DECEMBRE 2018

CYBERSÉCURITÉ

POUR LA MAINTENANCE DES INSTALLATIONS INDUSTRIELLES

ECC for Industrial and Urban Systems

The European CYBERSECURITY CLUSTER

iu

SOMMAIRE

La vocation du cluster ECC4iu est notamment de fédérer l'écosystème de la cybersécurité des systèmes industriels, de promouvoir le savoir-faire dans ce domaine et d'apporter des réponses concrètes au travers de guides comme celui-ci pour l'ensemble des acteurs concernés par le sujet, qu'ils soient donneurs d'ordres, sous-traitants, fournisseurs, prescripteurs, etc.

Depuis plusieurs années déjà, la cybersécurité des systèmes industriels est une préoccupation forte des autorités, qui soulignent régulièrement les conséquences importantes que provoqueraient des attaques sur ces systèmes omniprésents dans notre quotidien.

Bien que la prise de conscience de ce sujet progresse, sous l'impulsion parfois des réglementations, des questions très concrètes subsistent quant aux mesures à déployer pour renforcer la cybersécurité et la résilience des nombreux systèmes industriels qui nous entourent.
Les travaux français en la matière apportent de premières réponses au travers des guides publiés par l'ANSSI, et cela, dès 2012.

La réglementation, française dans un premier temps, avec l'article 22 de la loi de programmation militaire de 2014, puis européenne avec la directive NIS, transposée en droit national, renforcent les messages sur la nécessité impérieuse de prendre en compte la cybersécurité des systèmes numériques, dont les systèmes industriels font partie. En effet, ces réglementations imposent à de nombreux acteurs des exigences fortes pour renforcer la cybersécurité de leurs systèmes numériques importants.

Le constat, partagé par tous, est qu'une part importante des vulnérabilités rencontrées sur les systèmes industriels et les vecteurs d'attaques exploitables, résident dans les interventions sur ces systèmes, lors d'opérations de maintenance notamment.

L'argument fréquemment avancé, que certains systèmes industriels sont protégés parce qu'ils ne sont pas connectés à Internet ou non connectés au réseau informatique de l'entreprise ne tient pas. Ce mythe constitue une « vulnérabilité » majeure !

Certains auront en tête, les virus (rançongiciels ou autres) introduits sur des chaînes de production par un intervenant (interne ou externe), via une clés USB ou la connexion d'un PC portable, porteur de virus, utilisé dans le cadre d'interventions de maintenance par exemple.

Qu'on se le dise une bonne fois pour toute, la cybersécurité, concerne toutes les phases du cycle de vie des systèmes industriels et en particulier les phases de Maintien en Condition Opérationnelle (MCO) nécessitant l'intervention de nombreuses personnes.

Ce guide tente d'apporter des réponses pragmatiques pour renforcer la cybersécurité des opérations de maintenance afin de pouvoir sereinement assurer le MCO des systèmes industriels, sans que cette phase du cycle de vie des systèmes constitue une vulnérabilité importante et soit à l'origine d'incidents.

Pour les systèmes industriels d'ancienne génération, ceux n'ayant pas été conçus dans l'esprit de faire face aux menaces cybernétiques et sur lesquels peu de mesures de cybersécurité techniques sont applicables, la cybersécurité des opérations de maintenance constitue une étape importante et une des premières phases possibles d'un projet de prise en compte du risque cyber en réduisant une partie de la surface d'attaque de ces systèmes.

Enfin, les cas d'usage publiés par ECC4iu illustrent certains aspects abordés dans ce guide. Il est conseillé aux lecteurs de lire ces cas d'usage au préalable afin de disposer d'éléments de contexte métier, utiles à la compréhension des propos de ce guide.

Il s'agit d'un guide non exhaustif, qui en aucun cas, ne remplace les textes réglementaires. Il vient en appui de ces textes pour aider les parties prenantes à renforcer la cybersécurité et la résilience de leurs systèmes industriels. Les recommandations énoncées dans ce guide peuvent être une première étape dans la réduction du risque cyber des installations industrielles.
Ce guide est publié dans sa première version. Des commentaires, en vue d'une prochaine version, peuvent être transmis au cluster via l'adresse email suivante : contact[at]ecc4iu.eu

2. OBJECTIFS DU GUIDE

Il existe de nombreux guides sur la cybersécurité des systèmes industriels, comme ceux publiés par l'ANSSI (cf. bibliographie) ainsi que d'autres organisations étatiques ou non, abordant ponctuellement les questions de cybersécurité lors des opérations de maintenance, mais aucun n'est exclusivement dédié à cette activité importante, source majeure de vulnérabilités.

Ce guide a pour objet de proposer des bonnes pratiques en matière de cybersécurité à appliquer lors des opérations de maintenance, que l'on pourrait qualifier de « règles d'hygiène » pour ces opérations. Il s'appuie sur des recommandations figurant dans différents guides existants, notamment ceux de l'ANSSI [1] et de retours d'expérience.

Il vise également à fournir un référentiel commun, tant sur le fond que sur la forme, partagé par les donneurs d'ordre, les fournisseurs, et les autorités en la matière. Pour cela, le guide pose les bases d'un vocabulaire commun en reprenant des définitions issues de normes ou guides utilisés à la fois dans le domaine de la maintenance industrielle et de la cybersécurité.

Ce guide rappelle également les concepts fondamentaux de la maintenance et les concepts fondamentaux de la cybersécurité. Il est important de préciser que ce guide ne vise pas à remplacer le référentiel d'exigences pour les prestataires d'intégration et de maintenance de systèmes industriels[2]. En revanche, il pourra utilement compléter ses références et apporter une aide aux prestataires souhaitant s'engager dans une démarche de conformité à ce référentiel.

A QUI S'ADRESSE LE GUIDE ?

Le guide s'adresse à l'ensemble des personnes concernées par la maintenance et aux personnes concernées par la cybersécurité. Les opérations de maintenance des installations industrielles concernent de nombreuses personnes et en particulier :

- **Les donneurs d'ordres** (parfois appelés Opérateurs, notamment dans la réglementation) qui exploitent les installations et ont la responsabilité de leur maintien en condition opérationnelle ;
- **Les mainteneurs** composés de personnels internes ou de sous-traitants (souvent appelés les intégrateurs) qui réalisent les opérations de maintenance sur les installations et sont au coeur même des systèmes ;
- **Les chefs d'équipe** des mainteneurs ;
- **Les personnes en charge de la cybersécurité** lors des opérations de maintenance ;
- **Les bureaux d'ingénierie et des méthodes** qui définissent les plans et les procédures de maintenance nécessaires au MCO des installations ;
- **Les acheteurs et les juristes** (dans une moindre mesure), pour les aspects contractuels avec les fournisseurs.

Ce guide s'adresse à tout type d'organisation, publique ou privée, quel que soit son niveau de maturité en cybersécurité : Opérateurs d'Importance Vitale (OIV), Opérateurs de Service Essentiel (OSE), grands groupes, ETI, PME/PMI, établissements public, collectivités territoriales, etc.

PÉRIMÈTRE DU GUIDE

Les mesures de cybersécurité lors des opérations de maintenance ne suffisent bien évidement pas, à elles seules, à sécuriser les systèmes industriels. La cybersécurité est une démarche plus large concernant, comme cela a déjà été évoqué, toutes les phases du cycle de vie des systèmes. La prise en compte de la cybersécurité lors des phases de conception pour de nouvelles installations, lors de projets de rénovation ou d'évolutions d'installations existantes est essentielle. Mais malgré cela, les systèmes conçus et intégrés avec des mesures de cybersécurité (dits « secured by design ») resteront fragiles et vulnérables à de nombreuses menaces d'origine cyber, compte tenu des contraintes opérationnelles et de la durée de vie des systèmes au regard de l'évolution de la menace.

[1] Maitriser la SSI pour les systèmes industriels et Mesures détaillées. [2] Guide publié par l'ANSSI en 2015.

Si ce guide traite des mesures de cybersécurité pour les opérations de maintenance en général, il vise en priorité les systèmes peu sécurisés, conçus parfois il y a des dizaines d'années, à une époque où, pour être très clair, le concept de cybersécurité des systèmes industriels n'existait simplement pas.

Ces systèmes représentent, « malheureusement » aujourd'hui la majorité des systèmes en exploitation. Les personnes en charge de ces systèmes, souhaiteront éviter que les opérations de maintenance, très souvent externalisées, soient le principal vecteur d'entrée d'une cyber-attaque conduisant à un incident important.

Le terme « maintenance » ouvre à lui seul un champ des possibles gigantesque. Pour cette raison, le chapitre 4 fournit des rappels sur des définitions des différents types de maintenance. Dans un vocabulaire courant, les opérations de maintenance visées par ce guide sont les suivantes :

- **La maintenance dite « métier » de tous les jours**. Ces opérations de maintenance assurent l'entretien et le MCO des installations. Les mainteneurs peuvent être amenés à se connecter avec un PC pour réaliser un diagnostic par exemple ou connecter des médias amovibles sur les équipements industriels.
- **Les maintenances programmées** (potentiellement lors d'arrêt d'usine) qui peuvent être gérées sous forme de projets et pour lesquelles le risque en termes de cybersécurité est accru.
- **Les opérations mineures permettant** de réaliser des tâches comme les sauvegardes, les collectes de logs, des comparaisons des programmes, des relevés de configurations/paramétrages, etc.
- **Les maintenances curatives** qui, à la suite d'une défaillance sur les systèmes, ont pour objectif de remettre celui-ci en fonctionnement.
- **Les évolutions mineures** qui ne nécessitent pas une phase d'intégration mais qui modifient fonctionnellement ou techniquement les installations.

Remarque : ces opérations peuvent être réalisées sur le site où se trouvent les systèmes à maintenir ou peuvent être réalisées en télémaintenance.

En revanche le guide ne traite pas des questions portant sur le Maintien en Condition de Sécurité (MCS) des systèmes industriels. Le MCS doit en effet, être prévu et défini en amont, lors de la conception et de l'intégration des installations, par des procédures et des moyens techniques. Les opérations « d'administration de la cybersécurité » comme les changements de mots de passe ou l'application de correctifs de sécurité à la suite de la découverte de vulnérabilités, ne sont pas abordées dans ce guide. Là encore, ces opérations se prévoient et se définissent en amont sur la base des recommandations et des exigences réglementaires ou non déjà évoquées.

En revanche, le guide pourra citer ces actions, assimilables à de la maintenance préventive, et expliquer qu'elles peuvent être planifiées et réalisées en même temps que les opérations de maintenance « métier » sur les installations.

LES THÈMES ABORDÉS

Ce guide sur la cybersécurité pour la maintenance des installations industrielles aborde, sans être exhaustif, les thèmes, techniques et organisationnels ci-dessous :

- La formation ;
- Les médias amovibles ;
- La télémaintenance ;
- Les outils de maintenance (consoles de programmation et stations d'ingénierie) ;
- L'accès physique ;
- La traçabilité ;
- Le coût de la cybersécurité ;
- La cartographie des moyens, outils, procédures, personnes, etc. pour la maintenance (ou pour l'administration pour reprendre le vocabulaire du monde de l'informatique) ;
- L'aspect contractuel de la maintenance ;
- Les outils d'aide à la maintenance (GMAO, GED, gestionnaires de configurations, etc.) ;
- L'organisation et gouvernance ;
- Le forum de discussion et réseaux sociaux.

3. RAPPELS

LA MAINTENANCE

La norme européenne EN 13306 : 2017 intitulée « Maintenance - terminologie de la maintenance », apporte des définitions très claires et très précises sur la terminologie et les différents types de maintenance. Le guide reprend des définitions de la norme sans toutefois être exhaustif. Il est conseillé aux lecteurs de lire la norme afin, pour les non-experts, de se familiariser avec les concepts.

ATTENTION : la maintenance des logiciels pris isolément n'est pas couverte par cette norme.

DÉFINITIONS

MAINTENANCE : ensemble de toutes les actions, techniques, administratives et de management, durant le cycle de vie d'un bien, destinées à le maintenir ou à le rétablir dans un état dans lequel il peut accomplir la fonction requise. » Comme l'explique la norme, « la maintenance apporte une contribution essentielle à la sûreté de fonctionnement.

EXPLOITATION : combinaison de toutes les actions techniques administratives et de management, autres que les actions de maintenance, qui a pour résultat l'utilisation du bien.

BIEN : élément, composant, mécanisme, sous-système, unité fonctionnelle, équipement ou système qui peut être décrit et considéré individuellement. » Dans le présent guide, le terme « système » est utilisé pour désigner l'ensemble des « biens.

FIABILITÉ : aptitude d'un bien à accomplir une fonction requise, dans des conditions données, durant un intervalle de temps donné.

MAINTENABILITÉ : dans des conditions données d'utilisation, aptitude d'un bien à être maintenu ou rétabli dans un état où il peut accomplir une fonction requise, lorsque la maintenance est accomplie dans des conditions données, en utilisant des instructions et des moyens prescrits.

DISPONIBILITÉ : aptitude d'un bien à être en état d'accomplir une fonction lorsqu'elle est requise dans des conditions données, en supposant que les ressources externes nécessaires sont mises à disposition.

CYCLE DE VIE : phases successives par lesquelles passent un bien, de sa conception à sa mise au rebut.

OBSOLESCENCE (à des fins de maintenance) : impossibilité pour un bien d'être maintenu en raison de l'indisponibilité sur le marché des moyens nécessaires à des conditions techniques et/ou économiques acceptables.

DÉFAILLANCE : perte d'une aptitude d'un bien à accomplir une fonction requise.

CAUSE DE DÉFAILLANCE OU MODE DÉFAILLANCE (OBSOLÈTE) : circonstance au cours de la spécification, de la conception, de la fabrication, de l'utilisation ou de la maintenance qui entraîne la défaillance.

PANNE : état d'un bien inapte à accomplir une fonction requise, excluant l'inaptitude due à la maintenance préventive ou à d'autres actions programmées ou à un manque de ressources externes.

TÉLÉMAINTENANCE : maintenance d'un bien exécutée sans un contact physique direct du personnel au bien. Cette définition reviendrait potentiellement à considérer que lorsqu'un intervenant connecte sa console de programmation sur un commutateur réseau Ethernet dans une baie réseau à quelques dizaines de mètres de l'installation, il agit en télémaintenance. Dans l'usage courant, la télémaintenance est une maintenance exécutée depuis l'extérieur du site dans lequel se trouve le bien. Le télé-mainteneur se situe généralement dans des locaux n'appartenant pas au propriétaire du système. Cette définition sera retenue dans le cadre de ce guide.

Dans le guide, les « mainteneurs » ou « intervenants de maintenance » désignent le personnel interne ou externe à une organisation, réalisant les opérations de maintenance sur les installations industrielles.

TYPES DE MAINTENANCE

Seuls les principaux types de maintenance sont retenus pour le guide :

- **Préventive :** maintenance destinée à évaluer et/ou atténuer la dégradation et réduire la probabilité de défaillance d'un bien. La maintenance préventive comprend la maintenance :
  - Systématique : maintenance préventive exécutée à intervalles de temps préétablis ou selon un nombre défini d'unités d'usage mais sans contrôle préalable de l'état du bien.
  - Conditionnelle : maintenance préventive qui inclut l'évaluation des conditions physiques, l'analyse et les éventuelles actions de maintenance qui en découlent.
  - Prévisionnelle : maintenance conditionnelle exécutée à la suite d'une prévision obtenue grâce à une analyse répétée ou à des caractéristiques connues et à une évaluation des paramètres significatifs de la dégradation du bien.
- **Curative :** maintenance exécutée après détection d'une panne et destinée à rétablir un bien dans un état dans lequel il peut accomplir une fonction requise.

Ces types se combinent avec le caractère planifié ou non des opérations. Une maintenance curative peut ainsi être :

- Réalisée dans l'urgence et ne pas être planifiée ;
- Planifiée en l'absence de caractère d'urgence ;
- Planifiée, malgré le caractère d'urgence, afin d'assurer la protection des biens et des personnes.

LA CYBERSÉCURITÉ

La sécurité numérique, ou cybersécurité traite les menaces qui pèsent sur les systèmes numériques, qu'elles soient d'ordre intentionnel ou non, même si bien souvent le focus porte sur les menaces de type intentionnel, appelées « malveillances ».

La norme référence en matière de cybersécurité est la famille ISO 27000 « systèmes de gestion de la sécurité des systèmes d'information ». En particulier 27001 « Management de la sécurité des systèmes d'information » et 27002 « Code de bonnes pratiques pour le management de la sécurité de l'information », qu'il convient de compléter par les éléments fournis par les réglementations nationales ou internationales ainsi que les guides et référentiels publiés par les autorités nationales.

L'instruction interministérielle n°901, désignée « II901 » ci-après, signée le 28 janvier 2015, définit les objectifs et les règles relatifs à la protection des systèmes d'information sensibles, notamment ceux traitant des informations portant la mention « Diffusion Restreinte ».

Une définition de la sécurité numérique est : « ensemble des moyens techniques et non-techniques, 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. »

Les piliers de la sécurité numérique, qui définissent les objectifs de sécurité, d'un système sont[3] :

- **L'intégrité :** non altération des produits et des fonctions ou services délivrés ;
- **La disponibilité :** les fonctions ou les services sont accessibles au moment voulu ;
- **La traçabilité :** le parcours d'un produit ou d'une fonction ou d'un service est identifiable depuis sa production jusqu'à son utilisation. La traçabilité peut-être une exigence réglementaire ;
- **La confidentialité :** les fonctions ou les services fournis ne sont accessibles qu'aux personnes autorisées (protection des secrets industriels par exemple).

Ce rappel est fondamental car, les mondes de la sécurité numérique et des systèmes industriels se sont souvent opposés alors qu'ils possèdent des points communs importants sur le plan des objectifs et de la méthodologie.

Sans entrer dans le détail, car ce n'est pas l'objet de ce guide, l'atteinte aux objectifs de sécurité cités ci-dessous, peuvent provoquer des impacts en termes de sécurité des biens et des personnes, de protection d'environnement, de productivité, ou encore des impacts en termes de secret industriel.
Les cas d'usage publiés par ECC4iu abordent d'avantage les impacts métiers que peuvent provoquer des incidents de cybersécurité sur des systèmes industriels. La littérature regorge d'exemples[4] très concrets illustrant les cyberattaques et leurs conséquences. Ce guide n'a pas vocation à les reprendre.

[3] Par usage, la notion de « fonction » est utilisée dans le contexte industriel alors que la notion de « service » est utilisée dans le contexte informatique.

3.

Comme pour les opérations de maintenance industrielle, la cybersécurité s'appuie sur des mesures organisationnelles, techniques et juridiques et nécessite de déployer des mesures d'anticipation, de protection et de réaction.

La démarche cybersécurité et ses bonnes pratiques se construisent, comme en sûreté de fonctionnement, sur la base d'une analyse de risque, visant à identifier les risques pesant sur un système (un bien) afin de les réduire à un niveau acceptable. Étape souvent fastidieuse, l'analyse de risque en sécurité numérique peut être précédée, voire remplacée dans certains cas, par une analyse « allégée » telle que celle définie par l'ANSSI dans son guide « Méthode de classification et mesures principales ».

Cette analyse « allégée » a pour objectif de classer les systèmes industriels en trois niveaux (appelés « classes »), en fonction de critères simples, puis de proposer des règles de cybersécurité adaptées pour chacune des classes.

Les critères de définition des classes sont :

- **L'impact,** qui est généralement déjà identifié lors des analyses de risques réalisées en sûreté de fonctionnement (AMDEC par exemple) ;
- **La vraisemblance,** qui se détermine par les caractéristiques intrinsèques du système (son niveau de fonctionnalités et de connectivité principalement) et de son environnement ;
- **Le produit du niveau d'impact** par le niveau de vraisemblance donne le niveau de risque.

Toutefois, cette méthode de classification a été élaborée pour les opérateurs d'importance vitale (OIV) dans le contexte de la loi de programmation militaire 2014-2019. Afin de répondre à l'ensemble des publics visés par ce guide, la définition des classes telle que proposée dans la méthode de l'ANSSI est adaptée pour ne plus considérer les risques d'un point de vue de la nation uniquement mais aussi d'un point de vue de l'organisation.

Adaptation des définitions :

- **Classe 1 :** Il s'agit des systèmes industriels pour lesquels le risque où l'impact d'une attaque est faible pour l'entreprise ou l'organisation. L'ensemble des mesures préconisées pour cette classe doivent pouvoir être appliquées en complète autonomie. Ce niveau correspond principalement aux règles d'hygiène informatique énoncées dans le guide de l'ANSSI.
- **Classe 2 :** Il s'agit des systèmes industriels pour lesquels le risque ou l'impact d'une attaque est significatif pour l'entreprise ou l'organisation. Les mesures à mettre en place contiennent des « obligations » et « recommandations ».
- **Classe 3 :** Il s'agit des systèmes industriels pour lesquels le risque ou l'impact d'une attaque est critique pour l'entreprise ou l'organisation. Dans cette classe, les « obligations » sont plus fortes. Les systèmes doivent être homologués par l'entité responsable qui doit pouvoir apporter la preuve de la conformité des systèmes aux mesures prévues.

Parmi les règles principales définies pour les 3 classes, deux demandent une attention particulière afin d'éviter de mauvaises interprétations et des confusions.

- **L'homologation des systèmes :** l'homologation de sécurité[4] vise à donner et à garantir un certain niveau de confiance dans les services rendus par un système numérique au travers d'une démarche structurée, réglementaire pour certains acteurs, et engageant la responsabilité des acteurs concernés. Le principe de l'homologation existe dans d'autres domaines que la sécurité numérique, comme celui de la sûreté de fonctionnement. L'homologation peut porter sur tout type de système numérique et dans le cas présent, sur les systèmes faisant l'objet de maintenance mais aussi sur les moyens utilisés lors des opérations de maintenance.

- **Habilitation des personnes :** sur le principe de l'habilitation électrique, l'habilitation des personnes en sécurité numérique, consiste à s'assurer que les personnes possèdent les compétences nécessaires pour intervenir sur les installations afin de garantir un certain niveau de cybersécurité. Les personnes habilitées sont formées à la sécurité numérique et sont explicitement autorisées par leur hiérarchie à intervenir sur les installations. L'objectif de ce guide n'est pas de détailler le processus d'habilitation qui peut d'ailleurs être propre à chaque organisation.

[4] Cf. guide « l'homologation en 9 étapes » de l'ANSSI.

LA CYBERSÉCURITÉ ET LE RISQUE INDUSTRIEL

La cybersécurité introduit un risque important pour les systèmes industriels déjà confrontés à d'autres types de risques. Suivant les types de systèmes industriels, les risques peuvent porter sur la sécurité des biens et des personnes. Que cela soit pour les systèmes « safety », participant à la protection des biens et des personnes, comme ceux utilisés sur des sites Seveso ou plus largement les installations classées pour la protection de l'environnement (ICPE), ou les systèmes de sécurité (« security »), participant à la protection physique des installations (vidéoprotection, contrôle d'accès par exemple), la cybersécurité s'inscrit dans le dispositif global de la sécurité d'une installation industrielle.

La propriété d'intégrité, par exemple, est une caractéristique essentielle des systèmes « safety » et « security ». Une atteinte à ces systèmes peut conduire directement à un accident industriel tel que l'explosion d'une installation, un incendie, une pollution de l'environnement, etc.

Les incidents de cybersécurité peuvent être parfois plus sournois comme ceux liés à l'utilisation d'outils de maintenance compromis (modification du calibrage par exemple), qui, ne fournissant plus les bonnes mesures entraînent des diagnostics erronés conduisant à des impacts potentiellement importants sur le système maintenu.
La cybersécurité des installations doit être traitée en se repositionnant dans le contexte du risque industriel global.

LE RÔLE DES INTERVENANTS DE MAINTENANCE DANS LA CYBERSÉCURITÉ

De même qu'en inspectant visuellement une installation il est possible de détecter un dysfonctionnement (une fuite d'huile par exemple), les mainteneurs peuvent, lors d'opérations de maintenance sur les installations, détecter des problèmes potentiels de cybersécurité et les signaler aux personnes en charge de ce sujet. Ils peuvent par exemple :

- Noter qu'un poste de supervision déporté est resté dans une vieille version et n'a pas été mis à jour ;
- Remarquer que les voyants de diagnostic d'automates programmables industriels signalent des défauts qui n'ont pas été vus et signalés ;
- Remarquer que des sessions sont restées non verrouillées sur des Interface Homme Machine (IHM) ;
- Noter que des baies réseaux sont restées ouvertes ;
- Et bien d'autres dysfonctionnements encore.

Ces quelques exemples pourraient donner lieu à la création de check-lists que les personnes, amenées à intervenir régulièrement sur les installations, lors de rondes par exemple, pourraient appliquer. En complément, les intervenants de maintenance peuvent exécuter quelques actions simples comme le lancement de commandes de diagnostic sur des équipements ou l'exécution de commande pour collecter les logs par exemple. Ces actions valorisent le travail des mainteneurs et replacent le rôle de l'humain dans le dispositif global de la cybersécurité des systèmes industriels.

L'INTÉGRATION DE LA CYBERSÉCURITÉ DANS LES PLANS DE MAINTENANCE

Bien que ce sujet figure en marge de l'objectif principal du guide, l'intégration de la cybersécurité dans les plans de maintenance s'avère être un outil puissant pour, d'une part gérer efficacement le Maintien en Condition de Sécurité (MCS) des systèmes industriels et d'autre part, réconcilier les mondes de la sécurité numérique et des systèmes industriels.

La maintenance est une activité bien maîtrisée dans le monde des systèmes industriels. La complexité du MCO de ces systèmes demande parfois une logistique importante et surtout une forte capacité de planification des interventions. Les outils comme la Gestion de Maintenance Assistée par Ordinateur (GMAO) procurent une aide précieuse et pourraient tout à fait être mis à profit des actions de cybersécurité, non seulement pour tracer les opérations effectuées sur les installations, mais aussi pour planifier, dans les plans de maintenance, les opérations de cybersécurité à réaliser.

3.

Ces opérations de cybersécurité programmées, comme toute intervention de maintenance, peuvent être de deux types :

- Des interventions curatives planifiées comme la correction d'un bug non bloquant (ne provoquant pas de pannes pour le système) par exemple ;
- Des interventions planifiées classiques visant à assurer le MCS des systèmes.

Ces dernières, comme le changement de mots de passe, la vérification des mises à jour des logiciels, la réalisation de sauvegardes, etc. doivent être prévues en amont, dès la conception des systèmes et doivent être intégrées dans les gammes et plans de maintenance des installations. Les guides [Maîtriser la SSI pour les systèmes industriels et mesures détaillées] ainsi que la norme ISO27002 contiennent un ensemble de mesures relatives au MCS qu'il conviendrait d'intégrer dans la GMAO.

La sécurité numérique des applications de GMAO devrait être une préoccupation. La perte de la disponibilité ou de l'intégrité de cet outil, peut impacter indirectement les systèmes industriels en ne fournissant plus les informations nécessaires à son MCO et MCS. Si les données des systèmes de GMAO ou plus largement des systèmes industriels sont considérées comme des informations sensibles en termes de confidentialité alors elles peuvent être protégées en suivant les recommandations de l'II901.

MAUVAISES PRATIQUES

Le but n'est pas de donner des leçons car tout le monde a, un jour ou l'autre sans le savoir, mis en œuvre des mauvaises pratiques, que ce soit par ignorance (manque de formation), agissement dans l'urgence, manque de moyens, etc.

Identifier les mauvaises pratiques, pour ne plus les reproduire, est tout aussi important qu'acquérir les bonnes pratiques. Il s'agit même de la première bonne pratique dont l'efficacité au regard du coût est importante.

Les mauvaises pratiques fréquemment rencontrées sont d'ordre technique, organisationnel et juridique. Les principales mauvaises pratiques identifiées ci-dessous sont organisées par thèmes. Certaines sont transverses à plusieurs thèmes. L'objectif est de montrer que l'aspect méthodologique/organisationnel, et de fait, le côté humain sont fondamentaux pour la cybersécurité dans les interventions de maintenance.

TECHNIQUES :

- **Console de programmation « non maîtrisée » :** une console de programmation non maîtrisée peut présenter un niveau de cybersécurité faible et être la porte d'entrée pour compromettre un système industriel. L'absence de mises à jour de sécurité du système d'exploitation et des logiciels utilisés, l'absence de durcissement des configurations, ainsi que les usages multiples de la console (pour surfer sur internet par exemple ou consulter sa messagerie) augmentent considérablement le risque d'incident lors des opérations de maintenance. Le fait que le mainteneur utilise la même console pour plusieurs sites et plusieurs clients représente un risque de contamination croisée. De plus, ces consoles contiennent très souvent la documentation des systèmes maintenus (plan, Analyse Fonctionnelle, mode opératoire, mots de passe) ainsi que les sources des programmes automates et des applications SCADA. Ceux-ci constituent une mine d'or pour un attaquant souhaitant cibler une attaque sur un système. Or, il est fréquent de constater que les consoles de maintenance ne disposent d'aucune protection pour limiter le risque de vol d'information en cas de perte du poste.

- **Moyens de télémaintenance non maîtrisés :** la télémaintenance est clairement un sujet transverse sur les trois thèmes, technique, organisationnel et juridique. Néanmoins, son positionnement dans le thème technique provient du constat que les postes utilisés pour la télémaintenance sous souvent faiblement sécurisés et que les moyens de connexion sur les systèmes télé-maintenus le sont encore moins. L'utilisation d'outils de prise de main à distance (VNC, RDP, etc.) ne disposant d'aucun mécanisme de cybersécurité ou encore l'utilisation de solution de cybersécurité comme des VPN comportant des vulnérabilités connues sont fréquentes. La conséquence de cette mauvaise pratique est que des personnes non autorisées peuvent se connecter aux systèmes télé-maintenus en « volant » les identifiants de connexion par exemple lorsque ceux-ci ne sont pas suffisamment protégés et passent en clair sur les réseaux ou en exploitant des failles connues des moyens mis en œuvre.

ORGANISATIONNELLES :

- **Manque de formation des intervenants :** première source de vulnérabilité, le manque de formation, conduit à de mauvaises pratiques lors des interventions de maintenance. Pour limiter le risque d'accidents lors d'intervention sur des installations électriques les personnels sont formés et habilités. Cela ne supprime pas les accidents, surtout ceux liés aux habitudes ou à la répétition de certaines tâches, mais les réduit fortement.

- **Pas ou peu de traçabilité des actions réalisées :** l'absence de traçabilité complique l'analyse en cas d'incident et surtout ne permet pas d'identifier les « responsables » et à contrario, les « non responsables ».
Remarques : la traçabilité :
- Est en effet un des moyens de se protéger pour ne pas être « accusé » à tort en cas de problème.
- Permet également de revenir en arrière en cas de problème et limiter ainsi les effets d'un incident.

- **Pas de protection de la documentation :**
  - Les documents contenant des informations potentiellement sensibles sont laissés sur les installations, accessibles à tous. Pourtant, ces documents fournissent des informations précieuses aux personnes qui voudraient attaquer les systèmes. La remarque régulièrement avancée est qu'il faut venir sur le site pour atteindre ces documents. S'il est vrai que cela limite les risques, cela ne les supprime pas. Est-ce que toutes les personnes qui entrent sur le site sont de confiance ? Il est arrivé que des plans comportant des informations sensibles ou des mots de passe, soient pris en photos ou filmés lors de « visite » et se retrouvent ensuite sur Internet.
  - Les documents contenant des informations potentiellement sensibles sont stockés en version numérique dans des environnements n'offrant pas le bon niveau de cybersécurité. Pour des questions de commodité, il peut être tentant de stocker ces documents, même de manière provisoire, sur des espaces de stockage (souvent gratuits) de type cloud pour lesquels il n'existe aucune évaluation du niveau de cybersécurité et de confiance. De même, il peut être utile de transmettre des informations à son client, à ses collègues par email ou via des solutions de transfert de gros volumes de données. Sans mécanisme de protection robuste, cette pratique revient à diffuser des informations sur la place publique.

- **Pas de sauvegardes avant et après les interventions (ou sauvegardes incomplètes) :** l'absence de sauvegarde conduit à l'incapacité de revenir en arrière en cas d'incident et limite la traçabilité des actions apportées lors des interventions. Rappelons que les capacités de restauration de ces sauvegardes doivent être régulièrement testées au risque de n'être d'aucune utilité en cas de besoin.

- **Sessions des postes SCADA et IHM non verrouillées après leur utilisation :** ces situations permettent à toutes personnes n'ayant pas l'autorisation d'utiliser les équipements de le faire. Un simple clic de souris pour actionner une télécommande sur une IHM ou modifier un paramètre de procédé peut provoquer des dégâts sévères (coupure de l'alimentation électrique générale d'un site par exemple).

- **Connexions de média amovibles non maîtrisés :** les incidents de cybersécurité liés à l'utilisation de médias amovibles (clés USB, disques USB ou téléphones portables) connectés sur des installations industrielles ne se comptent plus. Ces médias, lorsqu'ils ne sont pas maîtrisés, peuvent contenir des codes malveillants, comme des rançongiciels, et infecter vos systèmes.

- **Rechargement de téléphones portables via un port USB :** le simple fait de recharger un téléphone portable ou une tablette en les connectant sur le port USB d'une IHM ou d'un PC est une mauvaise pratique. Les téléphones portables sont de véritables PC, aussi vulnérables, voire plus, aux cyberattaques. Leurs compromissions et fréquente. Cette pratique représente un risque majeur d'introduction de code malveillant (rançongiciels notamment) sur les installations industrielles.

- **Pas de procédure encadrant les interventions :** l'absence de procédures encadrant les interventions contribue fortement à l'usage de mauvaises pratiques telles que celles citées précédemment. Les 14 procédures permettent, y compris à des intervenants formés à la cybersécurité, de rappeler les évidences, les bonnes pratiques élémentaires et constituent une base de traçabilité des actions effectuées.

3.

- **Utilisation des forums de discussion :** l'utilisation de forum de discussion sur Internet peut être une source utile pour aider à régler des problèmes techniques. En effet, d'autres personnes ont probablement déjà été confrontées aux problèmes rencontrés. Plus sournois et probablement moins évident, l'utilisation de forums de discussion peut conduire à de véritables incidents de cybersécurité. Quelle confiance peut-on accorder à la personne qui se trouve à l'autre bout d'Internet, qui donne des conseils en réponse aux questions qui lui sont posées ?

- **Portes des baies serveurs ou des armoires automates laissées ouvertes :** quiconque peut effectivement accéder aux équipements, insérer une clé USB, un routeur pour les communications sans-fil (Wifi, 3/4G ou autres), voler un disque dur contenant des informations sensibles, etc.

- **Station d'ingénierie ou console de programmations connectées et actives en permanence :** bien qu'elles ne soient pas utilisées en permanence, il n'est pas rare de constater que les stations d'ingénierie sont connectées en permanence aux réseaux industriels et sont actives (poste démarré). Cela augmente la surface d'attaque et laisse le temps à un code malveillant ou une attaque ciblée d'atteindre la station d'ingénierie pour ensuite atteindre les systèmes industriels.

- **Connexions provisoires laissées actives :** si lors d'opération de maintenance, des connexions provisoires peuvent s'avérer indispensables, les laisser activées augmente la surface de vulnérabilité.

- **Connexion, sur un port série d'un PLC[5], d'un équipement disposant d'une interface sans fil :** tous les PC d'aujourd'hui ou presque, disposent de connexions sans-fil que ce soit Wifi ou 3/4G. Les connecter au port série d'un équipement industriel qui peut être « isolé » car non connecté à des réseaux, revient simplement à connecter l'équipement à Internet !

- **Utilisation de logiciels « pirates » :** l'utilisation de logiciels téléchargés sur des sites « douteux » ou le téléchargement de mises à jour ou de firmwares, mises à jour de composants logiciels sur d'autres sites que ceux des équipementiers augmente le risque d'introduire des codes malveillants sur les systèmes maintenus et les outils de maintenance.

JURIDIQUE :

- **Absence de clauses contractuelles définissant clairement les responsabilités :** l'absence de clauses contractuelles laisse un flou sur les obligations et devoirs en matière de cybersécurité de chacune des parties. En cas d'incident, il sera plus complexe de déterminer les responsabilités.

Cette liste pourrait être enrichie par les retours d'expérience et l'analyse des incidents ayant conduit à des incidents de cybersécurité.

Les lecteurs souhaitant contribuer sont invités à faire part de leurs expériences, cas concrets en contactant le cluster ECC4iu à l'adresse suivante : contact[at]ecc4iu.eu.

[5] Programmable logic controller.

4

BONNES PRATIQUES DE CYBERSÉCURITÉ POUR LES INTERVENTIONS DE MAINTENANCE

Les bonnes pratiques à prendre en compte pour renforcer la cybersécurité des interventions de maintenance ont pour objectif de réduire les risques d'incidents lors des interventions. Ces incidents, comme déjà évoqué pourraient provoquer des dégâts importants sur les installations (impacts sur la productivité, sur les biens et les personnes) ou conduire à des fuites de données sensibles de l'organisation (secret de fabrication, savoirfaire, etc.).

Mais ces bonnes pratiques visent également à protéger les intervenants de maintenance pour :

- Ne pas mettre en danger leur sécurité, celle de leurs outils qui, en se connectant sur une installation compromise pourrait être impactés. Si ces outils viennent à se connecter sur les systèmes d'information de l'entreprise (dans le cas de maintenance externalisée), la compromission peut s'étendre à toute l'entreprise de maintenance et toucher par rebond d'autres systèmes industriels chez d'autres clients.
- Ne pas porter la « faute » en cas d'incident si l'incident n'est pas du fait de l'intervenant. Un incident de cybersécurité peut survenir lors d'une intervention de maintenance mais ne pas être lié à l'action de l'intervenant ou être lié à l'action de l'intervenant mais à la suite d'une mauvaise configuration des systèmes industriels n'étant pas du fait de l'intervenant. Dans ces cas, il est important d'apporter des éléments pour démontrer que l'intervenant de maintenance n'est pas le responsable de l'incident.

37 mesures constituent les bonnes pratiques, règles d'hygiène de la cybersécurité de la maintenance des installations industrielles. Elles sont présentées en prenant en compte les classes de cybersécurité des systèmes. Lorsque la classe des systèmes n'est pas connue des lecteurs, il est conseillé d'appliquer, à minima, les mesures proposées pour la classe 1. Les bonnes pratiques ci-dessous couvrent l'ensemble des opérations de maintenance définies au chapitre 2 de celui-ci. Par défaut, les mesures s'appliquent aux trois classes. **Lorsque rien n'est précisé pour une classe, les mesures de la classe inférieure s'appliquent.**

Remarque : *Le coût des mesures proposées est variable en fonction des organisations et de leur niveau de maturité en termes de cybersécurité. Il appartient à chaque organisation d'identifier les coûts générés pour chaque mesure et de préparer un plan d'actions adapté pour être en adhérence avec le guide. Le nombre de personnes concernées par les activités de maintenance, le niveau de sous-traitance ainsi que le nombre et la complexité des systèmes maintenus sont des critères impactant fortement le coût des mesures.*

ORGANISATION ET GOUVERNANCE

La question de la gouvernance des opérations de maintenance est fondamentale. Une gouvernance adaptée permettra d'intégrer intelligemment la cybersécurité dans les opérations de maintenance, de réduire les coûts de la cybersécurité et d'améliorer son efficacité. Définir la meilleure gouvernance pour intégrer la cybersécurité dans les opérations de maintenance ne relève certainement pas de ce guide. Ce sujet, complexe, demande une analyse propre à chaque organisation. Toutefois, il est fortement conseillé d'impliquer les personnes en charge de la cybersécurité des systèmes « dits » de gestion. Même si elles ne portent pas toujours la responsabilité de la cybersécurité des systèmes industriels, leurs connaissances, leur expérience en matière de cybersécurité et leur regard externe, s'avèrent précieux.

Répondre aux quelques questions suivantes amorcera les réflexions menant à définir la gouvernance qui conviendra à chacun :

- Qui pilote ou qui devrait piloter la cybersécurité pour les opérations de maintenance : les équipes cyber ? Les équipes de maintenance ? Un binôme ?
- Qui définit les procédures à suivre pour renforcer la cybersécurité lors des opérations de maintenance ?
- Qui est responsable en cas de problème, sachant que les impacts porteront potentiellement sur la productivité, la sécurité des biens et des personnes ou la perte de secrets de fabrication ?
- Qui fournit et qui dispose des ressources (financières, RH) et des compétences pour mener à bien les travaux ?
- A qui doit reporter le responsable de la cybersécurité pour les opérations de maintenance ?

4. PRÉREQUIS (EN AMONT DES INTERVENTIONS)

Les bonnes pratiques à prendre en compte avant les interventions de maintenance ont pour objectif d'intégrer le plus possible d'éléments de cybersécurité en amont pour réduire les risques lors des interventions sur les installations. Ce sont les prérequis à toute intervention. **Lorsque rien n'est précisé pour une classe, les mesures de la classe inférieure s'appliquent.**

Les mesures complémentaires proposées sont les suivantes :

M1 FORMATION SENSIBILISATION

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		Toutes les personnes concernées par la maintenance doivent être sensibilisées aux risques et formées aux bonnes pratiques.
CLASSE 2	Les personnes devraient atteindre un niveau minimum lors de l'évaluation.	En complément de la classe 1, les personnes sont évaluées.
CLASSE 3	La recommandation de la classe précédente s'applique.	En complément de la classe 2, les chefs d'équipes et personnes intervenant en amont des opérations de maintenance (lors des phases de préparation par exemple) sont formés à la cybersécurité des systèmes industriels, évalués et doivent obtenir un niveau minimum.

A noter : les formations doivent être adaptées au profil des intervenants et aux enjeux de leurs missions. De quelques heures pour une simple sensibilisation des opérateurs à 2-3 jours pour les chefs de projets par exemple, suivant le guide publié par l'ANSSI et donnant lieu au label SecNumEdu-FC.

M2 HABILITATION DES INTERVENANTS

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		
CLASSE 2	Les intervenants devraient être habilités par leur hiérarchie à intervenir sur les installations industrielles.	
CLASSE 3	La recommandation de la classe précédente s'applique.	La recommandation de la classe 2 devient obligatoire.

M3 INVENTAIRE ET CARTOGRAPHIE

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1	Les moyens et outils mis en œuvre pour les opérations de maintenance devraient être inventoriés et cartographiés, ainsi que les procédures et les intervenants.	
CLASSE 2	La recommandation de la classe précédente s'applique.	La mesure de la classe 1 devient obligatoire.
CLASSE 3	La recommandation de la classe précédente s'applique.	En complément de l'obligation de la classe précédente, l'inventaire et la cartographie doivent être revus annuellement.

M4 GOUVERNANCE

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1	La personne portant la responsabilité de la cybersécurité des opérations de maintenance devrait être formellement identifiée.	
CLASSE 2		La mesure de la classe 1 devient obligatoire.
CLASSE 3		La recommandation de la classe 1 devient obligatoire.

M5 DOCUMENTATION

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		Les procédures « métiers » accompagnées de check-lists doivent intégrer des éléments relatifs à la cybersécurité.
CLASSE 2	La documentation devrait intégrer la cartographie des systèmes (vue fonctionnelle, vue applicative, vue composant, vue architecture).	
CLASSE 3		La recommandation de la classe 2 devient obligatoire.

A noter : les cas d'usage publiés par ECC4iu illustrent les différents types de vues.

M6 TRAÇABILITÉ ET GESTION DES CONFIGURATIONS

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1	Gérer la traçabilité des actions et des configurations des composants de l'installation.	
CLASSE 2		La recommandation de la classe 1 devient obligatoire.
CLASSE 3		La GMAO pourrait être utilisée comme outil de traçabilité et de gestion des configurations.

M7 OUTILS DE MAINTENANCE ET SOLUTIONS DE TÉLÉMAINTENANCE

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		
CLASSE 2	Les outils de maintenance et de télémaintenance devraient être homologués.	Les postes sur lesquels sont exploités les outils de maintenance et de télémaintenance doivent être dédiés à ces activités (et ne pas être utilisés pour des usages tels que la bureautique, la navigation sur Internet, etc.).
CLASSE 3		Les outils sont dédiés aux systèmes à maintenir et doivent être homologués.

M8 MAINTIEN EN CONDITIONS DE SÉCURITÉ (MCS) DES OUTILS DE MAINTENANCE ET TÉLÉMAINTENANCE

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1	Assurer le MCS des outils de maintenance et télémaintenance. Utiliser la GMAO (ou un autre outil) pour traiter le MCS comme une opération de maintenance préventive périodique.	
CLASSE 2		Le MCS des outils de maintenance et solutions de télémaintenance doit être assuré.
CLASSE 3		Le MCS doit être vérifié et le cas échéant réalisé avant chaque intervention sur les systèmes.

M9 CONTRATS DE MAINTENANCE

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1	Insérer des clauses portant sur la cybersécurité dans les contrats de maintenance. Les contrats de maintenance, les contrats de supports techniques avec les équipementiers et intégrateurs devraient disposer de clauses relatives à la cybersécurité définissant clairement les périmètres d'intervention, les moyens mis en œuvre pour assurer la cybersécurité, quel niveau de cybersécurité est visé et les pénalités en cas d'incidents.	
CLASSE 2	La recommandation de la classe précédente s'applique.	La recommandation de la classe 1 devient obligatoire.
CLASSE 3	La recommandation de la classe précédente s'applique.	Les clauses contractuelles doivent être revues annuellement.

4. PRÉPARATION DES INTERVENTIONS (JUSTE AVANT)

Cette phase ne consiste pas à établir les procédures et check-lists nécessaires à l'intervention. Celles-ci doivent être définies au préalable lors de la préparation la maintenance. Cette phase se situe juste avant l'intervention (le jour « J »), entre les intervenants et les donneurs d'ordres.

Les mesures complémentaires proposées sont les suivantes :

M10 RAPPEL DES CONSIGNES

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		Les consignes de cybersécurité, et en particulier qui contacter en cas de problème, doivent être rappelées avant chaque intervention.
CLASSE 2		
CLASSE 3		

M11 VÉRIFICATION « PRÉ-JOB BRIEFING »

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1	Un « pré-job briefing » spécifique à chaque intervention doit être réalisé. Il permet notamment de vérifier : - Que toutes les procédures nécessaires à l'intervention sont disponibles et bien identifiées par les intervenants ; - Que les outils de maintenance qui seront utilisés sont bien les bons ; - Que les moyens nécessaires à la traçabilité des actions sont bien disponibles ; - Que les logiciels et mises à jour qui seront utilisés sont les bons et qu'ils soient intègres.	
CLASSE 2		La recommandation de la classe 1 devient une obligation.
CLASSE 3		

M12 « PHOTO » DE L'INSTALLATION

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1	Les logs « systèmes » et/ou applicatifs doivent être sauvegardés. Ces logs peuvent contenir d'éventuelles traces de problèmes de cybersécurité, latents ou déjà présents.	Les sauvegardes nécessaires pour remettre en service l'installation en cas de problème doivent être effectuées.
CLASSE 2		En plus de l'obligation de la classe précédente; la recommandation de la classe 1 devient une obligation.
CLASSE 3		

M13 MÉDIAS AMOVIBLES

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		L'innocuité des médias amovibles qui seront utilisés lors de l'intervention doit être vérifiée (au moyen d'une station de décontamination par exemple).
CLASSE 2		
CLASSE 3		

A noter : il faut être vigilant sur la qualité des sauvegardes et les capacités à les restaurer. Il est conseillé de se rapprocher des éditeurs de solutions et équipementiers pour connaître les procédures de sauvegarde des différents composants ainsi que les procédures de restauration. Il est fortement conseillé de tester les opérations pour s'assurer que les procédures sont bien maîtrisées et pourront être applicables en cas de besoin.

PENDANT LES INTERVENTIONS

Les risques liés aux interventions de maintenance sont les suivants :

- Connexion d'outils de maintenance présentant des failles de sécurité, voire, déjà compromis et impactant le système faisant l'objet de l'intervention de maintenance.
- Désactivation temporaire de fonctions de cybersécurité ouvrant ainsi une fenêtre pendant laquelle les systèmes sont vulnérables.
- Mise en place de configurations « provisoires » qui perdurent après l'intervention (exemple d'une connexion temporaire) et dégradent le niveau de cybersécurité de l'installation.
- Utilisation de médias amovibles non maîtrisés comportant potentiellement des codes malveillants.

Les mesures complémentaires proposées sont les suivantes :

M14 PROTECTION PHYSIQUE

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		Ne pas laisser les outils et la documentation utilisés lors de l'intervention dans des locaux sans accès contrôlés.
CLASSE 2		
CLASSE 3		

M15 OUTILS DE MAINTENANCE

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		Seuls les outils autorisés et prévus pour l'intervention doivent être utilisés. De même, seuls les médias amovibles approuvés (validés/vérifiés) par l'organisation doivent être utilisés.
CLASSE 2		
CLASSE 3		

M16 COMPTES

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1	Utiliser des comptes dédiés pour se connecter aux installations lorsque cela est techniquement possible et prévu.	
CLASSE 2		La recommandation de la classe 1 devient une obligation.
CLASSE 3		

M17 TRAÇABILITÉ DES ACTIONS

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		
CLASSE 2	Les actions réalisées lors de l'intervention sont « enregistrées » et consignées dans une main courante par exemple.	
CLASSE 3		La recommandation de la classe 2 devient une obligation. L'enregistrement peut être manuel et dans ce cas, réalisé par une personne dédiée, ou automatisé si les systèmes disposent de fonctions de ce type.

4.

M18 PILOTAGE

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1	Communiquer régulièrement avec le responsable de l'opération pour donner des points de situation et s'assurer qu'il n'y a pas d'effet de bord liés à l'intervention.	
CLASSE 2		La recommandation de la classe 1 devient une obligation.
CLASSE 3		

M19 SUPPORTS TECHNIQUES

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1	Les autres formes d'aide « en ligne » (via les forums sur Internet) ne sont pas recommandées.	Seuls les supports techniques validés par l'organisation doivent être utilisés.
CLASSE 2		
CLASSE 3		

APRÈS LES INTERVENTIONS

Les risques après l'intervention sont les suivants :

- De ne pas sauvegarder les éventuelles modifications apportées ce qui pourrait conduire à restaurer une mauvaise version et impacter fortement les systèmes.
- De ne pas mettre à jour la documentation de l'installation ce qui pourrait conduire à de mauvaises manipulations ultérieures.
- De laisser actif des configurations provisoires, nécessaires pour l'intervention, dégradant le niveau de cybersécurité de l'installation.

Les mesures complémentaires proposées sont les suivantes :

M20 PHOTO DE L'INSTALLATION

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1	Sauvegarder les logs « systèmes » et logs « applicatifs » pour conserver des « preuves » du bon fonctionnement des installations.	Sauvegarder les modifications éventuelles de configurations ayant été apportées pour corriger un bug. Les sauvegardes doivent être réalisées dans une version « compilée » et « non compilée ».
CLASSE 2		
CLASSE 3		

M21 MISE À JOUR DE LA DOCUMENTATION

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		La documentation, dont la cartographie et l'inventaire doivent être mis à jour. Il se peut en effet que lors de l'opération de maintenance les intervenants découvrent que les documents ne sont pas à jour, qu'il manque une IHM dans l'inventaire ou un équipement qui était « caché » dans une armoire courant faible.
CLASSE 2		
CLASSE 3		

M22 VÉRIFICATION DES MODIFICATIONS

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		Les modifications ayant été apportées pour corriger un dysfonctionnement doivent être vérifiées afin de s'assurer qu'elles n'interfèrent pas avec les fonctions de cybersécurité existantes.
CLASSE 2		
CLASSE 3		

M23 CONTRÔLE

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1	Une check-list devrait être utilisée pour réaliser le contrôle	Un contrôle doit être réalisé afin de s'assurer de l'absence de vulnérabilités « évidentes » (console non déconnectée, portes laissées ouvertes, médias amovibles oubliés sur un équipement, session non verrouillée ou non fermée, etc.) après l'intervention.
CLASSE 2		
CLASSE 3		

M24 RAPPORT D'INTERVENTION

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		Un rapport d'intervention dans lequel seront reportées toutes les actions réalisées (celles qui étaient prévues et qui figurent dans le permis de travail et/ou check-list d'intervention et celles qu'il a été nécessaire d'ajouter) doit être réalisé.
CLASSE 2		
CLASSE 3		

M25 DEBRIEFING

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1	Procéder à un « Débriefing » pour capitaliser sur ce qui a bien fonctionné, les éventuelles difficultés rencontrées et les points sur lesquels une amélioration est nécessaire.	
CLASSE 2		La recommandation de la classe 1 devient une obligation.
CLASSE 3		Le debriefing doit intervenir à chaud, immédiatement après l'intervention et à froid, quelques temps après.

M26 VALIDATION RÉCEPTION

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		La bonne conduite de l'intervention doit être validée avec le donneur d'ordre et l'intervention doit être formellement réceptionnée.
CLASSE 2		
CLASSE 3		

M27 PÉRIODE DE SURVEILLANCE VIGILANCE

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1	Définir une période de vigilance afin de s'assurer qu'il n'y a pas de dérive dans les heures, les jours qui suivent l'intervention.	
CLASSE 2		La recommandation de la classe 1 devient une obligation.
CLASSE 3		

4. CAS PARTICULIER DES INTERVENTIONS À DISTANCE (TÉLÉMAINTENANCE)

Rappel des mesures du guide [Méthode de classification et mesures principales] : la télémaintenance n'est pas autorisée pour les systèmes de classe 3 et n'est pas recommandée pour les systèmes de classe 2 lorsque qu'elle est « NON MAÎTRISÉE ». La télémaintenance est considérée « NON MAÎTRISÉE » lorsque l'ensemble de la chaîne de télémaintenance ne dispose pas du même niveau de confiance que le système sur lequel est opérée la télémaintenance.

Ceci est à distinguer du cas de figure où un intervenant, appartenant à l'organisation, et habilité, se connecte depuis un site maîtrisé par l'organisation et depuis un système de même classe que le système télé-maintenu, et via une connexion offrant le même niveau de confiance et de cybersécurité. Dans ce cas, la télémaintenance peut être considérée « MAÎTRISÉE ».

Comme pour toute intervention de maintenance, les interventions de télémaintenance présentent des risques en termes de cybersécurité dans la mesure où une personne, disposant de privilèges pour modifier des configurations d'équipements, peut se connecter sur les systèmes et peut en modifier en profondeur le fonctionnement ; même si l'objet de la connexion se limite à du télédiagnostic. La supervision de l'opération de télémaintenance est complexe compte tenu de l'éloignement physique du télé-mainteneur. Cette phase ne consiste pas à établir les procédures et check-lists nécessaires à l'intervention. Celles-ci doivent être définies au préalable lors de la préparation la maintenance. Cette phase se situe juste avant l'intervention (le jour « J »), entre les intervenants et les donneurs d'ordres.

Ce type d'interventions conduit couramment aux risques supplémentaires suivants :

- La non-maîtrise des outils et de l'environnement utilisés par le télé-mainteneur. Dans une majorité des cas constatés, la télémaintenance est réalisée depuis le PC portable d'un intégrateur, PC utilisé pour les travaux de tous les jours, chez tous ses clients et permettant également de se connecter à internet, consulter des emails, etc.
- Les moyens de télémaintenance légitimes peuvent être utilisés par une personne n'en n'ayant pas l'autorisation. Une personne réussissant à voler ou à cloner les moyens de télémaintenance pourra se faire passer pour un utilisateur légitime et ne sera pas ou difficilement détectée.
- Une faille de sécurité dans les solutions déployées expose le système télé-maintenu.

Les mesures complémentaires proposées sont les suivantes :

M28 ÉTABLISSEMENT DE LA CONNEXION

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1	Il est recommandé que la procédure de rappel soit réalisée manuellement et non de manière automatisée par une fonction de « call-back » par exemple.	L'établissement de la connexion depuis le système maintenu doit faire l'objet d'une procédure de rappel du télé-mainteneur.
CLASSE 2		
CLASSE 3		

M29 LIMITATION DE LA CONNEXION

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		La connexion établie pour l'intervention de télémaintenance doit être limitée à une durée appropriée à l'opération. La limitation peut consister en un appel vers le télé-mainteneur lorsque le temps est dépassé pour lui notifier qu'il va être déconnecté.
CLASSE 2		La limitation de la durée de connexion doit être automatique. La connexion doit être coupée lorsque le délai est dépassé, en utilisant par exemple une minuterie physique.
CLASSE 3		L'obligation de la classe précédente s'applique.

M30 TRAÇABILITÉ DES ACTIONS

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1	La traçabilité des actions devrait être renforcée par des fonctions d'enregistrement et de détection d'incident de sécurité.	
CLASSE 2		La recommandation de la classe 1 devient une obligation.
CLASSE 3		

Remarques sur la traçabilité :
- L'enregistrement des flux de communication entrant sur le système télé-maintenu est une solution efficace et peu coûteuse. Néanmoins, cette solution « bas niveau » peut se révéler peu commode à exploiter pour identifier les causes d'un incident.
- La collecte des logs, sur site, après l'intervention est également une source de traçabilité à condition toutefois qu'ils n'aient pas été modifiés (intentionnellement ou non) lors de l'intervention. Un attaquant cherchant à pénétrer dans le système sans se faire remarquer, cherchera en effet à effacer toute trace de son passage.

M31 IDENTIFIANT DE CONNEXION

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		
CLASSE 2	Il est recommandé de changer les identifiants de connexion après chaque intervention.	Les identifiants de connexion doivent être changés une fois par an au minimum.
CLASSE 3	La recommandation de la classe précédente s'applique.	L'obligation de la classe précédente s'applique.

En complément des mesures proposées, il est recommandé de lire les cas d'usage publiés par ECC4iu qui proposent des mesures pour renforcer la cybersécurité des solutions de télémaintenance.

CAS PARTICULIERS LIÉS AUX OPÉRATIONS DE MAINTENANCE CURATIVE (NON PLANIFIÉES)

Ce type d'opération, particulièrement à risque d'un point de vue de la cybersécurité, nécessite de renforcer les mesures et de mettre en place des procédures « bris de glace » ou dérogatoires pour que les intervenants puissent de manière exceptionnelle intervenir au plus vite pour remettre en service les installations.

L'urgence de l'intervention conduit couramment aux risques supplémentaires suivants :
- Connexion dans l'urgence d'équipements potentiellement « non maîtrisés ».
- Tendance à ne pas suivre les procédures habituelles pour « aller vite ».
- Les fonctions de cybersécurité existantes peuvent être « shuntées » pour s'assurer qu'elles ne sont pas la cause de la panne et pour faciliter l'intervention des équipes de maintenance.
- Interventions potentielles de personnes non « habituelles » comme de personnes de support technique de constructeurs par exemple ou des personnes d'astreintes non formées, non habituées à la cybersécurité, à ses bonnes pratiques et qui ne connaissent pas les installations.

En effet, ce type d'opération est souvent soumis aux contraintes suivantes :
- Besoin d'intervenir rapidement pour limiter les impacts sur la productivité de l'organisation par exemple.
- Intervention potentiellement hors des horaires habituels, pendant lesquels les équipes sont en effectif réduit.
- Les moyens nécessaires pour réaliser l'intervention ne sont pas nécessairement tous disponibles
- Stress de l'intervention

4.

Les mesures complémentaires proposées sont les suivantes :

M32 PROCÉDURE

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		
CLASSE 2	Les interventions curatives non planifiées devraient suivre un processus de maintenance planifiée et être encadrées par les procédures associées. La planification peut être réalisée rapidement si les procédures sont adaptées pour cela.	
CLASSE 3		La recommandation de la classe 2 devient une obligation.

M33 SUPERVISION DE L'INTERVENTION

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		Une personne, interne à l'organisation, formée à la cybersécurité, devrait être présente pour superviser l'intervention afin d'évaluer au fil de l'eau si les actions sur le point d'être réalisées présentent des risques immédiats en termes de cybersécurité.
CLASSE 2		
CLASSE 3		

M34 VÉRIFICATION

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1	S'appuyer sur une check-list, telle que celle déroulée lors des interventions de maintenance évolutive.	Il doit être procédé à des opérations de vérification après l'intervention afin de s'assurer que tous les « shunts » / modes bris de glace ont été supprimés et que les fonctions de cybersécurité sont bien en place.
CLASSE 2		La recommandation précédente devient une obligation en plus de l'obligation de la classe précédente.
CLASSE 3		

CAS PARTICULIERS LIÉS AUX OPÉRATIONS DE MAINTENANCE ÉVOLUTIVE

Les mises à jour de sécurité telles que les correctifs ou les signatures d'antivirus par exemple soulèvent une question de fond. Ces opérations, visant à assurer le MCS des installations, doivent-elles être considérées comme des opérations de maintenance évolutive dans la mesure où elles modifient potentiellement le fonctionnement du système sans pour autant apporter d'évolutions du périmètre fonctionnel ? Il n'existe pas de réponse unique. Chaque organisation choisira d'intégrer ou non ce type d'intervention de MCS dans les opérations de maintenance évolutive.

Ce type d'interventions conduit couramment aux risques supplémentaires suivants :

- Régression et dégradation du niveau de cybersécurité par des interactions non souhaitées avec les éventuelles fonctions de cybersécurité du système.
- Effet de bord conduisant à des dysfonctionnements ultérieurs.

Les mesures complémentaires proposées sont les suivantes :

M35 PROCÉDURE

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		
CLASSE 2	Les opérations de maintenance évolutive devraient être réalisées selon les procédures d'intégration de nouvelles fonctionnalités et ne pas être traitées comme une maintenance.	
CLASSE 3		La recommandation de la classe 2 devient une obligation.

A noter : sur certains systèmes, des modifications « simples » telles que le changement de mot de passe, demandent de recharger une configuration sur l'équipement. Cela peut être le cas sur certains PLC. Ces modifications doivent être considérées comme des maintenances évolutives.

M36 IDENTIFIANT DES MODIFICATIONS

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		Les modifications qui seront apportées aux installations doivent être clairement identifiées.
CLASSE 2		
CLASSE 3		

M37 TESTS ET VALIDATIONS

	RECOMMANDÉE	OBLIGATOIRE
CLASSE 1		Les modifications doivent être testées afin de s'assurer de la non régression des éventuelles fonctions de cybersécurité existantes et doivent être validées avec le donneur d'ordres afin de s'assurer que seules les modifications légitimes ont été apportées.
CLASSE 2		
CLASSE 3		

5. CONCLUSION

Les activités de maintenance, nécessaires au bon fonctionnement des installations industrielles, présentent de nombreux risques en termes de cybersécurité et cela, quelles que soient les mesures de cybersécurité prévues lors de leur conception et a fortiori lorsqu'elles sont inexistantes.
Les différents types de maintenance, dont les principaux sont abordés dans ce guide, introduisent des risques différents mais tous conduisent in fine au dysfonctionnement des installations à des degrés de gravité plus ou moins sévères.
La télémaintenance en particulier, aujourd'hui incontournable qu'on le veuille ou non, augmente les risques d'incidents.

Si les mesures de sûreté de fonctionnement et les mesures qualité, fréquentes dans le monde des systèmes industriels, agissent positivement comme des garde-fous, elles ne suffisent pas pour autant à réduire les risques à un niveau suffisant. Néanmoins, il est important de souligner la contribution de ces démarches à la cybersécurité.

Les 37 mesures proposées dans ce guide visent à réduire les facteurs de risque d'incident de cybersécurité lors des interventions de maintenance dont une part importante provient de l'humain. Sur le principe des guides de l'ANSSI, les mesures se déclinent en fonction de la classe du système sur lequel est réalisée la maintenance.

La formation des intervenants et l'encadrement des interventions par des procédures prenant en compte la cybersécurité sont sans aucun doute les mesures les plus efficaces, celles qui présentent le retour sur investissement le plus élevé. Les « mauvaises pratiques » acquises au fil des années, doivent être progressivement éradiquées et remplacées par des bonnes pratiques bénéfiques à tout le monde et en premier lieu, aux intervenants de maintenance : repositionner l'humain au coeur du dispositif de la cybersécurité, valoriser son travail et en faire un acteur essentiel et reconnu constitue un premier challenge, c'est une certitude !

L'amélioration de la cybersécurité des outils utilisés lors des interventions ainsi que les usages associés à ces outils constituent un enjeu de taille et certainement un deuxième challenge. Ne plus utiliser de « console de programmation » pour également surfer sur Internet et lire ses mails par exemple, demandera à ne pas en douter encore quelques efforts. Pourtant la cybersécurité est à ce prix.

Enfin, la cybersécurité lors des opérations de maintenance soulève la question de fond de la responsabilité en cas d'incident. Si cette problématique n'est pas nouvelle dans les métiers de la maintenance, la cybersécurité introduit de nouvelles problématiques pas ou peu souvent prises en compte. Les clauses contractuelles précisant les limites de responsabilité, l'application rigoureuse des procédures définies et l'amélioration de la traçabilité deviennent indispensables et apporteront des aides précieuses en cas de litige.

BIBLIOGRAPHIE ET RÉFÉRENCES

- **Guides ANSSI :**
  - Maîtriser la SSI pour les systèmes industriels
  - Cas pratique
  - Méthode de classification et mesures principales
  - Les mesures détaillées
  - Le référentiel d'exigences pour les prestataires d'intégration et de maintenance de systèmes industriels (PIMSEC)
  - Guide pour une formation sur la cybersécurité des systèmes industriels
  - Guide d'hygiène informatique
  - L'homologation en 9 étapes

- **La norme NF 13306 relative à la maintenance industrielle**

GLOSSAIRE

INTITULÉ	DÉFINITION
COMPROMISSION	Prise de connaissance, certaine ou probable, d'une information ou d'un support protégé par une ou plusieurs personnes non-autorisées.
DISPONIBILITÉ	Aptitude d'une fonction à rendre le service attendu en temps voulu et dans les conditions d'usage prévu.
FAILLE	Vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.
INCIDENT DE SÉCURITÉ (AU SENS CYBER)	Un incident de sécurité est indiqué par un ou plusieurs évènement(s) de sécurité de l'information indésirable(s) ou inattendu(s) présentant une probabilité de compromettre les opérations liées à l'activité de l'organisme et/ou de menacer la sécurité de l'information.
INTÉGRITÉ	Propriété permettant de garantir l'exactitude, la fiabilité et l'exhaustivité des informations et des méthodes de traitement.
MESURE	Moyen de gérer un risque, comprenant la politique, les procédures, les lignes directrices, et les pratiques ou structure organisationnelles, et pouvant être de nature administrative, technique, gestionnaire ou juridique.
MENACE	Cause potentielle d'un incident indésirable, pouvant entraîner des dommages au sein d'un système ou d'un organisme.
RISQUE	Combinaison de la probabilité d'un événement de sécurité et de ses conséquences.
SOUS-TRAITANCE	Opération par laquelle le prestataire confie sous sa responsabilité à une entité tout ou partie de l'exécution d'un contrat conclu avec le commanditaire.
STATION D'INGÉNIERIE	Equipement informatique disposant des progiciels de paramétrage, de conception, de programmation, d'administration des équipements industriels comme les automates et les SCADA. Cet équipement est connecté sur le réseau industriel et mis à disposition des équipes de maintenance, d'ingénierie, de support, etc.
SÛRETÉ DE FONCTIONNEMENT	Etude 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.
SYSTÈMES D'INFORMATION SENSIBLES	Système qui traitent d ' informations dont la divulgation à des personnes non autorisées, l'altération ou l'indisponibilité sont de nature à porter atteinte à la réalisation des objectifs des entités qui les mettent en oeuvre.
TRAÇABILITÉ	Propriété permettant de fournir les moyens de preuve et de contrôle sur les informations et les méthodes de traitement.
TÉLÉMAINTENANCE	Action d'effectuer à distance, sous-entendu depuis l'extérieur des systèmes d'information de l'entité responsable, des tâches de maintenance sur des installations techniques. Ceci implique notamment de pouvoir faire des modifications de paramétrages ou de programmes.
VULNÉRABILITÉ	Faiblesse d'un bien ou d'un groupe de biens pouvant faire l'objet d'une menace.

LISTE DES ACRONYMES

INTITULÉ	DÉFINITION
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
GED	Gestion électronique de documents
GMAO	Gestion de la maintenance assistée par ordinateur
IHM	Interface homme machine
MCO	Maintien en condition opérationnelle
MCS	Maintien en condition de sécurité
OIV	Organismes d'Importance Vitale
OSE	Opérateur de service essentiel
PLC	Programmable logic controller
SCADA	Supervisory Control and Data Acquisition

INDEX PAR THÉMATIQUE

PAGE	THÉMATIQUE
10, 11, 14	Formation
11, 16, 17, 19	Médias amovibles
6, 10, 15, 20, 21	Télémaintenance
12, 15, 16, 17	Outils de maintenances
17	Accès physique
7, 11, 15, 16, 17, 21	Traçabilité
10, 13	Coût de la cybersécurité
14, 15, 18	Cartographie pour la maintenance
4	Aspects contractuels
9, 10, 15	Outils d'aide à la maintenance
11, 13, 14	Organisation et gouvernance
12, 18	Forum de discussion et réseaux sociaux

SOURCES

- Prestataires de détection des incidents de sécurité
- Prestataires de réponse aux incidents de sécurité
- Prestataires d'audit de la sécurité des systèmes d'information
- INSTRUCTION INTERMINISTÉRIELLE RELATIVE À LA PROTECTION DES SYSTÈMES D'INFORMATION SENSIBLES n° 901/SGDSN/ANSSI
- Instruction Relative à la procédure expérimentale de qualification des prestataires de services de confiance
- Processus de qualification d'un prestataire de services de confiance
- Maîtriser les risques de l'infogérance
- Référentiel de qualification de prestataires de services sécurisés d'informatique en nuage (cloud computing) - référentiel d'exigences
- PSSIE
- Formation à la cybersécurité des systèmes industriels - Cahier des charges
- Référentiel d'exigences pour la qualification des prestataires d'intégration et de maintenance de systèmes industriels spécialisés en cybersécurité
- Cybersécurité des systèmes industriels - Méthode de classification et mesures principales

CYBERSÉCURITÉ

POUR LA MAINTENANCE DES INSTALLATIONS INDUSTRIELLES

DECEMBRE 2018

Ces cas d'usages ont été réalisés par l'Association ECC4iu avec le concours des sociétés suivantes :
- Alstom
- Assystem
- Automatique et Industrie
- Calasys
- Ekium
- Siemens
- Stormshield
- Thales

Certitude Numérique a accompagné l'Association ECC4iu dans la rédaction des contenus.

A PROPOS...

ECC4iu est le cluster Européen dédié à la cybersécurité des systèmes industriels et urbains rassemblant l'ensemble des parties prenantes dans un écosystème de confiance depuis le 11 Juillet 2017 à Lyon. Cette association a pour vocation d'accompagner tout type de projets et/ou initiatives en rapport avec la sécurité des systèmes industriels et urbains.

ECC The European CYBERSECURITY CLUSTER for Industrial and Urban Systems iu

contact[at]ecc4iu.eu
www.ecc4iu.eu