Maîtriser la SSI pour les systèmes industriels

La cybersécurité des systèmes industriels

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Table des matières

AVANT-PROPOS

Alors qu'elle faisait, il y a encore peu, figure de science réservée à quelques experts, la sécurité des systèmes d'information a émergé ces dernières années vers une prise de conscience générale. Le Livre blanc sur la défense et la sécurité nationale établissait en 2008 que la cybersécurité était un enjeu majeur des quinze années à venir, et mettait déjà en exergue l'impérieuse nécessité de protéger les systèmes d'importance vitale.

Depuis le Livre blanc, une prise de conscience a bien eu lieu, même si elle s'est faite à marche forcée, au rythme des attaques et des incidents subis par les pays les plus développés. Indisponibilité massive du réseau, attaques contre des systèmes d'information gouvernementaux, espionnage d'entreprises stratégiques, opérations de déstabilisation et pannes en tous genres ont malheureusement occupé l'actualité des trois dernières années.

Les systèmes industriels, même lorsqu'ils ne sont pas connectés à Internet, sont exposés à ces risques. Le ver *Stuxnet*, apparu en 2010, est la preuve tangible que nos pires craintes d'attaques sur des installations sensibles peuvent se réaliser. En 2009 un adolescent ingénieux et inconscient a fait dérailler via Internet un tramway en Pologne, démontrant la vulnérabilité du système d'aiguillage. On pourrait également parler de rupture de pipeline ou encore de pollution des eaux... Ce ne sont malheureusement pas les exemples qui manquent.

Les systèmes industriels sont donc tout autant concernés, et probablement même davantage, que les autres systèmes d'information par les enjeux de la cybersécurité.

Le défi est là : comme l'ensemble de la société, les industries ont bien souvent intégré le numérique au fil de l'eau et sans stratégie initiale, des systèmes hétérogènes s'interconnectant avec comme soucis majeurs la productivité, l'efficacité et la sûreté – mais rarement la sécurité…

Faut-il relever ce défi ? La question ne se pose pas tant les enjeux sont considérables ! Ce serait comme se demander si on peut se passer de contrôle d'accès physique aux installations sensibles, ou de mesures sanitaires pour protéger ses salariés, les citoyens et l'environnement.

Les industries ont un atout pour la sécurité de leurs systèmes d'information : elles ont une forte culture de la sûreté de fonctionnement de leurs installations, et disposent le plus souvent en interne de compétences en matière de cybersécurité pour leurs systèmes bureautiques. Il faut désormais que ces deux cultures se rencontrent et que les forces s'unissent pour protéger convenablement les systèmes industriels.

Il revient aux directions générales d'en prendre la décision, de mandater formellement un coordinateur SSI pour renforcer la sécurité des systèmes industriels et de lui en donner les moyens matériels, financiers, organisationnels et humains.

Le guide sur la cybersécurité des systèmes industriels publié par l'Agence nationale de la sécurité des systèmes d'information est fait pour accompagner les entreprises dans cette démarche. Il vous est présenté ici dans sa première version publique. Il est destiné à évoluer avec les usages, mais aussi avec vos contributions et retours d'expérience.

Il s'accompagne d'un cas pratique destiné à illustrer des situations présentant des risques pour les entreprises et à en exposer leur traitement.

Enfin, ce guide ne s'adresse pas uniquement aux industries ; son contenu s'applique également – sans que cette liste soit exhaustive – aux *data centers*, aux *smartgrids*, aux systèmes de

gestion technique des bâtiments (GTB), de gestion technique centralisée (GTC), mais aussi à de nombreux systèmes embarqués.

Les publications de l'ANSSI sont diffusées sur son site Internet :

http://www.ssi.gouv.fr/publications/

Toutes remarques sur ce guide peuvent être adressées à : systemes_industriels@ssi.gouv.fr

OBJECTIFS DU GUIDE

Ce guide s'attache à étudier la sécurité des systèmes d'information industriels. Bien que spécifiques à chaque installation, ils se composent le plus souvent des éléments suivants :

- automates Programmables Industriels (API ou PLC) ;
- systèmes Numériques de Contrôle-Commande (SNCC) ;
- systèmes Instrumentés de Sécurité (SIS)[1] ;
- capteurs et actionneurs (intelligents ou non) ;
- bus de terrain ;
- logiciels de supervision et de contrôle : SCADA ;
- logiciels de gestion de production assistée par ordinateur (GPAO, MES) ;
- logiciels d'ingénierie et de maintenance ;
- systèmes embarqués.

Les systèmes industriels utilisent aujourd'hui abondamment les technologies de l'information alors qu'ils n'ont pas été conçus pour faire face aux menaces qu'elles introduisent. Les exemples de publication de vulnérabilités des systèmes industriels sont aujourd'hui nombreux (protocoles Modbus et OPC par exemple).

C'est pourquoi il est nécessaire de les intégrer dans la réflexion générale sur la sécurité des systèmes d'information de l'entreprise[2].

L'objectif de ce guide n'est pas de dresser un inventaire exhaustif de recommandations ni d'énumérer l'ensemble des composants d'un système industriel. Il propose une démarche de sensibilisation et de mise en œuvre de bonnes pratiques pour accompagner les entreprises dans le déploiement de la sécurité.

Il n'existe pas de solution idéale ou « passe-partout ». L'annexe B présente des bonnes pratiques possibles. Chaque installation présente des particularités et des risques propres qu'il convient d'analyser pour déployer des solutions adaptées en limitant les impacts sur l'activité métier de l'entreprise.

La sécurisation d'une installation engendre des coûts, bien souvent difficiles à estimer. Les gains apportés le sont également. Néanmoins, ce processus de sécurisation protège les investissements et la production de l'entreprise. C'est pourquoi, il est important de définir les bons objectifs et de les adapter aux besoins. Paradoxalement, la « sur-sécurité » peut provoquer des effets contraires à ceux recherchés et nuire aux performances industrielles.

Les sigles et acronymes utilisés dans le document sont reprise en annexe C.

1 Le terme sécurité désigne ici la sécurité des biens et des personnes. Certains domaines parlent alors de sûreté.

2 Le système d'information d'entreprise regroupe l'ensemble des systèmes d'information d'une entreprise, c'est à dire les systèmes d'information de gestion (systèmes d'information destinés aux services et applications de bureautique, de gestion des ressources humaines, de relations clients ou encore de gestion intégrée) et industriels.

1 - CONTEXTE ET ENJEUX DE LA CYBERSÉCURITÉ DES SYSTÈMES INSDUSTRIELS

1.1 - Mythes et réalités des SI industriels

1.1.1 - Réalités des systèmes d'information de gestion et des systèmes d'information industriels

Bien qu'utilisant de plus en plus des technologies standardisées de l'informatique « classique » ou « conventionnelle » (IT), les systèmes industriels présentent des spécificités propres aux contextes dans lesquels ils sont utilisés. Ils se différencient des systèmes d'information de gestion par le fait qu'ils pilotent des installations physiques (unités et chaînes de production, unités de distribution d'eau, d'énergie, infrastructures routières, ferroviaires…) ; certains assurent en outre des fonctions de protection des biens et des personnes ou de l'environnement.

	Systèmes d'information « de gestion »	Systèmes d'information industriels
Objectif des systèmes	traiter des données	piloter des installations (physique, concret), réguler des procédés, acquérir et traiter des données
Aspects Fonctionnels	contraintes métier et contraintes de confidentialité	contraintes métier et contraintes « temps réel », contraintes de sûreté de fonctionnement (SdF) , disponibilité 24/7
Culture des intervenants	informaticiens	automaticiens, instrumentistes électrotechniciens, spécialistes en génie du procédé
Environnement physique	salle serveur climatisée, bureau voire domicile	ateliers de production : poussière, température, vibrations, électromagnétisme, produits nocifs à proximité, environnement extérieur, etc.
Localisation géographique	majoritairement dans des locaux fermés (bureau, domicile dans le cas du télétravail)	dans des entrepôts, des usines, sur la voie publique, dans la campagne (stations de pompage, sous-stations électriques, etc.), des lieux isolés, en mer, dans l'air et dans l'espace
Durée de vie	environ 5 ans	plus de 10 ans (parfois 30 ou 40 ans)
Gestion des incidents	analyse post incident	la multitude de paramètres et la complexité de l'environnement limite la reproductibilité de l'incident
Composants	des systèmes standards ; des systèmes « durcis » face aux attaques informatiques	des systèmes temps réel et robustes par rapport aux conditions difficiles des milieux industriels ; des systèmes sur E^2PROM, sans disque dur

	Systèmes d'information « de gestion »	Systèmes d'information industriels
Hétérogénéité des composants	la compatibilité des composants est une exigence technique (homogénéité et interopérabilité).	la grande durée de vie des installations conduit à une « superposition » des vagues technologiques successives sur un même site entrainant un phénomène d'obsolescence des matériels et logiciels.

1.1.2 - Quelques mythes concernant les systèmes d'information industriels

Il existe un certain nombre de mythes relatifs aux systèmes d'information industriels. Les plus communément admis sont examinés ici.

Le mythe	La réalité
« Mes réseaux industriels sont isolés, je suis protégé. »	Les systèmes d'information industriels sont souvent connectés aux réseaux de gestion et parfois directement à Internet. Les clés USB et les consoles de maintenance sont par ailleurs des vecteurs majeurs de propagation de virus y compris sur des systèmes isolés. Les besoins croissants de remontée de données vers le SI de gestion rend, à terme, l'isolation des réseaux industriels utopique.
« J'utilise des protocoles et bases de données propriétaires, je suis protégé. »	Même les solutions propriétaires comportent des composants standards, pour des raisons d'interopérabilité (avec le système d'exploitation par exemple) et de moindre coût. Les solutions propriétaires sont suceptibles d'être vulnérables car elles peuvent n'avoir fait l'objet d'aucune analyse de sécurité.
« L'intégration des mécanismes de sécurité (chiffrement, filtrage, authentification) est incompatible avec les contraintes de temps de réponse exigées. »	Les performances des composants ne sont plus un frein au déploiement de fonctions de sécurité. En revanche, les difficultés existent pour les systèmes « temps réel ».
« La SSI est incompatible avec la Sûreté de fonctionnement (SdF). »	Au contraire la SSI et la SdF se rejoignent sur de nombreux points, voir §2.3.3
« Les mesures de SdF comme la redondance hétérogène protègent des attaques en disponibilité. »	Ce principe est de moins en mois employé car très coûteux. De plus des produits de constructeurs différents s'appuient parfois sur les mêmes technologies et intègrent parfois les mêmes composants matériels et logiciels. Ils contiennent donc dans ce cas des vulnérabilités identiques.

Le mythe	La réalité
« La SSI coûte cher. »	La SSI doit être proportionnée aux enjeux. Elle coûtera d'autant moins cher si elle est prise en compte intelligemment dans les phases amont des projets. Son coût doit en théorie rester inférieur à l'impact maximal d'une attaque, mais il est exact qu'il n'existe pas de mode de calcul de son retour sur investissement (ROI).
« Une attaque du SI Industriel aura toujours moins d'impact qu'un incident physique (vol de câbles, incendie,…), ou terroriste (explosion d'un réservoir de stockage de pétrole dans une raffinerie par exemple). »	Une attaque peut créer un dysfonctionnement global des installations plus difficile à identifier et plus pernicieux (sabotage industriel, ralentissement de la production) qu'une attaque physique pouvant entrainer un temps de rétablissement très long. Les dysfonctionnements provoqués peuvent devenir un facteur aggravant et provoquer une catastrophe industrielle, humaine ou écologique (ex. inhibition d'alarme de surveillance de produits dangereux sur un site SEVESO).
« La SSI m'empêchera de travailler comme je veux. »	La SSI doit être centrée sur les enjeux critiques. Elle n'a pas pour objet de bloquer des comportements utiles, mais de prévenir les comportements dangereux (ce qui suppose de les identifier au préalable). La SSI impose parfois de formaliser des mesures de contournement des modes nominaux de fonctionnement (des modes dégradés d'opérations).

1.2 - Les enjeux de la cybersécurité des systèmes industriels

1.2.1 - Généralités sur les attaques

On distingue plusieurs types d'attaques :

- **les attaques ciblées**, à objectif par exemple idéologique ou vénal, engagées par une personne ou un groupe de personnes contre une organisation dans le but de nuire, en perturbant ces processus, voire en provoquant des dégâts matériels. Les attaquants sont des personnes organisées disposant de moyens pour atteindre leurs objectifs. Des officines proposent sur Internet des services de cyber-attaque, ou publient des outils clés en main pour mener des attaques (« *packages* d'exploits »[3]) ;
- **les attaques « challenge »** dont l'objectif est de démontrer une capacité technique à s'introduire dans des systèmes réputés sécurisés, mais dont les effets en termes de production, de sécurité des biens et des personnes ou d'image de marque sont réels pour les victimes ;
- **certaines attaques non ciblées**, cherchant à impacter le plus de monde possible, peuvent créer des dommages significatifs dans les entreprises (virus, campagnes de spam par exemple).

1.2.2 - Les négligences humaines

Les négligences ne sont pas le fruit d'actions volontaires et malveillantes, mais leurs effets peuvent être similaires à ceux des attaques. Elles peuvent créer des vulnérabilités difficiles à détecter, qui pourront être exploitées par des attaquants ou simplement affecter la disponibilité des systèmes.

Par exemple, la modification involontaire de réglages d'asservissements, ou la modification d'une alarme peut avoir des conséquences désastreuses sur la qualité des produits, services délivrés, l'environnement, la santé ou la sécurité des personnes.

L'utilisation d'une clé USB – qu'elle soit personnelle ou non – pour transférer des données entre des systèmes industriels isolés, peut mener à une indisponibilité des systèmes si cette clé est porteuse de virus.

Dans ces deux cas très concrets issus d'expériences vécues, les intervenants n'ont pas eu la volonté de nuire. Les impacts sur les installations ont été pourtant bien réels.

Ces négligences peuvent avoir pour cause un manque de formation du personnel et d'information sur les enjeux.

3 Des « *packages* d'exploit » sont officiellement commercialisés comme outils SSI dans le but de détecter des vulnérabilités lors d'audits par exemple. Ces « *packages* » peuvent bien évidement aussi être utilisés par des personnes malveillantes.

1.2.3 - Vulnérabilités des systèmes d'information industriels

Les vulnérabilités peuvent être d'origines multiples et l'objet de ce guide n'est pas de les répertorier. Quelques exemples de vulnérabilités fréquemment rencontrées sur les installations industrielles sont listées en annexe A.

Les besoins croissants de consolidation des données de l'entreprise, de leur accès en temps réel depuis n'importe quel point de la planète, la réduction des coûts de développement et de possession ainsi que les contraintes de planning ont précipité la convergence du domaine de l'informatique industrielle et de l'informatique de gestion.

Les réseaux Ethernet sont désormais employés dans les systèmes industriels jusque dans le domaine des bus de terrain. Ils offrent de nouvelles fonctionnalités comme la mutualisation des infrastructures réseau et la possibilité d'utiliser les couches IP (pour la télémaintenance par exemple).

Les outils de développement, de maintenance et télémaintenance sont aujourd'hui entièrement développés sur des briques génériques issues de l'informatique de gestion (plateforme .Net, Java par exemple).

La standardisation des systèmes et les nouvelles fonctionnalités ont apporté aux systèmes industriels les vulnérabilités du monde de l'informatique de gestion. Les systèmes dits propriétaires, souvent pauvres en mécanismes de sécurité, ne sont pas pour autant à l'abri de vulnérabilités pouvant être exploitées par des attaquants motivés et organisés.

Alors que le monde de l'informatique de gestion parvient à corriger régulièrement les vulnérabilités, notamment par l'application de correctifs publiés par les constructeurs et les éditeurs de logiciels, le monde industriel, de par **ses contraintes de disponibilité et de sûreté**, ne peut pas adopter les mêmes protections. Cette différence de réactivité face aux vulnérabilités publiques est un des principaux risques des systèmes d'information industriels.

Le manque de formation des intervenants, les différences de cultures ou le manque de prise de conscience des risques liés à la SSI peuvent constituer une autre vulnérabilité majeure.

1.2.4 - Les impacts potentiels sur les systèmes industriels

De nombreux incidents sur les systèmes industriels surviennent chaque année, mais peu sont médiatisés, comme l'incident de centrale nucléaire au Royaume-Uni lié à *Conficker*, l'incident lié au ver *Slammer* aux USA, ou en 2010 la propagation généralisée du ver *Stuxnet*[4]. Leurs impacts peuvent être analysés selon différents axes, présentés ci-dessous :

4 *Stuxnet* est un code malveillant visant les systèmes industriels. Il exploite de multiples vulnérabilités présentent dans le système d'exploitation *Microsoft Windows* et le progiciel de *SCADA WinCC* de *Siemens*. Le code malveillant modifie le programme exécuté par certains automates industriels de la gamme *Simatic S7* de *Siemens*. Les modifications réalisées peuvent conduire au ralentissement de la production mais aussi à la destruction physique des installations pilotées par l'automate.

Dommages matériels / corporels	La modification des configurations nominales des installations peut provoquer des dégradations physiques avec le plus souvent des conséquences matérielles – mais parfois aussi humaines.
Perte de chiffre d'affaires	L'interruption de la production génère des manques à gagner importants. La modification de paramètres de fabrication conduisant à des produits non conformes génère des coûts importants.
Impact sur l'environnement	La défaillance du système suite à une prise de contrôle malveillante peut générer un dysfonctionnement des installations (ouverture de vannes de produits polluants) et provoquer une pollution du site et de son environnement. Un tel incident s'est produit en Australie ces dernières années.
Vol de données	Perte de secret de fabrication, contrefaçons, avantage pour la concurrence.
Responsabilité civile / pénale - Image et notoriété	L'indisponibilité du service comme la rupture de distribution d'électricité ou d'eau, ainsi que la fourniture de produits défectueux mettant en danger le consommateur peuvent aboutir à des poursuites pour les dommages occasionnés ou simplement dégrader l'image de l'entreprise (la satisfaction du client et sa confiance).

Ces différents impacts génèrent des pertes financières liées à la perte d'activité ou au versement de compensations aux victimes potentielles (clients, particuliers, collectivités territoriales, associations, État voire Union Européenne) ainsi qu'une atteinte à l'image de l'entreprise.

2 - MÉTHODE DE DEPLOIEMENT DE LA SSI

2.1 - Rappel du rôle de la SSI

L'objectif de la SSI est d'étudier les vulnérabilités des systèmes (matériel, logiciel, procédures, aspects humains) afin de déployer des mesures pour les limiter et permettre d'assurer la continuité des fonctions métier à un niveau acceptable.

Souvent perçue comme une contrainte, une SSI bien pensée contribue au contraire à améliorer la robustesse des installations et la productivité des entreprises.

Comme l'indique le Référentiel général de sécurité (RGS)[5], elle repose sur quatre piliers indispensables au bon fonctionnement des systèmes industriels :

- la **disponibilité** : dans un contexte de forte productivité, la dégradation de la disponibilité se traduit directement en perte financière et insatisfaction des clients (retards de livraison, augmentation des coûts de production, arrêts de production…) ;
- l'**intégrité** : son respect certifie que les produits et services fournis sont conformes aux exigences des clients ou aux exigences réglementaires. Pour les systèmes instrumentés de sécurité assurant la protection des biens et des personnes (commandes d'arrêt d'urgence par exemple), elle est même impérative.
  L'intégrité concerne l'ensemble des composants des systèmes industriels : les programmes des automates, des données échangées entre les installations, les bases de données des logiciels de SCADA par exemple ;
- la **confidentialité** : elle est parfois minimisée, mais une divulgation du patrimoine informationnel de l'entreprise peut avoir un impact bien réel sur ses profits et son avenir (perte de clients). Les systèmes industriels contiennent des paramètres et des données sensibles comme des recettes de fabrication, des quantités de produits utilisés, des plans d'installations, des plans de maintenance, des programmes PLC ou encore des listes d'adresses d'équipements. Ceux-ci peuvent être exploités par des concurrents ou des groupes malveillants pour diriger des attaques ciblées ou simplement collecter des données permettant de copier le savoir-faire de l'entreprise ;
- la **traçabilité** : il s'agit d'une exigence réglementaire dans de nombreux secteurs d'activité (agro-alimentaire, transport, nucléaire…). L'impossibilité d'apporter la preuve de la traçabilité des opérations réalisées, des matières utilisées ainsi que de leur origine, et le non-respect des exigences réglementaires peuvent conduire à des poursuites judiciaires pour l'entreprise.

2.2 - Les grands principes de la SSI

Le déploiement puis la gestion de la sécurité devraient être organisés afin de protéger l'installation des conséquences d'incidents de sécurité. Les activités peuvent être organisées selon les phases présentées ci-dessus. Il s'agit d'un processus continu, demandant des efforts permanents.

5 Voir sur le site de l'ANSSI : http://www.ssi.gouv.fr/rgs/

2.2.1 - Sensibilisation des personnels

Une partie importante des incidents est liée à une méconnaissance par les intervenants des risques sur l'installation. Leur sensibilisation aux règles d'« hygiène informatique » contribue à réduire les vulnérabilités et les opportunités d'attaques[6]. La sensibilisation doit être régulière car les risques évoluent en permanence.

2.2.2 - Cartographie des installations et analyse de risque

Il est illusoire de vouloir plaquer une démarche sécurité sur un SI industriel sans une compréhension préalable du besoin métier qu'il sert. Il est donc important de déterminer :

- les objectifs métier (production, distribution, protection des biens et des personnes…) et les services assurés ;
- les impacts en cas d'interruption de service ;
- les fonctions indispensables à l'atteinte des objectifs, et en particulier :
  - leurs niveaux d'implication et de criticité dans la réalisation des services,
  - systèmes qui les portent,
  - si ces systèmes sont centralisés, distribués, accessibles à distance, etc. ;

Un inventaire des installations matérielles, des systèmes et des applications critiques est un pré-requis incontournable à la mise en place de la sécurité des SI dans les installations industrielles. Cet inventaire est la première étape de l'analyse des risques, qui permettra de définir les différents niveaux de criticité, de sûreté, de disponibilité ou d'intégrité attendues pour les éléments cartographiés.

Tout projet doit en effet comprendre une analyse de risque afin d'identifier les éléments sensibles du système, leurs besoins et les objectifs de sécurité face aux menaces retenues.

Ces objectifs sont alors déclinés en exigences de sécurité, qui porteront sur le système lui-même (robustesse intrinsèque), sur son environnement de conception, de construction et d'exploitation. Ces exigences sont ensuite traduites en mesures techniques, physiques, et organisationnelles.

Clairement formalisées dans une **cible de sécurité,** elles forment la référence sécurité du système.

Les principes de l'analyse de risque en SSI ne diffèrent pas de ceux de la sûreté de fonctionnement même si les terminologies employées peuvent ne pas être identiques.

Il existe plusieurs méthodes d'analyse de risque. L'ANSSI propose la méthode EBIOS[7].

Les conclusions de l'analyse de risque aboutissent à la définition des mesures de sécurité adéquates, dont les efforts sont proportionnés aux enjeux et adaptés aux besoins réels. Celles-ci peuvent être techniques mais aussi organisationnelles.

6 Voir sur le site de l'ANSSI : http://www.ssi.gouv.fr/fr/bonnes-pratiques/principes-generaux/
7 Voir sur le site de l'ANSSI : http://www.ssi.gouv.fr/ebios/

2.2.3 - Prévention : concept de la défense en profondeur

La défense en profondeur consiste à protéger les installations en les entourant de plusieurs barrières de protection autonomes et successives. Elles peuvent être technologiques, liées à des procédures organisationnelles ou humaines.

Intrinsèquement, les logiciels ou les équipements embarqués contiennent des bogues et des vulnérabilités. Certains sont connus et d'autres sont découverts au fil du temps. Il faut réduire les surfaces exposées.

Adopter une démarche de défense en profondeur permet de se protéger contre des menaces qui ne sont pas encore connues, de diminuer le périmètre sur lequel une menace est exercée ou d'en atténuer l'impact.

Le simple cloisonnement des réseaux par des pare-feux ne suffit pas. D'autres mécanismes doivent l'accompagner et à différents niveaux (contrôle d'accès physique, durcissement des configurations, protection antivirale...).

Sur d'anciennes installations, les mises à jour automatiques peuvent être incompatibles avec les contraintes de disponibilité et les logiciels antivirus peuvent perturber le fonctionnement des applications métier qui n'ont pas été conçues pour cela.

D'autres mécanismes peuvent être déployés comme le durcissement des systèmes d'exploitation et la détection d'intrusion. Les solutions sont multiples. Il convient d'utiliser des barrières adaptées aux installations, qui ne nuisent pas aux objectifs métier, puis d'estimer les impacts résiduels.

Il peut être également utile de consulter les livres blancs et recommandations des équipementiers et consulter les pages Web de l'ANSSI[8] sur le sujet.

La stratégie de défense en profondeur doit intégrer non seulement une démarche de protection préventive, mais aussi des mesures de surveillance, de détection et de réaction.

2.2.4 - Surveillance des installations et détection des incidents

Détecter un incident est une action majeure dont l'importance est souvent sous-estimée.

Dans un environnement industriel, il peut être complexe, voire impossible, de déployer certaines barrières de protection sans impacter les fonctions métier. Les contre-mesures devraient inclure des mécanismes de détection et de surveillance des installations. Leur fonctionnement est transparent et ainsi ne perturbe pas les fonctions métier.

Ces mesures n'empêcheront pas un incident mais permettront de le détecter et d'en limiter autant que possible les effets.
Plus un incident sera détecté tôt, plus il sera possible de mettre en place des mesures pour en réduire et confiner les effets comme par exemple :

- isoler physiquement les installations en cas d'attaque virale pour limiter les risques de propagation ;
- arrêter une installation avant sa dégradation si des données de configuration ne sont

8 Voir sur le site de l'ANSSI : http://www.ssi.gouv.fr

plus intègres, suite à des erreurs ou des modifications intentionnelles (cela permet par exemple d'empêcher la détérioration des équipements qui pourrait être occasionnée par la propagation d'un ver tel que *Stuxnet*).

Enfin la collecte des informations au travers des journaux d'alarmes et d'événements est indispensable aux analyses ultérieures. Ces journaux pourront dans certains cas apporter des éléments utiles et des preuves dans le cadre d'une enquête judiciaire.

2.2.5 - Traitement des incidents, chaîne d'alerte

Un dispositif de détection n'a de sens qu'associé à la mise en place d'une organisation et de procédures pour traiter les incidents. Il convient de déterminer :

- que faire lors de la détection d'un incident ;
- qui alerter ;
- quelles sont les premières mesures à appliquer.

Un processus d'escalade doit être défini pour gérer les incidents au bon niveau de responsabilité, et décider en conséquence :

- s'il faut déclencher un Plan de Reprise d'Activité (PRA) ;
- si une action judiciaire est nécessaire.

Une note de l'ANSSI[9] décrit les bons réflexes en cas d'intrusion sur un système d'information.

La gestion des incidents doit également intégrer une phase d'analyse *post incident* qui permettra d'améliorer l'efficacité des mesures de SSI déployées initialement.

2.2.6 - Veille sur les menaces et les vulnérabilités

La SSI est une action continue nécessitant des efforts permanents.

Se tenir informé de l'évolution des menaces, des vulnérabilités en identifiant les incidents qu'elles favorisent, ainsi que de leurs effets potentiels constitue une mesure fondamentale de défense.

Les sites Internet comme celui du centre opérationnel de l'ANSSI[10] ou les sites des équipementiers sont des sources d'information importantes sur les vulnérabilités identifiées, les éventuels correctifs existants ou les contre-mesures qu'il est possible de mettre en place.

Les mises à jour des micrologiciels (*firmwares*) des PLC et autres équipements, correctifs des systèmes d'exploitation et des applications font l'objet d'alertes et d'avis. Des flux RSS ou Atom permettent souvent d'obtenir l'information rapidement.

Il peut être utile de se rapprocher des équipementiers pour connaître la meilleure façon de se tenir informé. Penser également à demander à ses fournisseurs, au travers des contrats, d'être tenu informé des vulnérabilités. L'activité de veille sera d'autant plus efficace que la cartographie sera exhaustive.

9 Voir sur le site du CERTA : http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html
10 Voir sur le site du CERTA : http://www.certa.ssi.gouv.fr/

2.2.7 - Les plans de reprise et de continuité d'activité (PRA / PCA / DRP)

La sécurité absolue et le risque zéro n'existent pas.

Se préparer à faire face à des événements exceptionnels pour lesquels toutes les mesures précédentes auraient échoué minimisera les impacts et permettra de redémarrer l'activité le plus rapidement possible.

Les Plans de Continuité d'Activité métier de l'entreprise (PCA) doivent donc intégrer les systèmes d'information industriels. Ils incluent la définition des Plan de Reprise d'Activité (PRA), ou *Disaster Recovery Plan* (DRP), qui identifient les moyens et procédures nécessaires pour revenir à une situation nominale le plus rapidement possible, en cas de sinistre ou d'événements exceptionnels. Ils devraient décrire comment reconstruire le système suite à une attaque virale, un incendie, une inondation ou une perte de données.

Le PCA devrait être régulièrement mis à jour, en fonction :

- des évolutions propres de l'infrastructure (maintenance, intégration de nouveaux composants, qui peuvent introduire de nouvelles vulnérabilités) ;
- de l'évolution des menaces.

2.3 - Une approche globale et structurée

La SSI ne se traite pas dans l'urgence, de façon ponctuelle ou isolée. Il s'agit d'une démarche qui se planifie et qui demande la participation de ressources et compétences multiples ainsi qu'un engagement fort au plus haut niveau de la hiérarchie.

2.3.1 - Une volonté à tous les niveaux (engagement de la direction)

Fixer des objectifs adaptés aux enjeux, définir une stratégie, sensibiliser et former les personnels sont autant de tâches qui incombent à la direction. La démarche peut être progressive, réalisée en plusieurs phases dans le temps en adressant les éléments du plus simple au plus complexe, du plus évident ou moins évident mais elle doit être globale. Elle peut s'appuyer sur les standards de la sécurité des systèmes d'information existants, en prenant en compte les contraintes spécifiques aux systèmes industriels.

Les systèmes d'information industriels doivent être intégrés dans les politiques de sécurité des systèmes d'information de l'entreprise, comme tout autre système d'information et ceci, dès l'origine du projet. Les problématiques de sécurité ne sont pas spécifiques à ce domaine, mais la mise en œuvre des solutions demande à ce qu'elles soient ajustées au contexte industriel.

Bien souvent, les organisations ne favorisent pas le rapprochement du monde de l'informatique classique de celui des systèmes industriels. C'est pourquoi le projet de déploiement de la sécurité sur les systèmes d'information industriels ne peut pas réussir sans l'implication du management au plus haut niveau de l'entreprise.

2.3.2 - Prise en compte de la SSI dans les projets

La sécurité du système doit être envisagée dès le début du projet, par l'utilisateur final qui doit exprimer ses besoins.

En phase de spécification :

- définir les moyens de réaliser les opérations de maintenance préventive et curative permettant de maintenir le niveau de SSI dans la durée : modes dégradés par exemple pour réaliser des mises à jour (par exemple figer les sorties automates pendant la mise à jour du *firmware*) ;
- définir la localisation des équipements afin d'assurer leur sécurité physique ;
- prévoir la possibilité de changer les configurations par défaut comme les mots de passe à partir de l'IHM ;
- exiger la non-adhérence des logiciels fournis à une version précise d'une autre brique logicielle (système d'exploitation, système de gestion de bases de données, etc.) ; à défaut, exiger que le fournisseur assure la compatibilité ascendante avec les évolutions des briques adhérentes ;
- intégrer des mécanismes pour faciliter la requalification d'une installation suite à des modifications (ex. simulation de *process*, forçage de valeurs, etc.) ;
- exiger que le logiciels non indispensables à la conduite des installations soient installés sur d'autres postes (des postes bureautique pour lire des fichiers PDF ou remplir des feuilles de calcul par exemple).

En phase de conception :

- réduire les interfaces et la complexité du système afin de limiter l'introduction de vulnérabilités lors de l'implémentation ;
- sélectionner les composants offrant les meilleures caractéristiques pour répondre aux exigences de sécurité (mécanismes d'authentification, ségrégation des droits, etc.) ;
- appliquer le principe du « besoin d'en connaître » ou du « moindre privilège », de la ségrégation des droits, et maintenir un principe d'« accès non accordé si non explicitement autorisé » pour les accès au système ;
- distinguer clairement les profils utilisateur et administrateur ;
- prévoir la gestion des exceptions (débordement de plage de valeurs, erreurs internes des composants…) ;
- prévoir des mécanismes permettant de généraliser les changements sur un ensemble d'équipements (changements de mots de passe par exemple).

En phase d'intégration :

- changer les configurations par défaut (mots de passe par exemple) ;
- supprimer ou désactiver les fonctions non utilisées mais activées par défaut ;
- penser à supprimer les fonctions de débogage comme les traces utilisées pour analyser le comportement des installations.

En phase de test :

- réaliser les tests fonctionnels de sécurité ;
- dérouler les tests aux limites, les tests d'erreur des fonctions métier et vérifier les exceptions ;

- tester des scénarios de menace (tests de pénétration et tentatives de prise de contrôle) ;
- tester les moyens de réaliser les opérations de maintien du niveau de SSI (déploiement de correctifs, analyse de journaux d'événements…) ;
- vérifier les performances du système.

Ces tests se déroulent de façon unitaire lors de la recette usine (*Factory Acceptance Testing* : FAT) puis de façon globale lors de la recette sur site (*Site Acceptance Testing* : SAT).

Il peut être important d'exiger la réalisation, par une équipe indépendante, d'un audit SSI pour vérifier l'adéquation des installations à la cible de sécurité exigée.

Les tests se concluent par une **phase de réception** qui permet :

- d'accepter en connaissance de cause les risques résiduels sur l'installation (principe de l'homologation des systèmes), formalisée par la signature d'un Procès Verbal (PV) de réception ;
- d'effectuer le transfert de propriété et de la responsabilité du système.

Les éléments listés précédemment sont loin d'être exhaustifs et dépendent des solutions envisagées pour chaque installation. Certaines sont construites à partir de « composants sur étagère », d'autres sont des solutions sur mesure utilisant des logiciels développés spécifiquement ou encore des solutions clés en main.

Processus de transfert en exploitation :

L'entreprise en charge de l'exploitation peut ne pas être le propriétaire de l'installation et donc ne pas avoir été impliquée dans le projet de réalisation de l'installation. Cela peut concerner les cas de délégations de service public, de concession d'exploitation ou de contrat d'exploitation avec obligation de résultat par exemple.

Dans ces cas, l'entreprise en charge du futur contrat d'exploitation doit établir un état des lieux exhaustif du niveau de sécurité de l'installation et des moyens disponibles pour le maintenir à un niveau acceptable. Cet état des lieux devra être accepté ou faire l'objet d'une négociation avec l'entreprise adjudicatrice du contrat d'exploitation afin que l'ensemble des parties soit d'accord sur le niveau de SSI de l'installation « telle que construite », ainsi que des moyens actuels qu'elle intègre pour le maintenir à un niveau acceptable. Le guide de l'externalisation[11] publié par l'ANSSI peut apporter des réponses à cette problématique.

Enfin, il est rappelé qu'il est essentiel de changer les mots de passe lors du transfert en exploitation.

2.3.3 - Prise en compte de la SSI dans les AMDEC /HAZOP

Les incidents d'origine SSI peuvent être la cause d'arrêts de production ou de catastrophes industrielles comme l'ont montré les exemples du chapitre 2.2.

L'intégrité d'un programme automate de sécurité, par exemple, est aujourd'hui un enjeu aussi bien du domaine de la SSI que du domaine de la sûreté. Un attaquant ou un virus qui modifie un programme de sécurité concerne les deux domaines. *Stuxnet* a montré que ce type de scénario était parfaitement crédible.

L'absence de SSI ou un niveau de SSI insuffisant peut donc être la cause potentielle de mode

11 Voir sur le site de l'ANSSI : http://www.ssi.gouv.fr/externalisation

de défaillance d'installations industrielles. L'analyse des modes de défaillance est traitée dans les méthodes de sûreté de fonctionnement comme AMDEC[12] ou encore HAZOP[13].

Couvrir l'ensemble des risques impose de traiter conjointement les sujets SSI et sûreté de fonctionnement dans une approche commune.

Par exemple, les causes potentielles d'une montée en température d'une installation au-delà de son seuil nominal peuvent être :

- un problème de mesure lié à la défaillance d'un capteur :
  - une défaillance matérielle du capteur,
  - un mauvais étalonnage du capteur,
  - la **modification des paramètres du capteur, de manière intentionnelle** par une personne non autorisée (prise de contrôle par un attaquant, un virus) ou **suite à une négligence** ;
- un problème lié à une vanne sur le circuit de refroidissement :
  - une défaillance mécanique,
  - une défaillance du servomoteur,
  - **le forçage de la commande de la vanne, de manière intentionnelle** par une personne non autorisée (prise de contrôle par un attaquant, un virus) **ou suite à une négligence**,
  - un problème de réglage du point de consigne de régulation du système de refroidissement,
  - une erreur de saisie d'un opérateur,
  - **un changement du point de consigne par une personne non autorisée.**

Les analyses de type AMDEC, FMEA ou HAZOP sont bien souvent complexes à réaliser et demandent du temps. Impliquer des compétences en informatique de gestion et en SSI dans les équipes réalisant ces travaux sera bien plus efficace qu'un travail autonome et non concerté où chacun dispose de la vision de son sujet, mais pas de la vision d'ensemble.

2.3.4 - Prise en compte de la SSI dans la maintenance

La SSI des installations industrielles doit être prise en compte lors de la rédaction des plans de maintenance. Ces derniers doivent intégrer les opérations nécessaires pour maintenir le niveau de sécurité des systèmes dans la durée :

- définir les opérations de maintenance propres à la SSI qui sont nécessaires au maintien en conditions opérationnelles (MCO) et au maintien en conditions de sécurité (MCS) : en particulier, l'intégration des correctifs proposés par l'équipementier doit être prévue ;
- intégrer dans les opérations de maintenance préventive métier (maintenance électrique, mécanique par exemple) les opérations de SSI qu'il n'est pas possible de réaliser lorsque l'installation est en fonctionnement.

Lorsqu'une chaîne de production est à l'arrêt, par exemple pour une maintenance mécanique ou des contrôles réglementaires, il peut être opportun d'appliquer les correctifs sur les

12 AMDEC : Analyse des Modes de Défaillance, de leurs Effets et de leurs Criticité ou FMECA en anglais (*Failure Modes, Effects and Criticality Analysis*). Outils d'analyse de risque de sureté de fonctionnement et de gestion de la qualité.

13 HAZOP : *HAZard and OPerability study*. Méthode d'analyse des risques utilisée dans le domaine de la sureté de fonctionnement

automates pilotant l'installation dans le cas où des vulnérabilités auraient été identifiées.

Les plans de maintenance des systèmes d'information industriels ne peuvent être dissociés des plans de maintenance des installations qu'ils pilotent. Les opérations de SSI devraient être suivies dans l'outil de gestion de maintenance des installations (GMAO[14]).

2.3.5 - Prise en compte de la SSI dans les achats

Les exigences de sécurité sur le système acheté doivent faire l'objet d'une étude et être clairement formalisées (dans une cible de sécurité ou dans le CCTP[15]) et intégrées dans les dossiers d'appels d'offres comme le sont les exigences fonctionnelles, de performance, de qualité, d'environnement, de sûreté ou encore de respect des réglementations en vigueur.

Elles concernent le système faisant l'objet de la consultation mais aussi la gestion du projet lui-même (formation voire habilitation des installateurs), en incluant les phases opérationnelles et de maintenance. Il convient donc de :

- vérifier dans les réponses à appel d'offres la couverture des exigences sécurité inscrites dans la consultation ;
- établir les clauses concernant la maintenance de l'équipement :
  - demander les plans de maintenance nécessaires pour maintenir l'installation en condition opérationnelle et de sécurité,
  - définir les processus de traitement des incidents et de fourniture de correctifs de sécurité : qui prend l'initiative, qui déploie, sous quels délais, qui fait les tests de bon fonctionnement et comment, etc. ;
- préciser les clauses concernant les conditions d'intervention des sous-traitants :
  - préciser les conditions de support et d'intervention sur site : la télémaintenance est-elle acceptée (si oui à quelle condition) ? le prestataire peut-il partir du site avec un équipement défectueux et sa configuration ? les intervenants peuvent-ils utiliser leurs propres outils ?
  - les intervenants doivent-ils disposer de qualifications particulières ?
- déterminer les clauses juridiques à intégrer dans les contrats ;
- définir les conditions de propriété des codes sources et des paramètres :
  - qui est propriétaire des différents codes source ?
  - les sous-traitants peuvent-ils disposer des codes source en dehors du site ?
  - définir le statut des paramétrages spécifiques à l'installation ; qui les maintient ? qui les sauvegarde ? qui est autorisé à les modifier ?

Pour plus d'information sur les recommandations en matière de sous-traitance, consultez le guide de l'externalisation publié par l'ANSSI[16].

14 GMAO : Gestion de la Maintenance Assistée par Ordinateur
15 CCTP : Cahier des Clauses Techniques Particulières
16 Voir sur le site de l'ANSSI : http://www.ssi.gouv.fr/externalisation

ANNEXE A : VULNÉRABILITÉS FRÉQUEMMENT RENCONTRÉES

Architecture et cartographie du SI :

- pas d'inventaire du parc de SI industriel, pas d'inventaire des équipements, absence de vision des « générations » technologiques qui cohabitent et de leurs vulnérabilités intrinsèques ;
- absence de plan de continuité ou de plan de reprise (DRP), pas d'analyse de risque sur le SI industriel.

Mesures techniques préventives :

- mot de passe par défaut pour les comptes de services, les bases de données, les applicatifs, les accès en mode console (PLC, passerelles, équipements réseau), usage de communautés SNMP ;
- mot de passe en clair dans les codes sources, dans les procédures d'exploitation et les données sauvegardées ;
- faiblesse de gestion des accès utilisateurs : les comptes restent actifs lorsque les intervenants quittent le site, existence de comptes génériques ;
- emploi de comptes avec des profils « administrateur » dans les applications, alors que des droits « utilisateur » suffisent ;
- partage de fichier sur le réseau en accès complet alors qu'un accès en lecture seule suffit ;
- accès en lecture (ou écriture) à des fichiers configurations via FTP ou TFTP ;
- outils de prise de main à distance non sécurisés (*VNC*, *Dameware*...) :
  - services activés sans utilité fonctionnelle,
  - emploi de services / protocoles non sécurisés : TFTP, HTTP, Telnet, SNMP v1 ou v2,
  - modification en ligne des programmes automates autorisée sans contrôle ;
- rechargement de la configuration au redémarrage *via* clé USB ou MMC[17].

Maintenir la sécurité dans la durée :

- absence de sauvegarde des données, des codes sources, et de la configuration des équipements ;
- absence de politique de gestion des médias amovibles (ex. : blocage des ports USB) alors que les clés USB non maîtrisées sont autorisées ;
- peu de supervision, peu de détection d'incidents ;
- absence de mise à jour (correctifs) des systèmes d'exploitation, des applications, des *firmwares* (pour les automates, capteurs/actionneurs intelligents…) ;
- absence de mécanisme de signature des *firmwares* (possibilité pour un attaquant de diffuser une mise à jour piégée).

17 MMC : *Multi Media Card*.

ANNEXE B : BONNES PRATIQUES (CHECK-LIST)

De nombreuses bonnes pratiques sont similaires à celles de l'informatique de gestion, mais leur mise en œuvre est à adapter aux contraintes du domaine industriel. Elles ne sont pas classées par ordre de priorité et leur facilité de déploiement est propre à chaque installation.

BP01 : Contrôle d'accès physique aux équipements et aux bus de terrain

Motivation	Maîtriser les points d'accès physique qui permettraient de s'introduire dans le système.
Méthode	Identifier qui a besoin d'accéder aux équipements, pourquoi et à quelle fréquence. Installer les serveurs dans des locaux fermés sous contrôle d'accès (si possible dans les salles informatiques). Placer les unités centrales des stations, les équipements réseaux industriels et les automates dans des armoires fermées à clé. Protéger l'accès au câble réseau et aux prises de connexion.
Périmètre	Stations, serveurs, équipements réseau, automates, capteurs/actionneurs, écrans tactiles.
Contraintes	Taille des installations - protection générale du site Maintenir l'autorisation d'accès en cas d'urgence.
Moyens de gestion des contraintes	Remonter un contact d'ouverture de la porte pour générer une alarme sur le SCADA. Procédure de type « bris de glace »

BP02 : Cloisonnement des réseaux

Motivation	Limiter la propagation des attaques et confiner les vulnérabilités.
Méthode	Établir une cartographie des flux. Séparer les réseaux par des équipements dédiés ou des VLAN. Filtrer les flux au moyen de pare-feu. Tracer les flux rejetés et les analyser.
Périmètre	Réseau SCADA, réseau d'automates, réseau de développement...
Contraintes	Contrainte de temps réel sur les réseaux procédé.
Moyens de gestion des contraintes	Le filtrage s'applique en amont de ces réseaux. L'accès physique au réseau procédé est limité et contrôlé.

BP03: Gestion des médias amovibles

Motivation	Réduire les risques d'attaque de virus véhiculés à partir de médias amovibles (clés USB, DVD, etc.) qui sont des vecteurs majeurs de propagation.
Méthode	Définir une politique pour l'utilisation de ce type de média. Activer les politiques de restrictions logicielles. Désactiver l'utilisation de ces médias et utiliser des sas (voir ci-dessous) pour échanger des données entre les réseaux si besoin. Désactiver les ports USB sur les systèmes, restreindre les fonctionnalités (voir La cybersécurité des systèmes industriels – Cas pratique, annexe C).
Périmètre	Stations, serveurs, console de programmation et de maintenance, écrans tactiles.
Contraintes	Il peut être nécessaire d'échanger des données entre des réseaux qui ne sont pas interconnectés.
Moyens de gestion des contraintes	L'installation de sas, machines dédiées aux transferts, peut être un moyen de répondre aux besoins utilisateur. Ces machines doivent être renforcées, régulièrement mises à jour, équipées de logiciel antivirus et faire l'objet d'une surveillance forte.

BP04 : Gestion des comptes (accès logique, authentification)

Motivation	Se protéger des accès illicites.
Méthode	Définir une politique de gestion des comptes utilisateur et des comptes d'application. Ne pas laisser les comptes par défaut sur les équipements et applications (admin/admin). Privilégier des mots de passe robustes (voir http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/ rubrique *Sécurité du poste de travail*-> calculer la « force » d'un mot de passe et la note d'information du CERTA sur les mots de passe). Ne pas oublier de changer régulièrement les mots de passe.
Périmètre	Les systèmes d'exploitation, les bases de données, les applications SCADA, les programmes automates, les équipements de réseau, les capteurs et actionneurs
Contraintes	Comptes « génériques », souvent historiques ; Accès « d'urgence ».
Moyens de gestion des contraintes	Tracer les actions réalisées avec ces *logins* pour détecter d'éventuelles dérives et comportements anormaux. Utiliser des procédures organisationnelles strictes (cahier de suivi) pour pouvoir déterminer à chaque instant l'identité des agents utilisant un compte générique.

BP05 : Durcissement des configurations

Motivation	Limiter la surface d'exposition aux attaques.
Méthode	N'installer que les logiciels nécessaires. Pas d'outils de développement sur des serveurs de production ou stations opérateur. N'installer ou n'activer que les protocoles et services nécessaires. Qui n'a jamais dit « Dans le doute je coche toutes les options d'installation » ? Éviter les choix proposés par défaut. Désactiver systématiquement les protocoles et fonctionnalités vulnérables et non sécurisés (serveur Web, NetBios, FTP,...). En particulier, désactiver les protocoles de découverte automatique d'équipements ou de topologie (LLDP) après avoir vérifié qu'ils ne sont pas utilisés par des applications. Désactiver les modes de configuration et de programmation à distance sur les installations critiques. Sur les automates, ce mode se configure parfois par un commutateur physique sur le CPU.
Périmètre	Systèmes d'exploitation, applications SCADA, automates, équipements réseau, capteurs/actionneurs intelligents, écrans tactiles
Contraintes	Impacts des modifications sur le fonctionnement des applications
Moyens de gestion des contraintes	Si malgré tout, certaines fonctionnalités non sécurisées sont nécessaires une analyse détaillée et documentée (traitement d'exception par exemple) doit apporter une justification et des contre-mesures doivent être mises en place.

BP06 : Gestion des journaux d'événements et d'alarmes

Motivation	Surveiller les systèmes / Détecter les intrusions / Traçer les actions et les interventions de maintenance (ou télémaintenance)
Méthode	Activer les fonctions de traçabilité si les équipements et logiciels le permettent (syslog, SNMP V3, « Windows Event », fichier texte, etc. Sélectionner les événements pertinents et organiser le stockage des événements (volumétrie, durée de conservation). Centraliser les journaux et générer des alertes pour certains événements ou suites d'événements.
Périmètre	Systèmes d'exploitation, bases de données, applications SCADA, équipements réseau, automates…
Contraintes	Problématique des volumes des journaux générés. Le nombre d'informations à traiter est important.
Moyens de gestion des contraintes	Des outils existent pour aider à traiter les événements et à les trier en fonction de critères prédéfinis.

BP07 : Gestion des configurations

Motivation	S'assurer que les versions actives dans les équipements (version N) n'ont pas été modifiées de façon malveillante. S'assurer que les différences entre les versions N et N-1 ne correspondent qu'aux modifications légitimes.
Méthode	Comparer les programmes et configurations actifs dans les équipements (version N exécutée) avec une version de sauvegarde identifiée comme la référence (version N sauvegardée). Identifier et analyser les écarts entre les versions N et N-1 avant la mise en service de nouvelles versions.
Périmètre	Les applications SCADA, les programmes automates, les fichiers de configurations des équipements de réseau, les capteurs et actionneurs.
Contraintes	Complexité et hétérogénéité des systèmes industriels.
Moyens de gestion des contraintes	Il existe parfois des outils de gestion des configurations permettant d'identifier rapidement les écarts entre deux versions.

BP08 : Sauvegardes / restaurations

Motivation	Disposer des données nécessaires au redémarrage complet d'un site après une attaque ou un désastre (ceci inclut les données des systèmes).
Méthode	Définir une politique de sauvegarde. Quelles sont les données nécessaires à sauvegarder pour répondre aux besoins des utilisateurs, reconstruire une installation suite à un incident ou satisfaire aux exigences réglementaires ?
Périmètre	Codes source de l'application, bases de données de configuration (utilisateurs, seuils d'alarmes…), historiques de SCADA, programmes, *firmwares* et données (variables, mots…) des automates, fichiers de configuration et *firmware* des équipements réseau (commutateur, VPN, routeur, *firewall*, …), paramètres de réglage et *firmware* des capteurs et actionneurs intelligents par exemple.
Contraintes	Il n'est pas toujours possible de sauvegarder automatiquement toutes les données, en particulier pour les capteurs et actionneurs et les automates.
Moyens de gestion des contraintes	Tracer les modifications des paramètres des capteurs/actionneurs, d'asservissement, de régulation (réglage de PID) ou de configuration d'alarmes …

BP09 : Documentation

Motivation	Maîtriser la documentation pour disposer d'une image exacte des installations et éviter des erreurs d'exploitation. Maîtriser la diffusion afin que seules les personnes ayant besoin des informations soient les destinataires.
Méthode	Définir une politique de gestion de la documentation (processus de mise à jour, durée de conservation, liste de diffusion, stockage…). La documentation relative à un système d'information ne doit pas être conservée sur le système lui-même.
Périmètre	Les documentations techniques des installations, schémas d'architecture, implantation géographique, plan d'adressage, manuel administrateur, plan de maintenance, analyse fonctionnelle, analyse organique…
Contraintes	Il peut être utile de disposer de documents d'exploitation contenant des mots de passe en version papier (pour des astreintes par exemple). La maitrise de ces documents peut se révéler complexe et interdire les versions papier n'est pas nécessairement envisageable.
Moyens de gestion des contraintes	Sensibiliser les utilisateurs aux risques liés à la documentation. Laisser des documents en évidence sur un bureau ou dans le coffre d'une voiture (à coté du PC d'astreinte par exemple) est une mauvaise pratique.

BP10 : Protection antivirale

Motivation	Se prémunir des attaques par virus.
Méthode	Définir une politique antivirale. Protéger en priorité les équipements et applications en contact direct avec l'extérieur et les utilisateurs.
Périmètre	Les applications de SCADA, les stations d'ingénierie, console de programmation et de maintenance.
Contraintes	Incompatibilité avec certaines applications de SCADA d'ancienne génération par exemple, pas de mécanisme de mise à jour de l'antivirus (postes isolés par exemple). Problématiques contractuelles comme la perte de la garantie constructeur.
Moyens de gestion des contraintes	Déployer le logiciel antivirus au moins sur les stations portables, les postes de télémaintenance, les stations d'ingénierie. Pour les nouvelles installations la compatibilité de l'antivirus doit être une exigence du CCTP. Renforcer les configurations des postes.

BP11 : Mise à jour des correctifs (planification)

Motivation	Se prémunir des attaques exploitant les vulnérabilités publiées par les équipementiers. Se prémunir de défaillances liées aux bogues corrigés par les correctifs.
Méthode	Définir une politique de gestion des correctifs (systématique, périodique ou ponctuelle) adaptée aux contraintes fonctionnelles et aux risques identifiés. Par exemple, définir les priorités de déploiement des correctifs, vérifier les compatibilités ascendantes, et l'interopérabilité. Appliquer systématiquement les correctifs aux stations d'ingénierie et postes nomades. Appliquer périodiquement les correctifs sur les stations opérateurs. Appliquer lors de la maintenance les correctifs sur les installations sensibles.
Périmètre	Correctifs des systèmes d'exploitation, des applications, des firmwares en fonction des vulnérabilités corrigées. Station d'ingénierie, postes opérateurs, serveurs, PLC, équipements télécom, écrans tactiles…
Contraintes	Les correctifs doivent être qualifiés avant d'être déployés. Certains équipements ne peuvent pas être arrêtés facilement.
Moyens de gestion des contraintes	Identifier les vulnérabilités adressées par les correctifs. Planifier les mises à jour lors d'arrêt de maintenance par exemple. Surveiller les flux et les journaux d'événement. Durcir les configurations. Isoler les équipements.

BP12 : Protection des automates (PLC)

Motivation	Protéger les programmes automates.
Méthode	Protéger l'accès aux automates par un mot de passe. Des matériels offrent la possibilité de configurer un accès en lecture seule pour les interventions de maintenance de premier niveau. Protéger l'accès au code source et au code embarqué dans les CPU. Désactiver les modes de configuration et/ou de programmation à distance lorsque la fonctionnalité existe. Fermer les armoires automates à clé. Sur les installations critiques remonter un contact sec lors de l'ouverture de l'armoire.
Périmètre	Automates en production, programmes automates sauvegardés ou en cours de développement

BP13 : Stations d'ingénierie, postes de développement

Motivation	Ces éléments constituent des points vulnérables et sont des vecteurs forts de contamination et de prise de contrôle. Ces machines, connectées au réseau industriel, contiennent les logiciels de configuration des équipements, de programmation des automates et des SCADA, parfois des versions de code source... Certains postes peuvent être nomades et se connecter sur d'autres réseaux comme des réseaux bureautiques.
Méthode	Toutes les recommandations précédentes. Appliquer systématiquement les correctifs. Activer systématiquement un antivirus. Ne pas connecter les consoles nomades sur d'autres réseaux que les réseaux SCADA. Les consoles sont nominatives ou alors leur utilisation est tracée. Éteindre les postes fixes lorsqu'ils ne sont pas utilisés et/ou les déconnecter des réseaux de production.
Périmètre	Stations de développement SCADA, console de programmation automate, Terminaux portables (PDA, Pockets PC par exemple) pour configurer les capteurs et les actionneurs intelligents.

ANNEXE C : SIGLES ET ACRONYMES

ADSL	Asymmetric Digital Subscriber Line
AMDEC	Analyse des modes de défaillance de leurs effets et criticités
API	Automate programmable industriel (PLC en anglais)
CPU	Central Processing Unit
DoS	Denial of Service (déni de service)
DRP	Disaster Recovery Plan
EIA	Electrical Industry Association
ERP	Enterprise Resource Planning
FMDS	Fiabilité, maintenabilité, disponibilité et sécurité
FMEA	Failure Mode and Effects Analysis
FAT	Factory Acceptance Test
GSM	Global System for Mobile
GTB	Gestion technique de bâtiment
GTC	Gestion technique centralisée
HAZOP	HAZard & OPerability method
ICS	Industrial Control System
IHM	Interface homme-machine
MES	Manufacturing Executive System
OLE	Object Linked & Embedded
OPC	OLE for Process Control
P&ID	Process & Instrumentation Diagram
PID	Proportionnel Intégral Dérivé
PLC	Programmable Logic Controller
PCA	Plan de continuité d'activité
PRA	Plan de reprise d'activité
PSSI	Politique de sécurité des systèmes d'information
RTC	Réseau téléphonique commuté
SAT	Site Acceptance test
SCADA	Supervisory Control And Data Acquisition
SdF	Sûreté de fonctionnement (= FMDS)
SIL	Safety Integrity Level
SNCC	Système Numérique de Contrôle Commande
SOAP	Service Object Access Protocol
SPC	Statistical Process Control
VFD	Variable Frequency Drive

ANNEXE D : RÉFÉRENCES BIBLIOGRAPHIQUES

Guides de bonnes pratiques et recommandations publiés par l'ANSSI

- http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/

Référentiel Général de Sécurité

- RGS v1.0 : http://www.ssi.gouv.fr/rgs

Outils méthodologiques proposés par l'ANSSI

- http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/
- voir en particulier la méthode EBIOS : http://www.ssi.gouv.fr/ebios

Publications du centre d'expertise et de traitement des attaques informatiques de l'ANSSI (CERTA)

- Acquisition des correctifs CERTA-2001-INF-004
- Les bons réflexes en cas d'intrusion sur un système d'information CERTA-2002-INF-002
- Sécurité des réseaux sans fil (Wi-Fi) CERTA-2002-REC-002
- Sécurité des applications Web et vulnérabilité de type « injection de données » CERTA-2004-INF-001
- Les mots de passe CERTA-2005-INF-001
- Filtrage et pare-feux CERTA-2006-INF-001
- Gestion des journaux d'évènements CERTA-2008-INF-005

Ce guide sur la cybersécurité des systèmes industriels a été réalisé par l'agence nationale de la sécurité des systèmes d'information (ANSSI)

avec le concours des ministères suivants :

et des sociétés suivantes :

À propos de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009 sous la forme d'un service à compétence nationale.

En vertu du décret n° 2009-834 du 7 juillet 2009 modifié par le décret n° 2011-170 du 11 février 2011, l'agence assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

Pour en savoir plus sur l'ANSSI et ses missions, rendez-vous sur www.ssi.gouv.fr.

Version 1.0 - Juin 2012

Agence nationale de la sécurité des systèmes d'information

ANSSI - 51 boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
Sites internet : www.ssi.gouv.fr et www.securite-informatique.gouv.fr
Messagerie : communication [at] ssi.gouv.fr