LES DOSSIERS TECHNIQUES

Cybersécurité des systèmes industriels :

Par où commencer ?

Panorama des référentiels et synthèse des bonnes pratiques

juin 2014

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador - 75009 Paris
Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88
clusif@clusif.fr – www.clusif.fr

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 :

Gérôme	**BILLOIS**	*Solucom*
Hervé	**SCHAUER**	*HSC*

Les contributeurs :

Patrice	**BOCK**	*ISA France, Sogeti France*
Jean	**CAIRE**	*RATP*
Emmanuel	**DE LANGLE**	*Solucom*
Loïc	**DIVAN**	*Andra Cigéo*
Anthony	**DI PRIMA**	*Solucom*
Loïc	**GUEZO**	*Trend Micro*
Philippe	**JEANNIN**	*RTE*
Thierry	**PERTUS**	*Conix*
Orion	**RAGOZIN**	
Éric	**SAVIGNAC**	*Airbus Defence and Space*

Le **CLUSIF** remercie également les adhérents ayant participé à la relecture.

Pour tout commentaire, veuillez contacter le CLUSIF à l'adresse suivante : scada@clusif.fr.

I. Introduction

Ce document, résultant d'une consolidation élargie des retours d'expérience des contributeurs et de la littérature existante, a pour but d'accompagner la communauté sécurité dans la prise en compte des problématiques liées à la sécurité des systèmes industriels.

Dans cette optique, un panorama des référentiels recensés, assorti des fiches de lecture respectives, est présenté afin de permettre au lecteur de mieux s'orienter dans ses choix pour établir un cadre de référence en cybersécurité ou plus simplement un programme de lecture.

À la lumière de ce panorama, il propose également une démarche synthétique, structurée et progressive en 5 phases clés, permettant à des protagonistes peu familiarisés avec les spécificités du contexte industriel d'appréhender ce type d'environnement et d'inscrire leur organisation dans une démarche d'amélioration continue.

Ce document s'adresse en premier lieu aux Responsables en Charge de la Sécurité des Systèmes d'Information (RSSI), amenés à intégrer des systèmes industriels dans leur périmètre de responsabilité, mais il peut également être utilisé par toutes les personnes impliquées dans des projets de cybersécurité des systèmes industriels.

Il est à noter que le panorama des référentiels recensés constitue une photographie de ces documents au 31 mars 2014.

II. Définition, constituants et enjeux

La notion de Système d'Information Industriel (SII) est large. De manière générale, il peut être défini comme tout système « numérique » permettant d'avoir une action directe dans le monde « physique ». Les acronymes ICS (Industrial Control System) ou IACS (Industrial Automation and Controls Systems) sont généralement utilisés pour l'identifier. Le SII peut aussi être étendu à un domaine proche : la Gestion Technique des Bâtiments (GTB) ou BMS (Building Management System).

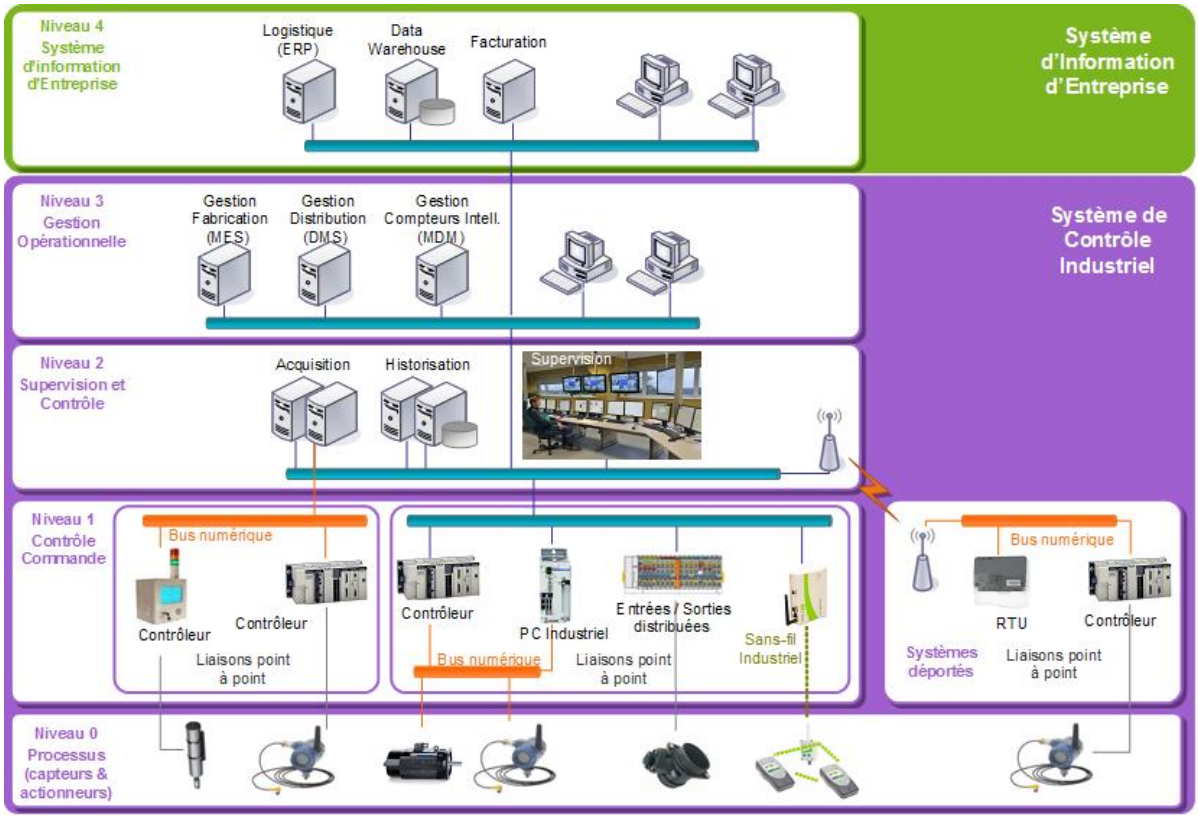
Ces systèmes sont constitués de 4 grandes catégories de composants décrits dans la pyramide CIM (Computer Integrated Manufacturing) :

- Les composants assurant l'interaction avec le monde physique. Il s'agit de capteurs (température, ouverture, humidité, lumière…) et d'actionneurs (pompes, vérins, moteurs, voyants…). Ils sont souvent reliés entre eux par un réseau spécifique appelé bus de terrain. Même si les technologies IP sont de plus en plus présentes, il existe encore des protocoles propriétaires. Certains modèles « smart » disposent d'une intelligence électronique embarquée (IED : Intelligent Electronic Device). Il s'agit du niveau 0 de la pyramide CIM.
- Les composants de pilotage industriel réalisant le pilotage sur le terrain des actionneurs en fonction des informations issues des capteurs et du programme embarqué. Ils peuvent être distribués (DCS : Distributed Control System) ou autonomes, sous la forme d'automates adaptés à un déploiement soit local (PLC (Programmable Logical Controler) ou API (Automate Programmable Industriel) en français), soit déporté (RTU : Remote Terminal Unit). Aujourd'hui ces distinctions ont tendance à s'estomper. Les composants de nouvelle génération (PAC : Programmable Automation Controler) disposent d'une plus grande palette de fonctionnalités que les composants traditionnels et sont reliés en IP au réseau informatique de pilotage de la production. Il s'agit du niveau 1 de la pyramide CIM.
- Les composants de supervision et de contrôle du processus composent le niveau 2 de la pyramide. Grâce à une interface homme-machine (IHM), ils permettent la visualisation de l'ensemble du processus, et son pilotage en fonction de consignes. Les acronymes utilisés sont souvent SCADA (Supervisory Control And Data Acquisition) ou MTU (Master Terminal Unit). Ces composants sont reliés aux systèmes de gestion de production (le niveau 3 de la pyramide) de l'entreprise d'où ils reçoivent leurs ordres. Ils sont composés le plus souvent d'éléments issus de l'informatique de gestion tels que des serveurs ou des postes de travail fonctionnant avec des systèmes d'exploitation usuels (Windows…).

Les trois types de composants peuvent être assemblés, mutualisés et utilisés différemment en fonction des processus associés pour former le Système d'Information Industriel.

De façon croissante, les systèmes industriels sont informatisés et interconnectés au Système d'Information (SI) de l'entreprise, dit aussi « SI de Gestion » (SIG) (le niveau 4 de la pyramide). Les SII sont également de plus en plus étendus et ouverts pour permettre des

traitements à distance (par exemple : télémaintenance via Internet ou le SI de gestion). Par voie de conséquence, les SII se voient de plus en plus exposés aux cyber-risques.



Déclinaison de la pyramide CIM (source : Thierry Cornu)

Il est possible de distinguer 3 grandes catégories de SII :

- **Les systèmes liés à un site**. Situation la plus couramment envisagée, il s'agit de systèmes d'information localisés sur un site physique défini et dans des distances courtes (au maximum de l'ordre de quelques kilomètres). Il s'agit par exemple des systèmes animant les chaînes de production dans l'industrie automobile, agroalimentaire ou pharmaceutique, des unités d'extraction ou de transformation d'énergie nucléaire/gaz/pétrole. De manière très fréquente on trouve sur ces sites un ou plusieurs systèmes industriels, on parle alors « d'installation ». Sont également souvent rencontrés les systèmes de gestion technique des bâtiments ou encore les processus de sûreté qui protègent tout ou partie des chaînes de production. Ces systèmes sont connus, facilement localisés et une présence humaine proche est fréquente.
- **Les systèmes étendus**. Il s'agit de systèmes répartis à l'échelle d'un pays ou d'une région. Les usages suivants sont recensés : réseau de transport/distribution d'énergie ou d'eau, de transport public, suivi de l'état de systèmes distribués sur des sites industriels distants (gestion de niveaux de cuves…). Ils nécessitent des réseaux télécoms longue distance, souvent gérés par un opérateur tiers. Autre caractéristique, les sites physiques peuvent également être inoccupés. Dans de nombreux cas, des

moyens d'accès à distance sont nécessaires pour le fonctionnement au quotidien comme pour la maintenance.

- **Les systèmes autonomes/mobiles/embarqués**. Il existe de très nombreuses définitions de ces termes. Dans le contexte de ce document, il faut le comprendre comme suit : Il s'agit des systèmes de taille plus restreinte, de l'ordre de la dizaine de mètres au maximum. Sont placés dans cette catégorie par exemple les équipements biomédicaux comme les scanners, IRM ou encore à plus petite échelle les pacemakers ou dispositifs médicaux autonomes. Les systèmes présents dans les moyens de transport (automobiles, avions…) entrent également dans cette catégorie. Peu visibles, ils font souvent partie intégrante d'un équipement et offrent une possibilité faible d'évolution sans la participation du fournisseur.

Bien entendu chacun de ces systèmes peut être combiné et présent sous des formes différentes. Mais cette catégorisation permet d'identifier des besoins de cybersécurité et des contraintes spécifiques selon le contexte considéré.

Dans le monde industriel, les critères liés à la sûreté de fonctionnement (disponibilité et intégrité en premier lieu) sont prioritaires par rapport aux critères de confidentialité ou de traçabilité. Cependant ceci peut être à relativiser en fonction des processus métiers concernés et des obligations règlementaires.

Il est à noter que ces systèmes partagent un certain nombre de caractéristiques spécifiques qui influent sur la gestion des risques et la manière de les sécuriser :

- Leur durée de vie est longue, elle se compte souvent en dizaines d'années d'une « génération » à l'autre.
- Ils sont déployés dans des environnements difficiles (poussière, humidité, électromagnétisme, température extrême, corrosion…).
- Ils peuvent être déployés sur un SI totalement isolé et déconnecté ce qui peut complexifier les opérations de maintien en conditions de sécurité.
- Les interruptions de services doivent être peu fréquentes et peuvent requérir une planification importante. L'arrêt d'un processus ou d'un équipement industriel peut être lié à des contraintes physiques fortes (par exemple durée requise pour lancer un processus industriel ou encore longueur d'interruption du processus avant qu'il soit possible d'intervenir sans risque). Il est à noter que les opérations liées à la cybersécurité peuvent être envisagées dans le cadre des phases de maintenance lorsqu'elles existent.
- Les interventions sur ces systèmes se réalisent potentiellement dans des environnements d'accessibilité délicate et/ou soumise à conditions, nécessitant parfois des habilitations particulières ou le respect de consignes de sécurité physique pointues.
- Dans la majorité des secteurs, la dépendance des SII aux fournisseurs est forte. En effet, ces derniers fournissent généralement l'intégralité du système « clé en main » avec un contrat de maintenance pluriannuel où les évolutions ou en tout cas la réversibilité sont rendues particulièrement délicates, voire inenvisageables (du fait du caractère spécifique, sinon propriétaire des technologies et implémentations mises en œuvre).

- La configuration et le paramétrage de certains composants du SII sont qualifiés par des autorités de tutelle. En cas de modification, elles peuvent demander à repasser le processus de qualification ce qui peut prendre un certain temps et qui peut entraîner l'obligation d'arrêter la production en attendant les résultats du processus.

III. Référentiels sur la sécurité des SI industriels

La liste des référentiels concernant la sécurité des Systèmes d'Information Industriels (SII) est très fournie. Ce nombre important de documents peut parfois rendre difficile leur lecture et la façon d'appréhender le sujet.

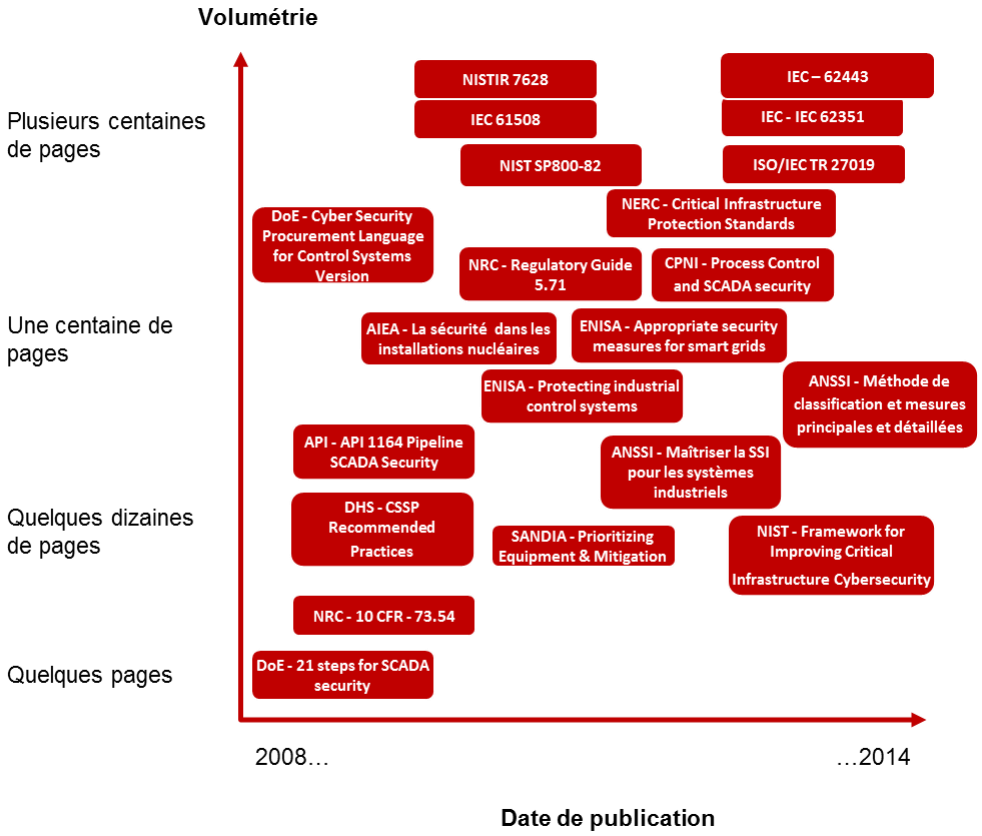
Devant ce constat est apparue la nécessité de créer un panorama des documents traitant de ces problématiques. L'objectif est de recenser les documents existants et d'identifier les plus pertinents. Ce chapitre vise ainsi à donner les clés afin d'identifier les référentiels les plus adaptés lorsque l'on souhaite démarrer une démarche de sécurisation des SI Industriels. Nous le verrons en dernière partie.

Comme l'actualité en témoigne, la sécurité des SII est un sujet clé pour de nombreux organismes. Plus de 50 documents ont pu être identifiés par le groupe de travail. Dans un souci de ne garder que les publications les plus pertinentes, une trentaine de documents a été initialement retenue. Cette sélection a été faite suite à des relectures et des analyses croisées entre les membres du groupe de travail. Ces documents ont été relus pour n'en conserver qu'une vingtaine, en fonction de leur pertinence, leur lisibilité et leur utilisation concrète.

En annexe se trouve un tableau recensant l'ensemble des documents relus par le groupe de travail.

III.1. Une littérature abondante et variée

La figure ci-dessous représente les documents finaux sélectionnés. Elle les classe en fonction de leur date de publication et de leur volume. Elle permet à la fois de mettre en évidence l'actualité riche, du fait des nombreux documents édités ces dernières années, ainsi que l'hétérogénéité de ces publications en termes de volume : de quelques pages à plus de mille pages.



Une littérature abondante et variée

III.2. Différents secteurs d'activité fortement représentés

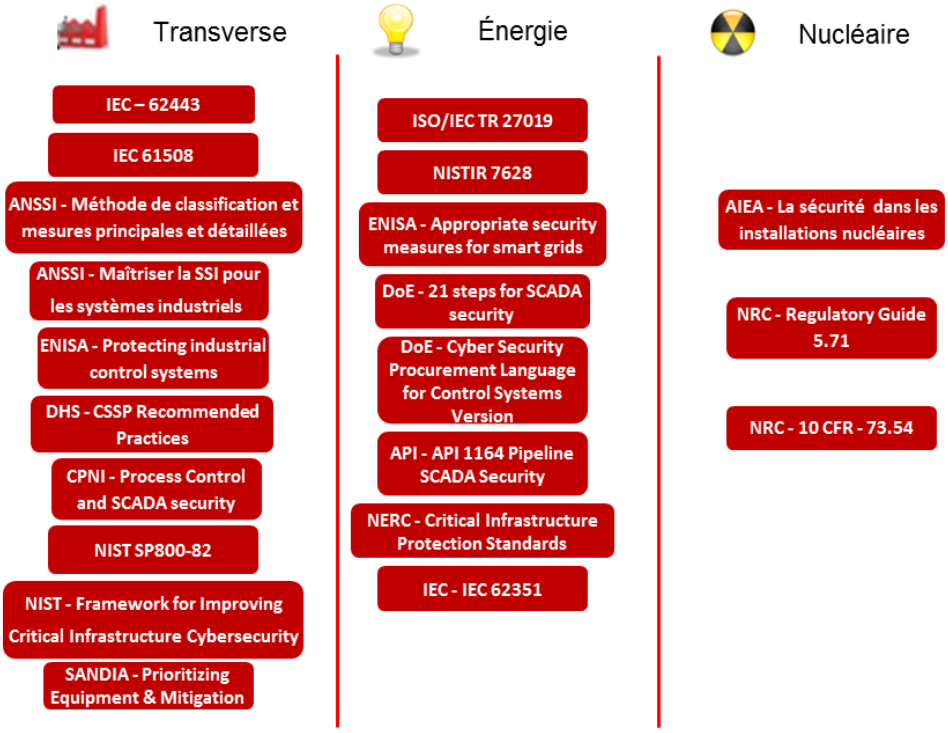
Les documents publiés abordent la sécurité des SII appartenant à différents secteurs. Plusieurs constats peuvent émaner de cette analyse. Il existe évidemment de nombreux documents transverses qui s'appliquent à tous les secteurs d'activité.

Mais il est intéressant de noter que le domaine de l'énergie est très prolifique. Et pour cause, de nombreux organismes se sont intéressés au secteur : à la fois des organismes internationaux, tels que l'ISO ou l'ENISA, qui ont publié des documents spécifiques au secteur de l'énergie. Mais aussi des organismes très spécialisés, tel que le Département de l'Énergie américain (DoE) ou l'AIEA, qui de fait se sont penchés sur leur propre secteur. De nombreux documents sont

encore en préparation, en particulier dans le domaine nucléaire où nous pouvons citer l'IEC 62645.

Enfin, il a été constaté que très peu de documents ont été publiés dans les secteurs de la santé et du transport de manière spécifique : les quelques publications sont soit assez anciennes, soit peu exhaustives.

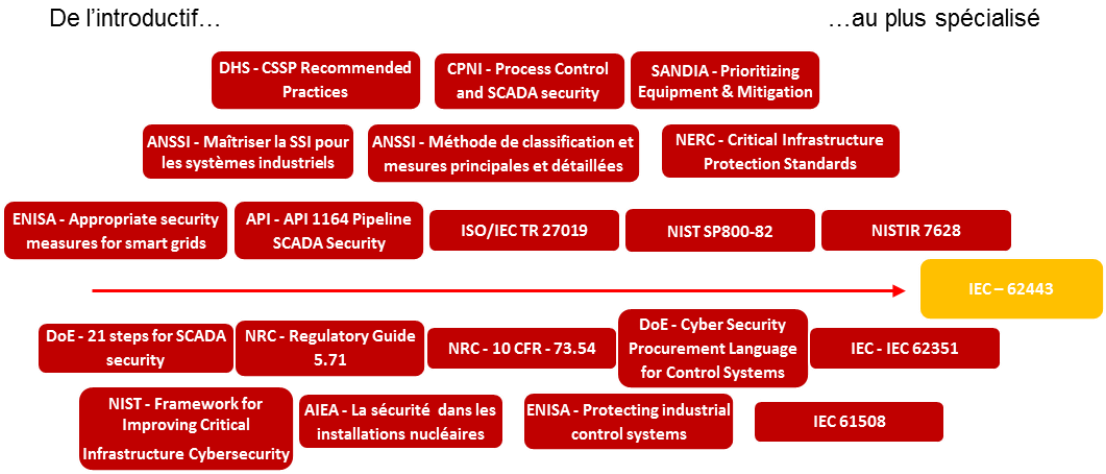
Pour autant, les documents présentés, bien que souvent spécifiques à un secteur, peuvent dans la majeure partie des cas être adaptés à d'autres secteurs, en changeant certains concepts ou en adaptant le vocabulaire. Par conséquent, le domaine de publication ne doit pas apparaître comme un facteur limitant, et il ne faut pas se résoudre à ne consulter que les documents propres à un secteur particulier.



Origine des documents

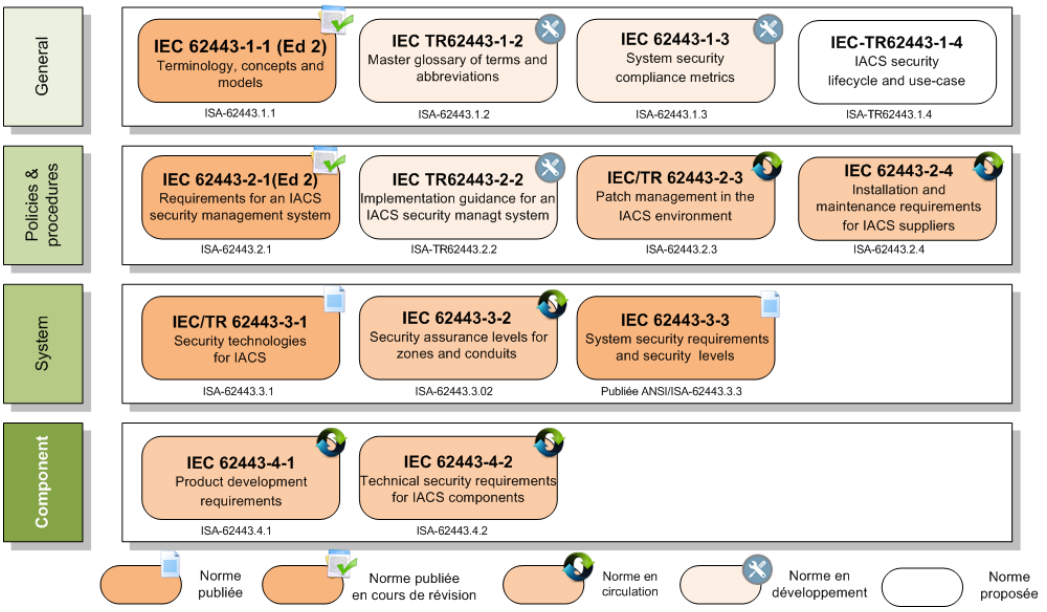
III.3. Des typologies de documents très variables

La finalité varie grandement selon les documents publiés : certains sont des documents introductifs dont l'objectif est surtout d'expliquer les grands concepts. D'autres au contraire sont très pointus et vont très loin dans les notions abordées.



Des typologies de documents très variables

Il est à noter que la norme IEC – 62443 (historiquement ISA 99) est en fait une famille de normes, balayant l'ensemble des typologies possibles. En effet, chaque référentiel peut aller de l'introductif jusqu'au plus spécialisé. Plusieurs de ces documents sont encore en cours de rédaction ou de refonte, ce qui rend le référentiel difficile d'accès. Ces documents se structurent de la façon suivante, en fonction de leur granularité et de la cible visée :



Structure de la norme IEC – 62443 (décembre 2013 – source : ISA France)

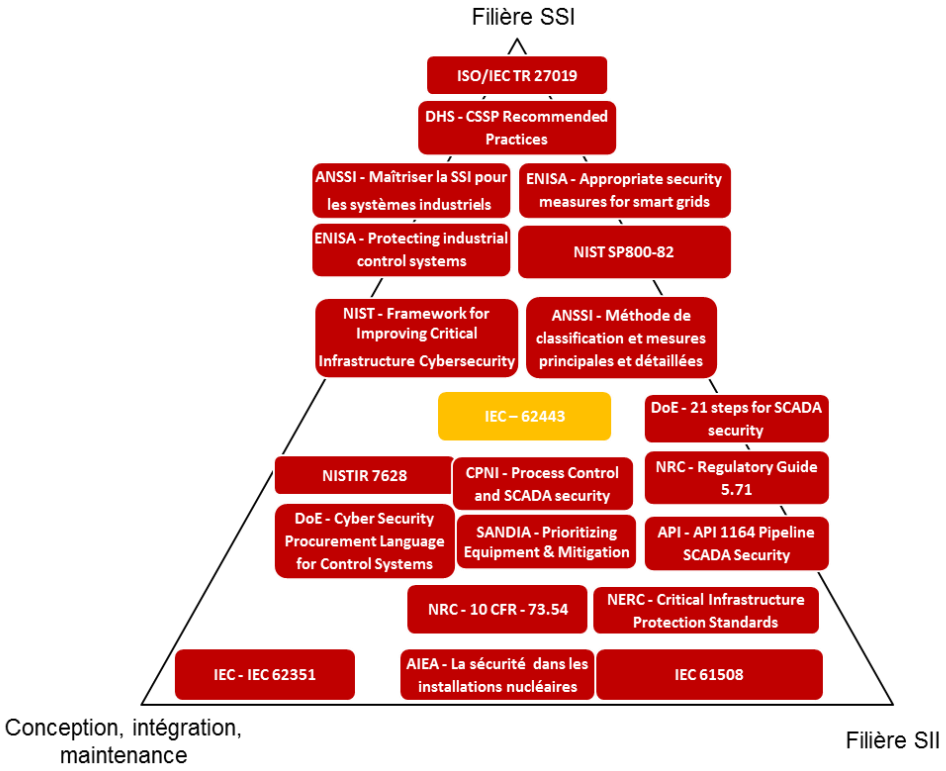
III.4. Des documents ciblant des populations différentes

Étant donné que les publications ne s'adressent pas toujours aux mêmes populations, il est intéressant d'identifier les documents les plus utiles suivant le type de population qui évolue dans le domaine de la sécurité des SII. Trois grandes populations (ou filières) ont été identifiées : la filière sécurité de

l'information (SSI), évoluant dans un environnement plus proche du SI de gestion ; la filière SII et la filière conception, intégration, maintenance, voire aussi constructeurs.

Plusieurs constats peuvent émaner de l'étude : d'abord, chaque filière peut être amenée à utiliser l'ensemble des documents et pourra en tirer des bénéfices. Pour autant, on note tout de même l'existence de documents spécifiques. En effet, certains d'entre eux correspondent davantage à des spécifications de protocoles et seront donc plus dédiés à la filière conception, intégration, maintenance (par exemple l'IEC – 62351). D'autres au contraire seront plus utiles à la filière SSI. C'est par exemple le cas du document ISO/IEC TR 27019 qui précise certaines mesures du référentiel ISO 27002 pour les adapter aux SI industriels, et parlera donc davantage à des personnes travaillant habituellement sur le SI de gestion, car les différences à prendre en compte dans ce nouveau document seront réduites. Enfin, certaines publications sont très axées métier et pourront être plus aisément abordées par la filière SII (par exemple l'IEC – 61508).

Un dernier constat se rapporte au fait que certains documents ne sont pas écrits exclusivement pour une filière, mais ont été rédigés de manière à être accessibles et utiles à tous. C'est notamment le cas de l'IEC – 62443 qui est organisé par familles de documents en fonction des interlocuteurs visés.



Des documents ciblant des populations différentes

III.5. Des documents incontournables

L'étude a permis de relever un certain nombre de documents incontournables, selon les besoins du lecteur.

Trois catégories de documents ressortent ainsi :

- **Des incontournables pour démarrer** : ce sont des documents que toute personne appartenant à la filière SSI ou SII devrait avoir lu ou parcouru. En effet, les éléments sont posés de manière simple, avec des exemples concrets afin d'aborder clairement les problématiques liées à la sécurité des SII. Ils sont incontournables pour démarrer, mais ne représentent pas pour autant simplement des documents de sensibilisation. Ils sont suffisamment complets et concrets pour être utilisés.
- **Des incontournables pour implémenter** : ce sont des documents que l'on peut suivre pour s'évaluer, orienter sa démarche et l'implémenter.
- **Des incontournables pour approfondir** : ce sont des documents qui permettent de creuser particulièrement un sujet (comme la sûreté par exemple), ou un secteur.

Les documents incontournables

III.6. Vers une meilleure cohérence

Il existe une multiplicité de référentiels et d'autres sont encore en préparation. Par ailleurs, l'étude ne permet pas de faire émerger un référentiel nettement supérieur aux autres.

Pour autant, la série de normes *IEC – 62443* occupe une position centrale dans les échanges entre acteurs du secteur. Elle représente le seul référentiel à portée internationale qui a l'ambition de couvrir tous les secteurs. Mais cette famille de référentiels comporte encore de nombreux documents en cours de réalisation ou de révision et elle est donc encore très difficilement utilisable en l'état. Deux documents, le 2-1 (version en cours de révision en mai 2014) et le 3-3 (version publiée), peuvent aujourd'hui être considérés afin de construire un référentiel de cybersécurité. Cependant, il faudra les simplifier et retenir les idées clés plutôt que de prévoir une application directe. Certains de ces écueils sont connus et partagés par les comités de normalisation concernés. Des améliorations et des simplifications sont à attendre dans les années à venir.

Du fait de cette multitude de référentiels, nous constatons parfois certaines incohérences : les notions sont parfois abordées de façon différente et le vocabulaire utilisé n'est pas toujours le même. Cela démontre ainsi le besoin de monter en maturité sur l'ensemble de ces sujets liés à la sécurité des SII, comme ce fut le cas lors de l'émergence des premiers travaux consacrés à la SSI.

Cependant, les représentants des organismes en charge de ces référentiels en ont conscience et un mouvement d'uniformisation est sans doute à prévoir dans les années à venir.

Enfin, une particularité du domaine industriel est que l'aspect métier est très prégnant. C'est l'une des raisons pour lesquelles la littérature y est si riche et variée ; et cela représente une différence majeure avec la SSI classique qui elle s'applique de façon plus universelle à des secteurs variés.

IV. Les 5 phases clés vers la sécurisation d'un SI industriel

La pratique au quotidien des différents membres du groupe de travail ainsi que l'analyse de l'ensemble des référentiels ont permis de dégager des tendances et des étapes clés dans la sécurisation des SI Industriels.

IV.1. Phase 1 : Assimiler le métier industriel de l'entreprise et réaliser un état des lieux de la sécurité

La mise en œuvre d'une démarche de cybersécurité pour les SII suppose préalablement une connaissance du métier industriel de l'entreprise afin d'être en capacité de mieux appréhender l'impact des cyber-risques (humains, environnementaux, opérationnels, etc.) et de mieux définir les priorités d'action.

Cette première phase peut comporter 2 étapes :

1. **Définir un échantillon représentatif d'installations à auditer, sur la base des activités métiers industrielles de l'entreprise.** Une entreprise peut exercer un ou plusieurs métiers industriels (Chimie, métallurgie, mécanique, manufacture…) selon le type de produits (finis / intermédiaires…) ou services délivrés. Cet échantillon peut être identifié en échangeant avec les responsables de la sûreté et les responsables de sites de production.
2. **Cartographier le périmètre d'audit et évaluer le niveau d'exposition aux cyber-risques.** Une fois l'échantillon représentatif identifié, il convient de l'auditer afin de se faire une idée de l'exposition aux cyber-risques. Pour cela, 3 volets sont à prendre en compte :
    - **Environnement technique** : Certaines installations sont composées d'un empilement de technologies qui peuvent s'avérer particulièrement obsolètes et très peu ou pas informatisées (par exemple utilisant des technologies analogiques ou numériques non-IP). Si toutes les technologies empilées sont anciennes, leur exposition aux attaques informatiques peut donc dans certains cas être très limitée. Les interfaces externes (en particulier avec le SIG) sont à inclure.
    - **Sûreté industrielle** : La prise en compte de la dimension sûreté et des résultats des analyses de dangers est essentielle pour évaluer l'impact des scenarii de cyber-risques. En effet, pour pallier un événement grave, des mécanismes de sûreté (Automate Programmable de Sûreté (APS), sécurité câblée, Systèmes Instrumentés de la Sécurité (SIS)) peuvent être mis en place afin de pouvoir stopper le procédé de façon sûre.

Lors de l'évaluation de l'impact des cyber-risques, il est possible de prendre en considération les mesures de sûreté afin d'en réduire l'impact.

Néanmoins, cela est possible uniquement dans le cas où la sûreté est assurée par des mécanismes non automatisés ou par un système industriel indépendant (physiquement disjoint). De plus, il convient de ne pas négliger la probabilité que les mécanismes de sûreté soient utilisés contre l'installation elle-même en déni de service (déclenchement des mécanismes de sûreté pour arrêter la production).

- **Cybersécurité** : Une analyse d'écarts basée sur les bonnes pratiques de sécurité à caractère généraliste « IT »[1] ou des référentiels sectoriels ou spécialisés[2] peut être menée pour identifier les vulnérabilités.

Lors de cette étape, il est indispensable de rencontrer certains acteurs clefs afin de les sensibiliser à la démarche et obtenir leur adhésion pour la suite du projet :

- Le **Directeur du site** : Il fournira une vision des risques métiers, des objectifs de production et des contraintes inhérentes (par exemple : durée d'arrêt de maintenance réduite afin d'atteindre les objectifs de production).
- **Le Responsable Sûreté / Qualité-Sécurité-Environnement** car il peut préciser certaines exigences permettant de contrôler et tracer, notamment, l'accès physique aux sites, les interventions sur les systèmes informatiques et métiers et fournir des indications sur la réglementation applicable au métier.
- Le **gestionnaire des risques**, afin qu'il prenne en compte les cyber-risques conjointement à ceux visant l'organisation, en particulier sur le sujet de la sûreté.

Il est important de connaître la réglementation qui s'applique au métier car certaines imposent la mise en place des mesures de sécurité (par exemple : NERC, NRC, FDA).

[1] Par exemple en utilisant l'ISO 27002

[2] ANSSI, AIEA, NIST, FDA

- Le personnel opérant les installations : **Responsable de la maintenance, Responsable de l'informatique industrielle, Responsable de l'informatique de gestion, les agents de maîtrise, les automaticiens, les opérateurs, etc.** Il pourra fournir les mesures de sécurité existantes ainsi que les mécanismes de sûreté mis en place.

IV.2. Phase 2 : Sensibiliser le comité de direction aux vulnérabilités informatiques induisant des risques industriels

La réussite de la démarche passe par le soutien du comité de direction. En effet, la sécurisation des installations industrielles demandera un investissement humain et financier conséquent pour accompagner leur transformation. L'investissement étant porté, la plupart du temps, par les sites, ils devront arbitrer entre les objectifs de production, la maîtrise des budgets et l'investissement en matière de cybersécurité. Il faut donc un appui inconditionnel du comité de direction afin de faire aboutir la démarche.

Pour cela, plusieurs axes peuvent être abordés auprès du comité exécutif :

1. **Mettre en avant les impacts humains, environnementaux, opérationnels, financiers, de réputation, et de non-conformité réglementaire**[3]. Si l'entreprise exerce plusieurs métiers industriels, il est intéressant, sur la base des résultats de la phase 1, de déterminer leur profil de risque respectif afin d'établir les priorités d'action. Dans le cadre d'une approche consistante et cohérente de la gestion des risques au niveau de l'entreprise, il faut impérativement impliquer la Direction des Risques pour ceux liés aux SII.
2. **Démontrer par l'exemple** les vulnérabilités des systèmes industriels en réalisant par exemple des audits et des tests d'intrusion.
3. **Proposer un plan d'actions pragmatique et applicable à court terme** pour initier la mise sous contrôle des risques. Ce plan pourra notamment être accompagné des actions suivantes :
    - Nommer un sponsor au niveau du comité exécutif ;
    - Nommer un responsable cybersécurité des SII (RSSI-I) et des correspondants sécurité au niveau des sites ;
    - Créer un cadre de référence cybersécurité ;
    - Élaborer une stratégie formalisée et diffusée en interne de mise sous contrôle des risques, par exemple au travers d'un schéma directeur, d'une politique « chapeau » ou encore d'une circulaire.

[3] Le non-respect de certaines exigences peut entraîner l'arrêt de la production et avoir des impacts, par exemple, sur le cours de la bourse de l'entreprise ou sur la relation avec les clients.

IV.3. Phase 3 : Élaborer la Politique de Sécurité des Systèmes d'Information Industriels (PSSI-I)

En parallèle de l'action de sensibilisation du comité de direction, l'élaboration de la Politique de Sécurité des SII (PSSI-I) peut être lancée. Afin qu'elle soit acceptée et rapidement applicable au niveau opérationnel[4], il est fortement souhaitable que les opérationnels référents SII contribuent à sa conception.

> La signature du document par les référents peut permettre de donner plus de poids au document aux yeux du personnel des sites.

Cette phase peut se structurer en trois étapes :

1. **Créer un groupe de travail impliquant le personnel référent opérationnel (Responsable d'exploitation et de maintenance, Automaticiens, Architecte SII, etc.)** afin de :
    - Lister les contraintes qui constituent un obstacle à la mise en œuvre : Opérations nécessitant le redémarrage des automates, freins contractuels, obligations réglementaires, redéveloppement coûteux d'applications obsolètes…
    - Identifier les mesures de sécurité en veillant à mettre en avant les Quick Wins[5]. Ces mesures doivent être concrètes et directives afin de faciliter leurs mises en œuvre.
2. **Structurer les résultats du groupe de travail en adoptant une approche graduée** basée sur le concept de niveaux de risque, tel que peuvent le proposer l'IEC, l'AIEA ou encore l'ANSSI[6]. On pourra dans ce cas ventiler les mesures de sécurité par niveau de risque cyber en se basant sur leur robustesse (ou efficacité) intrinsèque. Ainsi, plus le niveau de risque est élevé, plus les mesures de sécurité doivent être renforcées et plus les zones concernées doivent être séparées de l'Internet et des réseaux de gestion par plusieurs niveaux de sécurité logiques et physiques.

[4] La dernière partie de ce document précise les principaux référentiels utiles pour démarrer ce type de démarche.

[5] Mesure ayant un faible impact technique, humain et financier et ne nécessitant pas l'arrêt du procédé.

[6] Ces référentiels sont présentés dans la dernière partie du document.

3. **Élaborer un référentiel d'application de la PSSI-I.** Ce référentiel (directive, guide) présentera une méthodologie de mise en œuvre de la PSSI-I. Les thèmes pourront être, entre autres :
    - Découper le SII en un ensemble homogène de zones (ou sous-systèmes) hébergeant une ou plusieurs fonctions métiers ayant une forte interdépendance ;
    - Évaluer le niveau (ou classe) de cybersécurité de chacune de ces zones ;
    - Appliquer les mesures de sécurité afférentes au niveau de cybersécurité identifié. Ces mesures devront être réalistes par rapport au niveau de maturité et d'investissement prévu. Une vision idéaliste pourra démotiver la structure, une vision minimaliste ne pas couvrir les risques majeurs.

IV.4. Phase 4 : Décliner la PSSI-I au niveau opérationnel

Une fois le cadre établi et le support du comité exécutif obtenu, une trajectoire de mise en œuvre doit être définie, validée au plus haut niveau décisionnel et déclinée concrètement avec des mesures précises et opérationnelles. Il faudra s'assurer que les éléments suivants sont pris en compte :

- Définir un délai de 2 à 3 ans maximum.
- Budgétiser l'investissement nécessaire à la mise en œuvre de cette stratégie.
- Travailler en mode projet.
- Faire valider au plus haut niveau décisionnel afin de s'assurer du soutien de l'ensemble des parties prenantes.

Cette phase peut-être structurée autour de 3 étapes clefs :

1. **Nommer la chaîne fonctionnelle cybersécurité industrielle et mettre en place une instance de gouvernance du projet ou du programme.**
   Il est primordial que l'ensemble des acteurs soient identifiés et nommés au niveau central ainsi qu'au niveau des sites avant le démarrage du projet. L'animation de ces acteurs pourra se faire par le biais d'une instance de gouvernance pilotée de manière centrale afin de permettre une meilleure coordination des actions, faciliter le partage d'expérience et identifier des pratiques ou solutions qui pourraient être standardisées entre les sites.

Afin d'acquérir la légitimité auprès du personnel local, il est conseillé que le correspondant sécurité local soit choisi au sein du personnel métier et non de l'IT, par exemple le Responsable de l'Informatique Industrielle.

2. **Mettre en place des « Quick Wins »** sur le plus de sites possibles dans un délai très court, inférieur à 6 mois (par exemple : revue des flux ouverts, encadrement de l'usage des médias amovibles, sensibilisation sur les pratiques de sécurité, gestion des changements, etc.)

3. **Mener la démarche dans un premier temps sur les sites critiques.** L'identification devra être faite simplement au regard du profil de risque des métiers de l'entreprise couplé à l'analyse des impacts suivants : humains, environnement, opérationnel, financier, réputation, conformité légale et réglementaire.

IV.5. Phase 5 : Maintenir sous contrôle les cyber-risques

Pour assurer la maîtrise des cyber-risques, il est nécessaire de mettre en place une gouvernance permettant de maintenir un niveau de cybersécurité adapté à l'évolution de la menace. Leur mise en place peut s'appuyer sur les normes internationales qui suivent souvent une approche processus calquée sur la notion d'amélioration continue et le modèle PDCA (Plan – Do – Check – Act).

Quand les sites industriels sont autonomes (budget, ressources, etc.), il est conseillé que ces processus de gouvernance soient pilotés localement et de les intégrer au système de management local, ce qui permettra d'avoir une politique de sécurité mieux adaptée au contexte du site et surtout mieux acceptée.

Les processus clefs de gouvernance à mettre en œuvre ou à faire évoluer sont les suivants :

- **Gérer les cyber-risques** et assurer une **veille continue** afin de définir les fondamentaux en termes de protection des SII contre les cyber-risques et d'intégrer les nouvelles vulnérabilités ou menaces émergentes. Cette veille pourra être centralisée.
- **Former/Sensibiliser** tous les membres du personnel pour faire prendre conscience des cyber-risques et de leur responsabilité pour les maîtriser.

- **Intégrer la sécurité dans les projets et les évolutions** afin d'acquérir de la visibilité sur les projets métiers qui amènent de nouvelles fonctionnalités pouvant accroître l'exposition aux cyber-risques, mobilité, capteurs intelligents, télémaintenance, etc. et pouvoir les maîtriser. Une sélection des projets les plus sensibles pourra être réalisée pour initier le processus.
- **Gérer les incidents de sécurité** pour détecter, analyser et décider de la réponse appropriée à un incident de sécurité.
- **Auditer et assurer un contrôle interne** pour s'assurer de la conformité du SII à la PSSI-I.
- **Piloter les plans d'actions** élaborés suite aux constats d'audits ou lancés pour faire face à de nouvelles menaces ou vulnérabilités détectées.
- **Réaliser des revues de direction périodiques** permettant d'analyser la situation et d'ajuster le programme de sécurité ou encore de donner de nouvelles orientations stratégiques visant à renforcer la maîtrise du cyber-risque.

V. Annexes

V.1. Documents analysés

Fiche de Lecture	Éditeur	Publication	Pages
A Framework for Aviation Cybersecurity	AIAA	2013	16
La sécurité informatique dans les installations nucléaires	AIEA	2013	91
La sécurité des SII - Méthode de classification et mesures principales et détaillées	ANSSI	2014	164
Maîtriser la SSI pour les systèmes industriels	ANSSI	2012	40
API 1164, Pipeline SCADA Security	API	2009	64
Securing Control and Communications Systems in Transit Environments - Part II : Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones	APTA	2013	78
Securing Control and Communications Systems in Transit Environments - Part 1 : Elements, Organization and Risk Assessment / Management	APTA	2010	29
Informationstechnik in Prozessüberwachung und -steuerung	BSI	2008	5
Good Practice Guide "Process Control and SCADA security"	CPNI	2008 – 2011	215
Cyber Security Assessments of Industrial Control Systems - A Good Practice Guide	CPNI	2011	66
Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security	CSWG	2010	597
21 étapes pour améliorer la cybersécurité des réseaux des SCADA	DoE	2002	10
Pratique recommandée : améliorer la cybersécurité des systèmes de contrôle industriels avec des stratégies de défense en profondeur	DoH	2009	44
Can we learn from SCADA security incidents	ENISA	2013	10
Window of exposure ... a real problem for SCADA systems? - Recommendations for Europe on SCADA patching	ENSIA	2013	19
Appropriate security measures for Smart Grids	ENISA	2012	84
Protecting industrial control systems - Recommandations for Europe and member states	ENISA	2011	81

IEC 62443 – Security for industrial Automation and Control Systems	IEC	2013 - 2016	1010
IEC 62351 – Spécification technique – gestion des systèmes électriques et échanges d'informations – Sécurité des données et des communications	IEC	2013	500
IEC 61508 : Standard for Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems	IEC	2010	400
TR IEC 62210 – Contrôle et communications associées pour les systèmes électriques – sécurité des communications et des données	IEC	2003	52
ISO/IEC TR 27019	ISO/IEC	2013	320
Cyber Security Procurement Language for Control Systems	INL	2008	120
Critical Infrastructure Protection Standards	NERC	2012	320
Framework for Improving Critical Infrastructure Cybersecurity	NIST	2014	41
Guide to Industrial Control Systems (ICS) Security	NIST	2011 – 2013	155
Regulatory Guide 5.71 – Cyber security programs for nuclear facilities	NRC	2010	105
Protection of digital computer and communication systems and networks	NRC	2009	2
Cybersecurity Through Real-Time Distributed Control Systems (RTDCS)	OAK Ridge / DoE	2010	30
Methodology for Prioritizing Cyber-vulnerable Critical Infrastructure Equipment and Mitigation Strategies	Sandia	2010	42
Control System Devices : Architectures and supply Channels Overview	Sandia	2010	70
Security Framework for control System Data classification and Protection	Sandia	2007	33
Framework for SCADA Security Policy	Sandia	2005	6
Guide sur l'évaluation des vulnérabilités dans le cadre des standards CIP	Sandia	2008	19
SCADA and Process Control Survey	SANS	2013	18
Attack Methodology Analysis: Emerging Trends in Computer-Based Attack Methodologies and Their Applicability to Control System Networks	US – CERT	2005	30
Process Control Domain – Security Requirements for vendors	WIB	2010	52

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

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