Guide pour une formation sur la cybersécurité des systèmes industriels

Février 2015

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
01/02/2015	1.0	*Première version applicable.*	ANSSI

Sommaire

1 Introduction 4
2 Présentation générale 5
2.1 Objet du document 5
2.2 Structure du document 5
2.3 Identification du document 5
3 Description de la formation 6
3.1 Objectifs de la formation 6
3.2 Public visé 6
3.3 Niveau visé 6
3.4 Durée de la formation 6
3.5 Méthodes pédagogiques 7
3.6 Connaissances préalables 7
3.7 Profil des formateurs 7
4 Contenu pédagogique de la formation 8
4.1 Organisation en modules 8
4.2 Modules de mise à niveau 8
4.2.1 Module 1a pour le profil automaticien 8
4.2.2 Module 1b pour le profil informaticien 10
4.3 Module principal 11
4.4 Module complémentaire 13
5 Évaluation des stagiaires 14
5.1 Au début de la formation 14
5.2 A l'issue de la formation 14
6 Évaluation de la formation 15
Annexe 1 : Fiche de formation cybersécurité des systèmes industriels 16
Annexe 2 : Connaissances préalables 18
Annexe 3 : Questionnaire d'évaluation des stagiaires 21
Annexe 4 : Formulaire d'évaluation de la formation 30
Annexe 5 : Définitions et acronymes 32
Annexe 6 : Références bibliographiques 34

1 Introduction

De nouvelles actions sur les formations en cybersécurité ont été lancées par l'agence nationale de la sécurité des systèmes d'information (ANSSI) suite à la publication en 2013 du nouveau livre blanc sur la défense et la sécurité nationale. Celui-ci indique « qu'il importe également d'accroître le volume d'experts formés en France et de veiller à ce que la sécurité informatique soit intégrée à toutes les formations supérieures en informatique ». Ceci s'applique en particulier au domaine des systèmes industriels et leur sécurité.

Le groupe de travail sur la cybersécurité des systèmes industriels piloté par l'ANSSI, a publié deux guides en janvier 2014[1] contenant des mesures visant à renforcer la cybersécurité des systèmes industriels. Parmi ces mesures, la formation à la cybersécurité occupe une place importante. Le groupe de travail a donc établi ce document dédié à la formation des intervenants sur les systèmes industriels.

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**

[1] La cybersécurité des systèmes industriels – Méthodes de classification et mesures principales » [CSI_MESURES_PRINCIPALES] et « La cybersécurité des systèmes industriels – Mesures détaillées » [CSI_MESURES_DETAILLEES]

2 Présentation générale

2.1 Objet du document

Ce document a pour objectif de définir des exigences pour les organismes souhaitant délivrer une formation relative à la cybersécurité des systèmes industriels.

2.2 Structure du document

Ce document définit d'abord les modalités d'ordre général de la formation (cf. chapitres 2) ainsi que les exigences pour les formateurs (cf. chapitre 3).

Il définit ensuite les sujets que doit traiter la formation. Ceux-ci sont organisés en quatre modules (cf. chapitre 4 :

- deux modules de mise à niveau ;
- un module obligatoire ;
- un module optionnel.

Les connaissances préalables, utiles pour les stagiaires qui souhaitent suivre la formation, sont précisées en annexe 2.

2.3 Identification du document

Le présent document est dénommé « Guide pour une formation à la cybersécurité des systèmes industriels ». Il peut être identifié par son nom, numéro de version et sa date de mise à jour.

3 Description de la formation

3.1 Objectifs de la formation

L'objectif de la formation est de permettre aux stagiaires :

- de comprendre les enjeux liés à la cybersécurité des systèmes industriels et les particularités de ce domaine ;
- d'avoir les éléments de base d'identification des points faibles de ces systèmes ainsi que des recommandations et une méthodologie de renforcement du niveau de cybersécurité de systèmes existants ;
- de comprendre les points clés à examiner lors de la conception de systèmes industriels.

3.2 Public visé

Le public visé est constitué de personnes en charge de la conception, du développement, de l'intégration, de l'exploitation ou de la maintenance de systèmes industriels (maîtrise d'ouvrage, maîtrise d'oeuvre, exploitants, intégrateurs, etc.).

La formation s'adresse aussi aux personnes susceptibles de réaliser des audits ou d'accompagner des clients dans leurs projets de renforcement de la cybersécurité des systèmes industriels.

Ce public se répartit en deux profils :

- Le profil « automaticien » : personne ayant un bagage technique dans le domaine de l'automatisme et des systèmes industriels ;
- Le profil « informaticien » : personne ayant un bagage technique dans le domaine informatique et tout particulièrement la sécurité des systèmes d'information (SSI).

3.3 Niveau visé

La formation permettra à un public d'automaticiens et d'informaticiens d'acquérir les bases de la cybersécurité des systèmes industriels ainsi qu'un vocabulaire commun leur permettant ensuite de travailler ensemble sur des projets relatifs à la cybersécurité d'installations industrielles.

La formation n'a pas comme vocation de faire des stagiaires des experts de ce domaine.

3.4 Durée de la formation

Les organismes de formation peuvent adapter la durée de la formation à leur besoin mais elle sera au minimum de 2,5 jours. Le chapitre 4 donne le détail du contenu pédagogique pour chaque journée, la dernière journée étant optionnelle et reste à la discrétion de l'organisme de formation.

3.5 Méthodes pédagogiques

La formation devra comprendre des cours théoriques, des exercices et des travaux pratiques. Sans préciser outre mesure la part occupée dans la formation par ces trois activités, il doit être clair que pour atteindre les objectifs cités précédement, l'activité dominante consistera en travaux pratiques et exercices. La théorie doit servir à les éclairer. Les exercices doivent servir à montrer comment la théorie permet la compréhension de situations diverses et non encore examinées en travaux pratiques.

Les travaux pratiques devront être mis en œuvre sur une plateforme simplifiée mais représentative d'un système industriel réel.

3.6 Connaissances préalables

Afin de pouvoir suivre la formation, il est souhaitable que les stagiaires aient les connaissances préalables figurant à l'annexe 2.

L'organisme de formation peut proposer des modules portant sur les connaissances préalables au profit des stagiaires qui le souhaiteraient mais les modalités relatives à ces modules n'entrent pas dans le périmètre de ce document.

3.7 Profil des formateurs

Les formateurs devront justifier d'une expérience pratique de 3 à 5 ans dans le domaine de la cybersécurité des systèmes industriels, par exemple en ayant été en charge de l'exploitation d'installations. A défaut, la présence de deux formateurs au moins, l'un expérimenté en sécurité des systèmes d'information, l'autre en systèmes industriels, est nécessaire. Leur expérience doit être d'au moins 3 ans dans leur domaine respectif. Il est recommandé à l'organisme de formation de porter l'expérience et les compétences des formateurs à la connaissance des stagiaires.

4 Contenu pédagogique de la formation

4.1 Organisation en modules

La formation est organisée en quatre modules :

- Module 1a : mise à niveau à destination des automaticiens (½ à 1 journée)
- Module 1b : mise à niveau à destination des informaticiens (½ à 1 journée)
- Module 2 : module principal (2 journées)
- Module 3 : module complémentaire (optionnel)

Les stagiaires étant répartis en deux groupes suivant leur profil, la première demi-journée a pour objectif de donner aux automaticiens le vocabulaire et les notions nécessaires en matière de cybersécurité tels qu'ils sont connus par les informaticiens et, de même, de donner aux informaticiens les notions de bases sur l'automatisme et les systèmes de contrôle des procédés industriels.
La suite de la formation doit être consacrée à la cybersécurité des systèmes industriels, les stagiaires étant réunis en un seul groupe.

Le module complémentaire est optionnel et pourra être consacré à une étude de cas complète.

4.2 Modules de mise à niveau

4.2.1 Module 1a pour le profil automaticien

L'objectif essentiel de ce module est de donner les concepts principaux de la sécurité des systèmes d'information (SSI) à un public d'automaticiens. Pour cela, les éléments suivants doivent être présentés dans un but précis spécifié sous chaque élément :

- Définitions de la cybersécurité/SSI et principaux concepts :
  - Connaître l'objet de la sécurité dans les systèmes d'information et ses piliers : la disponibilité, l'intégrité, la confidentialité, l'authentification, la traçabilité, l'auditabilité, la non répudiation, etc.
- Enjeux de la cybersécurité/SSI ;
- Catégories d'attaques (DDOS, Advanced Persistent Threat (APT), Vers, MITM, spoofing, ingénierie sociale, détournement de sessions, etc.) et modes opératoires ;
- Exemples d'attaques ;
- Grands principes de déploiement d'un projet cybersécurité (analyse de risque, DEP, PSSI, etc.) :
  - Connaître les grands principes à prendre en compte pendant les différentes phases d'un projet : phase de spécification, phase de conception, phase d'intégration, phase de test, et processus de transfert en exploitation.
- Bonnes pratiques :
  - Connaître les bonnes pratiques décrites par exemple dans le « Guide d'hygiène informatique » [GUIDE_HYGIENE] publié par l'ANSSI : la formation devra présenter ces bonnes pratiques en détaillant leurs objectifs et les moyens de les réaliser.
- Panorama des normes et standards :

- Citer les normes ISO/IEC 2700X et connaître leurs objets : système de management de la sécurité de l'information (exigences, guide d'implémentation), mesures de la gestion de la sécurité de l'information, gestion du risque, exigences concernant l'audit,
- Connaître les certifications de produits au niveau international (critère commun, CC) et national (certification de sécurité de premier niveau, CSPN) et le site de l'ANSSI qui tient une liste de ces produits,
- Connaître les principaux référentiels français : prestataires d'audit de la sécurité des systèmes d'information (PASSI), PSSIE, etc.

- Introduction à la cryptographie :
  - Connaître les principes du chiffrement symétrique/asymétrique, les fonctions de hachage, la signature, etc. et le rôle de ces mécanismes,
  - Savoir que si la cryptographie est une technique utilisée en cybersécurité, son utilisation peut présenter des inconvénients. Par exemple, la gestion des clés, essentielle en cryptographie, peut se révéler complexe pour les systèmes industriels. De même, dans des systèmes en temps réel où le délai de réponse peut être critique, l'ajout de messages d'authentification peut ralentir les échanges au-delà du tolérable tout comme le temps de calcul associé à la cryptographie peut être prohibitif. Pour cette raison, on rappellera la nécessité d'étude particulière.

Les travaux pratiques suivants pourront être utilisés pour appuyer le discours. Toutefois, certains des outils mentionnés pouvant s'avérer intrusifs, il est recommandé d'effectuer un court rappel du code pénal sur ces questions.

Exemples de travaux pratiques :

- *Sur un poste SCADA, mettre en place quelques durcissements de base (pare-feu du poste, désactivation des ports USB, mécanisme basique d'authentification, etc.) ;*
- *Mettre en œuvre un pare-feu sur un réseau industriel pour filtrer les flux en amont d'un automate par exemple ;*
- *Mettre en œuvre un tunnel VPN entre un poste SCADA et une passerelle du réseau industriel ;*
- *Mettre en place un LAN simple comprenant quelques ordinateurs et des équipements réseau et utiliser des outils de tests de communication : ping, arp, traceroute, etc. analyser les trames avec un outil tel que Wireshark ;*
- *Mettre en œuvre les outils nmap et nc (netcat).*

Il n'est pas nécessaire de traiter chacun de ces travaux pratiques mais un panel adéquat permettant d'appréhender la réalité.

Il serait souhaitable que les exercices portent sur des équipements et technologies classiquement mis en œuvre par les stagiaires (par exemple une installation type que l'on peut rencontrer en France).

4.2.2 Module 1b pour le profil informaticien

Concepts principaux des systèmes industriels :

- Définitions, les différents types de systèmes industriels :
  - Connaître le modèle Computer Integrated Manufacturing (CIM),
  - Connaître les différents types : centralisés, décentralisés, étendus, etc,
  - Connaître les domaines d'activité et les contextes dans lesquels on rencontre des systèmes industriels (eau, énergie, transport, bâtiment, etc.). Des vidéos d'installations automatisées peuvent être utilisées pour illustrer les propos ;
  - Notion de temps réel (confusion entre temps de réponse rapide et garantie du temps de réponse).
- Composition d'un système industriel :
  - Identifier et savoir situer les éléments constitutifs d'un système industriel : automate programmable industriel (API/PLC), capteurs / actionneurs, logiciels de supervision et de conduite (SCADA), logiciel d'historisation (Historian), poste d'ingénierie, MES, RTU, IED, etc.
- Les langages de programmation d'un PLC :
  - Présentation rapide des cinq langages de programmation définis dans la norme IEC 61131-3. Montrer par exemple que le langage Ladder est inspiré des schémas électriques ou que le GRAFCET est une description logique des procédés industriels.
- Les protocoles et bus de terrain :
  - Notion de bus de terrain. Exemples de bus de terrain les plus répandus : Modbus, Profibus, Asi-bus, DeviceNet, etc,
  - Présentation des protocoles de communication industriels courants : Modbus, Profinet, Ethernet/IP, OPCUA, etc.
- Les architectures réseaux classiques d'un système industriel :
  - Savoir que la surface d'attaque d'un système industriel dépend en partie de son architecture et de sa complexité,
  - Connaître les deux échelles d'architecture proposées dans le guide [CSI_MESURES_PRINCIPALES] : niveau de fonctionnalité d'un système industriel et sa connectivité avec l'extérieur.
- Introduction à la sûreté de fonctionnement (SDF) :
  - Connaître les concepts de base de la SDF (prévention, tolérance, élimination et prévision des défaillances) et le principe des niveaux de sécurité fonctionnelle avec les Safety Integrity Level (SIL).
  - Expliquer les principes de l'analyse de risque en SDF et l'AMDEC par exemple, qui est une méthode régulièrement utilisée. Quels sont ses points communs avec une analyse de risque (type EBIOS) utilisée en SSI.
- Panorama des normes et standards :
  - Citer les principales normes en matière de sûreté de fonctionnement et notamment la norme IEC 61508 et IEC 61511. Afin d'éviter les éventuelles dérives, il est utile de noter que la formation des stagiaires à ces normes est en dehors du périmètre du présent guide. Les formateurs doivent donc se limiter à la présentation de ces normes.
  - Savoir que les normes portant sur la sûreté de fonctionnement ne traitent pas ou peu les questions liées à la cybersécurité.

Les travaux pratiques suivants pourront être utilisés pour appuyer le discours :

- *Configurer un PLC pour piloter une sortie TOR en fonction de boutons poussoirs selon une équation logique donnée ;*
- *Écrire un programme simple d'automate ;*
- *Configurer une IHM de supervision de quelques paramètres envoyant des télécommandes ;*
- *Manipuler un système de taille réduite intégrant un PLC, un ou plusieurs capteurs, un ou plusieurs actionneurs.*

Il n'est pas nécessaire de traiter chacun de ces travaux pratiques mais un panel adéquat permettant d'appréhender la réalité. En revanche, il serait souhaitable que les exercices portent sur des équipements classiquement mis en œuvre par les stagiaires (par exemple une installation type que l'on peut rencontrer en France).

4.3 Module principal

Étude de la cybersécurité pour les systèmes industriels :

- Enjeux :
    - Connaître les enjeux de la cybersécurité des systèmes industriels, en particulier du point de vue des impacts qui peuvent être différents de ceux des systèmes d'information classiques (dommages matériels, corporels, environnementaux, etc.).
- État des lieux et historique :
    - Connaître le contexte d'emploi contraignant des systèmes industriels (durée de vie importante des installations en comparaison à celle des systèmes informatiques, contraintes de disponibilités et de sûreté, etc.) et ses conséquences en termes de vulnérabilités (composants obsolètes, logiciels non mis à jour, etc.) ainsi que les conséquences de l'introduction de technologies standardisées issues de l'informatique de gestion.
- Dualité sûreté de fonctionnement (SDF) et cybersécurité :
    - Savoir distinguer la SDF de la cybersécurité qui tient compte des actes malveillants,
    - Apport de la SDF à la cybersécurité des systèmes industriels (les points communs),
    - Sensibiliser aux risques de confusions (mécanismes d'intégrité par CRC vs par fonction de hachage par exemple).
- Exemples d'incidents sur les systèmes industriels
- Les vulnérabilités et vecteurs d'attaques classiques :
    - Connaître les sources principales de vulnérabilités : cartographie du système industriel non maîtrisée, défaut de la politique de gestion de mots de passes, absence de gestion des comptes, défaut de maîtrise de la configuration, défaut de contrôle des interfaces de connexion, emploi de protocoles non sécurisés, mauvaise gestion des médias amovibles, absence de systèmes de détections d'incidents, etc.
    - connaître les vecteurs d'attaque par la télémaintenance, les interconnexions avec les réseaux bureautiques, les médias amovibles, les piégeages d'équipement, etc.
- Panorama des normes et standards :

    - Citer les principales normes, référentiels et standards de cybersécurité des systèmes industriels : AIEA, NERC CIP, IEC 62443, ISO 27019, OLF, NIST, etc[2]. et montrer pourquoi le sujet est complexe en expliquant les points communs et les divergences entre ces normes.
- En France, la LPM :
    - Champ d'application,
    - Classification des systèmes industriels,
    - Les principales mesures.
- Le projet de cybersécurité du système industriel :
    - Connaître les aspects organisationnels et techniques décrits dans le guide « Maîtriser la SSI pour les systèmes industriels » [CSI_MAITRISER_LA_SSI] dan sa partie « Méthode de déploiement de la SSI. »
- Les recommandations :
    - Connaître les bonnes pratiques citées en annexe du guide [CSI_MAITRISER_LA_SSI] : la formation devra présenter ces bonnes pratiques en détaillant leurs objectifs et les moyens de les réaliser.
    - Expliquer pourquoi les antivirus ne sont pas forcément une solution pour les systèmes industriels
    - Insister sur les aspects liés à la détection d'intrusion (IDS), solution peu intrusive et parfois la seule alternative pour la cybersécurité d'un système industriel : la formation devra présenter les bonnes pratiques en détaillant leurs objectifs et les moyens de les réaliser.
    - Connaître les mesures principales décrites dans le guide [CSI_MESURES]. La formation devra présenter ces mesures en détaillant leurs objectifs et les moyens de les réaliser.
    - Détailler le principe de l'homologation.
    - Connaître le principe de sécurité par le design (des protections mécaniques et électriques peuvent par exemple être intégrées aux fonctions critiques en compléments des systèmes automatisés),
    - Prise en compte de la cybersécurité dans les projets, etc.

Une présentation de l'état des lieux des équipements et produits de cybersécurité dédiés aux systèmes industriels peut être envisagée. Les apports mais aussi les limites de ces équipements et produits seront montrés. Il est souhaitable que le choix des produits ne se limite pas aux gammes proposées par un acteur industriel particulier. Cette partie est laissée à la discrétion de l'organisme de formation.

Les exercices et travaux pratiques suivants pourront être utilisés pour appuyer le discours :

- *Sur un plan d'installation donné, proposer la recherche par petits groupes des failles de sécurité probables et des recommandations d'amélioration à mettre en œuvre. A cette occasion, mettre en évidence les notions de sous-systèmes et de cloisonnement ainsi que les dangers liés aux accès distants et à l'interconnexion des réseaux industriels et de gestion ;*

[2]Le CLUSIF a publié sur son site Web un panorama des normes et standards sur la cybersécurité des systèmes industriels ainsi que des fiches de lecture associées.

- *Sur une architecture simplifiée formée d'un PLC et des entrées sorties associées, d'une IHM et d'une console de programmation, expliciter les mesures de cybersécurité à prendre. Dans ce cadre, montrer l'apport d'un accès VPN ;*
- *Sur un réseau industriel, configurer des commutateurs pour mettre en place un cloisonnement logique au moyen de VLAN ;*
- *Sur un réseau industriel, mettre en place un pare-feu entre un PLC et un SCADA ou entre ce SCADA et le reste du monde ;*
- *Sur un réseau industriel, mettre en place un VPN pour relier un SCADA "distant" à un système industriel ou pour réaliser des opérations de télémaintenance*
- *Renforcer la configuration d'un PLC ;*
- *Configurer les éléments de monitoring disponibles.*

Il n'est pas nécessaire de traiter chacun de ces travaux pratiques mais un panel adéquat permettant d'appréhender la réalité.
Il est recommandé, dans la mesure du possible, l'utilisation pour les travaux pratiques de matériel suffisamment à l'état de l'art.

4.4 Module complémentaire

La formation peut être prolongée par l'étude d'un cas pratique complet, s'appuyant sur la méthode de classification et les mesures proposées en support des travaux de la LPM. Cela sera l'occasion d'un approfondissement de la relation entre informaticiens et automaticiens par la création de petits groupes de travail comportant des participants des deux origines. Ce module est optionnel. Il peut s'organiser comme suit :

- Présenter une étude de cas simple d'un environnement industriel "non-sécurisé" comprenant des systèmes de classes différentes ;
- Appliquer la méthode de classification ;
- Dérouler la démarche pour renforcer la cybersécurité des systèmes ;
- Mettre en œuvre les mesures du guide de l'ANSSI « La cybersécurité des systèmes industriels- Mesure détaillées ».

5 Évaluation des stagiaires

5.1 Au début de la formation

Une évaluation des stagiaires, sous forme de questionnaire, sera réalisée en début de formation. Cela permettra aux stagiaires d'évaluer leur niveau avant la formation et au formateur de pouvoir ajuster si besoin la session de formation à son public. Des exemples de questions se trouvent en annexe 3.

N.B. : Cette évaluation ne constitue pas un mécanisme de sélection. Les organismes de formation restent libres de mettre en place un processus de sélection en amont de la formation s'ils le souhaitent.

5.2 A l'issue de la formation

Une évaluation des stagiaires sera réalisée en fin de formation afin d'évaluer leur progression. Le questionnaire peut être identique à celui proposé au début de la formation.

N.B. : Le but de la formation tel que décrit dans ce document n'est pas de délivrer une certification aux stagiaires. Les organismes de formation sont libres de mettre en place un tel processus s'ils le souhaitent.

6 Évaluation de la formation

Les organismes souhaitant proposer des formations selon le présent guide sont invités à faire remplir par chaque stagiaire, à la fin de chaque session de formation, un formulaire de satisfaction. Celui-ci aura pour objectif de d'assurer que la formation correspond bien aux attentes des stagiaires et de la faire évoluer si besoin en fonction des remarques formulées. Le formulaire se trouve en Annexe 4.

Les organismes de formations sont également invités à faire part à l'ANSSI d'une synthèse des remarques formulées par les stagiaires afin d'adapter le présent document aux besoins et d'assurer une évolution du contenu pédagogique.
Les synthèses pourront être envoyées à l'adresse suivante : **systemes_industriels@ssi.gouv.fr**

Annexe 1 : Fiche de formation cybersécurité des systèmes industriels

NIVEAU : Initiation

DUREE : 2,5j à 3j

OBJECTIFS :

Comprendre les enjeux liés à la cybersécurité des systèmes industriels et les particularités de ce domaine. Connaître les éléments de base pour identifier les points faibles de ces systèmes ainsi que les recommandations et la méthodologie pour renforcer le niveau de cybersécurité de systèmes existants et les points clés pour concevoir de nouveaux systèmes.

CONTENU :

La première demi-journée est une mise à niveau en fonction des profils des candidats.

I : Pour les profils "automaticiens" : 1/2 journée à 1 journée
Concepts principaux de la cybersécurité pour les systèmes d'information en général :

- Définitions de la cybersécurité et principaux concepts ;
- Enjeux ;
- Attaques classiques (MITM, spoofing, ingénierie sociale, déni de service, détournement de sessions, DDOS, APT, Vers) ;
- Exemple d'attaques ;
- Grands principes pour déployer un projet cybersécurité (analyse de risque, DEP, PSSI, etc)
- Bonnes pratiques ;
- Panorama des normes et standards (2700X, certification de produits, etc.) ;
- Introduction à la crypto (chiffrement symétrique/asymétrique, les fonctions de hachage, la signature, etc.).

I : Pour les profils "informaticiens" : 1/2 journée à 1 journée
Concepts principaux des systèmes industriels :

- Définitions, les différents types de systèmes industriels ;
- Composition d'un système industriel ;
- Les langages de programmation d'un PLC ;
- Les protocoles et bus de terrain ;
- Les architectures réseaux classiques ;
- Introduction à la sûreté de fonctionnement ;
- Panorama des normes et standards.

II : Pour les deux profils : 2 jours
Étude de la cybersécurité des systèmes industriels :

- Enjeux ;
- État des lieux, historique ;
- Dualité sûreté de fonctionnement et cybersécurité ;
- Exemples d'incidents ;
- Les vulnérabilités et vecteurs d'attaques classiques ;
- Panorama des normes et standards ;
- En France, la LPM ;
- Le projet de cybersécurité du système industriel ;
- Les recommandations.

II : Optionnel, pour les deux profils

Étude d'un cas pratique en s'appuyant sur la méthode de classification et les mesures proposés en support des travaux de la LPM.

MÉTHODES PÉDAGOGIQUES :

Cours théoriques, démonstrations, exercices et travaux pratiques.

PUBLIC :

Personnes en charge de la conception, du développement, de l'intégration ou de l'exploitation et de la maintenance de systèmes industriels (maîtrise d'ouvrage, maîtrise d'oeuvre, exploitants, etc.).

Personnes amenées à réaliser des audits ou à accompagner des clients dans leurs projets de renforcement de la cybersécurité des systèmes industriels.

PRE-REQUIS :

Connaissance de base en informatique et réseau.

Annexe 2 : Connaissances préalables

Pour le profil automaticien

1) Bases de l'informatique :
   - Notions d'architectures matérielles classiques (microprocesseur, mémoire, bus, périphériques, firmware)
   - Systèmes d'exploitation (les principaux systèmes utilisés)
   - Notions d'architectures logicielles, bases de données

2) Bases des réseaux :
   - Principaux concepts et vocabulaire en vigueur dans ce domaine :
     - modèle OSI à 7 couches,
     - unités de données (trame, paquet, segment, etc.),
     - adresse MAC, adresse IP, notion de ports (UDP/TCP),
     - découverte et diagnostic du réseau (ARP, ICMP),
     - mode connecté (TCP) et non connecté (UDP).
   - Services pouvant être présents dans les équipements industriels (PLC, IHM, VFD, borne sans fil, etc.) :
     - émulation de terminal (Telnet),
     - transfert de fichier (FTP),
     - Web (HTTP) et Web sécurisé (HTTPs),
     - gestion d'équipements (SNMP, SYSLOG, etc.).
   - Principe de cloisonnement des réseaux, moyens et équipements permettant de le réaliser :
     - VLAN au moyen de commutateur,
     - VPN au moyen de passerelle VPN,
     - flux unidirectionnel au moyen d'une diode réseau.
   - Réseaux privés, réseaux publics et principe de translation d'adresse (NAT) ;
   - Réseaux sans fil :
     - réseaux Wi-Fi (IEEE 802.11), réseaux de capteurs (IEEE 802.15.4)
     - réseaux GSM, GPRS, 3G
   - Principaux équipements réseau, leur rôle et le niveau de la couche OSI où ils opèrent :
     - commutateur,
     - pont,
     - routeur,
     - passerelle,
     - pare-feu.
   - Architecture d'un réseau :
     - topologies : en anneau, en étoile, en bus, etc.
     - étendue: LAN, MAN, WAN.

Pour le profil informaticien

- Les concepts de cybersécurité développés en section 4.2.1
- Contrôle d'accès logique :

    - Connaître les principes de gestion des comptes (comptes utilisateur, comptes de service, comptes temporaires, comptes par défaut, comptes invité, expiration de comptes, listes de contrôle d'accès),
    - Connaître les pratiques en matière de gestion de l'authentification : mot de passe à usage unique, authentification par certificats, mot de passe fort, politique de modification du mot de passe.
- Sécurisation de l'architecture d'un réseau :
    - Connaître les principes de cloisonnement réseau. Mise en œuvre de VLAN,
    - Connaître le rôle d'une DMZ. Mise en œuvre de DMZ,
    - Connaître les principes de gestion des interconnexions entre les réseaux, de séparation des flux, de politique de filtrage, etc. Mise en œuvre de pare-feu,
    - Connaître les principes d'interconnexion de sites distants et d'accès distants. Mise en œuvre de passerelles VPN (IPsec, SSL/TLS, MPLS, etc.),
    - Connaître les principes de sécurité d'interconnexion avec Internet.
- Sécurité des protocoles :
    - Connaître les services que peut apporter un protocole sécurisé (authentification et intégrité du trafic, authentification des utilisateurs, confidentialité, résistance au rejeu),
    - Connaître et éventuellement savoir mettre en œuvre les protocoles les plus connus : IPsec, SSL/TLS,
    - Connaître les recommandations en matière de configuration de ces protocoles et des choix de déploiement.
- Sécurisation des équipements :
    - durcissement des configurations,
    - gestion des vulnérabilités,
    - interfaces de connexion,
    - équipements mobiles,
    - sécurité des postes d'administration,
    - développement sécurisé (principe du moindre privilège, éviter les dépassements de capacité (buffer overflows)).
- Surveillance d'un réseau :
    - journaux d'évènements et alertes,
    - système de détection d'intrusion (IDS).
- Cryptographie :
    - chiffrement,
    - signature numérique,
    - gestion de certificats,
    - IGC, clés publiques et privées,
    - hachage,
    - gestion de clés
    - connaître les recommandations de l'ANSSI, en particulier concernant la taille des clés, le choix des algorithmes cryptographiques et leurs paramètres (cf. le RGS).
- Sécurité des points d'accès sans fil :
    - connaître les principales technologies de sécurité du Wi-Fi (WPA, etc.), cloisonnement, filtrage,
    - mettre en œuvre un point d'accès Wi-Fi sécurisé.

Annexe 3 : Questionnaire d'évaluation des stagiaires

Généralités sur la SSI/Cybersécurité

Répondre par Vrai (V) ou Faux (F) aux questions suivantes :

Mes réseaux industriels ne sont pas connectés à internet donc je suis protégé ? □

Mes réseaux industriels ne sont pas connectés à un Intranet donc je suis protégé ? □

J'utilise des systèmes et technologies propriétaires donc je suis protégé ? □

J'utilise des systèmes et technologies obsolètes donc je suis protégé ? □

Sans budget dédié, je ne pourrai déployer aucune mesure de cybersécurité ? □

La cybersécurité peut dégrader les performances de mes installations ? □

La cybersécurité empêche les utilisateurs de travailler efficacement ? □

La sécurité fonctionnelle englobe la cybersécurité ? □

La sûreté de fonctionnement englobe la cybersécurité ? □

Un système Linux est nécessairement plus sécurisé qu'un système Microsoft ? □

La GTB est concernée par le cybersécurité ? □

Je suis une collectivité locale donc je ne suis pas concernée par la cybersécurité ? □

Mon service IT est intégralement responsable de la cybersécurité des installations ? □

Il existe des produits de sécurité certifiés et gratuits ? □

La norme ISO 27001 concerne la cybersécurité ? □

En France, il existe une législation relative à la cybersécurité ? □

En France, il existe une autorité nationale en matière de cybersécurité ? □

La cybersécurité est une branche de l'informatique ? □

La cybersécurité est une branche de l'administration réseau ? □

La cybersécurité intègre la sécurité physique ? □

Les piliers de la cybersécurité sont :

- la confidentialité des données ? □

- la disponibilité des données ? □
- la traçabilité des données ? □
- la protection de la vie privée ? □

Mes fournisseurs sont concernés par la cybersécurité de mes installations ? □

Des négligences en matière de cybersécurité peuvent avoir des conséquences pénales ? □

L'utilisateur, est à son niveau, responsable de la cybersécurité des systèmes qu'il utilise ? □

Une « back door » ou « porte dérobée » est une bonne pratique de programmation ? □

La cybersécurité et la sûreté de fonctionnement sont indissociables ? □

La cybersécurité met en place des mesures techniques ? □

La cybersécurité met en place des mesures organisationnelles ? □

La cybersécurité commence par la qualité ? □

Les produits de sécurité sont suffisants pour sécuriser une installation ? □

Une analyse de risque en cybersécurité se réalise entre experts de la cybersécurité ? □

Les acronymes suivants désignent des méthodes d'analyse de risques :
- AMDEC □
- EBIOS □
- HAZOP □
- MEHARI □
- COCOMO □

Mettre dans l'ordre chronologique les étapes suivantes :
- Cartographie □
- Veille □
- Analyse de risques □
- Détection □
- Prévention □
- Sensibilisation/formation □
- Traitement d'incident □

La cybersécurité concerne les phases :
- d'élaboration du cahier des charges □
- d'achat □
- de spécification □
- de conception □
- de réalisation □
- d'intégration □
- de test □
- de transfert en exploitation □

- d'exploitation □

Acronyme

Répondre par Vrai (V) ou Faux (F) aux questions suivantes :

DOS est un acronyme désignant :
- un système d'exploitation ? □
- un type d'attaque ? □
- le nom d'un logiciel antivirus ? □

Stuxnet est :
- le nom d'une d'attaque célèbre ? □
- le nom d'un logiciel antivirus ? □
- le nouveau protocole de sécurité pour les SCADA ? □

APT est un acronyme désignant :
- une technique d'attaque ? □
- une technique de défense ? □
- autre ? □

DEP est un acronyme désignant :
- un type d'attaque ? □
- une technique de défense ? □
- Autre ? □

Un « 0 Day » est :
- un code malveillant agressif ? □
- le premier correctif corrigeant une vulnérabilité ? □
- Autres ? □

SIL est un acronyme signifiant :
- Software Intelligence Level ? □
- Safety Integrity Level ? □
- Security Integrated Level ? □

Menaces

Répondre par Vrai (V) ou Faux (F) aux questions suivantes :

Les personnes qui vous attaquent sont nécessairement des experts de haut niveau technique ? □

La production d'eau est un secteur d'importance vitale ? □

Un code malveillant (virus,ver, rootkit...) peut :
- détruire des données ? □
- falsifier des données ? □
- espionner des données ? □
- détruire des installations industrielles ? □

Cryptographie

Cocher la case lorsque les mécanismes ci-dessous assurent une fonctionnalité.

Mécanismes/ fonctions	Intégrité	Authenticité	Disponibilité
Signature			
Empreinte			
CRC			
VPN			
HMAC			

Répondre par Vrai (V) ou Faux (F) aux questions suivantes.

Les algorithmes de cryptographie asymétrique nécessitent de partager une clé secrète ? □

Les algorithmes suivants sont réputés fiables :

- RC4 □
- RSA □
- AES □
- DES □

Les algorithmes de hachage suivants sont réputés fiables :

- MD4 □
- MD5 □
- SHA1 □
- SHA256 □

Le mot de passe est le seul moyen de s'authentifier ? □

Les algorithmes de cryptographie symétriques sont plus rapides que les algorithmes asymétriques ? □

Réseau

Une DMZ est une zone sécurisée ? □

Une diode est un équipement assurant un filtrage réseau ? □

HTTPS signifie que la connexion est toujours sécurisée ? □

Les VLANs n'ont pas été conçus pour faire de la cybersécurité □

Les VLANs mettent en œuvre des mécanismes de cybersécurité ? □

La segmentation des réseaux industriels suffit pour assurer la cybersécurité de mes systèmes ? □

Les protocoles assurant l'intégrité entre le SCADA et les PLC suffisent pour se protéger ? □

Les protocoles assurant intégrité et authenticité entre le SCADA et les PLC suffisent pour se protéger ? □

Quel est, par défaut, le n° de port TCP de :

Modbus	____	FTP	____
S7	____	OPC UA	____
Telnet	____	HTTP	____
DNS	____	RDP	____

Syslog est le nom d'un :

- code malveillant ? □
- Protocole ? □
- Antivirus ? □

Parmi les protocoles suivants, lesquels peuvent être sécurisés :

Modbus	□	SSH	□	Telnet	□
Profinet	□	OPC UA	□		
DNP3	□	HartWireless	□		

Quelle est la différence entre IPSec et TLS ?_____

_____

Quelle est la différence entre TCP et UDP ?_____

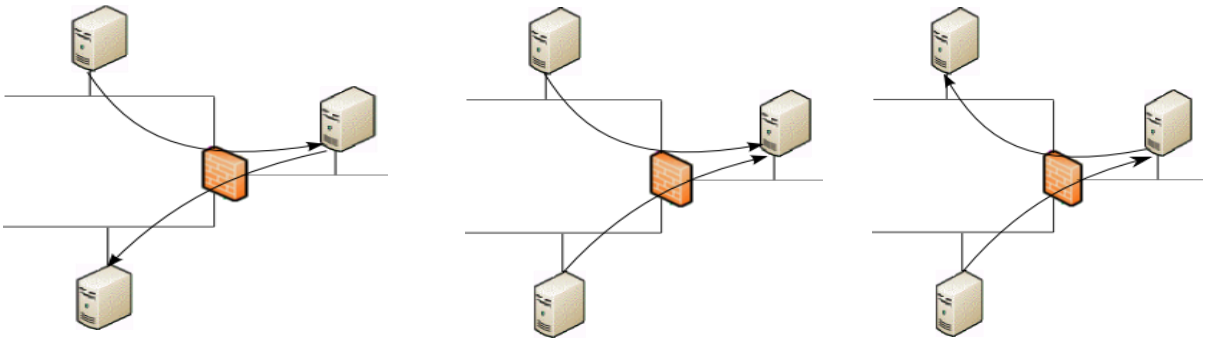
_____

Le modèle OSI est un modèle théorique des différentes couches d'un réseau ? □

Donner le nom de la couche 2 du modèle OSI : _____

Lequel de ces trois schémas correspond à une DMZ ?

A : □ B : □ C : □



Sans fil

Entre WEP et WPA-2, quel protocole choisissez-vous pour sécuriser une connexion WiFi ?_____

Répondre par Vrai (V) ou Faux (F) aux questions suivantes :

Une connexion sans-fil bien sécurisée assure :

- la confidentialité ? □
- l'intégrité ? □
- la disponibilité? □

Les capteurs sans-fil communicant en ISA100 intègrent des mécanismes de cryptographie ? □

Les communications GSM sont sécurisées ? □

Protocoles industriels

Répondre par Vrai (V) ou Faux (F) aux questions suivantes :

Modbus utilise :

- le protocole TCP ? □
- le protocole UDP ? □
- ni le protocole TCP, ni le UDP ? □

EtherNet/IP utilise :

- le protocole TCP ? □
- le protocole UDP ? □
- ni le protocole TCP, ni le UDP ? □

PING utilise :

- le protocole TCP ? □
- le protocole UDP ? □
- ni le protocole TCP, ni le UDP ? □

Le protocole OPC est nécessairement sécurisé ? □

Le protocole OPC UA est nécessairement sécurisé ? □

Parmi la liste suivante, lesquels sont des protocoles industriels :

Modbus	□	DeviceNet	□
EtherNetIP	□	IndustrialEthernet	□
TrolleyBus	□	Unitelway	□
BacNet	□	ControlNet	□
Sercos	□	PiraNet	□
Fipway	□	OPC	□
AS-i	□	PowerLink	□
SNMP	□	EtherCat	□
InterBus	□	TFPT	□

MiniBus □ CAN □

Pare-feu

Répondre par Vrai (V) ou Faux (F) aux questions suivantes :

Un pare-feu :

- filtre des flux ? □
- filtre les virus ? □
- bloque un attaquant ? □
- collecte des logs ? □
- ralentit le trafic ? □

Un pare-feu agit au niveau :

- MAC ? □
- IP/TCP ? □
- Application ? □

Je n'ai pas besoin de sécuriser mon poste si je suis derrière un pare-feu ? □

Un pare-feu n'a pas besoin de mises à jour ? □

Antivirus

Répondre par Vrai (V) ou Faux (F) aux questions suivantes :

Un antivirus protège potentiellement des virus ? □

Un antivirus ralentit l'exécution des tâches de la machine ? □

Un antivirus protège de tous les virus ? □

Un antivirus protège des virus connus uniquement ? □

Un antivirus me permet d'utiliser des clés USB en toute sécurité ? □

Un antivirus a besoin d'une connexion Internet pour se mettre à jour ? □

Composants d'un système industriel

Répondre par Vrai (V) ou Faux (F) aux questions suivantes :

Un PLC (ou API) est plus sécurisé qu'un poste SCADA ? □

Une HMI est plus sécurisée qu'un poste SCADA ? □

Un SNCC est plus sécurisé qu'un système à base de PLC et SCADA ? □

Un PLC est plus sécurisé qu'une HMI ? □

Un PLC dispose de fonctions de cybersécurité ? □

L'OB 35 est une interruption système pour certains automates ? □

Un VFD programmable est à l'abri des codes malveillants ? □

Une console de programmation sert à :

- programmer un PLC ? □
- programmer des capteurs et actionneurs ? □
- à accéder à ses emails professionnels ? □
- à surfer sur Youtube ? □
- à se connecter sur Internet pour télécharger des correctifs ? □

Le disque dur de la console de programmation devrait être chiffré ? □

Pourquoi :_____

_____

Une console de programmation durcie est :

- physiquement plus résistante qu'une console classique ? □
- plus résistante aux attaques informatiques ? □

Accès distants

Répondre par Vrai (V) ou Faux (F) aux questions suivantes :

La sécurité des systèmes de télégestion repose sur la sécurité des opérateurs de Telecom ? □

Un APN privé permet de renforcer la sécurité des communications sans fil ? □

Il est possible de garantir la sécurité avec des solutions de télémaintenance ? □

Une authentification forte sur la machine distante permet de sécuriser la télémaintenance ? □

Une solution VPN/MPLS m'affranchit de chiffrer mes données ? □

Annexe 4 : Formulaire d'évaluation de la formation

La fiche de formation en annexe 1 doit être remise aux stagiaires au même temps que ce formulaire.

Répondre pour « Oui » ou « Non » aux questions ci-dessous.

1. La formation vous a-t-elle permis d'appréhender les enjeux liés à la cybersécurité des systèmes industriels et de mieux comprendre en quoi cela est pertinent dans votre environnement professionnel ? _____

2. Pensez-vous être en mesure maintenant d'analyser la cybersécurité d'un système industriel et de mettre en œuvre les recommandations ?____

3. La notion d'articulation entre un système informatique et un système industriel a-t-elle été suffisamment clarifiée ?____

4. Selon vous, y a-t-il des informations manquantes qui auraient dû être présentées durant la formation ?____

5. Selon vous, les connaissances préalables demandées sont-elles adéquates ?____

6. Selon vous, le contenu de la formation est-il pertinent ?____

7. La documentation fournie est-elle adaptée ?____

8. Selon vous, les plateformes de tests étaient-elles bien adaptées ? ____

9. Selon vous, les exercices et travaux pratiques étaient-ils :
   □ inutiles
   □ partiellement utiles
   □ utiles
   □ très utiles

Commentaires : _____

_____

_____

10. Selon vous, les exercices et travaux pratiques étaient-ils en nombre suffisant ?____

11. Selon vous, les exercices et travaux pratiques étaient-ils bien répartis sur la formation (alternance entre parties théoriques et pratiques)?____

12. Selon vous, le niveau technique de cette formation est :
    □ pas assez élevé
    □ convenable
    □ élevé
    □ très élevé

13. Selon vous, les informations ont été présentées de manière :
    □ pas claire
    □ assez claire
    □ claire
    □ très claire

14. Les intervenants connaissaient-ils parfaitement leurs sujets ? ____

15. Les intervenants étaient-ils bons pédagogues ?____

16. Le rythme suivi par les intervenants était-il adapté ? ___

17. Selon vous, cette formation a été :
    □ incomplète
    □ assez complète
    □ complète
    □ très complète

Commentaires : _____

_____

_____

18. Selon vous, le contenu de cette formation, par rapport à celui précisé par le cahier des charges de l'ANSSI, est :
    □ non conforme
    □ raisonnablement conforme
    □ conforme
    □ au-delà des exigences

19. Finalement, est-ce que cette formation vous a apporté ce que vous attendiez ?____

20. Commentaires : _____

_____

_____

_____

Annexe 5 : Définitions et acronymes

Acronymes :

AIEA	Agence internationale de l'énergie atomique
AMDEC	Analyse des Modes de Défaillance, de leurs Effets et de leurs Criticité
ANSSI	Agence nationale de la sécurité des systèmes d'information
API	Automate programmable industriel
APT	Advanced Persistent Threat
CIP	Common Industrial Protocol
CIP	Critical Infrastructure Protection
CSPN	Certificat de sécurité de premier niveau
DDOS	Distributed Denial of Service attack
DEP	Defense En Profondeur
DMZ	DeMiliterized Zone
GRAFCET	graphe fonctionnel de commande étapes / transitions
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IGC	Infrastructure de gestion de clés
IHM	Interface homme machine
ISO	International Organization for Standardization
LPM	loi de programmation militaire
MITM	Man In The Middle Attack
MPLS	MultiProtocol Label Switching
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
OSI	Open Systems Interconnection
PASSI	Prestataires d'audit de sécurité des systèmes d'information
PLC	Programmable Logic Controller
PSSI	Politique de sécurité du système d'information
RGS	Référentiel Général de Sécurité
SCADA	Supervisory Control And Data Acquisition
SDF	Sûreté de fonctionnement
SIL	Safety Integrity Level
SNCC	Systèmes Numériques de Contrôle Commande
SSI	Sécurité des systèmes d'information
TOR	Tout ou rien
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VFD	Variable Frequency Drive
WPA	Wi-Fi Protected Access

Définitions :

Voici une liste des termes les plus utilisés dans ce document ainsi que leurs définitions respectives.

Une liste plus exhaustive peut être retrouvée dans les guides [CSI_MESURES_PRINCIPALES].

Attaque : tentative d'atteinte à des systèmes d'information réalisée dans un but malveillant. Elle peut avoir pour objectif de voler des données (secrets militaires, diplomatiques ou industriels, données personnelles bancaires, etc.), de détruire, endommager ou altérer le fonctionnement normal de systèmes d'information (dont les systèmes industriels)

Cybersécurité : état recherché pour un système d'information lui permettant de résister à des événements d'origine malveillante susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services rendus par ce système.

Organisme de formation : organisme qui délivre la formation**.**

Sécurité d'un système d'information : ensemble des moyens techniques et non-techniques de protection, permettant à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données, traitées ou transmises et des services connexes que ces systèmes offrent ou rendent accessibles.

Sûreté de fonctionnement : étude des défaillances et des pannes d'un système visant à s'assurer de l'aptitude de celui-ci à accomplir des fonctions, dans des conditions définies et durant un intervalle de temps donnés. La sûreté de fonctionnement traite en particulier les propriétés de fiabilité, maintenabilité, disponibilité et sécurité (FMDS). La sécurité est entendue ici au sens des biens et des personnes. L'Analyse des Modes de Défaillance, de leurs Effets et de leurs Criticités (AMDEC) est une méthode fréquemment employée en sûreté de fonctionnement.

Système d'information : ensemble organisé de ressources (matériel, logiciels, personnel, données et procédures) permettant de traiter et de diffuser de l'information.

Annexe 6 : Références bibliographiques

[CSI_MAITRISER_LA_SSI] Maîtriser la SSI pour les systèmes industriels, disponible sur http://www.ssi.gouv.fr/systemesindustriels

[CSI_CAS_PRATIQUE] Cas pratique, disponible sur http://www.ssi.gouv.fr/systemesindustriels

[CSI_MESURES_PRINCIPALES] Méthodes de classification et mesures principales, disponible sur http://www.ssi.gouv.fr/systemesindustriels

[CSI_MESURES_DETAILLEES] Mesures détaillées, disponible sur http://www.ssi.gouv.fr/systemesindustriels

[GUIDE_HYGIENE] Guide d'hygiène informatique publié par l'ANSSI disponible sur http://www.ssi.gouv.fr

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

- ✓ Airbus Defence and Space Cybersecurity,
- ✓ Arc Informatique,
- ✓ Atos Worldgrid,
- ✓ Belden,
- ✓ CLUSIF,
- ✓ Cofely Inéo,
- ✓ Euro system,
- ✓ Grenoble INP,
- ✓ Lexsi,
- ✓ RATP,
- ✓ RTE,
- ✓ Schneider Electric,
- ✓ Siemens
- ✓ Sogeti,
- ✓ Total,
- ✓ Université Paris 10.

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 – Février 2015

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