CLUSIF

Cybersécurité des Systèmes Industriels Panorama des référentiels

2ème édition

Octobre 2019

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:

Christophe	AUBERGER	*Fortinet*	Guillaume	LE HEGARET	*Setec ITS*
Patrice	BOCK	*Bock Conseil*	Mathieu	HERNANDEZ	*Ineo Cyber Sécurité*
Jean	CAIRE	*RATP*	Guillaume	MALGRAS	*Ineo*
Anthony	DI PRIMA	*Wavestone*	Thierry	MATUSIAK	*IBM*
Loïc	GUEZO	*TrendMicro*	Thierry	PERTUS	*CONIX*
Philippe	JEANNIN	*RTE*	Jérôme	RICHARD	*Econocom digital security*

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

Sommaire

- Présentation du Groupe de Travail « Cybersécurité des Systèmes Industriels »
- Présentation du document et de la démarche adoptée
  - Objectifs du document
  - Présentation de la démarche
  - Comment lire les fiches de lecture?
- Tendances observées
- Les incontournables de cette édition du panorama

Présentation du groupe de travail “Cybersécurité des Systèmes Industriels”

GT 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]. Ce document permet de sensibiliser aux enjeux de la sécurité des systèmes industriels.

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

Présentation du document et de la démarche adoptée

Objectifs du document

- Suite à la publication en 2014 du dossier technique Cybersécurité des systèmes industriels: Par où commencer?[1] présentant un panorama des référentiels les plus pertinents en milieu industriel et une synthèse des bonnes pratiques en matière de gouvernance de la cybersécurité, le GT a travaillé sur la mise à jour de l'annexe regroupant l'ensemble des fiches de lecture de ce panorama.

- L'objectif de ce document est de:
  - Réévaluer les fiches des référentiels ayant fait l'objet d'une révision depuis la première édition du panorama;
  - Intégrer de nouveaux référentiels publiés depuis la première édition du panorama;
  - Réévaluer plus finement les référentiels selon de nouveaux secteurs d'activité, populations ainsi que des thématiques clés préalablement définies.

[1] https://clusif.fr/publications/cybersecurite-des-systemes-industriels-par-ou-commencer-synthese-des-bonnes-pratiques-et-panorama-des-referentiels/

Présentation de la démarche

Vision globale

1. Définition des secteurs et catégories d'acteurs ciblés
2. Définition des thématiques de sécurité sur lesquelles les référentiels ont été évalués
3. Sélection des référentiels issus du précédent panorama à intégrer dans la mise à jour
4. Identification des nouveaux référentiels à intégrer dans le nouveau panorama
5. Mise à jour des anciennes fiches de lecture et rédaction de nouvelles pour les nouveaux référentiels
6. Analyse globale des référentiels

Présentation de la démarche

Définition des populations ciblées

Dans un premier temps, le groupe de travail a listé l'ensemble des acteurs amenés à participer à la cybersécurité des systèmes industriels quels que soient leurs rôles.
Ces acteurs ont alors été rassemblés sous différentes catégories.
Ci-dessous l'ensemble de ces catégories définies ainsi que les acteurs ciblés :

Nom de la catégorie	Populations incluses dans la catégorie
MOA	*Métier, Conduite d'affaire*
MOE	*Conduite de projet technique, Ingénierie, Intégrateurs, Ensembliers*
Autorités	*Autorités publiques, Investisseurs, Partenaires, Régulateurs*
Fournisseurs	*Fournisseurs de solutions, Constructeurs, Equipementiers, Editeurs, Revendeurs*
Exploitants	*Exploitants, Informatique industrielle, Opérateurs*
Mainteneurs	*Mainteneurs, Administrateurs*
RSSI	*RSSI industriel, Responsable cybersécurité*
Audit & Risk Mngr.	*Auditeurs, Risk Managers, Qualité et contrôle permanent*

Présentation de la démarche

Définition des secteurs d'activité

Le GT a aussi redéfini les principaux secteurs et sous-secteurs d'activité dans lesquels peuvent être retrouvés des systèmes industriels.
Ce travail a été effectué indépendamment des sujets traités par les référentiels.
La classification suivante a été retenue:

Industrie

- Industrie manufacturière
- Industrie métallurgique
- Industrie chimique

Transport

- Terrestre
- Maritime & Fluvial
- Aérien

Energie

- Gaz & Hydrocarbures
- Électrique
- Nucléaire

Gestion de l'eau

Santé

Multi-domaines / Framework

Présentation de la démarche

Définition des thématiques de sécurité

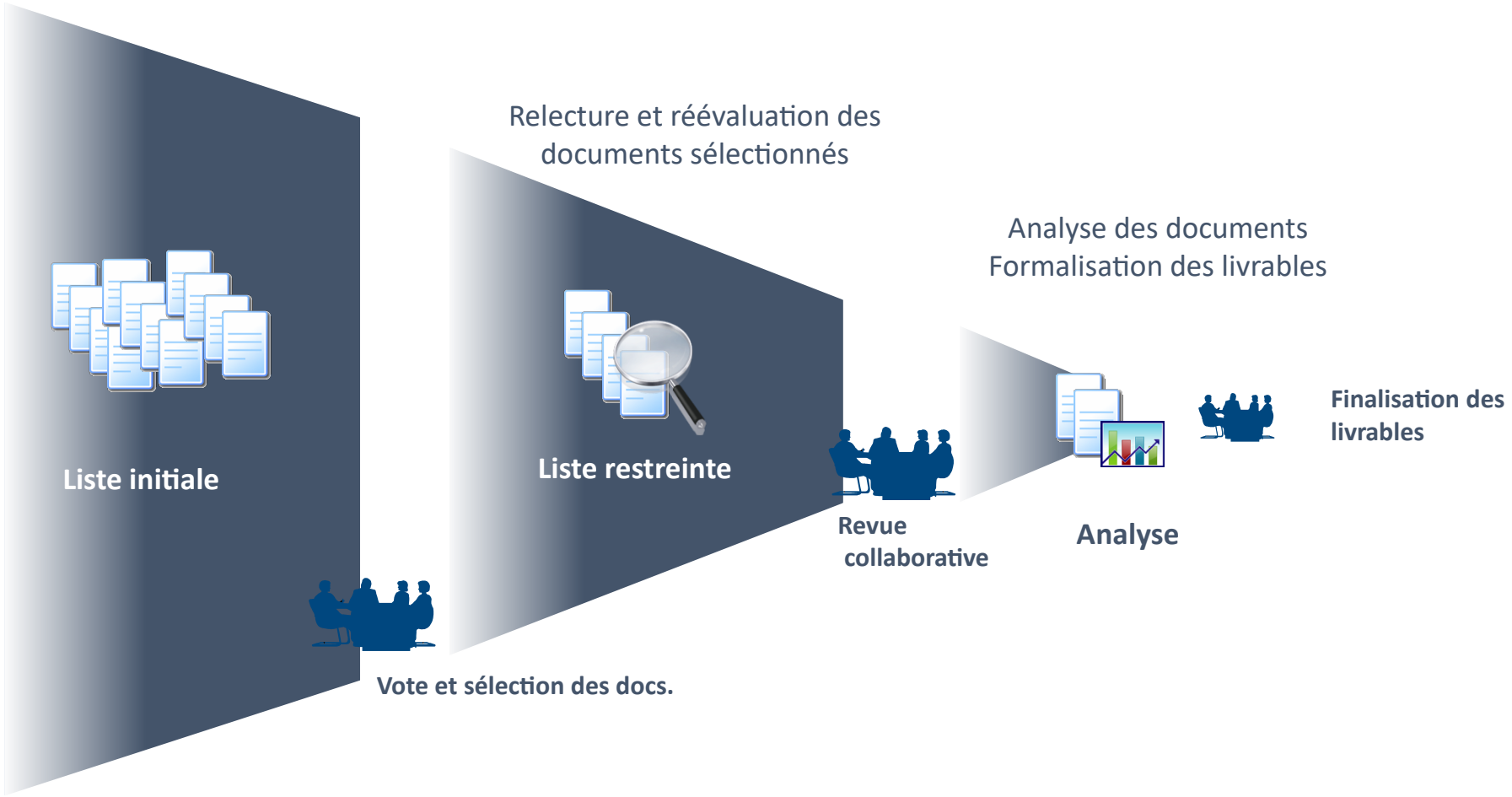
Tous les documents, qu'ils soient issus de l'ancien panorama ou les nouveaux documents inclus, ont été évalués selon les thématiques de sécurité suivantes :

Thématique	Exemples de sujets abordés		Thématique	Exemples de sujets abordés
Gouvernance	*Standard, Framework, Système de management, Conformité règlementaire et normative, Certifications, Organisation, Rôles et responsabilités, Sensibilisation, Indicateurs, Articulations avec les autres systèmes de management (sûreté, SIE, …), etc.*		**Maintien en condition de cybersécurité**	*Veille sur les menaces, Veille sur les vulnérabilités, Gestion des correctifs, Maintenance, etc.*
Modélisation et cartographie	*Vues fonctionnelles et techniques, Strates CIM, Cartographie des flux, etc.*		**Expertises en cybersécurité**	*Audit, Supervision, Cybersurveillance, Réponse à incident, etc.*
Management du risque et classification	*Démarche d'homologation, Méthodes de management de risques, Niveaux de cybersécurité, Zoning, Relation avec la sûreté, Veille prospective / anticipation du risque, etc.*		**Relation avec les tiers/ externalisation des services**	*Bonnes pratiques de rédaction de cahier de charges, Clauses contractuelles spécifiques (auditabilité, …), etc.*
Architecture et conception	*Conception, Cloisonnement, Résilience, Contrôle d'accès, Infrastructure de sécurité, Développement sécurisé, etc.*		**Étude de cas**	*Cas pratiques, Retours d'expérience, Rapports d'incidents, etc*
Intégration et déploiement	*Fiabilité des codes sources, Durcissement, Tests et recette, etc.*			

Présentation de la démarche

Sélection des référentiels et rédaction des fiches

Identification des documents par l'ensemble des membres du groupe
Sélection des documents de l'ancien panorama toujours d'actualité



Comment lire les fiches de lecture?

Secteurs ciblés par les rédacteurs du référentiel

Résumé du contenu du document

Synthèse du document

Titre	ANSSI - La cybersécurité des systèmes industriels - *Maîtriser la SSI pour les systèmes industriels | Cas pratique*						
Date de publication	2012	**Éditeur**	ANSSI	**Volume (pages)**	40 | 52	**Accès**	Gratuit

Secteur :	Multi-domaines / Framework

Populations concernées :			
MOA	MOE	Fournisseurs	Exploitants
Mainteneurs	RSSI		

Contenu	Guide de recommandations organisationnelles et techniques pour la sécurité des systèmes industriels et étude de cas pratique

Synthèse

Il s'agit d'un guide de bonnes pratiques accompagné d'une annexe traitant d'une étude de cas.

Le guide est organisé de la façon suivante : il présente dans un premier temps le contexte et les enjeux de la sécurité des SI industriels, en prenant soin de bien mettre en parallèle le SI de gestion et le SI Industriel, partant du principe que le lecteur et plus familier avec le premier contexte. En plus de mettre en regard les deux univers, le guide présente également un paragraphe visant à faire tomber certaines idées reçues fréquemment véhiculées concernant les SI Industriels : la prétendue sécurisation intrinsèque aux contextes industriels (isolation physique, technologies propriétaires) ou encore des prétendues incompatibilités entre SSI et sureté de fonctionnement.

Le guide présente ensuite des généralités sur la cybersécurité, avec notamment une description succincte des grandes typologies d'attaques (ciblées, challenge, non ciblées), les vulnérabilités des SI Industriels ainsi que les impacts d'une potentielle attaque pour une entreprise (dommages matériels, corporels, perte de CA, impact environnemental, vol de données, etc.)

La partie centrale du document (8 pages) traite quant à elle de l'intégration d'une démarche SSI adaptée au contexte des systèmes industriels. Les grandes thématiques sont abordées sur l'ensemble des phases du cycle de vie d'un projet (amont : analyse de risques, prise en compte de la SSI dans les achats (CCTP), etc. et aval : maintenance (GMAO), veille, surveillance, PRA/PCA, etc.), et présente des exemples concrets et précis avec des recommandations de haut niveau.

Le document propose également 2 annexes intéressantes : la première développe les principales vulnérabilités rencontrées par les SI Industriels (SII), la seconde propose un recensement de 13 bonnes pratiques sur la sécurité des SII (bonnes pratiques sous forme de tableau avec : motivation, méthode périmètre, contraintes, moyens de gestion des contraintes).

En complément, une étude de cas relativement détaillée présente sous la forme de retour d'expériences les situations auxquelles peut se retrouver confronté un RSSI ou un chargé de mission découvrant au fil de l'eau « l'historique des écarts » d'un site industriel et la façon, point par point, dont il convient de remettre les choses en ordre, moyennant une démarche méthodologique rigoureuse et un plan d'actions organisationnelles et opérationnelles. En annexes, le document aborde des thématiques types comme le déport d'écran depuis le SI de gestion, l'usage des médias amovibles ou les relations d'approbation entre domaines AD, puis termine sur des consignes d'exploitation (10 règles d'or).

Titre du document suivi par diverses informations

Populations principalement concernées par le référentiel si :

- Elles ont été explicitement ciblées par les rédacteurs du référentiel
- Elles ont été considérées par le GT comme pouvant être concernées par le document au vu du contenu de ce dernier

Comment lire les fiches de lecture?

Appréciation du GT quant à la pertinence du document dans une démarche de sécurisation des systèmes industriels. Le fond ainsi que la forme du document ont été évalués selon le barème suivant:

★★★★★ Document référence
★★★★ Document avec un fond pertinent, mais les messages ne sont pas clairement transmis
★★★ Document avec un manque d'éléments sur le fond pour la population prétendument ciblée
★★ Document avec un manque de plusieurs éléments sur le fond
★ Document avec plusieurs manquements au niveau du fond ainsi que la forme

Pertinence	Avis
★★★★	Document très pédagogique et accessible pour les néophytes, pouvant constituer un excellent point d'entrée sur le sujet de la cybersécurité des SII. Même si les recommandations essentielles peuvent paraître peut-être un peu minim… l'impact sur l'audience n'en est que plus important. L'étude de cas apporte une réelle valeur ajoutée au guide, en imm… véritablement le lecteur in situ au sein d'un environnement industriel plus vrai que nature, le tout assorti d'une démarche de progrès.

Avis du GT sur le référentiel dans sa globalité

Thématiques de sécurité		
Gouvernance	Modélisation et cartographie	Management du risque et classification
★★	★★★★	★★
Architecture et conception	Intégration et déploiement	Maintien en condition de cybersécurité
★★★★	★★★★	★★★★
Expertises en cybersécurité	Relation avec le… …ternalisation des ser…	Etude de cas
★★		

Évaluation du document selon les thématiques prédéfinies selon le barème suivant:

★★★★★ Approche différenciante et pertinente quant au traitement de la thématique
★★★★ Sujet adressé avec profondeur, qualité, pertinence
★★★ Sujet adressé avec une profondeur de traitement et une pertinence convenable
★★ Sujet évoqué, manquant de profondeur et/ou approche peu pertinente ou inadaptée
★ Sujet évoqué mais non traité et/ou renvoyant vers un autre document.
Approche non abordée
N/A Approche non abordée car le document ne s'y prête pas

Tendances observées

Répartition géographique des éditeurs de référentiels

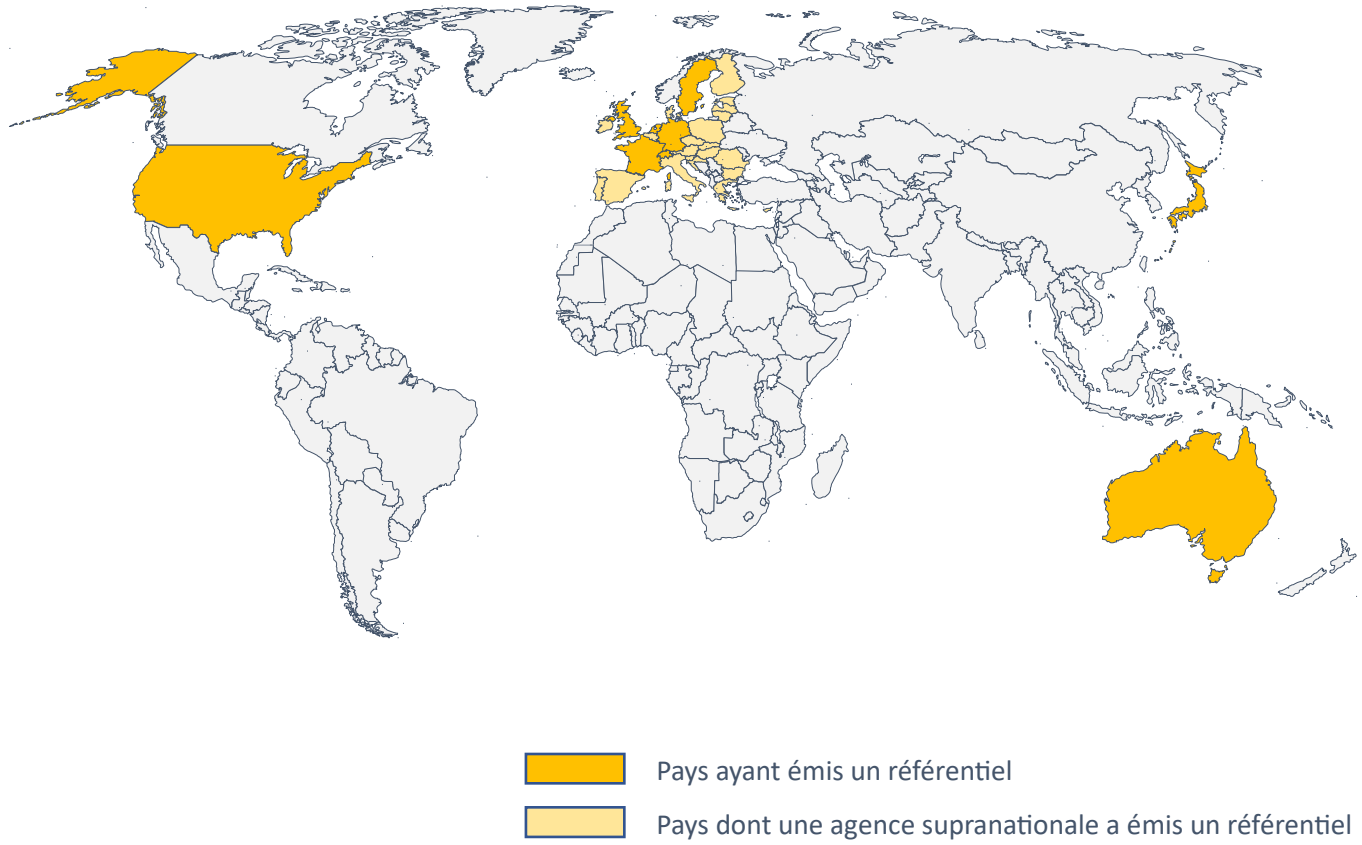
Pour cette édition du panorama des référentiels, le GT a sélectionné les documents selon 2 principaux critères :

- Le document doit traiter de la sécurité des systèmes industriels;
- Le document a été rédigé ou traduit dans une langue maîtrisée par les membres du GT (Français, Anglais et Allemand).

L'origine du pays émetteur n'a pas été un critère de sélection des référentiels.

Cette carte montre les pays dont sont issus les organismes émetteurs de référentiels étudiés par le Clusif.

Il a été noté une l'entrée de nouveaux pays émetteurs de référentiels par rapport à la première édition du panorama: par exemple : Allemagne, Australie, Japon et Suède. Ceci témoignerait d'une prise de conscience ainsi que d'une appropriation du sujet à l'échelle mondiale.



Quelle importance aux référentiels sectoriels?

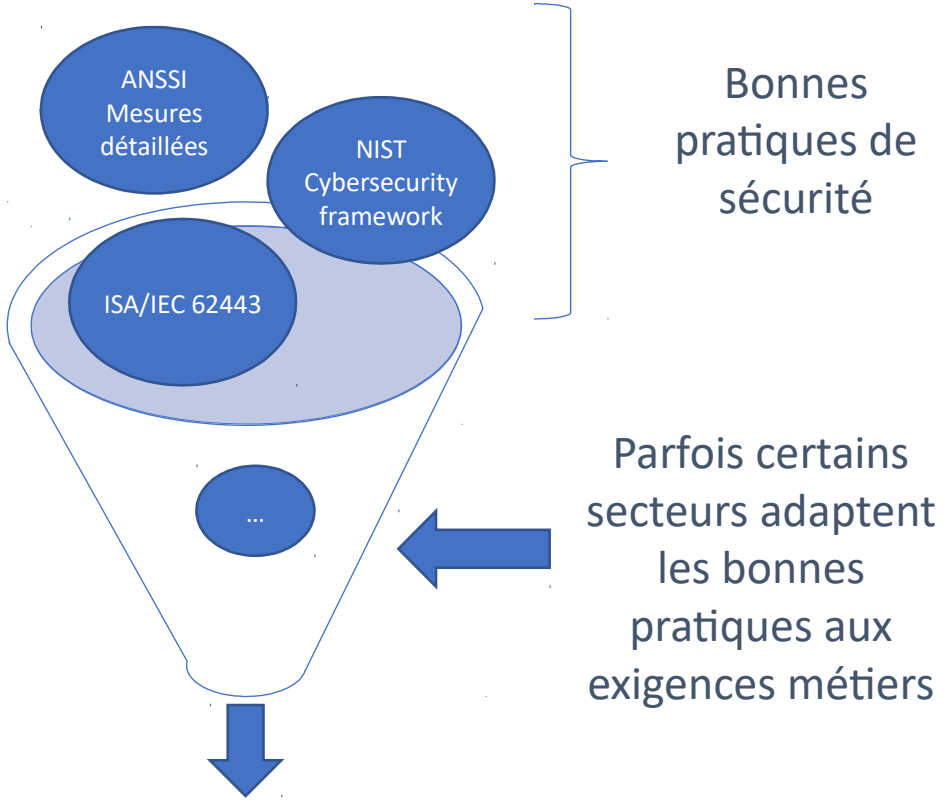
La répartition des référentiels de sécurité étudiés selon les secteurs d'activité a montré que ces derniers ne présentaient pas le même nombre de publications. De plus, certains secteurs d'activité possèdent peu de référentiels qui, pour la plupart, sont payants. Ces référentiels ne sont partagés que par les acteurs de ce secteur comme par exemple le secteur aérien. Au delà de cette différence sectorielle, il convient de noter que la plupart des référentiels tous secteurs confondus partagent des bonnes pratiques de sécurité communes via des références vers des normes ou framework.

Plusieurs référentiels sectoriels font référence aux documents à vocation normative (par exemple la série ISA/IEC 62443) ou des documents présentant des bonnes pratiques applicables à l'ensemble des systèmes industriels (par exemple les guides de l'ANSSI). Pourquoi alors cette multitude de référentiels sectoriels?

Ceci s'explique par un besoin initial qui était de produire des documents pour les systèmes industriels spécifiques afin de prendre en compte les spécificités sectorielles.

Dorénavant, la tendance est plus à réutiliser les concepts et mesures de sécurité répondant à des enjeux de sécurité communs (cloisonnement des systèmes, population diverse et non sensibilisée, durée de vie des systèmes et maintien en conditions de sécurité …). Ainsi la plupart des documents sectoriels préconisent les mêmes mesures de sécurité.

Enfin, ceci n'enlève rien à l'intérêt que peut représenter une publication sectorielle. En effet, un référentiel sectoriel peut faire office de document de référence et/ou autorité sur le secteur ou sous-secteur d'activité. Il faudra cependant éviter une multitude de tels documents pour ne pas disperser les efforts, interprétations et donc mises en œuvre.

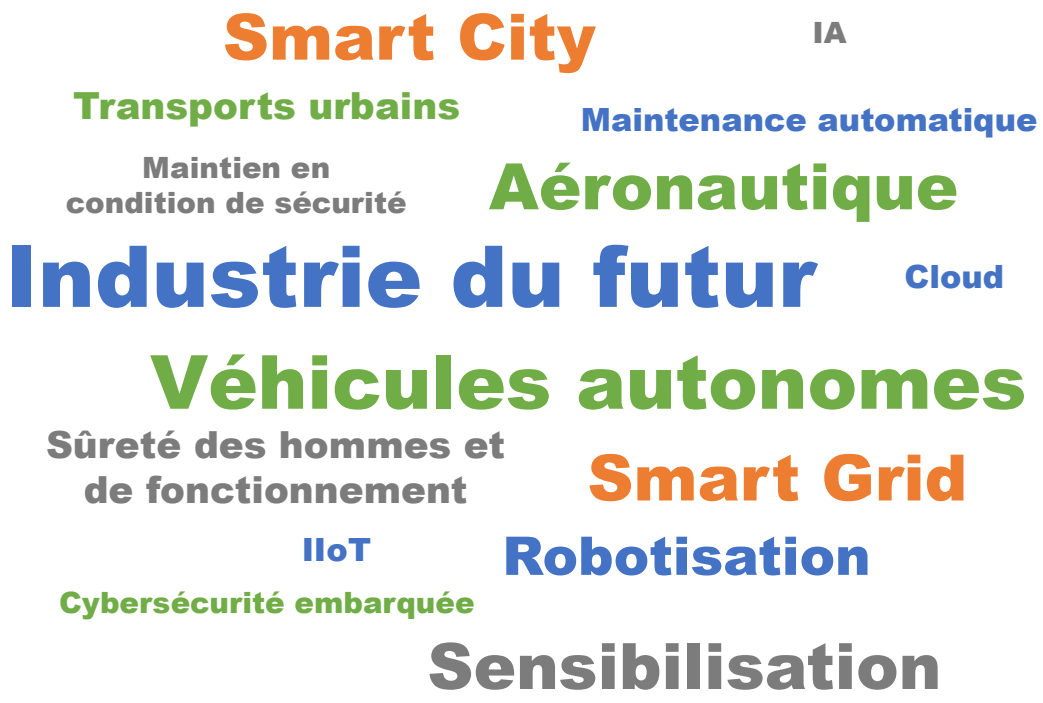


Quelle tendance pour les années à venir?

Les référentiels primo-entrants dans cette édition ou ceux ayant été révisés depuis la première édition du panorama sont globalement en ligne avec les évolutions des systèmes industriels ainsi que certains des enjeux liés à leur sécurisation.

En effet, les référentiels suivent l'évolution de l'industrie avec l'introduction de l'IoT dans les systèmes industriels (IIoT) mais aussi l'évolution des secteurs en traitant des problématiques de véhicules autonomes par exemple. De nouveaux référentiels apparaissent, dus à la numérisation complète de la société et la convergence informatique classique, informatique industrielle et objets connectés (par exemple la série de documents de l'ENISA sur les smart things).

Cependant, il faut aussi noter que certaines thématiques (par exemple le maintien en condition de sécurité, l'adhérence de la cybersécurité avec les études de sûreté de fonctionnement …) n'ont pas été traitées de manière approfondie tandis que d'autres n'ont pas été abordées par les référentiels. Nous pensons que ces thématiques devraient faire l'objet d'une analyse plus avancée. Cette analyse ne devant pas être synonyme de multiplication de référentiels, puisque comme en témoigne cette édition du panorama des référentiels, la littérature est déjà assez fournie.



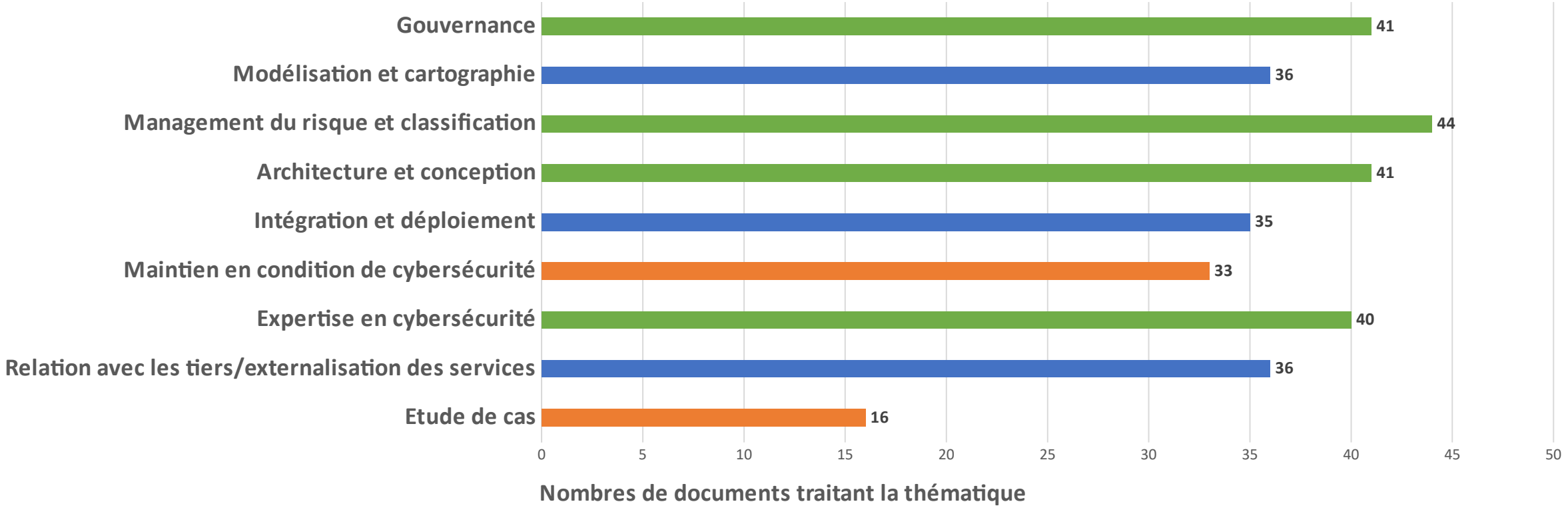
Les référentiels incontournables de cette édition du panorama

Les incontournables de cette édition du panorama

Quelques chiffres

55 documents étudiés dont **26** primo-entrants ou en version révisée depuis la première édition du panorama.

Voici les thématiques associées au nombre de référentiels ayant traité chacune d'entre elles (les référentiels peuvent traiter plusieurs thématiques en même temps):



Les incontournables de cette édition du panorama

Les incontournables par thématique

Gouvernance	AIEA - La sécurité informatique dans les installations nucléaires CPNI – Framework overview DHS - Recommended practice: Improving industrial control systems cybersecurity with defense-in-depth strategies ENISA - Appropriate security measures for smart grids - Recommendations for Europe and Member States ISA/IEC - IEC 62443 Part 2.1 : Industrial automation and control system security management system NIST - Framework for Improving Critical Infrastructure Cybersecurity (v1.1)
Modélisation et cartographie	ANSSI - La cybersécurité des systèmes industriels | Mesures détaillées DHS - Recommended practice: Improving industrial control systems cybersecurity with defense-in-depth strategies ISA/IEC – IEC 62443 Part 1.1 - Models and concepts ISA/IEC - IEC 62443 Part 3.2 : Security risk assessment and security levels NIST - SP800 82 R2 – Guide to Industrial Control Systems (ICS) Security
Management du risque et classification	AIEA - La sécurité informatique dans les installations nucléaires ANSSI – Exigences de cybersécurité pour les prestataires d'intégration et de maintenance de systèmes industriels DHS - Recommended practice: Improving industrial control systems cybersecurity with defense-in-depth strategies ISA/IEC - IEC 62443 Part 2.1 : Industrial automation and control system security management system NIST - SP800 82 R2 – Guide to Industrial Control Systems (ICS) Security

Un document est considéré incontournable lorsqu'il a eu 5 étoiles sur la thématique adressée

Les incontournables de cette édition du panorama

Les incontournables par thématique

Architecture et conception	ANSSI - La cybersécurité des systèmes industriels | Mesures détaillées DHS - Recommended practice: Improving industrial control systems cybersecurity with defense-in-depth strategies ISA/IEC – IEC 62443 Part 3.2 : Security risk assessment and security levels ISA/IEC – IEC 62443 Part 4.2 : Technical security requirements for IACS components NIST – SP800 82 R2 – Guide to Industrial Control Systems (ICS) Security
Intégration et déploiement	ANSSI - Exigences de cybersécurité pour les prestataires d'intégration et de maintenance de systèmes industriels ANSSI - La cybersécurité des systèmes industriels | Mesures détaillées ISA/IEC – IEC 62443 Part 4.1 : Secure product development lifecycle requirements NIST - SP800 82 R2 – Guide to Industrial Control Systems (ICS) Security SAE – Surface vehicle recommended practice
Maintien en condition de cybersécurité	ANSSI - La cybersécurité des systèmes industriels | Mesures détaillées ISA/IEC – IEC 62443 Part 2.3 : Patch management in the IACS environment

Un document est considéré incontournable lorsqu'il a eu 5 étoiles sur la thématique adressée

Les incontournables de cette édition du panorama

Les incontournables par thématique

Expertises en cybersécurité	ANSSI - La cybersécurité des systèmes industriels | Mesures détaillées
Relation avec les tiers / externalisation des services	ANSSI – Exigences de cybersécurité pour les prestataires d'intégration et de maintenance de systèmes industriels ENISA - Window of exposure… a real problem for SCADA systems? - Recommendations for Europe on SCADA patching ISA/IEC - IEC 62443 Part 3.3 - System security requirements and security levels ISA/IEC - IEC 62443 Part 4.1 : Secure product development lifecycle requirements
Étude de cas	ANSSI - La cybersécurité des systèmes industriels | Cas pratique ANSSI - Cas pratique d'un tunnel routier

Un document est considéré incontournable lorsqu'il a eu 5 étoiles sur la thématique adressée


LES DOSSIERS TECHNIQUES

Cybersécurité des Systèmes
Industriels Panorama des référentiels
2ème édition
Annexes : Fiches de lecture

Octobre 2019

CLUSIF

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

Les fiches de lecture des **52 documents analysés** se trouvent dans l'annexe de ce document, accessible via ce lien:

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