LES DOSSIERS TECHNIQUES

GUIDE CYBERSECURITE DES SYSTEMES INDUSTRIELS

Février 2021

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 :

Les responsables du groupe de travail :

Hervé	**SCHAUER**	HS2
Ilias	**SIDQUI**	Wavestone

Les contributeurs :

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 adhérents** ayant participé à la relecture.

I. 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 que le Panorama des référentiels de sécurité[2], dont la dernière mise à jour a été publiée en 2019.

[1] https://clusif.fr/publications/fiches-incidents-cyber-industriels-2017/
[2] https://clusif.fr/publications/panorama-des-referentiels-2eme-edition-2/

II. 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 au final 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 incompréhension de l'intérêt de ces mesures avec parfois même un abandon pur et simple de ces mesures.

II.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, où 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 venant 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 aux personnes issues du monde de l'automatisme avec des connaissances limitées sur la sécurité des systèmes d'information.

II.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 :

- cartographie des systèmes industriels ;
- appréciation des risques cyber ;
- architecture sécurisée ;
- intégration et recette de sécurité ;
- maintien en conditions de sécurité.

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.

II.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.

II.3.1. Cycle de développement d'un système industriel

Tout d'abord, il a été convenu que la conception d'un système industriel suit habituellement un cycle en V. Les méthodologies de conception agiles existent en milieu industriel, elles restent néanmoins moins présentes au vu notamment des 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.

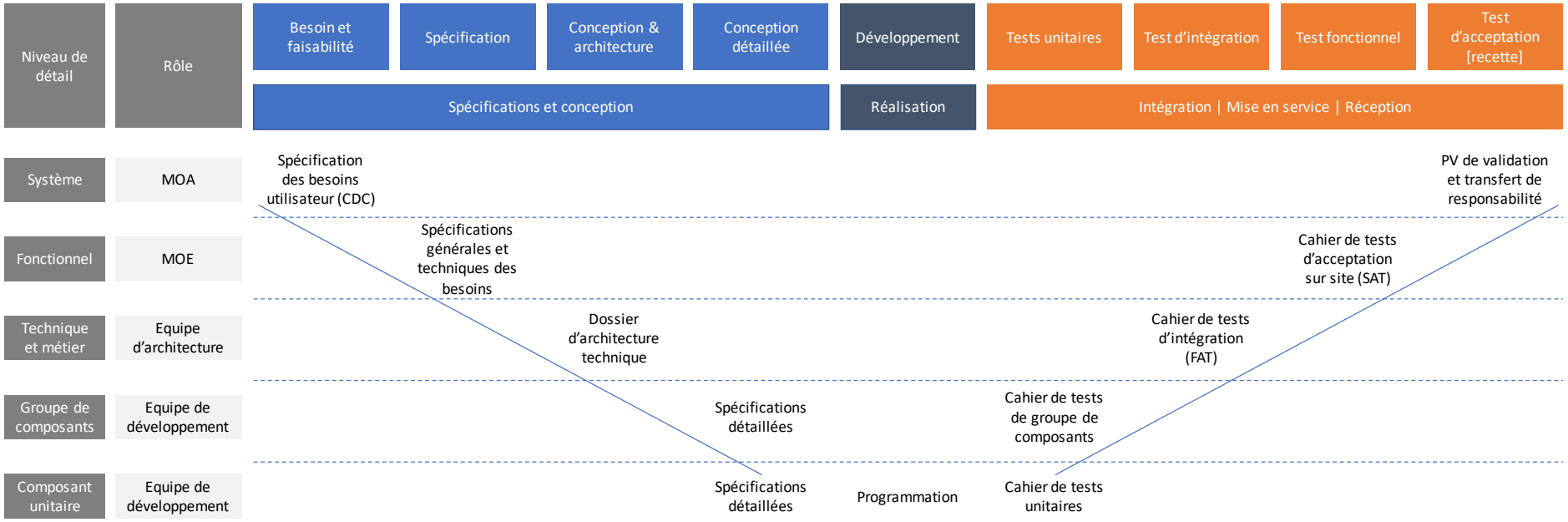

Figure 1. Étapes et principaux livrables d'un développement en cycle en V

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.

II.3.2. Sûreté 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 remplir les fonctions pour lesquelles il a été conçu. 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 industrielle, du point de vue de la sûreté de fonctionnement, est la capacité du système de ne pas provoquer d'incidents mettant en danger la santé des personnes, des biens ainsi que l'environnement.

La définition et la mise en œuvre des mesures visant à réduire le risque du point de vue de la sûreté 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 sûreté de fonctionnement), il a été convenu de désigner la « sécurité industrielle » par safety dans la suite du document.

III. Sécurité des systèmes d'information

La sécurité des systèmes d'information consiste en l'étude des vulnérabilités impactant un système afin de définir et 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.

Le champ d'application de la sécurité 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.) ;
  - rédaction 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 ;
  - serveurs et réseau d'administration ;
  - infrastructure de déploiement des mises à jour ;
  - architecture sécurisée pour les accès distants.

[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

- **Dossier de spécifications détaillées** : ce dossier doit inclure a minima les spécifications des équipements réseau et de sécurité de type :
  - pare-feu ;
  - 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 suite aux différents tests.

Une attention particulière devra être portée sur les documents cités plus haut, mais également sur 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.

IV. Inventaire et cartographie

IV.1. Que signifie « inventaire et cartographie » ?

IV.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 métadonnées permettant de les caractériser et les identifier, par exemple, le modèle, la référence, la version logicielle ou la localisation géographique.

IV.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 ; ou
- 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 : en particulier la cartographie peut représenter les flux et les positions physiques d'éléments, ou de groupes d'éléments, de l'inventaire.

IV.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 évaluer les impacts des interventions ;

- 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.

IV.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 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.

IV.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 peuvent 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).

IV.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 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 interconnections peuvent être facilement accessibles, comme dans le cas d'un réseau de téléphonie mobile, un réseau sans fil ou 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 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[4] 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

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

le modèle en couches CIM et qui permettent de structurer la cartographie. De même, de nouveaux objets ou attributs peuvent aussi être ajoutés à l'inventaire pour représenter les flux de matière, la redondance, les chemins alternatifs ou le sens d'initiation de la communication, par exemple.
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}.

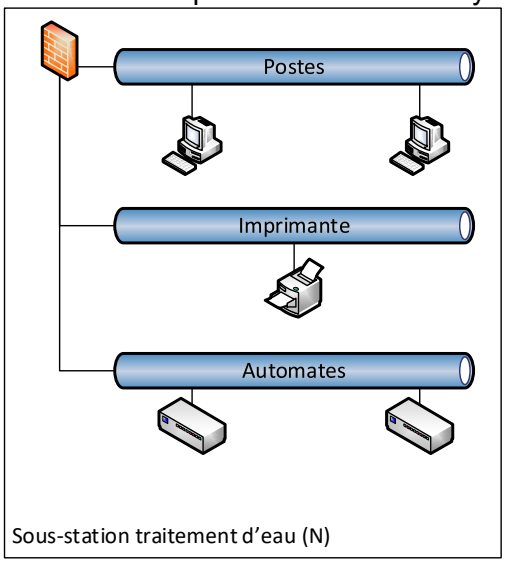

Figure 2. Représentation générique unitaire

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

IV.4. Quand est-il recommandé de réaliser un inventaire et une cartographie ?

IV.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 les plus sensibles, 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…), 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 VII « Intégration et recette de cybersécurité »).

IV.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.

IV.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, en impliquant les parties prenantes. Il s'agit là d'un enjeu de cybersécurité (capacité à analyser et 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.

IV.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).

IV.5. Quel est le coût de réalisation d'un inventaire et une cartographie ?

IV.5.1. Outils

IV.5.1.a. 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 non une représentation graphique : certains acteurs du service s'appuient sur ces outils pour réaliser des prestations d'inventaire et de cartographie.

IV.5.1.b. 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.

IV.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-feu 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 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.

IV.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 prévoir 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®.

IV.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 réalisés en externe, des ressources internes seront nécessaires pour mener à bien ce projet.

IV.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 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 le 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 toute 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 d'autre part, en cas d'indisponibilité du système, les informations qu'elle contient restent disponibles aux équipes de remédiation.

IV.7. Qui est en charge de la réalisation de l'inventaire et 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 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.

V. Appréciation des risques cyber

V.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, comprendre les facteurs clés de succès, et 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). Le lecteur qui souhaite une introduction aux principes d'analyse de risques et aux différentes méthodes générales est invité à consulter le document du groupe de travail « Méthodes » du Clusif intitulé « Gestion de risques[5] ».

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).

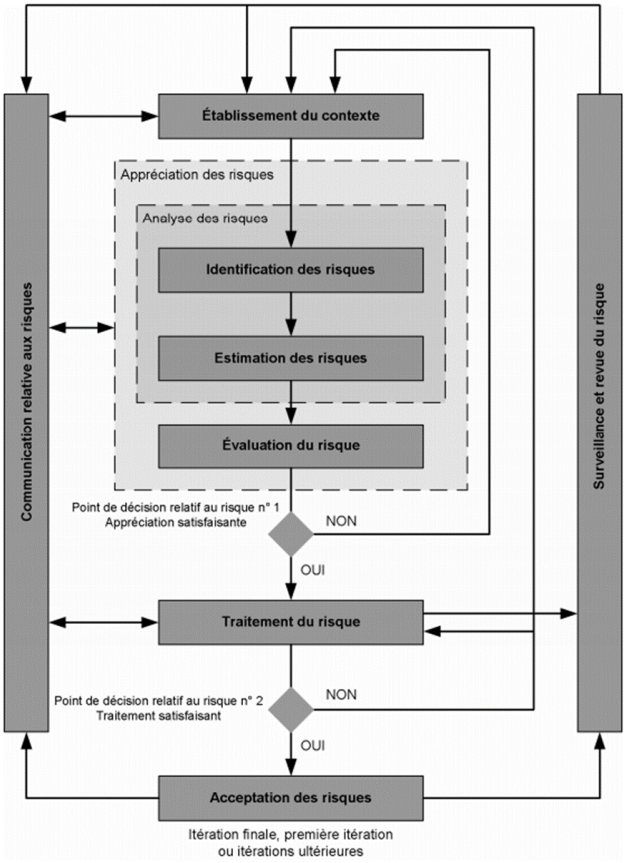

Figure 3. Schéma représentant un processus d'AR extrait de la norme ISO 27005

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).

[5] En cours de rédaction à la date de publication de ce document.

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 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 à ce 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 appliquer les mesures de sécurité correspondantes. Ce genre d'approches se veut « proportionné » 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).

V.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 rétrohomologation 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.

V.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).

V.4. Quand est-il recommandé de réaliser une appréciation des risques ?

Idéalement, l'AR doit être menée le plus en amont possible, soit 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 IV « Inventaire et cartographie »). Si la cartographie disponible est trop grossière ou non fiable, une macro-AR — comme indiqué dans le chapitre V.1 « 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 aient été appliqués (ou en anticipant l'application des mesures correspondantes), pour des raisons d'efficacité, un peu comme les méthodes hybrides évoquées précédemment.

V.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 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 VI « 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, 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 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).

V.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.

V.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 veut comparer les résultats d'analyses entre sites par exemple, l'achat ou le développement d'un tel outil est fréquent.

V.6. Comment réaliser une appréciation des risques ?

V.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…).

V.6.1.a. 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 rajoutant 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).

V.6.1.b. 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.

V.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, adapter ou compléter les critères et métriques en vigueur au sein de l'organisme (cf. fonction gestion des risques ou audit interne, selon organigramme).

V.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 compréhensibles 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.

V.6.3.a. 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, i.e. 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 ». 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 les négligences, car les erreurs et défaillances matérielles sont pour l'essentiel déjà couvertes par la sécurité fonctionnelle. Il est aussi possible de rajouter 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 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, à savoir en évitant de dépasser la trentaine de scénarios de risques.

L'évaluation du risque va consister à évaluer :

- **d'une part, la vraisemblance du scénario de risque** : 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.

V.6.3.b. 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, 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 soit avec une approche :

- quantitative : par exemple, lier 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).

V.6.3.c. 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.

V.6.3.d. 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).

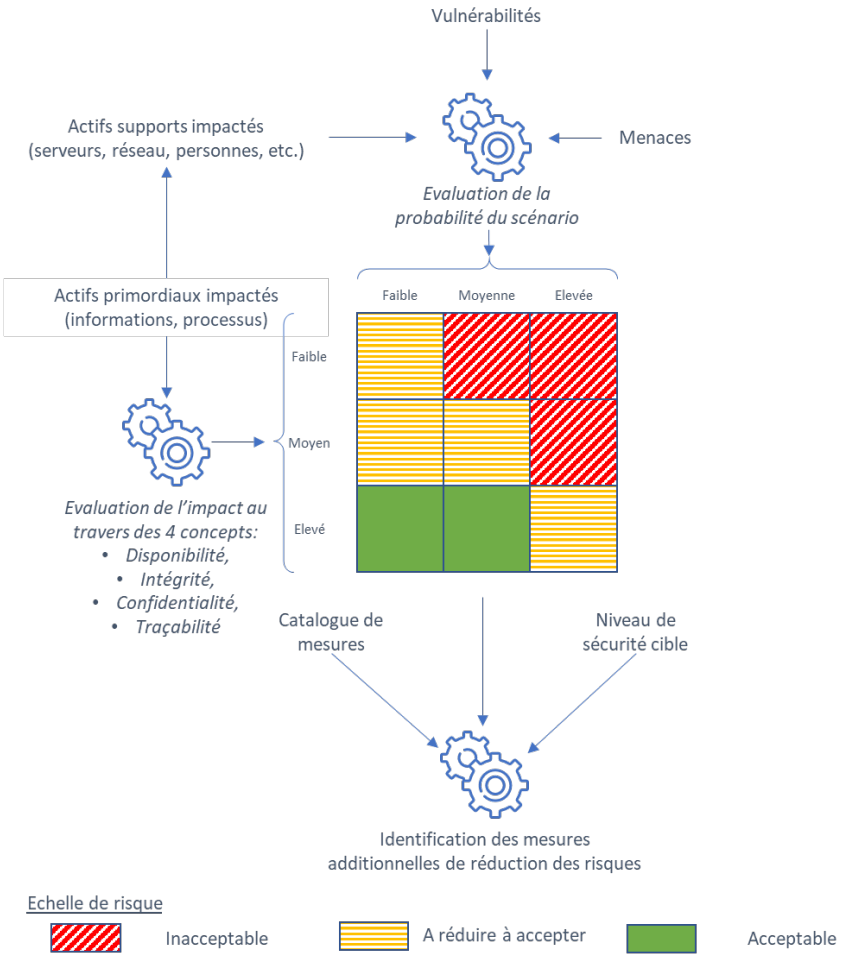

Figure 5. Principes de matrice de risques

V.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).

V.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[6], NIST Cybersecurity framework aux États-Unis, CPNI au Royaume-Uni, guides ANSSI en France, etc.)[7].

Il est nécessaire ici 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. chapitreVIII « 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 souvent est supérieur en montant actualisé au coût d'investissement.

[6] 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).

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

V.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, ou qui sont acceptables à court terme. Ces risques doivent alors faire l'objet d'une acceptation formelle, éventuellement pour une durée limitée, au titre des risques résiduels.

V.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 d'inclure, a minima, une séance de restitution (pré restitution en cercle restreint, séance plénière auprès d'une audience plus large, etc.) visant à la fois à démontrer la rigueur de la démarche employée et la pertinence des résultats obtenus et des recommandations. 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.

V.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.

V.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, 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 risque de sanction pénale ou non en cas de manquement.

VI. Architecture sécurisée

VI.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 au travers de la mise en œuvre de mesures de sécurité.

VI.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 propagation d'une infection 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. 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.

VI.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 ;
- les interconnexions avec les systèmes externes ;
- les systèmes sans-fils.

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 V « Appréciation des risques cyber »).

VI.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 rétrohomologation de la cybersécurité ou d'une évolution fonctionnelle majeure par exemple).

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 figée 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 V « Appréciation des risques cyber » et VIII « Maintien en conditions de sécurité ».

VI.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.

VI.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.

VI.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 « VI.3. 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.

VI.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.

VI.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 du public ou pas. 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 supervision (SCADA, DCS, etc.) ;
- système de contrôles des processus industriels (WMS, MES, etc.) ;
- systèmes de gestion (ERP, CRM, etc.).

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

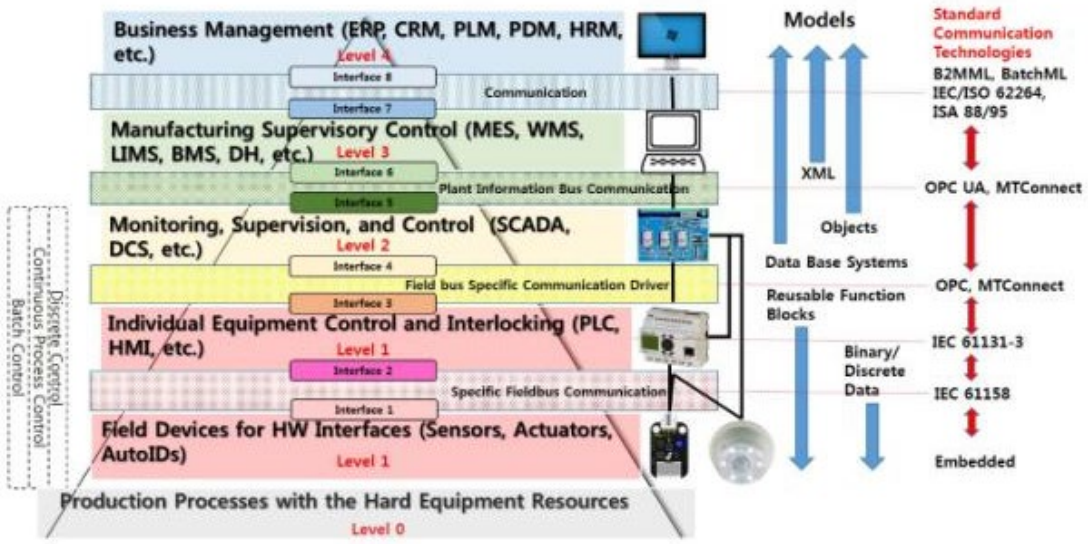

Figure 6. Modèle d'architecture fonctionnelle aligné sur le standard ISA-95/IEC 62264

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. Par exemple, une fonction pouvant compromettre le système de production est 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 afin d'éviter de complexifier l'architecture.

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

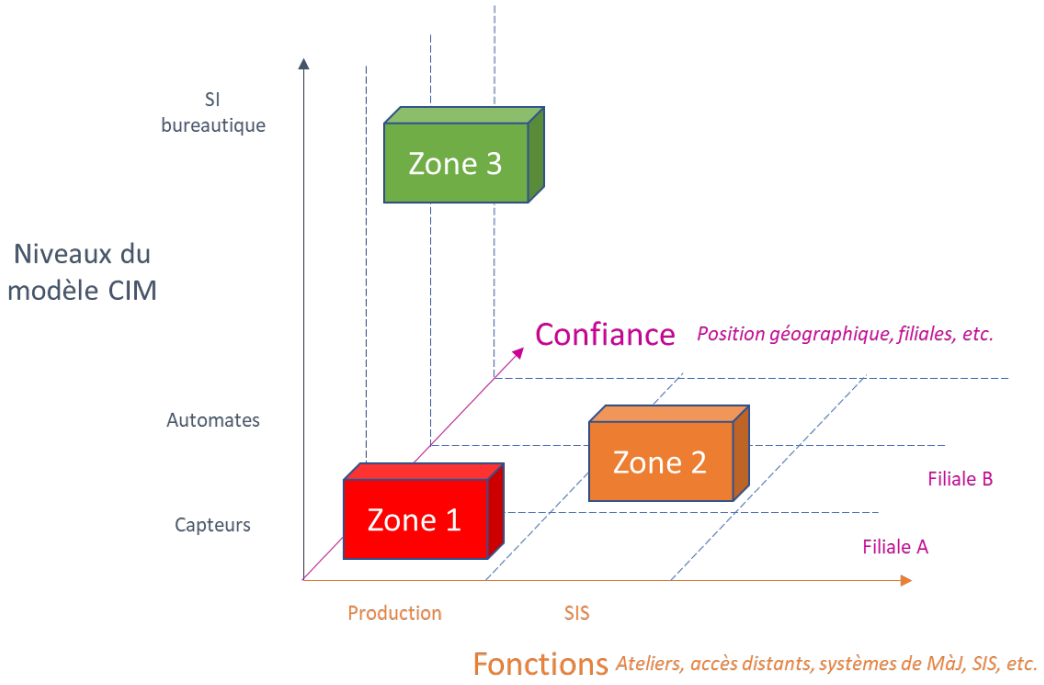

Figure 7. Représentation graphique de la méthodologie de construction des regroupements de ressources

VI.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-feu, double 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 informatique 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 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 source des flux ;
- mise en place de sondes d'analyse des flux afin de détecter des attaques ;
- mise en place de serveurs ou 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 criticité différente ;
- mise en place de mécanismes de chiffrement des flux (VPN) ;
- mise en place d'une solution de sécurisation des accès distants ;
- 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

VI.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, il est possible de noter :

- 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 ;
- etc.

VI.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.

VII. Intégration et recette de cybersécurité

VII.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 capacité de résister aux scénarios d'attaques identifiés dans l'analyse de risques.

VII.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 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 va donc se focaliser sur la méthode pour réaliser cette intégration et recette de cybersécurité.

De même, le document La cybersécurité des systèmes industriels – Mesures détaillées de l'ANSSI fournir 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.

VII.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 III « 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.

VII.4. Quand faut-il réaliser une intégration et recette de cybersécurité ?

Les phases d'intégration, mise en service et 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.

VII.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, suivant 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.

VII.6. Comment réaliser une intégration et recette de cybersécurité ?

VII.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 IV « Inventaire et cartographie ») ;
- les notices techniques de chaque appareil du système industriel ;
- des fiches de paramétrage ou configuration de chaque appareil du système industriel.

Outre les tests de cybersécurité de base liés à la programmation et 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 qui peut être :

- 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 (interréseaux, accès vers Internet, liaisons sans fils, 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, 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 de déclaration CNIL ;
- 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 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.

VII.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 (exemple : utilisation de bouchons ou simulateurs en plateforme de recette, et essais d'ensemble avec les vrais systèmes en plateforme de production).

VII.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 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.

VII.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 (handover) 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.

VIII. Maintien en conditions de sécurité

VIII.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 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, comme un arrêt de production dû a un incident de sécurité. 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 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.

VIII.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.). Par contre, la maintenance en conditions de sécurité est relativement peu prise en considération : en effet, en partant du principe qu'une fois un système informatique industriel est mis en production et que le process associé a été réceptionné et validé, il ne convient plus de le modifier 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 cours 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 déclinant 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.

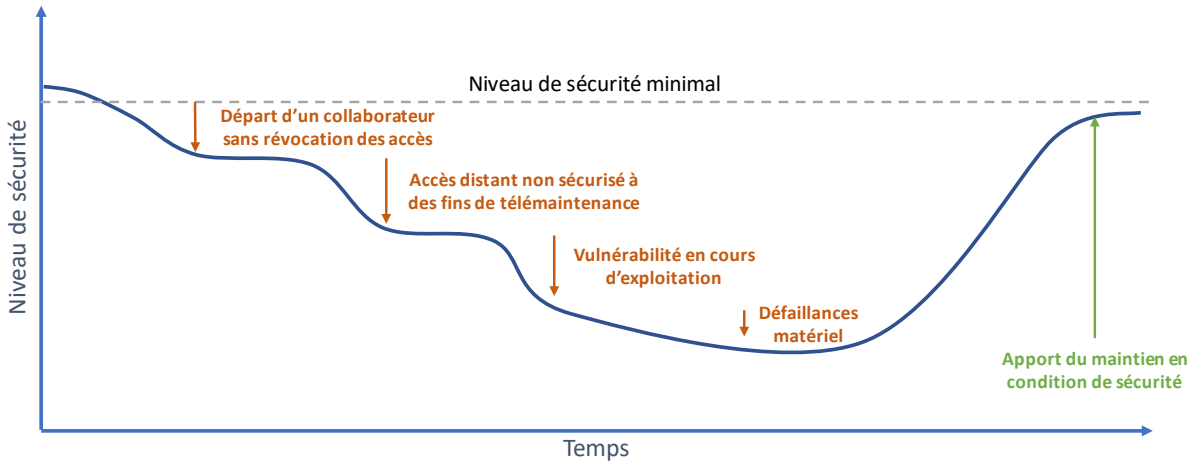

Figure 8. Représentation schématique de l'évolution du niveau de sécurité d'un système au cours du temps

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 V « 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 suite au 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 aussi réaliser les actions de sécurité identifiées. Ces actions permettront de réduire la probabilité d'une panne dont la cause est un incident de sécurité.

VIII.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 chapitreVI « 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 de nouvelles menaces). Les audits et contrôles de conformité permettront d'évaluer l'efficacité du MCS (évaluation vis-à-vis du niveau de sécurité).

VIII.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).

VIII.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).

VIII.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 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 peuvent avoir lieu de façon urgente et donc des procédures de maintenance immédiates pourraient être définies.

VIII.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 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, par exemple lors de l'intégration d'un nouveau système, 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.

VIII.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 méconnaissance des utilisateurs est le vecteur le plus souvent utilisé par les attaquants pour compromettre un système industriel. Une sensibilisation des utilisateurs quant 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 dans 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 chapitreV), la conduite d'une analyse de risques permet d'évaluer les risques bruts et 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 IV), 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 peuvent avoir un impact sur la production (par exemple pour l'installation de mises à jour de sécurité). Afin d'anticiper et 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 VI), 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 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 soient limités (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 facilement intégrer et se propager au sein d'un système industriel. 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 ne 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 quant 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 (par exemple 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.

VIII.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.

IX. Annexes

IX.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).

IX.1.1. Prérequis

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

IX.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 (supervision vers API) ;
- alarmes et défauts ;
- fonctions de base : Typicals ;
- actionneurs en marche manuelle ;
- séquences automatiques process ;
- communications :
  - communication interautomate,
  - autres communications ;
- autres communications ;
- fonctions non-process : « utilités » ;
- horodate des équipements ;
- etc.

IX.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.

IX.1.3.a. 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.

IX.1.3.b. Sauvegardes

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

IX.1.3.c. 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.

IX.1.3.d. Alertes

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

IX.1.3.e. Poste de travail (opérateurs, utilisateurs du système)

- 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 ;
- Etc.

IX.1.3.f. 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.

IX.1.3.g. 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.

IX.1.3.h. 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.

IX.1.3.i. 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.

IX.1.3.j. 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.

IX.1.3.k. 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 ;
- Etc.

IX.1.3.l. Cloisonnement

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

IX.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.

IX.1.4.a. Câblage

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

IX.1.4.b. 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.

IX.1.4.c. Locaux techniques

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

IX.1.4.d. Locaux d'exploitation

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

IX.1.4.e. Utilities

- Redondance alimentation ;
- Secours (onduleur) ;

- Secours (Groupe) ;
- Climatisation ;
- Etc.

IX.1.5. Performances

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

IX.1.5.a. 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.).

IX.1.5.b. Tests d'intrusion

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

IX.1.6. Procédures et modes opératoires de sécurité

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

Cible des tests	Description
Procédure de gestion des privilèges des utilisateurs	
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	
Procédure d'entrée/sortie	
Procédure de gestion des interventions sur le système	
PCA/PRA	
Procédure d'homologation	
Procédure spécifique de formation et de qualification des utilisateurs et administrateurs	Procédures liées aux équipements spécifiques déployées dans le cadre du système

IX.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 Disclosure 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

IX.3. Table des illustrations

IX.4. Table des références

L'ESPRIT D'ÉCHANGE

11 rue de Mogador

75009 Paris

France

✆+33 1 53 25 08 80

clusif@clusif.fr

Téléchargez toutes les productions du Clusif sur

www.clusif.fr