Cybersécurité des SIS

Quali-SIL

INERIS

Certification de compétence en sécurité fonctionnelle

INERIS

maîtriser le risque
pour un développement durable

Table des matières

1 Objet

1.1 Contexte

Les industries de l'énergie et du procédé, pour la plupart soumises à la réglementation relative aux installations classées pour la protection de l'environnement (ICPE) et pour certaines, aux prescriptions relatives aux Opérateurs d'Importance Vitale (OIV), mettent en œuvre des systèmes critiques de sécurité (SIS, SCS, I&C, …) conformément aux règlementations et normes relatives à la sécurité fonctionnelle (IEC 61511 et IEC 61508 notamment).

Les attaques récentes montrent combien ces systèmes critiques de l'OT sont tout autant concernés par les enjeux de la cybersécurité que les systèmes d'information (IT). Certaines ont été largement médiatisées. STUXNET a atteint l'automatisme des centrifugeuses enrichissant l'uranium en Iran, causant leur destruction. TRITON, via une attaque sur un poste de travail permettant la programmation du SIS a pu atteindre un automate de sécurité d'un complexe pétrolier. Sa conception et les autocontrôles du programme ont heureusement permis de détecter sa présence et de déclencher immédiatement une mise en sécurité des installations.

L'étude de la sécurité fonctionnelle des systèmes critiques industriels est largement répandue notamment au travers de l'application de la norme IEC 61511 et des réglementations mises en œuvre pour maîtriser la performance des mesures de maîtrise des risques instrumentées (MMRI) dans les installations classées.

Les enjeux liés à leur cybersécurité sont beaucoup moins pris en compte alors même qu'une cyber-attaque peut compromettre l'intégrité de ces systèmes critiques. L'exploitation de leurs vulnérabilités identifiées et généralement non corrigées, expose les installations industrielles et leur environnement à des conséquences physiques, humaines environnementales et/ou financières importantes. La formation des professionnels à la cybersécurité est devenue un enjeu majeur pour la nation et les entreprises (LPM 2019-2025).

Il est impératif que les acteurs (manager, ingénieur, technicien, …) de la sécurité fonctionnelle intègrent la cybersécurité dans le cycle de vie des systèmes critiques au travers de leurs activités afin d'articuler au mieux dans la conception et la validation des systèmes les exigences de sécurité fonctionnelle et les exigences de cybersécurité.

1.2 Objectif général

***Quali-SIL* Cyber** traite de l'intégration de la cybersécurité dans le cycle de vie de la sécurité fonctionnelle décrit dans la norme IEC 61511.

Le module de formation préparant à la certification vise à transmettre une culture et les compétences nécessaires aux professionnels en charge ou intervenant dans une des phases du cycle de vie de sécurité fonctionnelle afin d'être en mesure d'incorporer la cybersécurité dans leurs activités (série IEC 62443).

La certification ***Quali-SIL* Cyber** vise à garantir que ces compétences sont acquises. Elle est régie par le « Référentiel de certification de personnes en sécurité fonctionnelle selon la norme IEC 61511 – Quali-SIL », document référencé PR- 1056, disponible sur le site de l'Ineris. Le référentiel ***Quali-SIL*** définit :

- la structure organisationnelle dédiée au dispositif particulier de certification,
- le processus de certification qui repose sur le suivi d'une formation, une évaluation et une réévaluation périodique de la compétence,
- le management de l'impartialité de la délivrance des certifications.

Le référentiel ***Quali-SIL*** est intégré au système qualité mis en place au sein de l'Ineris, certifié ISO 9001 depuis l'année 2000. Il a été développé selon la norme européenne NF EN ISO/CEI 17024:2012.

Le présent document a pour objet de présenter l'intégration des certifications de compétences en cybersécurité délivrées par l'Ineris, dans le référentiel Quali-SIL.

La formation préparant à la certification de compétences en cybersécurité des SIS a été conçue par un groupe de travail regroupant les organismes de formation habilités Quali-SIL ouvert à des spécialistes de la cybersécurité apportant expertise et avis critique au cours du processus. Elle s'appuie sur l'expérience des membres du groupe de travail, les autres formations Quali-SIL, et les documents de références listés ci-après.

2 Documents de référence

2.1 Références normatives

[1] NF EN ISO 9000 collection.

[2] NF EN ISO/CEI 17024 (septembre 2012) : Évaluation de la conformité — Exigences générales pour les organismes de certification procédant à la certification des personnes.

[3] Série IEC 61511 :2016 : Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation.

[4] Série IEC 61508 : 2011 Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité.

[5] Série IEC 62443 - Security for industrial automation and control systems.

[6] ISA TR84.00.09 : 2017 Cybersecurity Related To The Functional Safety Lifecycle.

[7] ISO/IEC TR 19791:2010 Information technology — Security techniques — Security assessment of operational systems.

[8] Série ISO/IEC 27000 : Information technology — Security techniques — Information security management systems.

[9] IEC TR 63069, Industrial-process measurement, control and automation – Framework for functional safety and security.

[10] NIST 800-82 Rev. 2 - 2015 - Guide to Industrial Control Systems (ICS) Security.

[11] Guides ANSSI – La cybersécurité des systèmes industriels.

[12] AIEA – 2013 - La sécurité informatique dans les installations nucléaires.

[13] NIST 800-82 R2 Guide to Industrial Control Systems (ICS) Security.

2.2 Références réglementaires

[14] Directive 2012/18/UE du Parlement européen et du Conseil du 4 juillet 2012 relative à la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses.

[15] Directive 2016/1148/UE du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

[16] Loi n°2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense.

[17] Décret n°2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du code de la défense.

[18] Décret n°2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information.

[19] Code de la défense – articles L. 1332-1 à L. 1332-7, L. 2151-1 à L.2151-5 et R. 1332-1 à R. 1332-42.

[20] Arrêté du 28 novembre fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Industrie ».

[21] Arrêtés du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale, « Approvisionnement en hydrocarbures pétroliers », « Approvisionnement en gaz naturel », « Approvisionnement en énergie électrique ».

[22] Arrêté du 10 mars 2017 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Nucléaire ».

[23] Arrêté du 17 juin 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Gestion de l'eau ».

2.3 Références qualité Ineris

[24] M002 : Manuel qualité.

[25] Charte de déontologie.

[26] PR0861 : Règles générales de l’activité de certification.

[27] PR0864 : Fonctionnement général des comités de certification.

[28] DI1292 : Indépendance et impartialité dans le domaine de la certification.

[29] PR1056 : Référentiel de certification de personnes en sécurité fonctionnelle selon la norme IEC 61511- Quali-SIL.

3 Professionnels visés

3.1 Secteurs d'activité

Le public visé par la certification est toute personne intervenant sur des installations appliquant des référentiels de sécurité fonctionnelle et ayant des enjeux de cybersécurité. Les professionnels concernés interviennent dans le cycle de vie des systèmes de contrôle commande industriels d'installations susceptibles de générer des risques pour les personnes et l'environnement. Ces installations peuvent être soumises par exemple aux réglementations relatives aux OIV ou aux ICPE mais ne le sont pas nécessairement. Les secteurs d'activité concernés sont à répartir en deux catégories :

Les utilisateurs finaux de systèmes instrumentés de sécurité (SIS) :

Cette catégorie regroupe les industries de transformation et peut s'étendre à d'autres secteurs qui mettent en œuvre des procédés présentant des risques pour les personnes, l'environnement ou les biens (outils de production – stockages, installations ou ouvrages situés à proximité). Il s'agit principalement de :

- Industrie chimique, pharmaceutique et agro-pharmaceutique,
- Industrie pétrochimique,
- Industrie pétrolière amont et aval,
- Canalisations de transport et de distribution de produits dangereux,
- Industrie gazière,
- Electricité y.c. nucléaire,
- Sidérurgie,
- Industrie mécanique,
- Traitement de l'eau (eau potable et assainissement),
- Ouvrages hydrauliques,
- Traitement des déchets,
- Traitement des émissions atmosphériques,
- Transports,
- Etc.

Leurs prestataires de services :
Cette catégorie regroupe les entreprises de services qui interviennent dans le cycle de vie de sécurité mis en place par les utilisateurs finaux. Il s'agit principalement des :

- Bureaux d'étude spécialisés en évaluation des risques,
- Ingénieries en systèmes industriels (électricité, instrumentation et automatisme), intervenant dans la conception, l'installation, les essais et le commissioning des SIS,
- Sociétés spécialisées en maintenance industrielle,
- Sociétés spécialisées en informatique et architecture réseaux,
- Fournisseurs de matériel de sécurité proposant un accompagnement à la mise en service,

3.2 Emplois et métiers visés

La certification ***Quali-SIL* Cyber** vise principalement le personnel en contact avec les systèmes automatisés critiques et le matériel connexe, couvrant les fonctions et métiers suivants :

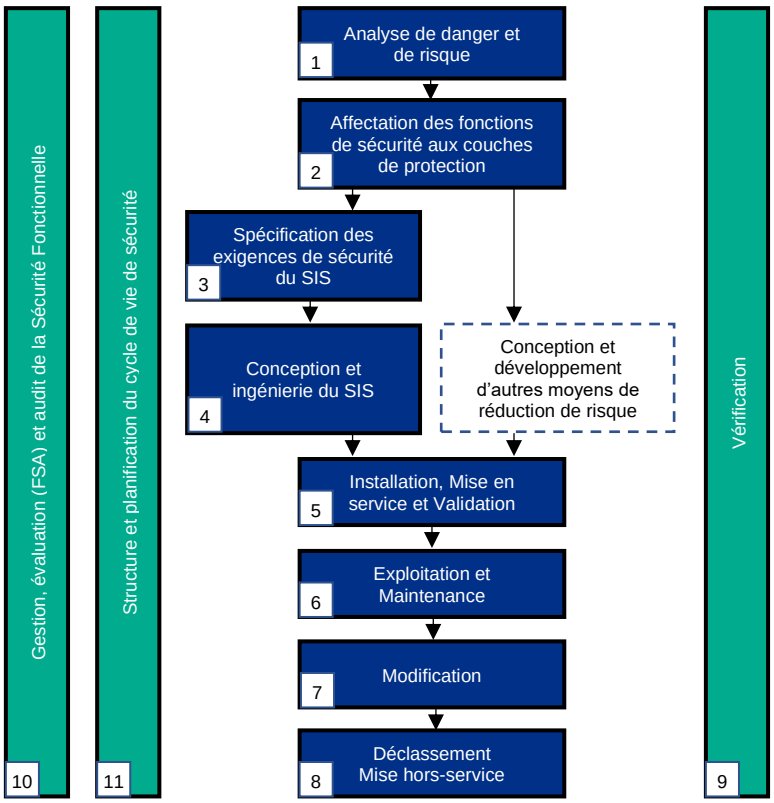
- Responsable sécurité fonctionnelle,
- Responsable sûreté (OIV),
- Responsable HSE,
- Ingénieur sécurité des procédés,
- Consultant évaluation des risques,
- Ingénieur en systèmes de contrôle-commande industriel,
- Chef de projet, chargé d'affaire en contrôle-commande industriel.
- Ingénieur et Responsable SSI (Sécurité des Systèmes d'Information)
- Automaticien, instrumentiste, électricien industriel
- Intégrateur de SIS,
- Prestataire en sécurité informatique,
- Responsable maintenance, production,
- Exploitant opérant des installations protégées par des SIS,
- Formateur en sécurité fonctionnelle,
- Auditeur,
- Inspecteur des installations classées.

Ces professionnels opèrent dans des services techniques supports tels que bureaux d'étude, installation, maintenance en EIA (Electricité, Instrumentation, Automatisme) et sécurité fonctionnelle mais également en production et gestion de production.

3.3 Activités

Les activités couvertes sont celles décrites par le cycle de vie de sécurité de la norme IEC 61511 et différentes normes et référentiels relatifs à la cybersécurité (série IEC 62443, ISA). Les activités relatives à la cybersécurité sont intégrées à ce cycle de vie :

- Intégration des cybers risques dans l'analyse des risques et allocation des SL (security Level),
- Spécifications et intégration des mesures de cybersécurité dans la conception des systèmes critiques (SIS, SCS, …),
- Mise en œuvre des mesures de défense en profondeur,
- Exploiter, maintenir et modifier ces systèmes conformément aux exigences pour ne pas dégrader leur intégrité et sûreté,
- Surveiller, détecter, mener des évaluations et des audits afin d'identifier des dérives et le cas échéant, apporter les actions préventives ou correctives nécessaires afin d'assurer la sécurité fonctionnelle,
- Intégrer les plans de repli et de continuité d'activité en cas d'attaques des systèmes critiques pour la sécurité.



Activités du cycle de vie de sécurité définies par l'IEC 61511-1:2016.

3.4 Missions

Les missions du professionnel certifié ***Quali-SIL* Cyber** sont diverses et couvrent tout ou partie du cycle de vie du système automatisé (API, SNCC, SCADA, capteurs, transmetteurs, actionneurs, IoT), en prenant en compte les exigences de sécurité fonctionnelle et les exigences de cybersécurité issues de différents référentiels réglementaires et normatifs :

- Planification et maîtrise du cycle de vie conjoint sécurité fonctionnelle/ cybersécurité ;
- Analyse des risques et définition des objectifs de sûreté sécurité ;
    - Définit ou applique les stratégies et techniques de cybersécurité des installations industrielles en fonction des études de risque (personnes, environnement et moyens),
    - Coordonne, participe ou réalise des études de risque relatives aux moyens de production,
    - Participe à l'identification et l'actualisation des besoins, des menaces et des niveaux de cybersécurité (SL) requis des fonctions critiques (SIF).
- Spécification, Conception et validation des systèmes ;
    - Met en place des mesures de défense et de surveillance contre les cyberattaques visant les systèmes opérationnels critiques.
    - Coordonne ou participe à l'intégration de la cyber sécurité dès la conception de systèmes industriels automatisés (de conduite et de sécurité) sur des équipements et applications de type FS-PLC, APIdS, API, PLC, SNCC, DCS, avec supervision et terminaux hommes-machines,
    - Etudie et optimise des solutions techniques de production/fabrication de biens ou de prestations techniques, à partir de dossiers de définition fonctionnels et études de sûreté et sécurité,

- Participe à la formalisation des solutions et de l'infrastructure sécurité de l'entreprise pour contrer ces menaces sous forme de documents techniques selon les normes réglementaires et les impératifs de qualité, coût, délais,
- Intègre les éléments de maîtrise de la cybersécurité au niveau de l'architecture du système OT dans son ensemble et des systèmes instrumentés de sécurité (règles de ségrégation, mise en place de moyen de protection et détection des attaques) et par l'intégration et maîtrise d'équipements ou logiciels disposant de certifications ou qualification de sécurité (CSPN, critères communs, certificat IEC 62443).

- Audit et évaluation ;
  - Réalise des inspections et des vérifications techniques et normatives dans un objectif de suivi, de mise en conformité réglementaire et de fiabilisation des équipements, matériels, installations industrielles.
- Installation, exploitation et maintenance ;
  - Effectue des actions préventives et correctives, des mises au point, des tests d'intrusion ou des mises en service de mesures pour contrer les cybermenaces,
  - Détermine et fait évoluer des opérations techniques, des pratiques et des procédés de réalisation (process et produits) en fonction des évolutions et menaces nouvelles,
  - Installe et règle des équipements automatisés autonomes ou des systèmes industriels automatisés et effectue leur maintenance (préventive, curative, ...), en intégrant les exigences de cybersécurité,
  - Participe à la veille sur les vulnérabilités et gère l'application des correctifs dans le respect des contraintes de sécurité fonctionnelle pour la gestion des modifications,
  - Planifie ou participe aux plans de continuité d'activité et plan de reprise d'activité.

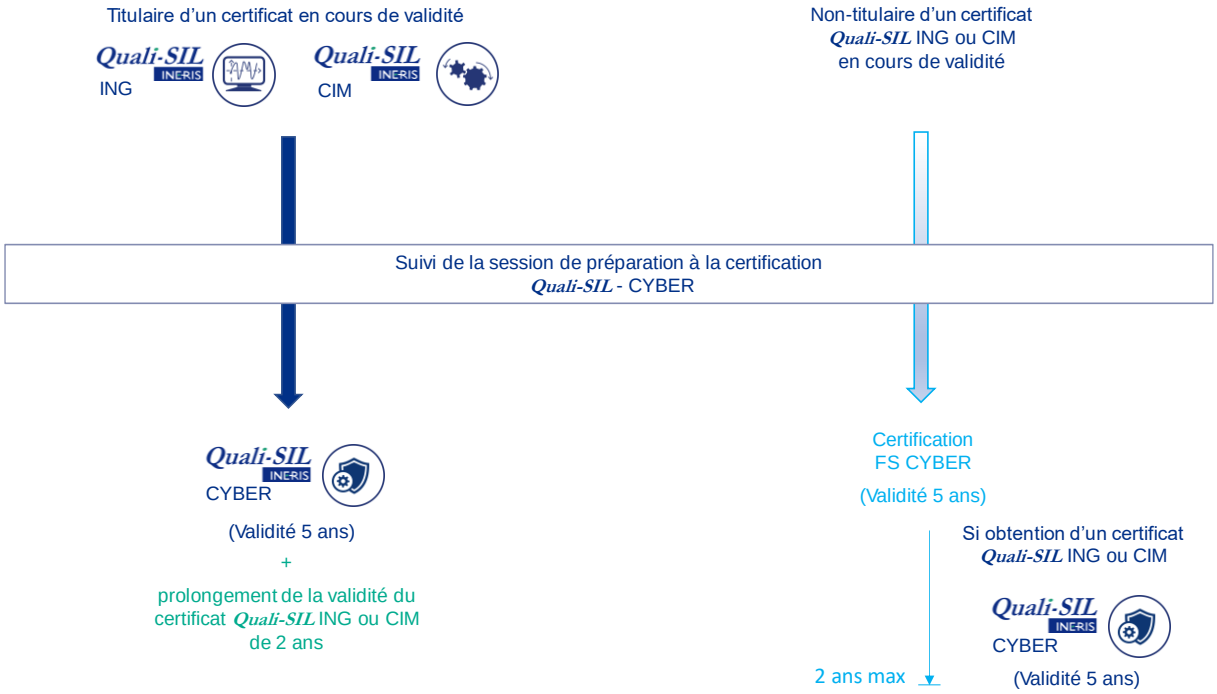
4 Certification de compétences

4.1 Niveau de certification et intégration dans le référentiel *Quali-SIL*

La certification de compétences en cybersécurité délivrée par l'Ineris est une reconnaissance de compétences à intégrer les exigences de cybersécurité dans les activités du cycle de vie de sécurité défini dans la norme IEC 61511 et par analogie, dans d'autres normes de sécurité fonctionnelle (IEC 61508 et IEC 62061). Elle se décline en deux niveaux, selon les prérequis des candidats :

- « *Quali-SIL* Cyber » pour les candidats titulaires d'un certificat *Quali-SIL* CIM ou ING en cours de validité,
- « FS Cyber » pour les candidats non-titulaires d'un certificat *Quali-SIL* CIM ou ING en cours de validité mais disposant de compétences et d'expérience en sécurité fonctionnelle.

La certification est obtenue au moyen d'un processus d'évaluation et de réévaluation périodique permettant de couvrir de façon optimale l'ensemble des compétences tel que décrit dans le référentiel *Quali-SIL* [29].



Intégration des certifications Quali-SIL Cyber et FS cyber dans le référentiel Quali-SIL.

4.2 Evaluation et certification

Le suivi de la formation « Préparation à la certification Quali-SIL Cyber » auprès d'un Organisme de Formation Habilité est fortement conseillé.

L'évaluation du candidat menée par l'Ineris, repose sur les éléments suivants :

- le dossier de prérequis dûment complété (intégrant notamment des exigences en termes de niveau d'étude, de compétences en sécurité fonctionnelle et de cybersécurité, et d'expérience dans ces mêmes domaines),
- la copie d'examen corrigée par le formateur certifié ; l'examen se compose de :
    - 52 questions à choix multiple,
    - 16 questions ouvertes.

La décision de certification est prise par une personne disposant d'une délégation du Directeur Général et n'ayant pas participé à l'évaluation ou à la formation du candidat.

L'évaluation et la certification sont conduites conformément aux règles définies dans les documents qualité applicables au sein de l'entité Certification de l'Ineris (Cf. documents [25] à [29]).

Institut national de l'environnement industriel et des risques
Parc technologique Alata • BP 2 • F-60550 Verneuil-en-Halatte
03 44 55 66 77 • ineris@ineris.fr • www.ineris.fr