SYSTÈMES DE CONTRÔLE-COMMANDE INDUSTRIELS

Table des matières

Liste des figures

1.0 OBJET DE LA PRÉSENTE FICHE TECHNIQUE

Cette fiche technique fournit des recommandations de prévention des sinistres pour les systèmes de contrôle-commande industriels (SCI) en utilisant une approche systémique pour évaluer l'ensemble des SCI d'un site, y compris les réseaux de communication SCI et les cyber-risques. L'objectif de ce document est de proposer des solutions pour réduire les risques, dans une optique de protection des biens et de continuité des activités.

Dans le cadre du présent document, un SCI désigne un ensemble de systèmes matériels et de programmes logiciels qui assure le contrôle, la protection et la surveillance des procédés, de la production, de la fabrication et des activités connexes au sein d'installations industrielles et non industrielles. La liste suivante, non exhaustive, donne des exemples d'équipements matériels pouvant être connectés au réseau SCI :

- système de supervision et contrôle à distance (SCADA) ;
- système numérique de contrôle-commande (DCS), dont les logiciels d'historisation ;
- automate programmable industriel (API) ;
- contrôleur d'automatisation programmable (PAC) ;
- passerelle FDG ;
- unité de terminal à distance (RTU) ;
- Périphériques réseaux, y compris commutateurs, pare-feux, routeurs, etc. ;
- appareils de terrain intelligents (par exemple, compteurs, vannes, relais et transmetteurs de process intelligents) ;
- bus d'instrument ;
- interface homme-machine (IHM) ;
- station ingénierie ;
- tableaux de commande industriels, dont les armoires d'équipements et d'instrumentation, les armoires d'entrées/sorties (E/S), etc. ;
- système de gestion technique des bâtiments ;
- appareils intelligents ou Internet industriel des objets (IIoT).

Cette fiche technique fournit des recommandations générales concernant les systèmes de contrôle-commande industriels. Si des fiches techniques plus détaillées sur des équipements ou procédés spécifiques sont disponibles, elles remplacent les recommandations de ce document.

Cette fiche technique ne couvre pas les points suivants :

- conception détaillée ou exploitation des équipements SCI ou des dispositifs de communication/réseau ;
- performances, compatibilité ou fonctionnalités des logiciels ;
- conception, exploitation, inspection, essai et maintenance des systèmes instrumentés de sécurité (voir la fiche technique de prévention des sinistres 7-45 de FM, *Safety Controls, Alarms, and Interlocks*) ;
- systèmes informatiques utilisés pour les activités d'ordre général (par exemple, systèmes d'envoi et de réception d'e-mails, systèmes d'accès à Internet).

1.1 Risque

Si la gestion et la maintenance des systèmes SCI ne sont pas adéquates, des dysfonctionnements mineurs peuvent prendre des proportions considérables, entraînant l'interruption de la production et/ou des dommages matériels potentiellement importants. De nombreux facteurs peuvent entraîner des défaillances du système de contrôle-commande, y compris des actes de cyber-malveillance visant à perturber le fonctionnement des SCI et l'absence de procédure de gestion des incidents et de plan de reprise d'activité après un cyber-incident.

1.2 Modifications

Juillet 2024. Révision intermédiaire. Des changements éditoriaux ont été apportés.

2.0 RECOMMANDATIONS RELATIVES À LA PRÉVENTION DES SINISTRES

2.1 Introduction

Chaque SCI fonctionne différemment selon le secteur d'activité auquel il est destiné. Il n'existe donc pas deux SCI identiques. Les SCI sont des systèmes complexes comprenant des contrôleurs, des unités logiques programmables, des moteurs, des pompes, des actionneurs, des équipements de surveillance et de détection, etc., tous connectés via des réseaux de communication.

Sur un site, il est primordial que le personnel en charge de l'ensemble des SCI en comprenne parfaitement le fonctionnement, les contraintes d'exploitation, les exigences de protection, les réseaux de communication et les logiciels nécessaires, afin de pouvoir identifier collectivement les risques inhérents à l'ensemble de ces systèmes.

2.2 Construction et emplacement

2.2.1 Installer les salles de commande des procédés et les locaux techniques importants en dehors des zones exposées au risque d'explosion. À défaut, prévoir une construction résistante à la pression conçue conformément à la fiche technique 1-44, *Damage-Limiting Construction*, en supposant que la surpression soit appliquée à la surface extérieure de la salle de commande. Pour les fenêtres, il est recommandé d'utiliser du verre feuilleté certifié ANSI Z97.1 (les normes ASTM E1886 et E1996, ou FBC TAS 201 et 203, sont également acceptables) pour la résistance aux impacts et certifié ASTM E1300 pour la surpression requise.

2.2.2 Installer les salles de commande des procédés et les locaux techniques associés de façon à ne pas les exposer à des dommages causés par des liquides corrosifs ou qui peuvent brûler, des vapeurs inflammables ou des équipements mécaniques tels que des ponts roulants.

2.2.3 Pour les salles de commande des procédés et les locaux techniques situés en hauteur et exposés à un risque d'incendie, prévoir un revêtement ignifuge adapté au risque (minimum une heure) au niveau des éléments de structure en acier.

2.2.4 Construire les salles de commande des procédés, les salles de contrôle et les locaux d'instrumentation de contrôle-commande industriel correspondants (c'est-à-dire les locaux abritant le système d'entrée/sortie) et/ou les tableaux de commande industriels avec des matériaux incombustibles. Cette construction concerne également, sans s'y limiter, les faux plafonds, les faux planchers, les murs de séparation, le mobilier, les matériaux d'isolation des tuyauteries et des systèmes de chauffage, ventilation et climatisation, ainsi que les filtres de ces systèmes.

Si des matériaux en plastique sont utilisés, veiller à ce qu'ils soient agréés FM ou testés selon les règles suivantes :

A. FM Approval Standard 4882, *Class 1 Interior Wall and Ceiling Materials or Systems for Smoke Sensitive Occupancies*

B. FM Approval Standard 4884, *Panels Used in Data Processing Center Hot and Cold Aisle Containment Systems*

C. ANSI/FM Approval Standard 4910, *Cleanroom Materials Flammability Test Protocol*

2.2.5 Prévoir une séparation présentant une résistance au feu d'une heure minimum entre les salles de commande des procédés et les zones adjacentes, y compris les locaux techniques et TGBT. Cette recommandation ne s'applique pas aux équipements autonomes situés à l'extérieur de la salle de commande des procédés.

2.2.6 Lorsque des systèmes de contrôle-commande des procédés redondants sont installés, placer les commandes, les équipements et les câbles de chaque système dans une zone coupe-feu séparée.

2.2.7 Prévoir des zones séparées pour les vestiaires, les salles de déjeuner, les cuisines, les salles de réunion, les bureaux, etc.

2.2.8 Obturer les ouvertures dans les planchers et murs coupe-feu traversés par des canalisations, des fils et des câbles, à l'aide d'un matériau agréé FM ou répertorié présentant une résistance au feu équivalente à celle du plancher ou du mur.

2.2.9 Acheminer les dispositifs d'évacuation des eaux de pluie en toiture, les canalisations d'eau domestique et autres conduites de liquides de sorte qu'ils contournent les salles de commande des procédés et les locaux techniques associés. Dans les bâtiments à plusieurs étages, étanchéifier le plancher situé au-dessus. Lorsqu'il n'est pas possible de faire passer les canalisations à distance de ces zones, installer une rétention (par exemple, une conduite concentrique) ou un bac récepteur, ainsi qu'un système de détection de fuite agréé FM avec transmission des alarmes vers un lieu occupé en permanence. Pour plus de détails, voir la fiche technique 1-24, *Protection Against Liquid Damage*.

2.2.10 Installer des systèmes d'évacuation au sol sous les faux planchers si de l'eau ou d'autres liquides sont susceptibles de s'accumuler.

2.2.11 Construire les tableaux de commande industriels, y compris les portes et/ou panneaux d'accès, avec des matériaux incombustibles. Respecter les normes internationales.

2.3 Protection

2.3.1 Protéger les salles de commande des procédés ainsi que les locaux techniques et tableaux de commande industriels correspondants contre le risque de feu externe conformément à la fiche technique 1-20, Protection Against Exterior Fire Exposure.

2.3.2 Prévoir un système de détection de fumée agréé FM pour les salles de commande des procédés, les salles de contrôle des procédés et les locaux techniques correspondants, avec un report d'alarme vers un poste de travail ou un lieu occupé en permanence.

2.3.3 Lorsqu'un niveau de détection supérieur est souhaité pour les systèmes stratégiques et/ou de sécurité, prévoir un système de détection de fumée de type très précoce dans le local technique et/ou à l'intérieur du tableau de commande industriel avec un report d'alarme vers un lieu occupé en permanence. Utiliser, selon les cas, un détecteur par aspiration ou un détecteur ponctuel ultrasensible correspondant à la configuration de l'enceinte.

2.3.4 Installer un système de détection de fumée agréé FM sous les faux planchers et au-dessus des plafonds où passent des câbles.

2.3.5 Installer un système de détection de fumée conformément à la fiche technique 5-48, *Automatic Fire Detection*.

2.3.6 Installer une protection incendie pour les salles de commande des procédés, les salles de contrôle ou les locaux d'instrumentation de contrôle-commande industriel comme suit :

2.3.6.1 Locaux avec matériaux de construction combustibles

A. Installer une protection sprinkleur automatique sous eau ou à préaction dotée de sprinkleurs automatiques à réponse rapide. Utiliser des critères de conception, des demandes en eau des lances incendie et une durée de l'alimentation en eau conformes à la fiche technique 3-26, *Protection incendie pour les activités hors stockage*.

B. Prévoir un système d'extinction à brouillard d'eau automatique agréé FM spécifiquement adapté aux locaux abritant des équipements informatiques et installé conformément à la fiche technique 4-2, *Water Mist Systems* ainsi qu'au manuel de conception, d'installation, d'exploitation et de maintenance du fabricant indiqué dans la liste des produits agréés FM. Installer une source d'eau permettant d'alimenter le système d'extinction à brouillard d'eau pendant 60 minutes.

Pour les points A et B ci-dessus :

- Utiliser la catégorie de risque 1 (HC-1) pour les salles de commande des procédés et les salles de contrôle dont la hauteur de plafond ne dépasse pas 9 m.
- Utiliser la catégorie de risque 2 (HC-2) pour les locaux d'instrumentation de contrôle-commande industriel des procédés ou les salles de commande des procédés et les salles de contrôle dont la hauteur de plafond est supérieure à 9 m.

2.3.6.2 Locaux avec matériaux de construction incombustibles

Installer un système d'extinction incendie à halocarbure ou à gaz inerte (agent propre) conformément aux instructions du fabricant et à la fiche technique 4-9, *Halocarbon and Inert Gas (Clean Agent) Fire Extinguishing Systems*. Une protection sprinkleur automatique sous eau ou à préaction ou des systèmes d'extinction à brouillard d'eau (conformément à la section 2.3.6.1 ci-dessus) sont également acceptables.

Pour les systèmes d'extinction incendie à halocarbure ou à gaz inerte (agent propre), s'assurer que les conditions suivantes sont remplies :

1. Système de détection de fumée de type très précoce ou dispositif de mise hors tension automatique du local et des équipements (à l'exception de l'éclairage de secours) en cas de détection de fumée, dès lors qu'une analyse des risques liés aux procédés ou une évaluation similaire démontre qu'une mise hors tension automatique n'endommagera pas l'équipement commandé (c'est-à-dire l'équipement de production) et/ou n'introduira aucun risque.
   a. Lorsqu'un dispositif de mise hors tension automatique est prévu, il doit être installé en tenant compte de l'isolement électrique des équipements informatiques et des systèmes de chauffage, de ventilation et de climatisation, conformément à la fiche technique 5-32.
   b. Pour basculer le procédé en mode sécurité, il est nécessaire d'ajuster le délai de mise hors tension, avec un facteur de sécurité de deux, de sorte qu'il ne dépasse pas le temps d'application du système d'extinction incendie à halocarbure ou à gaz inerte (agent propre).
2. Un système de détection de fumée de type très précoce avec une alarme/un signal de surveillance, est installé, afin que l'opérateur ou l'équipe d'intervention ait le temps de procéder à des vérifications avant la décharge du système d'extinction à agent propre.
3. Les équipements sont dotés d'enceintes métalliques.
4. L'utilisation de papier et d'autres matériaux combustibles est réduite au strict minimum dans le local.
5. Le stockage de matériaux d'emballage ou de cassettes en plastique est proscrit dans le local. **Remarque :** cette mesure inclut tous les supports combustibles (par exemple, bandes magnétiques).
6. Un dispositif d'arrêt et/ou un clapet est installé sur les systèmes de ventilation qui utilisent de l'air d'appoint ou de reprise.

2.3.7 Protéger les équipements de commande des procédés du site. Tenir compte de la criticité du procédé physique et des conséquences de la destruction du système de commande des procédés en cas d'incendie. Voir la section 3.1, Protection incendie pour les équipements de commande industriels. Installer l'un des équipements suivants (A ou B) :

A. Armoires incombustibles avec des cloisons, afin de limiter les dommages au strict minimum.

B. Un système d'extinction incendie à halocarbure ou à gaz inerte (agent propre) dans le local, à condition que les armoires soient ventilées et/ou agencées pour permettre un écoulement vers l'intérieur. Suivre les indications de la section 2.3.6.2 ci-dessus.

2.3.8 Installer une protection sprinkleur automatique conformément à la fiche technique 3-26, *Protection incendie pour les activités hors stockage* dans tous les espaces du bâtiment à proximité des salles de commande et de contrôle (y compris, sans s'y limiter, les bureaux, les espaces de repos, les archives, les zones nécessitant un permis, les salles de conférence, les salles de formation, les toilettes, etc.), selon la classification de risque correspondant à l'activité.

2.3.9 Installer les systèmes de protection incendie conformément à la fiche technique 2-0, *Guide d'installation des sprinkleurs automatiques*, et à la fiche technique relative au système de protection spécial applicable.

2.3.10 Protéger les data centers desservant les salles de commande des procédés conformément à la fiche technique 5-32, *Data Centers and Related Facilities*. Effectuer une analyse des risques liés aux procédés avant d'autoriser un arrêt automatique.

2.3.11 Protéger les groupes électrogènes conformément à la fiche technique 5-23, *Design and Protection for Emergency and Standby Power Systems*.

2.3.12 Protéger les groupes et chemins de câbles conformément à la fiche technique 5-31, *Cables and Bus Bars*.

2.3.13 Installer des extincteurs portables au dioxyde de carbone ou à agent propre (classe C) indiqués pour les risques électriques, afin de protéger les équipements électroniques conformément à la fiche technique 4-5, *Portable Extinguishers*.

2.3.13.1 Ne pas utiliser d'extincteurs à poudre sèche dans les locaux abritant des équipements électroniques.

2.3.13.2 Pour les matériaux combustibles ordinaires, utiliser un type ou plusieurs types d'extincteurs portables adaptés, conformément à la fiche technique 4-5, *Portable Extinguishers*.

2.3.14 Établir un plan de coordination avec les pompiers pour les incendies et les incidents électriques dans les salles de commande des procédés, les salles de contrôle, les locaux d'instrumentation de contrôle-commande industriel correspondants et/ou les tableaux de commande industriels.

2.3.14.1 S'assurer que le personnel électricien peut intervenir en même temps que les équipiers de lutte contre l'incendie et qu'il est formé pour mettre hors tension ou isoler les tableaux de commande des procédés touchés et déclencher la lutte contre le feu.

2.3.14.2 Si la mise hors tension de tous les équipements électriques des tableaux et des locaux d'instrumentation de contrôle-commande industriel n'est pas envisageable, s'assurer que la notification d'alarme incendie déclenche l'intervention de personnes formées, capables d'évaluer la situation (incendie/fumée) dans la zone touchée et de mettre en œuvre le plan de coordination local ou régional, ou de procéder à un isolement électrique manuellement.

2.4 Facteur humain

2.4.1 Programme de gestion des changements

2.4.1.1 Les programmes de gestion et de sécurité des SCI devraient être coordonnés avec le programme de gestion des changements.

2.4.2 Gestion des SCI

L'engagement de la direction est un facteur déterminant dans la réussite des programmes de gestion et de supervision des SCI. Un engagement rigoureux de la direction garantit que tous les aspects des systèmes SCI bénéficient de l'attention, des investissements et des ressources nécessaires.

2.4.2.1 Équipe de supervision des SCI

2.4.2.1.1 Les entreprises devraient créer une équipe de supervision des SCI composée de membres de la direction du groupe et du site local qui soit chargée de superviser la mise en œuvre des procédures de cyber-sécurité relatives aux SCI.

2.4.2.2 Programme de gestion des équipements

2.4.2.2.1 Établir et mettre en œuvre un programme d'inspection, d'essai et de maintenance des SCI. Voir la fiche technique 9-0, *Intégrité des équipements*, pour des recommandations relatives à l'élaboration d'un programme d'intégrité des équipements. Inclure les éléments suivants dans un programme de gestion des équipements, le cas échéant :

A. Tenir à jour un inventaire du matériel raccordé au réseau SCI, avec nom du fabricant, numéro de modèle, et firmwares, logiciels et applications installés (numéros de version compris).

B. Veiller à ce que la liste de l'inventaire mentionne une note de criticité pour chaque équipement SCI afin de prioriser les actions de sécurité et maintenir les mises à jour de sécurité applicables.

C. Conserver les schémas et la documentation des SCI (par exemple, schémas électriques/de commande, plans des réseaux, etc., et, le cas échéant, schémas de tuyauterie et d'instrumentation des systèmes). Actualiser ces documents lorsque des modifications sont apportées aux SCI.

D. Ranger l'inventaire des équipements, les schémas et la documentation détaillant la conception et les fonctionnalités des SCI dans un lieu contrôlé et à accès restreint. Leur accès ne devrait être accordé

qu'en cas de besoin réel. Si ces documents sont numériques, ils devraient être protégés par mot de passe, et des sauvegardes devraient être enregistrées sur un réseau de confiance. Ces fichiers doivent être cryptés si possible. Tous les réseaux extérieurs à l'environnement SCI/OT devraient être considérés comme non fiables, y compris le réseau IT local.

2.4.2.3 Programme de gestion de la chaîne d'approvisionnement

2.4.2.3.1 Inclure les éléments suivants dans un programme de gestion de la chaîne d'approvisionnement, le cas échéant :

A. Inclure les critères de cybersécurité des systèmes/applications ou des équipements dans la documentation fournie aux prestataires pour l'appel d'offres. Réévaluer les règles et procédures de sécurité des fournisseurs agréés pour le site, y compris les prestataires de services, avant de signer/renouveler tout contrat.

2.4.3 Sécurité des SCI

Dans tout procédé, la disponibilité des SCI est essentielle. Une stratégie efficace de sécurité des SCI peut jouer un rôle déterminant pour assurer cette disponibilité.

2.4.3.1 Programme de gestion des accès

2.4.3.1.1 Inclure les éléments suivants dans un programme de gestion des accès, le cas échéant :

A. Utiliser des identifiants pour contrôler l'accès aux SCI (c'est-à-dire un accès selon les rôles pour l'IHM/le poste de travail opérateur et les stations ingénierie). Limiter également l'accès aux stations ingénierie aux personnes habilitées à modifier un procédé. Pour faciliter le contrôle des accès aux SCI, appliquer les principes suivants :

1. Des identifiants de connexion partagés peuvent être utilisés pour les IHM/postes de travail opérateur.
2. Sur les stations ingénierie, chaque utilisateur devant accéder au système devrait disposer de son propre identifiant et mot de passe. De plus, un délai d'expiration de session devrait être configuré en cas d'inactivité pendant 30 minutes ou moins.
3. Les identifiants de connexion aux SCI sont gérés indépendamment de ceux des systèmes IT. Conserver les informations de connexion aux SCI dans un annuaire à jour dans l'environnement OT, revoir régulièrement les droits d'accès et supprimer ceux des utilisateurs qui n'en ont plus besoin. À défaut, des connexions locales hors réseau peuvent être acceptables.

B. Modifier les noms d'utilisateur et mots de passe d'usine par défaut de l'ensemble des systèmes, matériels et logiciels. Les mots de passe devraient être modifiés à intervalles réguliers ou en cas de changements importants et/ou de personnel ou de fournisseur stratégique. Éviter les noms d'utilisateur génériques et les mots de passe faibles.

C. Protéger les communications sans fil par le biais d'une authentification et d'un chiffrement.

D. Respecter les précautions suivantes concernant les appareils portables qui se connectent aux SCI :

1. Dispenser aux visiteurs et aux sous-traitants amenés à se rendre sur site une formation sur la cybersécurité des SCI avant de les autoriser à pénétrer sur le site. Cette formation devrait inclure une présentation des procédures et règles en vigueur sur le site, conformément à la section 2.4.3.1.1, parties D.2 à D.5.
2. Pour les appareils externes utilisés dans l'environnement SCI (ordinateurs portables, tablettes, etc.), désactiver les connexions sans fil, tenir à jour/vérifier les correctifs de sécurité et l'antivirus installés et procéder à une analyse antivirus avant chaque connexion aux SCI.
3. Pour les périphériques de stockage amovibles (cartes mémoire, clés USB, disques durs externes, etc.), procéder à une analyse de sécurité avant chaque connexion aux SCI.
4. Ne pas autoriser la connexion aux SCI des téléphones portables et de tout appareil pouvant se connecter à un réseau mobile.
5. Dans la mesure du possible, désactiver les ports inutilisés (USB, RJ45, série, etc.) sur les équipements connectés aux SCI.

2.4.3.2 Programme de gestion de la configuration

2.4.3.2.1 Inclure les éléments suivants dans un programme de gestion de la configuration, le cas échéant :

A. Limiter les fonctions/fonctionnalités au minimum requis pour le bon fonctionnement des SCI et des procédés. Il s'agit par exemple des appareils de terrain à réglages multiples et à communication numérique, des contrôleurs logiques qui effectuent des contrôles de base de la production et de sécurité, des équipements de supervision, des IHM et stations ingénierie, des logiciels d'historisation, des équipements réseau tels que les passerelles réseau, commutateurs et routeurs réseau, et des équipements de protection réseau tels que les pare-feux, notamment l'ensemble des dispositifs installés au sein d'une zone démilitarisée (DMZ) des SCI.

B. Dans le cadre du programme de gestion des changements, vérifier que l'équipe de supervision des SCI analyse, valide et approuve toute modification apportée à un appareil numérique connecté aux SCI pour en déterminer l'impact sur la sécurité avant son déploiement.

C. Surveiller le système afin d'identifier toute modification non autorisée sur les équipements de contrôle de base ou de contrôle de la sécurité, ainsi que sur les équipements du réseau OT.

D. Avant d'activer le système et de faire fonctionner les SCI, veiller à ce que le mode de fonctionnement sélectionné (exécution, programmation, commande à distance, etc.) pour les unités logiques programmables, les automates ou les contrôleurs utilisés dans le système de commande de base de la production et le système de sécurité soit conforme aux recommandations du fabricant. Inclure les changements du mode de fonctionnement dans la recommandation relative à la surveillance du système, ci-dessus.

2.4.3.3 Programme de gestion des correctifs

2.4.3.3.1 Inclure les éléments suivants dans un programme de gestion des correctifs, le cas échéant :

A. Veiller à ce que le programme de gestion des correctifs inclue les équipements de support et de communication, tels que, mais sans s'y limiter, serveurs d'accès à distance, les serveurs de rebond, les logiciels d'historisation, les protections antivirus, les réseaux privés virtuels et les autres composants réseau, y compris les pare-feux, etc. Inclure également tout équipement utilisé pour la maintenance des SCI : ordinateur portable, appareil portatif ou console d'analyse antivirus servant à vérifier les appareils mobiles tels que les kiosques USB, etc.

B. Consulter les bulletins et alertes sur les vulnérabilités de cybersécurité publiés par les fabricants des systèmes et équipements, les intégrateurs de SCI, les organismes publics/agences gouvernementales, etc.

C. En cas de notification de cybersécurité, l'équipe de supervision des SCI devrait déterminer les mesures à prendre pour protéger les SCI du site, en fonction de la criticité et du risque. Des mesures de protection supplémentaires pourraient s'avérer nécessaires jusqu'à l'installation d'un correctif logiciel.

D. Veiller à ce que l'équipe de supervision des SCI contacte le fournisseur de l'SCI concerné avant toute installation d'un correctif. Dans la mesure du possible, tester le correctif dans un environnement de simulation ou un système virtuel avant l'installation.

E. Pour les équipements et/ou logiciels obsolètes, compte tenu de l'absence de support de la part du fabricant, prévoir des mesures de protection supplémentaires contre les vulnérabilités de cybersécurité.

2.4.3.4 Protection du réseau

2.4.3.4.1 Sécuriser les accès à distance à l'environnement SCI/OT. Tous les réseaux extérieurs à l'environnement SCI/OT devraient être considérés comme non fiables, y compris le réseau IT local. Appliquer les précautions suivantes, le cas échéant :

A. Vérifier que les accès à distance aux SCI respectent les principes suivants :

1. Depuis un réseau interne (dont la connexion est établie sur le réseau du site), comme le réseau IT local, utiliser une authentification multifacteur via un serveur de rebond situé dans une DMZ industrielle (voir la section 2.4.3.4.2 B).

2. Depuis un réseau externe (dont la connexion est établie hors du réseau du site), utiliser un réseau privé virtuel (VPN) sécurisé et une authentification multifacteur via un chemin d'accès spécifique, reposant sur les systèmes de l'entreprise et débouchant sur un système intermédiaire (serveur de rebond dans la DMZ industrielle), avant de pouvoir accéder à l'environnement SCI/OT.
3. Interdire l'utilisation d'ordinateurs et autres appareils externes personnels pour accéder à distance à l'environnement SCI/OT.

B. Interdire les connexions à distance aux systèmes de sécurité spécifiques.

C. Interdire les connexions à distance persistantes à l'environnement SCI/OT. Pour les activités de surveillance à distance, de collecte de données et de diagnostic dont le flux de données est restreint à une seule direction, il n'est pas nécessaire de configurer une limite de temps pour la connexion aux SCI.

D. Remplacer les modems téléphoniques par des méthodes de communication modernes et sécurisées. À défaut, procéder comme suit :

1. Éteindre et/ou débrancher les modems téléphoniques lorsqu'ils ne sont pas utilisés.
2. Prévoir des mesures de protection supplémentaires pour les modems téléphoniques actifs (par exemple, configuration d'un rappel vers un numéro de téléphone donné, filtrage de l'identité de l'appelant, désactivation de la réponse automatique).

2.4.3.4.2 Mettre en œuvre les protections réseau suivantes, le cas échéant :

A. Mettre en place une séparation entre les réseaux SCI/OT et IT ou les autres réseaux d'entreprise par le biais d'une zone démilitarisée (DMZ), et acheminer l'ensemble des communications à destination des SCI et en provenance de ceux-ci via la DMZ.

B. Mettre en place une séparation entre le réseau du système de commande de base de la production et les réseaux des sécurités instrumentées, par ségrégation (isolement ou architecture connectée) ou par segmentation (architecture intégrée ou commune). Pour plus d'informations sur les systèmes de sécurité, voir la fiche technique 7-45, *Safety Controls, Alarms, and Interlocks* (SCAI).

C. Vérifier que les règles de pare-feu (ports ouverts, protocoles autorisés, etc.) sont revues régulièrement par des personnes expérimentées en matière de réseaux et de cybersécurité. Les modifications des règles de pare-feu sont mises en œuvre dans l'environnement SCI/OT et gérées via un programme de gestion des changements piloté par l'équipe de supervision des SCI.

D. Utiliser une « liste d'autorisations d'applications » dans l'environnement SCI, dans la mesure du possible. Procéder avec prudence lors de la mise en œuvre de cette solution.

E. S'appuyer si possible sur la surveillance réseau et les journaux d'activités du réseau SCI (système de détection d'intrusion) ainsi que sur un logiciel SIEM (gestion des informations et des événements de sécurité) pour détecter les activités non autorisées. Dans la mesure du possible, surveiller l'environnement OT par le biais d'un centre d'opérations de sécurité (SOC).

F. Utiliser un logiciel antivirus sur les SCI et dans l'environnement OT, y compris sur les systèmes SCADA. Collaborer avec les différents fournisseurs et prestataires SCI, et procéder avec prudence lors du choix et du déploiement de solutions antivirus.

2.5 Exploitation et maintenance

Il est essentiel de s'assurer qu'un SCI fonctionne correctement afin d'éviter d'importants dommages aux équipements et/ou aux biens, susceptibles d'entraîner des arrêts prolongés. Des procédures de surveillance et de notification, un plan d'intervention d'urgence/de reprise d'activité adéquat et un plan de secours des équipements SCI, ainsi que des opérateurs compétents, ayant suivi une formation appropriée et respectant les procédures d'exploitation standard et d'urgence écrites, permettent de réduire les risques de défaillances liées aux SCI et les arrêts de longue durée.

2.5.1 Fonctionnement des SCI

2.5.1.1 Programme de gestion des alarmes

2.5.1.1.1 Inclure la surveillance des équipements SCI et du réseau OT, s'il s'agit d'une opération envisageable selon la recommandation relative à la gestion de la configuration (section 2.4.3.2.1 C) :

A. Dans le cadre de la surveillance du système, configurer une alerte pour modification non autorisée des paramètres de configuration des SCI, y compris des systèmes de sécurité et des équipements du réseau OT.

Remarque : Les alertes indiquées ci-dessus ne sont pas destinées à être gérées par les opérateurs. Ces alertes devraient être signalées au personnel chargé de la surveillance des équipements du réseau OT et SCI.

Pour plus d'informations sur la gestion des alarmes, voir la fiche technique 10-8, *Operators*.

2.5.1.2 Procédures d'exploitation d'urgence

2.5.1.2.1 La planification et la préparation sont essentielles au bon déroulement d'une procédure d'exploitation d'urgence des systèmes SCI/en cas de cyber-incidents, notamment grâce à l'identification du personnel et, si nécessaire, des consultants tiers ou d'autres spécialistes dotés des compétences requises pour répondre à un événement de cyber-intrusion.

A. Vérifier que les rôles et responsabilités ont été définis pour gérer les cyber-incidents.

B. Tenir à jour les informations sur les fournisseurs qui sont autorisés/contractuellement tenus d'intervenir en cas d'événement cyber.

2.5.1.2.2 Inclure les éléments suivants dans les procédures d'exploitation d'urgence pour la cybersécurité ou les SCI, le cas échéant :

A. S'assurer qu'une procédure existe pour réduire l'impact de la perte d'un système ERP (progiciel de gestion intégré) ou MES (système de pilotage de la production) sur les systèmes SCI et la production.

B. S'assurer qu'une procédure d'arrêt du système et/ou du procédé existe (basculement du système en mode sécurité, par exemple) en cas de dysfonctionnement ou d'arrêt du système de commande de l'SCI. Cette procédure devrait notamment indiquer comment procéder en cas de cyber-incident connu ou suspecté, par exemple :

- écran noir/gel de l'écran de l'IHM ;
- déclenchement inexpliqué d'une unité ;
- affichage de messages de ransomware sur les postes de travail ;
- déplacements inopinés des curseurs sur les postes de travail sans intervention de l'opérateur ;
- modification non reconnue de la configuration ;
- problème rencontré lors de la configuration ou du calibrage de certaines parties des systèmes SCI.

C. Des procédures d'exploitation en mode manuel des équipements stratégiques.

D. Vérifier que les procédures d'exploitation d'urgence (EOP) sont effectuées (au minimum) dans le cadre d'exercices sur table de manière régulière.

2.5.1.3 Plan équipements

2.5.1.3.1 Plan de secours des équipements

Rédiger et tenir à jour un plan de secours des équipements pour les SCI conformément à la fiche technique 9-0, *Intégrité des équipements*. Consulter l'annexe C de cette fiche technique pour plus d'informations sur la procédure d'élaboration et d'actualisation d'un plan de secours des équipements adéquat pour les SCI. Dans cette même fiche technique, se reporter également aux recommandations relatives aux stratégies de réduction des risques liées aux équipements redondants, de rechange, et de location.

Inclure également les éléments suivants dans le plan équipements pour les SCI :

A. Préciser les mesures nécessaires à la gestion des arrêts accidentels et à la reprise des activités à la suite d'un arrêt des SCI dans le cadre de la procédure de gestion des incidents et du plan de reprise d'activité (voir la section 2.5.1.4).

B. Tester le plan par le biais d'exercices réalisés à une fréquence déterminée par le responsable de chaque équipement concerné et adaptée aux risques.

C. En fonction de l'inventaire du matériel (voir la section 2.4.2.2.1), notamment de la criticité du composant et des plans de gestion du cycle de vie, évaluer la nécessité de constituer un stock de pièces de rechange pour les composants des SCI et, le cas échéant, l'étendue de ce stock.

2.5.1.3.2 Les plans de secours des équipements des SCI sont revus chaque année.

2.5.1.4 Plan de reprise de l'activité en cas d'incident

2.5.1.4.1 Le cas échéant, inclure les éléments suivants dans une procédure de gestion des incidents et un plan de reprise d'activité s'inscrivant dans le cadre du plan équipements des SCI :

A. Déterminer la cause première de tout arrêt accidentel avant de tenter de redémarrer les SCI.

B. Dans la mesure du possible, conserver des dossiers électroniques à des fins d'expertise judiciaire en cas d'arrêt accidentel.

C. Conserver une copie adéquate et à jour de tous les fichiers de configuration des SCI (par exemple, dernière configuration fiable connue, configuration de base) et les documents requis pour que les systèmes soient totalement opérationnels. Conserver un historique des fichiers de sauvegarde à un emplacement protégé par contrôle des accès.

1. Si les fichiers de sauvegarde sont inaltérables (non réinscriptibles, non effaçables) :
    a. les stocker sur un lecteur réseau fiable séparé du réseau dont proviennent les données ;
    b. créer de nouveaux fichiers de sauvegarde lorsque des modifications ont été apportées au système et après chaque mise à jour.
    c. créer de nouveaux fichiers de sauvegarde avant la fin de la période de rétention du dernier fichier inaltérable.
2. Si les fichiers de sauvegarde ne sont pas inaltérables (s'ils sont réinscriptibles) :
    a. conserver au moins une copie de l'ensemble des fichiers de sauvegarde hors ligne, dans un emplacement protégé par contrôle des accès ;
    b. créer de nouveaux fichiers de sauvegarde lorsque des modifications ont été apportées au système et après chaque mise à jour.

D. Revoir les contrats de service avec les fabricants et/ou les fournisseurs des équipements pour identifier le délai de livraison des composants, l'objectif étant de déterminer la stratégie optimale en matière de reprise d'activité et d'approvisionnement en pièces de rechange pour les équipements.

E. Revoir régulièrement la procédure de gestion des incidents et le plan de reprise d'activité à une fréquence adaptée aux risques, et au minimum une fois par an. Actualiser ce programme en fonction des besoins afin de préserver son efficacité.

Pour plus d'informations sur le plan de coordination avec les pompiers et le plan de reprise d'activité, voir les fiches techniques 9-1, *Supervision of Property*, 10-1, *Planification de la coordination et de l'intervention d'urgence,* et 10-5, *Disaster Recovery Planning*.

Pour plus d'informations concernant les procédures d'investigation sur les incidents, voir les fiches techniques 10-8, *Operators*, et 7-43, *Process Safety*.

2.6 Formation

2.6.1 Dans le cadre du programme de formation des opérateurs du site, mettre en place un programme pour les former et les sensibiliser aux règles et procédures de sécurité des SCI. Ce programme devrait inclure des standards et bonnes pratiques en matière de cybersécurité.

2.6.2 Dispenser aux opérateurs et au personnel stratégique du site amenés à interagir avec les SCI une formation spécialisée avant de leur donner accès à ces systèmes. Dispenser une formation supplémentaire

aux administrateurs système et au personnel disposant de droits d'accès étendus (formation spécifique selon chaque rôle) dans le cadre de leurs attributions.

2.6.3 Dispenser chaque année au personnel intervenant sur les SCI des formations initiales et de remise à niveau sur la cybersécurité de ces systèmes.

2.6.4 Dispenser une formation aux membres de l'équipe d'intervention d'urgence sur le risque d'incendie dans les locaux de contrôle des procédés. Voir la section 2.7.1 de la fiche technique 5-32, *Data Centers and Related Facilities*.

Pour plus d'informations sur les opérateurs, voir la fiche technique 10-8, *Operators*.

2.7 Utilités

2.7.1 Prévoir des onduleurs et des groupes électrogènes pour permettre le fonctionnement des SCI jusqu'à ce qu'ils puissent être arrêtés en toute sécurité. Inclure des onduleurs pour tous les systèmes auxiliaires, tels que les circuits d'air d'instrumentation (le cas échéant) et les systèmes de chauffage, ventilation et climatisation, qui peuvent s'avérer nécessaires pendant la procédure d'arrêt sécurisé.

2.7.2 Réaliser les opérations d'inspection et de maintenance des utilités et des systèmes d'alimentation prévus pour les SCI (par exemple, les batteries, onduleurs, groupes électrogènes et systèmes de climatisation) dans le cadre du programme d'intégrité des équipements. Pour plus d'informations, voir les fiches techniques 5-28, *DC Battery Systems*, et 5-23, *Design and Protection for Emergency and Standby Power Systems*.

2.7.3 Installer un circuit d'air d'instrumentation fiable qui utilise des commandes pneumatiques (par exemple, un compresseur d'air indépendant avec redondance N+1 ou un réservoir d'air correctement dimensionné).

2.7.4 Installer un système fiable de chauffage, ventilation et climatisation (CVC) permettant de maintenir les conditions environnementales requises pour un fonctionnement normal des équipements SCI. Cette recommandation concerne principalement les équipements SCI considérés comme stratégiques pour l'activité.

3.0 BASE DES RECOMMANDATIONS

3.1 Protection incendie pour les équipements de commande industriels

S'assurer que la protection sprinkleur automatique installée est dimensionnée pour protéger la structure du local et l'activité voisine. Dans un petit local, tous les équipements pourraient être détruits, même si l'incendie était maîtrisé par un système sprinkleur ou un système d'extinction à brouillard d'eau. Un système d'extinction incendie à halocarbure ou à gaz inerte (agent propre) serait sans doute préférable si l'objectif est de protéger les équipements.

Un incendie dans des armoires d'équipements de commande des procédés bien subdivisées pourrait certes endommager celle dans laquelle il a démarré, mais beaucoup moins les autres. À l'inverse, un incendie dans une armoire d'équipements de commande des procédés sans subdivision pourrait se propager sur toute la longueur de l'enceinte. L'impact de la perte d'équipements de commande des procédés dépend de l'étendue des dommages causés par le feu, de la criticité des procédés, de la disponibilité des pièces de rechange, etc.

3.2 Gestion des SCI

Le responsable des équipements ou la personne désignée devrait mettre en œuvre une stratégie de cybersécurité pour protéger l'ensemble des SCI du site.

3.2.1 Équipe de supervision des SCI

La complexité de l'automatisation, l'interconnexion de différents systèmes et réseaux et l'acquisition de données à des fins d'analyse ont introduit une nouvelle catégorie de menaces pour les SCI : les cyber-risques. Pour garantir la continuité de la production sur le site, les SCI requièrent une personne capable de les protéger des cyber-risques et de comprendre l'impact potentiel des méthodes, produits et systèmes de cybersécurité sur leur fonctionnement.

3.2.2 Programme de gestion des équipements

Pour assurer la cyber-résilience des SCI, les entreprises doivent savoir quels équipements sont raccordés au réseau SCI. À défaut, elle ne pourra pas identifier les appareils qui exposent les SCI à des cyber-risques.

Les équipements à inclure dans le programme de gestion des équipements sont les appareils numériques connectés au réseau SCI, par exemple les IHM/postes de travail opérateur, les stations ingénierie, les commutateurs de réseau, les modems, les routeurs réseau, les pare-feux, les serveurs d'applications, les imprimantes, les systèmes numériques de contrôle-commande, les automates et autres contrôleurs logiques, et les appareils de terrain intelligents connectés au réseau. Les systèmes d'exploitation (par exemple, les équipements utilisés au niveau 3 du modèle de Purdue d'un réseau OT) devraient également faire l'objet d'un suivi. Les équipements généralement classés à ce niveau sont les logiciels d'historisation des données, les systèmes d'ordonnancement, les serveurs d'alarmes et autres serveurs d'applications, les services informatiques opérationnels tels que DHCP, LDAP, DNS, et les serveurs de fichiers. Sont également à prendre en compte les appareils de l'Internet industriel des objets (IIoT) voire les simples appareils de l'Internet des objets (IoT) susceptibles d'être connectés à tort au réseau SCI.

Des programmes de gestion des équipements adéquats permettent d'identifier les appareils numériques connectés au réseau SCI. Les appareils incluent, sans toutefois s'y limiter, les IHM, les automates, les stations ingénierie, les équipements de réseau, les serveurs, etc. Il est essentiel d'identifier le firmware, le logiciel et les applications de chacun d'entre eux. Sans ces informations complémentaires, les fonctionnalités et services disponibles pour chaque appareil ne peuvent pas être vérifiés, ce qui rend les SCI vulnérables.

De nombreux fournisseurs sur le marché proposent des solutions automatisées de recherche des équipements actifs et passifs/de cartographie du réseau. Dans la mesure du possible, l'utilisation de solutions de recherche des équipements passifs est à privilégier par rapport à des techniques manuelles de gestion des équipements.

3.2.3 Programme de gestion de la chaîne d'approvisionnement

Un programme de gestion de la chaîne d'approvisionnement adéquat permet de s'assurer que les équipements et logiciels sont configurés par les fournisseurs afin de répondre aux critères de sécurité de l'entreprise.

Avant d'installer un nouveau contrôleur ou tout autre appareil numérique, ou un logiciel et/ou une application sur les SCI, l'entreprise doit s'assurer que le dispositif concerné a suivi une chaîne de contrôle fiable allant du développeur au stockage, en passant par le fabricant, le fournisseur et l'expédition, et comprenant des essais de conformité et de mise en service.

3.3 Sécurité des SCI

3.3.1 Programme de gestion des accès

Les points d'accès non sécurisés des systèmes SCI constituent l'un des vecteurs d'attaque les plus vulnérables. Ils sont exposés à des cyber-intrusions, qu'elles soient délibérées ou involontaires. Les cybercriminels savent que les SCI doivent permettre un accès à distance et recherchent des points d'accès faciles dans le but de s'attaquer au système. Dans le pire des cas, un point d'accès peut être compromis pendant une période prolongée, permettant à des tiers non autorisés d'accéder aux systèmes SCI, et d'obtenir ainsi de précieuses informations sur ces systèmes et sur les procédés du site, ce qui leur laisserait tout loisir d'organiser une cyberattaque.

3.3.2 Programme de gestion de la configuration

Les appareils numériques/électroniques sont dotés de nombreuses options et fonctionnalités de performance et/ou de communication par firmware et/ou logiciel. Pour limiter le risque de cyberattaque, ces équipements sont soumis à un « durcissement » (par exemple, sur la base de leur criticité ou d'une analyse des cyber-risques liés aux procédés) afin de restreindre les options et fonctionnalités à celles qui sont strictement nécessaires pour le fonctionnement des SCI.

Une fois que la configuration voulue est définie et que le système fonctionne correctement, ces paramètres devraient être enregistrés en tant que configuration de base ou dernière configuration fiable connue. C'est

cette configuration qui sera utilisée pour rétablir le système en cas de défaillance matérielle, logicielle ou du firmware.

Une fois la configuration des automates de sécurité ou autres contrôleurs définie, ces équipements devraient fonctionner dans le mode recommandé par le fabricant (exécution, programmation, commande à distance, etc.). Cette configuration, comprenant les paramètres et le mode de fonctionnement, devrait être verrouillée en l'état par le retrait de la clé physique ou l'activation de la clé numérique. Cette procédure renforce le programme de gestion des accès en permettant l'accès aux seules personnes habilitées à modifier les paramètres de sécurité.

La surveillance des paramètres de configuration permet d'identifier les modifications non autorisées apportées aux SCI. Cette surveillance est utile pour identifier et, le cas échéant, prévenir les menaces internes ou externes visant les SCI.

3.3.3 Programme de gestion des correctifs

La gestion des correctifs consiste à apporter des mises à jour aux logiciels, pilotes et firmwares afin de les protéger contre les vulnérabilités. Les correctifs devraient être évalués pour déterminer les conséquences éventuelles d'un correctif sur le procédé.

Avant d'installer un correctif, authentifier le logiciel et en vérifier l'intégrité pour s'assurer qu'il est bien dans son état d'origine et n'a pas été altéré. La source du logiciel est également très importante ; sa fiabilité doit être confirmée avant tout téléchargement.

Si un correctif n'apporte aucun avantage sur le plan de la cybersécurité ou des performances, il n'est peut-être pas nécessaire. Le responsable des équipements devrait collaborer avec le fournisseur SCI lors du déploiement de correctifs dans l'environnement SCI/OT.

3.3.4 Protection du réseau

Avec les progrès techniques les environnements SCI/OT sont plus que jamais connectés. Cette connectivité accrue expose les environnements SCI/OT à des cyber-menaces qui n'existaient pas auparavant.

L'accès à distance est devenu une méthode courante d'assistance hors site pour les fournisseurs et un moyen pratique pour les employés de se connecter à l'environnement SCI/OT. Les communications qui proviennent de l'extérieur et demandent un accès à l'environnement SCI/OT doivent passer par un VPN sécurisé, avec une authentification multifacteur transitant par une zone démilitarisée (DMZ), pour enfin aboutir à un serveur de rebond ayant accès à l'environnement SCI/OT. Les communications qui proviennent de l'environnement de l'entreprise et demandent un accès à l'environnement SCI/OT doivent utiliser une authentification multifacteur en passant par une DMZ, pour aboutir à un serveur de rebond ayant accès à l'environnement SCI/OT.

Une zone démilitarisée est un réseau périphérique qui ajoute un niveau de sécurité supplémentaire au réseau OT interne de l'entreprise contre tout trafic non fiable. Une zone démilitarisée (DMZ) est une zone définie en limite d'un réseau de confiance qui fournit des ressources accessibles à des réseaux non fiables tels qu'Internet. De cette façon, les ressources dont les utilisateurs doivent se servir dans des zones non approuvées n'auront pas accès au réseau considéré comme sûr. Une DMZ industrielle fournit des services qui nécessitent une connectivité aux réseaux IT et OT tels que l'accès à distance, les correctifs, les antivirus, les logiciels d'historisation, les systèmes de pilotage de la production et les transferts de fichier.

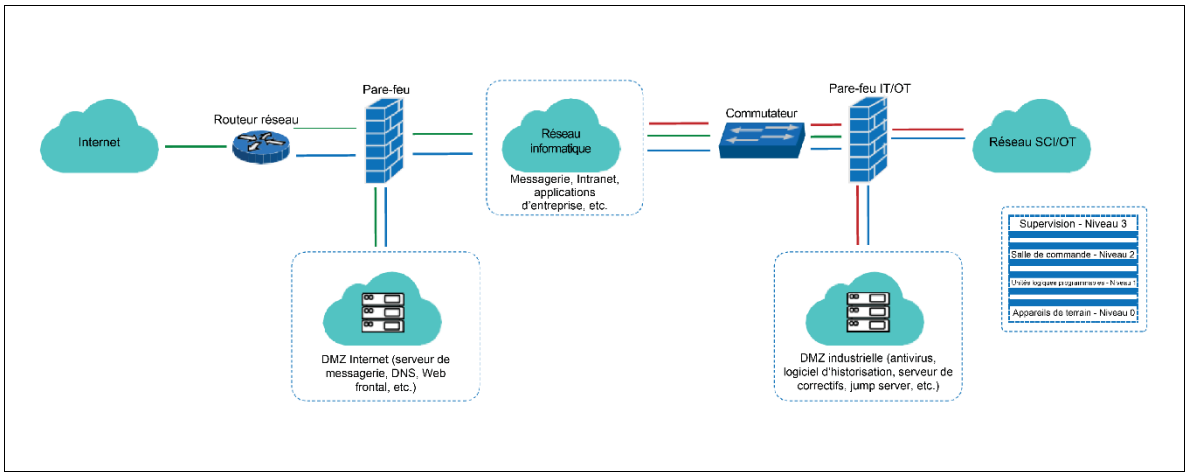

Fig. 3.3.4. Exemple de chemin de communication présentant la DMZ d'entreprise/Internet et la DMZ des SCI/industrielle

Les systèmes de détection d'intrusion (Intrusion Detection System - IDS) sont des dispositifs de sécurité destinés à surveiller le trafic réseau et les appareils en cas d'activité suspecte. Les alertes provenant des SCI doivent être transmises à un centre des opérations de sécurité (SOC) à des fins d'investigation.

Un système de détection d'intrusion basé sur les signatures recherche avant tout des signatures (c'est-à-dire des tendances ou schémas) pour détecter une intrusion. Ces signatures doivent être mises à jour régulièrement pour permettre d'identifier les schémas d'attaque les plus récents.

Un système de détection d'intrusion basé sur les anomalies analyse en premier lieu les schémas d'activité inattendus pour détecter une intrusion. Il peut s'agir par exemple d'un pic d'activité réseau, de plusieurs tentatives de connexion ayant échoué ou d'activités inhabituelles au niveau des ports réseau qui sont signalées comme suspectes. Ces alertes sont régulièrement transmises au centre des opérations de sécurité (SOC).

3.4 Exemples de sinistres

3.4.1 Réseau électrique ukrainien

Programme malveillant Crash Override. L'un des cas les plus importants de violation d'un SCI s'est produit en Ukraine le 23 décembre 2015, lorsque plusieurs coupures de courant non planifiées ont affecté environ 225 000 usagers. Ces pannes ont été causées par des cyber-intrusions à distance dans trois compagnies régionales de distribution d'électricité. En attendant le rétablissement de l'électricité, les entreprises concernées ont continué à fonctionner au ralenti.

D'après les informations recueillies, la cyberattaque aurait été synchronisée et coordonnée après une reconnaissance approfondie des réseaux visés. Certains rapports suggèrent que cette attaque aurait duré six mois. Les rapports indiquent que les cyberattaques de chacune des compagnies se sont produites à 30 minutes d'intervalle et ont visé plusieurs sites. Au cours de l'incident, plusieurs disjoncteurs ont été actionnés à distance et sans autorisation par plusieurs entités externes au moyen soit d'outils d'administration à distance qui existaient au niveau du système d'exploitation, soit de logiciels clients SCI distants via des connexions VPN. Selon les rapports, les entités externes se seraient procurées des identifiants légitimes avant la cyberattaque afin de faciliter leur accès à distance.

Les trois compagnies d'électricité ont indiqué que plusieurs systèmes avaient été détruits à l'issue de la cyberattaque au moyen du programme malveillant Kill Disk. Ce dernier efface certains fichiers des systèmes et altère le Master Boot Record (MBR), rendant ainsi les systèmes inopérants. En outre, les IHM Windows intégrées dans des unités de terminal à distance ont également été écrasées par Kill Disk. Plusieurs convertisseurs série vers Ethernet au niveau des postes électriques ont été rendus inutilisables par corruption de leur firmware. Les onduleurs ont été déconnectés via leur interface de gestion à distance dans le but de perturber les opérations de restauration.

Les trois compagnies ont indiqué avoir été infectées par le programme malveillant Black Energy, mais il n'est pas certain que celui-ci ait joué un rôle dans la cyberattaque. Le programme malveillant aurait été

diffusé par le biais d'e-mails d'hameçonnage ciblés contenant des pièces jointes malveillantes. Bien que cela n'ait pas été confirmé, il semblerait que Black Energy ait pu servir à obtenir des identifiants légitimes. Toutefois, n'importe quel cheval de Troie d'accès à distance aurait pu être utilisé.

À la suite de ces attaques, les compagnies n'ont pas pu réarmer les disjoncteurs à distance et ont donc dû dépêcher des opérateurs sur place pour les réarmer manuellement. Cette opération a entraîné une panne d'une durée de quatre à six heures. Il convient de noter qu'aucune centrale électrique n'a été endommagée à la suite de cet incident.

3.4.2 TRISIS

En décembre 2017, des chercheurs en sécurité informatique ont identifié une attaque par un programme malveillant sur les systèmes instrumentés de sécurité et les systèmes numériques de contrôle-commande d'un grand site industriel au Moyen-Orient. Les entreprises spécialisées en cybersécurité ont désigné ce programme malveillant sous les noms de TRITON et TRISIS, tandis que l'équipe SCI-CERT du département de la Sécurité intérieure des États-Unis l'a appelé HATMAN. Ce programme a infecté les contrôleurs de sécurité et l'interface homme-machine Triconex Tricon de Schneider Electric, permettant à un attaquant de lire/modifier le contenu de la mémoire des contrôleurs (c'est-à-dire d'écraser les programmes via une connexion réseau à distance).

D'après les informations disponibles, les attaquants ont réussi à accéder à distance à une station ingénierie du système instrumenté de sécurité et ont déployé le programme malveillant : un fichier exécutable sur PC Windows permettant de communiquer avec le contrôleur de sécurité (Triconex) et un composant binaire malveillant téléchargé sur le contrôleur. Mandiant, une entreprise de cybersécurité du groupe FireEye appelée à enquêter sur l'incident, a déclaré dans son rapport [1] que « le programme malveillant pouvait lire et écrire des programmes et interroger l'état du contrôleur. Il était également capable de communiquer avec le contrôleur à l'aide du protocole TriStation, un protocole exclusif utilisé par le logiciel TriStation (logiciel de programmation Tricon) pour communiquer avec les systèmes de sécurité Triconex. Il semble que l'attaquant connaisse bien le système Triconex et qu'il ait testé le programme malveillant avant l'attaque. »

L'analyse de Mandiant montre que les attaquants ont également eu accès au système numérique de contrôle-commande du site, mais qu'ils ont décidé de compromettre le système de sécurité. Ils ont accidentellement provoqué un arrêt du système en tentant de reprogrammer les contrôleurs pour causer des dommages physiques. Le système est passé en mode de sécurité positive en raison de l'échec d'un contrôle de validation entre les processeurs, ce qui a déclenché l'arrêt du système et l'alerte du propriétaire. Comme l'indique Mandiant, « la prise de contrôle simultanée du système numérique de contrôle-commande et du système instrumenté de sécurité aurait pu permettre à l'attaquant d'occasionner d'importants dommages ».

L'équipe SCI-CERT et la société Dragos ont déclaré que le protocole TriStation utilisé dans des contrôleurs anciens, comme celui qui était ciblé par cette attaque, ne dispose pas d'un mécanisme d'authentification ou de chiffrement pour les comptes de type « porte dérobée », qui sont essentiels pour garantir l'accès et le contrôle de l'appareil par l'administrateur en cas d'urgence. En revanche, les versions plus récentes des systèmes Triconex comportent un facteur d'authentification pour ces comptes et sont donc moins exposées à de telles attaques. Une notification de sécurité de Schneider Electric ayant confirmé cette vulnérabilité, un outil a été développé pour détecter et supprimer le programme malveillant dans un contrôleur Tricon. L'entreprise a également déclaré que l'interrupteur à clé permettant de contrôler le fonctionnement physique était resté en mode « Programme », pratique jugée inacceptable en dehors des opérations de programmation du contrôleur.

Les systèmes Triconex sont des systèmes de sécurité très performants disponibles sur le marché. Tricon est basé sur la technologie Triple Modular Redundant (TMR), qui intègre en un seul système trois systèmes de contrôle-commande isolés et parallèles ainsi que des diagnostics complets. Le système Tricon assure des procédés ininterrompus, exempts d'erreurs et à haute intégrité, sans point de défaillance unique. La technologie TMR s'applique aux entrées, aux sorties et à la logique. En raison de leur encombrement et de leur coût, ces systèmes sont principalement utilisés pour des applications stratégiques telles que les commandes de turbines (contrôle de la survitesse), et parfois comme système numérique de contrôle-commande. Même si ce programme malveillant était spécifiquement conçu pour les systèmes Triconex, les entreprises de cybersécurité estiment que des attaquants pourraient adapter ses fonctionnalités et sa méthodologie pour cibler les systèmes de sécurité d'un autre fournisseur. Cet incident a remis en question

la théorie selon laquelle le système de sécurité permet de parer à tout dommage, même si le système de commande des procédés est compromis.

4.0 RÉFÉRENCES

4.1 FM

Fiche technique 1-20, *Protection Against Exterior Fire Exposure*
Fiche technique 1-44, *Damage-Limiting Construction*
Fiche technique 2-0, *Guide d'installation des sprinkleurs automatiques*
Fiche technique 3-26, *Protection incendie pour les activités hors stockage*
Fiche technique 4-5, *Portable Extinguishers*
Fiche technique 4-9, *Halocarbon and Inert Gas (Clean Agent) Fire Extinguishing Systems*
Fiche technique 5-11, *Lightning and Surge Protection for Electrical Systems*
Fiche technique 5-23, *Design and Protection for Emergency and Standby Power Systems*
Fiche technique 5-28, *DC Battery Systems*
Fiche technique 5-31, *Cables and Bus Bars*
Fiche technique 5-32, *Data Centers and Related Facilities*
Fiche technique 7-43, *Process Safety*
Fiche technique 7-45, *Safety Controls, Alarms, and Interlocks*
Fiche technique 9-0, *Intégrité des équipements*
Fiche technique 9-1, *Supervision of Property*
Fiche technique 10-1, *Planification de la coordination et de l'intervention d'urgence*
Fiche technique 10-5, *Disaster Recovery Planning*
Fiche technique 10-8, *Operators*

4.2 Autres

International Society for Automation (ISA). Série de normes et rapports techniques ISA/IEC 62443.

National Institute of Standards and Technology (NIST). *Guide to Industrial Control Systems (SCI) Security*. NIST SP 800-82, Revision 2.

North American Electric Reliability Corporation (NERC). CIP Reliability Standards.

Electric Power Research Institute (EPRI), *Generation Cyber Security*.

US Department of Homeland Security, National Cybersecurity and Communications Integration Center's (NCCIC), SCI-CERT.

ANNEXE A GLOSSAIRE

Accès à distance : accès au périmètre de sécurité d'un système d'information par des utilisateurs (ou d'autres systèmes d'information) communiquant depuis l'extérieur (Source : NIST SP 800-53.) Utilisation de systèmes situés dans le périmètre de la zone de sécurité à partir d'un emplacement géographique différent avec les mêmes droits qu'en étant physiquement sur site. Exemples d'équipements utilisés en accès à distance :

1. Les modems modulent et démodulent les données en entrée et en sortie. Il s'agit essentiellement de convertir les signaux électriques analogiques provenant de l'extérieur du réseau en valeurs numériques binaires qui seront traitées par le routeur réseau, et inversement.
2. Les routeurs réseau se trouvent en aval du modem. Ils se connectent à un réseau étendu (WAN) ou à Internet avec une adresse IP publique. Ils guident et acheminent les données du réseau, tout en les hiérarchisant et en choisissant le meilleur itinéraire pour chaque transmission.
3. Les serveurs d'accès à distance fournissent des services de gestion des connexions à distance depuis l'extérieur du réseau local (LAN). Ils sont communément appelés serveurs de rebond.

Accès physique : accès physique réel, sur site, au matériel informatique et réseau, ou à d'autres éléments d'une installation réseau.

Accès : la capacité et les moyens de communiquer ou d'interagir avec un système afin d'utiliser ses ressources. L'accès peut être physique (autorisation de pénétrer physiquement dans une zone, détention

d'une clé physique, d'un code PIN, ou d'une carte d'accès ou de caractéristiques biométriques permettant l'accès) ou logique (autorisation de se connecter à un système et à une application par une combinaison de moyens logiques et physiques).

Annuaire : système qui stocke des informations sur les utilisateurs/membres d'un domaine particulier, dans l'objectif de fournir des fonctionnalités d'authentification et d'autorisation selon une approche centralisée. Microsoft Active Directory est un exemple d'annuaire couramment utilisé dans les réseaux IT et OT.

Appareil de terrain : équipement connecté du côté terrain d'un SCI. Les appareils de terrain comprennent notamment les unités de terminal à distance (RTU), les automates, les actionneurs, les capteurs, les interfaces homme/machine (IHM) et les dispositifs de communication correspondants.

Attaquant : personne qui crée et/ou modifie des logiciels et du matériel informatique à des fins criminelles ou financières. Les attaquants tentent généralement d'accéder à des systèmes informatiques pour obtenir des noms d'utilisateur et des mots de passe.

Auteur de menace : entité partiellement ou entièrement responsable d'un incident ayant un impact sur la sécurité d'une entreprise. Exemples d'auteurs de menace : hacktivistes, menace interne, État-nation, crime organisé.

Authentification multifacteur : méthode d'authentification faisant appel à deux facteurs ou plus (c'est-à-dire un élément que vous connaissez, comme un mot de passe, un élément que vous possédez, comme un jeton temporel/statique, ou un élément qui vous caractérise, comme une empreinte digitale). L'authentification à deux facteurs est, comme son nom l'indique, un cas particulier d'authentification multifacteur faisant intervenir exactement deux facteurs.

Authentification : action de prouver une assertion, telle que l'identité de l'utilisateur d'un système informatique. Contrairement à l'identification, qui consiste à indiquer l'identité d'une personne ou d'un objet, l'authentification est le processus qui consiste à vérifier cette identité. Le mot de passe fourni par un utilisateur pour se connecter constitue une méthode d'authentification courante.

Automate ou automate programmable industriel : Les automates sont des contrôleurs d'automatisation capables de commander des procédés complexes. Ils sont notamment utilisés dans les systèmes de supervision et contrôle à distance (SCADA) et les systèmes numériques de contrôle-commande. Les automates font également office de contrôleur principal dans les configurations système de petite taille. Ils sont très largement utilisés dans la plupart des procédés industriels.

Balayage de numéros de téléphone pour recherche d'accès non protégés : un composeur d'attaque, ou « war dialer », est un programme informatique utilisé pour identifier les numéros de téléphone qui permettent d'établir une connexion avec le modem d'un ordinateur. Le programme compose automatiquement une série définie de numéros de téléphone, puis consigne dans une base de données les numéros qui ont permis de se connecter au modem. Certains programmes peuvent également identifier le système d'exploitation spécifique de l'ordinateur et effectuer des tests d'intrusion automatisés. Dans ce cas, le composeur d'attaque balaye une liste prédéterminée de noms d'utilisateur et de mots de passe courants pour tenter d'accéder au système.

Capteur :

1. Dispositif qui produit une tension ou un courant de sortie représentant une propriété physique mesurée (par exemple, la vitesse, la température, le débit).
2. Dispositif qui mesure une quantité physique et la convertit en un signal pouvant être lu par un observateur ou un instrument.
3. Dispositif qui réagit à une quantité entrée en générant une sortie fonctionnellement liée, généralement sous la forme d'un signal électrique ou optique.

Centre des opérations de sécurité (SOC) : solution qui englobe les personnes, les processus et la technologie, y compris la solution SIEM, contribuant à surveiller les environnements numériques (c'est-à-dire IT et OT) dans le but de les protéger, à répondre aux événements qui peuvent évoluer en incidents, à faire des recherches sur les menaces connues/inconnues, à intervenir en cas d'incident et à partager des informations, entre autres actions.

Chiffrement : brouillage des données pour qu'elles ne soient lisibles que par celles et ceux qui détiennent la clé de chiffrement. Transformation cryptographique d'un texte en clair en texte crypté qui masque la signification initiale des données pour empêcher leur identification ou leur exploitation.

Cloisonnement : déconnexion complète d'un réseau par rapport à d'autres réseaux (isolement). Les systèmes instrumentés de sécurité sur les sites de grande envergure sont cloisonnés parce qu'ils ne sont pas contrôlés par le réseau SCI qui gère le système de commande de base de la production.

Configuration de base : spécification ou produit qui a fait l'objet d'un examen et d'une validation formels, qui sert ensuite de base à des développements ultérieurs et qui ne peut être modifié(e) que par des procédures formelles de gestion des changements.

Contrôle d'accès selon les rôles : forme de contrôle d'accès basé sur l'identité dans lequel les entités du système qui sont identifiées et contrôlées correspondent à des fonctions au sein d'une entreprise ou d'un procédé.

Correctif : extension logicielle conçue pour corriger les bogues et les problèmes de sécurité dans les systèmes d'exploitation ou les applications. Il est possible de réduire les risques pour la sécurité en mettant les logiciels à jour avec des correctifs.

Diode de données/passerelles unidirectionnelles : voir Passerelle unidirectionnelle ci-dessous.

Dispositif malveillant : dispositif qui n'est pas autorisé à accéder au réseau ni à fonctionner sur le réseau. Ce type de dispositif peut être malveillant par nature ou être détourné pour contourner les mesures de sécurité.

Durcissement : mesure de sécurité qui consiste à supprimer ou à désactiver des caractéristiques, fonctions, ports et services non nécessaires, et à appliquer des contrôles de cybersécurité pour empêcher toute utilisation non autorisée. Il existe deux types de durcissement :

1. Durcissement matériel : désactivation par des moyens physiques ; suppression de ports de communication inutiles, blocage de l'accès aux ports et aux disques, etc.
2. Durcissement logiciel : désactivation des protocoles réseau et de communication inutilisés, des pilotes de périphériques inutilisés, de serveurs Web, etc., puis application de contrôles de cybersécurité tels que la mise en place d'une protection par mot de passe pour la mise à jour du firmware et le chargement des programmes, l'activation de journaux et d'alertes, l'activation des technologies de sécurité fournies avec l'appareil, comme les antivirus ou les listes d'autorisations.

Équipement : objet physique ou logique appartenant ou confié à une entreprise, et ayant une valeur perçue ou réelle pour ladite entreprise.

Équipements de commande industriels : voir Tableaux de commande industriels.

Fiabilité : capacité d'un système à exécuter une fonction requise dans les conditions indiquées pendant une période de temps déterminée.

Fichier de sauvegarde inaltérable : fichier qui n'est ni modifiable, ni effaçable (non réinscriptible) et qui ne peut pas être supprimé avant la fin de la période de rétention (cette période de rétention doit être configurée au moment de la création du fichier inaltérable.) Étant donné que les fichiers inaltérables ne peuvent être ni modifiés ni supprimés, le contrôle des versions est essentiel.

Gestion de la configuration : règles et procédures de contrôle des modifications apportées au matériel, au firmware, aux logiciels et à la documentation, qui visent à protéger le système informatique contre toute modification injustifiée avant, pendant et après son déploiement.

Gestion des informations et des événements de sécurité (SIEM) : application qui permet de recueillir des données de sécurité à partir des composants du système d'information, de normaliser les pistes de vérification et d'enregistrer les essais par rapport à un ensemble de règles de corrélation qui, lorsqu'il est déclenché, crée des événements à des fins d'analyse et présente ces données sous forme d'informations exploitables via une interface unique.

Hameçonnage : type d'attaque contre la sécurité qui incite les victimes à divulguer des informations, en présentant un e-mail contrefait pour attirer son destinataire vers un site Web qui semble lié à une source légitime.

Identifiant : information se composant au minimum d'un nom d'utilisateur et d'un mot de passe, mais pouvant également être un élément physique ou biométrique humain tel qu'une empreinte digitale. Des identifiants servent à authentifier un utilisateur lorsqu'il se connecte à l'SCI. Des autorisations d'accès peuvent être liées à ces identifiants. Selon le niveau d'accès de l'utilisateur, des identifiants peuvent lui donner accès à un poste de travail opérateur ou à une station ingénierie, par exemple.

Intégrité : qualité d'un système reflétant la conformité logique et la fiabilité du système d'exploitation, l'exhaustivité logique du matériel et des logiciels mettant en œuvre les mécanismes de protection, ainsi que la cohérence des structures de données et des occurrences des données stockées.

1. Dispositif électronique intelligent (DEI) : tout dispositif qui intègre un ou plusieurs processeurs ayant la capacité de recevoir, d'envoyer et de contrôler des données/commandes depuis ou vers une source externe (par exemple, compteur électronique multifonctions, relais numérique, contrôleur).

Interface homme-machine (IHM) :

1. Matériel ou logiciel grâce auquel un opérateur interagit avec un contrôleur. Une IHM peut aller d'un simple panneau de commande comportant des boutons et des voyants lumineux à un PC industriel doté d'un écran graphique couleur et exécutant un logiciel spécialisé.
2. Logiciel et matériel permettant à des utilisateurs autorisés de surveiller et de contrôler les procédés et équipements, par exemple afficher l'état ou les tendances historiques, changer l'objectif du contrôle et prendre manuellement le relais des opérations de contrôle automatique en cas d'urgence.

Liste d'autorisations : liste d'entités distinctes, telles que des hôtes ou des applications, reconnues comme inoffensives et dont l'utilisation est approuvée au sein d'une entreprise et/ou d'un système d'information. Exemple : permettre à certaines applications et certains services uniquement de fonctionner sur un hôte dans le cadre de son durcissement.

Locaux d'instrumentation de contrôle-commande industriel : locaux abritant les équipements de commande des procédés, qui comprennent en général un certain nombre de tableaux de commande industriels et les équipements de réseau nécessaires pour assurer le fonctionnement des procédés physiques.

Logiciel anti-virus : logiciel qui protège un ordinateur contre les virus et programmes malveillants. Dès qu'il détecte la présence d'un code malveillant, le logiciel antivirus s'efforce de nettoyer, de supprimer ou de mettre en quarantaine les fichiers, répertoires ou disques infectés.

Logiciel d'historisation : un logiciel d'historisation de SCI est un logiciel spécialisé qui collecte des valeurs ponctuelles, des événements d'alarme, des enregistrements par lots et d'autres informations sur des dispositifs et systèmes industriels, et les stocke dans une base de données prévue à cet effet, c'est-à-dire une base centralisée permettant d'analyser les données par des techniques statistiques de contrôle des procédés.

Logiciel de supervision et contrôle à distance (SCADA) : logiciel permettant de contrôler des équipements dispersés dans les cas où une acquisition centralisée des données est aussi importante que le contrôle. Les systèmes SCADA sont utilisés dans les systèmes de distribution tels que les suivants :

1. réseaux de distribution d'eau et de collecte des eaux usées ;
2. oléoducs et gazoducs ;
3. systèmes de transport et de distribution d'électricité ;
4. réseaux ferroviaires et autres réseaux de transport public.

Les systèmes SCADA intègrent des systèmes d'acquisition de données, de transmission de données et des logiciels d'interface homme-machine (IHM) afin de centraliser la surveillance et le contrôle de nombreuses entrées et sorties de procédés. Ils sont conçus pour collecter des informations sur le terrain, les transférer à un centre informatique et les afficher à l'opérateur sous forme graphique ou textuelle, lui permettant ainsi de surveiller ou de piloter tout un système en temps quasi réel depuis un emplacement central. En fonction de la complexité et de la configuration, le contrôle d'un système, d'une opération ou d'une tâche peut être automatique ou effectué par des commandes opérateur.

Menace interne : menace (délibérée ou involontaire) provenant de personnes au sein de l'entreprise (employés mécontents, anciens collaborateurs, sous-traitants, partenaires, etc.) qui disposent d'informations

confidentielles concernant les pratiques de sécurité, les données et les systèmes informatiques de l'entreprise.

Mot de passe par défaut : mot de passe standard fourni sur un système à sa livraison ou son installation. Les utilisateurs devraient toujours modifier immédiatement le mot de passe par défaut.

Pare-feu : dispositif de sécurité destiné à surveiller le trafic réseau entrant et sortant, et à l'autoriser ou le bloquer en fonction d'un ensemble défini de règles de sécurité.

Passerelle réseau : mécanisme de relais rattaché à au moins deux réseaux informatiques aux fonctions similaires, mais aux déploiements différents, qui permet aux ordinateurs hôtes d'un réseau de communiquer avec les hôtes du ou des autres réseaux.

Passerelle unidirectionnelle : dispositif matériel comportant deux nœuds ou circuits (un qui émet uniquement et l'autre qui reçoit uniquement) qui ne laissent passer les données que dans un sens, d'une source vers une destination. Il utilise une LED comme émetteur de données d'un côté, et un photorécepteur de l'autre ; il est donc physiquement impossible que les données circulent dans l'autre sens. Dans certains cas, une solution logicielle (par exemple, via un paramètre de pare-feu), voire la configuration de commutateur ou de routeur réseau constitue une passerelle unidirectionnelle, mais une « vraie » passerelle unidirectionnelle se compose d'une ou de plusieurs diodes de données unidirectionnelles. D'après la norme NIST 800-82 : Les passerelles unidirectionnelles combinent matériel et logiciel. Le matériel permet aux données de circuler d'un réseau à un autre, mais est physiquement incapable de renvoyer la moindre information vers le réseau source. Le logiciel réplique les bases de données et émule les serveurs de protocole et les appareils. »

Périphérique d'entrée/sortie (E/S) : terme générique désignant l'équipement utilisé pour communiquer avec un ordinateur ou un système de contrôle-commande.

Politique : ensemble de règles régissant le déroulement de certaines procédures.

Poste de travail opérateur : poste de travail qui fournit une vue dynamique de tous les procédés du site nécessaires pour exploiter les systèmes de contrôle-commande. Elle présente des graphiques de contrôle, des diagnostics, des tendances, des alarmes et des affichages d'état.

Procédure : étapes effectuées pour réaliser une tâche donnée.

Progiciel de gestion intégré (ERP) : logiciel utilisé dans les environnements d'entreprise, par exemple SAP et Oracle/PeopleSoft. Ce type de logiciel permet essentiellement de gérer les ordres de production, le stockage, et le transport des commandes terminées.

Programme malveillant : terme générique utilisé pour décrire des logiciels malveillants tels que des virus, chevaux de Troie, logiciels espions et contenus actifs malveillants.

Protection en profondeur : pratique visant à superposer plusieurs contrôles de sécurité afin de protéger les environnements informatique et opérationnel.

Protocole : système de règles utilisé par deux composants partageant des données dans le but de comprendre les données partagées. Un protocole n'est pas un « langage », mais peut être considéré comme la grammaire et la syntaxe permettant de véhiculer ce langage. Dans le domaine des SCI, bon nombre de protocoles sont propres à chaque fournisseur, ont été conçus dans une optique de fonctionnalité et de fiabilité plutôt que de sécurité et sont généralement transmis en texte clair (non crypté). Il est donc d'autant plus nécessaire de séparer les environnements OT et IT. Des exemples de protocoles SCI courants dans l'industrie sont Modbus RTU, Modbus TCP, Profibus, Profinet, DNP3 et ControlNet. Côté IT, les protocoles basés sur TCP/IP (FTP, DNS, HTTP, HTTPS) sont répandus.

Ransomware : type de programme malveillant qui empêche le fonctionnement d'un équipement ou bloque l'accès aux données jusqu'à ce que le propriétaire ou l'opérateur réponde à une demande de rançon.

Réseau de technologie opérationnelle (OT) : le terme OT est souvent utilisé de manière interchangeable avec système de contrôle-commande industriel (SCI) ou réseau de systèmes de commande des procédés (PCN). Il vise à faire la distinction entre le réseau des technologies d'information (IT) et le réseau qui contrôle les équipements opérationnels (OT). Les SCI comprennent divers contrôleurs et instruments destinés à surveiller et à contrôler un procédé physique, tandis que le réseau OT englobe les systèmes et l'infrastructure informatiques qui gèrent les opérations industrielles (y compris les SCI).

Réseau des sécurités instrumentées : réseau qui connecte des systèmes instrumentés de sécurité pour la transmission d'informations liées à la sécurité.

Réseau des technologies d'information (IT) : réseau généralement utilisé dans le cadre d'activités faisant intervenir des ordinateurs pour créer, manipuler, stocker, récupérer et transmettre des données.

Réseau local (LAN) : réseau de communication conçu pour connecter des ordinateurs et d'autres dispositifs intelligents dans une zone géographique restreinte (généralement moins de 10 kilomètres).

Réseau privé virtuel (VPN) : connexion sécurisée entre un réseau public (généralement, Internet) et un réseau privé.

Réseau OT : réseau prioritaire généralement connecté à des équipements qui commandent des procédés physiques. Le réseau OT peut être subdivisé en zones, et plusieurs réseaux OT distincts peuvent coexister au sein d'une même entreprise et d'un même site.

Routeur réseau : passerelle entre deux réseaux au niveau de la couche 3 de l'interconnexion des systèmes ouverts (OSI), qui relaie et achemine les paquets de données dans cette interconnexion. Le type le plus courant de routeur réseau opère sur les paquets du protocole Internet (IP).

Salle de commande des procédés : local coupe-feu et/ou isolé dans lequel du personnel pilote et contrôle les procédés depuis un emplacement central ou distant. La salle de commande des procédés est généralement séparée, mais intégrée aux locaux des équipements de commande industriels, afin de contrôler le fonctionnement des équipements. Les systèmes de commande des procédés sont très répandus dans l'industrie. Ils permettent souvent de produire en masse avec des procédés continus (papier, produits pharmaceutiques, produits chimiques et électricité) ainsi que d'autres procédés industriels. Dans certaines configurations, les salles de commande des procédés/espaces techniques peuvent être inoccupés et pilotés à distance.

Salle de contrôle des procédés : voir Salle de commande des procédés.

Salle de contrôle SCADA : salle de commande utilisant des ordinateurs équipés du logiciel SCADA pour surveiller et commander des équipements situés sur un site ou sur plusieurs sites géographiquement distants. Elle se trouve généralement dans un bâtiment dépourvu de système de commande des procédés local (système numérique de contrôle-commande ou automate programmable industriel). Elle gère un trafic de données bidirectionnel et peut modifier le fonctionnement des équipements distants.

Salle de contrôle : voir Salle de commande des procédés.

Segmentation : division d'un réseau en sections plus petites et compartimentées qui font toujours partie du même réseau global. Dans les SCI, la segmentation s'effectue généralement par le biais de réseaux locaux virtuels (VLAN) ou de pare-feux matériels. Cette segmentation permet de ralentir la propagation de programmes malveillants ou de faire obstacle à un attaquant. Toutefois, l'utilisation de VLAN n'est pas une méthode acceptable pour séparer les réseaux IT et OT.

Séparation : Isolation adéquate de différents réseaux considérés comme mutuellement non approuvés. Cette isolation est obtenue généralement à l'aide de pare-feux (et idéalement d'une DMZ formelle) ou d'une passerelle unidirectionnelle. La séparation des réseaux SCI par rapport aux systèmes IT est essentielle.

Serveur de rebond : type de serveur qui fournit des services de gestion d'une connexion à distance depuis l'extérieur du réseau local. Communément appelés serveurs de rebond.

Solutions de recherche des équipements :

1. Surveillance passive : technique de surveillance discrète et non intrusive utilisée pour enregistrer le trafic d'un réseau en le copiant, souvent à partir d'un port SPAN ou miroir, ou via un TAP réseau. Les solutions de détection d'intrusion basées sur les systèmes OT ont recours à cette technique pour détecter les équipements ainsi que les activités non autorisées.
2. Surveillance active : technique de surveillance intrusive, consistant à émettre des requêtes dans le langage natif (protocole) du contrôleur concerné, qui varie légèrement selon le fabricant. Une approche de surveillance active suppose de demander à un contrôleur des informations détaillées (adresses IP et MAC, version du firmware, configuration de la carte mère, etc.).

Solutions WAN (réseau étendu) : un réseau étendu (WAN) est un réseau informatique qui s'étend sur de vastes régions, des pays, voire le monde entier. Les données sont transférées entre des réseaux qui

couvrent une zone géographique, différents types de connexions permettant de créer ces WAN. Parmi les solutions câblées figurent les technologies MPLS, T1, et les circuits virtuels persistants. Les services de communication sans fil incluent la 4G et la 5G, le Wi-Fi et les réseaux par satellite.

Station ingénierie : en général, plateforme informatique haut de gamme très fiable conçue pour la configuration, la maintenance et le diagnostic des applications et autres équipements du système de contrôle-commande. Elle contient généralement le logiciel spécifique du fournisseur qui permet de programmer les appareils, ainsi que les fichiers de projet utilisés pour programmer les appareils, tels que les automates et les IHM.

Système d'exploitation : logiciel sous-jacent qui permet d'interagir avec un ordinateur. Le système d'exploitation contrôle les fonctions de stockage, de communication et de gestion des tâches de l'ordinateur.

Système de commande de base de la production : système qui gère les équipements, la production et les procédés d'un site. À partir de conditions prédéfinies, le système de commande de base de la production utilise le retour d'information des boucles de contrôle pour automatiser et maintenir une condition, une production ou un procédé souhaité(e). Les systèmes de commande de base de la production sont personnalisés pour répondre aux besoins de tous types de procédés, qu'il s'agisse de systèmes très vastes et complexes comme la production d'énergie ou les procédés chimiques, ou de systèmes très simples avec une seule entrée et une seule sortie comme les détecteurs de mouvement ou les systèmes d'éclairage.

Système de contrôle-commande industriel (SCI) :

1. Terme générique qui englobe plusieurs types de systèmes de contrôle-commande souvent présents dans les secteurs industriels et les infrastructures stratégiques, notamment les systèmes de supervision et contrôle à distance (SCADA), les systèmes numériques de contrôle-commande et d'autres configurations telles que les automates et les unités logiques programmables de sécurité. Un SCI regroupe divers composants de contrôle-commande (par exemple, électriques, mécaniques, hydrauliques, pneumatiques) qui, ensemble, permettent d'atteindre un objectif industriel (par exemple, la fabrication, la production et le transport de matière ou d'énergie).
2. Ensemble du personnel, du matériel et des logiciels qui peuvent jouer un rôle dans le fonctionnement sûr, sécurisé et fiable d'un procédé industriel.

Système de détection d'intrusion : service de sécurité qui surveille et analyse les événements du réseau ou du système afin de détecter et de signaler en temps réel ou quasi réel toute tentative d'accès aux ressources du système par des moyens non autorisés. Un système de détection d'intrusion permet de détecter et d'alerter, mais ne peut ni bloquer ni rejeter le trafic indésirable.

Système de pilotage de la production (MES) : système informatisé utilisé dans les environnements de production et de fabrication pour assurer le suivi des inventaires ou d'autres informations sur la production, comparable à un progiciel ERP, mais davantage axé sur la fabrication (par exemple, suivi et documentation de la transformation des matières premières en produits finis).

Système de sécurité : système servant à mettre en œuvre une ou plusieurs fonctions instrumentées de sécurité. Il regroupe des capteurs, des unités logiques programmables et des actionneurs.

Système numérique de contrôle-commande : Un système numérique de contrôle-commande est un système de contrôle automatisé qui gère les procédés en distribuant les fonctions de contrôle sur plusieurs composants interconnectés. Il utilise des composants distribués plutôt qu'une seule unité centralisée. Il convient de noter que le terme « contrôleur du système numérique de contrôle-commande » désigne le contrôleur physique, tandis que le terme « système numérique de contrôle-commande » désigne l'ensemble du système, y compris les serveurs d'applications, l'IHM, etc.

Tableaux de commande industriels : assemblage comprenant au moins deux composants de circuit de commande et de circuit électrique. Parmi les composants de circuit de commande figurent les automates, les modules d'entrée et de sortie, les entraînements moteur et les modules de communication. Les composants de circuit électrique incluent des alimentations électriques, des onduleurs, des relais, des transformateurs électriques et des convertisseurs de tension/courant. Les tableaux de commande industriels fonctionnent en général avec une puissance de 600 volts ou moins, bien que les normes UL 508A et IEC autorisent une puissance de 1 000 volts.

Transmission unidirectionnelle : ensemble de stratégies utilisées pour assurer des communications unidirectionnelles sécurisées à partir de dispositifs ou entre différents réseaux/zones de protection, du type :

1. envoi d'un signal analogique seul (intensité ou tension) vers/depuis un dispositif au lieu de données numériques ;
2. utilisation d'une passerelle unidirectionnelle ;
3. utilisation de règles dans un pare-feu ou une DMZ pour transmettre des données entre des réseaux.

Unité de terminal à distance (RTU) : unité conçue pour prendre en charge les stations à distance des systèmes numériques de contrôle-commande et des systèmes de supervision et contrôle à distance (SCADA). Les RTU sont des appareils de terrain utilisés pour surveiller les paramètres. Ils communiquent avec un contrôleur de supervision à l'aide de fonctionnalités de communication à distance, qui peuvent inclure des interfaces par modem, téléphone portable ou radio, ou toute autre technologie de communication étendue. Parfois, des automates sont mis en place en tant qu'appareils de terrain pour servir de RTU. Dans ce cas, ils sont généralement appelés RTU. Ils sont souvent installés dans des endroits où l'accès à l'électricité est difficile et peuvent être alimentés par électricité photovoltaïque.

Vecteur d'attaque : procédé ou moyen par lequel un auteur de menace accède ou porte atteinte aux données ou au réseau informatique d'une entreprise. Le déni de service, les programmes malveillants, l'accès physique, les ransomwares et l'ingénierie sociale sont des exemples de vecteurs d'attaque.

Vulnérabilité : faille ou faiblesse dans la conception, la mise en œuvre, ou l'exploitation et la gestion d'un système qui pourrait être mise à profit pour violer l'intégrité ou la politique de sécurité du système.

Zone démilitarisée (DMZ industrielle) :

1. Interface d'un pare-feu de routage semblable aux interfaces présentes du côté protégé du pare-feu. Le trafic entre la zone démilitarisée et les autres interfaces du côté protégé du pare-feu passe toujours par le pare-feu et peut être soumis à des règles de sécurité du pare-feu.
2. Hôte ou segment de réseau intercalé en guise de « zone neutre » entre le réseau privé d'une entreprise et le réseau Internet. La plupart des zones démilitarisées sont entre et les environnements IT et OT de l'entreprise
3. Segment de réseau périphérique situé logiquement entre les réseaux internes et externes. Sa fonction est d'appliquer les règles du réseau interne en matière d'échange d'informations externes et de limiter l'accès des sources externes non approuvées aux seules informations pouvant être divulguées, tout en protégeant les réseaux internes des attaques extérieures.

ANNEXE B HISTORIQUE DE RÉVISION DU DOCUMENT

L'objet de cette annexe est de rendre compte des modifications apportées à ce document à chacune de ses publications. Veuillez noter que les numéros de section se réfèrent spécifiquement à ceux de la version publiée à la date indiquée. En d'autres termes, les numéros de section peuvent varier d'une version à l'autre.

Juillet 2024. Révision intermédiaire. Des changements éditoriaux ont été apportés.

Janvier 2024. Révision intermédiaire. Changements éditoriaux mineurs.

Juillet 2023. Révision intermédiaire. Les modifications importantes suivantes ont été apportées :

A. Amélioration et clarification des recommandations relatives à la protection incendie
    1. Amélioration des recommandations relatives à la protection incendie propre à l'activité et à celle des équipements
B. Mise à jour des recommandations relatives à la sécurité des SCI
    1. Ajout de recommandations relatives à la connexion à distance aux salles de contrôle SCADA
C. Ajout de termes à l'annexe A Glossaire

Janvier 2023. Révision intermédiaire. Les changements suivants ont été effectués :

A. Clarification des recommandations relatives à la protection incendie
B. Clarification des recommandations relatives à la gestion des SCI
C. Clarification et modification des recommandations relatives à la sécurité des SCI :

1. Modification des recommandations relatives à la surveillance de la configuration et du système pour les équipements des réseaux SCI et OT, y compris les systèmes de sécurité
2. Clarification des recommandations relatives à la gestion des correctifs
3. Clarification des recommandations relatives à la protection du réseau

D. Clarification et modification des recommandations relatives au fonctionnement des SCI :

1. Clarification des recommandations relatives à la gestion des alarmes
2. Modification du programme de reprise d'activité, notamment en ce qui concerne les types de fichiers de sauvegarde acceptables

E. Ajout de termes à l'annexe A Glossaire

Juillet 2022. Révision intermédiaire. Changements éditoriaux mineurs.

Octobre 2021. Révision intermédiaire. Mise à jour de la référence aux essais des batteries (section 2.7).

Juillet 2021. Révision intermédiaire. Mise à jour et clarification des points suivants :

A. Sécurité des SCI

i. Gestion des accès
ii. Gestion de la configuration
iii. Gestion des correctifs
iv. Protection du réseau

B. Fonctionnement des SCI

i. Procédures d'exploitation d'urgence

C. Recommandations relatives à la construction et au risque d'incendie

Juillet 2020. Révision intermédiaire. Mise à jour des recommandations relatives au plan de secours des équipements et à la disponibilité de pièces de rechange.

Octobre 2019. Il s'agit de la première édition de ce document.