LES DOSSIERS TECHNIQUES

Cybersécurité des systèmes industriels : Par où commencer ?

Synthèse des bonnes pratiques et panorama des référentiels

Annexes : Fiches de lecture

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

Afin de réaliser son étude, le groupe de travail a d'abord rassemblé l'ensemble des référentiels et publications existant à sa connaissance dans le domaine de la sécurité des SI industriels.

Ensuite, il s'est attaché à faire ressortir les documents les plus pertinents pour son étude. Pour se faire, le groupe de travail s'est organisé de la manière suivante : un vote de sélection initiale a été réalisé par chacun des membres sur les documents qu'il connaissait ou qu'il avait déjà utilisés. Les documents les mieux notés ont fait l'objet d'une analyse détaillée et d'une fiche de lecture. Celles-ci ont été rédigées pour chaque publication par une ou plusieurs personnes.

Ces fiches ont été conçues de façon à proposer des critères factuels permettant de classifier les publications relues (secteur, population visée, typologie de SII).

Une évaluation subjective (sous forme de notation en « étoile ») a été réalisée, en fonction de la pertinence des documents (qualité du fond et de la forme). Enfin, les différents acteurs de l'étude se sont rassemblés pour une relecture croisée des fiches de lecture. Les documents s'étant vu attribuer une note supérieure ou égale à quatre étoiles ont été a minima relus par deux personnes du groupe de travail et ont été retenus pour le livrable principal.

L'ensemble des fiches de lectures rédigées durant le groupe de travail est présenté dans l'annexe ci-dessous. Elles sont classées par éditeur puis par nom du document.

Il est à noter que cette annexe constitue une photographie des documents recensés au 31 mars 2014.

II. Annexes : fiches de lecture

Titre	*A Framework for Aviation Cybersecurity*

Date de publication	2013	Éditeur	AIAA	Volume (pages)	16	Accès	gratuit

Synthèse	« Decision paper » visant les directions dans le secteur de l'aviation

Synthèse

Ce document est un « decision paper » provenant de l'AIAA (American Institute of Aeronautics and Astronautics). Il s'agit d'un document de haut niveau, à destination des responsables métiers et des directions d'entreprise dans le secteur de l'aéronautique. L'analyse est réalisée très largement, incluant par exemple les éléments relatifs aux réseaux embarqués dans les avions comme les éléments liés au contrôle aérien.

Il présente les évolutions de l'aéronautique et le recours de plus en plus fréquent au système d'information pour assurer l'ensemble des activités du secteur. Il dispose d'un schéma très intéressant sur les acteurs et les flux de données dans le secteur.

Il présente des actions à réaliser (analyse de risque, sensibilisation, mise en place d'un programme…). Ces éléments restent à très haut niveau, ce qui est cohérent vu l'objectif du document, mais qui ne permettra pas à un RSSI ou à un RSII de construire opérationnellement son programme.

Il s'agit au final d'un document de sensibilisation des directions dans le secteur de l'aéronautique.

Pertinence	Avis
★	Ce document est un premier support pour sensibiliser les directions métiers dans le secteur de l'aéronautique au sens large, mais il ne permet pas d'aller au-delà.

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☑
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☑
RSSI	☐
Constructeurs	☐
Intégrateurs Maintenance	☐
Opérateurs sur site	☐
Auditeurs	☐
Autres : DG	☑

Typologie Réseau	
Embarqué	☑
Site	☑
Étendu	☑

Titre	*La sécurité informatique dans les installations nucléaires*

Date de publication	2013	Éditeur	AIEA	Volume (pages)	91	Accès	gratuit

Synthèse	Standard de recommandations réglementaires, organisationnelles et techniques pour la sécurité des installations nucléaires

Synthèse

Il s'agit d'un manuel de référence dont l'objectif premier est de sensibiliser les protagonistes du domaine nucléaire (des décideurs aux personnels techniques) sur les risques liés à la sécurité informatique et de prodiguer des orientations d'ordre réglementaire ou relevant de la gouvernance (partie I) mais également organisationnelles et techniques (partie II), visant à réduire ces risques.

Cette publication s'articule en 2 parties :

- Une première partie « **Guide de gestion** » rappelle, sous la forme de prescriptions, le rôle et les responsabilités de l'État, de la Direction mais également du personnel (au titre de la responsabilité individuelle) en matière de sécurité nucléaire élargie aux systèmes informatiques (évolution de la réglementation, coordination des acteurs, convergence entre sécurité informatique et sécurité physique). Elle introduit un certain nombre de concepts fondamentaux tels que la sécurité en profondeur, les habilitations du personnel et le besoin d'en connaitre, les systèmes de management, l'évaluation et la gestion de risques, la veille continue sur les nouvelles menaces, la culture de sécurité informatique, ou encore l'erreur humaine (base de vulnérabilités en annexes).
- Une deuxième partie « **Guide d'application** » fournit un set de recommandations permettant de mettre en œuvre la sécurité informatique dans les installations nucléaires dont les principaux éléments sont les suivants : mettre en place un plan de sécurité informatique (prolongement opérationnel de la PSSI), intégrer la sécurité informatique avec les autres domaines de la sécurité nucléaire (Physique, Personnels, Informations), classifier les systèmes informatiques qui composent une installation et appliquer des mesures de sécurisation adaptées aux enjeux de sécurité des SI identifiés.

La deuxième partie offre une vision intéressante des systèmes informatiques qui peuvent composer une installation nucléaire et fournit une approche pratique permettant de les classer selon le degré d'importance (selon la fonction de sûreté nucléaire assurée). Il peut être utilisé dans l'étude des risques et pour déterminer le niveau de sécurité exigé pour chacun de ces SI. Pour chacun de ces niveaux, qui sont au nombre de 5, il est proposé un set de mesures de sécurité à mettre en œuvre. Ces mesures sont composées de mesures génériques qui s'appliquent à l'ensemble des SI et de mesures spécifiques par niveau de sécurité (non cumulatif et augmentation du niveau de robustesse des mesures de sécurité à chaque niveau).

D'autre part, la publication aborde les concepts fondamentaux pour mener une analyse des risques et donne des éléments concrets pouvant être utilisés pour la réaliser : exemples de source de menace, exemples de conséquence d'une atteinte à la sécurité des SI d'une installation, des scénarii de menace (Annexe), une utilisation d'une méthodologie d'évaluation des risques (EBIOS), exemples d'erreur humaines à considérer, etc.

Enfin, le chapitre 7 donne des éléments de compréhension sur les installations nucléaires et sur les spécificités qui s'appliquent à celles-ci ;

Pertinence	Avis
★★★★	Même si sa structure gagnerait à être améliorée et qu'une section aurait pu inclure des schémas de principes d'architectures sécurisées types, ce document énonce parfaitement les enjeux et les mesures essentielles en matière de sécurité informatique applicables au nucléaire. La publication fournit notamment des éléments d'entrée intéressants pouvant être réutilisés dans une analyse de risques (scenarii d'attaques, type de sources

	de menace, exemple d'utilisation d'EBIOS, etc.). Elle vise surtout les RSSI et constitue un bon élément d'entrée pour créer une PSSI.

Secteur	
Énergie	☐
Nucléaire	☑
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☑
RSSI	☑
Constructeurs	☑
Intégrateurs Maintenance	☑
Opérateurs sur site	☑
Auditeurs	☑
Autres	☑

Typologie Réseau	
Embarqué	☑
Site	☑
Étendu	☑

Titre	*La cybersécurité des systèmes industriels - Méthode de classification et mesures principales + Mesures détaillées*

Date de publication	02/2014	Éditeur	ANSSI	Volume (pages)	64+100	Accès	gratuit

Synthèse	Cadre de référence national pour l'évaluation de la classe de cybersécurité des systèmes industriels et des mesures de sécurité applicables

Synthèse

Dans le contexte de la loi de programmation militaire (LPM), l'ANSSI, en collaboration ciblée, a élaboré ce référentiel pour définir les modalités d'application de certaines mesures relative à la cybersécurité des systèmes industriels (cf. chapitre III du texte de loi).

Le référentiel est constitué de deux documents faisant office de guides.

Le « guide de classification » décrit la méthode permettant de conduire une analyse de risques simplifiée (macro), s'inspirant d'EBIOS, sur un périmètre donné d'un système industriel, en vue d'évaluer sa classe de cybersécurité sur une échelle à 3 niveaux, donnant lieu, le cas échéant, à une homologation, en fonction des conséquences pour la Nation en cas d'incident de cybersécurité (sûreté de fonctionnement inclue) :

- classe 1 (traitement des risques jugés inacceptables, sans homologation particulière)
- classe 2 (homologation en mode déclaratif par l'entité responsable)
- classe 3 (homologation par un organisme accrédité, avec autorisation préalable de mise en service)

Des mesures plus ou moins contraignantes, applicables selon la classe attribuée, sont prescrites sur les principaux domaines organisationnels et techniques (rôles et responsabilités, analyse de risques, cartographie, formation et habilitations, veille, audits, continuité d'activité, mode d'urgence, alerte et gestion de crise, interconnexion réseau, télémaintenance, cyber-surveillance)

Le « guide des mesures » apporte quant lui plus de précisions, en commençant par rappeler un certain nombre de spécificités au contexte industriel, en termes de contraintes et de vulnérabilités répandues, puis en énumérant des mesures organisationnelles ainsi que des mesures techniques, systématiquement déclinées proportionnellement à la classe de cybersécurité considérée (certaines recommandations se transformant en directives d'une classe inférieure à l'autre), et ce, en indiquant les correspondances avec les référentiels SSI suivants : guide de classification, guide SCADA et guide d'hygiène informatique de l'ANSSI, et enfin l'ISO/IEC 27002 :2005. Enfin, sont fournis en annexe des éléments d'informations visant à établir la cartographie des systèmes industriels ou encore à assurer une gestion auditable des journaux d'évènements.

Pertinence	Avis
★★★★★	Ce référentiel, vraisemblablement amené à devenir « la norme » sur le territoire national pour les systèmes industriels, offre l'avantage de proposer une méthode d'évaluation simplifiée (pour être accessible et applicable), de la sensibilité et de l'exposition d'un SII aux risques cyber, avec une base de mesures de réduction de risques associées. En bémol, peut-être trop aligné sur la sureté de fonctionnement (prisme réduit à la disponibilité et l'intégrité. Les impacts financiers, de réputation ou de conformité légale et réglementaire ne sont pas pris en compte).

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☑
RSSI	☑
Constructeurs	☑
Intégrateurs Maintenance	☑
Opérateurs sur site	☑
Auditeurs	☑
Autres	☐

Typologie Réseau	
Embarqué	☐
Site	☑
Étendu	☑

Titre	*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

Synthèse	Guide de recommandations organisationnelles et techniques pour la sécurité des systèmes industriels

Synthèse

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

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).

Pertinence	Avis
★★★★★	Document simple à lire, facile d'accès (nombreux exemples) et pouvant constituer un bon point d'entrée sur le sujet de la sécurité des SII. Même si les recommandations essentielles peuvent paraitre peut-être minimalistes, l'impact n'en est que plus important. L'étude de cas apporte, non sans un certain talent, une réelle valeur ajoutée au guide, en immergeant véritablement le lecteur in situ au sein d'un environnement industriel plus vrai que nature avec des situations criantes de vérité (on perçoit bien le vécu), avec en prime une démarche de progrès.

Secteur	Populations visées	Typologie Réseau

Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

DSI	☑
RSSI	☑
Constructeurs	☑
Intégrateurs Maintenance	☑
Opérateurs sur site	☑
Auditeurs	☑
Autres	☐

Embarqué	☑
Site	☑
Étendu	☑

Titre	*API 1164, Pipeline SCADA Security*

Date de publication	06/2009	Éditeur	API (American Petrol Institute)	Volume (pages)	64	Accès	payant

Synthèse	Ce document apporte un guide de mise en sécurité pour les installations pétrolières et gazières, dédié SCADA (intégrité et sécurité).

Synthèse

Ce guide complète le référentiel précédent de 2004 « Security Guidelines for the Petroleum Industry » par nécessité resté général, qui présentait une simple approche « **Information (cyber) security** » (avec référence explicite au référentiel ISO/IEC2700x, en 6 pages, avec les têtes de chapitre ISO)

Ce document « Pipeline SCADA Security » est à considérer comme une approche « bonnes pratiques » à mettre en place lors de la revue d'un système existant ou pour la mise en place d'un système SCADA :

- Management System,
- Physical Security
- Acces control
- Information distribution
- Network Design and Data Interchange
- Field Communication

À noter, que ce document contient 2 annexes très utiles :

- Une annexe de 15 pages « checklist audit d'un système SCADA versus l'API 1164 »
- Une annexe de 15 pages « exemple de politique de sécurité SCADA »

Pertinence	Avis
★★★★	Pragmatique et pertinent avec des annexes particulièrement utiles.

Secteur	
Énergie	☑
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☑
RSSI	☑
Constructeurs	☐
Intégrateurs Maintenance	☑
Opérateurs sur site	☐
Auditeurs	☑
Autres	☐

Typologie Réseau	
Embarqué	☑
Site	☑
Étendu	☑

Titre	*Securing Control and Communications Systems in Transit Environments Part 1 : Elements, Organization and Risk Assessment / Management*

Date de publication	2010	Éditeur	APTA	Volume (pages)	29	Accès	gratuit

Synthèse	Description de l'architecture globale d'un système de transport public et recommandations sur la définition et la mise en œuvre d'un programme de sécurité adapté.

Synthèse

Ce guide de bonnes pratiques, premier volet du travail de l'APTA (American Public Transportation Association) sur la *cybersécurité des systèmes de pilotage et de communication* d'un mode de transport public – ferré ou routier, présente les grandes étapes d'un programme de sécurité.

La première partie recense les grandes familles d'équipements informatiques d'un système de transport (qui vont du pilotage du mouvement d'un train jusqu'à la ventilation d'urgence en passant par la billettique et le contrôle des voyageurs) en soulignant, d'une part, la cohabitation entre systèmes « historiques » non informatisés – qui ont des exigences de sécurité physique – et systèmes informatisés, d'autre part, l'importance des moyens de communication, notamment radio.

Des architectures types sur l'interconnexion de ces divers équipements sont également présentées.

La seconde partie définit les étapes d'un programme de sécurité, découpé en 4 phases :

- Prise de conscience des enjeux par la Direction et constitution d'une équipe dédiée.
- Évaluation des risques et financement d'un plan de sécurité.
- Développement du plan de sécurité, identification des mesures afférentes.
- Mise en œuvre des mesures de sécurité et du plan de maintenance associé.

La troisième partie détaille les étapes du processus d'évaluation des risques, de manière classique : décision de la Direction, choix et formation de l'équipe de gestion des risques, identification des biens critiques, des menaces, des vulnérabilités, puis évaluation et hiérarchisation des risques, enfin, détermination des contre-mesures applicables en prenant en compte les coûts.

Cette section fait de multiples références au catalogue des exigences du DHS (2008) et aux publications du NIST (SP 800-30 et -82), ainsi qu'au NERC (Security Guidelines for the Electricity Sector : Vulnerability and Risk Assessment).

La dernière partie introduit le second volet (cf. autre fiche).

L'Annexe A donne des exemples de cyberattaques sur un système industriel dans les transports et le nucléaire.

L'Annexe B reprend certains tableaux du NIST SP 800-82 mettant en exergue les différences entre systèmes ICT et ICS.

Pertinence	Avis
★★★	C'est un document pragmatique dont le premier intérêt est de présenter de manière synthétique et complète les équipements informatiques d'un système de transport en commun. Le volet programme de sécurité reste très classique.

Secteur	Populations visées	Typologie Réseau

Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

DSI	☑
RSSI	☑
Constructeurs	☐
Intégrateurs Maintenance	☐
Opérateurs sur site	☐
Auditeurs	☐
Autres	☑

Embarqué	☐
Site	☐
Étendu	☑

Titre	*Securing Control and Communications Systems in Transit Environments Part II : Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones*

Date de publication	2013	Éditeur	APTA	Volume (pages)	78	Accès	gratuit

Synthèse	Principes et règles pour bâtir une architecture de sécurité, basée sur la défense en profondeur, pour un système de transport ferroviaire.

Synthèse

Cette seconde partie, consacrée aux systèmes ferroviaires, est divisée en 5 parties plus une introduction qui décrit le contexte.

La première partie, relativement théorique, expose l'enjeu de la cybersécurité pour un système ferroviaire en mettant l'accent sur les zones critiques pour la sécurité ferroviaire (i.e. safety). Les difficultés et contraintes spécifiques au domaine (ex. durée du cycle de vie) sont rappelées.

La seconde partie définit l'approche de cybersécurité retenue en commençant par détailler et analyser les principes de la défense en profondeur, en adaptant l'architecture type du DHS pour une usine. Ensuite un modèle général de défense en profondeur (DeP) est élaboré, accompagné d'un exemple type (matériel roulant, voies et d'équipement fixes de signalisation, centre d'opérations).

Pour appliquer le modèle DeP le système est subdivisé en 5 zones, deux zones standard (Externe, Entreprise) et trois zones de sécurité (*Operationnally Critical, Fire Live-Safety, Safety Critical*), la dernière étant la plus critique.

Chacune des zones de sécurité est analysée en détail, ses constituants et ses interfaces avec les autres zones sont énumérés.

La troisième partie définit les mesures de sécurité pour la zone *Safety Critical*. Ces mesures, tirées du NIST SP 800-53, sont présentées selon un format normalisé :

- titre, description
- références
- argumentaire sur son utilité
- mesure de son efficacité
- exemples d'application

La quatrième partie illustre l'application de ces contrôles sur une architecture type.

La dernière partie introduit le 3^{e} volet de ces publications :

- protection de la zone Operationnally Critical
- sécurisation du pilotage et des communications avec le train
- application d'un modèle d'attaque afin de déterminer les seuils de risque.

Cette 3^{e} partie n'est pas encore publiée.

L'annexe A propose des fiches formatées pour identifier et classer les équipements des installations.

L'annexe B donne des recommandations sur deux sujets d'importance mais en dehors du périmètre de ce document : la sécurité des systèmes historiques, la mise en œuvre du confinement.

Pertinence	Avis
★★★	C'est un document intéressant qui montre bien comment décliner la défense en profondeur sur des systèmes réels. Bien qu'il soit focalisé sur le transport ferroviaire, la démarche proposée est potentiellement applicable à d'autres environnements.

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☑
RSSI	☑
Constructeurs	☑
Intégrateurs Maintenance	☑
Opérateurs sur site	☑
Auditeurs	☑
Autres	☑

Typologie Réseau	
Embarqué	☐
Site	☐
Étendu	☑

Titre	*Guide Pratique – Règles pour les dispositifs connectés d'un Système d'Information de Santé*

Date de publication	Novembre 2013 - V1.0	Éditeur	Agence des Systèmes d'information partagés de santé (asipsanté)	Volume (pages)	20	Auteur de la fiche	PBO/ ESA

Synthèse	Faisant partie d'un ensemble de guides concernant la PGSSI (Politique Générale des Systèmes d'Information de Santé), ce document édicte les règles de sécurité s'appliquant aux dispositifs médicaux connectés aux Systèmes d'Information de Santé (SIS).

Synthèse

Ce guide pratique décrit les règles de sécurité s'appliquant aux dispositifs médicaux connectés aux Systèmes d'Information de Santé (SIS) directement ou à distance (par exemple, via Internet). La notion de dispositif médical est défini dans les articles L 5211-1 et R 5211-1 du code la santé publique et comprend par exemple, les moniteurs de surveillance (respiratoire, cardiaque, multiparamétriques, …), les accélérateurs de radiothérapie… Sont exclus les dispositifs implantables dans des patients.

Ce guide s'insère dans la partie "guides pratiques spécifiques" du corpus documentaire de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S). Il s'adresse en particulier aux fabricants, aux fournisseurs, aux intégrateurs ou aux acteurs du processus d'achat (RSSI, ingénieurs biomédicaux…). Les fabricants sont invités à fournir une déclaration de conformité de leurs produits à ce document, pour aider au processus de sélection lors de l'achat.

L'intégration des dispositifs médicaux connectés dans un SIS engendrent des menaces spécifiques (modification du logiciel par exemple) auxquelles il faudra répondre par des mesures adaptées, et ce d'autant plus que l'exploitation malveillante ou non de vulnérabilités sur ces systèmes peut induire un risque humain fort (décès de patients). Le document traite uniquement d'exigences techniques, fait explicitement le parallèle avec les vulnérabilités des systèmes industriels (un dispositif médical connecté s'apparente pour la partie sécurité de l'information à un système industriel.), et recommande le guide « Maîtriser la SSI des systèmes industriels » de l'ANSSI pour la prise en compte de la sécurité.

Il se base sur un précédent travail réalisé par des RSSI et ingénieurs hospitaliers concernant des systèmes biomédicaux, pour élargir les exigences à tous dispositifs de santé connectés et tout établissement de santé.

Les exigences de sécurité, identifiées dans ce guide, sont évaluées selon 2 niveaux dénommés paliers : en palier intermédiaire (palier 1) pour les mesures prioritaires et en palier supérieur (palier 2) dont l'objectif est d'améliorer le niveau de sécurité en complétant les mesures prioritaires. Enfin, ces exigences ont été regroupées en 6 catégories principales:

1. Gestion des configurations: avec détail des versions FW, OS;
2. Sécurité physique: recommandations et protection des composants sensibles;
3. Exploitation et communications: communications : mises à jour sécurisés, protection contre malveillants, exigences sur l'intégrité et la confidentialité de données stockées et échangées, journalisation…;
4. Maîtrise des accès: authentification réseau et utilisateurs, politique de mots de passes, droits;

5. Développement et maintenance des logiciels: durcissement, règles de développement, mises à jour, tests et modes dégradés;

6. Conformité: il est demandé d'effectuer une analyse de risques et d'en fournir les détails.

Pertinence	Avis
★★★	Le principal intérêt de ce document est de montrer la posture SSI de l'Agence des Systèmes d'information partagés de santé (asipsanté) pour les dispositifs médicaux connectés ainsi qu'une identification des menaces spécifiques. En revanche, c'est dommage que les scenarii de risques propres à ces dispositifs n'aient pas été décrits et que la logique de sélection des mesures ne semble pas s'appuyer sur une analyse formelle, ou si elle l'est, cela n'est pas explicité. Enfin, la couverture des exigences techniques est bonne, et le niveau semble un bon compromis entre l'état de sécurité actuel (faible) et la capacité des constructeurs à rapidement adapter leur offre.

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☑
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☐

Populations visées	
DSI	☑
RSSI	☑
Constructeurs	☑
Intégrateurs Maintenance	☑
Opérateurs sur site	☐
Auditeurs	☐
Autres	☐

Typologie Réseau	
Embarqué	☐
Site	☑
Étendu	☑

Titre	*Informationstechnik in Prozessüberwachung und -steuerung*

Date de publication	2008	Éditeur	BSI	Volume (pages)	5	Accès	gratuit

Synthèse	Document en langue allemande de sensibilisation du BSI, organisme officiel du gouvernement allemand, sur les attaques contre les systèmes SCADA.

Synthèse

Le BSI a publié un document en langue allemande décrivant les problèmes de sécurité pouvant se poser avec des systèmes SCADA, en particulier lorsqu'ils sont raccordés ou accessibles via Internet.

Les moyens de protection proposés sont les suivants:

7. Éviter ce type d'accès, ou alors le restreindre et le protéger avec des outils supplémentaires de sécurité.
8. Surveiller ces accès.
9. Réduire les droits d'accès et interdire l'administration à distance sur les éléments les plus critiques des systèmes de contrôle industriel.
10. S'assurer que les contrats de gestion et d'entretien des SCADA sont appropriés, notamment sur la disponibilité des éléments de rechange au long terme.
11. Vérifier la possibilité d'appliquer des correctifs logiciels si nécessaire sur les SCADA.
12. Protéger systématiquement tous les systèmes sensibles (en termes de sureté de fonctionnement) qui contrôlent par exemple, la distribution de l'eau ou la production d'énergie de façon à éviter toute conséquence néfaste sur la population.

Pertinence	Avis
★★★	C'est un document de vulgarisation très succinct mais qui montre l'intérêt du gouvernement allemand pour la protection des infrastructures industrielles. Il est cependant difficile d'accès du fait de sa langue de publication.

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☑
RSSI	☑
Constructeurs	☐
Intégrateurs Maintenance	☐
Opérateurs sur site	☑
Auditeurs	☑
Autres	☑

Typologie Réseau	
Embarqué	☑
Site	☑
Étendu	☑

Titre	*Good Practice Guide "Process Control and SCADA security"*

Date de publication	2008 2011	Éditeur	CPNI	Volume (pages)	215	Accès	gratuit

Synthèse	Framework sur la sécurité des SCADA fourni par le CPNI (Centre for the Protection of National Infrastructure).

Synthèse

Le centre de protection des infrastructures nationales, organisme gouvernemental du Royaume-Uni, a développé un Framework pour assurer la sécurité des PCS (Process Control Systems), terme générique qui recouvre les PCS, DCS (Distributed Control System), SCADA (Supervisory Control and Data Acquisition)... Ce Framework est basé sur des bonnes pratiques issues de deux mondes : le premier concernant la sécurité IT et le deuxième celui du contrôle des processus industriels. Il s'appuie sur une structuration en 1 document introductif et 7 guides:

1. Le document introductif a pour objectif d'exposer le contexte et les enjeux de la sécurité des PCS, de présenter succinctement les 7 guides et les grands principes de ce Framework.

2. Le guide 1. **"Understand the business risk"** donne des conseils sur l'évaluation des risques métier y compris au fil du temps. En aucun cas, il a pour vocation de fournir des techniques ou des méthodologies d'analyse de risques.

3. Le guide 2. **"Implement secure architecture"** offre une vision de très haut niveau de ce que doit être ou contenir une architecture de sécurité destinée à protéger les systèmes de contrôle industriel (PCS).

4. Le guide 3. **"Establish response capabilities"** décrit les points importants à suivre pour gérer des incidents de sécurité (création d'une équipe de réponse à incident, plan de réaction sur incident, processus et procédures…).

5. Le guide 4. **"Improve awareness and skills"** fournit les bonnes pratiques pour améliorer la sensibilisation et la formation en sécurité (contenu d'un programme de sensibilisation par exemple) ainsi que la communication entre 2 communautés techniques différentes, celle de l'IT et celle des systèmes de contrôle industriel.

6. Le guide 5. **"Manage third party risk"** propose des bonnes pratiques pour la gestion des risques liées aux tierces parties (vendeurs, services ou organisation support, logistique) impliquées dans les systèmes de contrôle industriel.

7. Le guide 6. **"Engage projects"** montre brièvement comment intégrer la sécurité lors d'un projet de déploiement de systèmes de contrôle industriel. Il s'agit par exemple d'insérer une annexe de sécurité dans les contrats ou d'intégrer des exigences de sécurité dans les spécifications de la phase design.

8. Le guide 7. **"Establish ongoing governance"** donne des conseils pour définir et établir un cadre de gouvernance de la sécurité (responsabilités, politiques, standards, guides d'implémentation…) dont l'objectif est d'assurer une cohérence de l'ensemble des mesures prises.

D'autres guides plus récents détaillent des mesures techniques et opérationnelles pour assurer la sécurité des différents systèmes. En particulier, la protection des protocoles IP, le déploiement de pare-feu, la gestion des accès distants mais également les bonnes pratiques méthodologiques en matière d'évaluation de la cybersécurité des systèmes industriels (tests d'intrusions, tests de vulnérabilités) sont abordés dans ces guides complémentaires

Pertinence	Avis
	Framework intéressant pour l'approche structurée et couvrant 7 domaines. Il est relativement généraliste et peut s'appliquer à tous les secteurs.

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées (de façon générale car cela dépend des guides)	
DSI	☐
RSSI	☑
Constructeurs	☐
Intégrateurs Maintenance	☑
Opérateurs sur site	☑
Auditeurs	☑
Autres	☑

Typologie Réseau	
Embarqué	☐
Site	☐
Étendu	☐

Titre	*Cyber Security Assessments of Industrial Control Systems* *A Good Practice Guide*

Date de publication	2011	Éditeur	CPNI	Volume (pages)	66	Accès	gratuit

Synthèse	Présentation des différents processus permettant de tester et d'évaluer la cybersécurité d'un système industriel, en fonction de la nature et de la profondeur de l'analyse

Synthèse

Ce guide analyse les différents processus de tests pouvant être menés sur un système industriel.

La première section décrit les principaux types de test et compare les processus d'évaluation d'un ICS avec les tests de pénétration classiques pour les systèmes IT :

- 3 catégories de tests sont explicitées, l'évaluation des vulnérabilités qui recherche les faiblesses du système, les tests de pénétration usuels qui évaluent la résistance du système aux attaques, et les exercices de red team qui éprouvent la capacité de l'organisation à contrer une attaque, y compris avec de l'ingénierie sociale. Ce type de tests, mentionnés initialement, n'est malheureusement pas repris dans la suite du document.

- Les connaissances préalables du testeur, qui vont de l'absence totale (boîte noire) à la divulgation complète (boîte blanche), sont appréciées selon leurs avantages et inconvénients respectifs, au regard des objectifs du test.

- Le choix du périmètre testé est discuté en mettant l'accent sur les spécificités des ICS (e.g. protocoles) et la prise en compte de leurs architectures propres.

- Les impacts potentiels des tests sont étudiés, l'accent est mis sur la collaboration entre les parties prenantes, le propriétaire du système, l'équipe d'évaluation et, le cas échéant, l'équipementier.

La seconde section décrit précisément le processus d'évaluation : 1. planification ; 2. évaluation ; 3. rapport ; 4. remédiation des vulnérabilités ; 5. validation du test. Cette partie, assez classique, insiste sur:

- La sélection et les certifications des évaluateurs.

- Le choix des vecteurs d'attaque et l'exécution des tests de pénétration, découpés en phase (reconnaissance, exploration, identification de vulnérabilités, développement d'exploit).

- Les métriques de vulnérabilité en retenant le modèle CVSS v.2.

Un format type du rapport est présenté en détail. Les résultats sont compilés sous forme de scénarios d'attaque, répartis en 3 niveaux : démontré, probable, pire cas.

La troisième section analyse les « variables » essentielles d'une évaluation, à savoir le budget, les informations en entrée, l'accès au code source, les modalités de test (laboratoire, sur site), les règles d'engagement, enfin, l'implication de l'équipementier.

La quatrième section discute des différents environnements d'évaluation possibles, en différenciant les tests réalisés en laboratoire, les tests exécutés sur des systèmes en production, les tests d'intrusion menés de bout en bout, les tests dédiés aux composants, les revues de documentation technique, de fonctionnalité et de configurations, les entretiens avec le personnel, pour finir par l'évaluation globale du risque sur le système cible.

Cette discussion s'achève par un logigramme permettant de choisir la catégorie de test à effectuer

selon le type de cible (produits ICS, réseau ICS, périmètre du système ICS). La dernière section est une conclusion qui reprend et synthétise le corps du document.

Pertinence	Avis
★★★★	C'est un document très intéressant sur un sujet insuffisamment traité : la méthodologie d'évaluation. On peut seulement regretter qu'il ne soit pas aller encore plus loin dans l'analyse des spécificités des ICS du point de vue de l'évaluation de sécurité.

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☑
RSSI	☑
Constructeurs	☐
Intégrateurs Maintenance	☐
Opérateurs sur site	☐
Auditeurs	☑
Autres	☑

Typologie Réseau	
Embarqué	☐
Site	☐
Étendu	☑

Titre	*Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*

Date de publication	2010	Éditeur	Cyber Security Working Group (CSWG)	Volume (pages)	597	Accès	gratuit

Synthèse	Démarche de développement d'une stratégie de cybersécurité des systèmes Smart Grid (sous forme de guideline)

Synthèse

Processus d'élaboration des exigences de haut niveau : exigences de cybersécurité devant être satisfaites par domaine : contrôle d'accès, audit et traçabilité, politique de sécurité, procédures d'autorisations, etc.

- Le 1er volume donne une approche structurée d'analyse pour déterminer les exigences de sécurité ainsi que le processus d'évaluation des risques. Une architecture type de haut niveau est identifiée et décrite sous forme de couches et de liens logiques entre chacune d'elle : catégories d'interfaces. Le document se termine sur des questions pratiques concernant la gestion des clés et chiffrement.

- Le 2eme volume se focalise sur les aspects de confidentialité vis-à-vis des informations utilisées dans les Smart Grid, ainsi que sur les risques d'usurpation de ces informations vis-à-vis des personnes et les aspects réglementaires non encore traités. Des exemples de cas d'utilisation sont définis en annexes.

- Le 3eme volume est orienté sur des aspects pratiques et des ressources concernant l'élaboration des exigences de sécurité de haut niveau : définition des classes de vulnérabilité, l'analyse de la sécurité Bottom – Up, thèmes de recherche et développement sur la Cybersécurité, principaux Use Case des exigences de haut niveau vis-à-vis des différents systèmes électriques (Power system).

Pertinence	Avis
★★★★	Très centré sur les systèmes Smart Grid, ces guidelines peuvent néanmoins être utilisés comme guide support pour étudier une stratégie de cybersécurité sur des systèmes équivalents.

Secteur	
Énergie	☑
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☑
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☐

Populations visées	
DSI	☐
RSSI	☑
Constructeurs	☑
Intégrateurs Maintenance	☑
Opérateurs sur site	☐
Auditeurs	☐
Autres	☑

Typologie Réseau	
Embarqué	☑
Site	☑
Étendu	☐

Titre	*21 étapes pour améliorer la cybersécurité des réseaux des SCADA*

Date de publication	2002	Éditeur	DoE (Department of Energy)	Volume (pages)	10	Accès	gratuit

Synthèse	Guide US de recommandations techniques et organisationnelles pour la sécurité des systèmes d'information industriels (SII)

Synthèse

Il s'agit d'un guide qui propose des actions contextualisées aux SCADA, relatives à la sécurité des réseaux industriels. Elles se présentent en 21 recommandations, dont la moitié sont techniques (cartographier les réseaux, identifier les SPOF, installer des firewalls et IDS, désactiver les connexions et services inutiles, sécuriser la télémaintenance, …) et l'autre moitié organisationnelles (implication de la Direction et sensibilisation du personnel, définition des rôles et des responsabilités, management des risques, « Red Team » et plan de réaction en cas d'incidents, DRP, auto-évaluation et audits, …),

Chacune des 21 recommandations est rédigée de manière très synthétique (un paragraphe d'une dizaine de lignes), ce qui donne un document facile à lire et qui contient en substance l'essentiel pour qui veut sécuriser ses systèmes industriels.

Ce document, élaboré suite aux attentats du 11 Septembre 2001, reste encore pertinent malgré l'absence de recommandations relatives à la question de la lutte anti-malware et du contrôle des médias amovibles, sujet qui n'aurait sans doute pas pu être évité si le document avait été postérieur aux affaires « stuxnet ou Duqu ». Les concepts de défense en profondeur, DMZ et du besoin d'en connaitre (notamment face à l'ingénierie sociale/divulgation) sont par contre bien présents.

Quoique rédigé par le département de l'énergie US, ce document a une portée beaucoup plus large et peut s'appliquer à tous les secteurs industriels. On le trouve cité à de nombreuses reprises dans la littérature. Il y a même un outil de l'I3P (Institute for Information Infrastructure Protection) créé en 2007 qui permet de mesurer son positionnement par rapport à ces recommandations.

Pertinence	Avis
★★★	Document synthétique présentant les principales lignes directrices pour la sécurisation d'un réseau industriel mais qui ignore certaines menaces actuelles.

Secteur	
Énergie	☑
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☑
RSSI	☑
Constructeurs	☐
Intégrateurs Maintenance	☐
Opérateurs sur site	☐
Auditeurs	☐
Autres	☐

Typologie Réseau	
Embarqué	☐
Site	☑
Étendu	☑

Titre	*CSSP Recommended practices : Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*

Date de publication	10/2009	Éditeur	DHS	Volume (pages)	44	Accès	gratuit

Synthèse	

Synthèse

Il s'agit d'un document très didactique qui propose des mesures d'amélioration de la sécurité des systèmes industriels. Le début du document décrit une architecture type non sécurisée, expose les différents types de menaces qui peuvent s'en suivre (man in the middle, injection SQL,…) et propose ensuite différentes mesures graduées de sécurisation basées sur le principe de la défense en profondeur, à savoir :

- Découpage en zones de confiance
- Coupe-feux
- DMZ
- Systèmes de détection d'intrusion
- Politiques et procédures (patch management, formations, réponse aux incidents…)

Ce document est illustré d'assez nombreux schémas d'architecture détaillant les différentes étapes listées ci-dessus et il est complété d'une assez volumineuse bibliographie.

La généricité des recommandations proposées s'adapte à la plupart des domaines de l'industrie du moment qu'il s'agit de commander un processus avec un SCADA.

Pertinence	Avis
★★★★★	Document très intéressant et didactique sur la sécurisation des réseaux industriels

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☑
RSSI	☑
Constructeurs	☐
Intégrateurs Maintenance	☑
Opérateurs sur site	☐
Auditeurs	☐
Autres	☐

Typologie Réseau	
Embarqué	☐
Site	☑
Étendu	☑

Titre	*Can we learn from SCADA security incidents - White Paper*

Date de publication	2013	Éditeur	ENISA	Volume (pages)	10	Accès	gratuit

Synthèse	

Synthèse

Ce document cible les opérationnels sur le terrain et vise à améliorer la gestion des incidents touchant les SII. Il se focalise en particulier sur l'analyse post-mortem.

Le document fait tout d'abord un parallèle entre une démarche forensic « classique » et celle pouvant être appliquées sur un SII en donnant quelques exemples de particularités de systèmes industriels.

Ensuite, une organisation est proposée. Elle met en parallèle les rôles « classiques » avec des rôles spécifiques au SII (par exemple un « Control Systems Incident Manager » ou un « Control Systems Engineering Support »). Une répartition des tâches est ensuite proposée.

Le document précise ensuite les challenges relatifs à la gestion des incidents dans ces environnements souvent propriétaires et peu dotés en mécanismes assurant la traçabilité (difficultés d'analyse).

Le dernier chapitre correspond à des recommandations d'assez haut niveau pour améliorer la situation.

Pertinence	Avis
★	Ce document présente de manière trop succincte les enjeux de la gestion des incidents dans les environnements SII. Il peut être utile pour se donner un aperçu général de la problématique et entamer des premières réflexions.

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☐
RSSI	☑
Constructeurs	☐
Intégrateurs Maintenance	☐
Opérateurs sur site	☑
Auditeurs	☑
Autres : forensic	☑

Typologie Réseau	
Embarqué	☑
Site	☑
Étendu	☑

Titre	*Window of exposure ... a real problem for SCADA systems? - Recommendations for Europe on SCADA patching*

Date de publication	12/2013	Éditeur	ENISA	Volume (pages)	19	Accès	gratuit

Synthèse	Guide UE de recommandations organisationnelles et méthodologiques pour la gestion des vulnérabilités et des correctifs SCADA

Synthèse

Il s'agit d'un guide structuré en 3 parties, autour de la problématique de la « fenêtre d'exposition », délai entre la découverte/publication d'une vulnérabilité et la mise à disposition (généralement par l'éditeur) d'un correctif (patch ou montée de version), mais surtout de son déploiement effectif sur les systèmes SCADA ou DCS vulnérables au sein des installations industrielles.

Après une brève introduction sur les spécificités des systèmes de contrôle industriels (ICS), en particulier la faible tolérance aux pannes ou interruptions de service suite ou pour l'application d'un patch, le document débute par une présentation de l'état de l'art en matière de *patch management* des systèmes SCADA (PLC et autres automates exclus du périmètre d'étude), en se référant à un certain nombre de standards existants tels que NERC CIP, NIST SP 800-40 et SP 800-82, IEC/TR 62443 (ISA-99), guides du BDEW, ISO/IEC 27002 et ISO/IEC TR 27019, et en particulier du guide émis par l'ICS-CERT (DHS/US-CERT) « *Recommended practice for patch management of control Systems* ».

Le chapitre suivant énonce ensuite les enjeux liés au patching des SCADA, en termes organisationnels (ex : limites de responsabilités via les contrats de maintenance, système d'évaluation contextualisé de la criticité des vulnérabilités, modes de publication des vulnérabilités), techniques (ex : récupération des patchs via sandboxing, systèmes obsolètes non patchables) et législatif (ex : règlementation différentiée selon les pays, patching des composants open source, garantie constructeur)

Enfin, le guide propose un ensemble de bonnes pratiques et de recommandations d'ordre organisationnel et technique (plus méthodologiques en fait), répartis entre mesures palliatives (à titre compensatoire, principalement basé sur le principe de défense en profondeur) et mesures correctives (dans le cadre d'un programme de *patch/release management* : *patching policy*, *asset management*, qualification/re-certification, système centralisé et confiné, déploiement phasé en commençant par les systèmes pilotes dits « *early Adopter* »).

Pertinence	Avis
★★★★★	Ce Livre blanc adresse plutôt bien (même si les 3 parties sont un peu redondantes) les principales problématiques liées au patch management appliqué aux SCADA et fournit une démarche structurante et compilée (par rapport aux standards établis) pour traiter la question avec discernement.

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☑
RSSI	☑
Constructeurs	☑
Intégrateurs Maintenance	☑
Opérateurs sur site	☑
Auditeurs	☑
Autres	☐

Typologie Réseau	
Embarqué	☐
Site	☑
Étendu	☑

Titre	*Appropriate security measures for Smart Grids - Recommendations for Europe and Member States*

Date de publication	2012	Éditeur	ENISA	Volume (pages)	84	Accès	gratuit

Synthèse	Guide UE de recommandations organisationnelles et techniques pour la sécurité des Smart Grids

Synthèse

Il s'agit d'un guide proposant un catalogue de 39 mesures de sécurité organisationnelles et techniques contextualisées, réparties sur 10 domaines associés à des objectifs de sécurité, selon une structure similaire à l'ISO/IEC 27002 (le « *should* » est d'ailleurs systématiquement employé). Les 10 domaines sont les suivants :

1. Gouvernance Sécurité & Risk Management
2. Gestion des tierces parties
3. Processus sécurisé de gestion du cycle de vie des composants/systèmes Smart Grids et des procédures opérationnelles
4. Sensibilisation/formation du personnel à la sécurité
5. Réaction aux incidents et partage d'information
6. Audit & Traçabilité
7. Continuité d'activité
8. Sécurité physique
9. Sécurité des systèmes d'information
10. Sécurité réseau

Chacune des 39 mesures de sécurité est présentée selon une première approche synthétique, sous le forme d'une énumération (ID, intitulé, description sur 3 lignes) assortie d'exemples explicitement tirés de référentiels réputés (NERC CIP, NISTIR 7628, IEC 62351, IEC 62443, ISO/IEC 27002, ISO/IEC 27011, ISO/IEC TR 27019, ISO/IEC 27036-2, BDEW).

Le chapitre suivant présente de façon plus détaillée une nouvelle énumération où chacune de ces mêmes mesures se voie associer systématiquement une déclinaison opérationnelle sur 3 niveaux d'implémentation (« *sophistication levels* »), à appliquer avec discernement au regard de la maturité de l'organisation en termes de gestion des processus (approche PDCA), mais également et surtout en fonction de la sensibilité du contexte. Une colonne proposant des éléments de preuve relativement précis est également présente (utile aux auditeurs !).

Enfin, une grille de correspondance est donnée entre les mesures de ce guide, celles de l'ISO/IEC 27002 (complété par l'ISO/IEC TR 27019 le cas échéant) et celle du NISTIR-7628 respectivement.

À noter que le guide intègre également au préalable une section « *Lessons identified* » listant une vingtaine de constats (sorte de REX) assez révélateurs sur les écarts couramment relevés et le degré de sécurisation relativement perfectible des Smart Grids, aisément transposables aux systèmes industriels en général.

Pertinence	Avis
★★★★★	De par la clarté de sa structure et de son ouverture aux standards réputés pour consolider des mesures pertinentes et graduelles sur 3 niveaux en fonction de degré de sécurité à atteindre, ce guide pourrait prétendre à devenir une référence, du moins dans l'UE, pour ce qui relève des « points de contrôle » à satisfaire ou à vérifier concernant la sécurité des Smart Grids. Seul bémol, l'absence de chapitre préconisant des architectures techniques sécurisées fait défaut. En effet, cela aurait permis de combler un certain vide au regard des documents traitant des Smart Grids de façon générale (ex : charte Smart Grid Côte d'Azur - CCI Nice Côte d'Azur - déc.2012).

Secteur		Populations visées		Typologie Réseau	
Énergie	☑	DSI	☑	Embarqué	☑

Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

RSSI	☑
Constructeurs	☑
Intégrateurs Maintenance	☑
Opérateurs sur site	☑
Auditeurs	☑
Autres : traders, législateurs, régulateurs	☑

Site	☑
Étendu	☑

Titre	***Protecting industrial control systems*** *- Recommendations for Europe and member states*

Date de publication	2011	Éditeur	ENISA	Volume (pages)	81	Accès	gratuit

Synthèse	Guide UE de recommandations stratégiques pour la sécurité des systèmes industriels

Synthèse

Il s'agit d'un rapport d'étude, à portée pan-européenne, préconisant 7 recommandations de « haut niveau » destinées principalement aux décideurs (politiques, pouvoirs publics, autorités de régulation, industriels) dans l'optique d'améliorer la sécurité des systèmes de contrôle industriels (ICS) en Europe.

Le document dresse tout d'abord un état des lieux au travers d'une série de 86 constats majeurs (« *key findings* ») réparties en 15 thématiques. Ces constats ont été établis et consolidés à partir d'enquêtes par questionnaire et d'entretiens avec une population composées d'une cinquantaine d'experts dans le domaine des ICS, représentant un panel de parties prenantes relativement large (fabricants industriels, mainteneurs, organismes publics, monde universitaire et R&D, etc.).

Parmi ces constats, sont notamment pointés certaines insuffisances au niveau de la gouvernance en termes d'appétence aux risques liées à la sécurité des ICS, un manque de synergie entre nations européennes pour arriver à publier un standard commun tel que le NERC CIP, un certain vide réglementaire à caractère prescriptif sur ce même domaine (essentiellement restreint aux OIV), la nécessité de mettre en place des CSIRT à l'échelle nationale, le besoin de disposer d'un modèle de plan de sécurité adaptable et qui puisse être contextualisé, la relative incompatibilité des bonnes pratiques en sécurité (ex : hardening, patch management, anti-malware, gestion de l'obsolescence) ainsi que des solutions de sécurité IT traditionnelles (ex : IDS/IPS, FW/DPI, VPN, NAC, Sécurité Wi-Fi) avec les particularités (ex : protocoles ou algorithmes propriétaires, exigences de fiabilité et de performance) des systèmes industriels, le rôle fédérateur des pouvoirs publics (ex : PPP), le besoin de disposer de référentiel de certification de produits de sécurité industriels (ex : CC, FIPS pour les ICS), le manque d'intégration de la sécurité dans le cycle de développement aussi bien dans la conception (analyse de risques, recommandations de sécurité, sécurité embarquée) que dans la validation (audit de conformité, tests d'intrusion).

L'ensemble de ces constats sont alors repris en guise de justification au sein de 7 recommandations délivrées à titre d'orientations stratégiques, incluant une description, un objectif, des étapes de mise en œuvre, des éléments de mesure du succès, les parties prenantes concernées.

Pertinence	Avis
★★★	Si un certain nombre de constatations ne sont pas dénuées de pertinence ni d'intérêt pour les organisations et fabricants industriels, la portée hautement stratégique des recommandations ne trouverons audience que dans le cadre d'un programme d'actions sponsorisé au niveau de l'UE.

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☑
RSSI	☑
Constructeurs	☑
Intégrateurs Maintenance	☑
Opérateurs sur site	☐
Auditeurs	☑
Autres	☐

Typologie Réseau	
Embarqué	☑
Site	☑
Étendu	☑

Titre	*IEC 62443 – Security for industrial Automation and Control Systems*

Date de publication	2013 - 2016	Éditeur	IEC	Volume (pages)	1010	Accès	payant

Synthèse	

Synthèse

L'IEC 62443 correspond à une famille de normes traitant très largement de la problématique de la sécurité des SI industriels sans viser un secteur en particulier.

Les normes sont organisées en quatre familles. La première pose les bases de la terminologie, les concepts et le vocabulaire. La deuxième est destinée aux détenteurs d'actifs, les organisations qui possèdent les SII. La troisième vise les intégrateurs qui mettent en œuvre ces systèmes. La quatrième cible les fabricants de matériel composant le SII.

Les normes sont très nombreuses, avec des niveaux de granularité différents et sont également très verbeuses. Il peut être difficile de se retrouver dans un volume de plus de 1000 pages ou certains sujets se recoupent. Il est important de préciser que la plupart des normes sont encore en cours d'élaboration.

Cependant, les normes sont explicatives et reprennent de nombreux concepts qui permettent d'attaquer le sujet de la sécurité de SII. Les normes de la famille 1 positionnent par exemple les concepts de défense en profondeur ou encore les notions de zones et de conduits. La norme 2-2 se veut comme un ajout à l'ISO/IEC 27002 en y ajoutant les principes spécifiques au SII. Les autres normes proposent un certain nombre de zooms concrets comme la gestion des correctifs. Il est dommage que la norme 3-2 sur l'analyse de risque ne mentionne pas les normes ISO relatives (31000/27005).

Le public visé est principalement des experts en SI industriels qui attaquerait le sujet de la sécurité mais un RSSI peut également être intéressé par certaines de ces normes, en particulier celles de la famille 1 sur les détails entre la sécurité et la sureté mais également la famille 2 avec la liaison avec l'ISO/IEC 27002.

Pertinence	Avis
★★★★	La famille IEC62443 comprend de très nombreux éléments sur de multiples volets qui peuvent parfois se recouper. Cette complétude en fait un incontournable. Elle nécessite cependant un travail important d'appropriation et de sélection parmi les thèmes redondants pour être utilisé opérationnellement.

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☑
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☐
RSSI	☑
Constructeurs	☑
Intégrateurs Maintenance	☑
Opérateurs sur site	☑
Auditeurs	☑
Autres	☐

Typologie Réseau	
Embarqué	☐
Site	☑
Étendu	☑

Titre	*Security for industrial automation and control systems* *IEC 62443 – Part 1-1 : Terminology, Concepts and Models*

Date de publication	2012	Éditeur	IEC	Volume (pages)	87	Accès	payant

Synthèse	Présentation de la terminologie, des concepts et modèles essentiels pour la cybersécurité des IACS

Synthèse

La première partie qui est uniquement informative fournit un glossaire, analyse le contexte en soulignant les besoins de sécurité spécifiques des IACS (intégrité et disponibilité), puis présente les concepts généraux de la SSI avec un focus sur les politiques et procédures de sécurité.

La seconde partie qui est normative introduit puis développe les concepts fondamentaux :

- Les dimensions essentielles de la sécurité (Personnels, Procédures, Technologies).
- Le programme de sécurité (i.e. la combinaison de toutes les mesures concourant à la sécurité) et sa maturité, qui s'appuie sur un système de management de la cybersécurité et couvre les 5 phases du cycle de vie du système.
- Les 3 modèles de base : modèle de référence du système industriel (cf. ISA 95), l'architecture physique et la segmentation du système.
- Le périmètre du système analysé, défini à partir des modèles précédents.
- Les exigences fondamentales techniques de sécurité, divisées en 7 catégories : **identification, authentification et contrôle d'accès** ; **contrôle d'usage** ; **intégrité du système** ; **confidentialité des données** ; **restriction des flots de données** ; **réponse opportune aux événements** ; **disponibilité des ressources**. Elles sont exprimées selon les 4 niveaux de sécurité (cf. ci-dessous).
- Les principes de segmentation du système (cf. modèle).
- Les niveaux d'assurance de la sécurité, inspirés des SIL, répartis en 3 classes : le niveau cible, le niveau réalisé, le niveau de capacité. Ces 3 scalaires combinés définissent le vecteur de niveau de sécurité. Ils sont définis pour une zone ou un conduit et divisés en 4 niveaux :
  - Niveau 1 : protection contre les violations accidentelles ou fortuites.
  - Niveau 2 : protection contre les violations intentionnelles basées sur des ressources faibles, des compétences génériques et une motivation limitée.
  - Niveau 3 : protection contre les violations intentionnelles basées sur des ressources significatives, des compétences spécifiques (vis-à-vis du système) et une motivation modérée.
  - Niveau 4 : protection contre les violations intentionnelles basées des ressources étendues, des compétences spécifiques et une motivation élevée.
- Le cycle de vie de sécurité qui définit les activités à mener pour développer une zone (ou un conduit) de manière à respecter son niveau de sécurité cible.

Ce modèle est articulé autour des dimensions essentielles de la sécurité que sont le personnel, les processus et la technologie.

Pertinence	Avis
★★★★	Document important, très riche, qui introduit le standard IEC

Titre	*Security for industrial automation and control systems* *IEC 62443 – Part 1-2 : Master Glossary*

Date de publication	2012	Éditeur	IEC	Volume (pages)	37	Accès	payant

Synthèse	Glossaire général

Synthèse

Ce document présente un glossaire général pour la série ISA 62443. Il reprend et étend les glossaires des documents…

On peut noter que ce glossaire n'est pas complet puisqu'il ne comprend pas certains termes importants utilisés par ailleurs comme le concept de résilience (cf. Partie 1-3). De plus tous les termes ne sont pas définis (ex. capability security level)

D'autre part il introduit plusieurs notions importantes qui ne sont pas développées dans la version actuelle du standard comme les arbres d'attaque.

Pertinence	Avis
★★★	Glossaire indispensable mais non complet. Cependant, une version en ligne a vocation à être la référence.

Titre	*Security for industrial automation and control systems IEC 62443 – Part 1-3 :*

Date de publication	2012	Éditeur	IEC	Volume (pages)	73	Accès	payant

Synthèse	Description et analyse d'un ensemble de métriques de cybersécurité

Synthèse

Ce document présente un cadre général pour le développement et la mise en œuvre de métriques de cybersécurité applicables aux IACS.

La conformité d'une métrique nécessite la définition préalable d'une cible.

Ces métriques devraient satisfaire une série d'exigences générales définies dans les travaux de Hermann, Jaquith et du NIST (SP800-55) : les métriques sont mesurables à l'aune de critères objectifs, contextualisés, quantitatifs, et, autant que possible, automatisables.

Ces métriques couvrent les domaines suivants : la confiance (i.e. gestion de risques et surveillance des fonctions de sécurité), le chiffrement, la protection de la vie privée, les 7 exigences fondamentales de sécurité (cf. Partie 1-1), la fiabilité et la disponibilité de l'IACS, la planification et l'organisation du programme de sécurité, pour finir, l'acquisition et l'implémentation des mesures constitutives de ce programme.

Un point particulier est l'adoption du modèle formel de Clark-Wilson (conçu en 1987) pour aligner les métriques avec les exigences du système et les critères d'audit tout en étant adapté au concept de maturité avec ses 4 niveaux : réactif, conforme, proactif, optimisé.

Le document définit un processus précis pour choisir les métriques composé de deux volets : d'abord la sélection d'un jeu convenable de métriques, ensuite leur application précise au système considéré.

Pertinence	Avis
	Intéressant, (trop) riche et travail en cours : il manque une consolidation théorique

Titre	*Security for industrial automation and control systems* *IEC 62443 – Part 2-1 : Industrial automation and control system security management system*

Date de publication	2012	Éditeur	IEC	Volume (pages)	285	Accès	payant

Synthèse	Description du système de gestion de la cybersécurité d'un IACS

Synthèse

Ce document présente et détaille les processus d'implémentation, de gestion et d'exploitation d'un système de management de la cybersécurité appliqué à un IACS.

C'est donc une approche classique, largement fondée sur les ISO/IEC 27001 et 27002.

Les mesures gérées par ce système sont regroupées en 11 familles :

- politique de sécurité
- organisation de la cybersécurité
- gestion des actifs
- sécurité des ressources humaines
- sécurité physique et environnementale
- gestion des opérations et des communications
- contrôle d'accès
- acquisition, développement et maintenance des systèmes d'information
- gestion des incidents de cybersécurité
- gestion de la continuité des activités
- conformité

Dans une version ultérieure du document, chacune de ces mesures sera complétée et déclinée selon les différents niveaux de sécurité.

L'annexe B fournit une liste supplémentaire de recommandations portant sur la définition du périmètre, la formation et la culture de sécurité, la sécurité du personnel, l'identification, la classification et l'évaluation des risques. Ce dernier point est relativement détaillé.

Pertinence	Avis
	Le processus est très proche de l'ISO/IEC 27001, mais le travail n'est pas finalisé.

Titre	*Security for industrial automation and control systems* IEC 62443 – Part 2-2 : Implementation Guidance for an IACS Security Program

Date de publication	2013	Éditeur	IEC	Volume (pages)	69	Accès	payant

Synthèse	Mise en œuvre du programme de sécurité applicable à un IACS

Synthèse

Ce document est le pendant de l'ISO/IEC 27002 pour les IACS.

Le vocabulaire n'a pas encore été aligné sur les autres documents (*information security* au lieu *cyber security*)

Le document reprend les 11 catégories de mesure : politique de sécurité, organisation de la sécurité, gestion des actifs, sécurité des ressources humaines, sécurité physique et environnementale, gestion des opérations et des communications, contrôle d'accès, acquisition, développement et maintenance des systèmes d'information, gestion des incidents, gestion de la continuité des activités, conformité

Les 3 premières ne sont pas encore traitées. Outre la description classique des mesures quelques recommandations spécifiques aux IACS sont apportées.

Certaines mesures ont des exigences supplémentaires sur le format du NIST SP 800-53. Ces exigences (**ce n'est pas explicitement indiqué dans le document**) devraient logiquement permettre de distinguer entre les différents niveaux de sécurité.

L'annexe B dédiée au tableau de correspondance entre les contrôles de la partie 2-2 et les 7 exigences fondamentales présentées en 1-1 n'est pas encore développée.

Pertinence	Avis
★★★★	Document en cours, ne s'appuie pas suffisamment sur le détail défini dans d'autres parties du standard (cd. modèles de base de la partie 1-1). Cependant, il contient des éléments assez exhaustifs dont il est possible de s'inspirer.

Titre	*Security for industrial automation and control systems* *IEC 62443 – Part 2-3 : Patch management in the IACS environment*

Date de publication	2013	Éditeur	IEC	Volume (pages)	83	Accès	payant

Synthèse	Description du processus de gestion des correctifs pour un IACS

Synthèse

La Partie 2-3 traite du problème particulier de la gestion des correctifs pour les IACS. Après avoir rappelé le contexte, notamment l'utilisation grandissante des COTS qui représentent de nouvelles opportunités de cyber-attaques contre les IACS, le document analyse :

- les difficultés inhérentes à la gestion des correctifs en milieu industriel (conséquences éventuelles sur la fiabilité, effort de préparation en amont, sauvegardes au cas où etc.) qui doivent être appréhendées par une approche de gestion des risques;
- les conséquences d'une médiocre gestion des correctifs ;
- le cas des composants obsolètes, qui nécessitent des mesures palliatives

Sont ensuite étudiées les exigences respectives du propriétaire du système (inventaire, tests, planification du déploiement…), du fournisseur du produit (politique spécifique pour le produit, qualification préliminaire…) ; puis les exigences de communication entre ces deux parties : le document propose une structure (VPC) pour échanger des informations sur les correctifs.

L'annexe A propose le VPC au format XML.

L'annexe B détaille les recommandations concernant le propriétaire du système. Elles portent principalement sur :

- le recueil d'information (inventaire y compris par des outils, contact avec le fournisseur, support du produit, évaluation de l'environnement du produit, classification et catégorisation des composants matériels/logiciels)
- la planification et l'implémentation (étude économique, attribution des rôles avec un RACI, l'environnement de test, le déploiement (*mentionné mais non encore traité*), les sauvegardes
- les procédures et processus fondés sur le cycle de vie de surveillance, évaluation des patches, critères déploiement, test et qualification des patches, test du retour arrière, mesures palliatives de réduction des risques en cas de non installation, déploiement
- règles générales sur la gestion d'un programme complet de gestion des patches

L'annexe C détaille les recommandations concernant les fournisseurs. Elles portent sur l'organisation, la découverte de vulnérabilités, la mise au point des correctifs, leur distribution et la communication avec leurs parties prenantes.

Pertinence	Avis
★★★	Le processus défini en annexe B est plutôt complet mais il n'est pas décliné sur les constituants précis d'un IACS : on devrait envisager des politiques de gestion de correctifs adaptés aux différents niveaux de l'IACS. L'intérêt commercial du format-type est discutable.

Titre	*Security for industrial automation and control systems* *IEC 62443 – Part 3-1 : Security Technologies for Industrial Automation and Control Systems*

Date de publication	2012	Éditeur	IEC	Volume (pages)		Accès	payant

Synthèse	Présentation des principales technologies de cybersécurité pour les IACS

Synthèse

Ce document généraliste présente une série de mesures techniques de sécurité visant à identifier et traiter les vulnérabilités afin de réduire les risques d'intrusion et d'atteinte aux besoins de sécurité.

Les mesures de sécurité sont subdivisées en 8 domaines de type cyber, auxquels s'ajoutent la sécurité physique.

Les domaines cyber sont : l'authentification et l'autorisation ; contrôle d'accès, filtrage et blocage ; chiffrement ; validation des données ; audit ; Mesures ; outils de détection et de surveillance ; systèmes d'exploitation.

Chaque type de mesure est décliné selon le modèle suivant :

- description générale du type de technologie, éventuellement subdivisée en différentes technologies, chaque type étant ensuite analysé selon :
- vulnérabilités contrées
- contraintes de déploiement
- faiblesses connues
- diffusion dans le domaine industriel
- prospective (évolutions)
- recommandations de mise en œuvre compte tenu de ce qui précède
- bibliographie spécifique

Les mesures sont ainsi catégorisées et accompagnées de conseils quant à leur déploiement, leurs faiblesses connues, leur évaluation dans le contexte particulier des IACS, leurs évolutions futures.

Pertinence	Avis
	D'une part ces mesures techniques ne sont pas déclinées sur les différents composants d'un IACS, d'autre part elles devraient être reliées aux exigences fondamentales de sécurité (cf. Partie 1-1)

Titre	*Security for industrial automation and control systems* *IEC 62443 – Part 3-2 : Security risk assessment and system design*

Date de publication	2013	Éditeur	IEC	Volume (pages)	28	Accès	payant

Synthèse	Présentation du processus de gestion des risques et des principes de conception des IACS

Synthèse

Ce document présente une méthode pour conduire une analyse/évaluation des risques et en déduire l'architecture de sécurité (i.e. les zones et conduits).

Ces exigences de sécurité s'appuient sur la combinaison de l'analyse fonctionnelle et de l'analyse des conséquences.

Ce document contient un glossaire très important qui reprend entre autres des termes définis ailleurs (ex. *achieved security assurance level*)

Il définit ensuite un processus de détermination des zones et des conduits

- Choix du périmètre
- Évaluation préliminaire des risques
- Détermination des exigences de sécurité
- Détermination des zones et conduits : séparation intranet business / réseau industriel ; séparation réseau de contrôle-commande / réseau de sécurité fonctionnelle ; séparation des équipements mobiles, des communications radio
- §4.5 : Évaluation détaillée du risque :
  - identification des sources de menace,
  - identification des vulnérabilités,
  - calcul du risque (vraisemblance / impact)
- §4.6 : Comparaison risque résiduel / risque acceptable.

Ces descriptions s'accompagnent de logigrammes précis. A noter que le second (detailed risk assessment) fait référence à une notion de *target effectiveness* jamais explicitée dans le document.

On trouve en annexe un exemple de scénario qui est en cours de développement, il manque des informations pour bien le comprendre.

Pertinence	Avis
	Ce document est intéressant mais trop incomplet. La démarche proposée fait penser comparer aux modèles de Stackelberg (séquence Défenseur – Attaquant – Défenseur) issus de la théorie des jeux et employés dans certaines études du risque terroriste.

Titre	*Security for industrial automation and control systems* *IEC 62443 – Part 3-3 : System security requirements and security levels*

Date de publication	2012	Éditeur	IEC	Volume (pages)	78	Accès	payant

Synthèse	Détail des exigences fondamentales de sécurité et répartition selon les niveaux de sécurité.

Synthèse

Ce document détaille sous forme de mesures précises les 7 exigences fondamentales de sécurité.

Un premier chapitre détaille les contraintes relatives à ces mesures de sécurité :

- le support des fonctions essentielles (les mesures de sécurité ne doivent pas entraver la disponibilité des fonctions essentielles)
- les contremesures de compensation (i.e. dépendance des mesures de sécurité fournies par une entité tierce, cf. Part 3-2)
- le principe de moindre privilège.

Ensuite chacune des exigences est présentée ainsi :

- expression de l'exigence au regard des 4 niveaux de sécurité
- découpage de l'exigence fondamentale en exigences élémentaires, pour chacune d'elle :
  - description
  - argumentaire et recommandations supplémentaires
  - renforcement de l'exigence
  - correspondance entre les niveaux de sécurité

Le format adopté est celui du NIST SP 800-53. Les mesures renforcées prennent tout leur sens avec les niveaux de sécurité supérieurs.

L'annexe A est une réflexion méthodologique sur l'utilisation du vecteur de niveau de sécurité (cf. Partie 1-1) dans le cadre de la gestion des risques.

L'annexe B fait la synthèse de la correspondance exigences élémentaires de sécurité / niveau de sécurité.

Pertinence	Avis
	Document intéressant, en particulier l'annexe A. De manière générale, l'ensemble des réflexions sur l'évaluation des risques distribuées dans les différentes parties du standard, mériteraient d'être rassemblées au sein d'une seule et même discussion.

Titre	*Security for industrial automation and control systems IEC 62443 – Part 4-1 :*

Date de publication	2013	Éditeur	IEC	Volume (pages)	74	Accès	payant

Synthèse	Descriptions des exigences de développement des produits d'un IACS

Synthèse

Ce document présente un cycle de vie du développement sécurisé (à ne pas confondre avec le cycle de vie de sécurité cf. Partie 1-1 §14).

Ce cycle bâti à partir de quelques-uns des travaux les plus significatifs dans le domaine (ISO 15408, CLASP, SDLC de Microsoft, IEC 61508, DO-178) est composé de 12 phases :

- Phase 1 : processus de gestion de la sécurité (processus global qui supporte les autres activités)
- Phase 2 : spécification des exigences de sécurité
- Phase 3 : conception de l'architecture sécurisée
- Phase 4 : modélisation de menaces et évaluation des risques (La définition de la modélisation de la menace - recherche de vulnérabilité - est étonnante…)
- Phase 5 : conception détaillée du logiciel
- Phase 6 : Guides de sécurité
- Phase 7 : Vérification et implémentation des modules
- Phase 8 : Test d'intégration de sécurité
- Phase 9 : Vérification du processus de sécurité
- Phase 10 : Planification de de la réponse de sécurité
- Phase 11 : Validation de la sécurité
- Phase 12 : Exécution de la réponse de sécurité

S'ajoute à ces phases un processus d'intégration de systèmes ou composants préexistants.

Pertinence	Avis
	Document intéressant mais inachevé. Les limites exactes du cycle de vie ne sont pas claires car la dernière phase concerne la phase opérationnelle du système qui est par définition en dehors du cycle de vie du développement.

Titre	*Security for industrial automation and control systems* *IEC 62443 – Part 4-2 : Technical Security Requirements for IACS Components*

Date de publication	2011	Éditeur	IEC	Volume (pages)	110	Accès	payant

Synthèse	Description des exigences techniques applicables aux équipements d'un IACS

Synthèse

Ce document présente les exigences techniques de sécurité devant être déployées sur l'ensemble des composants d'un IACS. Ces exigences sont le raffinement des exigences fonctionnelles présentées dans la Partie 3-3 et distribuées selon 4 types de composant :

- application
- équipement embarqué
- équipement hôte
- nœud réseau

Les exigences sont développées selon le même modèle : description générale de l'exigence, assortie d'un argumentaire puis déclinaisons sur les 4 types de composant.

Pour certaines exigences, la correspondance avec les niveaux de sécurité est exprimée.

Toutefois ce travail de raffinage des exigences est incomplet puisqu'il ne reprend pas l'ensemble de la Partie 3-3.

Pertinence	Avis
	Document non finalisé bien que la version courante date de 2011.

Titre	*IEC 62351 – Spécification technique – gestion des systèmes électriques et échanges d'informations – Sécurité des données et des communications*

Date de publication	2013	Éditeur	IEC	Volume (pages)	500	Accès	payant

Synthèse	

Synthèse

Cette spécification technique est produite par la TC57 de l'IEC. C'est un document très volumineux découpé en 11 chapitres.

Le chapitre 1 fait d'abord un panorama des risques et des contre-mesures possibles dans l'environnement des systèmes électriques, et contient ensuite une synthèse des chapitres suivants.

Le chapitre 2 est un glossaire.

Le chapitre 3 présente les mesures à prendre au niveau TCP-IP pour sécuriser les protocoles de communication. Il propose une implémentation de TLS plutôt qu'IPSEC.

Le chapitre 4 traite de la sécurisation des protocoles utilisant la couche MMS, à savoir TASE2 et 61850.

Le chapitre 5 traite de la sécurisation des protocoles de la série 60870-5 (protocoles 101 à 104). Il traite du cas de la version réseau de ces protocoles, auquel cas on peut utiliser TLS, sous réserve que les canaux de communication supportent les flux induits, mais aussi le cas de la version liaison série point à point.

Le chapitre 6 traite des mesures additionnelles spécifiques au protocole 61850, complémentaires à celles des chapitres 3 et 4.

Le chapitre 7 définit des modèles d'objets, construits à la manière des MIB SNMP, adaptés à la supervision des équipements d'un système électrique et de leur sécurité. Il s'agit d'objets abstraits, le protocole porteur n'étant pas forcément SNMP, il peut être aussi 61850, TASE2,…

Le chapitre 8 traite du contrôle d'accès à base de rôles (RBAC) pour les utilisateurs et les automates.

Enfin, le chapitre 10 est un guide d'architecture de sécurité.

Les deux derniers chapitres (no9 management et no11 sécurité pour xml) ne sont pas encore parus.

Pertinence	Avis
★★★★	Document fondamental pour qui désire sécuriser les communications dans le monde des systèmes électriques. Ce document s'adresse aux compagnies électriques, mais aussi et surtout aux constructeurs d'équipements et de SCADA de cette industrie ainsi qu'aux développeurs de souches de communication. On peut cependant noter qu'il ne traite pas de la sécurisation des communications basées sur des web services, pourtant de plus en plus utilisés dans les Smart Grids. Néanmoins, d'autres initiatives plus avancées existent sur ce sujet (openADR Alliance, notamment)

Secteur	
Énergie	☑
Nucléaire	☐
Santé	☐

Populations visées	
DSI	☑
RSSI	☐
Constructeurs	☑

Typologie Réseau	
Embarqué	☐
Site	☑
Étendu	☑

Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Intégrateurs Maintenance	☑
Opérateurs sur site	☑
Auditeurs	☐
Autres	☐

Titre	*IEC 61508: Standard for Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*

Date de publication	2010	Éditeur	IEC	Volume (pages)	400	Accès	payant

Synthèse	Standard de développement et de maintenance de systèmes fonctionnels sécurisés

Synthèse

- Norme proposant une démarche de certification des fonctions de sécurité et de leurs composants.

- IEC 61508 est destinée à être une norme de sécurité fonctionnelle de base applicable à tous les types d'industrie. La norme permet de couvrir l'ensemble du cycle de vie de sécurité : depuis les exigences jusqu'au retrait du système (Parties 1-3 les exigences normatives de la norme, Parties 4-7 sont des guides et exemples de mise en œuvre de la démarche).

- C'est une norme orientée « Performance » (à l'instar des normes dites déterministes et prescriptives) qui est basée sur une analyse et évaluation du risque associé au système E/E/EP intégrant une classification des risques en 4 classes (un peu comme la DO178B/ED 12C).

- Elle fournit une approche pragmatique et surtout, via les normes sectorielles 61511/62061/61513/Ferroviaire EN501x) une mise en œuvre et une démarche applicable pour permettre de réaliser une analyse de sécurité et aussi de permettre d'établir les objectifs attendus vis-à-vis du système.

- Elle intègre aussi bien la partie développement (système et logiciel) que les aspects d'organisation et de management de la sécurité.

- Est parfaitement utilisable avec d'autres méthodes d'analyse tels qu'EBIOS ou HISA

Pertinence	Avis
★★★★★	Norme orientée vers une approche système de la sécurité en prenant en compte l'ensemble du cycle de vie du système. Son applicabilité est facilité par les normes sectorielles (industrie : 61511, nucléaire : 61513…). A promouvoir lors de la prise en compte de la sécurité vis-à-vis des nouveaux projets, à utiliser comme démarche initiatique sur des systèmes existants.

Secteur	
Énergie	☑
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☑
Eau / Assainissement	☐
Chimie / Pharmacie	☑
Autre / Transverse	☑

Populations visées	
DSI	☐
RSSI	☑
Constructeurs	☑
Intégrateurs Maintenance	☑
Opérateurs sur site	☐
Auditeurs	☑
Autres	☑

Typologie Réseau	
Embarqué	☐
Site	☑
Étendu	☑

Titre	*Technical report IEC 62210 – Contrôle et communications associées pour les systèmes électriques – sécurité des communications et des données*

Date de publication	05/2003	Éditeur	IEC	Volume (pages)	52	Accès	payant

Synthèse	

Synthèse

Les principaux protocoles de communication temps réel utilisés dans les systèmes électriques sont des normes IEC (60870-5, 60870-6 et 61850). Or, ils ont été conçus avant que les questions de sécurité ne deviennent de réelles préoccupations. Ils n'implémentent donc pas nativement de fonctions de sécurité. Ainsi, dès 1997, la TC57 s'est intéressé à la question et a produit le rapport technique 62210 (le présent document) puis, plus tard, la spécification technique 62351 qui développe des standards de sécurité pour les protocoles susnommés.

Ce document traite essentiellement des menaces spécifiques aux réseaux électriques. Il constitue la trame d'une analyse de risques globale d'un système électrique.

Pertinence	Avis
★	Document assez peu utile depuis la publication de la spécification 62351 qui reprend l'essentiel de son contenu.

Secteur	
Énergie	☑
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☐
RSSI	☑
Constructeurs	☐
Intégrateurs Maintenance	☐
Opérateurs sur site	☐
Auditeurs	☐
Autres	☐

Typologie Réseau	
Embarqué	☐
Site	☐
Étendu	☑

Titre	*ISO/IEC TR 27019*

Date de publication	2013	Éditeur	ISO/IEC	Volume (pages)	320	Accès	payant

Synthèse	Lignes directrices de management de la sécurité de l'information fondées sur l'ISO/IEC 27002 pour les systèmes de contrôle des procédés spécifiques à l'industrie de l'énergie

Synthèse

Cette norme se présente comme un complément à l'ISO/IEC 27002. Le document reprend la structure de ce guide de bonnes pratiques tout en y intégrant les spécificités des SI industriels, notamment par l'ajout de nouvelles sections.

L'ISO/IEC TR 27019 complète et donne des précisions quant à la mise en œuvre de mesures de sécurité dans le contexte particulier des systèmes industriels du secteur de l'énergie.

Les exigences d'inventaires sont précises et inclues des exemples d'actifs de type industriels. Le document rappel la nécessité d'identifier les risques relatifs à l'écosystème industriel. Les intégrateurs, fournisseurs, et personnels de maintenance, l'interconnexion avec des systèmes tiers, la difficulté de protéger des équipements situés dans des lieux difficiles d'accès, inoccupés, des lieux publics, ou des locaux de tiers sont mentionnés.

Le fait de prendre en compte les aspects sécurité dans les contrats avec les tiers est précisé, en particulier avec les opérateurs télécom : mesures de gestion de crises et de communication d'urgence en cas de blackout, anticipation du risque de surcharge...

Les principes de cloisonnement sont largement abordés. Ils reposent sur les concepts de zones et de conduits mis en avant dans l'IEC 62443.

L'ISO/IEC TR 27019 souligne également les risques provenant des systèmes dît « historiques », potentiellement très vulnérables car rarement voire jamais tenus à jour.

En termes d'évolution du SI industriel, le recours à des simulateurs et des environnements dédiés de développements est recommandé par cette norme sans pour autant être une obligation suivant le contexte.

Enfin, les problématiques de sureté des sites et des bâtiments (localisation de salles, risque de séismes, inondation, manipulation de matières dangereuse, incendies…) ainsi que la sureté des installations (isolation et protection des systèmes de sureté, interdiction d'accès à distance, journalisation…) sont également abordées dans cette norme.

Pertinence	Avis
★★★★	L'ISO/IEC TR 27019 tente d'aller à l'essentiel en se focalisant uniquement sur les spécificités des SI industriels. L'ISO/IEC 27002 voire 27001 est à utiliser en complément de cette norme pour être exhaustif sur le sujet sécurité (volet technique et organisationnel) Toutes les réponses ne s'y trouvent pas. En effet ce guide permet avant tout de se poser les bonnes questions. Celles qui y sont soulevées devront inciter les RSSI et l'ensemble des responsables des SI industriels à réfléchir ensemble pour concevoir la sécurité de leur SI Industriel.

Secteur	
Énergie	☑
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☑

Populations visées	
DSI	☑
RSSI	☑
Constructeurs	☑
Intégrateurs Maintenance	☑
Opérateurs sur site	☑

Typologie Réseau	
Embarqué	☐
Site	☑
Étendu	☑

Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☐

Auditeurs	☑
Autres	☐

Titre	*Cyber Security Procurement Language for Control Systems Version 1.8*

Date de publication	02/2008	Éditeur	INL (U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance)	Volume (pages)	120	Accès	gratuit

Synthèse	Ce document est une boîte à outils à destination des Acheteurs et des chefs de projet leur permettant d'embarquer la sécurité dans leurs projets industriels.

Synthèse

Ce document est une boîte à outils à destination des Acheteurs et des chefs de projet. Il propose, pour une quarantaine d'objectifs de sécurité, ventilés sur de nombreux domaines (durcissement des systèmes, Segmentation Réseau, Protection périmétrique, Gestion des comptes, Pratiques de développement, Accès distants, Sécurité Physique, Terminaux Utilisateurs…) les informations suivantes :

- Un rappel du risque.
- Une description des bonnes pratiques de sécurité.
- Un libellé traduisant en termes compréhensibles non techniques, les objectifs de sécurité que la solution doit embarquer pour couvrir les vulnérabilités communément identifiées dans des systèmes industriels. Ce libellé, prêt à l'emploi, peut être intégré directement dans un cahier des charges ou un appel d'offre.
- Une liste des tests à opérer lors de la recette de l'équipement pour vérifier que chaque exigence de sécurité prévue est effectivement intégrée dans le produit et qu'elle répond aux objectifs de sécurité attendus.
- Une liste des tests à opérer pour s'assurer qu'une opération de maintenance sur le produit ne provoque pas des non-régressions sur les mesures de sécurité.

Pertinence	Avis
★★★★	Catalogue complet et prêt à l'emploi. Un plus indéniable pour intégrer la sécurité au cœur des systèmes industriels, dès le processus d'achat.

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☐
RSSI	☐
Constructeurs	☐
Intégrateurs Maintenance	☑
Opérateurs sur site	☐
Auditeurs	☐
Autres, Acheteurs	☑

Typologie Réseau	
Embarqué	☐
Site	☐
Étendu	☐

Titre	*Critical Infrastructure Protection Standards*

Date de publication	2012	Éditeur	NERC	Volume (pages)	320	Accès	gratuit

Synthèse	Norme pour la sécurité des réseaux électriques rendue obligatoires sur l'ensemble des réseaux de transport électrique Nord-Américains (États Unis et Canada)

Synthèse

Plus qu'une norme, la suite de standards NERC CIP est un guide de conformité que doivent respecter les opérateurs des réseaux électriques nord-américains.

Le guide est constitué de 11 volumes abordant respectivement les exigences relatives à l'obligation de signalement d'actes de sabotage (CIP-001), l'identification des actifs « informatiques » et l'évaluation de leur niveau de criticité (CIP-002), la formalisation de politiques de sécurité spécifiques sur les sujets adressés dans les standards CIP-004 à CIP-011 (CIP-003), la sensibilisation et la formation du personnel (CIP-004), la protection logique des actifs « informatiques » constituants les réseaux électriques (CIP-005), la protection physique de ces mêmes constituants (CIP-006), la mise en œuvre de mesures de durcissement des systèmes (renforcement des contrôles d'accès aux systèmes, patch management, protection contre les codes malveillants) et de leur supervision (CIP-007), la mise en œuvre d'un programme de gestion et de réponses aux incidents (CIP-008), la définition d'un plan de secours et de reprise (CIP-009), la gestion des modifications et des vulnérabilités (CIP-010) et enfin la protection des informations (CIP-011).

Chaque volume du guide NERC CIP énonce des exigences, liste des mesures à implémenter répondant aux exigences et décrit les méthodes à mettre en œuvre pour vérifier la conformité des installations à ces exigences et mesures de sécurité. Une échelle est d'ailleurs proposée pour déterminer le niveau de « non-conformité » au standard (4 niveaux).

Pertinence	Avis
★★★	La suite de standards NERC CIP est fondamentalement destinée aux réseaux électriques nord-américains et la question de son application à d'autres territoires peut se poser. Elle nécessitera dans tous les cas des adaptations (éléments de langages, règlementations, autorités différentes…). Même si la structure proposée semble claire, globalement les documents ne sont pas simples à lire. Il y a en effet de multiples pointeurs intra et inter standards qui complexifient la compréhension et la lecture de ces documents. Néanmoins, la suite de standards NERC CIP tente d'être exhaustive sur le sujet de la CyberSécurité. Viser la conformité à ces standards reviendrait ni plus ni moins à mettre en place un Système de Mangement de la Cybersécurité des Réseaux Électriques.

Secteur	
Énergie	☑
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☐

Populations visées	
DSI	☐
RSSI	☑
Constructeurs	☐
Intégrateurs Maintenance	☐
Opérateurs sur site	☑
Auditeurs	☑
Autres	☐

Typologie Réseau	
Embarqué	☐
Site	☑
Étendu	☑

Titre	*Framework for Improving Critical Infrastructure Cybersecurity*

Date de publication	02/2014	Éditeur	NIST	Volume (pages)	41	Accès	gratuit

Synthèse	Cadre de référence pour la gestion des risques en cybersécurité des infrastructures critiques

Synthèse

Il s'agit d'un document d'orientation proposant un *Framework* générique de cybersécurité spécifiquement destiné aux systèmes critiques (incluant en premier lieu les ICS et OIV), élaboré par le NIST mandaté par l'ordonnance (*Executive Order 13636 - Improving Critical Infrastructure Cyber Security*) publiée par le Président Obama en février 2013 et au calendrier associé.

Ce Framework est structuré en 3 parties : *Core*, *Implementation Tiers*, et *Profiles*.

La partie *Core* identifie 5 fonctions de haut-niveau (core functions) : *Identity*, *Protect*, *Detect*, *Respond*, et *Recover*, permettant en principe de couvrir de façon exhaustive l'ensemble des activités de cybersécurité, allant de la gestion de risques par l'exécutif à l'implémentation des mesures de sécurité appropriées au niveau opérationnel. Chacune de ces fonctions est divisée en catégories, elles-mêmes subdivisée en sous-catégories.

La partie *Implementation Tiers* (niveau d'implémentation) définit 4 niveaux d'implémentation (ou de maturité) : Parial (Tier 1), Risk informed (Tier 2), Repeatable (Tier 3) et Adaptive (Tier 4), permettant de choisir la cible de sécurité en fonction de la tolérance aux risques du système considéré.

La partie *Profiles* permet enfin d'évaluer l'alignement du management de la cybersécurité (via profil d'évaluation pour chaque fonction, catégorie, sous-catégorie du Core) au regard de la cible de sécurité (*Tier*) définie par l'organisation, de façon à définir la trajectoire à suivre au travers d'un plan de progrès priorisé et optimisé pour atteindre les objectifs fixés.

Le contenu détaillé du Framework est présenté en Annexe A sous la forme d'un plan de contrôle mis en correspondance avec les référentiels COBIT 5, CCS Top 20 Critical Security Controls, IEC 62443-2-1:2009, IEC 62443-3-3:2013, ISO/IEC 27001:2013 et NIST SP 800-53 Rev.4.

Ainsi, ce Framework vise au final à établir les lignes directrices d'un programme de cybersécurité basé sur un processus comportant 7 étapes clés (état des lieux, analyse de risques, analyse d'écarts, plan d'actions, etc.), à appliquer en amélioration continue.

Pertinence	Avis
★★★★	À défaut d'être fondamentalement révolutionnaire, ce référentiel (probable futur standard « incontournable », surtout outre-Atlantique) offre principalement l'avantage d'être relativement consensuel en proposant une démarche structurante, applicable à tout contexte (industriel ou non d'ailleurs) et dont la déclinaison opérationnelle est laissé à la discrétion des organisations, par système de renvoi aux référentiels internationaux réputés. À noter également que ce document s'intéresse à la protection de la propriété intellectuelle, de la vie privée et des libertés individuelles mais également à l'applicabilité ainsi qu'au coût de mise en œuvre des mesures de réduction des risques, sans approfondir pour autant.

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☑
RSSI	☑
Constructeurs	☑
Intégrateurs Maintenance	☑
Opérateurs sur site	☑
Auditeurs	☑
Autres	☐

Typologie Réseau	
Embarqué	☐
Site	☑
Étendu	☑

Titre	*Guide to Industrial Control Systems (ICS) Security*

Date de publication	06/2011 / révision en 2013	Éditeur	NIST	Volume (pages)	155	Accès	gratuit

Synthèse	Ce document du NIST donne une vue d'ensemble de la problématique de la sécurité des systèmes de contrôle industriel (menaces et vulnérabilités, contre-mesures...)

Synthèse

Ce document propose une approche structurée en 5 parties:

1. **Présentation des différents éléments faisant partie d'une implémentation de systèmes de contrôle industriel** (composants réseau et de contrôle par exemple) avec en particulier un focus sur les systèmes SCADA (Supervisory Control And Data Acquisition), les DCS (Distributed Control Systems) et les PLC (Programmable Logic Controllers) qui sont englobés sous le terme générique d'ICS.

2. **Description des caractéristiques des ICS, des menaces et des vulnérabilités associées à ces systèmes, ainsi que des incidents (sources et scenarii d'incidents**). Une liste intéressante des éléments menaçant est fournie et comprend notamment les groupes criminels ou terroristes et les agences de renseignement étrangères. Les vulnérabilités potentielles ainsi que les facteurs de risque sont catégorisés. Par exemple, les vulnérabilités sont scindés en 3 grands groupes: le premier portant sur les politiques et procédures, le deuxième sur les plates-formes (configuration, hardware, software…) et le dernier sur celles liées aux réseaux (réseau sans-fil…).

3. **Aide à la création d'un programme de sécurité spécifique** aux ICS dont la rédaction d'un business case constitue la première étape.

4. **Définition des composants (firewalls…), des grands principes et concepts** (ségrégation des réseaux, défense en profondeur, redondance, tolérance aux pannes…) à utiliser et à appliquer dans une architecture réseau incluant des ICS pour améliorer son niveau de sécurité. Une liste de protocoles réseau à filtrer au niveau des firewalls est aussi fournie.

5. **Détail des contrôles de sécurité à mettre en œuvre** qui se divisent en 3 catégories: les contrôles managériaux (estimation et évaluation du risque, planning…), les contrôles opérationnels (sécurité du personnel, maintenance, protection des médias, gestion de la configuration…) et les contrôles techniques (identification et authentification, contrôle d'accès, audit…).

Pertinence	Avis
★★★★★	Document incontournable bien que datant de 2011, il est régulièrement revu.

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☑
RSSI	☑
Constructeurs	☐
Intégrateurs Maintenance	☑
Opérateurs sur site	☐
Auditeurs	☑
Autres	☑

Typologie Réseau	
Embarqué	☐
Site	☐
Étendu	☐

Titre	*Regulatory Guide 5.71 – Cyber security programs for nuclear facilities*

Date de publication	01/2010	Éditeur	NRC (Nuclear Regulatory Commission)	Volume (pages)	105	Accès	gratuit

Synthèse	Description assez détaillée de la mise en œuvre d'un plan de cybersécurité et des actions et mesures à prendre en compte afin de réduire les risques, ceci en conformité avec les exigences de la réglementation 10 CFR 73.54 et vis-à-vis des fonctions relatives et importantes pour la sûreté, des fonctions de sécurité, des fonctions relatives/associées aux situations d'urgence.

Synthèse

Documents de référence : **10 CFR 73.54** - Réglementation concernant la mise en œuvre et le maintien d'un plan de cybersécurité relatif aux équipements informatique, aux systèmes et réseaux de communication ; **10 CFR 73.1** - Définition de la menace de base (Design Basic Threat) ; **NIST SP 800-82** - Guide to Industrial Control System Security et **NIST SP 800-83** - Guide to Malware Incident Prevention and Handling.

La RG 5.71 :

- Fournit une synthèse des exigences et dispositions réglementaires relatives à la cybersécurité (section C1),
- Fournit des éléments sur le contenu d'un plan de cybersécurité et une méthode de développement du plan (section C2)
- Fournit une méthode de création d'équipe chargée de la cybersécurité et d'identification des éléments à protéger, aborde les cyber-risques potentiels pouvant nuire à un élément à protéger, introduit les stratégies de défense dont la défense en profondeur (section C3),
- Traite des moyens nécessaires au maintien en condition opérationnelle du plan (section C4),
- Liste, non exhaustivement, les données à enregistrer et à conserver dans le but, notamment, de tracer et de découvrir la source des attaques (section C5).

Appendix A : Méthode/procédures de développement/mise en place d'un plan de cybersécurité. Cette partie correspond à l'appendix A de la NEI 08-09.

Appendix B : Mesures à mettre en œuvre dans le but d'assurer la disponibilité, l'intégrité et la confidentialité d'un système. Cette partie correspond à l'appendix D de la NEI 08-09.

Appendix C : Activités de management d'un plan de cybersécurité. Cette partie correspond à l'appendix E de la NEI 08-09.

Document clair et très complet, essentiellement orienté méthodologie/procédures, qui donne des pistes de développement mais sans proposer de solutions quant à l'architecture et aux équipements à mettre en œuvre.

Pertinence	Avis
★★★★	Document très intéressant du point de vue du GT car faisant référence aux systèmes de contrôle-commande dont les systèmes relatifs à la sûreté. Ce document est pratiquement redondant avec le document « NEI 08-09 – Cyber Security Plan for Nuclear Power reactors ».

Secteur	
Énergie	☐
Nucléaire	☑
Santé	☐
Aérien	☐

Populations visées	
DSI	☐
RSSI	☑
Constructeurs	☐
Intégrateurs Maintenance	☑

Typologie Réseau	
Embarqué	☐
Site	☑
Étendu	☐

Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☐

Opérateurs sur site	☑
Auditeurs	☑
Autres : ingénierie système	☑

Titre	*Protection of digital computer and communication systems and networks*

Date de publication	11/2009	Éditeur	NRC (Nuclear Regulatory Commission)	Volume (pages)	2	Accès	gratuit

Synthèse	Exigences à satisfaire dans le cadre de la mise en œuvre d'un plan de cybersécurité relatif aux équipements informatique, aux systèmes et réseaux de communication.

Synthèse

Ce document précise :

- Les fonctions et systèmes à protéger contre les cyber-attaques et leurs conséquences ;
- La méthodologie à mettre en place dans le cadre de l'établissement du plan ;
- Les objectifs à atteindre dans le cadre de la mise en place du plan de cybersécurité ;
- Les actions à mettre en œuvre afin de sensibiliser les acteurs et de maintenir le niveau de performance objectif ;
- Les réponses que doit apporter le plan de sécurité vis-à-vis des exigences et des cyber-attaques ;
- Les actions de gestion du plan de cybersécurité à mener dans le cadre de son maintien opérationnel ;
- Les actions de mise en œuvre (intégration) du plan de cybersécurité vis-à-vis du programme global de sécurité physique du site.
- Les actions d'enregistrement et de gestion documentaire

Pertinence	Avis
★★★	Document de référence intéressant donnant les bases (exigences) à respecter dans le cadre de la mise en œuvre d'un plan de protection.

Secteur	
Énergie	☐
Nucléaire	☑
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☑
RSSI	☑
Constructeurs	☐
Intégrateurs Maintenance	☑
Opérateurs sur site	☑
Auditeurs	☑
Autres	☑

Typologie Réseau	
Embarqué	☐
Site	☑
Étendu	☐

Titre	*Cybersecurity Through Real-Time Distributed Control Systems (RTDCS)*

Date de publication	2010	Éditeur	OAK Ridge / US DoE	Volume (pages)	30	Accès	gratuit

Synthèse	Vue d'ensemble sur la démarche de cybersécurité des RTDCS

Synthèse

- Classification des vulnérabilités de Cybersécurité d'un RTDCS (Top 10), Tableaux sur les différents types et sources de vulnérabilités.

- Définition d'un Modèle Cybersécurité Attaque/Vulnérabilité/Dommage orienté étude des modes de défaillance (style FMECA, HISA).

- Description des vulnérabilités liées aux communications filaires et sans fil.

- Stratégie de minimisation basée sur les méthodes et techniques utilisées dans l'industrie Nucléaire et adaptée pour la Cybersécurité : tableau de ressources utiles sur la cybersécurité.

Pertinence	Avis
★★	Bon document de vulgarisation sur l'aspect de cybersécurité concernant les systèmes industriels ouverts vers l'extérieur (style BYOND).

Secteur	
Énergie	☑
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☑
Eau / Assainissement	☑
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☑
RSSI	☑
Constructeurs	☐
Intégrateurs Maintenance	☐
Opérateurs sur site	☐
Auditeurs	☐
Autres	☑

Typologie Réseau	
Embarqué	☐
Site	☑
Étendu	☑

Titre	*Methodology for Prioritizing Cyber-vulnerable Critical Infrastructure Equipment and Mitigation Strategies*

Date de publication	2010	Éditeur	Sandia	Volume (pages)	42	Accès	gratuit

Synthèse	Méthode générique d'évaluation de la cybersécurité d'un système industriel

Synthèse

Ce document est le premier d'une série de trois rapports destinés à élaborer puis mettre en œuvre une démarche permettant, d'abord, d'identifier et de hiérarchiser des composants (cyber)-vulnérables d'un infrastructure vitale, ensuite, de choisir une stratégie efficace de maîtrise des risques.

Remarque : les deux autres rapports, qui montrent les applications particulières de la méthode générique aux secteurs de la distribution électrique et de la gestion de l'eau, ne sont pas publics. Pour autant, ce premier rapport est difficilement dissociable du second document intitulé « Categorizing Threat Building and Using a Generic Threat Matrix ».

Après une introduction rappelant les objectifs et le champ d'application, le document se compose de 5 sections.

La première définit la méthode d'analyse et d'assurance des éléments essentiels de l'infrastructure vitale considérée. La démarche proposée consiste à :

- Constituer l'équipe d'évaluation et recueillir les données d'entrée nécessaires : l'accent est mis sur les compétences requises
- Construire un modèle représentatif du système-cible, puis évaluer les impacts d'une attaque et déterminer la criticité des constituants (qui dépend aussi des différentes interdépendances et pas seulement des impacts)
- Déterminer les niveaux de menace éligibles puis développer les scénarios d'attaque.
    - L'étude des menaces s'appuie sur le modèle particulier que Sandia a mis au point pour ses activités de *red teaming*, tout en le mettant en correspondance avec la grille standard du DHS (4 niveaux – de *nation state* à *garden variety*),
    - Les scénarios sont développés en identifiant les points d'entrée puis les chemins d'attaque vers la cible, sous la forme d'une séquence d'actions,
    - Le niveau de menace minimal est explicité pour chacune de ces actions, ce qui va permettre d'évaluer,
- Analyser puis évaluer l'efficacité des mesures de sécurité en estimant l'effet de ladite mesure sur le niveau de menace requis pour cette action ; si la mesure est efficace, ce niveau minimal doit croître.
- Choisir à partir des analyses précédentes un ensemble de mesures de sécurité constituant la stratégie de défense.

La seconde section propose une discussion générale sur :

- Les stratégies de protection, définies comme l'ensemble des actions visant à empêcher ou à réduire les occurrences d'une attaque en augmentant les capacités requises pour l'exécuter ;
- Les stratégies de réduction des conséquences, en séparant les actions de court terme, comme la gestion de modes dégradés, ou de plus long terme, comme la redondance

d'équipements ou leur ré-ingénierie pour développer leur robustesse.

Les troisième et quatrième parties, qui sont assez succinctes, discutent respectivement des analyses coût / bénéfice et du processus formel de vérification et validation (V&V).

La conclusion donne quelques éléments d'appréciation supplémentaires sur la mise en œuvre de cette démarche, à partir des deux exemples d'application.

Le document sur une série de recommandations, en soulignant notamment la nécessité d'impliquer toutes les parties prenantes.

Pertinence	Avis
	C'est un document très intéressant pour les infrastructures vitales, car il présente une démarche bien structurée permettant de conduire une analyse de risque approfondie, notamment fondée sur l'étude détaillée des sources de menace, puis de choisir avec une grande finesse des mesures de sécurité adaptées aux risques. Malheureusement, les exemples d'application ne sont pas disponibles.

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☐
RSSI	☐
Constructeurs	☐
Intégrateurs Maintenance	☐
Opérateurs sur site	☐
Auditeurs	☐
Autres	☑

Typologie Réseau	
Embarqué	☐
Site	☐
Étendu	☑

Titre	*Control System Devices : Architectures and supply Channels Overview*

Date de publication	2010	Éditeur	Sandia	Volume (pages)	70	Accès	gratuit

Synthèse	Rapport sur la sécurité matérielle des composants des systèmes de contrôle

Synthèse

Ce rapport s'inscrit dans les études sur la réduction des menaces vis-à-vis des systèmes de contrôle des infrastructures critiques et se focalise sur la sécurité des PLC qui, au contraire des équipements de type PC, ont été peu étudiés. Une analyse détaillée des composants matériels et des logiciels de bas niveau est nécessaire pour développer des stratégies de défense efficaces contre des adversaires sophistiqués.

Une première partie présente une architecture des systèmes de contrôle à 2 niveaux - le centre de contrôle et les sites - qui est une version simplifiée d'un modèle objet général non fourni, puis fournit une description générique mais détaillée d'un PLC.

La partie suivante est consacrée à une étude de marché des fournisseurs de PLC.

Pertinence	Avis
★	Ce document centré sur l'étude de marché est peu intéressant

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☐
RSSI	☐
Constructeurs	☐
Intégrateurs Maintenance	☐
Opérateurs sur site	☐
Auditeurs	☐
Autres	☑

Typologie Réseau	
Embarqué	☐
Site	☑
Étendu	☐

Titre	*Security Framework for control System Data classification and Protection*

Date de publication	2007	Éditeur	Sandia	Volume (pages)	33	Accès	gratuit

Synthèse	Guide sur la classification et la protection des données pour les systèmes industriels

Synthèse

Constatant les grandes difficultés rencontrées sur le terrain pour appliquer les recommandations et/ou exigences réglementaires de sécurité des systèmes industriels, ce rapport définit une démarche générique d'identification, de classification et de protection des données.

La multiplication des COTS remplaçant progressivement les produits propriétaires, la variété des types de données mises en jeu, ainsi que la nécessité d'avoir une protection adaptée aux enjeux rendent nécessaire l'établissement d'une démarche rationnelle et générique.

A partir de ses propres retours d'expérience, de différents modèles et standards existants, et en s'appuyant sur une représentation détaillée, Sandia a élaboré un processus subdivisé en 4 phases :

- Identification des données à partir d'une représentation détaillée d'un système de contrôle dans le domaine énergétique (considéré comme applicable à tout système de contrôle)

- Classification des données par une approche itérative qui établit le lien entre les données identifiées et les services fournis par le système

- Élaboration d'un profil de protection constitué de l'ensemble des exigences de sécurité nécessaires pour contrer des menaces qui auront été préalablement déterminées. Les attributs habituels DIC sont complétés par la fiabilité, l'authenticité et la non-répudiation.

- Lignes directrices pour l'implémentation sous la forme d'une liste de questions guidant la mise en œuvre de la démarche.

Pertinence	Avis
★★	Le processus générique présenté est intéressant en soi mais il reste à un niveau théorique et mériterait d'être accompagné d'un véritable exemple, articulé autour du modèle général de système de contrôle industriel de Sandia.

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☐
RSSI	☑
Constructeurs	☐
Intégrateurs Maintenance	☐
Opérateurs sur site	☐
Auditeurs	☐
Autres	☐

Typologie Réseau	
Embarqué	☐
Site	☐
Étendu	☑

Titre	Framework for SCADA Security Policy

Date de publication	2005	Éditeur	Sandia	Volume (pages)	6	Accès	gratuit

Synthèse	Principes et règles pour établit une Politique de Sécurité spécifique aux Systèmes Industriels

Synthèse

Dans une première partie, ce livre blanc établit différents constats sur la mise en œuvre d'une politique de sécurité pour les systèmes informatiques industriels :

- difficultés de mise en œuvre de certains principes de sécurité informatique traditionnels (ex. anti-virus, gestion des correctifs) ;
- besoins de sécurité particuliers (ex. gestion du temps),

Il conclut à la nécessité de définir et appliquer une politique de sécurité dédiée aux systèmes industriels et séparée de la politique de sécurité IT « traditionnelle ». Premier jalon d'un programme de sécurité – cette politique doit, d'une part, s'appuyer sur les exigences des métiers, d'autre part, être pilotée par un processus de gestion des risques qui identifie précisément où le système est vulnérable à des attaques.

La seconde partie rappelle les concepts fondamentaux d'une politique de sécurité.
La troisième partie expose le cadre élaboré par Sandia : SCADA Security Policy Framework ™.

Ce cadre organise la politique de sécurité en 9 sections : Sécurité des données ; Sécurité des plateformes ; Sécurité des communications, Sécurité du personnel ; Gestion de la configuration ; Audit ; Sécurité des applications ; Sécurité physique ; Sécurité des opérations manuelles.

Chacun de ces domaines est ensuite présenté de manière succincte.

Pertinence	Avis
★★	C'est un document qui présente de façon claire une structure possible pour une politique de sécurité des SI industriels. Malheureusement, il ne montre pas comment répondre aux problèmes identifiés dans sa première partie.

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☐
RSSI	☑
Constructeurs	☐
Intégrateurs Maintenance	☐
Opérateurs sur site	☐
Auditeurs	☐
Autres	☐

Typologie Réseau	
Embarqué	☐
Site	☐
Étendu	☑

Titre	*Guide sur l'évaluation des vulnérabilités dans le cadre des standards CIP*

Date de publication	2008	Éditeur	Sandia	Volume (pages)	19	Accès	gratuit

Synthèse	Guide sur l'évaluation des vulnérabilités dans le cadre des standards CIP

Synthèse

Ce document définit une démarche complète d'évaluation des cyber-vulnérabilités à mettre en œuvre dans le cadre des standards CIP (Critical Infrastructure Protection) du NARC (North American Reliability Corporation) qui énoncent une série d'exigences relatives à la gestion des vulnérabilités.

Cette démarche adapte dans le cadre des standards CIP les méthodes d'évaluation pratiquées par le Sandia qui décomposent le processus en 4 phases : planification de l'évaluation; conduite de l'évaluation ; rapport des résultats ; planification du traitement des vulnérabilités.

Un accent particulier est mis sur l'organisation et documentation pour chacune des phases.

Les différentes activités composant le processus sont ensuite présentées de manière détaillées en suivant les exigences particulières des standards CIP :

- CIP-007 Critical Cyber Assets vulnérabilité Assessment qui concerne les équipements situés à l'intérieur du périmètre de sécurité (restriction des ports et services actifs, gestion des comptes).

- CIP-005 Security Perimeter Cyber Vulnerability Assessment qui couvre tous les points d'accès (découverte des points d'accès, sécurité des comptes et des mots de passe, sécurité des fonctions de gestion du réseau).

Un travail supplémentaire est mené pour analyser les interactions avec l'exigence CIP-006 relative à la sécurité physique.

Pertinence	Avis
	Le principal intérêt de ce guide, qui reste très général, est de rappeler l'importance de l'organisation et de la planification qui doivent précéder la conduite effective de l'évaluation des vulnérabilités

Secteur	
Énergie	☑
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☐

Populations visées	
DSI	☐
RSSI	☐
Constructeurs	☐
Intégrateurs Maintenance	☐
Opérateurs sur site	☐
Auditeurs	☑
Autres	☐

Typologie Réseau	
Embarqué	☐
Site	☐
Étendu	☑

Titre	*SANS SCADA and Process Control Survey*

Date de publication	02/2013	Éditeur	SANS	Volume (pages)	18	Accès	gratuit

Synthèse	Synthèse résultant d'une enquête menée aux États-Unis d'Amérique par le SANS Institute.

Synthèse

Ce document est la synthèse résultant d'une enquête menée aux États-Unis par le SANS Institute auprès de plus de 700 entreprises, disposant de systèmes de contrôle industriel, sur leur sensibilisation aux risques SSI et sur leurs pratiques en termes de sécurité.

Ce document se compose de 4 parties inégales:

1. **Analyse de l'origine des participants** (domaine d'activités de l'entreprise, taille de l'organisation et fonction de la personne ayant répondu à l'enquête). Toutefois, les entreprises qui étaient principalement visées sont celles appartenant aux 18 secteurs d'importance vitale (pétrole et gaz, industrie chimique, transport, production d'électricité, eau…) pour les États-Unis d'Amérique et qui sont identifiées dans le NIPP (National Infrastructure Protection Plan).

2. **Leur sensibilisation aux risques.** Des résultats sont donnés sur leur perception des risques SSI liés aux systèmes de contrôle industriel (53,2% ne peuvent l'estimer) et sur leur appréciation des menaces (les malwares de type Stuxnet ou Flame ainsi que les menaces internes sont cités le plus souvent). Des statistiques sont aussi fournies sur les incidents de sécurité. Par exemple, 40 % des participants ont répondu que leurs systèmes ont été compromis ou qu'ils ne le savent pas.

3. **Leurs programmes de sécurité.** Dans cette partie, l'objectif est de dresser un panorama des pratiques de sécurité de ces entreprises. Par exemple, sur leurs drivers pour implémenter des mesures de sécurité (70 % des personnes qui ont répondu veulent éviter des interruptions sur les systèmes de contrôle industriel), sur la gestion et la corrélation des logs provenant de différentes sources citées dans le questionnaire (équipements réseaux, SCADA…), sur les standards appliqués (le guide NIST "SCADA and ICS" est le plus cité), sur les pratiques de patch et de mises à jour…

4. **Liste de recommandations.** 8 recommandations générales et de bon sens sont données à la fin du document en particulier sur la nécessité de mettre à jour les systèmes et de détecter leurs vulnérabilités, de surveiller en temps réel certaines activités, d'avoir une approche basée sur les risques ou sur la nécessité d'actions de formation ou de sensibilisation.

Pertinence	Avis
★★	Document essentiellement destiné à une sensibilisation. Les recommandations représentent une faible partie du document et n'apportent de nouveautés particulières.

Secteur	
Énergie	☑
Nucléaire	☑
Santé	☑
Aérien	☑
Industrie	☑
Eau / Assainissement	☑

Populations visées	
DSI	☑
RSSI	☑
Constructeurs	☐
Intégrateurs Maintenance	☑
Opérateurs sur site	☑
Auditeurs	☐

Typologie Réseau	
Embarqué	☐
Site	☐
Étendu	☐

Chimie / Pharmacie	☑
Autre / Transverse	☑

Autres	☑

Titre	*Attack Methodology Analysis: Emerging Trends in Computer-Based Attack Methodologies and Their Applicability to Control System Networks*

Date de publication	2005	Éditeur	US-CERT Control Systems Security Center	Volume (pages)	30	Accès	gratuit

Synthèse	Démarche itérative d'analyse d'évaluation des menaces basée sur l'expérience et la veille des failles

Synthèse

Processus d'évaluation des vulnérabilités proposant une approche mixant une démarche type Analyse des menaces associée à une étude de veille sur les failles découvertes par les Hackers ou les recherches au niveau des constructeurs. Surtout si le système est basé sur un nombre de produit COTS important.

C'est une démarche qui se veut complémentaire et surtout associée au cycle opérationnel de la mise en œuvre des actions de sécurisation (plan d'action des mesures de défense palliative et préventive).

Un point intéressant concerne la vision la définition d'un profil de « Chercheur en sécurité », personne dont la responsabilité est d'investiguer sur les nouvelles failles et vulnérabilités issues du monde IT, et de se comporter comme un « White Hats » afin d'évaluer si cela est applicable à son système. La problématique est que le maintien au niveau opérationnel du plan d'action de sécurisation est qu'une fois les études, le plan d'actions et les actions prioritaires mises en place doit se faire durant toute la durée du cycle de vie du système. Et ce n'est pas le RSSI qui peut faire cette démarche d'analyse continue et de veille (.qui intègre souvent des aspects très techniques).

Pertinence	Avis
★	À garder uniquement comme document de veille pour minimiser les vulnérabilités de son système de façon opérationnelle.

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☑
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☐
RSSI	☐
Constructeurs	☐
Intégrateurs Maintenance	☑
Opérateurs sur site	☐
Auditeurs	☐
Autres	☑

Typologie Réseau	
Embarqué	☐
Site	☑
Étendu	☐

Titre	*Process Control Domain – Security Requirements for vendors*

Date de publication	10/2010	Éditeur	WIB	Volume (pages)	52	Accès	gratuit

Synthèse	Document produit par le groupement « International Instrument Users' Associtations – EWE (EI, WIB, EXERA) afin d'améliorer la sécurité des installations livrées aux utilisateurs finaux par les intégrateurs et équipementiers.

Synthèse

Ce document a pour objectif de fournir des exigences de sécurité informatique pour les intégrateurs, équipementiers, mainteneurs de Systèmes de Contrôle Industriels. Elles s'appliquent aux services / solutions / équipements fournis et sont découpées en 3 niveaux (Bronze/Argent/Or) pouvant être assimilés à des niveaux de maturité.

La structuration des exigences est faite comme suit :

- 4 catégories d'exigences de sécurité : 1/Organisation, 2/Construction, 3/Livraison et recette de l'installation, 4/Maintenance
- 35 objectifs de sécurité (PA)
- 127sous objectifs de sécurité (BP)
- 272 exigences de sécurité (Bronze 148/272 – Argent 218/272 – Or 272/272)

Le document est repris dans le cadre des travaux de l'IEC avec la référence IEC 62443-2-4 [*Certification of IACS supplier policies and practices*].

Une certification existe [Wurldtech Achilles] pour les produits et les solutions.

Pertinence	Avis
★★★★	Ce document est un incontournable pour les utilisateurs finaux qui veulent adjoindre une annexe de sécurité au contrat lorsqu'une nouvelle installation est construite. Le niveau exigé sera en fonction des enjeux de sécurité de l'installation. Le document gagnerait en lisibilité avec une meilleure explication sur la façon de l'utiliser.

Secteur	
Énergie	☐
Nucléaire	☐
Santé	☐
Aérien	☐
Industrie	☐
Eau / Assainissement	☐
Chimie / Pharmacie	☐
Autre / Transverse	☑

Populations visées	
DSI	☑
RSSI	☑
Constructeurs	☑
Intégrateurs Maintenance	☑
Opérateurs sur site	☐
Auditeurs	☑
Autres	☐

Typologie Réseau	
Embarqué	☑
Site	☑
Étendu	☑

III. Documents non analysés

Les documents suivants ont été identifiés mais n'ont pas fait l'objet d'une fiche de lecture :

Fiche de Lecture	Éditeur
Guidance for Addressing Cyber Security in the Chemical Industry	ACC
Making Strides to Improve Cyber Security in the Chemical Sector	ACC
X60-500	AFNOR
AGA Report No. 12, Part 1	AGA
ATA Spec 42	ATA
Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software	CDRH
Rappport Energies Carbones (Partie Smartgrid)	DGEC (Direction Générale de l'Énergie et du Climat)
Cyber Security for Control Systems	DHS
CSSA	IACRB
IAONA Handbook - Network Security	IAONA
IEC 60300 series (FMDS/RAMS)	IEC
IEC 60812 (AMDE/FMEA)	IEC
IEC 61025 (AAP/FTA)	IEC
IEC 61882 (HAZOP)	IEC
IEC 80001-1	IEC
IEEE P1686	IEEE
EDSA (ISA Secure)	ISCI
NSTB - Study of Security Attributes of Smart Grid Systems	INL
NTSB Assessment	INL
NSTB series	INL
Vulnerability Analysis	INL
Cyber Attack Task Force	NERC
Cyber Security Maturity	NERC
FDPP	NIST
Security Profile Specification	NIST
OLF Guideline N°104	SINTEF

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