parties prenantes et leurs rôles au sein de l'organisation de la sécurité peuvent varier. Ci-dessous, quelques exemples d'acteurs pouvant être amenés à s'impliquer dans une organisation globale de la sécurité des systèmes industriels :

- Parties prenantes chez l'exploitant ou le client pouvant s'impliquer dans la gouvernance de la sécurité de systèmes industriels en exploitation :
    - Responsable de site[4] : connaissance du métier, des budgets et relations institutionnelles ;
    - Responsable de maintenance et automaticiens : connaissance des automates, des fenêtres de maintenance et souvent premiers contacts en cas d'incident ;
    - Responsable d'exploitation (des opérations) : utilisateurs des systèmes industriels et garant de la bonne exploitation des systèmes ;
    - Travaux neufs : acteurs à mobiliser dans le cas de la conception de nouveaux systèmes industriels ;
    - Responsable de risques industriels et Spécialistes en sûreté de fonctionnement : connaissance des risques industriels – leur vision des impacts humains, environnementaux et sur les biens est essentielle pour l'évaluation des risques dans le cas d'un incident cyber ;
    - Informatique industrielle : en charge de la fourniture des ressources informatiques en contexte industriel, du maintien en condition opérationnelle et en sécurité de ces systèmes ;
    - Informatique bureautique : en charge du maintien en condition opérationnelle et de la sécurité des ressources informatiques bureautiques et interlocuteur privilégié pour intégrer les bonnes pratiques bureautiques en contexte

[4] Ce type d'acteur n'est pas présent en contexte multisite.

industriel ;
    - Responsable qualité et auditeurs en sûreté de fonctionnement[5] : acteurs à mobiliser pour expliciter l'importance de la cybersécurité dans la sûreté de fonctionnement, mais également afin de pérenniser les procédures de maintien en condition de sécurité.
- Les différentes directions à mobiliser en fonction du contexte pour disposer du soutien auprès de l'ensemble des équipes dans la conduite des processus :
    - Direction générale ;
    - Directions industrielles ;
    - Directions des différentes Business Unit ;
    - Direction de maintenance ;
    - Direction d'exploitation ;
    - Direction de la sûreté ;
    - Direction de la sécurité ;
    - Direction des systèmes d'information/usage numérique.
- Autres parties prenantes à mobiliser dans le cas par cas :
    - Responsables juridiques et relations publiques ;
    - Responsables en ressources humaines ;
    - Direction de la communication.
- Parties prenantes chez le fournisseur ou vendeurs pouvant s'impliquer dans la gouvernance de la sécurité de systèmes industriels en conception (pour un ou plusieurs clients) ou réalisation :
    - Architectes : connaissance des solutions et produits conçus ;
    - Responsable R&D : connaissance des nouveaux besoins et des nouveaux produits ;
    - Responsable sécurité des produits : connaissance des mécanismes de sécurité intégrés dans les systèmes et productions ;
    - Marketing : stratégie commerciale pour la vente des produits et des systèmes ;
    - Intégrateur : connaissance des procédures de déploiement et configuration des systèmes et produits ;
    - Responsables production et logistique : responsable de la sécurité de la supply chain. Interlocuteur à privilégier pour s'assurer que les acteurs intervenant dans la fabrication des produits et systèmes prennent en compte les contraintes de sécurité ;
    - Développeurs : chargés du développement des systèmes et produits. Ils sont à mobiliser pour intégrer la sécurité dans le développement des systèmes et produits ;
    - Responsables des services de sécurité : certains services de sécurité peuvent être proposés suite à la vente de produits et systèmes (déploiement de mises à jour, surveillance, etc.). Le responsable est à mobiliser pour s'assurer que les services nécessaires sont mis en place.

Afin de pouvoir définir les rôles et responsabilités entre les différentes parties prenantes (certaines listées ci-dessus), il est recommandé de s'appuyer sur des questions similaires à celles ci-dessous :

- Lors d'un projet de création, modification conséquente, décommissionnement ou démobilisation (dépose) d'un système industriel :
    - Qui aura la responsabilité de la cybersécurité des équipements de support (email, accès aux ressources bureautiques, gestion de la sécurité physique des plateformes de développement et de recette client) ?
    - Qui aura la responsabilité de la cybersécurité liée aux équipements achetés

[5] Principalement dans les domaines ferroviaire, santé et pharmaceutique.

(qualification des composants, SDLC [6]…) ?
    - Qui aura la responsabilité du respect par les sous-traitants des exigences de cybersécurité (cybersécurité de la supply chain) ?
    - Qui aura la responsabilité de la conformité aux exigences réglementaires liées au client final ?
- Lors de la phase d'exploitation d'un système industriel :
    - Qui aura la responsabilité de la cybersécurité des équipements utilisant des produits bureautiques (stations ou serveurs utilisant Windows OS, Oracles, Acrobat Reader…) ou les équipements IT périmétriques utilisés pour accéder aux systèmes industriels (pare-feux, VPN, rebonds, etc.) et de leur maintien en condition de sécurité ?
    - Qui aura la responsabilité de la mise à jour des produits de la partie industrielle ?
    - Qui aura la responsabilité du maintien de la conformité aux exigences réglementaires ?
    - Qui aura la responsabilité des choix opérationnels liés à la sécurité (réaction opérationnelle face à un incident, déploiement de correctifs sur le système, etc.) ?

Enfin, il est nécessaire de mettre en place des mécanismes de contrôle de cette gouvernance. Il conviendra donc de mettre en place des indicateurs (de suivi de risques, de performances, etc.) ainsi que des audits, afin de s'assurer de l'efficacité de l'organisation et des processus.

Les indicateurs seront à adapter en fonction du niveau de maturité cybersécurité, mais également de l'état d'avancement dans le plan de sécurisation des systèmes industriels.

Ci-dessous, des exemples d'indicateurs pouvant être mis en place (il est important de noter qu'ils ne sont donnés qu'à titre indicatif et qu'il est important de les adapter au contexte de l'entreprise) :

- Évolution de l'évaluation des risques à la suite d'une appréciation des risques sur le périmètre ;
- État d'avancement sur le plan d'audit et de contrôle[7] ;
- État de conformité à un référentiel sélectionné (PSSI de la société, ANSSI, IEC 62443, etc.) ;
- État d'avancement dans le plan de sensibilisation ;
- Nombre d'incidents dans l'année ;
- Nombre de violations constatées des règles ou procédures de sécurité ;
- Indicateurs à fournir nécessairement dans le cadre d'une réglementation (par exemple, les indicateurs exigés par la loi de programmation militaire).

4.7 Qui est en charge de la mise en place d'une gouvernance de la sécurité des systèmes industriels ?

La gouvernance de la sécurité d'un système industriel est de la responsabilité de son propriétaire. Elle peut être déléguée formellement à son exploitant si celui-ci est différent.

Dans ce cadre, la gouvernance de la sécurité des systèmes industriels est mise en œuvre par différents acteurs de la société responsable. Cependant, un responsable de la sécurité des systèmes industriels doit être désigné afin d'animer cette organisation. Ce dernier devra être soutenu par un sponsor, qui sera le garant de la mise à disposition des ressources humaines

[6] Cycle de développement - Software Development Life Cycle.

[7] Voir la thématique Audit Cybersécurité.

et matérielles nécessaires pour l'atteinte des objectifs de sécurité.

Le responsable de la sécurité des systèmes industriels doit avoir une connaissance de la sécurité informatique, mais également de l'informatique industrielle. Ainsi, il est possible d'attribuer ce rôle à un connaisseur de l'informatique sensibilisé au contexte industriel. Il est également possible de l'attribuer à un connaisseur des processus industriels (responsable exploitation ou maintenance, par exemple) formé à l'informatique et à la sécurité informatique. En fonction du profil sélectionné, le responsable pourra être épaulé par un autre acteur avec qui les responsabilités seront partagées.

De plus, en fonction de la taille du site et des systèmes industriels, il pourra être nécessaire de mettre en place plusieurs responsables sécurité des systèmes industriels (par exemple, un responsable par site industriel, un responsable par plaque géographique, un responsable par type de système, etc.). Cependant, afin d'assurer une cohérence, une efficacité et un suivi global du niveau de sécurité, il est nécessaire qu'un responsable soit identifié à la tête de ce dispositif.

Plusieurs types d'organisations de la sécurité des systèmes industriels existent, par exemple :

- Un responsable par site reportant au responsable régional ;
- Un responsable par plaque géographique répondant au responsable sécurité industrielle qui reporte au responsable sécurité des systèmes d'information ;
- Un responsable de la sécurité des systèmes industriels sous la responsabilité directe du directeur des systèmes d'information ou du directeur administratif et financier ;
- Un responsable de la sécurité des systèmes industriels sous la responsabilité du responsable de maintenance.

Il est impossible de recommander une organisation en particulier, tant les contextes sont différents. Il peut exister des conflits d'intérêts entre les parties prenantes, par exemple entre la cybersécurité et les opérationnels en charge de l'exploitation. Il est important, dans le cas de conflits entre différentes directions, de mobiliser la hiérarchie et notamment le sponsor, à des fins d'arbitrage.

L'essentiel préalable à toute nouvelle gouvernance est de bien assimiler l'organisation actuelle et de s'y intégrer fonctionnellement, afin de bénéficier des synergies existantes en lien avec la stratégie de l'entreprise.

5 Inventaire et cartographie

5.1 Que signifie « inventaire et cartographie » ?

5.1.1 Inventaire

D'une manière générale, un inventaire consiste en une revue détaillée, minutieuse, d'éléments sur le périmètre considéré.

Dans le contexte de la cybersécurité d'un système industriel, l'inventaire donne la liste des équipements communicants, comme les automates, les postes de travail, les stations opérateurs ou les routeurs.

Pour chacun de ces éléments, l'inventaire apportera un ensemble de données et de métadonnées permettant de les caractériser et de les identifier, par exemple, le modèle, la référence, la version logicielle ou la localisation géographique.

5.1.2 Cartographie

De manière générale, le terme « cartographie » désigne une représentation schématique d'un ensemble d'informations et de systèmes permettant de disposer d'une vision synthétique d'une installation localisée ou répartie. Les informations représentées sont choisies de façon pertinente pour répondre efficacement à une ou des questions posées.

Dans le contexte de la cybersécurité d'un système industriel, la cartographie permet de représenter le système d'information d'un organisme, ainsi que ses connexions internes et avec l'extérieur. Cette représentation peut être plus ou moins détaillée, soit :

- Représentative d'une unité, dans le cas d'un système similaire distribué ;
- Exhaustive, en incluant par exemple les biens matériels, logiciels, les réseaux de connexion, mais aussi les informations, activités et processus qui reposent sur ces biens.

La cartographie peut inclure d'une façon spécifique (par exemple en pointillés ou dans une couleur différente bien identifiée) des évolutions prévues, de manière à permettre aux différents utilisateurs de l'information d'anticiper ces évolutions.

La cartographie et l'inventaire sont, par définition, liés : la cartographie représente ainsi les flux et les positions physiques d'éléments ou de groupes d'éléments de l'inventaire.

5.2 Quel est l'intérêt de réaliser un inventaire et une cartographie des systèmes industriels ?

La cartographie permet les analyses, les modifications en limitant les risques, la détection d'anomalies et les actions correctives. Une cartographie et un inventaire à jour permettent aux parties prenantes d'exercer leurs activités plus efficacement.

Le temps consacré à la cartographie est ainsi compensé par celui économisé, notamment grâce à l'évitement d'incidents, dans les domaines d'activité où elle s'applique :

- Activités de maintenance :
    - Préventive : grâce à la centralisation des informations de version des équipements industriels, par exemple, les cas d'obsolescence ;
    - Curative ou corrective : en permettant de localiser rapidement et d'évaluer les impacts des interventions ;

    - Prédictive : remontée des données en temps réel pour anticiper et prévenir les pannes d'équipements.
- Nouveaux projets ou évolutions : une cartographie à jour permet de prévoir une intégration de nouveaux systèmes à l'existant. L'évolution peut être étudiée avant l'installation pour permettre aux autres acteurs de l'anticiper ;
- Informatique et réseau : l'exploitant a besoin d'une représentation du système pour gérer les flux, les équipements et les incidents, a fortiori si la gestion se fait à distance, par une infogérance, par exemple ;
- Maintien en conditions opérationnelles : les régleurs, opérateurs, bureaux d'études peuvent accéder aux informations d'inventaire et de cartographie pour identifier et localiser les systèmes, leurs caractéristiques et leurs propriétaires, dans le cadre de leur activité.

Concernant la cybersécurité, de nombreuses activités, précisées ci-dessous, nécessitent une représentation détaillée et fiable du périmètre considéré.

5.2.1 Intérêt de l'inventaire pour la cybersécurité

Les apports de l'inventaire aux fins de cybersécurité peuvent se classer ainsi :

- Prévenir :
    - Répertorier les vulnérabilités, traiter les alertes d'un CERT ;
    - Gérer l'obsolescence et les vulnérabilités grâce à la connaissance des versions des firmwares et des matériels des différents équipements pour planifier leurs mises à jour ;
    - Disposer d'équipements de remplacement (spares utilisés dans le cadre de PRA).
- Détecter :
    - Les équipements non identifiés ;
    - Les disparitions d'équipements ;
    - Les modifications de configuration, de logiciel et de matériel.
- Réagir :
    - Connaître l'administrateur de l'équipement ;
    - Connaître la criticité ou fonction d'un équipement (est-ce possible de le déconnecter ? quel en serait l'impact ?).

En environnement industriel, ces informations sont le plus souvent dispersées, obsolètes ou incomplètes (plusieurs fichiers Excel, dossiers fournis à la livraison d'un atelier) et les mises à jour de ces informations répondent aux seuls besoins de comptabilité (actifs et amortissements) et de maintenance, quelquefois d'infogérance si la gestion et la maintenance d'une partie sont externalisées.

Il faut donc à la fois consolider et vérifier les informations, mais aussi initier des projets permettant de garder les informations à jour.

5.2.2 Intérêt de la cartographie pour la cybersécurité

La cartographie fait le lien entre les différents équipements de l'inventaire, l'environnement physique et les systèmes externes. Différents types de flux doivent être renseignés. Comme l'inventaire, la cartographie est indispensable pour de nombreux objectifs de cybersécurité et présente souvent initialement les mêmes lacunes que les inventaires : partielle, non fiable, non tenue à jour. On visera donc à ce qu'elle soit le plus à jour possible.

Les apports de la cartographie aux fins de cybersécurité peuvent se classer ainsi :

- Prévenir :
  - Indispensable pour l'analyse de risques cybersécurité ;
  - Nécessaire pour établir un PCA/PRA.
- Détecter :
  - Nécessaire pour la détection d'intrusion et d'anomalies.
- Réagir :
  - Nécessaire pour contextualiser un événement de sécurité (impacts, criticité, localisation physique…) et pour l'investigation numérique ;
  - Un support pour la remédiation, notamment pour savoir ce qu'on peut déconnecter.

De plus, la cartographie incluant la sécurité physique (périmètres, contrôles d'accès, armoires fermant à clé) est importante, car :

- Les équipements sont souvent plus vulnérables aux attaques physiques (par exemple, accès en face avant des automates, sites accessibles au public et peu sécurisés) : la cartographie permet d'identifier qui peut y accéder ;
- La sécurité physique permet souvent de pallier une absence de sécurité logique (par exemple, les mesures de protection des personnes et des biens contribuent à la cybersécurité).

5.3 Quel est le périmètre à couvrir en réalisant un inventaire et une cartographie ?

Au même titre qu'un système d'information, le périmètre d'un système industriel ou d'un système d'information incluant un sous-système industriel couvert par la cartographie doit répondre à l'objectif ou aux objectifs préalablement définis. De même que dans le cas d'un système d'information, les systèmes industriels les plus exposés ou les plus critiques doivent être cartographiés.

Cependant, à la différence des systèmes d'information, la notion de « périmètre physique » est cruciale dans la mesure où, par nature, le processus métier ou industriel (par exemple, la production et la distribution d'eau potable) est ici physique.

Les informations pertinentes d'un système industriel sont multiples et variées : elles concernent les biens physiques, tels que les automates industriels, les processus métier ou encore les flux de matière.

Ces informations peuvent reposer sur des systèmes ou sous-systèmes divers, tels que des usines ou des sous-stations, pouvant être localisés sur une zone géographique étendue (par exemple, les réseaux électriques ou le réseau des voies ferrées) et dont les interconnexions peuvent être facilement accessibles (comme dans le cas d'un réseau de téléphonie mobile, d'un réseau sans fil ou d'une armoire sur le domaine public).

L'ensemble de l'information paraît donc difficile à modéliser sur un même schéma, compte tenu de la complexité et du caractère protéiforme de cette information. Une représentation permettant de rassembler les informations de même nature et avec un niveau de détail suffisant en fonction de l'objectif doit ainsi être privilégiée.

Une représentation mentionnant la localisation géographique des équipements permet, par

exemple, de réagir à une indisponibilité géographiquement localisée (tempête, inondation, etc.) ou à une compromission consécutive à une intrusion physique.

Une cartographie par vision (visions métier, applicative et infrastructure) et par vue (une vue pour la vision infrastructure, une autre pour les infrastructures logiques et une troisième pour les infrastructures physiques) et un inventaire sous forme de liste d'éléments (ou d'objets) avec attributs proposés par le guide *Cartographie du système d'information*[8] de l'ANSSI sont envisageables. Dans un contexte industriel, des vues supplémentaires peuvent compléter cette représentation (par exemple, une vue « zone » au sens ISA/IEC 62 443) avec des équipements qui ont le même besoin en termes de sécurité, ou des vues en cohérence avec le modèle en couches CIM et qui permettent de structurer la cartographie. De même, de nouveaux objets ou attributs sont à ajouter à l'inventaire pour représenter, par exemple, les flux de matière, la redondance, les chemins alternatifs ou le sens d'initiation de la communication.

Dans le cas de sous-systèmes identiques et multiples, tels que les sous-stations des réseaux de distribution, une représentation générique peut être souhaitable avec l'usage de notation adaptée (par exemple, la vue unitaire N représentant les sous-systèmes notés N_1 à N_{300}).

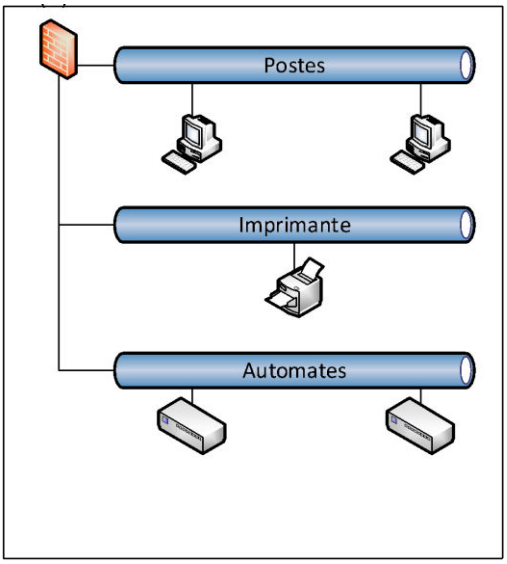


Figure 2. Représentation générique unitaire

L'énumération des éléments de ces sous-systèmes avec leurs caractéristiques devra néanmoins être faite dans l'inventaire.

[8] Cartographie du système d'information sur https://www.ssi.gouv.fr/guide/cartographie-du-systeme-dinformation/

5.4 Quand est-il recommandé de réaliser un inventaire et une cartographie ?

5.4.1 Projet de sécurisation pour une installation existante

Pour la plupart des installations en exploitation, un projet de consolidation et de vérification des inventaires et cartographies doit être réalisé comme première étape d'un projet de sécurisation avant de mener des analyses de risques et, a fortiori, de mettre en place des mesures de sécurité.

Pour l'établissement d'un inventaire et d'une cartographie initiale, il peut être nécessaire de procéder par étape, en priorité aux périmètres dont les enjeux de sécurité sont les plus élevés.

Ceci permet aussi d'établir un programme global, avec des équipes dédiées pour chaque étape (inventaire et cartographie, analyse de risques, sécurisation des flux, mises à jour des procédures…) et avec une séquence des activités sur les différents périmètres.

Peuvent ensuite être finalisés l'inventaire détaillé, puis la cartographie, qui positionne les différents liens logiques et flux entre les éléments de l'inventaire.

Dès qu'un périmètre a été traité, cette activité doit être systématiquement intégrée à tout nouveau projet, interne ou livré par ensemblier ou intégrateur : les dossiers de livraison doivent comprendre une cartographie et un inventaire selon le niveau de détail indiqué dans ce document, car les tests de recette attendent ces documents en entrée (voir la partie « Intégration et recette de cybersécurité »).

5.4.2 Conception d'un nouveau système

Des éléments de cartographie et d'inventaire doivent être fournis naturellement au cours du projet : documents d'architecture, analyse fonctionnelle et liste de matériels.

Il faudra s'appuyer sur ces éléments pour finaliser l'inventaire et la cartographie de l'ensemble du système industriel après l'intégration, de manière à disposer des informations lors de la recette.

5.4.3 Maintien à jour

Une fois réalisés, l'inventaire et la cartographie devraient être mis à jour en permanence, en intégrant cette activité d'actualisation dans les différents processus métier, ceci en impliquant les parties prenantes. Il s'agit là d'un enjeu de cybersécurité (capacité à analyser et à réagir de manière pertinente), mais aussi économique, comme expliqué au chapitre suivant.

L'intégration aux processus de maintenance (fiches d'interventions, autorisations de travail…) permet de conserver les informations à jour lors des évolutions normales et des arrêts de maintenance.

5.4.4 Audit et vérification

Enfin, il reste nécessaire de procéder à des opérations régulières de vérification des inventaires et des cartographies pour corriger d'éventuelles erreurs, anomalies et obsolescences. Ces vérifications peuvent être réalisées annuellement ou en fin de chaque période de maintenance, ou par l'utilisation de moyens de détection rapide des anomalies les plus flagrantes (connexion d'un équipement non autorisé, activité anormale d'un équipement).

5.5 Quel est le coût de réalisation d'un inventaire et une cartographie ?

5.5.1 Outils

5.5.1.1 Outils de collecte automatisée des données

Le volume de données des inventaires (souvent des milliers d'équipements connectés) et les flux en découlant posent souvent des problèmes pratiques de collecte et de consolidation des données. De nombreux acteurs issus du champ de l'audit et des industriels ont développé leurs propres outils, reposant souvent sur de la collecte de trafic de réseau Ethernet avec des scripts permettant de présenter les données dans un format utilisable.

Depuis 2013, une douzaine de startups ont développé des systèmes de détection d'intrusion (N-IDS) qui reposent sur un apprentissage automatique de la configuration du réseau, et permettent également de générer des fichiers d'inventaires et de flux, avec ou sans représentation graphique : certains acteurs du service s'appuient sur ces outils pour réaliser des prestations d'inventaire et de cartographie.

5.5.1.2 Outils de gestion des inventaires et de représentation des cartographies

Selon les cas, des évolutions parfois coûteuses des outils de cartographie peuvent être nécessaires. En effet, ceux disponibles dans le monde informatique bureautique peuvent être incomplets ou inadaptés aux besoins du contexte industriel. Les propriétés attendues sont les suivantes :

- Propriétés attendues d'un outil d'inventaire :
    - Stockage des données ;
    - Importation/exportation des données dans des formats standards ;
    - Mise à jour facile par toutes les parties prenantes ;
    - Personnalisation des champs ;
    - Interconnectable avec d'autres outils (ticketing, etc.) ;
    - Gestion de l'historique.
- Propriétés attendues d'un outil de cartographie :
    - Exportation des données ;
    - Importation des données ;
    - Vues hiérarchiques : permettant dynamiquement la consultation selon plusieurs niveaux de détails (site, bâtiment, zone, etc.) ;
    - Évolution aisée ;
    - Gestion de l'historique.

5.5.2 Inventaire

Si des outils de gestion de parc informatique sont déjà présents, il est possible de les utiliser, notamment pour collecter les informations (outils de gestion des pare-feux ou équipements réseau, par exemple). Il faut alors prévoir un stockage adapté des informations concernant les équipements industriels du fait de leur criticité plus élevée (vulnérabilités, FW…). En particulier, les adresses IP et les versions de firmware et de matériel devraient être stockées avec un niveau de confidentialité adapté.

L'outil le plus fréquemment employé reste la feuille de calcul (type Microsoft Excel®), on trouve quelquefois des bases de données, voire des systèmes CMDB liés à des outils de support (ticketing).

L'utilisation d'outils du marché permet de simplifier la saisie, et surtout les mises à jour : ces saisies sont à inclure dans les contrats liant l'entreprise et son exploitant des systèmes IT et OT.

En termes de budget, cela peut représenter quelques milliers d'euros pour l'utilisation d'un fichier Excel et d'un document Visio, jusqu'à quelques centaines de milliers d'euros pour un outillage complet.

5.5.3 Cartographie

Pour compléter le dispositif, il est en effet opportun de disposer d'un outil de cartographie à couches (architecture fonctionnelle, technique, matrice des flux). La difficulté d'un tel outil réside dans le caractère restreint aux informations. C'est une base partagée par un nombre, en général, assez important d'utilisateurs (architectes, exploitants, équipes du SOC…). Or, l'ensemble des informations constitue une base sensible d'informations. Il faut donc prévoir dès la conception une gestion rigoureuse des accès et un stockage sécurisé. Il faut également sécuriser les accès distants à cette base s'il est souhaité que les intégrateurs renseignent les données des nouveaux systèmes.

Ces étapes initiales peuvent rapidement devenir coûteuses et lourdes à maintenir ; il convient donc de bien identifier les usages, la cible.

Au-delà de certains outils spécialisés, les solutions les plus fréquemment employées pour la cartographie sont Microsoft Visio® ou Microsoft PowerPoint®.

5.5.4 Prestations

Les coûts du maintien à jour des informations peuvent être intégrés dans les phases de projets lors des différentes étapes (architecture, déploiement). Ces coûts ne sont pas neutres, mais il est plus aisé de lisser la charge dans les phases du projet, que de les réaliser a posteriori.

En fonction de l'objectif fixé, des contraintes de délai et des moyens financiers, il sera possible d'envisager :

- Une cartographie et un inventaire de « haut niveau » à affiner dans le temps, permettant un coût initial limité, puis un budget réparti dans le temps ;
- Une réalisation soit en interne soit en externe, sachant que, même réalisées en externe, des ressources internes seront nécessaires pour mener à bien ce projet.

5.6 Comment réaliser un inventaire et une cartographie ?

Élaborer une cartographie et réaliser un inventaire d'un système industriel sont des projets d'envergure dont l'un des principaux facteurs de réussite réside, au même titre que pour un système d'information, dans le caractère incrémental de la démarche. Les systèmes industriels étant souvent assez vastes et peu centralisés, la construction de la cartographie et de l'inventaire en partant d'une vue générale du système qui s'affine de manière itérative est parfois plus appropriée.

De plus, cette démarche permet de prévoir, dès le début, les évolutions des systèmes et éventuellement des flux qui nécessitent généralement de mettre à jour la cartographie et l'inventaire. Dès lors, des mesures organisationnelles doivent être mises en œuvre pour inclure la mise à jour de ces documents par toutes les parties prenantes. En effet, certaines mises à jour peuvent être décidées localement ou réalisées par un prestataire externe.

La construction de la cartographie et de l'inventaire nécessite la collecte des informations à partir des diverses sources documentaires (actifs financiers du service de comptabilité, contrat de maintenance des équipements, etc.) et d'outils d'analyse de flux réseau actifs ou passifs dédiés ou non.

Les informations constituant l'inventaire devraient inclure a minima les éléments d'inventaire suivants :

- Numéro d'actif si enregistré (amortissements) ou toute autre référence unique ;
- Type d'équipement (serveur, station, HMI, automate, RTU, commutateur, etc.) ;
- Niveau de criticité de l'équipement (classification, niveau ou degrés de sécurité, etc.) ;
- Nom ou noms (nom commun, nom Netbios, etc.) de l'équipement, avec, le cas échéant, son adresse MAC, son adresse IP, etc. ;
- Marque, modèle ou référence constructeur ;
- Propriétaire ou service responsable ;
- Version de l'équipement ;
- Version du firmware, et éventuellement sa version matérielle ;
- Caractéristiques matérielles (options, RAM, CPU, etc.) ;
- Emplacement physique ou géographique (bâtiment, salle, cabinet, emplacement, etc.).
- Mainteneur, interne ou externe.

D'autres informations peuvent être répertoriées, soit dans la même base d'information, soit dans des systèmes liés, par exemple :

- Les fournisseurs et références d'achat ;
- Les obsolescences et remplacements ;
- Les vulnérabilités présentes par rapport à un CERT ou une base interne.

Dans tous les cas, durant toutes ces étapes, plusieurs réunions ou groupes de travail seront organisés avec tout ou partie des acteurs (voir paragraphe « IV.7 Qui est en charge de la réalisation de l'inventaire et la cartographie ? »). Des audits réguliers et outillés seront nécessaires pour garantir l'exactitude des informations et éventuellement corriger les écarts.

De plus, il est recommandé que cette base ne soit pas stockée sur le système qu'elle représente, afin que, d'une part, en cas de compromission du système, celle-ci ne soit pas disponible à l'attaquant, et que, d'autre part, en cas d'indisponibilité du système, les informations qu'elle contient restent disponibles aux équipes de remédiation.

5.7 Qui est en charge de la réalisation de l'inventaire et de la cartographie ?

Il existe plusieurs acteurs qui pourront être des contributeurs ou des consommateurs de la cartographie et de l'inventaire. Chacun de ces acteurs pourra, le cas échéant, participer à l'élaboration et à la mise à jour de la cartographie et de l'inventaire.

Il est possible de distinguer plusieurs profils d'acteurs :

- Les fournisseurs de solutions (équipementiers, logiciels, etc.), qui pourront livrer les détails des différents composants de l'inventaire (version, référence, numéro de série…) et les flux de communications entrants et sortants ;
- Les intégrateurs et ensembliers, qui fournissent un système constitué d'un ensemble de solutions matérielles et logicielles identifiées et documentées ;
- L'exploitant ;
- Le maître d'ouvrage ;
- Le responsable de la sécurité du système, qui s'assure de l'exactitude des données avant la recette ;
- L'acteur de la maintenance en conditions de sécurité ;
- L'acteur de la maintenance en condition opérationnelle (pouvant être commun avec l'acteur précédent) ;
- etc.

Parmi l'ensemble des acteurs intervenant sur la cartographie et l'inventaire, il est nécessaire de pouvoir identifier un ou plusieurs individus responsables de leur mise à disposition et de leur mise à jour.

6 Appréciation des risques cyber

6.1 Que signifie une « appréciation des risques » ?

L'appréciation des risques (AR) est l'étape clé du processus de gestion des risques d'un système d'information (SI) industriel. L'AR peut être réalisée dès qu'une connaissance suffisante du périmètre à sécuriser est obtenue (cartographie, inventaire) pour un système existant, ou que des études suffisamment détaillées ont été menées (type d'architecture, fonctions, systèmes) pour les nouveaux projets. Ce chapitre du guide a pour objet d'aider à choisir l'approche la plus pertinente, à comprendre les facteurs clés de succès et à connaître les principales étapes et points clés d'une AR. Cette thématique s'adresse aux acteurs de l'industrie souhaitant comprendre l'intérêt et la manière de réaliser des AR en cybersécurité dans le domaine des SI industriels et urbains. Il est supposé que le lecteur ait une connaissance des méthodes d'analyse de risques en général (par exemple, en safety).

La gestion des risques fait l'objet d'une normalisation ISO (ISO 31 000 de façon générique, ISO/IEC 27 005 concernant spécifiquement la sécurité de l'information).

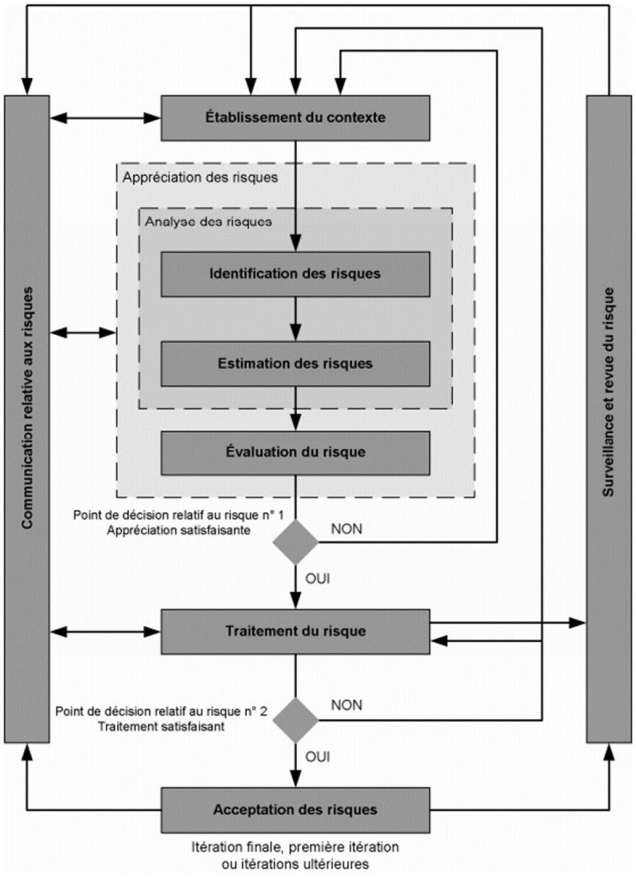


Figure 3. Schéma représentant un processus d'AR extrait de la norme ISO 27005

Pour la conduite de l'AR, il est recommandé d'utiliser ou de s'inspirer d'une méthode, telle que EBIOS (v2010) ou EBIOS Risk Manager (développée par l'ANSSI et supportée par le Club EBIOS).

Quand il s'agit de traiter les risques sur un périmètre, il est possible de distinguer deux approches :

- L'approche consistant à prendre en compte les risques identifiés dans une AR et à appliquer une méthode de gestion des risques pour définir des mesures à mettre en œuvre ;
- L'approche consistant à appliquer un ensemble de mesures prédéfinies par un ou plusieurs référentiels donnés.

En effet, une approche alternative à l'AR pour spécifier les mesures de sécurité consiste à se mettre en conformité avec un référentiel faisant office de catalogue de mesures organisationnelles et/ou techniques (ou check-list de bonnes pratiques). Par exemple, en Amérique de Nord, NERC CIP doit être appliqué avec l'ensemble des mesures à tous les actifs des systèmes de production ou de distribution électrique à partir d'une puissance donnée.

Chaque approche présente des avantages et inconvénients, mais en résumé :

- L'approche par conformité à un catalogue de mesures a pour :
    - Principaux avantages : standardisé, opposable et auditable, raison pour laquelle elle est privilégiée par certains législateurs (NERC CIP, « Mesures détaillées pour SI industriels » de l'ANSSI) ;
    - Principaux inconvénients : les mesures ne sont pas toujours adaptées aux enjeux ou applicables au regard de certaines contraintes opérationnelles, notamment propres au contexte industriel. En appliquant les mêmes mesures à tous les actifs (au sens d'équipements, appelés « actifs supports » dans la norme ISO 27005) du périmètre, certains actifs qui ne supportent pas de données sensibles ou de processus critique risquent d'être « surprotégés », inversement, certains sous-systèmes critiques nécessiteraient des mesures renforcées.
- L'approche par AR a pour objet d'évaluer les risques pesant sur les actifs clés (appelés dans la norme ISO 27 005 « actifs primordiaux » : processus, données…) en identifiant tous les scénarios pertinents, et en estimant leur impact et vraisemblance. Sur la base de ces risques sont identifiées les mesures « strictement nécessaires et suffisantes » pour réduire le risque à un niveau acceptable pour l'organisation :
    - Principal avantage : rationalisation économique des mesures, en les ajustant au mieux aux risques pondérés ;
    - Principaux inconvénients : estimation qualitative du risque et recommandations exprimées à dire d'expert (susceptible de varier d'un expert à l'autre, etc.), complexité de mise en œuvre de la méthode, coût de l'étude elle-même qu'il faut prendre en compte dans l'équation économique globale, et plus grande difficulté à auditer et évaluer la bonne mise en œuvre.

Il est recommandé, pour mener une appréciation des risques, d'identifier un minimum de mesures d'hygiène cybersécurité à mettre en place avant de conduire l'appréciation des risques, comme l'indique par exemple la méthode EBIOS RM. Cette recommandation permettra d'éviter un épuisement dans l'AR évident pouvant être couvert par un ensemble de mesures issues de bonnes pratiques élémentaires. Inversement, certains textes réglementaires (LPM en France, par exemple) demandent qu'une AR soit menée en complément de l'application des mesures exigées dans le texte.

En guise de compromis, des approches hybrides ont été proposées par l'AIEA (NSS #17) ou l'ISA (ISA/IEC 62443). Ces approches consistent à réaliser une étude d'impact sur une zone, un système ou processus, avec éventuellement une approche d'estimation de vraisemblance afin d'en déduire un niveau de cybersécurité cible, puis à appliquer les mesures de sécurité correspondantes. Ce genre d'approche se veut « proportionnée » au risque, car il s'agit d'une combinaison entre :

- Une macro-AR permettant de classifier les actifs, systèmes ou processus selon un « niveau » (ISA/IEC 62443), un « degré » (AIEA, IEC 62645) ou une « classe » (ANSSI) de sécurité (les terminologies sont différentes, mais le concept reste identique) ;
- L'application secondaire de mesures selon le « niveau », « degré », « classe », avec des exigences graduées en fonction du risque pondéré par la vraisemblance d'une cyberattaque (compte tenu du niveau d'exposition à la menace pressentie).

Quel est l'intérêt de réaliser une appréciation des risques ?

6.2 Quel est l'intérêt de réaliser une appréciation des risques ?

Les différents cas d'usage pour réaliser une AR sont :

- AR rétroactive : réaliser une AR sur des systèmes existants dans le but de :
  - Réaliser une rétro-homologation d'un système (ex. : SIIV) ;
  - Identifier, évaluer et mettre sous contrôle les principaux risques ;
  - Établir les priorités du plan de traitement du risque (quel système, quel site, quelle mesure… ?) ;
  - Sensibiliser la direction et les métiers afin d'obtenir des moyens d'action ;
  - Établir les priorités dans la mise en œuvre de la sécurité.
- AR préalable : réaliser une AR dès la conception d'un nouveau système en projet dans le but de :
  - Définir les besoins, objectifs et exigences de cybersécurité selon une approche by design ;
  - Anticiper et prévenir les risques ;
  - Sensibiliser les parties prenantes du projet ;
  - Formaliser les exigences de cybersécurité en interne et les contractualiser en externe auprès des soumissionnaires et partenaires (industriels, sous-traitants, prestataires) avec obligations de diligence et d'« auditabilité » à la clé.

6.3 Quel est le périmètre à couvrir lors de la réalisation d'une appréciation des risques ?

Les différents éléments du périmètre sont :

- Champ d'application de l'AR (champ « horizontal ») :
  - Il s'agira d'identifier le périmètre par lequel initier l'AR dans le système étendu ou complexe. En se basant sur une cartographie des systèmes et des sites, il conviendra de commencer l'AR par les systèmes les plus sensibles (au regard des enjeux et des impacts potentiels en cas d'incident de sécurité majeur) selon un système de classification établi (ex. : SIIV LPM, systèmes sensibles II901, classification selon le document ANSSI éponyme…) ou à définir en interne.
- Profondeur de l'AR (champ « vertical ») :
  - Analyse simplifiée : il s'agira de privilégier ce type d'analyse pour des systèmes estimés peu sensibles ou dont la sécurité est peu mature, afin de ne pas perdre des ressources dans la définition de mesures de sécurité poussées tandis que les bonnes pratiques ne sont pas mises en place ;
  - Analyse approfondie : il s'agira de privilégier ce type d'analyse pour les

systèmes dits sensibles (a fortiori si SIIV).

6.4 Quand est-il recommandé de réaliser une appréciation des risques ?

Idéalement, l'AR doit être menée le plus en amont possible, c.-à-d. dès l'expression des besoins d'un nouveau système, afin de pouvoir déterminer les exigences de sécurité et les principaux risques auxquels il sera confronté. Il est nécessaire que les principes d'architecture soient connus. Ainsi, une cartographie la plus à jour possible est nécessaire (voir le chapitre « Inventaire et cartographie »). Si la cartographie disponible est trop grossière ou non fiable, une macro-AR (comme indiqué dans le chapitre « Que signifie une "appréciation des risques" ? ») peut être utile. Dans tous les cas, il faut éviter de faire une AR détaillée qui sera erronée.

Il est cependant préférable de réaliser une analyse de risques après que les bonnes pratiques ou le guide d'hygiène informatique de l'ANSSI ont été appliqués (ou en anticipant l'application des mesures correspondantes), ceci pour des raisons d'efficacité, à l'instar des méthodes hybrides évoquées précédemment.

6.4.1 Cas des périmètres concernés par des analyses de risques de safety

Les analyses des risques industriels (AMDEC, par exemple) consistent à évaluer le risque que fait peser l'installation industrielle aux personnes, à l'environnement et aux biens en cas de défaillance ou d'erreur. Ces approches, bien antérieures aux appréciations de risques de cybersécurité, sont exigées par les autorités avant de pouvoir exploiter des installations dangereuses, comme celles classées Seveso.

Se pose alors la question de l'articulation entre les deux approches, sachant qu'il n'y a pas encore de méthode d'analyse combinée safety-cybersecurity (il est précisé dans le chapitre « Intégration et recette de cybersécurité » que le même problème se pose au moment des tests). Le consensus (au moins au sein du Clusif) est que :

- Les analyses de risques safety précèdent en général les AR en cybersécurité, ceci principalement afin que l'AR cybersécurité puisse identifier les risques sur les mesures de sécurité dégagées par l'AR safety. En effet, ces systèmes pouvant être des cibles d'attaques informatiques, il est important de pouvoir identifier ce type de risques ;
- Néanmoins, des macro-AR de cybersécurité sont pertinentes à réaliser en phase amont (avant analyse safety) pour définir certains principes d'architecture et choix de solutions, qui, s'ils ne sont pas respectés, rendront difficile la sécurisation d'un point de vue cybersécurité du périmètre. Par exemple :
    - Le principe d'isolation dans des zones distinctes entre automates de pilotage et automates de safety, qui n'est pas toujours indispensable pour la safety, est incontournable en cybersécurité ;
    - Le principe de redondance (systèmes 2 out of 3, etc.), qui permet d'atteindre des niveaux élevés d'exigence safety, n'est utile, en termes de cybersécurité, que si un minimum de cloisonnement ou de surveillance est mis en œuvre ;
    - Les solutions de sécurité apportant de la diversité (différents matériels ou logiciels exécutant les fonctions de sécurité) sont également un plus en matière de cybersécurité.

De ce principe de safety first, il résulte qu'il est possible que les AR de cybersécurité remettent en cause des choix effectués, qui, s'ils concernent des systèmes de safety, peuvent engendrer un besoin de revoir certaines études. Ce risque peut être limité si un dialogue existe entre les fonctions safety et cybersécurité, avec connaissance minimale des disciplines réciproques.

Des arbitrages ou des adaptations sont parfois nécessaires lorsque le traitement des risques

de cybersécurité s'oppose à la sûreté de fonctionnement (par exemple, la porte coupe-feu qui devrait rester fermée mais qui devra plutôt être surveillée).

6.4.2 Motifs de révision de l'AR d'un système :

L'AR doit être reconduite ou mise à jour régulièrement. En général, en environnement informatique, il est recommandé de réaliser une revue tous les ans. Il est fréquent que la période soit plus longue (deux ou trois ans) en environnement industriel. Il faut que l'appréciation des risques soit réexaminée même si le système n'évolue pas.
A fortiori, l'AR est à remettre à jour en cas d'évolution des principaux paramètres. Voici les critères pour revoir l'AR, en dehors de la revue programmée :

- Évolution majeure du système (système de nouvelle génération, extension géographique, nouvelle interconnexion externe, ajout de nouveaux composants et/ou fonctionnalités…) ;
- Évolution significative de la menace (nouvelles techniques ou vecteurs d'attaque, organisme faisant potentiellement l'objet d'une menace ciblée…) ;
- Évolution des vulnérabilités (publication de failles de sécurité applicables au périmètre) ;
- Rapports d'audits (constats établissant l'existence de vulnérabilités avérées) ;
- Rapports d'incidents, retours d'expérience (survenance d'incident ou de presque-incident de cybersécurité sur le périmètre ou sur des périmètres internes ou externes comparables) ;
- Évolution de l'écosystème : nouveaux sous-traitants, fournisseurs ;
- Évolution de la réglementation.

6.5 Quel est le coût d'une appréciation des risques ?

Les moyens pour réaliser une AR dépendent de multiples facteurs, comme la complexité du périmètre considéré et son degré de connaissance, la profondeur d'analyse (macro ou détaillée), ou encore la finalité recherchée (approche exhaustive ou spécifique sur certaines menaces). En termes de charge, cela peut aller de quelques jours-hommes (périmètre simple et maîtrisé) à plusieurs dizaines, avec analyse documentaire, entretiens et ateliers à la clé.

Il est possible de prévoir un budget pour acheter ou développer des outils permettant de cadrer les analyses de risques entre périmètres, et d'assurer une cohérence et un suivi dans le temps. Pour une organisation d'une certaine taille, qui, par exemple, veut comparer les résultats d'analyses entre sites, l'achat ou le développement d'un tel outil est fréquent.

6.6 Comment réaliser une appréciation des risques ?

6.6.1 Procéder à un cadrage général

Au début de l'analyse de risques, il faudra établir un référentiel documentaire constitué des documents clés à étudier : référentiels, contexte réglementaire, données d'entrée (cartographie, organisation…).

6.6.1.1 Élaborer une méthode adaptée au contexte

Il convient de s'appuyer sur une méthode en établissant ses propres catalogues (composants, cybermenaces, scénarios de cyberattaque, registre d'exigences…) et en étayant, moyennant des supports méthodologiques et pédagogiques, un outillage (sous tableur ou logiciel spécialisé).

Il est préférable que celle-ci soit compatible avec les autres approches (non-cyber) déjà en

vigueur dans l'entreprise. Il faudra donc s'approprier et enrichir les grilles d'échelle d'impact en ajoutant par exemple la perte de production aux impacts sur les personnes et environnement.

De plus, il est important d'établir un vocabulaire réfléchi avec les analyses de risques safety (AMDEC, HAZOP, etc.) ou les métriques déjà en vigueur au sein de la direction des risques.

Des termes sont définis ou utilisés différemment entre safety et cybersécurité (événement redouté, sécurité, probabilité…), il faut soit expliciter les différences, soit changer de vocabulaire (vraisemblance versus probabilité, par exemple).

6.6.1.2 Choisir la bonne granularité de l'analyse

La granularité de l'analyse est clé, qu'elle soit basée sur une méthodologie externe ou propre à l'entreprise.

En général, en environnement industriel, il est rarement possible d'obtenir le même niveau de détail que lors d'études portant sur un périmètre en informatique de gestion. En effet, il est compliqué d'étudier chaque vulnérabilité pour chaque actif support, car les deux sont trop nombreux et variés.

Il pourra cependant être envisagé la réalisation d'une analyse détaillée sur un équipement industriel, en particulier quand celui-ci va être produit en grand nombre (systèmes embarqués de signalisation ferroviaire, par exemple).

Il conviendra de travailler au niveau des ensembles de composants, systèmes, voire fonctions. De plus, pour les analyses prospectives, il sera nécessaire de s'intégrer dans le cycle de vie du projet (engineering) :

- À l'issue de l'expression des besoins : il s'agira d'une analyse simplifiée ;
- À la rédaction du dossier d'architecture : il pourra s'agir d'une analyse approfondie.

6.6.2 Étude du contexte

Le contexte dans lequel l'appréciation du risque sera conduite devra également être étudié. Il faudra ainsi procéder à l'établissement :

- Du cadre lié au projet et/ou à l'activité considérée ;
- Du cadre légal et réglementaire (ex. : LPM/NIS, II901…) ;
- Du cadre normatif (normes sectorielles : sûreté nucléaire, IEC 62351, nouvelles réglementations ferroviaires…) ;
- Du référentiel de risques (critères, métriques…). Il s'agira de reprendre et, le cas échéant, d'adapter ou de compléter les critères et métriques en vigueur au sein de l'organisme (cf. fonction gestion des risques ou audit interne, selon organigramme).

6.6.3 Appréciation du risque

Il est capital de mener une étude avec le bon degré d'analyse, suffisamment fine pour ne pas occulter des risques majeurs, suffisamment compréhensible pour être partagée avec les parties prenantes.

Dans ce chapitre seront indiqués les points clés qui doivent être suivis dans toute appréciation des risques, et les choix à faire qui déterminent le degré d'analyse.

6.6.3.1 Établissement des scénarios

Principe d'une appréciation des risques

Le vocabulaire et les définitions varient, mais les points fondamentaux restent les mêmes. Il s'agit d'identifier des « événements » (modification d'une vitesse de rotation…) initiés par des « sources de menaces » (sous-traitants négligents, auteurs de rançongiciels…) et ayant des « impacts » négatifs (ex. : destruction d'une chaîne de production…), avec une certaine « vraisemblance ».

Le risque se définit comme la combinaison d'un niveau d'impact et de vraisemblance de ces événements. Le niveau de risque que l'on accepte permet de définir les risques sur lesquels il faut agir, c.-à-d. ceux qui ne sont pas acceptables pour les décideurs.

Une méthode d'appréciation des risques est utile pour aider à identifier les événements, soit :

- Évaluer leur impact (au regard des conséquences directes et indirectes) ;
- Évaluer leur vraisemblance (au regard des causalités potentielles) ;
- Éventuellement, définir comment traiter ceux dont le risque n'est pas acceptable.

L'objectif de ce document n'est pas de développer et d'expliciter les différentes méthodes permettant d'identifier tous les « événements redoutés». Cependant, il sera envisagé différents facteurs et scénarios :

- **Facteurs :**
  - **Sources de menaces** : personnes malveillantes externes, négligence interne, organisations criminelles crapuleuses… En général, les AR réalisées sur les systèmes industriels se focaliseront sur la malveillance (actions humaines délibérées), éventuellement sur les négligences, car les erreurs et défaillances matérielles sont pour l'essentiel déjà couvertes par la sécurité fonctionnelle. Il est aussi possible d'ajouter des sources de menaces pesant sur l'ensemble d'un site (risque organisationnel ou environnemental, ex. : inondation) ;
  - **Types de menaces** : vol, destruction, modification de matériel, interception de communication, etc. ;
  - **Vulnérabilités** : faiblesse organisationnelle, de personnes, d'équipements, favorisant un événement ;
  - **Scénarios** : combinaison des paramètres ci-dessous conduisant à l'événement.

Exemple de scénario

> **Un stagiaire, un peu « zélé » (non malveillant)**, profite d'un certain **laxisme dans la gestion des droits d'accès à une application, et d'un manque de surveillance de l'activité**, **pour modifier un paramètre de pilotage du procédé industriel**, entraînant des défauts de production (événement redouté).

De plus, il est possible d'agréger plusieurs scénarios en un seul, permettant d'éviter de multiplier les scénarios de risques similaires (par abstraction). Concrètement, l'exercice consiste à :

- Rationaliser les techniques d'attaques voisines sous un terme générique (ex. : code malveillant désignant aussi bien des virus, vers, rançongiciels, logiciels publicitaires…) au sein d'une même causalité ;
- Fusionner les scénarios de menace par rapport à un sous-périmètre ou à une classe commune d'actifs en support (ex. : infrastructure de transmission désignant les équipements réseau et télécom, les médias de transmission…) ;
- Fusionner les scénarios de risques par rapport à des événements redoutés voisins (ex. : compromission de la sécurité des procédés industriels désignant aussi bien une atteinte à la disponibilité qu'à l'intégrité des fonctions en support de ces mêmes procédés).

L'objectif est de garder un esprit de synthèse et de manipuler des objets sur une échelle accessible aux parties prenantes, c.-à-d. en évitant de dépasser la trentaine de scénarios de risques, voire en se focalisant dans un premier temps sur une première vague d'une dizaine de scénarios considérés comme pertinents

L'évaluation du risque va consister à évaluer :

- **D'une part, la vraisemblance du scénario de menace** : combien de stagiaires y a-t-il ? A-t-on des systèmes vulnérables comme indiqué ? Les stagiaires ont-ils un accès physique/logique à la configuration ?
- **D'autre part, l'impact du scénario** : quel est l'impact lié aux défauts de production (coût de remise en état de l'appareil de production, pertes financières dues aux retards de production, atteinte à la confiance des investisseurs, etc.) ?

Les paragraphes suivants visent à détailler ces concepts et aider à choisir les facteurs de risque, métriques d'évaluations, méthodes, bases de connaissances, etc.

6.6.3.2 Échelles d'impact

En cas d'événement de cybersécurité avéré, les impacts peuvent être de différents types : opérationnel (arrêt de production), sécurité des personnes, légal, image, financier, etc.

Il faut, en début, d'analyse définir une échelle d'impact avec plusieurs niveaux, permettant, pour ces différents types d'impacts, d'arriver à une évaluation :

- Quantitative : par exemple, liée à un montant financier, et traduire les impacts safety (blessure, mort…) et arrêts de production en termes financiers, ce qui est généralement possible ;
- Qualitative : utiliser des niveaux « faible », « modéré », « fort », en donnant des exemples pour ces différents paramètres.

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

Figure 4. Exemple d'échelle d'impact (ANSSI - Méthode de classification) — ici sur un seul facteur.

Il faudra veiller autant que possible à la cohérence avec les autres appréciations des risques déjà effectuées : risque de sûreté de fonctionnement (impact-personne et environnement), risques financiers (si une analyse a été faite au niveau de l'équipement industriel).

6.6.3.3 Échelle de vraisemblance

La vraisemblance (terme préféré à celui de « probabilité ») est le paramètre le plus délicat à estimer pour chaque risque avec, en cas de mauvaise évaluation, un risque sous-estimé ou surestimé.

Plusieurs approches peuvent être suivies :

- Évaluation à dire d'expert, donc qualitative par définition ;
- Évaluation par décomposition en variables (comme l'approche ANSSI « Classification ») : « plus on décompose, plus c'est factuel ». Il sera possible de se faire accompagner pour objectiver des paramètres : nombre d'intervenants, ambiance dans l'entreprise ;
- Évaluation par un groupe de travail représentatif.

Il faudra éviter, dans tous les cas, contrairement aux approches de sûreté de fonctionnement, de se baser sur l'expérience passée : le risque cybersécurité sur les systèmes d'information industriels est récent et en augmentation, avec une menace évoluant rapidement.

6.6.3.4 Matrice de risque

Le principe est de combiner vraisemblance et impact pour arriver à un niveau de risque, sachant qu'on aura préalablement décidé du niveau de risque acceptable.

Dans l'exemple simplifié ci-dessous, une échelle de vraisemblance qualitative à trois niveaux, une échelle d'impact à trois niveaux également, et trois niveaux de risque (vert, jaune, rouge) ont été définies comme pour les analyses de risques de sûreté de fonctionnement. Le nombre de degrés des échelles relève d'un libre choix ; il faudra toutefois éviter de multiplier les niveaux en analyse qualitative.

Chaque scénario peut ainsi être mis dans une des cases de la matrice de risques.

Dans l'exemple simplifié ci-dessous :

- Risque vert : accepté (c'est notre « niveau cible de sécurité ») ;
- Risque rouge : inacceptable, à réduire ;
- Risque jaune : à réduire si possible (ALARP de safety), ou à arbitrer en fonction du coût des mesures (décision à prendre par la direction).

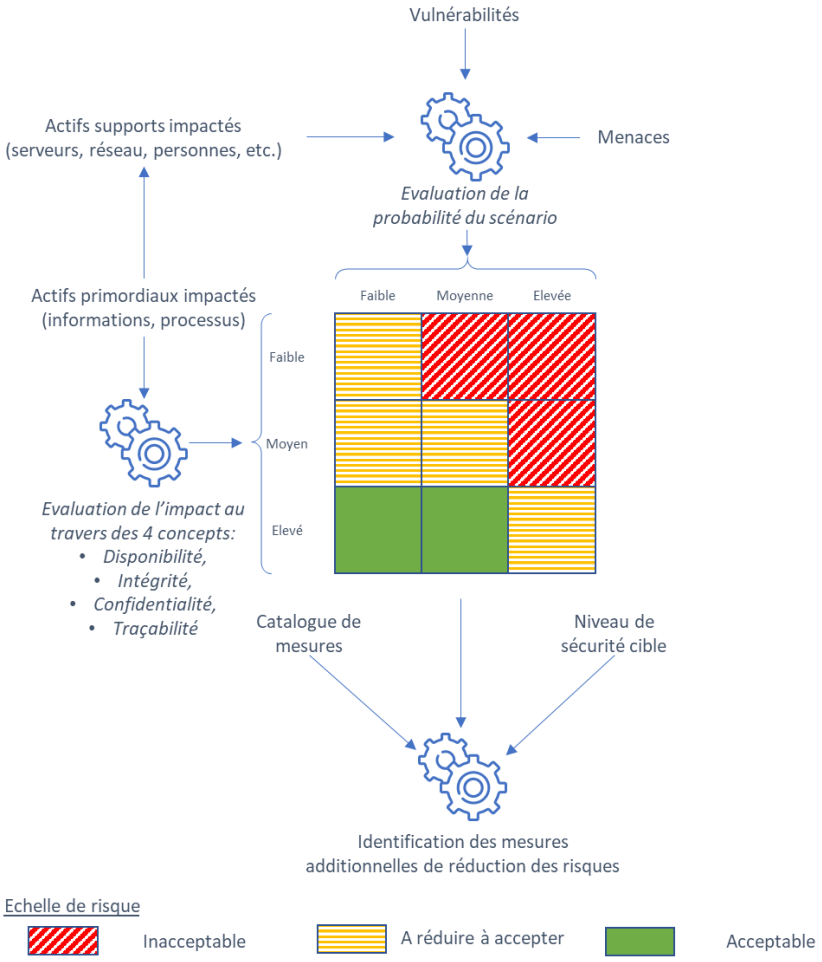


Figure 5. Principes de matrice de risques

6.6.4 Choix de traitement du risque

Pour chaque risque, il faut décider de son traitement :

- Accepter : les risques « verts » ont vocation à être acceptés ;
- Réduire : nécessaire a priori pour les cas rouges, à discuter (ou décider par la direction) pour les risques jaunes, selon le cadrage de l'analyse ;
- Éviter : le risque est supprimé en supprimant l'un des paramètres de l'analyse (par ex. : on ne prend plus de stagiaire, etc.) ;
- Transférer : faire porter le risque par un autre acteur, par infogérance et indicateurs avec pénalités par exemple, ou via une assurance (sans que cela n'affranchisse l'organisation de supporter la majeure partie des impacts opérationnels, juridiques ou réputationnels).

6.6.5 Sélection des mesures/exigences de cybersécurité

Pour les risques (voir la matrice de risques ci-dessus) qui sont jugés « inacceptables » ou pour lesquels il a été décidé de les « réduire », des mesures doivent être mises en œuvre.

Pour choisir les mesures de réduction des risques, il est préférable de s'appuyer sur les standards pertinents (normes internationales type ISA/IEC 62443[9], NIST Cybersecurity framework aux États-Unis, CPNI au Royaume-Uni, guides ANSSI en France, etc.)[10].

Il est ici nécessaire de se rapprocher des interlocuteurs qualifiés (ingénierie sûreté de fonctionnement, responsable PCA, responsable sécurité/sûreté physique, DPO) pour s'assurer de l'adhérence du plan de traitement du risque avec les domaines connexes, tels que :

- La sûreté de fonctionnement ;
- La continuité d'activité ;
- La sûreté des bâtiments (contrôle d'accès, système anti-intrusion, vidéosurveillance, réseaux mobiles privés de type PMR…) ;
- La sécurité physique et environnementale (sécurité électrique, sécurité incendie, dégâts des eaux, chantiers, etc.) ;
- La protection des données à caractère personnel (données usagers, vidéoprotection dans les espaces publics…).

Il convient aussi de s'assurer de la non-redondance des mesures (voire de mesures contradictoires).

Appréciation du coût des mesures : leur mise en place et maintien à niveau

Le coût des mesures doit être évalué en termes de dépenses d'investissement ainsi que d'exploitation (ces dépenses d'exploitation sont nécessaires pour le maintien en conditions de sécurité – cf. chapitre « Maintien en conditions de sécurité »).

À l'issue de l'évaluation du coût des mesures, il est possible d'arbitrer entre les différentes options afin de réduire au maximum le risque avec la combinaison la plus efficace.

Attention à bien prendre en compte le coût du maintien en conditions de sécurité, qui est souvent supérieur en montant actualisé au coût d'investissement.

---

[9] La norme internationale ISA/IEC 62443-3-3 (par ailleurs certifiante) propose un catalogue de sept Foundational Requirements (FR), domaines d'exigences de cybersécurité (sous un angle fonctionnel). À noter que cette norme permet également une approche graduée, sur la base de cinq niveaux de sécurité (Security Levels), qui permet de définir des mesures de sécurité en fonction d'un niveau de menace. L'approche ressemble alors aux classes de sécurité de l'ANSSI (sur trois classes).

[10] Le livrable du GT Cybersécurité des systèmes industriels intitulé Cybersécurité industrielle – Panorama des référentiels présente une analyse des référentiels traitant du sujet.

6.6.6 Risques résiduels

Après l'AR, peuvent subsister des risques dont le niveau se situe au-dessus de la limite fixée pour les risques acceptables mais qui s'avèrent trop coûteux ou trop complexes à réduire, des risques qui sont acceptables à court terme ou des risques incompressibles. Ces risques doivent alors faire l'objet d'une acceptation formelle, éventuellement pour une durée limitée, au titre des risques résiduels.

6.6.7 Rapport et restitution

À l'instar d'un audit, une analyse de risques doit déboucher sur des livrables (rapport, grilles d'analyse pour l'« auditabilité » de la démarche, etc.) et inclure a minima une séance de restitution (prérestitution en cercle restreint, séance plénière auprès d'une audience plus large, etc.) visant à démontrer la rigueur de la démarche employé, la pertinence des résultats obtenus et des recommandations formulées. L'exercice se doit par ailleurs de présenter un caractère hautement pédagogique (notamment face à des parties prenantes ou des arguments contradictoires), avec la prise en compte du contexte et de la culture du risque considérés.

6.6.8 Facteurs clés de succès

Le fait de disposer de l'intégralité des éléments d'analyse et de restitution (au titre de la traçabilité) est généralement apprécié par les commanditaires et contributeurs, car ils leur permettent de mieux s'approprier la démarche et d'être ainsi en mesure de l'exposer aux parties prenantes ou encore de conduire des itérations ultérieures de l'analyse sur le périmètre considéré ou sur d'autres périmètres.

Un autre élément appréciable est de prévoir, à l'attention des décideurs, une synthèse managériale (executive summary) sous la forme d'un support de restitution (par exemple, présentation PowerPoint®) accompagnant le rapport détaillé de l'analyse, visant à restituer les enjeux et les éventuels arbitrages sous un angle le plus compréhensible et percutant (estimation de l'impact financier en cas de concrétisation d'un risque, coût d'une mesure…) pour des décideurs non techniques.

6.7 Qui est en charge de la réalisation de l'appréciation des risques ?

L'AR est une activité par nature collégiale et multidisciplinaire devant impliquer les responsables cybersécurité du périmètre, les responsables métier, le responsable safety (HSE), l'architecte, le responsable d'exploitation, le responsable de maintenance et un animateur expérimenté en analyse de risques dans un contexte industriel, sans oublier la maîtrise d'ouvrage pour sponsoring et approbation.

Les décisions (grille et échelles de risques, niveau de risque accepté, acceptation de risques résiduels…) sont prises in fine par le responsable du périmètre (directeur, ou, par délégation, directeur industriel ou responsable cybersécurité). L'éventuelle délégation sera plus ou moins formelle selon qu'il y a ou non risque de sanction pénale en cas de manquement.

7 Architecture sécurisée

7.1 Que signifie une « architecture sécurisée » ?

Il est entendu par « architecture sécurisée » une architecture fonctionnelle et technique intégrant l'ensemble des principes et dispositifs de sécurité permettant la protection du système industriel des attaques, leur détection, ainsi que le ralentissement de leur propagation.

La construction d'une architecture sécurisée est la définition d'un ensemble de règles régissant l'articulation des composants du système industriel. Parmi les thématiques traitées :

- Les types de flux de communication autorisés et leurs caractéristiques ;
- Les fonctions et mécanismes de sécurité à mettre en place pour le traitement de l'information ;
- Les types d'accès au système industriel (accès physiques et logiques).

Les règles d'architecture sont appliquées sur un système à travers la mise en œuvre de mesures de sécurité.

7.2 Quel est l'intérêt d'une architecture sécurisée ?

La définition d'une architecture sécurisée, notamment via la mise en place des mesures de sécurité qu'elle définit, permet d'assurer une défense en profondeur du système industriel. L'objectif d'une architecture dite « sécurisée » est donc de réduire le risque de la compromission d'un système industriel :

- Une compromission du système industriel en provenance d'une source de menace externe sera plus complexe (particulièrement lors d'attaques ciblées) ;
- Une atteinte à la disponibilité ou à l'intégrité des systèmes pourra être maîtrisée plus rapidement (particulièrement lors d'attaques diffuses).

La définition d'une architecture sécurisée permet aussi de construire les outils et les méthodologies permettant la tenue des opérations industrielles de façon sécurisée, en évitant ainsi que les opérations de maintien en conditions opérationnelles des systèmes industriels ne constituent une source de risque. Par exemple, la mise en place de poste d'administration dédié à l'administration des équipements industriels mis à disposition des fournisseurs permet de réduire le risque de la compromission du système industriel lors d'une opération de maintenance.

Les mesures peuvent aussi compenser en partie une obsolescence possible des systèmes industriels, notamment grâce aux mesures de segmentations. En effet, la durée de vie des systèmes industriels est incompatible avec la durée de vie d'un système informatique standard (des dizaines d'années pour les systèmes industriels contre quelques années pour les systèmes standards). Or, de plus en plus de systèmes industriels intègrent des équipements de l'informatique bureautique standard. Cette différence de durée de vie des systèmes rend très probable une obsolescence des systèmes informatiques standards utilisés dans un contexte industriel. Alors que, dans un contexte d'informatique standard, la mise à niveau des systèmes peut être réalisée avec un impact limité, en milieu industriel une mise à niveau peut s'avérer plus difficile, voire impossible (nécessité de reconstruire une nouvelle ligne d'assemblage, fournisseurs qui n'existent plus, etc.). Afin de pallier les risques induits par cette obsolescence, la mise en place de mesures de sécurité (par exemple, implémentation de système d'autorisation de programmes par liste blanche) permet de réduire (sans le retirer) le risque de compromission de systèmes obsolètes.

7.3 Quel est le périmètre à couvrir par une architecture sécurisée ?

La conception d'une architecture sécurisée devrait concerner un système industriel dans sa globalité, qu'il s'agisse d'un système existant ou d'un nouveau système à concevoir.

L'architecture sécurisée devra traiter de l'ensemble des cas d'usage métier rencontrés (consultation de l'état d'une production, paramétrage, maintenance à distance, etc.) et les potentielles déviances associées.

Parmi les systèmes se trouvant en milieu industriel et pour lesquels une architecture sécurisée doit être conçue, on peut citer :

- Les systèmes industriels de production ;
- Les systèmes de maintenance et/ou de programmation (stations engineering) ;
- Les systèmes instrumentés de sûreté (GTBE, GTBC, GTC...) ;
- Les interconnexions avec les systèmes externes (accès fournisseurs de plus en plus présent, cloud ou autre environnement propre aux problématiques Industrie 4.0 ;
- Les systèmes sans-fils (4G, 5G, wifi, réseaux IoT...).

Il est aussi possible de délimiter les périmètres à traiter via les éléments issus d'une appréciation des risques.

En effet, l'appréciation des risques permettra d'identifier les scénarios de risques et le périmètre à couvrir (voir sur ce point le chapitre « Appréciation des risques cyber »).

7.4 Quand est-il recommandé de construire une architecture sécurisée ?

Cette pratique est incontournable dans les situations suivantes :

- Nouvelle installation ;
- Système industriel en projet ;
- Installation ou système industriels faisant l'objet d'un audit ou d'une revue d'architecture (dans le cadre d'une rétro-homologation de la cybersécurité ou d'une évolution fonctionnelle majeure, par exemple).
- Mise en conformité réglementaire.

Sous réserve que le commanditaire spécifie formellement son besoin de sécurisation, elle intervient une fois que les spécifications fonctionnelles ont été définies (High-Level Design) sur le périmètre d'étude et globalement figées par le bureau d'étude (du moins dans le cadre d'une itération considérée).

Il est alors possible de mener une analyse d'impact (high-level risk analysis selon ISA/IEC 62443) pour estimer le besoin de sécurité des différents groupes d'actifs ou zone, comme abordé dans les chapitres « Appréciation des risques cyber » et VIII « Maintien en conditions de sécurité ».

7.5 Combien coûte la conception d'une architecture sécurisée ?

Selon la nature et la complexité du périmètre d'étude, cette pratique peut varier de deux jours d'étude pour un système simple et maîtrisé, à un minimum de vingt jours environ pour une installation considérée comme complexe.

7.6 Comment concevoir une architecture sécurisée ?

Plusieurs démarches et méthodes peuvent être suivies afin de concevoir une architecture sécurisée. Il est à noter qu'il n'est pas possible de proposer une architecture sécurisée applicable à l'ensemble des systèmes industriels. En effet, chaque système présentant des spécificités qui lui sont propres, certaines mesures de sécurité préconisées dans une architecture peuvent ne pas être applicables dans une autre. Dans ces cas, il est important de traiter le risque via l'identification de nouvelles mesures (techniques ou organisationnelles).
La suite du document propose une démarche pratique afin de construire une architecture sécurisée.

7.6.1 Présentation de la démarche globale

La définition d'une architecture sécurisée commence par l'identification du périmètre à traiter. Ce périmètre peut être un système existant, à concevoir ou un cas d'usage (comme expliqué au sein de la partie « Quel est le périmètre à couvrir par une architecture sécurisée ? »).

Sur le périmètre identifié, il faudra :

1. Identifier les machines et équipements (ressources) le constituant ;
2. Regrouper ces ressources au sein de groupements ;
3. Identifier les mesures de sécurité encadrant les échanges entre les groupements ;
4. Identifier les mesures de sécurité à définir au sein d'un groupement.

7.6.2 Identification des ressources

Afin d'identifier les ressources à couvrir, il faudra disposer d'éléments de cartographie et aussi de certains éléments de l'appréciation de risques (particulièrement si l'architecture sécurisée cherche à traiter un cas d'usage particulier). En effet, l'appréciation des risques permet l'association des ressources avec les besoins opérationnels et l'évaluation des besoins de sécurité. Cette évaluation est nécessaire pour définir les groupements de ressources et le niveau des mesures de sécurité à mettre en place.

7.6.3 Identification des groupements

Le regroupement des ressources permet la définition de mesures de sécurité communes entre elles, et ainsi d'éviter de mettre en place des règles d'architecture propres à chaque ressource. Par exemple, lors de la conception d'un bâtiment, les pièces peuvent être regroupées en fonction de leur vocation à accueillir ou non du public. Les règles de sécurité incendie sont alors différentes selon les périmètres.

Afin de proposer une méthodologie de regroupement, ce guide propose trois critères de regroupement :

- Fonctionnalité de la ressource ;
- Criticité de la ressource ;
- Niveau de confiance.

Le modèle Purdue Enterprise Reference Architecture (PERA) spécifie cinq niveaux de fonctionnalité (Computer Integrated Manufacturing – CIM) :

- Équipements de terrain (capteurs, moteurs) ;
- Équipements intelligents (automates, interfaces hommes-machines, etc.) ;
- Systèmes de contrôle et de supervision (SCADA, DCS, etc.) ;
- Système de contrôles des processus industriels (WMS, MES, etc.) ;
- Systèmes de gestion (ERP, CRM, etc.).

Une architecture selon ce modèle permet de partager une vision commune de l'installation et d'esquisser les premières pistes de segmentation.

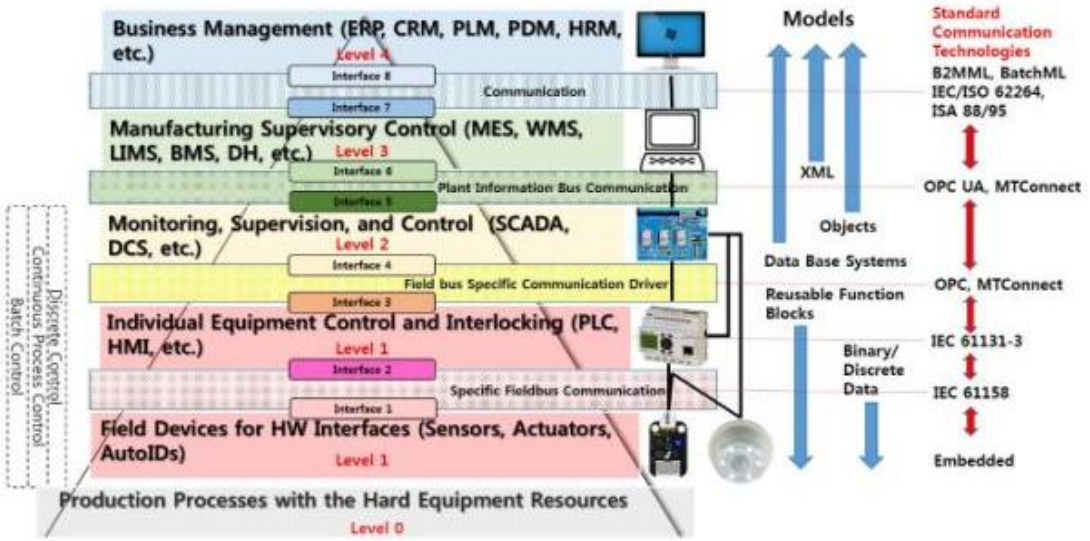


Figure 6. Modèle d'architecture fonctionnelle aligné sur le standard ISA-95/IEC 62264

Une fois l'ensemble des ressources regroupées selon les niveaux de fonctionnalité, il est nécessaire de déterminer les fonctions auxquelles elles participent. Ainsi, il faudra identifier les ressources qui assurent un type de production (atelier, gestion technique d'une salle, etc.) ou de fonction support (maintenance de systèmes, système d'accès distant, etc.). Les fonctions devront aussi être classées par niveau de criticité (une fonction pouvant compromettre le système de production est par exemple considérée comme critique).

Le lien fonctionnel et la criticité sont donc deux critères de regroupement des ressources. Le troisième critère concerne le niveau de confiance qui leur est porté. Ainsi, une ressource installée sur une voie publique, dont la sécurité physique n'est pas assurée, aura potentiellement un niveau de confiance inférieur à celui d'une ressource présente chez un partenaire avec qui un contrat a été signé. Cette dernière ressource aura elle aussi un niveau de confiance inférieur à celui d'une ressource hébergée dans une armoire électrique présente sur une ligne de production protégée des accès physiques.

L'ensemble de ces trois éléments d'analyse permet d'identifier les ressources en différents regroupements. Ces regroupements peuvent aussi parfois porter le nom de « zone » ou « classe », selon la littérature. Ces regroupements ne doivent pas être très larges afin que les mesures de sécurité soient les plus efficaces possibles. Il n'est pas non plus recommandé que ces regroupements soient d'un niveau de granularité très fin, ceci afin d'éviter de complexifier l'architecture.

Ce travail peut être itératif en regroupant ou divisant certains regroupements.

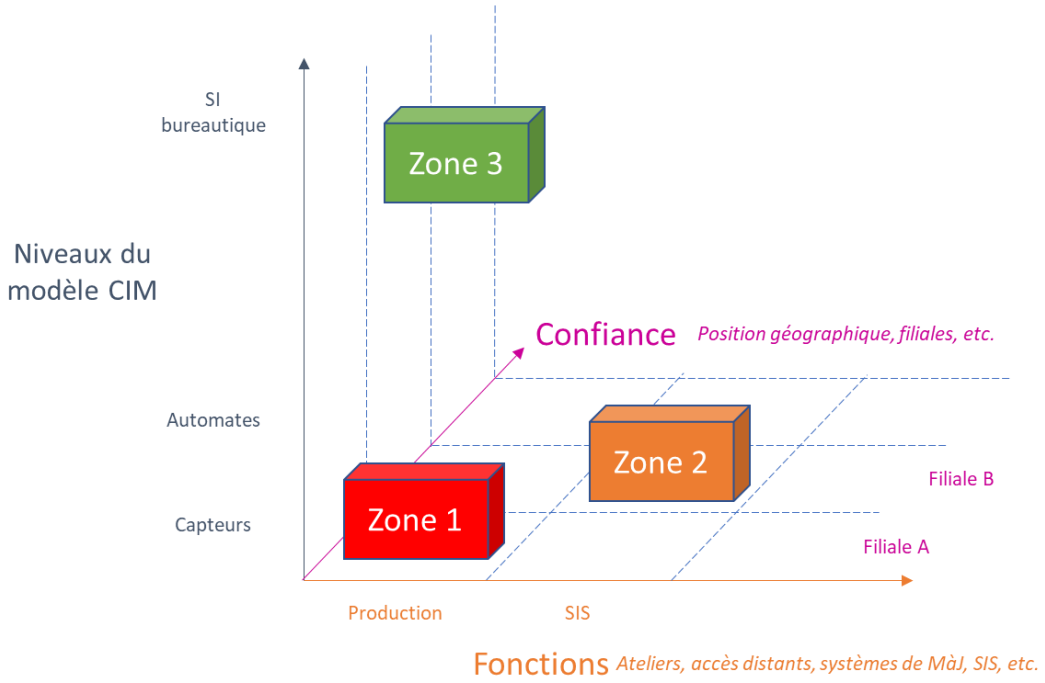


Figure 7. Représentation graphique de la méthodologie de construction des regroupements de ressources

7.6.4 Identification des mesures de sécurité encadrant les échanges entre les regroupements

À partir du travail de regroupement réalisé lors de l'étape précédente, l'objectif de cette phase est de définir les règles encadrant les échanges d'information entre les différents regroupements ainsi que les mesures de sécurité permettant leur mise en œuvre.

Parmi les règles importantes à prendre en compte pour chaque architecture :

- Les flux entre les différents groupements doivent être filtrés ;
- Les flux doivent être initiés depuis une zone de criticité élevée vers une zone de criticité moindre ;
- Les flux initiés depuis une zone de moindre confiance ne doivent être à destination que d'une zone présentant un même niveau de criticité.

Par exemple, une mesure de sécurité peut consister à revoir le câblage entre les ressources d'une même zone (fil à fil).

Le respect de ces règles va impliquer la création de zones intermédiaires aussi appelées « zones démilitarisées » (DMZ). Ces zones ont un rôle de passerelle sécurisée hébergeant des systèmes relais (patch management, signatures antimalware, télémaintenance, consolidation d'indicateurs, etc.) et assurant l'interfaçage sécurisé entre l'environnement de contrôle industriel et « le reste du monde » (par le biais d'un SI de gestion classique généralement).

Les DMZ incluent des mesures de sécurité selon le niveau de criticité de la zone à atteindre (console de gestion des règles implémentées dans les pare-feux, doubles barrières, MCS, accompagnement des changements…). Un simple pare-feu entre SI industriel et SI de gestion s'est avéré insuffisant dans de nombreux incidents de sécurité (attaques sur réseaux électriques ukrainiens, nombreuses diffusions récentes de rançongiciels ayant touché les SI industriels, etc.).

En pratique, il doit y avoir a minima une DMZ pour séparer, avec rupture de flux, les domaines informatiques de gestion et informatique industrielle.

Afin de déterminer les mesures de sécurité à mettre en place, il est recommandé de se reposer sur des standards ou référentiels de sécurité, tels que l'ISA/IEC 62443 ou sur les guides de l'ANSSI. Il est possible de noter parmi les mesures de sécurité :

- Mise en place d'un pare-feu afin d'assurer un filtrage des flux ;
- Mise en place d'un proxy ou reverse proxy afin de s'assurer de la destination ou de la source des flux ;
- Mise en place de sondes d'analyse des flux afin de détecter des attaques ;
- Mise en place de serveurs ou de postes de rebonds durcis pour assurer un niveau de confiance élevé pour accéder à une zone de criticité élevée ;
- Mise en place de postes d'administration dédiés ;
- Mise en place d'un serveur d'échange de fichiers permettant de réaliser une analyse antivirale des fichiers échangés entre des zones de confiance ou de criticité différentes ;
- Mise en place de mécanismes de chiffrement des flux (VPN) ;
- Mise en place d'une solution de sécurisation des accès distants ;
- Mise en place d'une diode unidirectionnelle ;
- etc.

Un exemple de regroupements pouvant être mis en place est présenté ci-dessous :

- Zone d'échange de fichiers : zone permettant l'échange de fichiers entre le système industriel et le système d'information bureautique ;
- Zone d'accès distant : zone hébergeant l'ensemble des mécanismes permettant un accès distant au système industriel ;
- Zone d'administration à distance : zone hébergeant l'ensemble des mécanismes permettant l'administration à distance des systèmes industriels ;
- Regroupement de postes de maintenance : zone où se trouvent les postes de maintenance ;
- Zone de mise à jour : zone hébergeant les outils permettant le téléchargement des mises à jour depuis le système d'information bureautique ou Internet et leur installation sur le système industriel ;
- Zone de consultation d'informations de production : zone permettant la lecture des informations relatives aux processus industriels (lecture des relevés des différents capteurs) ;
- Zone des postes d'ingénierie : zone hébergeant l'ensemble des postes d'ingénierie ;
- Zone des automates d'un atelier ou processus particulier : zone regroupant l'ensemble des automates d'un processus industriel (atelier, ligne de production, etc.) ;
- etc.

Illustration d'une architecture intégrant les équipements cités : https://www.us-cert.gov/ics/Secure-Architecture-Design

7.6.5 Identification des mesures de sécurité au sein de chaque regroupement

Dans cette étape, il conviendra de définir des mesures de sécurité qui permettent d'élever le niveau de confiance de chaque regroupement.

Ces mesures de sécurité permettent de compliquer la compromission du regroupement, ainsi que de limiter les capacités d'un attaquant à se propager au sein d'un système industriel. Parmi les mesures de sécurité possibles :

- Durcissement des équipements (mise en place d'une configuration sécurisée) ;
- Mise en place d'un contrôle d'accès physique ;
- Surveillance de l'activité au sein d'une zone ;
- Mise à jour des équipements (fréquence et démarche) ;
- Règles d'authentification sur les équipements ;
- Gestions des accès tiers ;
- etc.

7.7 Qui est en charge de la conception d'une architecture sécurisée ?

Les principaux acteurs sont :

- Les bureaux d'étude de l'ingénierie système, l'équipementier et intégrateur, de façon à constituer une équipe comportant un ou plusieurs experts cybersécurité en réalisation ;
- Des experts en automatisme et sûreté de fonctionnement, en support ;
- Le chef de projet technique et le responsable de la cybersécurité (ou à défaut le responsable métier), en approbation des livrables d'étude ;
- Les responsables locaux ayant une connaissance approfondie du système existant.

8 Sécurisation des flux

8.1 Que signifie « sécurisation des flux » ?

La sécurisation des flux réseau dans le contexte des réseaux industriels fait référence à l'ensemble des mesures prises pour protéger les communications entre les équipements industriels connectés en réseau, telles que les stations de travail, les capteurs, les actionneurs, les contrôleurs, etc.

L'objectif est de garantir la disponibilité, l'intégrité, la confidentialité et la traçabilité des données échangées entre ces équipements, afin de prévenir toute interruption malveillante du système, altération ou intrusion.

La sécurisation des communications consiste d'une part à « *protéger les informations dans les réseaux et les moyens de traitement de l'information support contre la compromission via le réseau* » (ISO 27002 - § 8.20 « Sécurité des réseaux »), et d'autre part à assurer le maintien de la disponibilité des échanges.

Dans le domaine des systèmes industriels, si des liaisons séries étaient privilégiées dans les premières années et répondent globalement aux besoins de disponibilité, la tendance actuelle consiste à déployer des réseaux informatiques (TCP-IP) afin de satisfaire de nouveaux besoins, comme l'accès facilité depuis des systèmes de contrôle de gestion, la mutualisation des infrastructures et la baisse des coûts de mise en œuvre et d'exploitation.

8.2 Quel est l'intérêt de la sécurisation des flux ?

Les réseaux industriels ont pour but principal de contrôler et surveiller des équipements parfois critiques dans des environnements industriels sensibles, tels que les usines chimiques, les centrales électriques, les installations pétrolières et gazières, etc. Malheureusement, la plupart des protocoles industriels basés sur TCP-IP, comme Modbus TCP, n'intègrent pas nativement de mécanismes de sécurité, les rendant vulnérables aux attaques.

La non-sécurisation de ces flux peut entraîner des risques de perturbation ou de sabotage avec des conséquences pour les installations, les personnes et l'environnement. Par exemple, une attaque cyber sur un pipeline russe a causé la plus grosse explosion non nucléaire (Guide « Fiches Incidents Cyber SI Industriels », Fiche 12), et une attaque menée par un adolescent sur un tramway en Pologne a blessé une dizaine de personnes (Fiche 22).

La sécurisation des flux contribuera à la réduction des risques d'origine cyber, en particulier en évitant la propagation d'une attaque entre des réseaux de sensibilité ou de criticité différents.

8.3 Quand est-il recommandé de sécuriser les flux ?

La sécurisation des flux peut être mise en œuvre sur les systèmes industriels existants, y compris les plus anciens.

Cependant, lors de la conception d'un nouveau projet, dans une démarche de sécurisation globale, il est essentiel d'intégrer la sécurité des communications dès les phases initiales du projet (ex. : avant-projet, conception, etc.), afin d'atteindre le niveau de sécurité attendu sur le système avant sa mise en production

8.4 Combien coûte la sécurisation des flux ?

Le coût de la mise en œuvre d'une sécurisation des flux peut être très variable selon l'environnement, le périmètre et le contexte. Il est important de prendre en compte les facteurs principaux ci-dessous, afin d'estimer et d'anticiper les coûts :

- Le type de projet :
  - Pour un projet neuf (construction d'une usine, extension d'une ligne) les contraintes de sécurité et les coûts associés doivent être inclus dès les phases d'étude et de cadrage du projet ;
  - Un projet de mise en conformité des installations existantes peut souvent présenter des coûts sujets à aléas selon le niveau de maîtrise de l'infrastructure existante et sa complexité ;
- Les études préalables permettant l'établissement des critères de sécurité sur les différents regroupements et flux ;
- Le coût (d'investissement, de possession, de remise à niveau) des équipements de sécurité réseau (pare-feux, VPN, PKI…) ;
- L'environnement d'installation (le type d'équipement matériel pouvant être contraint par des spécificités environnementales selon leur emplacement : humidité, poussière, température négative, etc.) ;
- Les modalités d'intégration technique (certains changements réseau pouvant effectivement nécessiter l'intervention de tiers, tels que des automaticiens, tiers mainteneurs ou électriciens, impactant davantage les coûts) ;
- L'impact du changement : de fait, le coût d'intervention est à prévoir si ce changement nécessite une interruption de tout ou une partie du système de production, en heures ouvrées ou en heures non ouvrées ;
- Le coût du maintien en condition de sécurité des installations ;
- Le coût de l'évolution des équipements ne supportant pas des protocoles sécurisés ;
- Le coût du maintien de la documentation associée.

8.5 Comment réaliser une sécurisation des flux ?

Voici les prérequis à la sécurisation des communications industrielles, sans lesquels une sécurisation des communications industrielles sera peu efficace ou rendue complexe :

1. Avoir un inventaire et une cartographie de l'écosystème industriel de l'organisation (voir le chapitre du guide « Architecture Sécurisée ») ;
2. Identifier les regroupements et les flux, ainsi que leurs besoins de sécurité associés.

La sécurisation repose notamment sur une surveillance permanente des performances (cf. IEC 62443 – FR6) et sur la capacité de traiter les événements de sécurité correspondants.

Une fois ces prérequis validés, l'ordre des étapes de segmentations permettant une sécurisation des flux (tel que défini dans le chapitre du guide « Architecture Sécurisée ») est le suivant :

1. Ségréguer le réseau bureautique du réseau en instaurant une DMZ et appliquer les mesures adaptées pour atteindre les niveaux de sécurité attendus (définis à l'étape 2) ;
2. Segmenter le réseau OT en choisissant une séparation physique ou logique (ou les deux) en fonction du besoin de sécurité ;
3. Intégrer de la micro-segmentation au sein des VLANs présents dans le réseau OT.

La sécurité des communications dans le monde industriel consiste plus particulièrement à protéger la confidentialité, l'intégrité et l'authenticité des informations transférées via, par exemple l'utilisation de techniques de cryptographie (chiffrement, hachage, etc.). On parle également de protection de l'intégrité de la communication (cf. IEC 62443 – SR 3.1) ; de

protection des communications contre l'écoute illicite et l'altération (cf. IEC 62443 – SR 4.1) ; d'utilisation de moyens de protection cryptographiques proportionnés aux conséquences d'une violation de données, à la durée de confidentialité, aux contraintes de fonctionnement du système de commande (cf. IEC 62443 – SR 4.3).

Plusieurs démarches et méthodes peuvent être suivies afin de sécuriser les flux, notamment le principe de défense en profondeur. Voici quelques pistes et manières de sécuriser des flux :

- La segmentation et le filtrage des communications qui permettent de contrôler le trafic réseau entre deux sous-réseaux physiques et/ou logiques ayant des niveaux de sécurité différents :
    - En fonction des conclusions de l'analyse de risques, il peut être préconisé de mettre en place une ségrégation IT/OT, soit :
        - Unidirectionnelle (diodes) ;
        - Avec doubles barrières (doubles pare-feux de différents vendeurs/technologies) et rupture protocolaire (voir également le chapitre « Architecture sécurisée » pour plus de détails), qui permettent de limiter l'exposition des équipements OT aux attaques venant du réseau de gestion tout en permettant l'utilisation de protocoles vulnérables.
    - Le blocage par défaut des communications et l'autorisation par exception (au travers d'équipements tels qu'un pare-feu ou routeur) ;
    - Une attention particulière aux regroupements et aux flux doit être apportée dans le cadre de déploiement sans fil ;
    - Remarque : la mise en place de cette segmentation peut avoir un impact sur les composants en place : modification des adresses IP, impact sur les performances (par exemple, en cas de besoin de communication en temps réel). Ainsi, des solutions de contournements peuvent être mises en place afin de limiter ces impacts sur l'architecture (par exemple, l'isolement des équipements ayant des besoins de communication en temps réel pour limiter leur exposition, sachant que la mise en place d'un pare-feu entre ces différents équipements pourrait entraîner une latence dans le flux et impacter la production).
- L'utilisation de protocoles industriels sécurisables permettant d'assurer la confidentialité des données :
    - La déclinaison de certains protocoles industriels peut être sécurisée, tels qu'OPC-UA ou encore BacNet secure.
      Attention, ces protocoles sont rarement sécurisés par défaut et nécessitent un effort de configuration pour le devenir, et un effort d'organisation, notamment sur la gestion des certificats. Par ailleurs, le chiffrement peut parfois limiter le contrôle des flux (monitoring) et fonctions applicatives transitant.
    - La mise en place de mesures de remédiation sur les protocoles non sécurisés faisant appel au chiffrement, comme de l'encapsulation TLS, ou encore l'utilisation de VPN.
- La détection et le blocage de flux avec l'analyse IDS/IPS sont parfois disponibles sur des équipements de segmentation, en particulier pour les protocoles industriels ;
- La mise en place d'une politique de journalisation des événements de sécurité générés par les équipements réseau, d'une organisation de surveillance permanente des communications et d'une organisation de réponse aux événements de cybersécurité (cf. IEC 62443 – FR6 Timely Response to Event) ;

La sécurisation des flux pour les connexions à distance (que ce soit dans les cas de sous-traitance ou pour des besoins d'administration depuis l'extérieur du réseau industriel) doit être mise en œuvre selon les recommandations figurant au § « Sous-traitance », et doit notamment bénéficier d'une rupture protocolaire.

Il conviendra enfin de maintenir en conditions de sécurité ces mesures (cf. Chapitre « Maintien

en conditions de sécurité »).

Pour aller plus loin : Les équipements réseau contribuant à la sécurité des flux liés à la sûreté/sécurité des installations industrielles critiques doivent être capables de fonctionner en mode île (le réseau industriel étant complètement isolé des réseaux de criticité moindre) et en cas de dysfonctionnement de bloquer toutes les interconnexions avec les réseaux de différents niveaux de criticité (cf. IEC 62443 – FR5 Restricted Data Flow).

8.6 Qui est en charge de la sécurisation des flux réseaux ?

Les règles de sécurisation des flux réseaux doivent être données et/ou validées par le responsable sécurité des systèmes industriels. Ces contraintes de sécurité doivent être communiquées à l'ensemble des acteurs intervenant sur le réseau, et plus généralement sur le système industriel.

La mise en œuvre de la sécurisation des flux réseau peut quant à elle être effectuée par différents acteurs selon le contexte :

- Les bureaux d'étude, les architectes réseau, les administrateurs réseau dans le cadre d'un projet ;
- Les partenaires tiers (mainteneurs, automaticiens, etc.) doivent aussi prendre en compte et implémenter les critères de sécurité le cas échéant.

Les intervenants métiers/fonctionnels doivent être sensibilisés à ces contraintes dans les constructions des solutions et dans la définition des processus d'intervention et d'exploitation

Un point de coordination pour le suivi des opérations doit être effectif entre le RSSI et les équipes projets et opérationnelles.

Chaque intervenant/acteur intervenant sur le réseau doit documenter ses actions et maintenir l'inventaire et les matrices de flux associées.

À la réception d'une fin d'intervention, il faudra s'assurer de la cohérence et de la complétude de la documentation (DAT, matrice de flux, etc.), vérifier les configurations effectives des équipements et recetter le niveau de sécurité.

Ces opérations peuvent être effectuées directement par les équipes Sécurité ou faire l'objet d'une délégation à un partenaire spécialisé (ex. : audit ou test d'intrusion sur le périmètre concerné).

Le responsable métier du périmètre (ex. : direction de site, direction métier) doit être impliqué dans la gestion de la sécurité inhérente à son outil de production.

En outre, quelle que soit l'entité en charge de la mise en œuvre (interne ou externe), l'entreprise doit a minima conserver un niveau de connaissance et de maîtrise de ses systèmes.

9 Intégration et recette de cybersécurité

9.1 Que signifie « intégration et recette de cybersécurité » ?

L'intégration et la recette de cybersécurité couvrent les activités relatives aux essais préalables à la réception d'un système, et plus particulièrement les essais propres aux exigences de cybersécurité spécifiées à l'issue de l'appréciation des risques. La recette de cybersécurité comprend :

- Des tests de conformité : ces tests visent à s'assurer de l'existence, du respect, de l'application et de la mise en œuvre des mesures et mécanismes de cybersécurité conformément aux exigences du cahier des charges ;
- Des tests de robustesse : ces tests visent à s'assurer que les mécanismes de cybersécurité implémentés sont en mesure de résister aux scénarios d'attaques identifiés dans l'analyse de risques.

9.2 Quel est l'intérêt d'une intégration et recette de cybersécurité ?

Les spécifications des besoins utilisateur, d'architecture métier sont souvent suffisamment précises aux niveaux opérationnel et fonctionnel (dont la sûreté de fonctionnement), mais vagues, voire inexistantes au niveau de la cybersécurité. Ce besoin en cybersécurité des systèmes industriels doit donc être défini à chaque étape du projet dès la phase de conception, à travers des spécifications distinctes ou des chapitres dédiés au sein de chaque spécification opérationnelle et fonctionnelle. Ces spécifications et cette conception correspondent à la partie descendante du cycle en « V » représentée en introduction de ce document.

La partie ascendante de ce cycle en « V » permet de mettre en exergue les différentes phases d'intégration, de tests et de recettes associées aux spécifications et conceptions décrivant les besoins opérationnel et fonctionnel.

L'intégration et les recettes de cybersécurité doivent suivre le même cheminement en s'appuyant sur les spécifications et conceptions en cybersécurité. Ce chapitre considère que ces spécifications et cette conception en cybersécurité sont déjà définies et se consacrera donc à la méthode pour réaliser cette intégration et recette de cybersécurité.

De même, le document La cybersécurité des systèmes industriels – Mesures détaillées de l'ANSSI fournit quelques éléments pour la phase d'intégration, de mise en service et réception dans les chapitres 3.3.4 et 3.3.5, comme :

- Des tests aux limites de charge ;
- Des tests d'erreur des fonctions métier ;
- Des tests de la vérification et de la gestion des exceptions ;
- Le déroulement de scénarios de menace (tests de pénétration et tentatives de prise de contrôle : ces tests pouvant entraîner des défaillances, ils doivent être exécutés dans le cadre de maintenance ou avant la mise en production des systèmes) ;
- La vérification des mécanismes de cybersécurité (déploiement de patchs, analyse de journaux d'événements, restauration de sauvegarde, etc.) ;
- L'évaluation des performances du système.

Les phases d'intégration, de mise en service et de recette ne sont pas un audit. Alors qu'un

audit a pour but de vérifier que les procédures en place sont bien respectées, la recette de cybersécurité a pour but de s'assurer de l'existence de telles procédures.

Les recettes ont pour but de vérifier que les procédures sont existantes en plus des mesures techniques (par exemple : le mécanisme de sauvegarde fonctionne bien), mais pas de vérifier si la procédure de changement est appliquée (comme la mise à jour des documents). Néanmoins, certains points peuvent être vérifiés lors de la recette, comme la nomination d'un référent de cybersécurité avec une fiche de poste.

9.3 Quel est le périmètre à couvrir par une intégration et recette de sécurité ?

Ce document a pour objectif de servir de base à la rédaction des cahiers de tests, jusqu'aux cahiers de recettes spécifiques à la cybersécurité des systèmes industriels. Ces cahiers de tests et recettes sont nécessaires pour les phases en aval du cycle en « V » présenté en introduction du document. Ce document n'est pas un cahier de tests ou de recette, n'a pas vocation à expliquer comment les tests et recettes doivent être réalisés ni de préciser les résultats attendus.

Les phases du cycle en « V » sont décrites à travers le chapitre « Exigences de cybersécurité pour les prestataires d'intégration et de maintenance de systèmes industriels » du Référentiel des exigences pour les prestataires d'intégration et de maintenance de systèmes industriels de l'ANSSI.

9.4 Quand faut-il réaliser une intégration et recette de cybersécurité ?

Les phases d'intégration, de mise en service et de recette de cybersécurité sont généralement initiées à l'issue des tests opérationnels et fonctionnels du système.

Si les tests de cybersécurité entraînent un dysfonctionnement du système, des tests opérationnels et fonctionnels devront être alors reconduits partiellement ou intégralement.

9.5 Combien coûtent une intégration et recette de cybersécurité ?

Il est complexe d'estimer de façon globale le coût de réalisation des essais de cybersécurité d'un système industriel. Celui-ci dépend du type de process automatisé, de l'activité (process continu ou discontinu, transport, environnement, pétrochimie, pharmacie, etc.), de l'architecture des systèmes industriels (nombre de composants, architecture centralisée ou distribuée, liaisons avec l'IT, etc.), des solutions retenues pour répondre au cahier des charges cybersécurité (bastion, annuaire, authentification, SIEM, serveurs de mise à jour des patchs, etc.) et, surtout, des tests de cybersécurité prévus pour répondre aux usages spécifiques des systèmes industriels, selon les recommandations de ce document (notamment les tests d'intrusion, les tests de robustesse…).

Le coût de la recette cybersécurité peut aussi dépendre du niveau de cybersécurité défini lors de la phase de spécifications. Plus le niveau de cybersécurité est élevé, plus la recette doit être exhaustive, et ainsi, plus coûteuse. L'utilisation de produits qualifiés par des organismes de cybersécurité peut limiter le nombre de tests à effectuer puisque les fonctionnalités de cybersécurité ont été testées dans leur phase de qualification. Cependant, lors de la phase de recette, il faut vérifier la bonne configuration de ces équipements.

9.6 Comment réaliser une intégration et recette de cybersécurité ?

9.6.1 Prérequis

C'est à partir des spécifications générales et détaillées de cybersécurité que le système a été conçu, programmé et paramétré. Il conviendra donc de réutiliser ces mêmes documents pour réaliser les tests.

Les spécifications opérationnelles et fonctionnelles du système, les Process Instrumentation Diagram (PID) et les plans de masse indiquant la position des équipements (mécaniques, électriques, automatisme, informatique, etc.) ont contribué à l'élaboration de la conception du système et devront être disponibles en cas de complément d'information.

Il faut également disposer des documents techniques suivants :

- Cartographie complète détaillée du système et de ses interconnexions externes si elles existent (voir le chapitre « Inventaire et cartographie ») ;
- Notices techniques de chaque appareil du système industriel ;
- Fiches de paramétrage ou configuration de chaque appareil du système industriel.

Outre les tests de cybersécurité de base liés à la programmation et à la configuration des appareils du système industriel, les tests doivent également s'assurer de la présence de la documentation propre à la cybersécurité des systèmes industriels, par exemple :

- Politique de sécurité des systèmes d'information (PSSI) et de ses règles associées ;
- Plan de formation et de sensibilisation ;
- Liste des personnes en charge de la cybersécurité (interne et externe) ;
- Inventaire des équipements ;
- Cartographies du système ;
- Dossier d'analyse de risques de cybersécurité ;
- Processus de gestion documentaire ;
- Règles de communication ou politique de filtrage (inter réseaux, accès vers Internet, liaisons sans fil, accès distants, etc.) ;
- Politique de sécurité physique (contrôle d'accès physique aux locaux, sécurité physique des équipements, protection des équipements des dommages physiques, etc.) ;
- Politique de sécurité des accès logiques (comptes nominatifs, protection de l'authentification, privilèges, etc.) ;
- Maîtrise des équipements (utilisation des équipements internes et externes et médias amovibles, durcissement de la configuration, protection contre les codes malveillants, gestion de l'obsolescence, etc.) ;
- Maintenance et gestion des équipements (processus d'intégration d'un nouvel équipement, processus de changement, procédure d'intervention d'urgence, gestion des compétences, etc.) ;
- Détection et traitement des incidents (veille des vulnérabilités, traçabilité des actions, examen des traces, traitement des incidents, etc.) ;
- Sauvegarde et continuité (plan de sauvegarde des données et logiciels, processus de restitution, plan de continuité, etc.) ;
- Audit et contrôle (audit des systèmes, des partenaires, suivi du plan d'action, etc.) ;
- Dossier d'homologation et certification ;
- Stratégie de surveillance ;
- etc.

En fonction des phases traitées (phases d'intégration, mise en service et recette de cybersécurité), les prérequis peuvent différer entre les phases d'intégration, de recette et de mise en service. Cependant les éléments ci-dessous sont nécessaires en amont de chaque phase :

- Identification et convocation des parties prenantes ;
- Planning prévisionnel ;
- Rédaction des fiches de tests en précisant :
- Le périmètre ;
- L'objectif ;
- La ou les références des exigences vérifiées par les tests ;
- Le matériel ou l'équipement spécifique requis pour réaliser le test ;
- La documentation nécessaire (spécifications, notices techniques, résultats des tests opérationnels et fonctionnels) ;
    - Les conditions initiales (état du système) ;
    - La procédure à suivre pour mener le test ;
    - Le résultat attendu pour valider le test ;
    - Les réserves potentielles ou les compléments de test ;
    - Des champs libres pour noter :
        - Les résultats obtenus ;
        - La validation ou non de la fiche (validée, validée avec réserves, non validée) ;
        - Les réserves potentielles ou les compléments de tests.

À noter que l'ensemble des spécifications et documents techniques doit être tenu à jour pendant toute la phase de conception et de programmation, mais également lors de modifications durant les tests et durant la durée de vie du système (gestion des modifications).

Avant d'initier les tests opérationnels, fonctionnels et surtout de cybersécurité, les parties prenantes doivent s'assurer que tous les paramètres et règles de cybersécurité sont renseignés et actifs.

9.6.2 Identification du matériel constituant la plateforme de recette

La plateforme de recette devra reproduire le plus fidèlement possible la plateforme de production qui permettra de réaliser le plus grand nombre d'essais possible chez l'intégrateur. Pour cela, les équipements et logiciels utilisés devront être identifiés, ainsi que toutes les déviations entre la plateforme de recette et la plateforme de production, notamment :

- Désignation ;
- Référence ;
- Version ;
- Configuration.

Les différences entre les plateformes de recette et de production se traduiront par des essais complémentaires à réaliser sur la plateforme finale (ex. : utilisation de bouchons ou de simulateurs en plateforme de recette, et essais d'ensemble avec les vrais systèmes en plateforme de production).

9.6.3 Chronologie des tests

Il est conseillé d'activer l'ensemble des mécanismes de cybersécurité avant de démarrer les essais fonctionnels et opérationnels des FAT.

Cette activation consiste à déployer les configurations cibles logicielles et matérielles dans les matériels physiques et logiques : règles réseau, chiffrement, LDAP, bastion, serveur de rebond, VLAN, WAN, VPN, BDD, applications, FW, routeurs, sauvegardes, etc.

L'activation de ces mécanismes dès le début des essais permettra de vérifier qu'elle ne perturbe pas le procédé métier testé.

À l'issue des essais fonctionnels et opérationnels, les essais de cybersécurité seront réalisés.

Il est parfois nécessaire d'activer des mécanismes de sécurité de façon incrémentale. Certains mécanismes ne seront alors activés qu'après la validation de certains tests fonctionnels et opérationnels et avant la conduite des tests de cybersécurité. Les tests fonctionnels qui seront alors conduits ou refaits pour vérifier que l'activation de ces mécanismes de sécurité n'impacte pas le fonctionnement du système permettront de valider fonctionnellement ces mécanismes.

Si des modifications sont apportées aux systèmes au cours des essais de cybersécurité, il est conseillé de retester une partie du procédé (non-régression).

L'objectif consiste à permettre la réalisation des essais de cybersécurité en phase de FAT. Certains essais nécessiteront toutefois la connexion à des équipements ou à des systèmes accessibles uniquement depuis l'environnement de production, non disponibles durant les FAT. Ils devront alors être validés directement in situ durant les SAT, avant la mise en production (en amont de la vérification de service régulier – marche à blanc), par exemple :

- Pare-feu ;
- Équipement d'administration ;
- VPN ;
- etc.

Pour réaliser des tests dans des conditions optimales, il pourra être nécessaire que le programme automate dialogue avec une application qui simule la partie opérative c'est-à-dire que toutes les variables de sortie puissent être visualisées et que les variables d'entrée puissent être activées.

Les essais à réaliser dans le cadre du processus d'homologation cybersécurité doivent être programmés à l'issue des SAT. Il est recommandé toutefois de s'assurer de leur bon déroulement au cours des essais préalables (FAT et SAT).

Un exemple de tests à réaliser se trouve en Annexe de ce dossier.

9.7 Qui est en charge de la conduite de l'intégration et recette cybersécurité ?

Les parties prenantes aux essais dépendent de la nature des tests à réaliser. Ces parties doivent connaître parfaitement le sujet et comprendre les attendus. Une des parties prenantes doit être le rédacteur des spécifications de cybersécurité, qui doit être joignable durant toute la durée des tests.

Dans le cas d'un projet important et complexe, une équipe de metteurs en route dédiée aux SAT peut être mobilisée afin d'assurer une transmission du savoir qui sera lui-même transmis à l'équipe en charge de la maintenance. De plus, dans ce type de projet, l'intégrateur peut être amené à réaliser la maintenance durant les premières années de vie du projet. À la fin de cette phase, une passation est réalisée (Hanover) entre l'intégrateur et l'acteur de maintenance choisi.

À l'instar de la phase de spécification et conception, il est fortement recommandé de rédiger une matrice RACI :

- Responsable (de la réalisation/exécution des tâches à mener) ;
- Approbateur (ou valideur des tâches à réaliser ou réalisées) ;
- Contributeur (participant à la réalisation des tâches) ;
- Information (personne informée et/ou consultée lors de la réalisation des tâches).
- Les parties prenantes aux essais peuvent être :
- Le maître d'ouvrage (MOA) dans la phase de test d'acceptation (opérateur, exploitant), soit :
    - Le chef de projet ;
    - Le responsable fonctionnel ;
    - Le responsable technique ;
    - L'équipe en charge de réaliser les tests ;
    - L'équipe en charge d'assurer la maintenance ;
    - Le RSSI (par extension de la DSI) ou le responsable de la cybersécurité des systèmes industriels ;
    - L'équipe en charge de la qualité de la production.
- Le maître d'œuvre (MOE) ou l'intégrateur dans les phases d'intégration et mise en service (FAT et SAT) :
    - Le chef de projet ;
    - Le responsable fonctionnel ;
    - Le responsable technique ;
    - L'équipe en charge de réaliser les tests ;
    - L'équipe de mise en route sur site ;
    - Le RSSI ou le responsable de la cybersécurité des systèmes industriels.
- Le sous-traitant en charge de la programmation, du paramétrage, de la fourniture des matériels, etc.

Il est conseillé que le sous-traitant en charge de la programmation et du paramétrage fonctionnel soit également en charge des fonctions cybersécurité afin de simplifier les responsabilités. Néanmoins, ce sous-traitant devra avoir les compétences nécessaires et suffisantes pour mener à bien l'ensemble de ses missions incluant la cybersécurité. Il devra donc prouver que ces multicompétences sont bien disponibles et opérationnelles pour le projet concerné.

10 Gestion de la sous-traitance

10.1 Que signifie la gestion de la sous-traitance ?

Dans le cadre de ce document, la « sous-traitance » correspond à l'action de confier la réalisation à une société tierce appelée « sous-traitant », d'une ou plusieurs activités qui peuvent être, par exemple : spécification, conception, développement, prototypage, fabrication, intégration, maintenance ou exploitation de tout ou partie d'un système industriel de contrôle-commande pour le compte du donneur d'ordre.

Les opérations de sous-traitance peuvent être classées en trois catégories :

- Sous-traitance de spécialité (l'entreprise n'a pas les compétences ou les moyens de gérer une tâche donnée) ;
- Sous-traitance de capacité (l'entreprise n'est pas en mesure de gérer tout ou partie du système industriel) ;
- Sous-traitance de marché (obligation d'utiliser un sous-traitant dans le cadre d'un marché).

Ce processus de recours à une organisation tierce est limité à des opérations identifiées et définies par un donneur d'ordre. Le sous-traitant devra se conformer exactement à ces directives. Ces dernières sont principalement des spécifications techniques, organisationnelles ou fonctionnelles. Ce type de prestation doit naturellement être effectué avec le même niveau de sécurité que n'importe quelle autre opération réalisée en interne. Ainsi, il est vivement conseillé d'intégrer les bonnes pratiques adéquates dans toutes les activités sous-traitées.

La sécurité de la sous-traitance est l'ensemble des moyens contractuels, techniques et organisationnels qui permettent de mettre en œuvre une sous-traitance conforme aux exigences de sécurité du donneur d'ordre.

Les sous-traitants sont des prestataires de services pouvant être catalogués selon 6 profils différents :

Profil de sous-traitant	**Rôle**	**Lieu d'intervention**
Bureau d'étude	Le bureau d'étude a un rôle d'assistance et de conseil au donneur d'ordre. En fonction du besoin d'accompagnement, le bureau d'étude peut intervenir durant les phases suivantes d'un projet : • Faisabilité du projet • Étude et conception de projet • Planification de la réalisation • Assistance aux contrats de travaux • Suivi de l'exécution : validation des études d'exécution et direction de l'exécution • Ordonnancement, gestion et pilotage de l'intégration et coordination • Assistance aux opérations de réception À noter que le bureau d'étude n'intervient généralement pas en phase d'exploitation, excepté pour des missions d'audit ou de diagnostic.	Les prestations sont généralement réalisées au sein du bureau d'étude
Fournisseur de matériels et logiciels	Le fournisseur de matériels et de logiciels peut s'appuyer sur un réseau d'intégrateurs et de prestataires de maintenance afin d'assurer le déploiement et la maintenance de son offre. Dans certains cas, il peut être amené à intervenir directement auprès du donneur d'ordre. Et là, il se présente en tant que fournisseur et intégrateur de son offre.	Les prestations peuvent être réalisées depuis son propre site pour les phases de conception, de programmation et de paramétrage. Mais elles doivent être réalisées dans les locaux du donneur d'ordre pour les phases de mise en service et de garantie.

Intégrateur	L'intégrateur est chargé de la réalisation, de la modification ou de la rénovation de tout ou partie d'un système industriel. Il pourra notamment réaliser les actions suivantes : • Conception des spécifications de l'installation • Analyse de l'étude fonctionnelle • Programmation des composants du processus • Paramétrage des composants du système d'information • Conception et configuration des applications métier • Mise en service des installations	Les prestations peuvent être réalisées depuis son propre site pour les phases de conception et d'intégration du système. Mais elles doivent être réalisées dans les locaux du donneur d'ordre pour les phases de mise en service et de garantie.
Exploitant	L'exploitant est le spécialiste métier chargé de l'exploitation des installations industrielles. Il peut être privé ou public.	Les prestations sont réalisées sur site.
Mainteneur	Il intervient sur des installations industrielles déjà en place afin de maintenir ou de rétablir le fonctionnement du système. Son rôle est de traiter ou prévenir des défaillances afin de réduire et, si possible d'éviter les arrêts de production.	Les prestations peuvent être réalisées sur le site du donneur d'ordre ou au moyen d'un accès distant lui permettant d'intervenir sur le système (télémaintenance).
Administrateur	L'administrateur est chargé de l'installation, la suppression, la modification et la consultation d'un système. Il est susceptible de modifier son fonctionnement ou sa sécurité. Les tâches de l'administrateur peuvent être : • Installation ou désinstallation d'un équipement ou d'un logiciel • Modification de configuration et de paramétrage • Mise à jour de composants ou de systèmes • Gestion des sauvegardes • Gestion des droits d'accès pour les utilisateurs	Les prestations d'administrations peuvent être réalisées à distance ou sur site.

10.2 Quel est l'intérêt de la gestion de la sous-traitance ?

En faisant appel à la sous-traitance, un donneur d'ordre introduit de nouvelles parties prenantes disposant de privilèges élevés sur le système industriel, il accroît également la surface d'attaque de son système du fait d'échanges de données, de connexions inter-sites potentiellement cibles de cyberattaques.

Quelques exemples de compromission du système du donneur d'ordre, survenues lors d'une sous-traitance :

Durant la conception : des données relatives à la conception : schéma de réalisation, architectures réseau, plan d'implantation des composants du projet… En bref, de nombreux documents critiques sont échangés entre tous les acteurs du projet. Volées, elles fournissent des informations à l'attaquant, qui peuvent être exploitées pour lancer d'autres attaques. Par exemple, le vol d'un schéma d'architecture du système pourra faciliter l'accès et les déplacements au sein du réseau.

Type de sous-traitant concerné : bureau d'étude, intégrateur

Durant l'intégration : il convient de s'assurer de la non-compromission du système d'information de l'intégrateur durant les phases de spécification, d'assemblage et de paramétrage du système destiné au donneur d'ordre. En effet, par rebond, l'attaquant peut s'introduire sur le système en phase de spécification ou d'intégration et y déposer des composants qui lui permettront plus tard de s'introduire dans le système d'information du donneur d'ordre.

Type de sous-traitant concerné : intégrateur

Durant la maintenance :

- **À distance:** le sous-traitant est utilisé par l'attaquant pour accéder à distance au système d'information du donneur d'ordre. Ainsi, dès lors qu'il y a un canal ouvert entre le mainteneur et le système maintenu, l'attaquant peut intervenir sur le processus industriel, injecter un malware et bloquer la production ou rebondir sur le réseau IT pour voler des données. Il est à noter que ce type d'attaque est de plus en plus utilisé, car particulièrement rentable pour un attaquant qui va pouvoir utiliser le sous-traitant pour atteindre plusieurs cibles finales.
- **Sur site:** le sous-traitant est utilisé par l'attaquant pour accéder sur site au système d'information du donneur d'ordre. Il peut connecter au SI un matériel (clé USB, PC...) compromis capable de lancer une attaque en s'affranchissant des bonnes pratiques de cybersécurité ou des éventuelles mesures de cybersécurité mises en œuvre par le donneur d'ordre.

Type de sous-traitant concerné : prestataire de maintenance et d'administration

Durant l'intégration et la maintenance :

Le sous-traitant stocke des données critiques du donneur d'ordre sur son propre système d'information. Un attaquant peut s'introduire sur ce système et exfiltrer des données critiques.

Type de sous-traitant concerné : intégrateur, prestataire de maintenance

Lorsque le prestataire ne travaille plus pour le donneur d'ordre :

Le contrat de prestation du sous-traitant n'est pas renouvelé, pourtant, il conserve des données critiques du donneur d'ordre ou des accès à son système d'information.

Type de sous-traitant concerné : bureau d'étude, intégrateur, prestataire de maintenance

10.3 Quel est le périmètre de la gestion de la sous-traitance ?

L'ensemble des mesures de sécurité doivent être prises en compte par les différents intervenants sur les périmètres décrits ci-dessous :

- Les zones de partage de données ;
- Le système d'information où est conçu le système industriel. Il s'agit le plus souvent du SI de l'intégrateur ;
- Le système d'information où est déployé et exploité le système industriel. Il s'agit du SI du donneur d'ordre ;
- Les équipements nécessaires à la mise en œuvre de la sous-traitance (PC de maintenance, clé USB…) : en fonction de la politique de sécurité du donneur d'ordre, il peut s'agir des équipements de l'intégrateur ou du donneur d'ordre ;
- Les moyens de communication et de connexion entre le SI du donneur d'ordre et ceux de ses prestataires.

10.4 Quand faut-il sécuriser la gestion de la sous-traitance ?

La sécurité de la sous-traitance doit se faire :

- En phase de précontractualisation (vérification du cadre légal et notamment SLA et pénalités associées, réversibilité sortante, période de résiliation du contrat, pérennité du sous-traitant compte tenu de la longévité du SI industriel, interopérabilité...) ;
- En début de contrat avec un sous-traitant ;
- En cas de modifications contractuelles avec le sous-traitant ;
- Au renouvellement du contrat de sous-traitance.

10.5 Combien coûte la gestion de la sous-traitance ?

10.5.1 CAPEX / OPEX

Le coût des exigences en termes de sécurité doit être intégré au coût global du projet. Il doit être également supporté par le métier. Pour maintenir le métier concerné par les problématiques cyber, il est important de l'impliquer en termes de coûts.

Lors de la phase de contractualisation, il est important de différencier les types de dépense :

- Les dépenses liées à l'exploitation (OPEX : operational expenditure) qui ne sont pas amortissables (par exemple, les dépenses liées aux services cloud) ;
- Les dépenses d'investissement (CAPEX : capital expenditure) qui sont par définition amortissables comptablement. Elles ont vocation à perdurer dans le temps.

Pour une même prestation, les dépenses d'exploitation ont tendance à être plus onéreuses, mais offrent une vision complète du coût. Les dépenses d'investissement ne prennent en compte que les frais liés à la solution, sans prendre en compte les frais annexes (frais de sauvegarde, achat de matériel, MCO, MCS, gestion des changements).

Avant chaque choix de solution, il est important de connaître la stratégie de l'entreprise sur ces types de dépenses pour pouvoir opter pour la bonne solution. Le choix du modèle (d'investissement ou d'exploitation) est directement lié au mode de fonctionnement du service proposé par le sous-traitant (SaaS ou On-Premise).

Il est important de garder en tête qu'il sera plus difficile de justifier l'arrêt d'une prestation avec

un sous-traitant ayant fait l'objet d'une dépense d'investissement en comparaison avec une dépense d'exploitation. Cette question doit être abordée avant la contractualisation avec le métier et la direction des opérations.

10.5.2 ROSI (Return on Security Investment)

La publication suivante du Clusif donne des indications sur la façon de mesurer les retours sur investissement de cybersécurité : *ROSI – Retour sur investissement en sécurité des systèmes d'information : quelques clés pour argumenter*[11]

10.6 Comment faire de la gestion de la sous-traitance ?

La sous-traitance d'une fonction ou d'une partie d'un système SCADA doit être faite avec discernement. Il convient bien entendu de déterminer le niveau de criticité vis-à-vis du métier et de la direction générale. Pour rappel, un système critique devra avoir une exposition au risque réduite, là où un système non critique pourra par exemple admettre une perte de disponibilité.

10.6.1 Système critique pour l'organisation

Pour les systèmes critiques, le donneur d'ordre doit lister l'ensemble de ses besoins de sécurité en s'appuyant sur :

- Les guides de bonnes pratiques (Guide d'hygiène de l'ANSSI, guides du Clusif...) ;
- Les normes et réglementations générales (NIST, IEC-62443, Directive RED, Cyber Resilience Act, LPM, Directive NIS...) ;
- Les normes et réglementations relatives au secteur d'activité de l'entreprise du donneur d'ordre (HDS, Marquage CE des dispositifs médicaux...) ;
- …

Avant de préciser les mécanismes de sécurité technique, l'organisation doit traduire ses besoins en termes de disponibilité, d'intégrité, de confidentialité et de traçabilité. C'est une analyse de risques qui permettra de définir les besoins en termes de sécurité.

Ensuite, l'ensemble des besoins en termes de sécurité doit être traduit en mécanismes techniques (par exemple : segmentation des réseaux, sécurité des protocoles, gestion des sauvegardes et des configurations, sécurité du cloud, etc.) et organisationnels. L'ensemble des mécanismes techniques et organisationnels seront sous forme de référentiel de sécurité (ou « blueprint »).

Ce référentiel de sécurité doit être annexé au contrat liant le sous-traitant à l'organisation. En complément, il est important d'inclure une sensibilisation du personnel et de préciser le nom d'un contact unique qui sera chargé des aspects cyber chez le prestataire.

Le prestataire propose des moyens adaptés pour atteindre le niveau de sécurité requis. Au-delà de ce niveau attendu par le client, il est tenu à un devoir de conseil s'agissant de l'état de l'art de son périmètre métier, incluant les aspects cybersécurité.

Par ailleurs, pour les services critiques, une comitologie rapprochée (COPIL mensuel, trimestriel) doit être mise en place avec des indicateurs de pilotage (performance, qualité) et une revue du niveau de service (comparaison entre niveau de service attendu et réalisé) afin de s'assurer que celui-ci est bien rendu.

Cette comitologie doit également être clairement annexée au contrat avec les niveaux de service attendus. En cas de non-respect, un système de pénalisation financière contraignante

[11] https://clusif.fr/publications/rosi-retour-sur-investissement-en-securite-des-systemes-dinformation-quelques-cles-pour-argumenter/

doit être envisagé et opposable au prestataire (il faut en effet s'assurer que la pénalité soit proportionnée, mais dissuasive pour le sous-traitant). Bien entendu, cela aura un impact direct sur le coût de la prestation. Une attention particulière doit être portée sur la gestion des vulnérabilités et les corrections apportées. En fonction des niveaux de criticité des vulnérabilités (e.g CVSS >= à 7), les modalités de correction doivent être indiquées dans le contrat, tant en termes de délai que de conséquences en cas de non-respect (pénalité, possibilité de dénoncer le contrat en cas de manquement grave).

Et si, pour des raisons opérationnelles, une vulnérabilité ne peut être corrigée (ex. : OS obsolète, ou en EOL), des mécanismes de contournement doivent être envisagés (segmentation, filtrage des flux, virtual patching…). En cas d'impossibilité de modification du système, cela doit être clairement indiqué dans le blueprint et connu par le donneur d'ordre.

10.6.2 Système non critique pour l'organisation

Pour les systèmes non critiques, tous les éléments indiqués ci-dessus doivent être également présents. La différence se situera au niveau de l'absence de système de pénalisation financière. Ainsi, en cas de manquement du prestataire par rapport au niveau de service annoncé (SLO), le prestataire sera en mode « best-effort ».

10.6.3 Exemples de mesures de sécurité

Pour mettre en œuvre une sous-traitance sécurisée, un certain nombre de mesures techniques, organisationnelles et juridiques sont nécessaires. Voici, ci-dessous, celles parmi les plus importantes.

10.6.3.1 Zero Trust

Le concept de Zero Trust en cybersécurité se réfère à une approche de sécurité qui consiste à ne faire confiance à aucun utilisateur, dispositif ou application, aussi bien à l'intérieur qu'à l'extérieur d'un réseau. Cela implique d'authentifier et d'autoriser chaque demande d'accès aux ressources, et de monitorer continuellement le trafic réseau pour détecter toute activité suspecte. En somme, il s'agit de considérer que tout est potentiellement dangereux jusqu'à preuve du contraire, et de limiter l'accès aux données et systèmes à ceux qui ont besoin d'y accéder pour leur travail.

10.6.3.2 Gestion des accès

Pour couvrir ces risques, il est indispensable d'imposer au sous-traitant un descriptif des dispositifs de télémaintenance ou de prise de main à distance, ainsi que les mesures de sécurité associées (Accès VPN, MFA, traçabilité des accès, comptes nominatifs support, bastion d'administration, serveurs de rebond, consoles de maintenance dédiées, etc.).

10.6.3.3 Planification de la maintenance

Le plan de maintenance (préventif, curatif) doit être annexé au contrat. Ce document doit faire mention des éléments suivants :

- La fréquence de maintenance (hebdomadaire, mensuelle, annuelle) : il est recommandé de prévoir les périodes d'intervention pour limiter les impacts sur la production (e.g : HNO, W.E, journée) ;
- Les exigences en termes de délai de déploiement des mises à jour de sécurité, publiées par les éditeurs de logiciel et fabricants de matériel, doivent être indiquées dans le contrat.

Par définition, les maintenances correctives et curatives revêtent souvent un caractère non prévisible et/ou urgent. Dans ce cas, il est plus difficile de les anticiper.

Avant chaque intervention planifiée, le prestataire doit fournir les éléments suivants :

- La date prévisionnelle d'intervention (délai de prévenance à respecter) ;
- Le temps prévu d'intervention ;
- L'impact sur la production.

Après chaque intervention, le prestataire doit fournir un compte rendu détaillé des actions réalisées.

10.6.3.4 Mécanismes de sécurité dans les contrats

Pour aider à sécuriser les interventions réalisées en sous-traitance, il est donc fortement recommandé, entre autres, de formaliser les exigences et objectifs dans un Plan d'Assurance Cybersécurité (PAS). Ce dernier permet de poser des questions ciblées liées à l'activité, au référentiel utilisé, etc.

10.6.3.5 Sécurisation de la relation contractuelle

S'agissant d'un aspect juridique, cette partie doit être coconstruite avec le service juridique du donneur d'ordre, le service achat, les équipes sécurité et le métier.

Les points à vérifier sont :

- Présence d'un plafond de responsabilité à la hauteur du préjudice subi. La non-présence d'indemnisation peut présenter un risque pour le donneur d'ordre ;
- Vérification que le tiers détient une assurance en responsabilité professionnelle couvrant la nature de la prestation et avec des montants et zones géographiques (e.g : USA, Canada…) de couverture adaptées ;
- Possibilité d'auditer le tiers et la chaîne de sous-traitance a minima une fois par an par un tiers habilité à cet effet pour s'assurer du niveau de sécurité. En cas de non-conformité, le donneur d'ordre doit avoir la possibilité de résilier le contrat de manière anticipée sans frais pour manquement grave aux obligations du contrat ;
- Intégration d'un plan d'assurance cybersécurité dans le contrat.

10.7 Qui est en charge de faire la gestion de la sous-traitance ?

Il est important de souligner qu'il est de la responsabilité du donneur d'ordre de s'assurer que les moyens de protection mis en place par le sous-traitant correspondent bien au niveau attendu, et ce, tout au long de la relation contractuelle.

Plusieurs acteurs complémentaires dans leurs domaines doivent intervenir dans la gestion de la sous-traitance pour le donneur d'ordre :

- Le service achat :

Lors de la sélection du prestataire et notamment lors de la soutenance, le service achat devra s'assurer :

  - De l'intégration des exigences de cybersécurité dans la matrice de notation ;
  - Des exigences contractuelles décrites dans la partie « Sécurisation de la relation contractuelle ».

- Le RSSI :

Le RSSI devra être partie prenante du choix du prestataire. Il devra s'assurer que celui-ci est conforme aux exigences de cybersécurité et devra vérifier l'ensemble des déclarations du prestataire.

Lors du choix d'un prestataire et notamment durant la soutenance, le RSSI sera responsable de la notation du prestataire au regard des exigences cyber décrites dans le contrat.

Une fois contractualisé, il s'assurera de la bonne mise en place des exigences de cybersécurité par le nouveau prestataire et mettra à disposition l'ensemble des ressources et

accès nécessaires à cette mise en place.

Le RSSI ou son représentant devra être présent lors des COPIL pour s'assurer du maintien des exigences de cybersécurité dans le temps.

Il s'assurera de la sensibilisation des équipes métier aux exigences de cybersécurité pour les prestataires à travers un programme.

- Les équipes métier :

Les équipes métier devront s'assurer du respect des bonnes pratiques exigées par le RSSI, notamment sur les possibilités d'interventions, les horaires, les équipements utilisés, les gestions éventuelles des clés USB…

Au besoin, le donneur d'ordre peut s'appuyer sur un prestataire qualifié afin de disposer de garanties sur les compétences ou les capacités cyber de ce dernier.

PAMS : Prestataires d'administration et de maintenance sécurisées

L'ANSSI a publié un schéma de qualification visant à valoriser les prestataires d'administration et de maintenance sécurisées. Elle permet aux donneurs d'ordre d'identifier facilement les prestataires fournissant une qualité de service à la hauteur des enjeux de sécurité actuels sur deux axes : techniques et organisationnels. Toutefois, cette labellisation engendre un coût supplémentaire pour le donneur d'ordre. Il faudra mesurer le besoin en fonction des enjeux métiers et de la stratégie cyber de ce dernier.

Le référentiel est accessible via le lien suivant : https://www.ssi.gouv.fr/actualite/publication-du-referentiel-dexigences-pams/

PACS : Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information

L'ANSSI prévoit de publier un référentiel d'exigences qui permet au donneur d'ordre de disposer de garanties sur les compétences cyber sur des activités d'étude d'un projet.

IEC 62443-2-4

La norme IEC 62443 présente dans la section 2-4 un ensemble d'exigences de capacité cybersécurité pour les prestataires de service intervenant sur des activités d'intégration et de maintenance des systèmes industriels. Cette norme propose notamment des exigences de capacités de sécurité sur les sujets suivants : accès à distance, gestion des correctifs, sauvegarde et restauration, gestion de la configuration...

11 Maintien en conditions de sécurité

11.1 Que signifie le « maintien en conditions de sécurité » ?

Le maintien en conditions de sécurité (MCS) recouvre l'ensemble des actions entreprises visant à maintenir le niveau de sécurité des systèmes à un niveau acceptable. Ceci est assimilable au maintien en conditions opérationnelles (MCO) des dispositifs, mécanismes et processus de sécurité.

Afin d'assurer la continuité du service rendu par les systèmes industriels, et pour que le service soit conforme aux exigences établies initialement, plusieurs actions peuvent être entreprises durant le cycle de vie des systèmes. Ces actions, aussi appelées « actions de maintenance », visent à maintenir les systèmes dans un état spécifié. L'ensemble de ces actions est inclus dans des procédures de maintien en conditions opérationnelles des systèmes. Ces procédures comprennent des actions de maintenance corrective (maintenance effectuée lors de la détection d'une panne) et de maintenance préventive (maintenance prévisionnelle ou systématique réalisée pour réduire la probabilité d'occurrence d'une panne).

D'un autre côté, le MCS vise à gérer les mesures, dispositifs et processus de sécurité des systèmes tout au long de leur cycle de vie afin qu'ils restent au même niveau de risque accepté. Le maintien en conditions de sécurité d'un système permet ainsi d'assurer la continuité du service fourni par le système, en réduisant la probabilité d'occurrence d'une panne (arrêt de production dû à un incident de sécurité, par exemple). Le maintien en conditions de sécurité est interdépendant et fortement couplé au MCO dont il constitue généralement un sous-ensemble.

Enfin, certaines thématiques adressées par le maintien en conditions opérationnelles permettent aussi de réaliser un maintien en conditions de sécurité.

Le maintien en conditions de sécurité est souvent perçu uniquement comme la gestion des patchs de sécurité d'un système IT et OT. Or, le MCS a un spectre beaucoup plus large.

Le maintien en conditions de sécurité est donc un travail à effectuer quotidiennement, ce qui vise à s'assurer que les systèmes respectent les règles et mesures de sécurité préalablement définies (au travers de la PSSI ou des analyses de risques des systèmes). Les systèmes étant amenés à évoluer, le maintien en conditions de sécurité (MCS) évolue avec ces systèmes.

11.2 Quel est l'intérêt de réaliser un maintien en conditions de sécurité ?

Dans l'industrie, mais pas uniquement, le MCO des composants mécaniques est courant. Il permet de réaliser la maintenance préventive et curative des équipements (pompe, vanne, ventilateur, disque dur, écran, etc.). En revanche, la maintenance en conditions de sécurité est relativement peu prise en considération : en effet, une fois un système informatique industriel mis en production et le process associé réceptionné et validé, il ne conviendrait plus de le modifier, ceci afin de conserver la garantie des équipementiers et la qualification délivrée par des organismes certificateurs (FDA, etc.), mais aussi pour plus de « tranquillité ».

Cependant, au cours du cycle de vie du système, le niveau de sécurité décline au fil du temps. Les sources de cette baisse du niveau de sécurité sont multiples, parmi lesquelles on retrouve :

- L'évolution des usages :
  - Rapprochement entre les différents métiers (commercial, production) avec une interconnexion des systèmes industriel et bureautique de gestion (rapprochements ERP, MES, SCADA, etc.) exposant ainsi le système industriel aux menaces issues des systèmes de gestion ;
- L'évolution de la menace :
  - Nouveaux outils d'attaques (développements d'outils ciblant de nouvelles technologies, publication des SI industriels exposés sur Internet, etc.) ;
  - Nouveaux acteurs de menace (certains acteurs ciblent des secteurs d'activité en particulier, professionnalisation de la malveillance avec des enjeux pour la cybercriminalité, etc.) ;
- Découverte de nouvelles vulnérabilités :
  - Une vulnérabilité peut être exploitée par des acteurs malveillants pour compromettre les systèmes et ainsi impacter les processus industriels.

La conduite d'une appréciation des risques sur les systèmes permet d'identifier les nouveaux risques faisant décliner le niveau de sécurité des systèmes au cours du temps.

L'objectif du maintien en conditions de sécurité est d'assurer le maintien du niveau de risque résiduel accepté par la MOA. Les actions entreprises visent à compenser les défauts de sécurité du système et son environnement afin de rétablir un niveau acceptable.

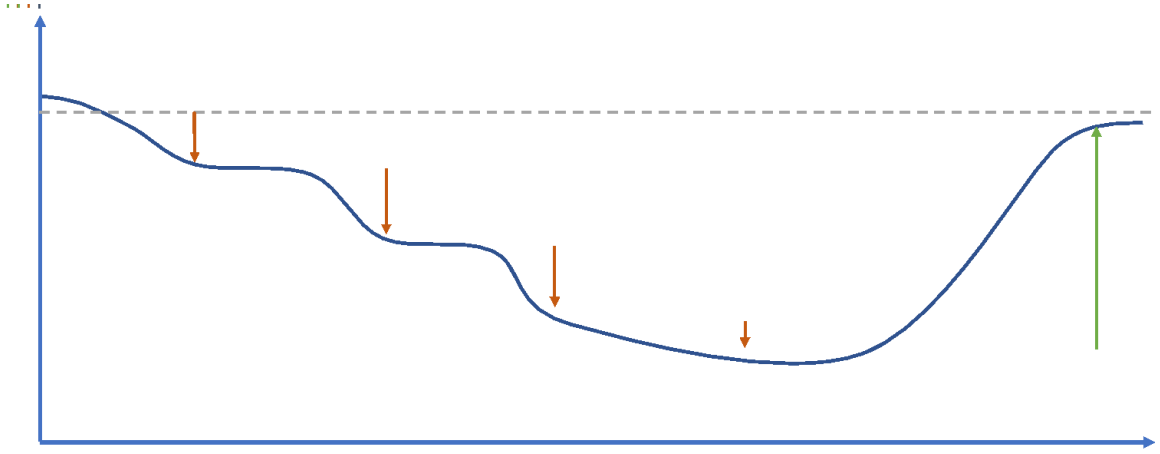


Figure 8. Représentation schématique de l'évolution du niveau de sécurité d'un système au cours du temps

Ce niveau doit être défini lors de l'analyse de risques du système. L'analyse de risques permet de définir des mesures de sécurité afin de se prémunir des risques identifiés (détails dans le chapitre « Appréciation des risques cyber »).

Il est à noter que le niveau de sécurité peut lui aussi évoluer au cours du temps, par exemple avec l'évolution de la réglementation qui définit de nouvelles exigences de sécurité.

L'objectif final du MCS est donc de contribuer au maintien de la performance des systèmes tout au long du cycle de vie du système.

Les mesures de sécurité maintenues lors du MCS peuvent être déployées lors de la conception du système ou déployées à la suite du plan d'action défini lors d'une analyse de risques. Le maintien en conditions de sécurité doit contribuer au déploiement des mesures de sécurité et réaliser les actions de sécurité identifiées. Ces actions permettront de réduire la probabilité d'une panne dont la cause est un incident de sécurité.

11.3 Quel est le périmètre d'application du maintien en conditions de sécurité ?

Le maintien en conditions de sécurité s'applique sur toutes les composantes du système d'information ciblé de l'infrastructure technique le supportant, jusqu'aux acteurs interagissant avec :

- Le périmètre technique :
  - Maintien en conditions de sécurité des mesures et dispositifs de sécurité ;
- Le périmètre organisationnel :
  - Maintien en conditions de sécurité des processus.

Lors de la conception d'un système, des mesures de sécurité sont identifiées et mises en place (pour plus d'informations, voir le chapitre « Architecture sécurisée »). Le maintien en conditions de sécurité se charge alors du maintien des mesures de sécurité en place et de la réalisation des actions identifiées.

Durant le cycle de vie d'un système, le maintien en conditions de sécurité sera amené à déployer de nouvelles mesures de sécurité (par exemple, avec l'identification de nouveaux risques à l'issue d'une analyse de risques : ouverture du système d'information pour de la télémaintenance, par exemple, ou nouvelles menaces). Les audits et contrôles de conformité permettront d'évaluer l'efficacité du MCS (évaluation vis-à-vis du niveau de sécurité).

11.4 Quand faut-il réaliser le maintien en conditions de sécurité ?

Le MCS s'applique à l'ensemble des composantes, ponctuellement et en continu (récurrent).

11.4.1 Ponctuel : Intégration de la sécurité dans les projets

Le MCS intervient ponctuellement en intégrant la sécurité dans les projets à destination des systèmes maintenus. Le MCS accompagne les projets en s'assurant qu'une analyse de risques est effectuée sur les nouveaux projets. Cette analyse de risques permet d'identifier les nouveaux risques créés par le projet sur le système maintenu. L'analyse de risques permettra d'identifier les mesures de sécurité permettant de limiter ces risques. Le MCS devra alors s'assurer de l'application de ces mesures de sécurité.

Le MCS pourra s'appuyer sur un cahier des charges incluant l'ensemble des mesures de sécurité minimales nécessaires à être mises en place par un projet. Ces mesures de sécurité pourront être mises en place par le fournisseur. Dans ce cas, il faudra s'assurer que les contrats de maintenance définissent les rôles et responsabilités de chaque partie dans la conduite de la MCS. Le projet devra s'assurer que le fournisseur produise les documents permettant la conduite des actions de maintien en conditions de sécurité (par exemple : procédure de modification des mots de passe, procédure de mise à jour, procédure de réalisation de sauvegardes).

11.4.2 Récurrent : veille, surveillance et application des mesures de sécurité

Le MCS travaille quotidiennement au maintien du niveau de sécurité des systèmes. Les tâches quotidiennes du MCS concernent :

- La surveillance des systèmes, afin de détecter tout écart d'état par rapport à l'état défini initialement ;
- La gestion des incidents : traitement des crises, traitements des incidents de sécurité ;
- La veille sur les nouvelles vulnérabilités et menaces ;
- La sensibilisation et formation aux mesures de sécurité.

Certaines actions de MCS pouvant avoir un impact sur le processus industriel (ralentissement, redémarrage) doivent être identifiées et anticipées. Ces interventions, ainsi que celles des mainteneurs sur les systèmes, doivent être cadrées par des procédures de MCS qui :

- Détaillent le protocole d'intervention ;
- Définissent la fenêtre de maintenance et d'intervention possible ;
- Précisent le protocole à suivre pour un retour à un état normal (rollback).

La définition de la fenêtre de maintenance doit être réalisée avec le métier dont le système supporte les fonctions. En effet, l'intervention pouvant affecter la continuité de service, la fenêtre de maintenance doit être convenue préalablement par toutes les parties. Il convient de préciser que certaines interventions pouvant avoir lieu de façon urgente, des procédures de maintenance immédiates pourraient donc être définies.

11.5 Combien coûte le maintien en conditions de sécurité ?

Il est complexe d'estimer de façon globale le coût de la MCS d'un système industriel. Celui-ci dépend du type de process automatisé, de l'activité (process continu ou discontinu, transport, environnement, pétrochimie, pharmacie, impact potentiel d'un incident de sécurité, aspects réglementaires, etc.), de l'architecture des systèmes industriels (nombre de composants, architecture centralisée ou distribuée, liaisons avec l'IT, etc.), des solutions retenues pour répondre au cahier des charges cybersécurité (bastion, annuaire, authentification, SIEM, serveurs de mise à jour des patchs, etc.), du nombre de personnels à former et à sensibiliser régulièrement et de la maturité de l'organisation concernée.

Lors du déploiement des dispositifs de sécurité, il convient d'étudier les dépenses liées à l'exploitation de la solution (OPEX). De plus, lors de la modification des systèmes industriels (lors de l'intégration d'un nouveau système, par exemple), l'équipe projet devra être accompagnée dans l'évaluation de l'impact de ce nouveau projet sur les dépenses d'exploitation liées au maintien en conditions de sécurité.

11.6 Comment faire du maintien en conditions de sécurité ?

Les actions liées au maintien en conditions de sécurité sont diverses. Ces actions doivent être définies à partir de :

- La PSSI ;
- Les spécifications de sécurité définies lors de la conception d'un système ;
- Les mesures de sécurité définies lors d'une analyse de risques ;
- Une réglementation contractuelle ou émanant d'un organisme externe.

Les documents suivants pourront être nécessaires pour la réalisation du maintien en conditions de sécurité :

- Dossier d'ingénierie ;
- Dossier de réalisation ;
- Dossier d'exploitation ;
- Cahier de recette ;
- Cartographie et inventaire détaillés du système dans son environnement incluant le détail des versions et releases des logiciels, middlewares, systèmes d'exploitation, firmwares et patchs, matrice de flux et cartographie des flux, identification des moyens de sécurité, comptes à privilèges, éventuelles dérogations, car elles présentent souvent des particularités ;
- Suivi des intervenants (utilisateurs, mainteneurs, administrateurs techniques et fonctionnels) internes et externes (avec indicateurs des Plans d'Assurance Sécurité).

Plusieurs actions peuvent être entreprises sur un même système. Il est préférable de définir le niveau de sécurité à atteindre sur les systèmes au travers d'une appréciation des risques (le niveau de détails de l'AR dépendra du périmètre à analyser ainsi que de sa complexité). L'appréciation des risques permettra ainsi d'éviter l'application de mesures de sécurité non nécessaires (mesures ne permettant pas la réduction du risque) et donc de limiter les dépenses. Cependant, un niveau minimal d'hygiène informatique doit être suivi. La liste suivante, issue des retours d'expérience des membres du GT, permet d'identifier les initiatives importantes à mettre en place pour tout système industriel :

- **Sensibilisation des utilisateurs :**
  - La négligence ou la méconnaissance des utilisateurs est le vecteur le plus souvent utilisé par les attaquants pour compromettre un système industriel. Une sensibilisation des utilisateurs aux risques liés à la cybersécurité ainsi qu'aux bonnes pratiques d'hygiène informatique est nécessaire. La sensibilisation des utilisateurs peut prendre plusieurs formes, par exemple : formation présentielle, e-learning, démonstration d'attaques, retours d'expérience (les fiches des incidents cyber créés par le GT Cybersécurité industriel du Clusif permettent d'assister la sensibilisation des acteurs avec des exemples d'attaques ou incidents ayant eu lieu en milieu industriel), affichage sur les postes, etc.
- **Conduite d'une analyse de risques** :
  - Comme indiqué dans la thématique « Appréciation des risques cyber » (voir chapitre), la conduite d'une analyse de risques permet d'évaluer les risques bruts et d'identifier les mesures de sécurité à mettre en place pour atteindre un niveau de risque résiduel accepté et maintenu dans le cadre du MCS.
- **Réalisation d'une cartographie et inventaire des équipements ou vérification de sa mise à jour** :
  - Comme indiqué dans la thématique « Inventaire et cartographie » (voir chapitre dédié), la réalisation d'une cartographie du système industriel est nécessaire. Cette cartographie doit être régulièrement mise à jour ;
  - En particulier, cette cartographie va permettre la veille vis-à-vis des nouvelles

vulnérabilités publiées par les constructeurs et éditeurs logiciels.

- **Définition de fenêtres de maintenance** :
    - La conduite de certaines procédures de maintien en conditions de sécurité nécessite un redémarrage de système ou peut avoir un impact sur la production (pour l'installation de mises à jour de sécurité, par exemple). Afin d'anticiper et de planifier les actions de MCS, il est nécessaire de disposer de la fenêtre de maintenance de chaque système. Cette information peut être incluse au sein de l'inventaire du système industriel.
- **Revue des règles de filtrage** :
    - Comme indiqué dans la thématique « Architecture sécurisée » (voir chapitre dédié), la présence d'un dispositif de filtrage des flux est nécessaire. La configuration de ce dispositif doit être revue (manuellement ou au travers d'outillage spécifique) afin de s'assurer que seuls les flux nécessaires au fonctionnement du système industriel sont autorisés ;
    - Il est important de mettre en place un processus de modification des règles de filtrage. Ce processus devra s'assurer que toute demande de modification de règles de filtrage ne représente pas un nouveau risque au système industriel.
- **Modification de la configuration par défaut des équipements et applicatifs constituant le système industriel** :
    - Les comptes et mots de passe par défaut sont souvent présents dans les documents techniques de l'équipement. S'ils ne sont pas modifiés, ils peuvent être utilisés par un attaquant pour avoir accès au système industriel ;
    - Il est important donc de modifier les comptes par défaut non nécessaires, mais aussi de désactiver les services non exploités ouverts par défaut sur les systèmes.
- **Mise en place d'équipements dédiés à la maintenance : équipements sécurisés, durcis d'un point de vue sécurité, antivirus installés** :
    - Au vu des privilèges nécessaires à la réalisation des opérations de maintenance, les équipements utilisés dans ce cadre sont critiques. Leur sécurité doit donc être renforcée via l'installation des logiciels strictement nécessaires, une mise à jour régulière du système d'exploitation et des logiciels, une revue de la configuration pour n'autoriser que les processus strictement indispensables, l'installation d'un antivirus et sa mise à jour régulière… Il est aussi préférable que ces postes soient mis à la disposition des mainteneurs et prestataires externes intervenant sur le système industriel. Les mainteneurs utilisent un compte, si possible nominatif, avec le principe des moindres privilèges. Il est recommandé qu'ils ne soient pas administrateurs de ces postes, sans accès à Internet ni messagerie.
- **Revue des accès logiques aux ressources** :
    - Il est possible qu'un ex-employé réutilise ses comptes pour avoir à nouveau accès au système industriel. Il est nécessaire que les comptes d'accès créés soient revus de façon régulière. Un compte doit être désactivé une fois qu'il n'est plus utilisé. Cependant, une revue, au minimum annuelle, des droits d'accès doit être réalisée. De plus, il est préférable que les comptes soient nominatifs (un compte par utilisateur). Dans le cas où les comptes ne seraient pas nominatifs, il est important de s'assurer que le nombre d'utilisateurs y ayant accès soit limité (deux personnes maximum) ou que le compte n'ait aucun droit particulier (compte de lecture, par exemple, pour la visualisation de l'état d'une chaîne de production).
- **Sécurisation des systèmes obsolètes : cloisonnement, durcissement, surveillance spécifique** :
    - Les systèmes obsolètes sont exploités par des attaquants pour intégrer facilement un système industriel et s'y propager. Ces composants ne pouvant plus être maintenus et ne disposant plus des derniers patchs de sécurité, une attention particulière doit leur être accordée. Il faut s'assurer que leur nombre

est limité et qu'ils sont à jour de leurs patchs de sécurité. Il faudra ensuite les cloisonner au sein de réseaux spécifiques (de préférence un réseau par système obsolète) et en n'autorisant que les flux nécessaires à leur fonctionnement. Il est important de n'autoriser que les logiciels nécessaires au fonctionnement de l'application. Certains systèmes de sécurité permettent de s'assurer que seuls les programmes autorisés fonctionnent sur ces systèmes (protection par liste blanche). Enfin, une surveillance accrue doit être réalisée afin d'anticiper le plus tôt possible toute compromission du système.

- **Désactivation des ports et déploiement des bouchons de protection des ports (port USB, séries, RJ45…)** :
    - Les ports peuvent être utilisés pour différents cas d'usage (échanger des données, recharger les smartphones…). Un utilisateur négligent peut ainsi infecter un système via ces ports. De plus, les composants du système industriel peuvent être dégradés par la poussière et l'humidité. Il est donc important de protéger ces ports avec des bouchons à clé. La clé ne devant être mise à disposition que des utilisateurs autorisés et sensibilisés aux risques liés à la cybersécurité.
- **Verrouillage des câbles (câble locker)** :
    - Les câbles peuvent être débranchés pour connecter un dispositif non maîtrisé sur un système industriel. La mise en place de protection des câbles peut donc être nécessaire.
- **Sauvegarde des systèmes et stockage sur des supports hors-ligne (supports non connectés sur le réseau)** :
    - La réalisation de sauvegardes des systèmes d'exploitation, programmes automates et firmwares permet la reconstruction de systèmes ayant subi une attaque. Cependant, les sauvegardes peuvent aussi être la cible des attaquants, rendant ainsi une reconstruction impossible. Il est donc nécessaire de stocker certaines sauvegardes sur des dispositifs hors-ligne (disque dur externe, cassette..) en plus des sauvegardes en ligne. La fréquence de mise à jour des sauvegardes doit être étudiée de telle sorte que la reconstruction permette le rétablissement des systèmes. La sécurité physique des supports de sauvegarde hors-ligne devra être étudiée. Enfin, il est nécessaire de tester périodiquement les sauvegardes réalisées pour s'assurer qu'un rétablissement du système est possible, ainsi que pour entraîner les équipes en cas de crise.

Comme indiqué dans la partie VIII.2 « Quel est l'intérêt de réaliser un maintien en conditions de sécurité ? », les sources de la baisse du niveau de sécurité sont nombreuses. Il est important que les équipes en charge du MCS se tiennent informées des évolutions de la menace. Les équipes de MCS pourront alors reposer sur des sources de veille externes, des équipes chargées de la surveillance du système industriel (SOC), les équipes chargées du maintien en conditions opérationnelles du système industriel, les équipes des ressources humaines, etc. De plus, les équipes en charge du MCS doivent être formées aux nouvelles pratiques de sécurité et sensibilisées aux nouvelles menaces.

11.7 Qui est en charge du maintien en conditions de sécurité ?

Étant donné le nombre d'actions à entreprendre ainsi que leur diversité, plusieurs acteurs seront amenés à réaliser les actions de MCS. Par exemple :

- Les actions en lien avec la sécurité physique seront réalisées par le responsable de la sécurité physique du site ;
- Les audits pourront être réalisés en partie par le responsable de la conformité et risque du site ;
- Les actions de sensibilisation et formation pourront être gérées par le responsable des ressources humaines.

L'équipe sécurité sera ainsi amenée à assurer un rôle d'accompagnement et de pilotage de l'ensemble des actions.

Il est donc nécessaire de construire un RACI, qui permet de s'assurer que les rôles et responsabilités de chacun sont bien définis pour couvrir l'ensemble des actions de MCS avec, a minima, les actions identifiées dans la partie VIII.6 « Comment faire du maintien en conditions de sécurité ? ». Le RACI permettra aussi que l'ensemble de ces actions s'articulent bien entre elles.

12 Résilience et réponse à incident

12.1 Que signifie la « résilience et la réponse à incident » ?

Une indisponibilité des systèmes d'information peut avoir un fort impact sur l'ensemble des services et des processus d'une industrie. Pour être prêt à réagir dans de telles conditions, il devient capital de bien identifier au préalable les enjeux et les mesures à mettre en œuvre afin de permettre à l'entreprise d'être résiliente en cas d'incident.

12.1.1 Résilience

La résilience constitue la capacité d'une organisation à s'adapter aux incidents perturbateurs (panne informatique, piratage…) afin d'en minimiser les impacts sur l'activité des services métier. Les différentes actions à mener doivent permettre aux systèmes industriels de faire preuve d'une plus grande adaptabilité et réactivité de l'organisation aux attaques (les attaques ransomware, par exemple) et de faire face à la croissance exponentielle des menaces informatiques.

Selon l'AFNOR, la gestion des risques est la gestion de tout ce qui pourrait interférer avec les objectifs et missions d'un organisme. La politique de gestion des risques contribue donc à renforcer la résilience d'une organisation. Cette dernière est propre à chaque entreprise et s'appuie sur des moyens organisationnels, humains, financiers et techniques.

Pour rendre un SI industriel résilient, deux étapes sont indispensables : la première est de tenir compte et d'appliquer les bonnes pratiques informatiques usuelles dans ce domaine ; la seconde consiste à se préparer à faire de la gestion des incidents.

12.1.2 Gestion des incidents

La gestion des incidents consiste à définir et implémenter les procédures et activités à déclencher en cas d'incident informatique sur les systèmes industriels, afin d'y répondre en rétablissant les services le plus rapidement possible.

Elle vise à protéger les activités industrielles de l'organisation, en s'appuyant sur les enjeux métiers précisés via le temps de rétablissement maximal tolérable des processus concernés (RTO), la durée maximale durant laquelle les données peuvent être perdues (RPO), et la quantité maximale de temps d'arrêt tolérable sans causer de préjudice à la mission de l'organisation (MTD).

La gestion des incidents est un processus permettant de suivre, détecter, classifier et traiter les incidents informatiques (donc numériques) dans un environnement industriel historiquement sécurisé d'un point de vue physique. Elle suppose donc (i) de définir les cas d'usage de comportement anormal de ces systèmes, (ii) d'implémenter des outils de détection adaptés aux outils industriels d'une chaîne de production et (iii) de transmettre l'information aux équipes de détection (SOC).

Elle nécessite également l'implication d'interlocuteurs liés à l'activité industrielle, comme les responsables de sécurité physique, les automaticiens ou les chefs de sites.

Les incidents les plus critiques (affectant un service essentiel à l'organisation, impactant la réputation de l'entreprise, entraînant une perte financière importante ou menaçant son intégrité physique) devraient être considérés comme des crises. Ce mécanisme d'escalade fait l'objet d'une matrice de criticité inhérente à l'organisation. La gestion d'une crise s'articule en

plusieurs phases :

- Les premières mesures de traitement (isolement et assainissement des systèmes touchés par la crise) en fonction de la gravité ou de la criticité du système touché ;
- La communication entre les parties prenantes de l'incident ;
- Le mode de fonctionnement dégradé permettant d'assurer le fonctionnement des activités de manière plus ou moins dégradée en fonction des risques acceptables pour l'entreprise ;
- Le processus de retour au fonctionnement normal du système affecté par l'incident.

Pour pouvoir être pertinent et activable à tout moment, le dispositif de gestion de crise doit être testé de manière régulière, en impliquant les acteurs en charge du SI industriel. Il doit être mis à jour en fonction des leçons apprises des exercices ou des crises précédentes, mais aussi de l'évolution de l'organisation ou des nouvelles menaces pouvant affecter celle-ci.

12.2 Quel est l'intérêt de mettre en place de la résilience et de la réponse à incident ?

Le but de la mise en œuvre des opérations de résilience (anticipation de la réponse à incidents, correction des éventuelles défaillances du système…) est de préserver l'activité de l'entreprise en limitant les interruptions de service liées aux incidents et de permettre un retour à la normale dans les meilleurs délais.

Au-delà de la minimisation des temps d'indisponibilité de service, d'autres bénéfices peuvent être attendus de la mise en œuvre d'une résilience et d'une réponse à incident :

- La réduction des coûts pour l'entreprise en cas d'incident à travers, par exemple, la réduction des temps d'indisponibilité, du coût de la reprise, du montant de la prime d'assurance (...) ;
- Un avantage concurrentiel possible dans le cadre de certaines réponses à appels d'offres ;
- Une possibilité de certification ou d'homologation (ISO 22301, ISO 27001, NIST, LPM…) ;
- Un gain ou un maintien dans la maîtrise de son patrimoine industriel à travers la mise à jour documentaire ;
- Une meilleure gestion de la communication au sein de l'organisation lors d'incidents l'affectant.

12.3 Quel est le périmètre à couvrir par la résilience et la réponse à incident ?

En prérequis : il est recommandé d'avoir mené au préalable une analyse d'impacts métier sur le système étudié avant de se lancer dans les étapes suivantes.

La pertinence d'un plan de gestion des incidents pour maintenir ou reconstruire une activité est fortement dépendante du périmètre à couvrir. Il est important d'identifier un périmètre d'applicabilité du Plan de Continuité d'Activité (PCA) et du Plan de Reprise d'Activité (PRA) en adéquation avec les objectifs métier, sachant que la mise en place d'un PCA/PRA peut être coûteuse et chronophage.

La mise en place de la résilience informatique repose sur la mise en œuvre d'actions concrètes à différents niveaux, qui visent à assurer la robustesse d'un périmètre donné. La définition de ce périmètre de couverture dépend de plusieurs éléments :

- Événements redoutés à prendre en compte vis-à-vis d'impacts métier identifiés ;
- Processus/actifs/données essentiels.

Il est nécessaire d'adapter le périmètre en fonction de l'entreprise et des spécificités de chacun

de ses processus industriels. Il peut être également déterminé avec l'aide des différentes directions et acteurs concernés (voir chapitre « Qui doit le faire ? »).

12.3.1 Événements redoutés à prendre en compte

Les plans de continuité ou de reprise d'activité reposent principalement sur une analyse d'impact sur l'activité. La sélection des causes vraisemblables des événements redoutés en fonction de leurs impacts permettra de proposer des actions pertinentes. Les causes les plus vraisemblables associées aux impacts les plus importants seront à considérer en priorité.

12.3.2 Processus, actifs et données essentiels

Les axes techniques et organisationnels suivants devront être couverts :

- La sécurité physique des sites ;
- L'administration, la sécurité et la maintenance des systèmes industriels ;
- L'hébergement et la sauvegarde des données ;
- Les outils mis en place pour les collaborateurs, messagerie incluse ;
- L'organisation et les procédures mises en place par l'entreprise ;
- La sensibilisation et la formation des collaborateurs, permettant de réduire les risques d'erreurs et permettant de ne pas rendre plus vulnérable l'entreprise vis-à-vis des menaces ciblant tout particulièrement le facteur humain ;
- La sécurité liée aux fournisseurs ;
- L'existence de modes dégradés.

12.4 Quand faut-il mettre en place de la résilience et de la réponse à incident ?

Il est possible d'aborder le sujet de la Résilience :

- À n'importe quelle étape d'un projet d'entreprise ;
- Lors de la mise en place d'un Système de Management de la Sécurité de l'Information ;
- Lors d'un changement au sein de la société ;
- Lorsque des risques importants émergent du contexte international ;
- etc.

La prise en compte de la cybersécurité (y compris même l'application des bonnes pratiques de sécurité) fait partie de la mise en œuvre du concept de résilience au sein d'un système industriel. Une approche « Security by Design » permet d'inclure des mesures de sécurité lors de la définition du cahier des charges d'un projet et d'assurer une homogénéité dans l'application de ces mesures.

Il reste tout à fait possible d'analyser l'existant cyber et de mettre en place une résilience pour des projets en cours, ce qui nécessitera une forte implication de l'ensemble des équipes. De plus, une compréhension par la direction de la nécessité d'une amélioration continue du projet est requise, afin d'intégrer la cybersécurité de manière efficiente, sans déstabilisation du service associé au projet. La définition d'objectifs clairs est essentielle dans un tel contexte.

Note : Il est important de profiter des arrêts planifiés dans la vie du système industriel pour mettre en place les actions nécessaires aux PCA/PRA (par exemple, la création de backup).

12.5 Combien coûte la mise en place de la résilience et réponse à incident ?

Le coût à engager va dépendre des actions définies dans le plan d'action de cyberrésilience. Il peut être très important.

Il est donc primordial de cadrer l'investissement à réaliser en fonction de la valeur et de la criticité des éléments à protéger. Une analyse de risques préliminaire devra permettre de déterminer les éléments à protéger ainsi que le niveau de protection à envisager. L'investissement à consentir doit toutefois rester proportionnel aux enjeux et aux capacités financières de l'entreprise. Afin de chiffrer le coût de mise en place, il faudra notamment prendre en compte les facteurs suivants :

- En phase de mise en œuvre (Build) :
  - Coûts relatifs aux analyses permettant d'identifier les services critiques de l'entreprise et les modes dégradés pouvant être envisagés pour assurer la continuité d'activité en cas d'incident ;
  - Coûts relatifs à l'information et à la formation du personnel en interne ;
  - Provisionnement des matériaux et logiciels requis (pour la redondance des systèmes critiques, infrastructure de surveillance...) ;
  - Intégration et configuration des solutions retenues (incluant la phase de test et de validation).
- En phase d'exploitation (Run) :
  - Coûts relatifs à la veille régulière sur les vulnérabilités et menaces, et aux audits des systèmes d'information à protéger (internes ou par des tiers de confiance) ;
  - Coûts liés aux simulations d'incidents afin de tester la réaction des équipes opérationnelles ;
  - Dépenses de maintenance et de mise à jour des logiciels et infrastructures concernées ;
  - Coûts relatifs aux tests et revues régulières des mécanismes et procédures prévues en réponse à incident.

Le budget correspondant peut-être pris en charge, au moins partiellement, par les métiers (hors IT ou maintenance), car il est étroitement lié à la continuité d'exploitation.

12.6 Comment mettre en place la résilience et réponse à incident ?

La sécurité des systèmes industriels vise en priorité le maintien de la disponibilité de l'activité ou du service rendu. L'ensemble des actions à mener pour correctement construire une résilience et une réponse à incident (investigation ou restauration du service) doit être défini en gardant à l'esprit que la priorité est de limiter autant que possible un arrêt des infrastructures critiques.

La construction de cette résilience nécessite une implication de nombreuses ressources. En fonction de la taille de l'entreprise, il peut être nécessaire de segmenter les PCA/PRA en sous-périmètres (business, régions…) en fonction de leur homogénéité.

12.6.1 En préventif

La phase préparatoire est essentielle pour préparer les équipes et garantir un temps d'interruption le plus réduit possible. Voici une liste d'actions préventives qu'il est possible de mettre en place pour améliorer la résilience :

- Mise en place d'une hygiène de sécurité visant à se protéger des attaques ;
- Veille sur les menaces, surveillance et audits du SI afin d'en maîtriser les vulnérabilités

(outils de scan de vulnérabilités, audits externes...) et d'en augmenter la protection dans le temps ;
- Maîtrise/Cartographie du parc informatique (DAT, CMDB, sonde réseau, etc.) ;
- Identification des actifs critiques pour l'activité de l'entreprise (processus, activités, données, applications) ainsi que les menaces qui pèsent sur ceux-ci ;
- Mise en place de mesures permettant le maintien de ces actifs en cas de panne :
    - Redondance des serveurs hébergeant les applications critiques ;
    - Restauration des données en cas de perte ;
    - Définition en amont de l'organisation et des responsabilités en cas de crise ;
    - Identification des modes dégradés selon les différentes pannes possibles et vérification d'absence d'actifs communs (réseau, stockage, sauvegardes…) ;
    - Programmation des exercices annuels de crise ;
    - Construction de procédures régulièrement mises à jour et testées pour la mise en œuvre des Plans de Continuité d'Activité (PCA) et de Reprise d'Activité (PRA).

Le SGDSN donne dans sa publication Guide de construction d'un Plan de Continuité d'Activité, édition 2013[12], une démarche qui facilite la création d'un tel document.

C'est la mise en œuvre conjointe de l'ensemble de ces éléments qui permettra d'améliorer la résilience du SI de l'entreprise.

12.6.2 La réponse à incident

12.6.2.1 En préambule

Afin de préparer au mieux la procédure de réponse à incident, il est nécessaire d'identifier plusieurs points :

- **Identification des acteurs** : Les différentes personnes de l'organisation identifiées comme membres des équipes de réponse à incident, ainsi que leur rôle et leurs coordonnées ;
- **Organisation** : L'organisation pour mener la réponse à incident avec la description des rôles et responsabilités de ces personnes et équipes dans le processus, ainsi que les étapes ordonnées de la reprise d'activité. Il faut par exemple être vigilant à ne pas reconstruire un système alors que la menace continue de se propager.

L'identification préalable de ces différents points va permettre de limiter la perte de temps lors de la gestion de crise. Les premières heures étant les plus critiques pour maintenir l'activité et limiter les impacts, il est fortement recommandé d'accorder de la valeur à cette phase de préparation.

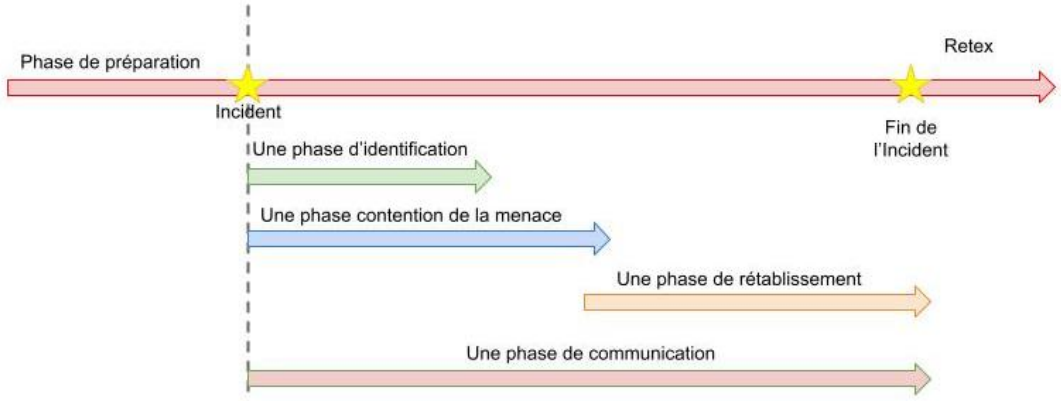
12.6.2.2 Les différentes étapes de la réponse à incident

De manière standard, le processus de réponse à incident peut prévoir les phases suivantes :

- Une phase de préparation ;
- Une phase de communication ;
- Une phase d'identification et d'évaluation des incidents :
    - Levée de doute (événement ou incident avéré) ;
    - Classification et évaluation de la criticité en cas d'incident avéré ;
- Une phase de contention de la menace ;
- Une phase de rétablissement ;
- Une phase de « leçons apprises ».

[12] http://www.sgdsn.gouv.fr/uploads/2016/10/guide-pca-sgdsn-110613-normal.pdf

Ces phases sont là pour structurer la méthodologie de réponse à incident, et s'enchaînent naturellement au fil du temps.



- Une phase de préparation

Elle a pour objectif de mettre sur pied une équipe d'intervention et de définir et prévoir les moyens techniques, humains (internes comme externes) et de communication requis pour mener la réponse à incident.

- Une phase de communication

Celle-ci est transverse : elle commence dès que l'incident est avéré et s'étend jusqu'à sa résolution. Une équipe dédiée à la communication doit être constituée en cas de crise, et doit faire le lien avec les équipes de réponse à incident, la direction, et les parties prenantes externes à l'organisation (clients, ANSSI, CNIL, communication publique…).

Cette phase de communication doit être préparée, car elle permet de limiter les impacts sur l'image et participer à une reprise d'activité plus rapide tout en rassurant les parties prenantes.

- Une phase d'identification et évaluation des incidents

Celle-ci a pour but d'évaluer la gravité et la menace correspondantes à une anomalie ou activité suspecte détectée, afin de définir la réponse appropriée. Durant cette phase, les éléments suivants doivent être étudiés :

- Levée de doute (événement ou incident avéré) ;
- Évaluation en cas d'incident avéré :
    - Catégorisation de l'incident ;
    - Portée de l'incident ;
    - Impact de l'incident ;
    - Gravité de l'incident et temps de réponse associé ;
- Une phase de confinement de la menace :
    - Définition des stratégies de confinement en fonction de la nature de l'incident ;
    - Les différentes étapes de confinement ;
    - La préservation des preuves ;
    - Le recueil des données et traces de l'attaque.
- Une phase de remédiation

Elle doit permettre l'élimination complète de la menace (nettoyage des systèmes affectés, coupure des accès de l'attaquant au système, arrêt des systèmes compromis).

Une fois que la menace a été éradiquée, il est nécessaire de mettre en place un plan d'action de reconstruction pour revenir à un fonctionnement normal.

- Une phase de « leçons apprises »

Il s'agit ici de réaliser une analyse post-incident qui implique l'identification de la cause

originale de l'incident, l'analyse de sa chronologie et permette d'améliorer continuellement la sécurité, les capacités d'intervention et les procédures applicables en cas de nouvel incident.

Nota Bene: la reconstruction doit se faire après que les preuves légales ont été collectées pour transmissions aux instances judiciaires.

12.6.2.3 Les notifications et communications

Il est nécessaire d'anticiper les communications à réaliser en fonction de la nature de l'incident, internes comme externes, et de prévoir ici les éventuelles interactions avec les forces de l'ordre ou la CNIL en cas de violation de données personnelles. Dans le cas où un système de communication a été compromis par un attaquant, il est important de s'être doté au préalable d'un mode de communication alternatif, indépendant du système nominal.

12.6.2.4 La planification des tests et revues de la procédure de réponse à incident

Afin de garantir une réponse à incident efficace, il est important de tester et revoir régulièrement la procédure la régissant.

12.6.2.5 La coordination des équipes opérationnelles et cybersécurité lors d'une réponse à incident

Attention aux actions antagonistes entre les actions des opérationnels avec les procédures d'investigation cyber : les équipes opérationnelles pourraient par exemple anticiper la remise en service de leur système industriel alors que les équipes forensics n'ont pas terminé leurs investigations.

12.7 Qui est en charge de la mise en place de la résilience et réponse à incident ?

Cette partie aborde l'ensemble des acteurs et des responsabilités pour la mise en place de la résilience et de la réponse à incident. Dans un premier temps, une identification des différents acteurs sera réalisée pour ensuite distribuer les rôles et responsabilités de chacun.

12.7.1 Les acteurs

La mise en place de la résilience d'une entreprise doit se réaliser au niveau de plusieurs directions. Au même titre que la sécurisation ou la gestion des risques, il est nécessaire de faire intervenir tous les acteurs d'une entreprise pour avoir une vision exhaustive de la problématique.

La liste des différents acteurs identifiés pour la mise en place de la résilience doit a minima contenir:

- *DG :* Direction générale
- *DC :* Équipe/Direction cybersécurité
- *DM :* Équipe/Direction métier
- *DR :* Direction des risques
- *DT :* Équipe/Direction technique
- *DJ.* Équipe/Direction juridique
- *RH :* Équipe/Direction des Ressources humaines
- *HSE :* Équipe/Direction Hygiène, Sécurité et Environnement
- *RP :* Équipe de communication/relations publiques
- *PE :* Les prestataires de l'entreprise (infogérance, mainteneur)
- *CERT/CTI :* Organisation spécialisée en investigation cyber (CERT/CTI)
- *F :* Fournisseurs

Cette liste peut être à adapter en fonction de l'organisation de l'entreprise.

12.7.2 RACI – En préventif

Exemple des différentes étapes pour mettre en place une résilience, liste des acteurs nécessaires comprise.

	DG	DC	DM	DT	DR	DJ	RH	HSE	RP	PE	CERT	F
Mise en place d'un socle de sécurité	I	**A**/R	R	R	I	I	I	C		I		R
Veille sur les menaces		C			I					R	**A**/R	
Maîtrise/Cartographie		I	**A**									R
Identifier les actifs critiques (y compris humains)		C	R		**A**	C	C	C				
Mise en place des mesures	I	**A**	R	R		C	R	R	R	R		R

Un lien doit être assuré entre le MCO/MCS et la résilience d'une entreprise afin de garantir en tout temps la capacité d'intervention et la connaissance des installations.

12.7.3 RACI – En cas d'incident

Voici une proposition des différentes étapes avec les acteurs nécessaires en cas d'incident pour garantir la résilience

	DG	DC	DM	DT	DR	DJ	RH	HSE	RP	PE	CERT	F
Une phase de préparation	I	**A**	R	R	I	R	R	R	R	I/R		I/R
Une phase de communication	A	C	C	C		R	C/R	C	R		I	
Une phase d'identification et d'évaluation des incidents				C	**A**	C					R	
Levée de doute (événement ou incident)		R		C	**A**						C	
Évaluation en cas d'incident avéré	I	**A**	R	R	C	C	C	C	I		C	I
Une phase de confinement de la menace		**A**	R	R			C	R	R	C/R		
Une phase de remédiation		C	R	**A**			C		R	C/R		
Une phase de « leçons apprises »	I	**A**	C	R	I	C	R	R	R	I	C	I

13 Audit cybersécurité

13.1 Que signifie un « audit cybersécurité » ?

L'audit de cybersécurité en milieu industriel fait appel à une ou plusieurs expertises permettant d'évaluer le niveau de cybersécurité d'un périmètre considéré. Il peut s'agir d'un système de management (SMCS au sens ISA/IEC 62443-2-1, ISO 27001, etc.), d'un système industriel (le cas échéant complexe, multisites...), d'une architecture, d'une installation industrielle particulière (site), ou encore d'un système de contrôle-commande (SCADA…), d'un sous-système, d'un équipement spécifique (automate, capteur/actionneur connecté...) ou d'un produit (dans le cadre d'une qualification/certification, par exemple).

L'audit vise à évaluer la sécurité d'un périmètre, tel que décrit ci-dessus, par rapport à un référentiel. L'objectif peut être de :

- Évaluer sa maturité (vis-à-vis de l'état de l'art et des bonnes pratiques de sécurité) pour définir une feuille de route dans le cadre d'un plan de progrès ou d'une démarche d'amélioration continue ;
- Contrôler la conformité aux exigences d'une réglementation (LPM, NIS, IGI 1300 …), d'un référentiel (ex. : ISA 62443), d'une politique, d'un contrat et du Plan d'Assurance de la Sécurité ;
- Obtenir une certification (ex. : ISO 27001, ISA 62443, CSPN, établissement de santé…).

Plusieurs catégories d'audit de cybersécurité existent. Le tableau suivant présente les différentes catégories définies par l'ANSSI et par l'ISA :

ANSSI - PASSI v2.1	ISA/IEC 62443
Audit d'architecture Audit de configuration Audit de code source Tests d'intrusion (« Pentest ») Audit organisationnel et physique	 High-level vulnerability assessment Detailed vulnerability assessment CSMS audits

13.2 Quel est l'intérêt d'un audit cybersécurité ?

Le fait de réaliser un audit par un tiers indépendant permet d'objectiver le niveau de cybersécurité estimé (en termes de vulnérabilités organisationnelles ou techniques).

À ce titre, ce genre d'exercice pédagogique (preuves d'audit à l'appui) permet de construire une feuille de route où les priorités sont identifiées (via les recommandations exprimées dans le plan d'action de sécurisation) pour élever le niveau de cybersécurité par rapport à un objectif fixé en termes de conformité et/ou de management du risque cyber.

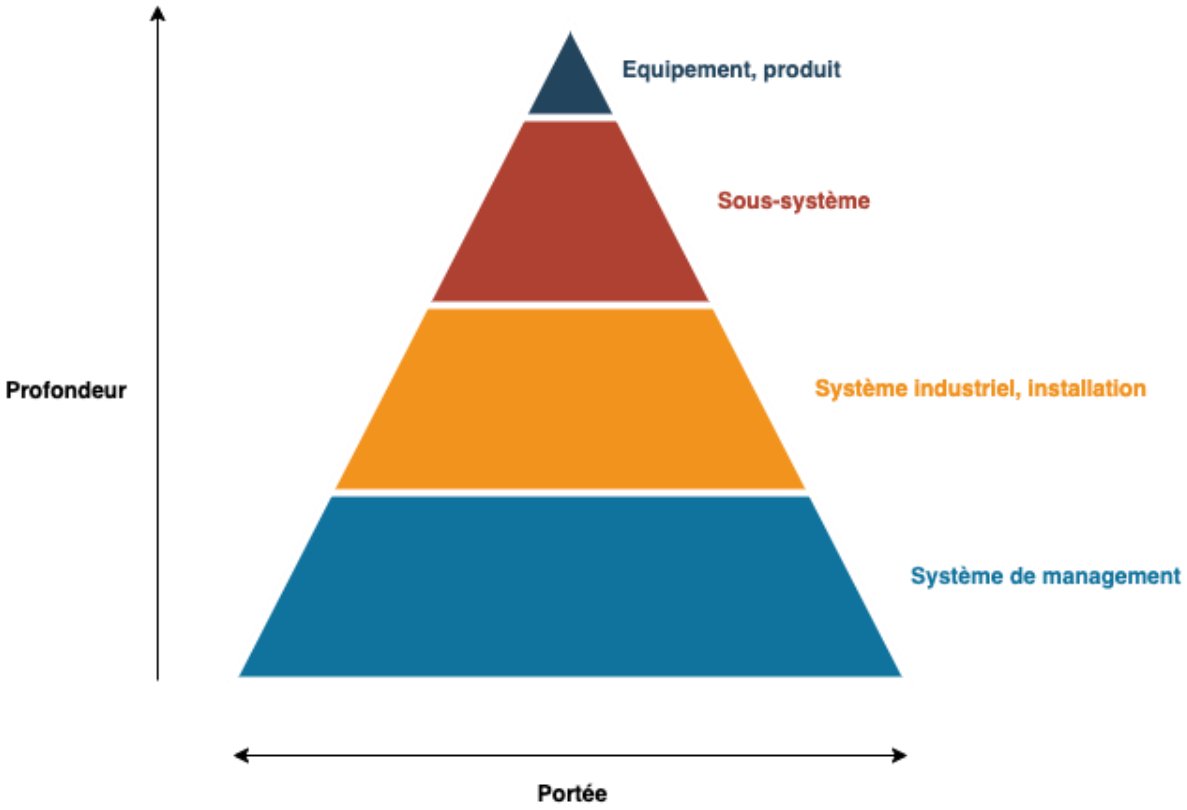
Le résultat de l'audit permet aussi d'obtenir une meilleure visibilité sur le périmètre audité (découverte d'équipement, mise à jour de l'inventaire).

Des pentests internes et externes peuvent venir compléter les audits organisationnels et techniques (audits de configuration, d'architecture, par exemple). Ils ont pour intérêt de mieux comprendre les faiblesses exploitables du système.

13.3 Quel est le périmètre à couvrir par un audit cybersécurité ?

En principe, le périmètre à auditer doit être en cohérence avec la finalité recherchée.

En règle générale, plus le périmètre est large (système de management, système industriel, installation), plus l'audit sera à portée organisationnelle. À l'inverse, plus le périmètre est restreint (équipement, produit), plus l'audit sera à portée technique. Une approche combinée organisationnelle et technique permet d'évaluer le niveau de cybersécurité global conformément au principe de défense en profondeur.



Dans tous les cas, il est important de noter qu'un audit n'est pas, par définition, exhaustif, puisqu'il adresse un périmètre défini lors d'une réunion de cadrage préliminaire. En revanche, il permet d'identifier les vulnérabilités les plus critiques, de proposer des plans de remédiation et ainsi d'éviter que les vecteurs d'attaque ne puissent les exploiter.

En environnement industriel, la réalisation d'un audit technique peut impacter significativement le process industriel et, par conséquent :

- La vie humaine (blessure, maladie, incapacité, mort) ;
- L'environnement (fuite de produit, feu, inondation) ;
- L'économie (perte de production, temps d'arrêt et de redémarrage, moyens nécessaires au redémarrage) ;
- Le fonctionnement de l'Etat et de ses infrastructures critiques (OIV) ;
- Et, bien entendu, toutes les conséquences similaires à un audit sur un environnement IT (l'image, l'organisation…).

Pour limiter ces impacts, il est fortement recommandé de réaliser les audits techniques dans le respect des prérequis suivants :

- Une plateforme de test ou préproduction est à disposition pour la réalisation des tests ;
- La plage horaire identifiée est appropriée :
    - Par exemple, en heures creuses (la nuit ou bien pendant les périodes d'arrêt de la production) ;
    - Plutôt en début de semaine pour avoir du temps pour redémarrer l'installation au besoin ;
- Le personnel qualifié pour redémarrer les installations est présent et disponible ;
- Les PRA/PCA sont à jour et accessibles ;
- Les sauvegardes hors lignes sont disponibles ;
- Les tests sont le moins intrusifs possible (accès en lecture seule, audit de configuration plutôt que vulnérabilités...).

13.4 Quand faut-il faire un audit cybersécurité ?

L'audit de cybersécurité peut être réalisé à plusieurs moments du cycle de vie du système étudié.

En fin de conception, avant la mise en service (ex. : VABF) pour s'assurer :

- De l'acceptabilité du niveau de sécurité atteint, et qu'il corresponde aux attentes (niveau de risque acceptable) ;
- Du niveau de conformité par rapport aux exigences ;
- Ou lorsqu'une homologation est requise.

De même, il sera nécessaire d'auditer le système à la suite d'évolutions fonctionnelles ou techniques majeures, car ces changements sont susceptibles d'introduire de nouveaux risques. Il est aussi conseillé lors de la mise en œuvre de nouvelles mesures de sécurité, ceci pour s'assurer de leur efficacité.

Il est utile de réaliser un contre-audit après l'audit initial, afin de confirmer que les écarts constatés ont bien été corrigés. Il est en effet courant que les organisations corrigent uniquement certaines failles et non la totalité de celles détectées. Dans ce cas, la commission d'homologation ou le management doit accepter les risques résiduels.

Durant la phase de production du système, il peut être utile d'avoir des réévaluations périodiques par échantillonnage, ou bien d'utiliser des outils d'analyse de vulnérabilités en continu.

L'audit est aussi préconisé à la suite d'un incident survenu en interne, dans la filière ou dans un environnement technologique similaire, ou suite à l'émergence de menaces sur le système étudié.

De manière générale, il est recommandé d'auditer le périmètre complet régulièrement selon sa criticité, son exposition, ou d'autres critères en fonction du contexte. Par exemple, pour les périmètres SIIV (Systèmes d'Information d'Importance Vitale), l'audit d'homologation à la loi de programmation militaire doit être réalisé a minima tous les 3 ans et après chaque modification majeure du SIIV.

13.5 Combien coûte un audit cybersécurité ?

Le coût d'un audit cyber est dépendant de plusieurs facteurs :

- La portée de l'audit (pentest, organisationnel, architecture, configuration) ;
- Les technologies présentes dans le périmètre ;
- Le nombre d'entretiens à réaliser en fonction des interlocuteurs à rencontrer ;
- Le nombre d'équipements ;
- L'existence de rapports récents ;
- La quantité de documentation (par exemple, une éventuelle homologation afin de répondre à la réglementation applicable demande souvent plus de documentation) et sa qualité ;
- Le nombre d'auditeurs (composition d'une équipe - responsable d'audit) ;
- La compétence et l'expérience des auditeurs (technologique, normative, méthodologies, qualification PASSI) ;
- Les contraintes de l'audité (horaires, habilitations, nécessité de formation sur site - risques NRBC, risques électriques, autres).

Le coût d'un audit cyber sera aussi directement lié à la durée de l'audit et du niveau d'expertise demandé. Il peut durer quelques heures (on parle dans ce cas d'« audit flash ») et n'a pas de maximum. L'audit flash a pour avantage d'être moins coûteux, mais n'entre pas dans le détail du périmètre étudié. Il a pour objectif de faire un premier état des lieux et d'identifier les domaines qui doivent être approfondis lors d'un audit plus complet.

Le coût pourrait être réduit par la capacité à réaliser ces audits avec des équipes internes. Certaines entreprises ont des consultants en permanence dans leurs locaux pour effectuer ce type de prestation.

Il est aussi important de noter qu'un audit engendre des coûts indirects dus à la mise à disposition de ressources internes : personnes se rendant disponibles, système mis hors production, gestion des visites…

13.6 Comment réaliser un audit cybersécurité ?

En général, les étapes réalisées dans le cadre d'un audit sont :

1. Définition du périmètre : périmètre géographique, de l'organisation/service et des systèmes (les équipements, les locaux, les documents, les personnes, type de SI…) ;
2. Sélection du ou des types d'audits à réaliser (architecture, configuration, code source, test d'intrusion, organisationnel et physique, de conformité, passif, actif, agressif, destructif, etc.) ;
3. Choix du ou des référentiels :
    a. interne : l'avantage d'utiliser le référentiel interne de l'audité est qu'il est contextualisé et adapté au métier de l'audité ;
    b. externe (ISA 62443, LPM, NIST SP 800-82,…) : à utiliser dans le cas où l'audité ne dispose pas de référentiel ou que ce dernier souhaite évaluer son niveau de sécurité par rapport à des entités externes. C'est le cas pour obtenir une certification/qualification.
4. Choix de réaliser l'audit avec des auditeurs internes ou externes ;
5. Si externes : procédure d'appel d'offres (pouvant inclure Plan d'Assurance Sécurité, planning, organisation de l'équipe d'audit, compétences/certifications, références d'audits similaires réalisés…) ;
6. Signatures des documents administratifs : NDA, convention d'audit qui précise notamment les limites de responsabilité et décharge (lettre de mission, charte...) ;
7. Exécution de l'audit :
    a. Préparation : validation du planning, communication et validation des prérequis ;

   b. Construction et validation du plan d'audit ;
   c. Réalisation du plan d'audit ;
   d. Si besoin, remise en état nominal ;
8. Présentation des résultats et du plan d'action pour remédier aux écarts constatés. Livraison du rapport (synthèse managériale + détails) et des résultats.

La mise en œuvre du plan d'action est généralement hors de périmètre de la mission d'audit. Néanmoins, pour optimiser les coûts et les délais, il peut être demandé aux auditeurs (s'ils en ont les compétences) de mettre en œuvre les actions correctrices.

13.7 Qui est en charge de la réalisation d'un audit cybersécurité ?

Plusieurs critères permettent de choisir qui sera le mieux placé pour réaliser l'audit :

- Les compétences et qualifications en audit (formations/certifications) ;
- l'expérience (références) ;
- Les compétences et qualifications technologiques (connaissances des systèmes et produits) ;
- Les autorisations (habilitations de défense, droits d'accès aux zones, certifications électriques…) ;
- La connaissance de l'environnement étudié (secteur d'activité, l'entreprise, le service, le système) ;
- Les éventuels conflits d'intérêts (relation de management, concurrence) ;
- La disponibilité (nombre d'auditeurs composant l'équipe, respects des délais, assurer une continuité de prestation).

Le profil des auditeurs amenés à intervenir en milieu industriel est différent de celui des auditeurs de SI de gestion, il est donc parfois nécessaire de réaliser des concessions sur les critères cités ci-dessus au regard de la disponibilité des spécialistes présents sur le marché.

14 Surveillance

14.1 Qu'est-ce que la surveillance de la sécurité des systèmes industriels ?

La surveillance de la sécurité des systèmes industriels est l'ensemble des moyens techniques et humains mis en œuvre permettant d'être en capacité de détecter les comportements anormaux afin de détecter les incidents de sécurité informatique (qu'elle soit d'origine malveillante ou non) et d'y répondre de façon efficace.

La surveillance des systèmes informatiques industriels n'est pas à confondre avec leur supervision. En effet, la supervision opérationnelle des équipements informatiques consiste au contrôle du bon fonctionnement des systèmes via la détection de surchauffes, espaces disques, etc.

Dans la suite du traitement de cette thématique, il ne sera question que de la surveillance des systèmes industriels.

14.2 Quel est l'intérêt de mettre en place une surveillance de la sécurité des systèmes industriels ?

Une attaque d'origine informatique suit souvent un même schéma :

- Reconnaissance : ensemble des activités de recherche menées par l'attaquant afin de cibler au mieux les systèmes ;
- Intrusion : ensemble des actions entreprises par un attaquant afin de s'introduire sur le système d'information de la cible ;
- Propagation : ensemble des actions conduites par un attaquant afin de se propager au sein du système d'information ;
- Exploitation : exécution par l'attaquant de sa charge afin de corrompre ainsi le niveau de sécurité du système d'information.

La détection d'une attaque ou d'une compromission de systèmes industriels au plus tôt permet d'éviter un impact important sur la production. En effet, l'exploitation d'indicateurs de compromission permet de mettre en œuvre les mécanismes de réponse visant à contenir et éradiquer la menace.

14.3 Quel est le périmètre à couvrir par une surveillance de la sécurité des systèmes industriels ?

La surveillance des systèmes industriels consiste en la collecte et l'analyse d'indicateurs, aussi appelés journaux.

Afin d'identifier le périmètre à surveiller, il est nécessaire de disposer d'une cartographie des systèmes industriels la plus à jour possible (cf. V « Inventaire et cartographie »). Cette cartographie devra inclure également les systèmes d'information en interface avec les systèmes industriels.

Le périmètre de collecte peut être traité selon deux axes :

- Horizontal : ensemble des dispositifs à surveiller ;
- Vertical : profondeur de surveillance d'un même dispositif.

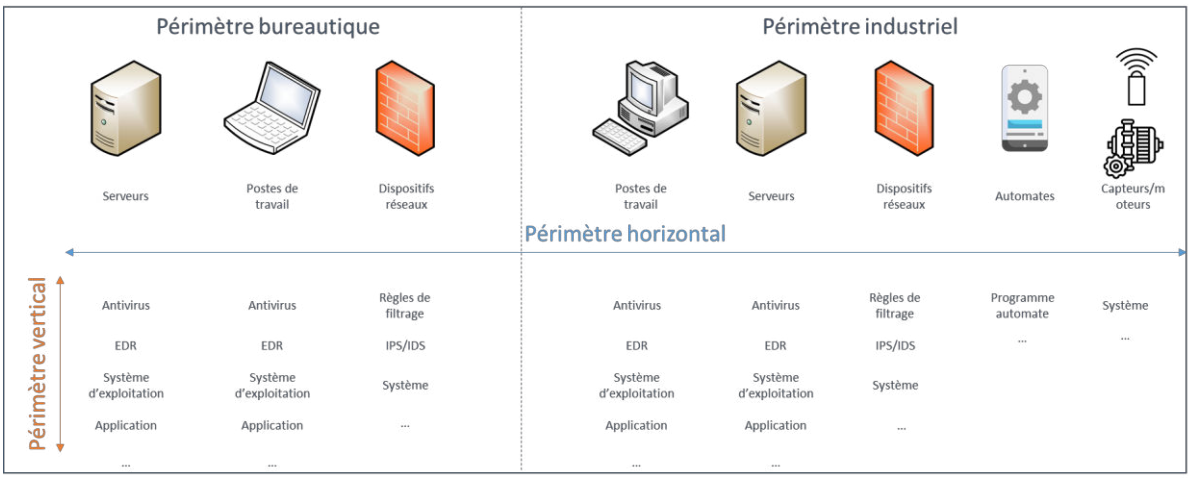


Figure 8. Représentation schématique des différents périmètres à surveiller

Il est nécessaire de définir le périmètre à surveiller ainsi que la profondeur d'analyse en termes de collecte de journaux. L'idéal est de surveiller l'ensemble du périmètre. Néanmoins, le risque est d'être confronté à de nombreux journaux difficiles à traiter, et notamment un nombre important de faux positifs.

Il est recommandé de surveiller également le périmètre bureautique (ce dernier pouvant être un chemin de compromission du périmètre industriel) au travers d'une surveillance dédiée, différente de celle du périmètre industriel.

Ensuite, afin de délimiter le périmètre à surveiller, il est recommandé d'adopter une double approche :

- Socle de surveillance de base : il est nécessaire de réaliser prioritairement une surveillance des outils de sécurité déjà présents sur le périmètre, avec notamment la surveillance des antivirus, firewalls, etc ;
- Approche par le risque : cette approche consiste, au travers d'une appréciation des risques (cf. « Appréciation des risques cyber »), d'identifier les chemins de compromission et l'impact potentiel d'incidents. En effet, cette analyse permet d'identifier les biens essentiels visés, leur criticité, puis les biens supports avec les vulnérabilités associées exploitables. Il s'agira ensuite d'identifier les journaux à générer et à surveiller tout au long du chemin de compromission afin de détecter les incidents.

Cette double approche permet de limiter les journaux à générer au strict nécessaire.

A noter que le périmètre à surveiller peut-être évolutif, en fonction des besoins de sécurité, criticité des éléments.

14.4 Quand faut-il mettre en place une surveillance de la sécurité des systèmes industriels ?

La surveillance des systèmes industriels doit être réalisée dès lors que le système est opérationnel. De plus, il est recommandé de mettre en place cette surveillance une fois les prérequis suivants mis en place :

- Un socle de sécurité de base : il est nécessaire de mettre en place un premier socle de sécurité de base (cloisonnement réseau, déploiement d'antivirus, maîtrise de l'exposition externe des systèmes industriels, etc.) afin de simplifier la génération des journaux et de se doter de moyens de répondre aux incidents de sécurité ;
- Une gouvernance de la sécurité : la surveillance s'inscrit au sein d'une organisation globale et il est nécessaire de bien cadrer les rôles et responsabilités des parties prenantes, par exemple, lors de l'identification des chemins de compromission, ou la gestion des incidents de sécurité ;
- Moyens financiers suffisants : la surveillance nécessite des ressources humaines spécialisées et une maîtrise technique importante. Il est donc primordial de bien cadrer le budget à disposition afin de délimiter le périmètre à auditer.

14.5 Combien coûte la mise en place d'une surveillance de la sécurité des systèmes industriels ?

La mise en place d'une surveillance de la sécurité des systèmes industriels est un investissement qu'il convient de définir et maîtriser. Plusieurs facteurs sont importants afin de chiffrer le coût d'une surveillance :

- Lors de sa mise en place :
    - Coûts relatifs aux analyses afin d'identifier les journaux à générer ;
    - Charges et développements nécessaires pour la génération et la collecte des journaux ;
    - Investissements liés à la mise en place de l'architecture de collecte des journaux ;
    - Achat et intégration des sondes d'inspection réseau industrielles ;
    - Achat, intégration et configuration des dispositifs d'analyse et corrélation des journaux ;
- Pour son exploitation :
    - Recrutement des analystes en charge de la surveillance et des investigations ;
    - Charges liées au maintien en condition opérationnel et sécurité de l'architecture de collecte et d'analyse des journaux ;
    - Paiement des différentes licences utilisées, notamment pour les systèmes d'analyse et de corrélation ;
    - Organisation à mettre en place pour le traitement des alertes, notamment avec les astreintes et formations des analystes, ou recours à une organisation externe (cf. « Qui est en charge de la mise en place d'une surveillance de la sécurité des systèmes industriels ? »).

Dans le cas de l'externalisation de la surveillance des systèmes industriels, plusieurs facteurs sont également à prendre en compte. En effet, un investissement pour la configuration des équipements, ainsi que l'intégration des systèmes à surveiller avec le prestataire, sont à prévoir en plus des coûts liés à l'abonnement. Le coût des prestations de surveillance peut varier en fonction des SLA souhaités (surveillance uniquement en heure ouvrée, en follow the

sun, etc.), mais également en fonction du type de prestataire (prestation qualifiée PDIS ou non).

14.6 Comment mettre en place une surveillance de la sécurité des systèmes

Avant de mettre en place une surveillance des systèmes industriels, il est nécessaire de délimiter le périmètre (cf. 10.3 « Quel est le périmètre à couvrir par une surveillance de la sécurité des systèmes industriels ? »).

Sur le périmètre à surveiller, une attention particulière sera apportée sur les spécificités des systèmes industriels qui pourraient impacter la méthodologie suivie pour la surveillance :

- Présence de systèmes obsolètes : par exemple, il faudra vérifier si ces systèmes peuvent générer des journaux, est-ce qu'il est possible de modifier leur configuration, si des mises à jour de sécurité sont toujours disponibles pour être appliquées en fonction des nouvelles vulnérabilités détectées, etc. ;
- Utilisation de systèmes embarqués : par exemple, il conviendra d'analyser l'architecture de collecte des journaux et la connectivité réseau ;
- Contraintes de connectivité réseau : par exemple, pour les sites étendus, il s'agira de vérifier l'impact de la remontée des journaux sur la connectivité réseau, ainsi que les surcoûts que cela peut engendrer (augmentation du débit de connexion satellite, par exemple) ;
- Protocoles industriels : par exemple, il conviendra de disposer de pare-feux et de sondes réseaux qui permettent l'interprétation des protocoles industriels ;
- Plage de maintenance : par exemple, la connaissance des plages de maintenance permet d'identifier les périodes possibles d'intervention pour une configuration informatique des systèmes ;
- Capacité de calcul des systèmes industriels : par exemple, l'identification des capacités dont dispose le dispositif pour générer des journaux sans que les opérations ne soient impactées. Il sera dans ce cas, par exemple préférable d'éviter de chiffrer des journaux pour ne pas surcharger des systèmes ;
- Contrainte réglementaire imposant la journalisation ;
- etc.

Lors de cette étape préliminaire, il est ainsi important de disposer de :

- La cartographie des systèmes industriels ;
- Le résultat de l'appréciation des risques, avec notamment les chemins de compromission identifiés ;
- Les mesures compensatoires identifiées dans le résultat du plan d'action défini suite à l'appréciation des risques.

14.6.1 Mise en place de scénarios

À partir des éléments recueillis en amont, il conviendra, pour chaque scénario de compromission, de :

- Identifier les journaux à générer et notamment
    - Le dispositif sur lequel ils sont générés (horizontal)
    - Quelle(s) ressource(s) les génère(nt) (vertical) ;
- Définir la méthode de corrélation des journaux, afin de pouvoir détecter au mieux l'incident (aussi appelée workbook). En effet, un scénario de compromission correspondra à une succession d'événements détectés dans les journaux ;
- Identifier la partie prenante responsable de diagnostiquer le scénario de détection et lever le doute ;
- Identifier la partie prenante en charge d'intervenir au cas où l'incident est avéré ;

- Définir la méthodologie d'intervention (aussi appelée playbook) permettant d'indiquer les étapes à suivre afin de contenir et corriger l'incident, ainsi que celles requises pour assurer le retour au fonctionnement nominal.

La méthodologie d'intervention est importante et doit être adaptée au contexte industriel. Par exemple, la détection d'une compromission par un logiciel malveillant sur un poste en milieu bureautique peut induire une réponse sous forme de mise en quarantaine du poste, suivie de sa remasterisation. Cette réaction n'est pas envisageable pour de nombreux types de postes industriels.

De plus, la méthodologie d'intervention doit être validée par les responsables de l'exploitation industrielle. Il est primordial que les rôles et responsabilités en cas de détection d'une compromission soient clairement définis. Par exemple, une définition comme suit peut-être envisagée :

- Détection d'une compromission mineure localisée sur un dispositif (par exemple, un virus mis en quarantaine par un antivirus) : la responsabilité du traitement peut être déléguée au responsable du dispositif ;
- Détection d'une compromission importante localisée sur un dispositif ou étendue sur un système (par exemple, la présence d'un cryptomineur) : la responsabilité du traitement peut être déléguée au responsable métier avec une mise en place d'une surveillance accrue des dispositifs périmétriques ;
- Détection d'une compromission majeure pouvant mettre en péril l'ensemble des systèmes industriels et bureautiques (par exemple, rançongiciel généralisé) : le responsable sécurité prend en main la gestion de la réponse. Cette réponse pourrait impacter les systèmes non compromis avec leur mise en arrêt afin d'éviter une propagation de l'attaque.

Il est donc important de s'accorder sur les personnes portant la responsabilité du choix d'arrêt des systèmes en fonction du niveau de gravité des attaques pouvant survenir.

14.6.2 Génération des journaux

Lors de cette étape, il s'agira de configurer les dispositifs afin qu'ils génèrent les journaux. Il est recommandé d'utiliser les protocoles dédiés (observateurs d'événements ou syslog) afin d'éviter l'installation des agents de collecte sur les systèmes (notamment s'ils sont qualifiés). Parfois, pour les automates, des développements peuvent être nécessaires.

Les journaux générés devront être stockés localement sur les systèmes, mais également être centralisés. En effet, les journaux locaux peuvent être corrompus par l'attaquant. De plus, la centralisation des journaux permet leur mise en corrélation avec des événements survenus sur d'autres systèmes.

Le stockage local des journaux permet une analyse locale du système en cas de compromission de lui seul ou d'une compromission de l'infrastructure entière. Il est par ailleurs primordial de réaliser une étude afin de déterminer la durée de rétention des journaux pour ne pas surcharger les capacités de stockage local des systèmes.

Enfin, afin d'assurer une cohérence temporelle entre les différents journaux, il est nécessaire de mettre en place une infrastructure de synchronisation temporelle. L'ensemble des systèmes devront être synchronisés auprès de sources de temps de référence, internes au système d'information et cohérents entre elles.

14.6.3 Mise en place d'une infrastructure de collecte

Il est primordial de mettre en place une architecture de collecte des journaux afin de les centraliser dans des serveurs centraux aussi appelés « puits de logs ». Il faut ainsi étudier les flux à ouvrir, mais également le débit nécessaire pour réaliser cet acheminement des journaux, et l'espace de stockage requis pour ceux-ci.

En effet, des surcoûts sont possibles si les systèmes dont il faut récupérer les journaux sont isolés (étudier, donc, la fréquence de récolte des journaux, l'apport sécurité pour ce type de systèmes, etc.), mais également si la connectivité de ces systèmes au reste du réseau est limitée (connexion satellite, récupération sur site en physique par exemple).

L'architecture de collecte devra être sécurisée afin d'éviter une corruption des journaux, mais aussi afin que cette dernière puisse être un chemin de compromission des systèmes à surveiller (il est également possible d'étudier l'intérêt de surveiller des systèmes critiques isolés).

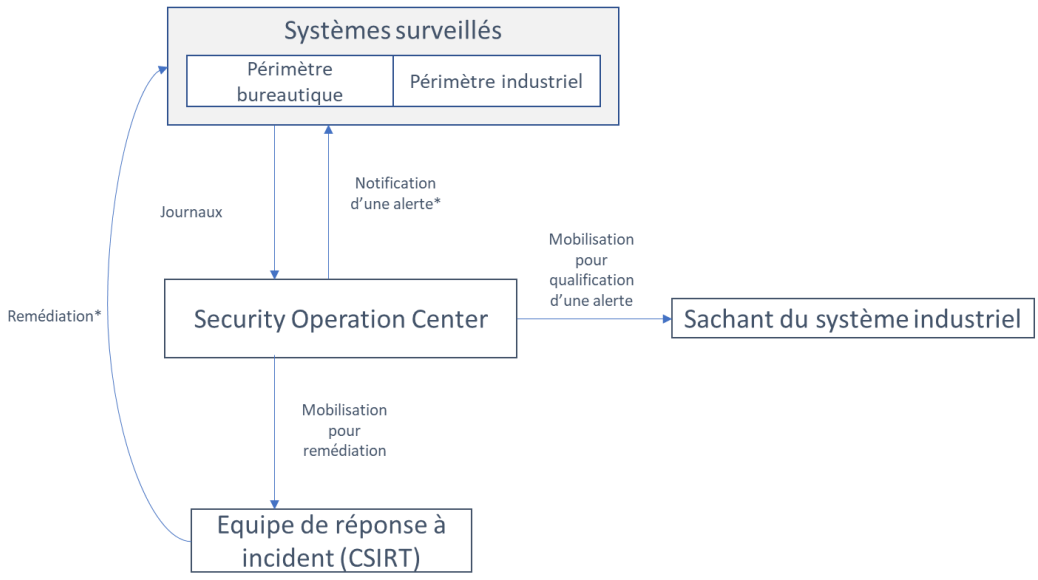
14.6.4 Configuration des systèmes d'analyse et mise en place d'une équipe de surveillance

Les journaux collectés dans le « puits de logs » alimentent un système d'analyse et de corrélation des journaux. Ces derniers, aussi appelés SIEM (Security Information and Event Management), sont chargés de normaliser les journaux collectés et de remonter des alertes lorsque des événements suspects ont été remontés selon un scénario défini. Il faudra ainsi configurer le SIEM conformément aux scénarios définis en amont.

Une équipe de surveillance devra ainsi être mise en place afin de traiter les alertes remontées par le SIEM. Cette équipe sera en charge des premières investigations basées sur les journaux récoltés, afin de filtrer les faux positifs, prioriser la réponse et mobiliser les acteurs adéquats pour les investigations plus poussées et le traitement de l'incident conformément au playbook. Certaines actions de réponse peuvent être automatisées à travers un SOAR (Security Orchestration, Automation and Response) : par exemple, envoi de mail, récupération d'informations depuis les postes, etc.

L'ensemble de cette organisation, sa gouvernance et les outils mis en place correspondent au SOC (Security Operation Center).

Afin de disposer d'exigences détaillées sur la mise en place d'une prestation de détection des incidents de sécurité, il est recommandé de prendre connaissance du référentiel de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) concernant les Prestataires de Détection d'Incidents de Sécurité (PDIS).



* Les conditions de remédiation et d'alerte sont à définir en amont et validée par les parties prenantes (responsable sécurité, responsable des opérations, etc.)

Figure 8. Représentation schématique d'un exemple de processus de traitement d'alerte cybersécurité

14.7 Qui est en charge de la mise en place d'une surveillance de la sécurité des systèmes industriels ?

La mise en place d'un système de surveillance est sous la responsabilité du responsable sécurité des systèmes industriels. Lors de la phase de construction, plusieurs acteurs seront mobilisés :

- Acteurs métiers afin d'identifier les scénarios redoutés dans le cadre de l'appréciation des risques ;
- Experts des systèmes permettant de correctement configurer les systèmes afin de générer les journaux ;
- Analystes SOC qui seront en charge de la configuration des outils de collecte et d'analyse des journaux ;
- Ingénieurs réseaux et infrastructure mobilisés dans le cadre de la mise en place de l'infrastructure de collecte des journaux.

Une fois le SOC mis en place, les analystes seront chargés d'assurer l'exploitation des systèmes et la mobilisation des différents acteurs dans le cadre d'une réponse à incident (responsable de maintenance, responsables métier, etc.).

Le SOC doit être sensibilisé au périmètre qu'il surveille (sensibilisation aux enjeux liés à la sécurité des systèmes industriels). Il faut qu'une personne avec des connaissances industrielles (sans que ce soit un analyste SOC industriel) soit mobilisable par le SOC à des fins d'investigation (par exemple, responsable de maintenance, exploitant). Un connaisseur du métier peut réaliser des analyses (pour identifier les faux positifs) et mettre en place les mesures correctrices. Il est également recommandé de sensibiliser les opérateurs, exploitants et responsables des systèmes industriels à la cybersécurité afin qu'ils puissent reconnaître les signes d'une attaque informatique et entreprendre les premières actions (communication aux responsables informatiques, déconnexion des postes, etc.).

Il peut être intéressant de disposer d'un SOC externe pour capitaliser sur leur vision du niveau de la menace en fonction des secteurs d'activités (connaissance d'attaques ciblant les énergéticiens, par exemple).

En revanche, il est nécessaire de s'assurer que la remontée des journaux se fait de façon sécurisée. Et il faudra également s'accorder sur les rôles et responsabilités des parties prenantes (quel est le point de contact côté industriel pour l'investigation poussée, qui est autorisé à isoler les systèmes, sur quels périmètres, etc.).

Enfin, il est possible de mettre en place un SOC hybride (interne et externe). Cette démarche est intéressante, car elle permet de disposer de compétences internes nécessaires à la contextualisation des incidents, mais également de compétences et expertises externes permettant la capitalisation sur les incidents touchant le secteur d'activité avec la capacité de réaliser des astreintes (24x7).

La sélection du type de SOC (interne, externe ou hybride) est à déterminer en fonction des compétences à disposition en interne, du niveau de maturité, ainsi que des ressources financières à disposition.

15 Annexes

15.1 Détails des tests à réaliser en intégration et recette de sécurité

Le cahier de recette spécifiera la liste des essais pouvant être réalisés durant les phases de :

- FAT uniquement ;
- SAT uniquement ;
- FAT et en SAT.

De même que pour les essais fonctionnels, il est nécessaire de s'interroger sur les impacts de toute correction appliquée en cas de non-conformité observée (traitement de la non-régression). Une correction d'une vulnérabilité de sécurité peut entraîner une anomalie fonctionnelle (ex. : paramétrage d'un pare-feu).

15.1.1 Prérequis

La phase de développement informatique doit être terminée, la plateforme de recette-usine doit être isolée du réseau de développement.

15.1.2 Fonctions applicatives de sécurité

Les essais suivants peuvent être réalisés sur la plateforme de recette.

Les tests à réaliser doivent permettre de s'assurer du bon fonctionnement et de la complétude de la fonction. Certains tests peuvent être réalisés par échantillonnage :

- Test de valeurs et de fonction par rapport aux droits accordés ;
- Test des valeurs limites (saisie de valeurs au-delà des valeurs attendues) ;
- Test de valeurs inattendues ;
- Test de fonctions simultanées inattendues ;
- Test de variations de valeurs régulières inattendues ;
- Revue de code ;
- etc.

Ces tests peuvent être appliqués aux :

- Paramètres et consignes d'entrée (API) ;
- Alarmes et défauts ;
- Fonctions de base ;
- Actionneurs en marche manuelle ;
- Séquences automatiques process ;
- Communications :
    - Communication inter-automate,
    - Autres communications.
- Fonctions non-process : « utilités » ;
- Horodatage des équipements ;
- etc.

15.1.3 Infrastructures

Les essais suivants peuvent être réalisés sur la plateforme de recette, si celle-ci correspond à la plateforme finale de production qui sera déployée sur site.

Les tests à réaliser doivent permettre de s'assurer de la bonne configuration et du bon paramétrage en matière de sécurité des différents composants mis en œuvre, notamment :

- L'absence de vulnérabilité connue (obsolescence en matière de patch sécurité) ;
- L'absence de configuration par défaut ;
- La mise en œuvre du strict nécessaire en matière de fonctions ;
- La prise en compte de la sécurité dans l'architecture.

15.1.3.1 Protection des flux

- Absence de protocole non sécurisé (Telnet, HTTP, etc.) ;
- Chiffrement des flux sur Internet (HTTPS) ;
- Chiffrement des flux sur IP (protocole Ipsec…) ;
- Chiffrement des flux entre certaines zones.

15.1.3.2 Sauvegardes

- Dispositif de sauvegarde automatique ;
- Dispositif de sauvegarde hors-ligne ;
- Dispositif de restauration ;
- Protection des données ;
- etc.

15.1.3.3 Protection contre les infections informatiques

- Mécanismes de restriction logicielle (afin de restreindre l'exécution des programmes d'un poste à une liste de programmes dûment autorisés : liste blanche) ;
- Dispositifs de déploiement de patchs ;
- Dispositifs d'alerte virale ;
- etc.

15.1.3.4 Alertes

- Dispositif de détection ;
- Dispositif d'alarme ;
- Dispositif d'enregistrement et de gestion des journaux ;
- etc.

15.1.3.5 Poste de travail (opérateurs, utilisateurs du système)

- Version OS et patch management ;
- Durcissement de la configuration ;
- Protection de l'antivirus ou EDR ;
- Limitation des ports physiques externes ;
- Gestion des supports amovibles ;
- Absence de compte par défaut ;
- Limitation des services non utiles ;
- Absence de mot de passe par défaut ;
- Gestion des sessions ;
- etc.

15.1.3.6 Poste de développement (plateforme de test, de préproduction)

- Version OS et patch management ;
- Durcissement de la configuration ;
- Protection de l'antivirus ;

- Limitation des ports physiques externes ;
- Gestion des supports amovibles ;
- Absence de compte par défaut ;
- Limitation des services non utiles ;
- Absence de mot de passe par défaut ;
- Gestion des sessions ;
- Absence de données de production ou de données sensibles ;
- etc.

15.1.3.7 Poste de travail Administrateur

- Version OS et patch management ;
- Durcissement configuration ;
- Protection de l'antivirus ;
- Limitation des ports physiques externes ;
- Gestion des supports amovibles ;
- Absence de compte par défaut ;
- Limitation des services non utiles ;
- Absence de mot de passe par défaut ;
- Chiffrement des flux ;
- Cloisonnement avec un PVLAN dédié ;
- Gestion des sessions ;
- etc.

15.1.3.8 Serveurs

- Version OS et patch management ;
- Durcissement de la configuration ;
- Protection de l'antivirus ;
- Limitation des ports physiques externes ;
- Absence de compte par défaut ;
- Absence de mot de passe par défaut ;
- Limitation des services non utiles ;
- etc.

15.1.3.9 Base de données

- Patch management ;
- Durcissement du logiciel de base de données (limitation des droits, options de sécurité retenues…) ;
- Absence de compte par défaut ;
- Absence de mot de passe par défaut ;
- etc.

15.1.3.10 Équipements réseau

- Vérification des conditions d'usage prescrites par le fabricant ou par la certification associée ;
- Limitation des ports physiques externes ;
- Désactivation des ports non utilisés ;
- Limitation de machine par port (ex. : port-security) ;
- Détection de connexion/déconnexion ;
- Absence de compte par défaut ;
- Absence de mot de passe par défaut ;
- Limitation des services non utiles ;
- etc.

15.1.3.11 Automates

- Limitation des ports physiques externes ;
- Absence de compte par défaut ;
- Absence de mot de passe par défaut ;
- Limitation des services non utiles ;
- Désactivation des fonctions de maintenance ;
- Cloisonnement du réseau de terrain ;
- etc.

15.1.3.12 Cloisonnement

- Cloisonnement vis-à-vis d'Internet ;
- Cloisonnement interne SI opérationnel ;
- Cloisonnement SI de gestion ;
- Etc

15.1.4 Environnement

Les tests à réaliser doivent permettre de s'assurer que les paramètres d'environnement des bâtiments, locaux techniques, salles serveurs, salle d'exploitation, etc., hébergeant les ressources des systèmes sont conformes.

15.1.4.1 Câblage

- Identification ;
- Cahier de câblage ;
- Solidité des connexions/borniers ;
- Cheminement extérieur ;
- Séparation courant faible/courant fort ;
- Accessibilité maîtrisée des prises de connexion ;
- etc.

15.1.4.2 Local d'hébergement SI

- Robustesse des murs ;
- Robustesse des ouvrants ;
- Contrôle d'accès physique ;
- Détection intrusion ;
- Vidéosurveillance ;
- Détection humidité ;
- Détection incendie ;
- Faux plancher/faux plafond ;
- Fermeture des baies techniques ;
- Extinction feu ;
- Cheminement canalisation ;
- etc.

15.1.4.3 Locaux techniques

- Robustesse des murs ;
- Robustesse des ouvrants ;
- Contrôle d'accès physique ;
- Détection intrusion ;
- Vidéosurveillance ;
- etc.

15.1.4.4 Locaux d'exploitation

- Contrôle d'accès physique ;
- Détection intrusion ;
- Vidéosurveillance ;
- Détection incendie ;
- Extinction feu ;
- Cheminement canalisation ;
- etc.

15.1.4.5 Utilities

- Redondance alimentation ;
- Secours (onduleur) ;
- Secours (Groupe) ;
- Climatisation ;
- etc.

15.1.5 Performances

La réalisation de ces essais peut nécessiter l'utilisation d'outils spécifiques.

15.1.5.1 Respect des exigences en termes de charge

Ces essais consistent à vérifier que le système reste disponible dans les conditions d'usage extrêmes décrites dans le cahier des charges (nombre de transactions par seconde, nombre d'équipements connectés, etc.).

15.1.5.2 Tests d'intrusion

Ces essais consistent à détecter les vulnérabilités résiduelles d'un équipement ou de l'ensemble de l'installation.

15.1.6 Procédures et modes opératoires de sécurité

Les tests à réaliser doivent permettre de s'assurer de l'existence, de la complétude et de l'efficience des principales procédures et modes opératoires de sécurité suivants :

Cible des tests	Description
Procédure de gestion des privilèges des utilisateurs	Attribution, modification et révocation des droits d'accès selon les rôles et responsabilités (gestion des comptes à privilèges, application du principe du moindre privilège, traçabilité des élévations de droits…)
Procédure de surveillance	Surveillance des événements de cybersécurité (modification des règles d'administration, corrélation des alertes de sécurité…)
Procédure d'alerte	Signalement des incidents de sécurité
Procédure de connexion à distance	Règles à respecter par les utilisateurs ou systèmes souhaitant disposer d'une connexion à distance (VPN…)
Procédure de maintien en conditions opérationnelles et de gestion de l'obsolescence	Suivi de l'état des systèmes et applications pour garantir leur bon fonctionnement (mise à jour des correctifs de sécurité, supervision de l'état des composants critiques, planification du remplacement des éléments obsolètes…)
Procédure d'entrée/sortie	
Procédure de gestion des interventions sur le système	Encadrement des actions de maintenance ou d'administration, internes ou externes (planification des interventions, traçabilité des opérations réalisées, supervision des prestataires, validation des changements en environnement de production…)
PCA/PRA	Organisation des mesures pour assurer la continuité ou la reprise des activités en cas d'incident majeur
Procédure d'homologation	Évaluation de la conformité du système d'information avant sa mise en service ou son évolution (analyse de risques, vérification des exigences de sécurité, validation par l'autorité compétente, formalisation de la décision d'homologation…)
Procédure spécifique de formation et de qualification des utilisateurs et administrateurs	Procédures liées aux équipements spécifiques déployées dans le cadre du système

15.2 Acronymes

ALARP	As low as reasonably practicable
ANSSI	Agence nationale de la sécurité des systèmes d'information
AR	Appréciation des risques
BDD	Base de données
CERT	Computer emergency response team
CIM	Computer integrated manufacturing
CMDB	Configuration management database
CNIL	Commission nationale de l'informatique et des libertés
CPU	Central processing unit
CRM	Customer relationship management
DCS	Distributed control system
DMZ	Demilitarized zone
DPO	Délégué à la protection des données
EBIOS	Expression des besoins et identification des objectifs de sécurité
ERP	Enterprise ressource planning
FAT	Factory acceptance test
FDA	Food & Drug Administration
FW	Firewall
HMI	Human machine interface
IDS	Intrusion detection system
IEC	International electrotechnical commission
IP	Internet protocol
IOT	Internet of things (Internet des objets)
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information technology
LDAP	Lightweight directory access protocol
LPM	Loi de programmation militaire
MAC	Media access control
MCO	Maintien en conditions opérationnelles
MCS	Maintien en conditions de sécurité
MES	Manufacturing execution system
MOA	Maîtrise d'ouvrage
MOE	Maîtrise d'œuvre
NDA	Non nisclosure agreement
NIS	Network and information security

OPEX	Operational expenditure
OT	Operational technology
PAS	Plan d’assurance sécurité
PCA	Plan de continuité d’activité
PERA	Purdue enterprise reference architecture
PID	Process instrumentation diagram
PRA	Plan de reprise d’activité
PSSI	Politique de sécurité des systèmes d’information
RACI	Responsible, accountable, consulted, informed
RAM	Random access memory
RGPD	Règlement général sur la protection des données
RSSI	Responsable de la sécurité des systèmes d’information
RTU	Remote terminal unit
SAT	Site acceptance test
SCADA	Supervisory control and data acquisition
SI	Système d’information
SIEM	Security information and event management
SIIV	Système d’information d’importance vitale
SOC	Security operation center
USB	Universal serial bus
VLAN	Virtual LAN
VPN	Virtual private network
WAN	Wide area network
WMS	Warehouse management system

Campus Cyber
Tour Eria
5 rue Bellini
92800 Puteaux

France

✆ +33 1 53 25 08 80

clusif@clusif.fr

clusif.fr