Exigences de cybersécurité pour les prestataires d'intégration et de maintenance de systèmes industriels

mars 2016

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
10/03/2016	1.0	*Première version applicable*	ANSSI

SOMMAIRE

I. Introduction

Les systèmes industriels sont omniprésents dans notre quotidien, que ce soit en termes d'infrastructures critiques ou non. Leur cybersécurité est une préoccupation majeure prise en compte au plus haut niveau des Etats. Afin d'en renforcer le niveau, il est important de pouvoir s'appuyer sur des prestataires de confiance d'un point de vue de la cybersécurité, impliqués tout au long du cycle de vie des systèmes industriels.

Le groupe de travail sur la cybersécurité des systèmes industriels (GT CSI) piloté par l'ANSSI a identifié les prestataires d'intégration et de maintenance de systèmes industriels comme famille de prestataires stratégiques. Ils interviennent en effet tout au long du cycle de vie des systèmes industriels et de ce fait il est important qu'ils prennent en compte la cybersécurité dans leurs activités.

Les publications de l'ANSSI sont diffusées sur son site Internet :
http://www.ssi.gouv.fr/publications/

Toute remarque sur ce document peut être adressée à **:** **systemes_industriels@ssi.gouv.fr**

II. Présentation générale

II.1. Objet du document

Ce document constitue les exigences en matière de cybersécurité pour les prestataires d'intégration et de maintenance de systèmes industriels.

Les mesures prises pour référence à l'établissement des exigences du présent document sont celles définies pour les systèmes de classe 2 dans les guides intitulés la cybersécurité des systèmes industriels, Méthode de classification et mesures principales [CSI_MESURES_PRINCIPALES] et mesures détaillées [CSI_MESURES_DETAILLEES].

Une partie des mesures de ces guides concernent effectivement directement ou indirectement les prestataires d'intégration et de maintenance.

Les exigences portent sur le prestataire lui-même, ses intervenants, son système d'information ainsi que sur le déroulement des interventions.

Ce document constitue également une aide pour les commanditaires qui voudront intégrer dans leur cahier des charges des clauses de cybersécurité issues des exigences du présent document. Ils pourront demander à leurs prestataires d'être conformes à ce référentiel d'exigences.

Enfin, ce document pourra évoluer pour devenir un référentiel d'exigence pour la qualification des prestataires d'intégration et de maintenance.

II.2. Structure du document

Le document définit d'abord les activités exercées par les prestataires d'intégration et de maintenance (chapitre 3) puis les exigences que ces derniers doivent mettre en œuvre (chapitre4).

Les définitions et acronymes figurent en annexe.

II.3. Identification du document

Le présent document est dénommé «Exigences de cybersécurité pour les prestataires d'intégration et de maintenance de systèmes industriels». Il peut être identifié par son nom, numéro de version et sa date de mise à jour.

III. Activités des prestataires d'intégration et de maintenance

Ce chapitre présente les différentes activités, que réalisent les prestataires d'intégration et de maintenance traitées dans le présent document et dont les exigences spécifiques associées sont décrites au chapitre IV ainsi que les domaines sur lesquels elles s'emploient.

Sans mention particulière, les exigences s'appliquent à toutes les activités visées par le référentiel.

Ces activités portent sur les types de systèmes suivants, regroupés sous le terme générique de « systèmes industriels » :

- les Systèmes Automatisés de COntrôle de Procédés Industriels (SACOPI) ou Industrial Control Systems (ICS) ;
- les systèmes de Gestion Technique de Bâtiments (GTB) ou Building Management Systems (BMS) ;
- les Smartgrids, SmartWater, SmartCities, etc. ;

Ces systèmes sont mis en œuvre dans divers secteurs d'activité[1] comme l'énergie, le transport, la gestion de l'eau, l'agroalimentaire, la défense, l'aéronautique, l'automobile, etc.

Les activités visées par le document couvrent le cycle de vie des types de systèmes cités précédemment.

La définition des activités peut être très variable suivant les interlocuteurs. L'objectif ici, n'est pas de proposer une définition formelle ou normalisée des différentes activités mais de fixer une définition pour ce document.

Les conséquences de l'absence de prise en compte de la cybersécurité sont différentes suivants les activités. Pour certaines, comme la maintenance, les conséquences peuvent être immédiates alors que pour d'autres, comme les spécifications, elles seront indirectes et à plus longue échéance.

L'annexe A du guide [CSI_MAITRISER_LA_SSI] fournit des vulnérabilités fréquemment rencontrées et le guide [CSI_CAS_PRATIQUE] les complète en proposant des illustrations.

De même le guide [CSI_MESURES_DETAILLEES] liste un ensemble de vulnérabilités et rappelle les contraintes liées aux systèmes industriels.

III.1. Spécification

La spécification du système est réalisée par le Maître d'œuvre (MOE), le commanditaire, ou l'Assistance à la Maîtrise d'ouvrage déléguée (AMOD ou AMOAD) qui peut être un prestataire de service d'intégration et de maintenance.

Cette phase de spécification doit être précédée par une étude (étude préalable), qui décrit l'existant, les attentes et exigences générales exprimées par le commanditaire (maitrise d'ouvrage, MOA) qui peut se faire aider (assistance à maitrise d'ouvrage, AMO ou AMOA). Cette étude du besoin et de l'objectif du système à construire est formalisée dans un document appelé Cahier des Charges (CdC) ou Cahier des Clauses Techniques Particulières (CCTP).

La spécification fonctionnelle est :

- la description des fonctions d'un système en vue de sa réalisation ;

[1] L'IGI 6600 [IGI-6600] cite 12 secteurs d'activité d'importance vitale,

- la description dans le détail de la façon dont les exigences seront prises en compte ;
- indépendante de la façon dont sera réalisé le système en question.

Il existe plusieurs sortes de spécifications fonctionnelles :

- les spécifications fonctionnelles générales (SFG) : précisent les fonctionnalités générales attendues du système;
- les spécifications fonctionnelles détaillées (SFD) : précisent le fonctionnement détaillé attendu du système.

III.2. Conception

Ensemble des études menant à la définition organique puis technique du système industriel à développer afin de satisfaire aux spécifications du commanditaire. La conception conduit à la formalisation des fonctions et de l'architecture du système dans le dossier de conception.

Conception de l'architecture : désigne la structure générale inhérente à un système, l'organisation des différents éléments du système (logiciels et/ou matériels et/ou humains et/ou informations) et des relations entre les éléments. Cette structure fait suite à un ensemble de décisions stratégiques prises durant la conception de tout ou partie du système.

III.3. Développement

Ensemble des prestations menant à la réalisation d'un système industriel ou un sous-ensemble de système industriel. Ces études et processus incluent notamment :

- le développement des différents programmes exécutés par les sous-systèmes ;
- les tests unitaires.

III.4. Intégration

Ensemble des activités de définition, d'assemblage (de matériels, logiciels, progiciels) et développements permettant, à partir d'un ensemble de produits / solutions, de réaliser un système pour un commanditaire répondant au besoin fonctionnel qu'il a exprimé.

Cette activité comprend :

- la configuration des matériels et logiciels ;
- la réalisation des tests unitaires et des tests plateformes ou Factory Acceptance Test (FAT).

III.5. Mise en service

Ensemble des études et processus menant à la mise en œuvre d'un système ou d'un composant matériel ou logiciel chez le commanditaire. Ces études et processus incluent notamment :

- la livraison des matériels et logiciels sur site ;
- l'installation des matériels et logiciels sur site ;
- la configuration ou modification éventuelle de configuration des matériels et logiciels ;
- la programmation ou modification mineure de programmes des matériels et logiciels ;

- la validation de l'ensemble des fonctions définies dans l'AF lors de tests appelés tests sur site ou Site Acceptance Tests (SAT) ;
- le démarrage de l'installation.

III.6. Test / qualification / recette /livraison

Ensemble des processus menant à la validation d'un système par rapport à l'ensemble d'exigences applicables. Ces exigences peuvent être définies par des besoins utilisateur, une norme ou standard métier, une réglementation, etc.

Cette activité comprend également la réception formelle du système ainsi que son transfert de responsabilité vers le commanditaire, parfois appelée livraison.

III.7. Maintenance

Ensemble des processus et activités mis en œuvre afin de maintenir (maintenance préventive ou prédictive et corrective), de rétablir (maintenance curative) un système industriel dans un état spécifié afin que celui-ci soit en mesure d'assurer un service déterminé, conforme aux besoins exprimés par le commanditaire.

Ces prestations comprennent par exemple :

- les interventions curatives (appelées parfois de premier niveau) : remplacement des équipements en panne, redémarrage des applications, etc. ;
- les interventions de maintenance corrective ;
- les interventions pour des modifications mineures ;
- la gestion des obsolescences matériels et logiciels.

La maintenance comprend le maintien en condition opérationnelle (MCO) et maintien en condition de sécurité (MCS) d'un système.

La maintenance peut comporter des activités « évolutives » afin d'apporter au système des petites adaptations ne remettant pas en cause le principe de fonctionnement général.

La maintenance est parfois réalisée à distance, via des dispositifs de télémaintenance.

IV. Exigences relatives au prestataire d'intégration et de maintenance

IV.1. Exigences générales

Les exigences listées dans ce chapitre portent sur les aspects suivants : juridique, organisationnel, responsabilité et impartialité du prestataire d'intégration et de maintenance. Elles ne sont pas spécifiques aux prestataires d'intégration et de maintenance. Elles doivent être précisées dans le cadre du contrat établi entre le commanditaire et le prestataire.

IV.1.1. Organisation et contrat

a) Le prestataire doit être une entité ou une partie d'une entité dotée de la personnalité morale de façon à pouvoir être tenu juridiquement responsable de sa prestation.

b) Le prestataire a, en sa qualité de professionnel, un devoir de conseil vis-à-vis du commanditaire.

c) Le prestataire d'intégration et de maintenance réalise ses prestations dans le cadre d'une convention (ou d'un contrat) préalablement approuvée par le commanditaire.
   - La loi applicable à la convention est la loi française.
   - La convention doit préciser les exigences en matière de cybersécurité comme par exemple le niveau de cybersécurité visé pour le système objet de la prestation. Le niveau pourra être défini suivant le guide [CSI_MESURES_PRINCIPALES].
   - Il est recommandé que le commanditaire identifie dans la convention de service les éventuelles exigences légales et réglementaires spécifiques auxquelles il est soumis et notamment celles liées à son secteur d'activité.

d) Le prestataire doit décrire l'organisation de son activité d'intégration et de maintenance en termes de cybersécurité au bénéfice de chaque commanditaire.

e) Le prestataire doit mettre en place une chaîne de responsabilité de la cybersécurité pour les besoins de ses prestations. En particulier, il doit définir un point de contact pour la cybersécurité lors de la prestation, qui sera en charge : de la liaison avec la chaîne de responsabilité du commanditaire, de la garantie du respect de la politique de cybersécurité, de la communication sur les divergences par rapport aux exigences et des éventuelles non-conformités.

f) Le prestataire doit accepter les audits demandés par son commanditaire ayant pour objectif de vérifier que l'ensemble des mesures de cybersécurité demandées contractuellement sont bien appliquées. Ces audits seront limités aux moyens techniques et organisationnels relatifs à la prestation et respecteront la déontologie des audits. Il est conseillé de suivre le référentiel d'exigences définies pour les prestataires d'audits à la sécurité des systèmes d'information [PASSI].

g) Le prestataire doit fournir au commanditaire un Plan d'Assurance Sécurité (PAS) pour les prestations qu'il effectue, détaillant la prise en compte des aspects liés à la cybersécurité lors des différents types de prestations d'intégration et de maintenance qu'il effectue, répondant aux exigences de cybersécurité demandées par ce dernier.

IV.1.2. Ethique

a) Le prestataire doit disposer d'une charte d'éthique que l'ensemble de ses intervenants doit signer.

b) Dans le cas où le prestataire intervient comme expert technique pour le compte d'un autre prestataire, il devra respecter les règles de déontologie et en particulier garantir son impartialité. Sauf cas exceptionnel où le prestataire est le seul compétent dans un domaine, il ne pourra pas être expert pour un système qu'il a lui-même intégré ou pour lequel il dispose d'un contrat (contrat de maintenance par exemple).

IV.1.3. Propriété intellectuelle

a) La propriété intellectuelle, et en particulier, celle des codes sources développés ou intégrés par le prestataire pour le système du commanditaire doit être précisée dans la convention ou le contrat passé entre le prestataire et le commanditaire.

IV.2. Exigences particulières liées aux activités du prestataire

L'objectif n'est pas de détailler des exigences pour chaque activité listées au chapitre III mais d'insister sur des points spécifiques.

IV.2.1. Compétence des intervenants

a) Le prestataire doit s'assurer, pour chaque prestation, que les intervenants désignés pour réaliser la prestation ont les qualités et les compétences requises en matière de cybersécurité pour mettre en œuvre les mesures figurant dans les guides [CSI_MESURES_PRINCIPALES] et CSI_MESURES_DETAILLES]. De ce fait, les intervenants :
   - doivent avoir suivi une formation en cybersécurité des systèmes industriels telle que définie dans le guide portant sur la formation [CSI_GUIDE_FORMATION] ;
   - devraient être habilités[2] à la cybersécurité par le prestataire.
   - doivent justifier d'une expérience suffisante (supérieure à deux ans).

IV.2.2. Documentation

a) Le prestataire doit s'assurer que les informations relatives à ses activités avec le commanditaire sont traitées avec un niveau de confidentialité suffisant. En l'absence d'exigences particulières du commanditaire, l'ensemble des documents relatifs à la conception, à la configuration ou au fonctionnement du système industriel doivent être considérés de niveau « Diffusion Restreinte ». Il devra s'appuyer de l'instruction sur le sensible [II_901] pour la mise en œuvre des mesures.

b) Le prestataire doit être en mesure de détruire tout ou partie des informations relatives au projet sur simple demande écrite du commanditaire. Le prestataire doit être en mesure d'apporter la preuve de la destruction de ces informations. Pour les informations sensibles le prestataire doit se référer aux instructions figurant dans [II_901].

IV.2.3. Méthodes et outils

a) Le prestataire est responsable des méthodes et outils (logiciels ou matériels) utilisés par ses intervenants et de leur bonne utilisation (précautions d'usage, maîtrise de la configuration, etc.). Pour

[2] L'habilitation est un acte formel par lequel le prestataire déclare qu'un intervenant est compétant sur son domaine d'habilitation.

cela, il doit mettre en œuvre un processus de formation des intervenants à ses outils et assurer une veille technologique sur les mises à jour, la pertinence de ces outils ainsi que les risques éventuels liés à leur utilisation.

b) Le prestataire doit disposer des licences valides des outils (logiciels ou matériels) utilisés pour la réalisation de la prestation ;

c) les intervenants ne recourent qu'aux méthodes et outils validés par le prestataire.

Remarque : cela signifie de prendre en compte les outils et méthodes nécessaires pour les situations d'intervention lors de réponse aux incidents et autres modes d'urgence.

IV.2.4. Développement /intégration

a) Le prestataire doit démontrer que ses processus de développement emploient des méthodes d'ingénierie à l'état de l'art, des processus de contrôle qualité et des techniques de validation afin de réduire les défaillances logicielles et les vulnérabilités. Dans le cadre de cette exigence, le terme logiciel s'applique aux logiciels développés par le prestataire : développement d'applications spécifiques ou développement des programmes utilisateurs PLC et SCADA sur la base de composants logiciels (progiciels par exemple) fournis par un équipementier ou un éditeur logiciel.

b) Les caractéristiques de cybersécurité des équipements ainsi que leurs certifications doivent être un critère de choix dans le processus d'achat du prestataire lorsque les équipements ne sont pas imposés par le commanditaire. Il pourra s'appuyer sur les profils de protection publiés sur le site de l'ANSSI (http://www.ssi.gouv.fr). Le prestataire doit soumettre à validation par le commanditaire la liste et caractéristiques de l'ensemble des équipements qui seront intégrés chez le commanditaire.

Remarque : lorsque les équipements sont imposés par le commanditaire, le prestataire doit être en mesure d'apporter un conseil au commanditaire pour lui signaler que le niveau de cybersécurité des équipements n'est pas en adéquation avec le niveau de cybersécurité visé pour le système final.

c) Le prestataire doit définir et appliquer des règles de bonnes pratiques de programmation. En plus de bonnes pratiques de développement, des règles de développement de sécurité (au sens cybersécurité) doivent être mises en place et appliquées.

Il faut distinguer les développements mettant en œuvre des langages de programmations classiques (C, Java, …) pour lesquels la mesure précédente peut s'appliquer, des développements utilisant les outils des équipementiers (pour développer les applications pour les automates et SCADA par exemple) pour lesquels la mesure ne peut pas techniquement toujours s'appliquer ;

d) Le prestataire doit vérifier la mise en œuvre des règles de bonnes pratiques. Pour cela, il pourra par exemple utiliser les options avancées de certains compilateurs (y compris pour le développement d'application automates) ou des outils dédiés à la vérification des bonnes pratiques de programmation.

e) Le prestataire doit utiliser, lorsque des solutions existent, des outils d'analyse statique et des tests de robustesse pour les développements qu'il réalise. L'objectif est de vérifier la qualité des développements et l'absence de bugs « élémentaires » régulièrement utilisés lors d'attaques informatique (débordement de pile « buffer overflow », par exemple).

f) Le prestataire doit être en mesure d'accepter, sur demande explicite du commanditaire, un audit des codes sources développés par ses soins.

g) Le prestataire doit être en mesure de réaliser des tests unitaires et d'ensemble pour vérifier que les exigences de cybersécurité sont bien implémentées.

IV.2.5. Traçabilité et livraison

a) Le prestataire doit être en mesure de tracer les mises à jour et modifications qu'il a apportées aux systèmes déployés et de fournir ces traces aux commanditaires.

b) Le prestataire doit garantir, dans son processus de livraison, l'intégrité et l'authenticité de l'ensemble des logiciels, programmes, éléments de configuration et documentation. Les éléments concernés sont en particulier : les micro-logiciels ; les systèmes d'exploitation; les progiciels SCADA et autres logiciels utilisés; les programmes d'automates et de SCADA ; les fichiers de configuration des équipements réseau, les mises à jour, etc.

c) Le prestataire doit être en mesure de garantir la confidentialité des éléments précédents si le commanditaire en fait la demande. En particulier, il est recommandé que la confidentialité des éléments de configuration soit systématiquement assurée.

IV.2.6. Veille

a) Le prestataire doit déployer un processus de veille sur les menaces et vulnérabilités sur les produits et technologies mises en œuvre sur les systèmes qu'il a déployés. Il pourra s'appuyer sur les informations publiées par les CSIRT étatiques ou privés ainsi que les sites web des équipementiers.

b) Le prestataire doit mettre en œuvre un processus de veille sur l'évolution des moyens techniques pour renforcer le niveau de cybersécurité des systèmes industriels.

IV.3. Protection du système d'information du prestataire d'intégration et de maintenance

IV.3.1. Exigences générales

a) Le prestataire d'intégration et de maintenance doit être en mesure de mettre en œuvre des mesures pour protéger le système d'information qu'il utilise pour ses prestations avec le commanditaire et en particulier s'assurer que son système d'information est en mesure d'accueillir des informations sensibles non classifiées de défense de niveau Diffusion Restreinte. Les exigences spécifiques sont disponibles dans l'instruction [II_901]. En particulier, le système devra être homologué.

b) Ce, ou ces SI, devront être homologués suivant les processus détaillés dans le guide d'homologation [HOMOLOGATION]. L'homologation doit comprendre un audit réalisé conformément au référentiel d'exigences [PASSI].

N'est concernée par ces mesures que la partie du SI du prestataire nécessaire à ses activités d'intégration et de maintenance pour lesquelles il est qualifié.

Le système de facturation, par exemple, pourrait être exclu du périmètre. En revanche, le système de gestion documentaire, contenant les études, les documents des commanditaires sera inclus au périmètre, de même que les ateliers d'intégration, plateformes de développement et de tests.

IV.3.2. Exigences relatives aux outils et à l'environnement de développement

a) Le prestataire doit utiliser un environnement de développement sécurisé afin que celui-ci ne soit pas le point d'entrée pour atteindre les systèmes chez les commanditaires (par l'insertion de codes malveillants par exemple). Il est conseillé de dédier des locaux physiques pour le développement. Le mécanisme de contrôle d'accès doit permettre de tracer l'identité des personnes y pénétrant et l'heure d'accès.

b) Le prestataire doit également veiller à la protection des documents au format papier utilisés dans le cadre de sa prestation.

c) Il est fortement conseillé d'appliquer les exigences et recommandations de sécurité des systèmes de classe 2 figurant dans [CSI-DETAILLEES] aux outils de développement (en particulier les stations d'ingénierie), notamment les règles de sécurisation des équipements (durcissement des configurations, gestion des vulnérabilités, interfaces de connexion, équipements mobiles, sécurité des consoles de programmation, des stations d'ingénierie et des postes d'administration).

d) Il est fortement conseillé que l'environnement de développement soit dédié et séparé des autres environnements informatiques du prestataire. En particulier, cet environnement ne doit pas être connecté à internet ni directement (sans filtrage et mesures de sécurité) au réseau bureautique du prestataire.

e) Les outils de gestion des configurations (« versioning ») devront garantir l'intégrité, l'authenticité et la traçabilité des éléments qu'ils contiennent et suivant les besoins, la confidentialité.

f) Les outils permettant d'assurer les exigences précédentes doivent être mis en œuvre suivant les règles de l'art. Il est recommandé d'utiliser des produits qualifiés par l'ANSSI lorsqu'ils existent.

g) Le niveau de sécurité de l'environnement de développement doit être vérifié par des audits (organisationnels et techniques) réguliers. Il est conseillé que l'environnement de développement soit homologué en s'appuyant pour cela sur le guide d'homologation et les guides de bonnes pratiques comme le guide d'hygiène par exemple.

IV.3.3. Exigences relatives aux plateformes de tests et d'intégration

a) Lorsque les plateformes de tests et d'intégration appartiennent au prestataire, celui-ci doit appliquer les mêmes exigences que pour les environnements de développement.

b) Lorsque les plateformes de tests et d'intégration appartiennent au commanditaire mais sont hébergées chez le prestataire, les mesures de sécurité doivent être précisées par le commanditaire. A défaut, les mesures de l'alinéa précédent seront appliquées.

IV.3.4. Exigences relatives aux outils de maintenance

a) Le prestataire doit mettre en place une procédure de gestion des outils de maintenance afin de vérifier qu'ils sont conformes aux exigences de sécurité du système pour lequel ils seront utilisés chez le commanditaire. Ces exigences figurent dans le guide [CSI_MESURES_DETAILLEES].

b) Le prestataire doit s'assurer que les outils de maintenance ne contiennent pas de données sensibles du commanditaire ou alors que les outils pour en assurer la confidentialité sont bien mis en oeuvre.

c) Le prestataire doit mettre en œuvre des éléments pour renforcer la sécurité des outils de maintenance. Il pourra pour cela, s'appuyer sur les guides et notes techniques publiés sur le site de l'ANSSI.

IV.3.5. Exigences relatives aux outils de télémaintenance

a) Lorsque la télémaintenance est autorisée sur le système du commanditaire, le prestataire doit être en mesure de dédier un poste pour la télémaintenance du système industriel du commanditaire à la demande de ce dernier.

b) Le prestataire doit être en mesure de mettre en œuvre les recommandations et directives figurant dans le guide [CSI_MESURES_DETAILLEES]

c) Les solutions de télémaintenance devront être auditées régulièrement afin de vérifier la bonne mise en œuvre des mesures de vérifier le niveau réel de sécurité. L'audit est réalisé conformément au référentiel d'exigences [PASSI].

d) Le prestataire doit être en mesure d'effectuer les opérations de télémaintenance depuis des locaux maîtrisés disposant du même niveau de sécurité que le système du commanditaire si celui-ci le demande.

IV.3.6. Usage de plateformes de travail collaboratif

a) Dans le cas où le prestataire mettrait à disposition du commanditaire une plateforme de travail collaboratif pour échanger des données (pour les études par exemple), le niveau de sécurité de celle-ci doit être clairement indiquée et portée à la connaissance du commanditaire.

c) Le niveau réel de sécurité doit être vérifié régulièrement par des audits réalisés conformément au référentiel d'exigences [PASSI].

IV.4. Exigences relatives aux interventions d'intégration et de maintenance chez le commanditaire

Les exigences ci-dessous portent sur les interventions réalisées sur les systèmes chez les commanditaires. Cela concerne en premier lieu les intervenants réalisant des activités de maintenance mais cela peut également concerner les intervenants réalisant des activités de mise en service par exemple. Certaines mesures peuvent être redondantes avec celles décrites précédemment.

IV.4.1. Protocole d'intervention

a) Les intervenants devant intervenir sur les systèmes du commanditaire doivent être individuellement clairement identifiés et leurs rôles précisés. En particulier, un référent cyber (assuré par le chef d'équipe par exemple) doit être identifié.

b) L'accès aux installations doit être validé par le commanditaire.

c) Les intervenants doivent respecter les règles de cybersécurité du commanditaire et s'être assurés qu'un protocole d'intervention, identifié dans un permis ou bon de travail par exemple, a bien été validé par les deux parties.

IV.4.2. Bons comportements

a) Les intervenants appliquent les bonnes pratiques lors de leurs interventions chez le commanditaire sans que celles-ci ne soient systématiquement rappelées par ce dernier.

b) Les intervenants se conforment aux règles en vigueur chez le commanditaire.

c) Les intervenants doivent être capables de signaler au commanditaire, des situations anormales qu'il aurait constatées, présentant des risques en termes de cybersécurité.

IV.4.3. Moyens utilisés lors de l'intervention

a) Les interventions sur l'installation du commanditaire doivent être réalisées avec des outils validés. C'est-à-dire qui respectent les exigences détaillées au chapitre IV.3.4 et IV.3.5.

b) L'ensemble des équipements matériels et logiciels utilisés pour les interventions sur les systèmes industriels (comme les consoles de programmation et de maintenance) doit être recensé dans la gestion du parc afin d'être bien identifié pour faciliter leur maintien en condition de sécurité.

c) Les équipements utilisés doivent être exclusivement dédiés aux systèmes industriels (pas de bureautique). Les équipements utilisés devraient être exclusivement dédiés aux systèmes industriels du commanditaire.

d) En cas de besoin particulier, suite à un incident (de cybersécurité ou autres) par exemple nécessitant l'utilisation d'outils spécifiques non identifiés parmi les outils habituels, l'intervenant doit être en mesure d'analyser, avec le commanditaire, les risques liés à leur utilisation et de mette en œuvre les mesures pour traiter ces risques.

IV.4.4. Rapport d'intervention

a) La fourniture d'un rapport ou compte-rendu d'intervention doit être systématique.

b) Le rapport doit contenir une liste de contrôle (check-list) des actions à réaliser après l'intervention, et en particulier vérifier que les sauvegardes des données (données de configuration, modifications de programmes, etc.) ont été réalisées.

c) Le rapport doit lister les anomalies constatées et assurer une traçabilité des actions réalisées et des modifications apportées sur le système du commanditaire.

d) Le rapport d'intervention doit permettre au commanditaire de gérer le cycle de vie de son système et d'en assurer le MCS.

Remarque : le format du rapport d'intervention est à la discrétion du commanditaire. Le rapport d'intervention peut être saisi dans une base de données de maintenance (GMAO) ou des outils de gestion du parc du commanditaire par exemple. L'objectif n'est pas d'alourdir les processus déjà en place chez le commanditaire mais de s'appuyer sur ces derniers.

Annexe 1 Références documentaires

Codes, textes législatifs et réglementaires

Renvoi	Document
[LPM]	Loi de programmation militaire n°2013-1168 du 18 décembre 2013. Disponible sur http://www.legifrance.gouv.fr.
[LOI_IL]	Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés définissant le cadre juridique pour le traitement des données à caractère personnel. Disponible sur http://www.legifrance.gouv.fr.
[II_901]	Instruction interministérielle relative à la protection des systèmes d'information sensibles, n°901/SGDSN/ANSSI, 28 janvier 2015. Disponible sur http://www.legifrance.gouv.fr.

Normes et documents

Renvoi	Document
[CSI_MESURES_PRINCIPALES]	Cybersécurité des systèmes industriels, Méthode de classification et mesures principales, disponible sur http://www.ssi.gouv.fr/systemesindustriels
[CSI_MESURES_DETAILLEES]	Cybersécurité des systèmes industriels, Mesures détaillées, , disponible sur http://www.ssi.gouv.fr/systemesindustriels
[CSI_MAITRISER_LA_SSI]	Cybersécurité des systèmes industriels, Maitriser la SSI pour les systèmes industriels, disponible sur http://www.ssi.gouv.fr/systemesindustriels
[CSI_CAS_PRATIQUE]	Cybersécurité des systèmes industriels, Cas pratique, disponible sur http://www.ssi.gouv.fr/systemesindustriels
[HOMOLOGATION]	L'homologation de sécurité en neuf étapes simples, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[HYGIENE]	Guide d'Hygiène Informatique, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[PASSI]	Référentiel d'exigences pour les prestataires d'audit à la sécurité des systèmes d'information. Disponible sur http://www.ssi.gouv.fr
[GUIDE_ACHAT]	Guide d'achat de produits de sécurité et de services de confiance qualifiés, version en vigueur.
[CSI_GUIDE_FORMATION]	Cahier des charges portant sur la formation à la cybersécurité pour les systèmes industriels, disponible sur http://www.ssi.gouv.fr/systemesindustriels

Annexe 2 Définitions et acronymes

Acronymes :

ANSSI	Agence nationale de la sécurité des systèmes d'information
AMOA	Assistance à Maitrise d'Ouvrage (parfois désignée AMO)
AMOE	Assistance à Maitrise d'Œuvre (parfois désignée AME)
AMOAD	Assistance à Maitrise d'Ouvrage Déléguée
AO	Analyse Organique
AF	Analyse Fonctionnement
BMS	Building Management System
CCTP	Cahier des Clauses Techniques Particulières
CdC	Cahier des Charges
CSI	Cybersécurité des Systèmes Industriels
CSIRT	Computer Security Incident Response Team
FAT	Factory Acceptance Test (recette usine)
GTB	Gestion Technique de Bâtiment
ICS	Industrial Control System
LPM	Loi de Programmation Militaire
MCO	Maintien en Conditions Opérationnelles
MCS	Maintien en Conditions de Sécurité
MOA	Maitrise d'Ouvrage
MOE	Maitrise d'Œuvre
PCA	Plan de Continuité d'Activité
PAS	Plan d'Assurance Sécurité
PLC	Programmable Logic Controler
SACOPI	Systèmes Automatisés de Contrôle de Procédés Industriels
SAT	Site Acceptance Test (recette site)
SCADA	Supervisory, Control and Data Acquisition
SFD	Spécifications Fonctionnelles Détaillées
SFG	Spécifications Fonctionnelles Générales
VPN	Virtual Private Network

Définitions :

Le guide intitulé « La cybersécurité des systèmes industriels, Méthode de classification et mesures principales » [CSI_MESURES_PRINCIPALES] fournit un ensemble de définitions complémentaires aux termes utilisés dans ce référentiel.

Analyse fonctionnelle - analyse, formalisée dans un document, décrivant les fonctionnalités du système afin de répondre aux besoins exprimés par le client.

Analyse organique - analyse, formalisée dans un document, utilisée en ingénierie d'automatisme et d'informatique industrielle, décrivant de manière détaillée les éléments (composants physiques et logiques) mis en œuvre pour répondre aux fonctionnalités identifiées dans l'analyse fonctionnelle.

Commanditaire - entité faisant appel au service des prestataires d'intégration et de maintenance de systèmes industriels.

Développement sécurisé - développement réalisé à l'aide de méthodes, règles, outillages et compétences humaines spécifiques dans le but de fournir un programme sécurisé.

État de l'art - ensemble des bonnes pratiques, des technologies et des documents de référence relatifs à la sécurité des systèmes d'information publiquement accessibles à un instant donné, et des informations qui en découlent de manière évidente. Ces documents peuvent être mis en ligne sur Internet par la communauté de la sécurité des systèmes d'information, diffusés par des organismes de référence ou encore d'origine réglementaire.

Intervenant - employé ou sous-traitant d'un prestataire réalisant une mission pour celui-ci.

Maintenance - ensemble des activités de type curative, préventive, corrective et évolutive permettant le maintien en condition opérationnelle (MCO) et maintien en condition de sécurité (MCS) d'un système.

Politique – intentions et dispositions générales formellement exprimées par la direction d'une entité.

Prestataire – organisme proposant une offre de services.

Prestataire d'intégration/maintenance - organisme réalisant des prestations d'intégration/maintenance de systèmes industriels et/ou des prestations d'intégration/maintenance de composants matériels/logiciels à destination des systèmes industriels.

Spécification - ensemble explicite d'exigences à satisfaire pour un produit ou un service.

Test unitaire - procédure permettant de vérifier le bon fonctionnement d'une partie précise d'un système (un de ses composants ou sous-ensemble). Les résultats des tests sont consignés dans un dossier de tests.

Tiers – personne ou organisme reconnu(e) comme indépendant(e) du prestataire.

Annexe 3 Liste des documents types utilisés lors des prestations

Les documents suivants devraient être utilisés lors des prestations :

- plan d'assurance sécurité ;
- charte d'éthique :
- permis de travail et protocole d'intervention ;
- rapport d'intervention ;
- constat d'anomalie cyber.

Ce guide a été réalisé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) avec le concours des sociétés et organismes suivants :

- ✓ Actemium,
- ✓ Assystem,
- ✓ Atos Worldgrid,
- ✓ Cofely Inéo,
- ✓ DCNS,
- ✓ DGA Maîtrise de l'information,
- ✓ Euro system,
- ✓ Gérard Perrier Industrie,
- ✓ RATP,
- ✓ Schneider Electric,
- ✓ Siemens,
- ✓ Spie,
- ✓ Euriware,
- ✓ Total.

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 – Mars 2016

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