RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

APPROCHE SSI POUR L'INTERNET DES OBJETS INDUSTRIELS

ANSSI-PG-109
30/05/2025

PUBLIC VISÉ :

Développeur **Administrateur** **RSSI** **DSI** Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI s'intitule **« Approche SSI pour l'Internet des objets industriels »**. Il est téléchargeable sur le site `cyber.gouv.fr`.

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

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	30/05/2025	Version initiale

Table des matières

1
Introduction

L'Internet industriel des objets (ou *Industrial Internet of Things*, abrégé en IIoT en anglais) est un terme générique désignant une « infrastructure industrielle d'entités, de personnes, de systèmes et de sources d'informations interconnectés ensemble et proposant des services qui traitent les informations provenant du monde physique et du monde virtuel et qui réagissent à ces informations » (ISO 24591-1 :2024, 3.1.7). Dans la pratique, ce terme reflète une captation accrue des données sur le terrain et leur valorisation au moyen de systèmes de traitement automatisés de masse.

Cette valorisation des données IIoT se fait au travers de nouveaux usages, qui dépassent le périmètre historique de l'usine :

- en important des usages d'une industrie à l'autre, par exemple, la maintenance prédictive pour des industries qui ne bénéficiaient pas de la structure technologique permettant un tel usage ;
- en exploitant de nouveaux procédés de traitement (ex. : *deep learning*, intelligence artificielle) sur de nouveaux ensembles de données, notamment l'ajout de traitement par corrélation de données issues de capteurs variés et précédemment incompatibles ;
- en incluant les données IIoT dans des modèles de simulation ou de recherche et développement, notamment pour améliorer et éprouver les méthodes de l'industrie de manière transverse ;
- en donnant accès aux données à une population externe à l'usine, par exemple pour l'aide à la décision lors d'opérations boursières (ex. : spéculation sur le marché de l'électricité) ;
- en revendant les données IIoT.

En plus de la valorisation des données, on constate l'apparition de systèmes commandés depuis des infrastructures distantes non industrielles et sur la base d'algorithmes complexes (calcul statistiques, IA, etc.) via l'utilisation de consignes intelligentes permettant, par exemple :

- la reconfiguration des lignes de production basée sur une estimation prédictive des commandes ;
- l'optimisation de la production d'énergie basée sur une analyse prédictive du marché de l'énergie ;
- l'optimisation des coûts d'installation et de maintenance par le déport des calculs dans des infrastructures distantes, qui ne laissent que des modules d'entrée/sortie déportés dans l'usine.

L'IIoT génère suffisamment de valeur pour justifier son déploiement dans les usines (nouvelles ou existantes) et son avènement fait évoluer les concepts fondamentaux d'une usine et de son système d'information. Sans préjuger de la pertinence de ce nouveau socle technologique, l'IIoT s'impose doucement dans les usines et dans les métiers. Plus particulièrement, il n'est pas exclu qu'à l'usage, les procédés industriels [1] deviennent dépendants de l'IIoT [2].

1. L'IEC62443 défini un processus industriel comme une série d'opérations effectuées lors de la fabrication, du traitement ou du transport d'un produit ou d'un matériau

2. C'est le cas de systèmes « utilitaires » (*utilities*), souvent classifiés de faible criticité mais nécessaires au bon fonctionnement de l'usine, par exemple le système de traitement des eaux usées d'une usine de fabrication de textile.

Ces nouveaux usages induisent une modification des risques SSI (sécurité des systèmes d'information) pesant sur les systèmes industriels. Ces systèmes sont susceptibles d'être (i) la cible d'attaques à but lucratif par des groupes cybercriminels menant des actions de masse et (ii) la cible d'attaques à but d'espionnage ou de déstabilisation de groupes d'attaquants appuyés par des États. Ces menaces doivent être prises au sérieux d'autant qu'elles sont soutenues dans le temps. L'IIoT offre une surface d'attaque supplémentaire pour ces attaquants. Il convient donc d'adopter une approche SSI dans les choix d'utilisation et de déploiement.

Ce document, présenté lors de la conférence C&ESAR23 [3], propose une approche SSI pour l'IIoT dans le domaine industriel [4] en se focalisant sur l'usine de production. Cependant, les axes explorés peuvent être transposés à d'autres contextes industriels, tel que les systèmes géographiquement étendus ou la logistique.

3. *Cybersecurity Approach Proposal for the IIOT* – https://2023.cesar-conference.org/detailed-program/

4. Les recommandations relatives à la sécurité des objets, et systèmes d'objets, connectés ont été développées dans un guide disponible sur le site de l'ANSSI.

2
Impact de l'IIoT sur l'architecture de l'usine

Le procédé industriel et le système d'information qui le soutient sont pensés comme un ensemble indépendant des autres SI, en vase clos. Une illustration de cette philosophie est la recommandation du mode de fonctionnement dégradé de type îlot [5] dans l'IEC62443 suggérant la capacité d'un SI industriel déconnecté du reste du monde à pouvoir maintenir un fonctionnement minimal du procédé.

Les systèmes industriels (regroupés sous le terme OT pour *Operational Technology*) se composent d'équipements ayant pour but d'assurer la continuité du procédé, sa sécurité fonctionnelle et son intégrité. Les systèmes bureautiques (regroupés sous le terme IT pour *Information Technology*) sont les systèmes généralement utilisés au quotidien pour le traitement des courriels, les systèmes permettant la facturation, la mise à disposition d'information, etc.

Historiquement, IT et OT ayant été construits de manière disjointe, les interactions entre ces deux mondes sont limitées et maîtrisées. La mise en œuvre de système IIoT oblige à les repenser.

Ce chapitre a pour but de préciser la représentation historique de l'usine selon le modèle de Purdue et d'y ajouter un capteur IIoT ainsi que les équipements associés au traitement des données IIOT [6].

2.1 Le modèle de Purdue comme représentation historique de l'usine

Un système industriel, et de manière plus générale une usine, peuvent être décrits en suivant le modèle de Purdue [7] qui représente l'usine comme un empilement de zones (cf. figure 1).

5. IEC62443 - SR 5.2 RE 2 : *Island mode – The automation solution shall realize capability and the operating organization shall use the capability to prevent any communication through the automation solution boundary (also termed island mode).*

6. Pour faciliter la lecture, on appelle *donnée IIoT*, les données générées par les systèmes IIoT.

7. Le modèle de Purdue (ISA95) est une grille de lecture des systèmes industriels, dont l'application stricte est généralement nuancée dans la réalité.

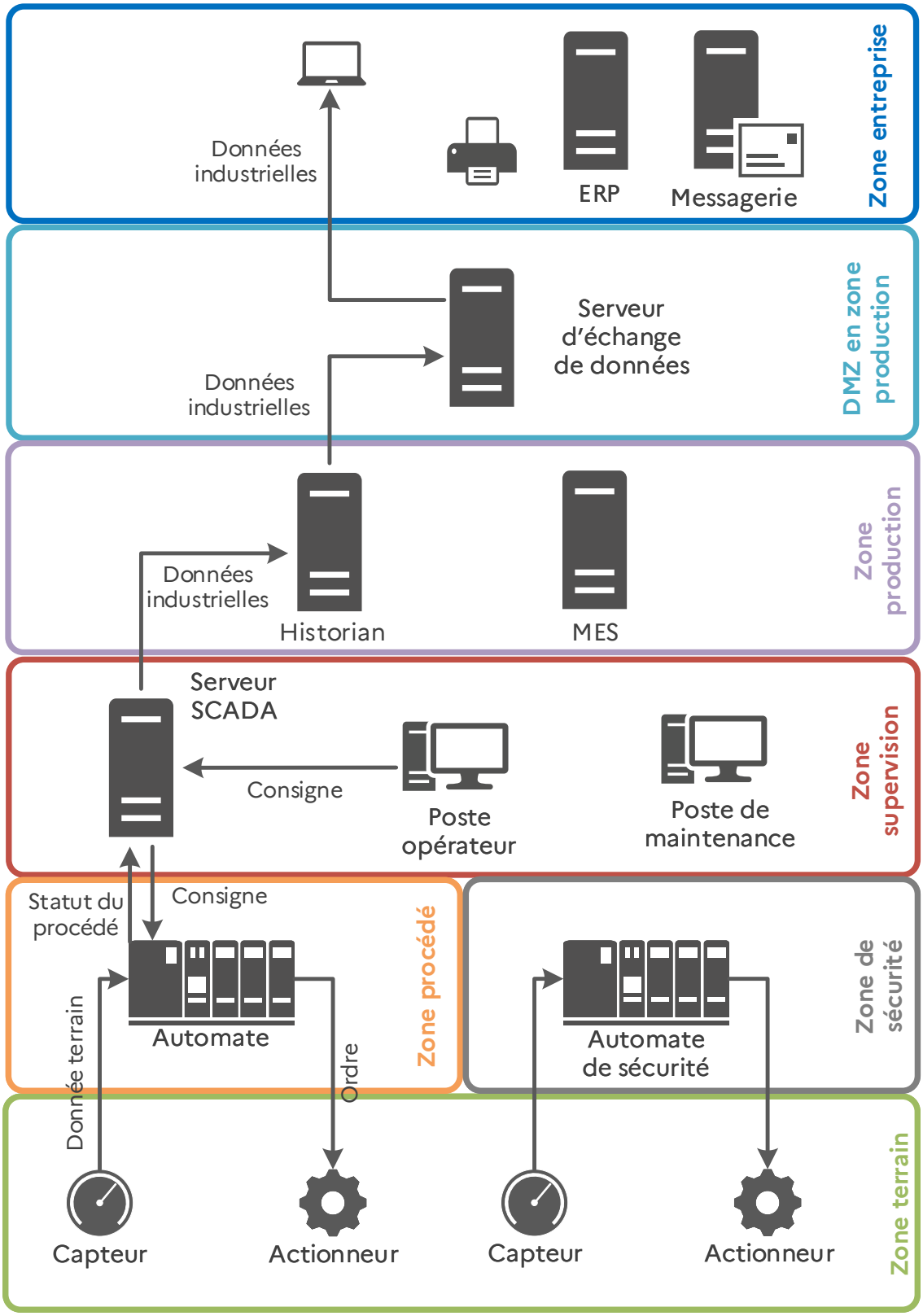

FIGURE 1 – Modèle de Purdue

Le modèle est composé des zones (ou niveaux) suivantes :

- Zone **entreprise** - IT (niveau 4) : il s'agit de la zone bureautique, permettant notamment la gestion des stocks, des commandes et de la facturation, au moyen, par exemple d'un progiciel de gestion intégré (ou *Enterprise Ressource Planning* abrégé en ERP en anglais). Cette zone n'est pas considérée comme appartenant au système d'information (SI) du système industriel (OT).
- Zone **démilitarisée** (DMZ, niveau 3.5) : il s'agit de la zone d'échange de données entre le système industriel et la zone entreprise (IT).
- Zone **production** (niveau 3) : il s'agit de la zone de contrôle des opérations du procédé. Cette zone permet d'optimiser le procédé selon un ensemble de données issues du système industriel ou de la zone entreprise. Ces données sont stockées et exploitées sur des serveurs spécialisés tel qu'un *historian* (base de données spécialisée pour le procédé) ou un logiciel de pilotage de la production (ou *Manufacturing Execution System*, abrégé en MES en anglais).
- Zone **supervision** (niveau 2) : il s'agit de la zone de supervision et de commande du procédé industriel. C'est depuis cette zone que les opérateurs poussent les consignes au procédé.
- Zone **procédé** (niveau 1) : il s'agit de la zone comprenant l'ensemble des automates programmables industriels (API) et des pupitres (IHM locales), qui permettent de réaliser l'asservissement du procédé.
- Zone **sécurité** (niveau 1) : il s'agit de la zone comprenant l'ensemble des automates programmables industriels de sécurité (APS). Cette zone permet de réaliser le traitement garantissant la sécurité des biens et des personnes.
- Zone **terrain** (niveau 0) : il s'agit de la zone qui regroupe les équipements d'acquisition de données sur le terrain (les capteurs) et les organes de commande (les actionneurs).
- Zone **externe** (non représentée) : il s'agit de la zone regroupant d'autres systèmes et équipements connectés au système industriel. En particulier, ceux non maitrisés par l'opérateur de l'installation industrielle (télémaintenance ou programmation de l'installation par un tiers par exemple).

2.2 Fonctionnement de l'usine : l'importance de la boucle d'asservissement

Le capteur appartient à la zone terrain (niveau 0). La donnée générée par le capteur est envoyée à un automate (niveau 1). Sur la base d'un ensemble de données internes (par exemple des données issues des capteurs) et externes (par exemple des commandes clients ou la météo), et selon une programmation en fonction de consignes (objectifs à atteindre), l'automate envoie un ordre à un actionneur (niveau 0) qui agit sur le terrain. Ce mécanisme est appelé régulation ou asservissement. Il peut être représenté sous la forme d'une boucle (cf. figure 2).

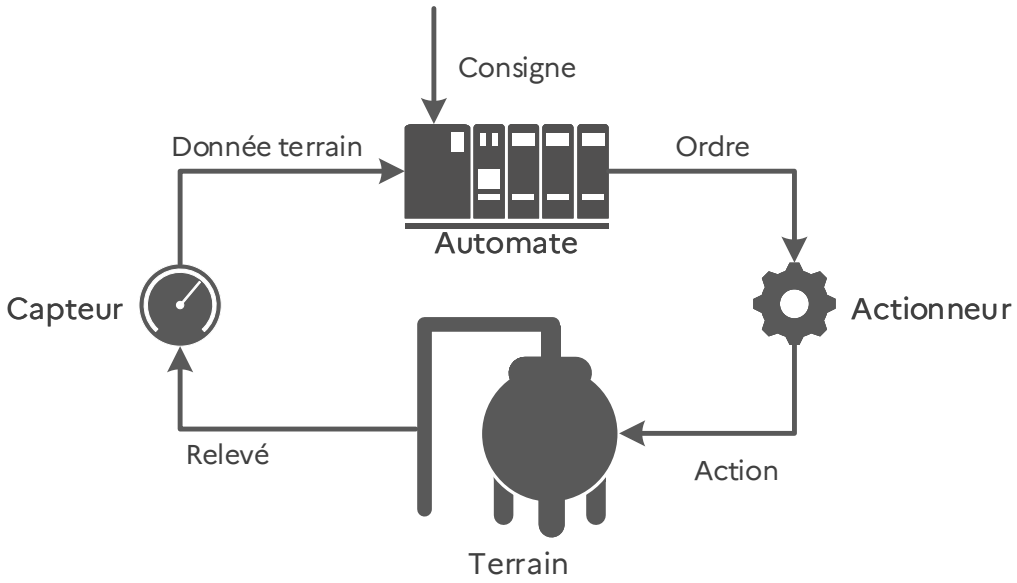

FIGURE 2 – La boucle d'asservissement

- Le capteur mesure une grandeur du terrain (par exemple, une température).
- Le capteur envoie à l'automate une donnée reflétant la valeur mesurée.
- En fonction de la donnée du capteur et de la consigne (un objectif à atteindre, par exemple 60°C), l'automate calcule un ordre (par exemple, chauffer).
- L'ordre est envoyé à l'actionneur.
- L'actionneur réalise l'action associée et modifie le procédé (par exemple, la température augmente).
- Le procédé change sous l'effet de l'actionneur, une nouvelle grandeur est mesurée, l'automate recalcule un ordre, etc.

Dans la boucle de rétroaction, la consigne pilote le système industriel : l'objectif de la boucle est de modifier le procédé pour lui faire atteindre l'état de la consigne, par exemple faire chauffer de l'eau à 60°C, 75°C, 80°C ou 95°C.

Dans le schéma traditionnel de l'usine, la consigne est généralement issue de la saisie ou d'une action d'un opérateur humain.

La figure 3 présente une vue simplifiée du système et du réseau de l'usine qui supportent la boucle d'asservissement. Pour simplifier les représentations, les zones du modèle de Purdue ne sont pas représentées sur ce schéma.

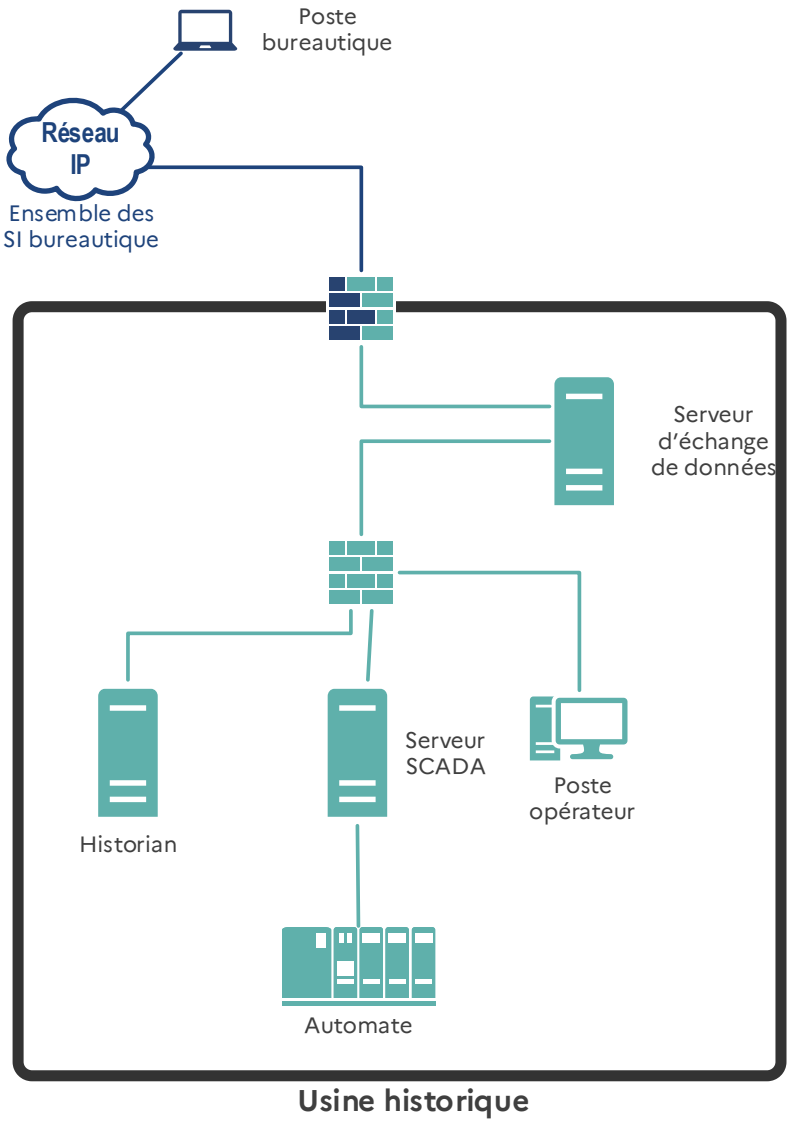

FIGURE 3 – Représentation simplifiée du système et du réseau de l'usine

Ceci n'est pas une architecture recommandée, il s'agit d'une représentation simplifiée, à visée didactique. Pour faciliter la lecture, le SI d'administration du SI industriel et les équipements de sûreté n'ont pas été représentés.

- L'automate est connecté à ses capteurs et actionneurs par des liens non IP, qui ne sont pas représentés ici.
- L'automate est connecté directement au serveur SCADA.
- Le serveur SCADA et l'*historian* sont sur un même sous-réseau.
- Les postes opérateurs sont les seuls équipements exposés à des utilisateurs. Du point de vue de la sécurité des SI, ces postes sont un point d'entrée privilégié sur le SI industriel (connexion de clefs USB, tentative de navigation sur Internet, ouverture de fichiers importés de la zone entreprise, etc.). Pour cette raison, ils sont isolés dans un sous-réseau dédié afin de limiter les capacités de latéralisation d'un attaquant ayant pris le contrôle de ces postes.
- Les postes opérateurs communiquent avec le serveur SCADA au travers d'un pare-feu dédié au filtrage des flux internes du système industriel.
- Le serveur d'échange de données, situé en DMZ, permet de mettre à disposition du SI bureautique des données issues du système industriel.

La boucle d'asservissement caractérise le système industriel. Son intégrité impacte directement l'intégrité du procédé et des produits. Il est donc impératif pour les industriels de garantir l'intégrité de la boucle d'asservissement, notamment en s'assurant que :

- les données mesurées et transmises par les capteurs reflètent la réalité du terrain ;
- les programmes chargés dans les automates calculent des ordres permettant d'atteindre la consigne ;
- les ordres transmis aux actionneurs ne mettent pas en danger l'usine ;
- les actionneurs sont fiables et exécutent les ordres tels que communiqués par les automates.

Toutes ces pratiques sont généralement associées au domaine de la sûreté de fonctionnement ou de la qualification fonctionnelle. Elles permettent, *in fine*, d'assurer la sécurité des biens et des personnes ainsi que la qualité des produits.

En conséquence, l'industrie a normalisé ces pratiques pour s'assurer du niveau de confiance dans la boucle d'asservissement (et le niveau de confiance en chacun des composants de cette boucle), par exemple :

- la délivrance d'autorisations de mise en service du procédé ;
- les recettes fonctionnelles et techniques systématiques et successives des composants lors des différentes phases de la création de l'usine ;
- la mise en place de standards, aussi bien de haut niveau (tel que l'IEC 61 131) que de bas niveau (par exemple la définition et l'usage systématique de programmes minimaux approuvés pour

la programmation des automates interdisant l'usage de programmes développés à discrétion pour certaines fonctions des automates [8]);

- la qualification fonctionnelle des automates, en particulier ceux portant des fonctions critiques. Cela se traduit notamment par de nombreux standards en gestion de la sûreté de fonctionnement, comme AMDEC [9] ou QMU [10].

Les objectifs de la SSI dans le contexte industriel sont :

- la protection des des personnes, des biens et de l'environnement, en complément à la sûreté de fonctionnement appliquée au périmètre des systèmes d'information de l'usine [11]. Les objectifs principaux dans ce contexte sont, d'une part, assurer la disponibilité constante du système industriel pour permettre une supervision efficace de la sûreté de l'usine, et d'autre part, garantir l'intégrité de ce même système pour assurer une réaction appropriée en cas d'incident et prévenir toute déviation du procédé qui pourrait compromettre la sûreté.
- la protection économique de l'usine. Dans ce cadre, les objectifs principaux sont la disponibilité (pour que l'usine continue à produire) et la confidentialité (pour permettre à l'industriel de conserver un avantage concurrentiel au travers de la protection de son expertise).

Aussi, l'introduction de nouvelles technologies, notamment celles liées à l'IIoT [12], doit se faire en respectant les besoins de sécurité du procédé (au sens de la sûreté de fonctionnement) au regard des nouvelles menaces SSI induites.

2.3 Intégration de l'IIoT dans le modèle de Purdue

Avant de présenter l'intégration de l'IIoT dans l'environnement industriel, il convient de définir les équipements et fonctions de l'IIoT. Dans le contexte de ce document, l'attention est portée sur les capteurs qui collectent de l'information depuis le terrain et l'ensemble des équipements qui transmettent et traitent cette information au travers d'une infrastructure dédiée : la chaîne IIoT.

La chaîne IIoT a pour objectif de valoriser des données issues du terrain, indépendamment de la valeur créée par le procédé, afin d'optimiser les opérations de maintenance préventive et/ou d'optimiser la production du système industriel par l'élaboration de consignes intelligentes.

Dans ce contexte, le capteur IIoT, contrairement à son homologue historique (le capteur câblé directement sur l'automate), n'alimente pas directement la boucle d'asservissement. La donnée produite par le capteur IIoT est envoyée dans un concentrateur de données situé dans la zone entreprise. La chaîne de traitement de la donnée IIoT échappe donc aux pratiques issues de la sûreté de fonctionnement industriel ou de la qualité du procédé.

La figure 4 précise la représentation de l'usine avec le capteur IIoT. À noter que la partie de droite n'a pas évolué, elle a été précédemment décrite.

8. Transposé à l'IT, il ne serait pas possible de construire un programme sur la base d'objets et de méthodes développées à discrétion et forcerait le recours exclusif à quelques librairies approuvées.
9. L'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC) est un outil de sûreté de fonctionnement et de gestion de la qualité.
10. La méthode QMU (*Quantification of Margins and Uncertainties*) est une méthodologie permettant de déterminer le niveau de confiance que l'on peut accorder au bon fonctionnement d'équipements.
11. Existe-t-il des modes opératoires impliquant le numérique et permettant de déclencher des évènements redoutés cartographiés par la sûreté de fonctionnement ? Les systèmes assurant la sûreté sont-ils numériques ?
12. L'IIoT, au sein d'une usine, introduit de nouvelles technologies (par exemple le *cloud)* ainsi que de nouveaux équipements (les équipements IoT et leur écosystème).

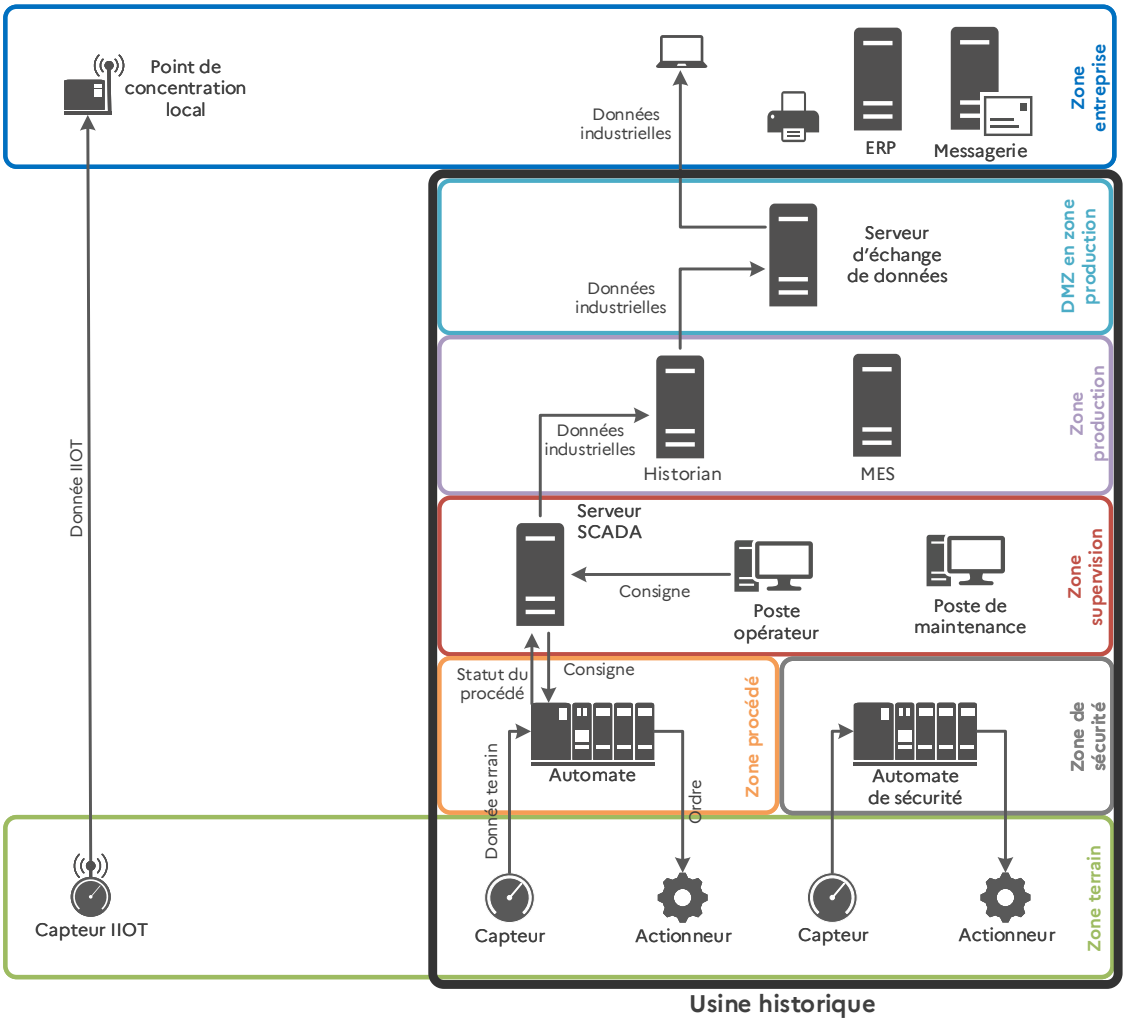

FIGURE 4 – Positionnement du capteur IIoT dans la représentation fonctionnelle de l'usine

Le capteur IIoT (en zone terrain) transmet les valeurs qu'il mesure (les données IIoT) à son point de concentration local.

Le point de concentration local peut être dans la zone production du modèle de Purdue si les données IIoT sont utilisées par le système industriel. Cependant, la donnée IIoT n'est en général pas utilisée directement par le système industriel. Le point de concentration local est donc souvent en zone entreprise, comme représenté ici. Les données IIoT sont utilisées indirectement à travers la zone entreprise.

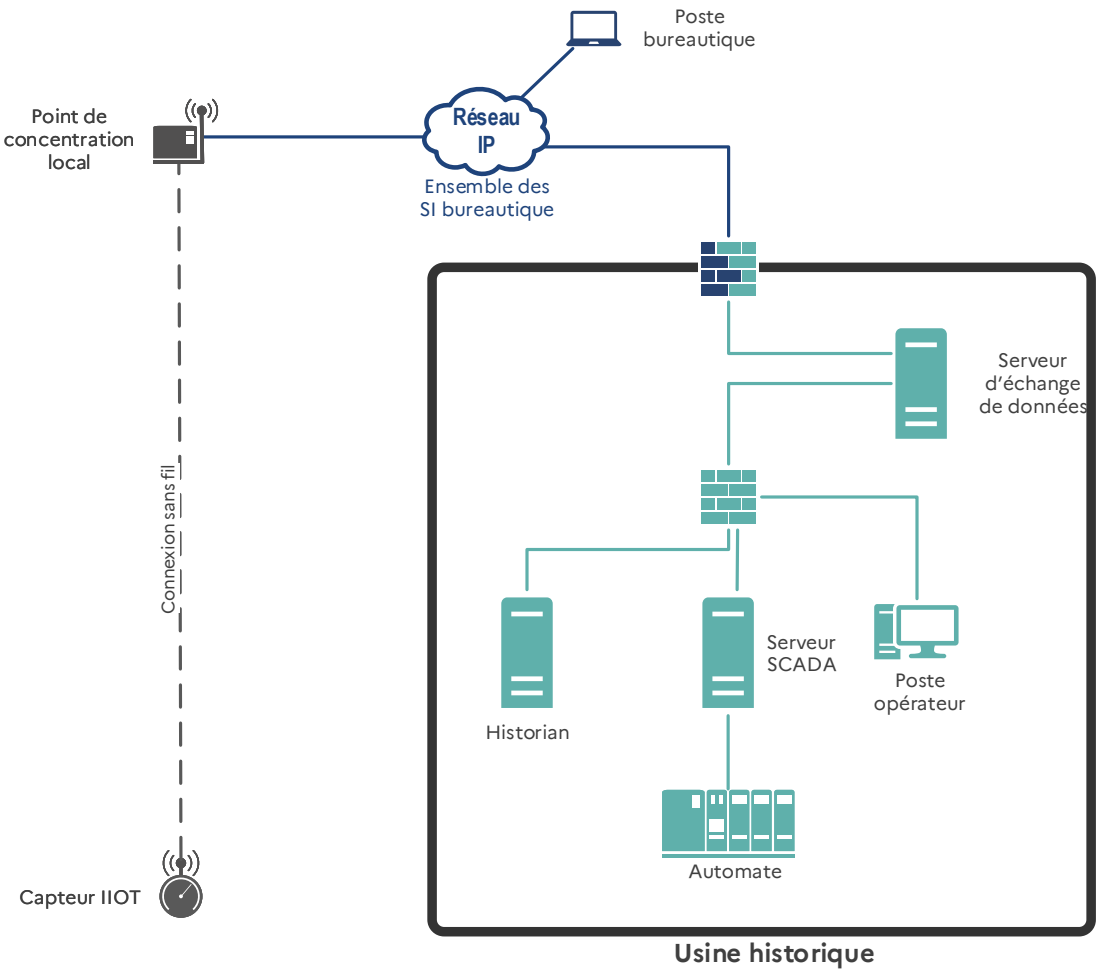

FIGURE 5 – Positionnement du capteur IIoT dans la représentation du système et du réseau de l'usine

Le capteur IIoT (en zone terrain) envoie les valeurs qu'il mesure (les données IIoT) à son point de concentration local, ici une passerelle.

Par exemple, des capteurs sans fil pourraient être positionnés sur une machine tournante pour mesurer les vibrations ainsi que la température de la machine. Ces valeurs reflètent directement l'état de santé de la machine. Elles permettent de planifier une opération de maintenance prédictive, lors d'un temps naturel d'arrêt de la machine, avant l'apparition d'une casse matérielle.

La chaîne IIoT peut être décomposée comme suit :

- **une infrastructure de collecte**, au plus proche du système industriel :
  - le capteur IIoT,
  - le point de concentration local qui peut être physiquement très proche du procédé ou plus loin si le protocole de communication sans fil le permet (par exemple, SigFox et LoRaWan),
  - un canal de communication entre le capteur IIoT et le point de concentration local ; il s'agit souvent de communication sans fil, par exemple au travers du protocole Zigbee ou LoRaWan ;
- **une infrastructure centralisée de stockage et de traitement**, accueillant les données de multiples infrastructures de collecte :
  - un système de stockage des données, par exemple sous forme de lacs de données (ou *data-lakes*),
  - des systèmes de traitement des données qui, au regard de la quantité de données, peuvent être amenés à utiliser des technologies d'intelligence artificielle,
  - des systèmes de visualisation des données ;
- **une infrastructure de transport des données**, faisant le lien entre les infrastructures de collecte et l'infrastructure centralisée de stockage et de traitement :
  - un ensemble de réseaux (et tous les équipements sous-jacents) permettant de transporter les données IIoT,
  - éventuellement, des concentrateurs de données intermédiaires dans la zone entreprise.

Ce découpage est représenté sur la figure 6.

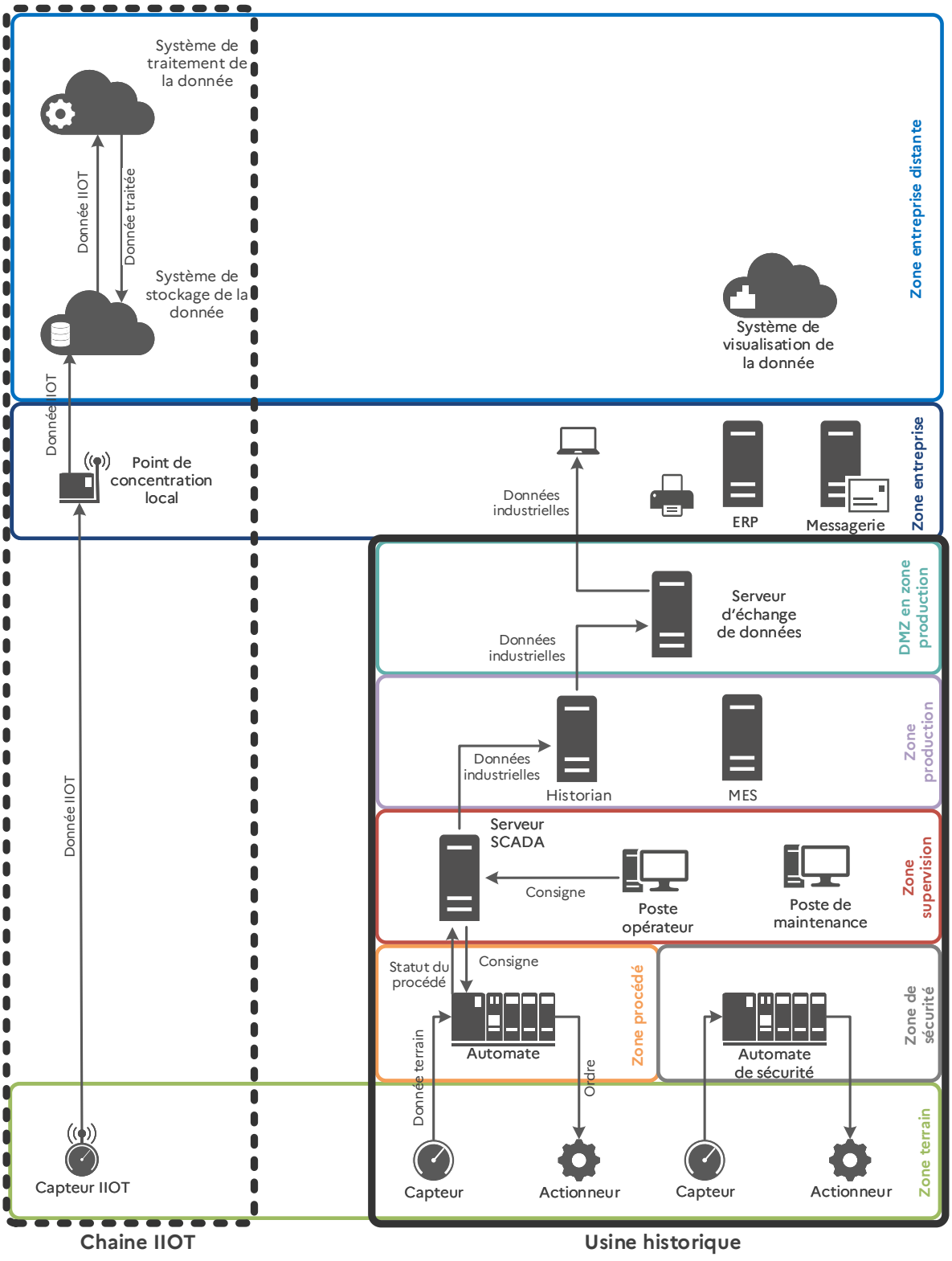

FIGURE 6 – Positionnement de la chaîne IIoT dans la représentation fonctionnelle de l'usine

3
Impacts de l'introduction de l'IIoT sur le modèle de sécurité de l'usine

La génération et le traitement de la donnée IIoT reposent sur un nouveau système composé notamment des capteurs IIoT et de la chaîne de traitement des données IIoT. S'il existe quelques spécificités dues au capteur et à la communication sans fil associée, la faible adhérence du reste des équipements de la chaîne IIoT à des technologies spécifiques aux systèmes industriels permet d'appliquer les bonnes pratiques de la SSI à la chaîne IIOT, et de les inscrire dans les schémas de gouvernance existants au sein des organisations.

Il est recommandé de réaliser ou de mettre à jour une analyse de risque SSI s'appuyant sur la méthode EBIOS RM en incluant dans son périmètre le système IIoT. L'objectif pour l'entité est de pouvoir adapter les mesures de sécurité en fonction des menaces retenues et des évènements redoutés associés aux valeurs métiers du système industriel.

L'analyse doit englober à la fois les nouveaux scénarios susceptibles de déclencher des événements redoutés déjà identifiés dans le système industriel via le système IIoT, ainsi que les scénarios pouvant engendrer de nouveaux événements redoutés spécifiques à la chaîne IIoT. En particulier, il est nécessaire de traiter les scénarios de risques impactant :

- la disponibilité et/ou l'intégrité du système industriel (à partir du système IIoT) ;
- la confidentialité des données de la chaîne de collecte du système IIoT ;
- la disponibilité et/ou l'intégrité de la chaîne de collecte du système IIoT ;
- la disponibilité et/ou l'intégrité de la chaîne de traitement du système IIoT.

Information

Certains systèmes de maintenance préventive pour les machines tournantes sont entièrement intégrés au système industriel et connectés directement aux automates. Ces systèmes matérialisent à l'extrême le modèle des systèmes IIoT traité dans ce document. Par conséquent, pour ces systèmes, une étude poussée doit être menée et mise à jour régulièrement. De manière générale, toute interconnexion IT/OT ne s'appuyant pas sur la zone DMZ (couche 3.5 du modèle de Purdue) doit être étudiée avec soin.

3.1 Les scénarios de risques portant atteinte à la disponibilité et/ou l'intégrité du système industriel

Les deux principaux éléments à prendre en compte dans les scénarios de risques pouvant impacter la disponibilité et l'intégrité du système industriel sont les suivants :

- **Attaques par latéralisation :** la mise en œuvre d'un système IIoT augmente la surface d'attaque du système industriel en créant de nouvelles interconnexions et donc la possibilité de latéralisation d'un attaquant vers le système industriel. Un soin particulier doit être apporté au cloisonnement entre ces deux systèmes. Dans de nombreux cas, ils n'ont pas besoin de communiquer : il est donc inutile de les interconnecter.
- **Attaques de l'homme du milieu (*Man-in-the-middle Attacks*) :** les consignes intelligentes pourraient être supprimées, modifiées et/ou rejouées entre le système IIoT et le système industriel. Il est important de considérer des mesures de protection en intégrité et authenticité sur les flux transportant les consignes intelligentes et/ou sur la passerelle d'interconnexion entrante vers le système industriel.

Par exemple, selon les cas d'usage et l'adhérence entre l'IIoT et le système industriel, ces menaces pourraient mener à un arrêt durable d'exploitation du système (via latéralisation et prise de contrôle du système industriel à partir de l'IIoT) ou à un comportement erratique du procédé industriel par la réception de consigne intelligente non intègre et non authentifiée.

3.2 Les scénarios de risques portant atteinte à la confidentialité des données de la chaîne de collecte du système IIoT

La centralisation des données du système industriel au sein du système IIoT augmente les potentiels impacts sur le système industriel en cas de divulgation de celles-ci. Dans ce cas de figure, les principaux éléments à prendre en compte sont :

- **Attaque par administration non autorisée de l'infrastructure hébergeant les données :** il est important de prendre en compte, en cas d'infogérance, la capacité de l'infogérant d'accéder aux données et aux traitements.
- **Attaque par accès non autorisés aux données par un utilisateur tiers :** en cas de mutualisation des moyens avec d'autres clients (par exemple dans un contexte *cloud*), le niveau de confiance dans l'infogérant, comme par exemple un *Cloud Service Provider* (CSP), et le niveau de cloisonnement des données doivent être pris en compte pour évaluer le risque associé.
- **Attaque par exfiltration de données :** en cas de compromission de l'espace de stockage par un attaquant malveillant, l'ensemble des données pourrait être exfiltré. Il est donc important de s'assurer du niveau de sécurité de cet espace de stockage, d'envisager des mécanismes de chiffrement des données au repos et de contrôler que seules les données autorisées y sont remontées via la passerelle d'interconnexion sortante.

Selon le domaine industriel d'application et les données choisies pour les nouveaux cas d'usage, une perte de confidentialité des données peut avoir par exemple des impacts sur l'avantage concurrentiel lié au savoir-faire de l'entité.

3.3 Les scénarios de risques portant atteinte à la disponibilité et l'intégrité des données sur la chaîne de collecte du système IIoT

Les traitements réalisés par le système IIoT sont naturellement très dépendants de l'intégrité et de la disponibilité des données remontées par la chaîne de collecte IIoT. Les principales menaces à considérer sont :

- **Attaque par modification ou prise de contrôle des équipements IIoT depuis la zone entreprise (voire depuis Internet) :** la modification ou perte d'intégrité des capteurs de collecte de données (c.-à-d. les capteurs IIoT) peut impacter la disponibilité et/ou l'intégrité des données traités par le système IIoT. Les mesures à envisager sont l'authentification et le contrôle d'intégrité des commandes qui ont pour destination le système IIoT, l'utilisation des capteurs IIoT embarquant des fonctions de sécurité et disposant de certifications ou qualifications de sécurité.
- **Attaque physique sur les capteurs IIoT :** notamment le changement du positionnement du capteur dans l'usine peut impacter l'intégrité des mesures [13].

Les impacts de ce type de menaces peuvent par exemple inclure une indisponibilité du système industriel faute de déclenchement d'actions préventives de maintenance en l'absence d'alerte émise par le système IIoT, ou alors des pertes économiques induites par le déclenchement trop fréquent de d'actions préventive de maintenance.

Information

Dans l'évaluation des risques, s'ajoute la particularité des communications entre le capteur IIoT et le point de concentration local à l'usine. Ces communications peuvent être portées par un réseau étendu à basse consommation (ex. : LPWAN). Dans ce cas, le niveau de sécurité cryptographique de ces communications est limité par la contrainte de faible consommation électrique des capteurs. La majorité des produits proposés sur le marché aujourd'hui offrent un niveau de protection cryptographique insuffisant.

De fait, les communications entre le capteur IIoT et le point de concentration local sont vulnérables en raison de faiblesses inhérentes au protocole. Si les risques associés sont considérés inacceptables au regard des usages et de la menace, il est recommandé de ne pas recourir à l'IIoT. Il faut par ailleurs encourager une montée du niveau de sécurité des équipements chez les constructeurs, par exemple en indiquant clairement le niveau minimal de sécurité pour l'achat et l'emploi de l'IIoT dans un contexte donné.

13. Notamment a) un capteur situé dans une zone accessible de l'usine pourrait être déplacé, sa mesure ne refléterait plus la valeur attendue (ex. : capteur de température d'un environnement clos déplacé en extérieur) ou b) un capteur dont l'interface de maintenance, accessible depuis le terrain, pourrait être réétalonné afin de fournir une valeur faussée.

3.4 Les risques sur la disponibilité et l'intégrité des fonctions de la chaîne de traitement du système IIoT

Sur la chaîne de traitement du système IIoT, il est important de prendre en compte le risque de non-fiabilité de la donnée d'entrée, en particulier dans le cas de l'utilisation d'algorithmes de traitements reposant sur l'analyse statistique ou sur l'intelligence artificielle. Ces principales menaces d'origine accidentelle sont :

- **les biais statistiques dans les modèles de traitements des données :** ceux-ci peuvent produire des résultats erronés et donc biaiser les prises de décisions. Ces biais peuvent être dus au fait que :
  - l'entraînement des modèles sur la base d'un jeu de données incomplet induit des corrélations incomplètes et donc des causes infondées,
  - il y a un décalage entre le modèle travaillé dans un environnement de laboratoire et ce même modèle déployé en environnement réel,
  - une confiance excessive est placée dans un indicateur donné,
  - de nombreuses variables peuvent être oubliées dans le calcul final (contraintes d'environnement physique, etc.);
- **l'usage d'un ensemble de données parcellaires :** cela peut fausser les résultats d'un modèle de simulation;
- **l'usage d'un ensemble de données erronées/non intègres :** par exemple l'achat ou la vente de stock pourrait mener à une perte de disponibilité et des pertes financières.

3.5 Synthèse des risques liés à l'IIoT

L'utilisation de l'IIoT induit de nombreuses menaces qui doivent être prises en compte. Cela est plus particulièrement vrai dans des contextes d'utilisation où un fort niveau de dépendance existe entre l'IIoT et le système industriel. Par exemple, un procédé industriel dont la maintenance prédictive repose entièrement sur l'IIoT pourrait engendrer un arrêt (maîtrisé ou non) inacceptable.

Il est donc important de mettre en place des mesures SSI adaptées afin d'assurer un niveau de confiance suffisant dans la chaîne de collecte des données et donc des traitements effectués. Un cas d'usage en particulier doit être traité avec vigilance. Il s'agit de l'utilisation de consignes intelligentes à partir de données industrielles (IIoT et non IIoT) au travers d'algorithmes de traitement statistique ou d'intelligence artificielle pour optimiser le procédé. Pour mettre en œuvre cet usage, il est nécessaire de traiter les points suivants :

- le stockage hors système industriel des données provenant du système industriel;
- les algorithmes permettant de calculer la consigne intelligente;
- le transport de la consigne intelligente vers le système industriel.

La figure 7 ci-après illustre la boucle d'asservissement intelligente.

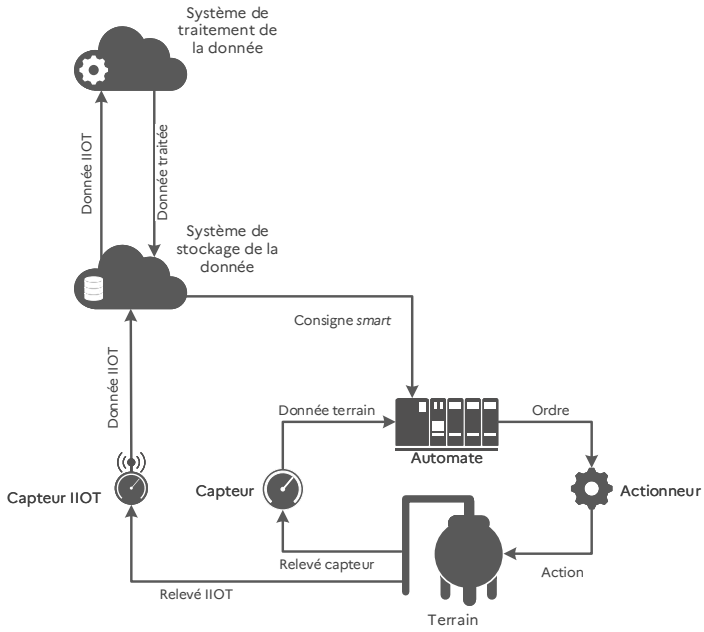

FIGURE 7 – La boucle d'asservissement intelligente

La branche intelligente de la boucle :

- Le capteur IIoT mesure une grandeur sur le terrain (par exemple une pression).
- La donnée IIoT est envoyée dans le système de stockage des données.
- Le système de traitement de la donnée calcule une consigne à partir des données présentes dans le système de stockage des données (données IIoT, données industrielles, données externes).
- La consigne intelligente est envoyée à l'automate.

La branche locale de la boucle :

- Le capteur mesure une grandeur sur le terrain (par exemple une température).
- Le capteur envoie à l'automate une donnée reflétant la valeur mesurée.

- En fonction de la donnée du capteur et de la consigne (un objectif à atteindre, par exemple 60°C), l'automate calcule un ordre (par exemple, chauffer).
- L'ordre est envoyé à l'actionneur.
- L'actionneur réalise l'action associée et modifie le procédé (par exemple, la température augmente).
- Le procédé change sous l'effet de l'actionneur. De nouvelles grandeurs sont mesurées, la boucle intelligente calcule une nouvelle consigne intelligente, l'automate recalcule un ordre, etc.

L'apparition dans le système industriel d'une consigne intelligente calculée en dehors du système industriel ou importée d'un système tiers ne découle pas strictement de l'IIoT. Cependant, il serait tentant, à des fins d'optimisation des coûts, d'adapter la chaîne IIoT pour le calcul et la redescente de la consigne intelligente dans le procédé et, en particulier, le serveur d'échange de données situé dans la DMZ en zone de production. Cette architecture exposerait le procédé à un risque important en cas de consignes intelligentes non-intègres et non-authentifiées pouvant modifier le comportement du système industriel et mener à un arrêt d'exploitation.

Les besoins de sécurité de l'interconnexion IT vers OT (consigne intelligente) et ceux relatifs à l'interconnexion OT vers IT (IIoT) sont différents et doivent donc faire l'objet de canaux distincts.

Il est nécessaire de traiter deux points structurants pour limiter les risques avant de mettre en place la consigne intelligente en répondant aux questions suivantes :

- Est-il acceptable, du point de vue de la sûreté de fonctionnement, de piloter la procédé avec la consigne intelligente ?
- Comment mettre en place de manière sécurisée la chaîne de communication associée ?

4
Assurer la confiance dans les données IIoT et la consigne intelligente

4.1 Vérification de l'intégrité fonctionnelle de la donnée

Il s'agit ici de traiter le risque d'une exploitation fonctionnelle de la consigne intelligente : un attaquant pourrait contrôler sa valeur pour modifier le comportement du SI industriel.

Exemple

Considérons un procédé composé, notamment, d'une centrifugeuse.

- La centrifugeuse [14] est fragile et critique pour le procédé [15]. Elle est remplacée exclusivement lors de maintenances préventives ayant lieu lors des grands arrêts de l'usine selon un cycle de maintenance propre à l'industriel.
- Pour optimiser la production en prenant en compte les limites d'usures acceptables, la vitesse de rotation de la centrifugeuse est ajustée en temps réel sur la base d'informations issues de l'IIoT et de facteurs externes.
- Un attaquant prend le contrôle du système IIoT lors d'une maintenance préventive et il neutralise les alertes que le système génère.
- De plus, l'attaquant modifie la consigne intelligente envoyée à l'automate en charge de la centrifugeuse, et augmente de manière ponctuelle et infime la vitesse de rotation.
- Cette modification minime n'est pas détectée par les opérateurs. L'usure de la centrifugeuse est prématurée, celle-ci casse avant les opérations de maintenance planifiée, la production de l'usine est mise à l'arrêt.

Ce risque se traite principalement au travers des mesures fonctionnelles suivantes :

- la vérification du niveau de confiance contextualisé [16] de la donnée par le SI industriel. Ce niveau pourrait être obtenu en combinant les trois critères d'intégrité, de disponibilité et de confidentialité. Ceci peut être fait par exemple au niveau de passerelles d'interconnexion IT/OT ou

14. Équipement ayant pour objectif de séparer les composés d'une solution par force centrifuge (par exemple pour l'enrichissement de l'uranium).

15. En 2010, le ver *Stuxnet* a été conçu pour s'attaquer aux centrifugeuses iraniennes d'enrichissement d'uranium afin de conduire au ralentissement de la production mais aussi à la destruction physique des installations.

16. Dans certaines entreprises, ce niveau de confiance se reflète dans le critère de « criticité » des systèmes et des données. À noter qu'il est illusoire de concevoir une formule mathématique universelle combinant les trois critères pour en déterminer la criticité. Il est nécessaire de contextualiser ces critères au regard des enjeux métier.

idéalement par le SI industriel lui-même. Par exemple, il serait possible d'envisager un score de confiance de la donnée et des actions associées :

- score de confiance très élevé : intégration en temps réel de la consigne au procédé,
- score de confiance élevé : intégration en temps réel au procédé et signalement pour vérification de la consigne *a posteriori*,
- score de confiance médiocre : demande de validation humaine avant d'intégrer la consigne au procédé ;

- la capacité du SI industriel à rejeter une consigne (de manière manuelle ou automatique) dans la ligne directe du mode *island* préconisé par l'IEC 62443. Il s'agit ici de rendre le SI industriel capable de passer en mode local si nécessaire ;
- la récupération de la consigne intelligente à l'initiative du SI industriel, primaire pour la relation avec le concentrateur de données.

Malgré la mise en place de mesures compensatoires, il est possible que le risque ne soit pas réduit à un niveau acceptable, en particulier dans le cas d'une consigne intelligente calculée dans le *cloud* (environnement non maîtrisé) ou au travers d'algorithmes dont les comportements sont complexes (traitement statistiques, IA, etc.). Il n'est donc pas recommandé, *a priori*, de faire usage de la consigne intelligente pour piloter le procédé.

4.2 Architecture sécurisée

Malgré les risques relevés dans la section 4.1, dans le cas où la communication IT/OT doit être mise en œuvre, il est nécessaire de sécuriser les échanges entre la chaîne IIoT et le SI industriel. Pour cela, il est recommandé de construire une architecture sécurisée composée d'une infrastructure de transport de la donnée et de deux passerelles.

4.2.1 Passerelle d'interconnexion OT vers IT (de l'usine vers l'entreprise)

Dans le sens OT vers IT, la passerelle doit :

- garantir la confidentialité de la donnée OT, c'est-à-dire s'assurer que seules les données destinées à l'IT y sont envoyées afin d'assurer la confidentialité du savoir-faire de l'usine (qui peut être reflété dans ses données OT) ;
- garantir l'intégrité des données de l'OT, c'est-à-dire s'assurer que la donnée circulant dans l'IT correspond à sa source OT ;
- limiter les capacités de latéralisation d'un attaquant, et en particulier l'établissement d'un lien avec un serveur de commande et de contrôle [17].

L'architecture proposée tient compte d'une possible compromission du SI industriel (hors passerelle).

17. Outillage utilisé par un attaquant pour administrer les ressources compromises du système ciblé et propager son attaque ; il se caractérise notamment par l'infrastructure distante, par l'applicatif installé sur la ressource compromise et permettant les opérations à distance, ou par le protocole de communication employé entre la ressource compromise et le serveur distant de commande et de contrôle.

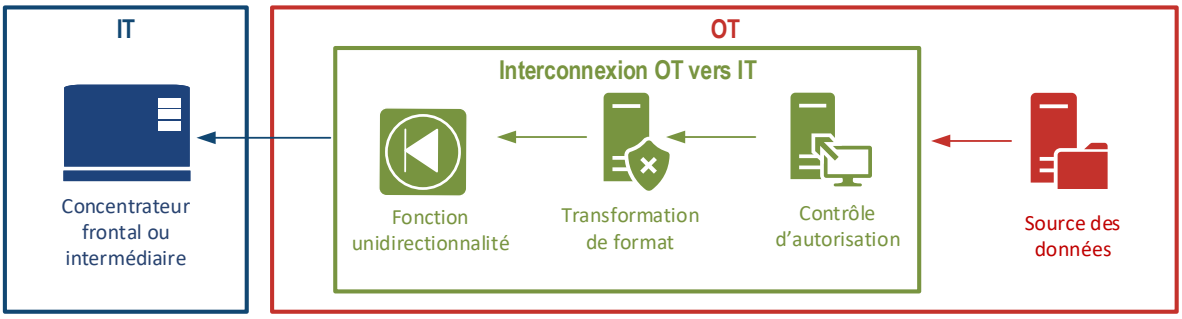

FIGURE 8 – Proposition de passerelle OT vers IT

Pour assurer ces fonctions, le fonctionnement de la passerelle peut être le suivant (cf. figure 8) :

- Les données OT à communiquer à l'IT – et ces données uniquement – sont envoyées à l'initiative du système industriel à la passerelle. L'envoi peut se faire grâce à des protocoles industriels.
- Contrôle d'autorisation : sur la base d'une liste d'autorisations, la passerelle s'assure que les données envoyées par le système industriel peuvent être transmises à l'IT. La donnée OT envoyée étant issue du système industriel, son format est compact et connu.
- Transformation de format : la passerelle transcode les données au format attendu par le système IT. Lors de cette opération, il est possible d'assurer l'intégrité des données lors de leurs stockage et transport vers l'IT, au moyen d´un mécanisme cryptographique.
- Une fonction d'unidirectionnalité, pour protéger en intégrité le système industriel, est préférablement positionnée au plus proche de la frontière IT/OT. Cette fonction met à disposition de l'IT les données transcodées et permet notamment d'assurer que la passerelle ne peut être utilisée par un attaquant pour se latéraliser depuis l'IT vers l'OT.

4.2.2 Passerelle d'interconnexion IT vers OT (de l'entreprise vers l'usine)

Dans le sens IT vers OT, la passerelle doit :

- garantir la disponibilité et l'intégrité du procédé, c'est-à-dire que la donnée envoyée par l'IT vers l'OT, et en particulier les consignes, ne menace pas le procédé ;
- limiter les capacités de latéralisation d'un attaquant, et en particulier de propagation de l'IT vers l'OT.

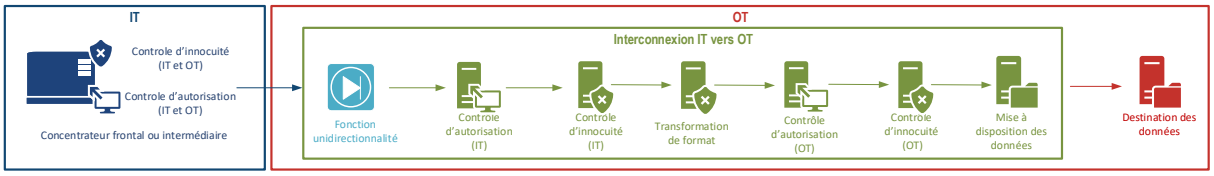

FIGURE 9 – Proposition de passerelle IT vers OT

Pour assurer ces fonctions (réparties sur un ou plusieurs équipements virtualisés ou non), le fonctionnement de la passerelle peut être le suivant, comme illustré dans le figure 9 :

- Une source de données maîtrisée [18] dans l'IT envoie des données à la passerelle.
- Une fonction d'unidirectionnalité est préférablement positionnée au plus proche de la frontière IT/OT, pour les propriétés d'isolation qu'elle confère à la passerelle, d'où son positionnement dans le schéma. Elle participe à réduire la surface d'attaque.
- Contrôle d'autorisation (IT) : la passerelle contrôle la source des données. Ce contrôle s'appuie sur une liste de sources et de données autorisées.
- Contrôle d'innocuité (IT) : la passerelle effectue une vérification antivirale de la donnée reçue pour s'assurer qu'elle n'est pas vectrice de risques pour le procédé. Ce contrôle d'innocuité bénéficie idéalement des mêmes politiques antivirales et de supervision de sécurité que l'OT.
- Transformation de format : la passerelle transcode les données au format attendu par le système OT.
- Contrôle d'autorisation (OT) : la passerelle contrôle la destination des données. Ce contrôle s'appuie sur une liste de destination et de données autorisées.
- Contrôle d'innocuité (OT) : la passerelle exécute une vérification fonctionnelle de la donnée reçue pour s'assurer que les données reçues ne sont pas vectrices de risques pour le procédé. Ce contrôle d'innocuité s'appuie notamment sur des contrôles de sûreté de fonctionnement.
- La passerelle met à disposition la donnée au système industriel qui est à l'initiative de la connexion et de la récupération.

Les contrôles d'innocuité doivent être renforcés par la source de données IT (probablement le point de concentration IT), qui doit avoir elle-même réalisé ces contrôles en amont. Cela permet d'assurer que le contrôle des données n'est pas à la seule charge de la passerelle située dans la DMZ en zone de production.

4.2.3 Infrastructure de transport de la donnée

L'architecture de transport des données dans l'IT peut s'articuler autour de la mise en place d'une chaîne de concentrateurs de données dans des DMZ permettant de franchir les zones de sécurité. En particulier :

- Un concentrateur frontal : ce concentrateur assure l'interconnexion entre le système de traitement/stockage des données et les passerelles d'interconnexion IT vers OT et OT vers IT. Il est recommandé que ce concentrateur soit maîtrisé et administré par l'entreprise et hébergé dans une DMZ dédiée.
- Des concentrateurs intermédiaires : ces concentrateurs reflètent la structure organisationnelle de l'entreprise, ils sont optionnels. Ils sont situés dans les DMZ aux frontières des zones de sécurité [19] à franchir entre le concentrateur frontal et les passerelles d'interconnexion.
- Une passerelle d'interconnexion IT vers OT dans la DMZ en zone de production.
- Une passerelle d'interconnexion OT vers IT dans la DMZ en zone de production.

18. Ceci exclut tout équipement dont l'administration n'est pas effectuée par l'entreprise, en particulier les sources de données *cloud*. Si les données sont stockées dans le *cloud*, il est nécessaire de positionner un concentrateur intermédiaire dans la zone entreprise.
19. Ces zones de sécurité sont notamment la zone de production côté OT, et les zones entreprise et entreprise distante côté IT.

Afin de limiter les capacités de latéralisation d'un attaquant d'une zone de sécurité à l'autre et de maîtriser les interfaces de communication ainsi que les émetteurs et récepteurs des flux, les mesures suivantes doivent être mise en œuvre :

- Préférer des passerelle d'interconnexions indépendantes et cloisonnées entre elles (c'est à dire une chaine IT vers OT et une chaine OT vers IT).
- Imposer que les DMZ en zone de production (DMZ IT/OT), qui hébergent les passerelles, n'acceptent que les flux entrants (cf. figure 11).
- Intégrer cette infrastructure à la supervision de sécurité (au SOC [20] s'il existe) de l'entreprise.
- Conduire des évaluations de sécurité (audit, test d'intrusion, évaluation du niveau de sécurité) sur :
  - l'infrastructure mise en place (système et réseau) ;
  - les protocoles mis en œuvre ;
  - et tout autre composant logiciel ou matériel jugé sensible.
- Appliquer et maintenir les plans d'actions découlant de ces évaluations de sécurité dans le temps.

Information

Une attention particulière doit être portée à la chaîne IIoT qui traverse des périmètres de responsabilités multiples : les zones industrielles de l'usine, la zone entreprise (de l'usine ou au-delà dans l'entreprise) et éventuellement une zone dans le *cloud*. Une difficulté majeure à sa sécurisation réside ainsi dans la maîtrise de la chaîne IIoT de bout en bout par l'organisation. En particulier, l'implication d'équipes qui n'étaient historiquement pas sollicitées sur le sujet de la SSI dans le domaine industriel.

20. SOC, *security operation center*, ou centre opérationnel de sécurité.

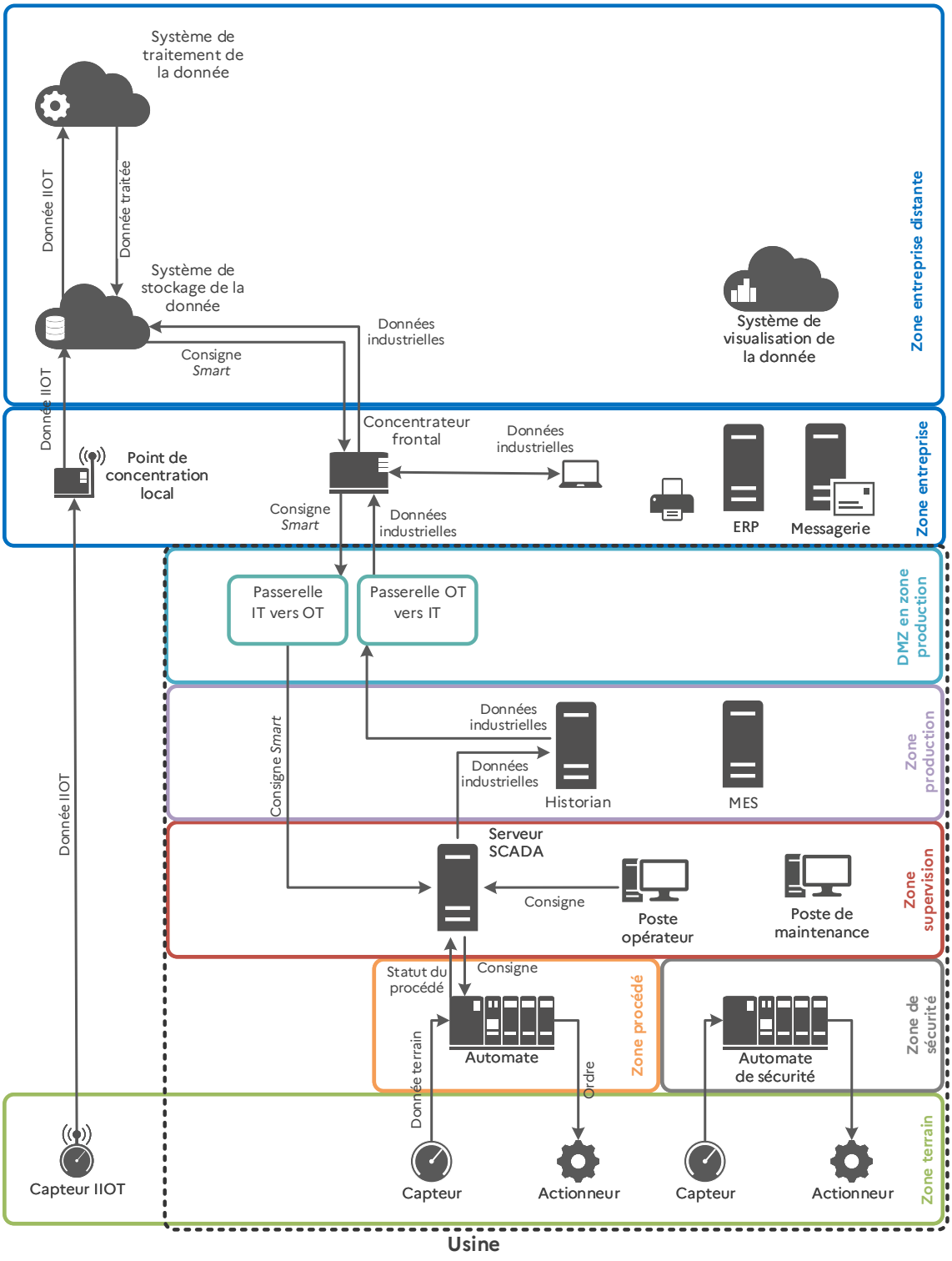

FIGURE 10 – Proposition d'architecture fonctionnelle

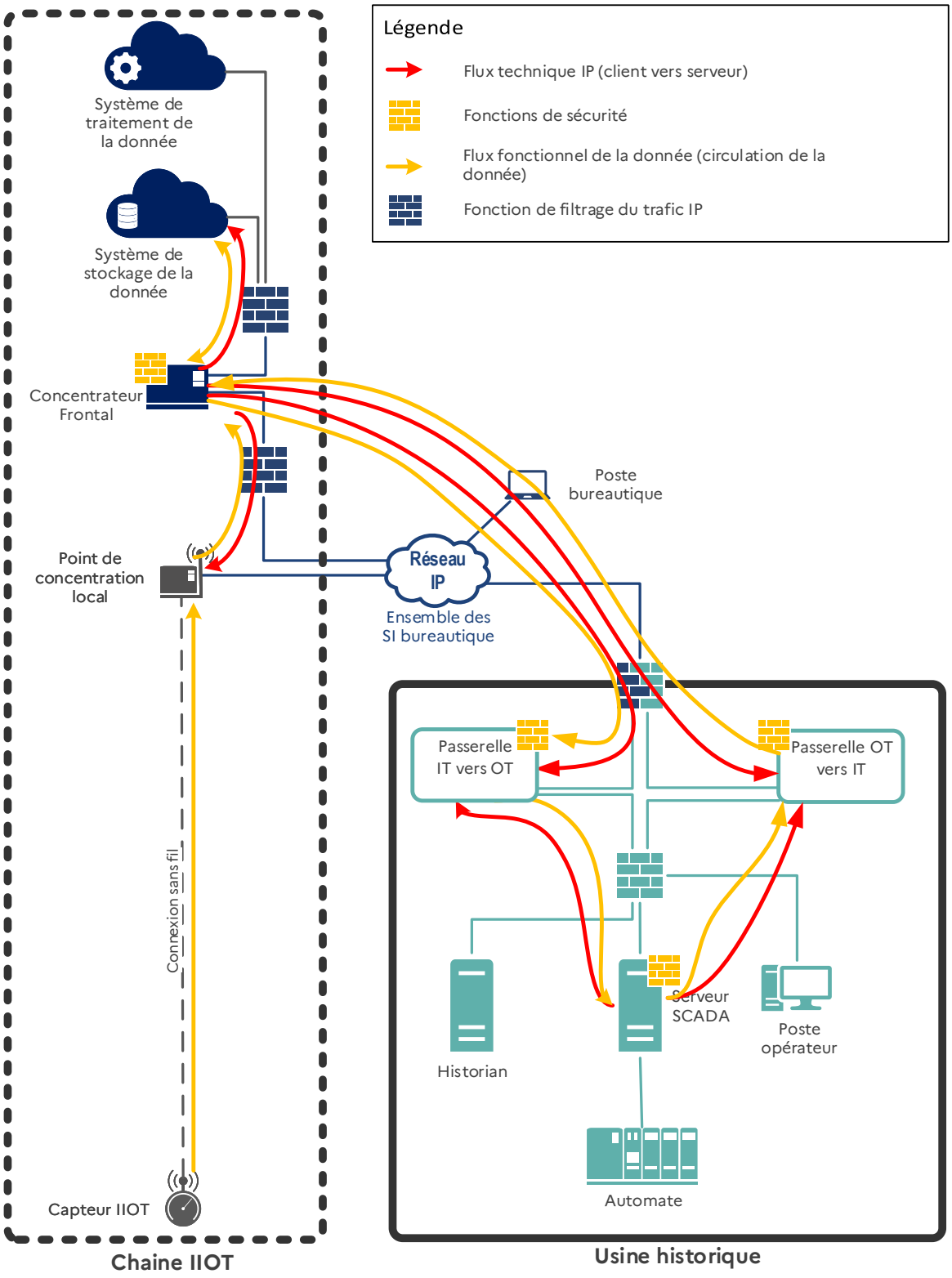

FIGURE 11 – Proposition d'architecture système et réseau

5
Conclusion

Si l'IIoT et l'usine « connectée » présentent de nombreux attraits métier, ils sont porteurs de risques difficiles à atténuer techniquement. La quantification de ces risques doit se faire au moyen d'une approche traditionnelle d'analyse des risques, en distinguant deux aspects principaux :

- la sûreté des traitements, incluant à la fois les traitements des consignes et des valeurs calculées par les automates industriels, devant être évaluée en fonction de la sûreté de fonctionnement de l'usine et des exigences d'assurance qualité ;
- la sécurité de l'infrastructure (système et réseau) devant reposer sur les bonnes pratiques usuelles de la SSI bureautique (IT) et industrielle (OT).

L'usine, historiquement perçue comme un objet indépendant et fonctionnant en vase clos, voit son périmètre s'agrandir avec l'introduction de l'IIoT dans les systèmes industriels (cf. figure 12). Il s'agit désormais :

- d'inclure les mesures de sécurité de la données dans ce nouveau périmètre élargi ;
- de prendre en compte la zone entreprise, même externalisée.

Il persiste toutefois une problématique d'organisation, dans la mesure où cette approche requiert la participation d'équipes qui, auparavant, n'étaient pas sollicitées sur le sujet de la sécurité des systèmes d'information industriels. Il faut donc doter la gouvernance SSI des moyens et de la légitimité nécessaire à la couverture de ces nouveaux enjeux, d'une part en sensibilisant le plus haut niveau de la hiérarchie, et d'autre part en constituant des équipes pluridisciplinaires.

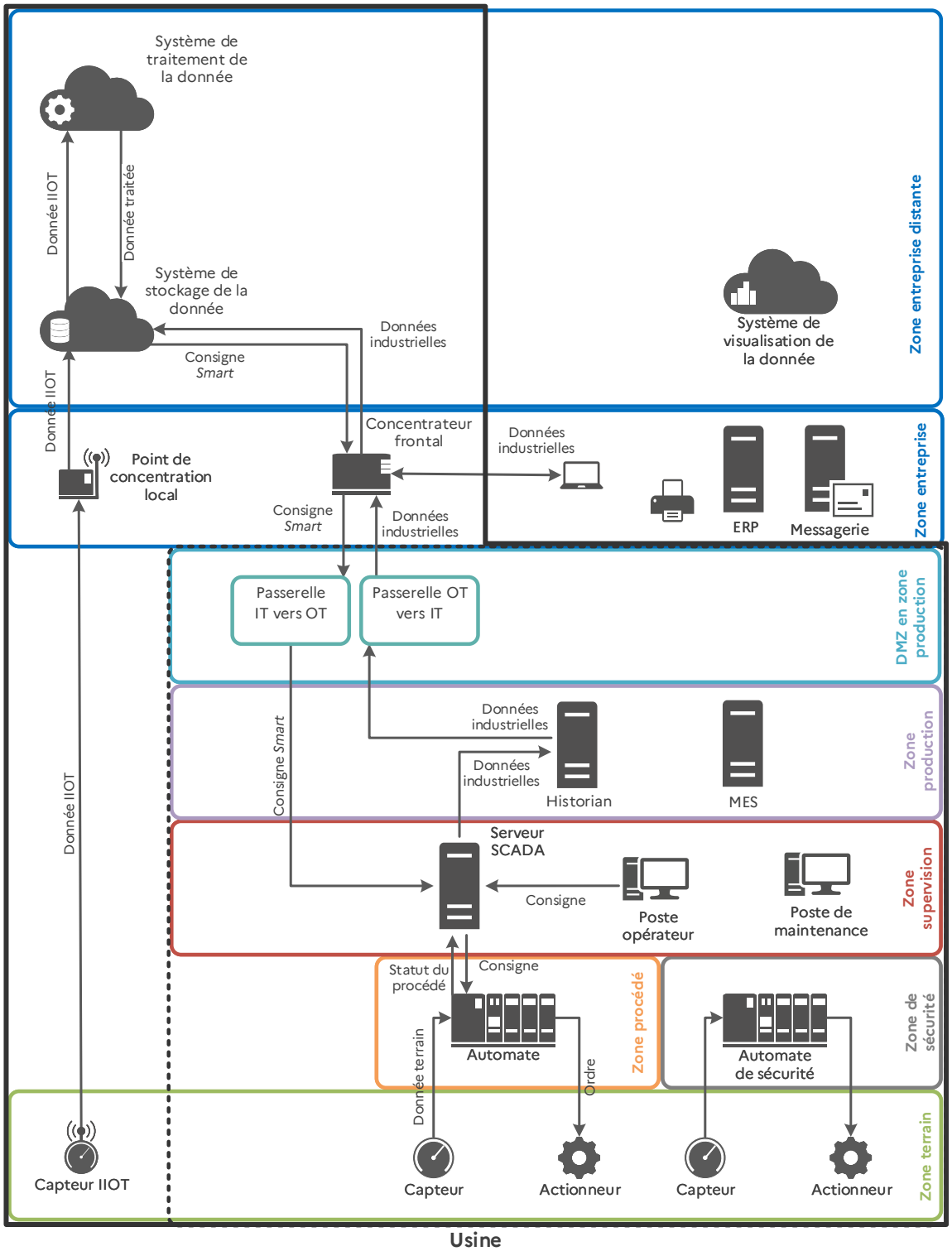

FIGURE 12 – Le nouveau périmètre de la sécurité des systèmes industriels

Version 1.0 - 30/05/2025 - ANSSI-PG-109

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

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

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité