Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Secrétariat général

Centre national pour la cybersécurité NCSC
www.ncsc.admin.ch

NCSC

Liste de contrôle et instructions

Mesures de protection pour les systèmes de contrôle industriels (SCI)

Table des matières

1 Introduction

Les systèmes de contrôle ou de pilotage se composent d'un ou plusieurs appareils qui assurent, commandent ou surveillent le fonctionnement d'autres appareils ou systèmes. L'expression «systèmes de contrôle industriels» (*industrial control systems*, SCI) est largement utilisée dans le domaine de la production industrielle. Depuis quelque temps, les systèmes de contrôle ou de pilotage industriels trouvent de nouveaux débouchés également en dehors de l'industrie manufacturière, par exemple dans la domotique ou la gestion du trafic. On peut parler de système de contrôle industriel pour tout système de contrôle qui commande ou surveille un processus physique. La plupart des règles de base destinées à protéger de tels systèmes s'appliquent aussi en dehors de l'industrie manufacturière, d'où l'emploi dans le présent document du terme SCI pour les systèmes de contrôle industriels au sens large.

Le SANS[1], un institut américain spécialisé dans la sécurité, a publié 20 éléments-clés[2] indiquant comment protéger les infrastructures informatiques en général. Ces éléments s'appliquent en partie également aux SCI. D'autres recommandations ont été émises par l'US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT[3]) et par le National Institute of Standards and Technology (NIST[4]).

Les instructions suivantes se fondent sur les documents susmentionnés.

2 Résumé

Vous trouverez des instructions détaillées à la fin du présent document.

11 Mesures de protection des systèmes de contrôle industriels (SCI)

1. Créer et tenir à jour une base de données des ressources matérielles
2. Mettre en place un cycle de vie et une gestion des correctifs (*patchs*) pour les logiciels
3. Définir et utiliser des configurations sécurisées
4. Planifier et mettre en place des architectures réseau robustes
5. Mettre en place plusieurs niveaux de protection contre les maliciels
6. Mettre en place un système d'authentification et d'autorisation
7. Procéder à une évaluation centralisée des fichiers journaux
8. Garantir la protection physique
9. Effectuer et tester régulièrement les sauvegardes et la récupération de fichiers
10. Établir et exercer les processus de gestion des incidents de sécurité
11. Instaurer une culture de la sécurité

[1] SANS: http://www.sans.org

[2] SANS Top 20 Critical Security Controls: http://www.sans.org/critical-security-controls/

[3] ICS CERT: http://ics-cert.us-cert.gov/

[4] NIST: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

3 Mesures de protection des systèmes de contrôle industriels (SCI)

Les mesures énumérées ci-après devraient faire partie d'un processus de sécurité global qui en garantisse l'application, le contrôle régulier et l'amélioration constante. Il est en outre important que l'exploitant d'une installation connaisse les menaces actuelles et qu'il les évalue régulièrement afin d'améliorer les mesures de sécurité ou d'en mettre en place de nouvelles. À cet effet, une étroite collaboration est cruciale entre les processus de gestion des risques, de l'ingénierie et d'exploitation.

Dans la plupart des cas, il n'est pas possible de renforcer la sécurité par une action ponctuelle. Il s'agit d'un processus continu qui ne devrait jamais être interrompu. Nous vous conseillons par conséquent de vous fixer des objectifs réalistes et réalisables, et de vous concentrer en premier lieu sur les points qui permettent de renforcer sensiblement la sécurité moyennant peu d'efforts. Vous pouvez par exemple dans un premier temps modifier tous les mots de passe par défaut et protéger les interfaces de commande accessibles de l'extérieur.

3.1 Base de données des ressources matérielles

Mesure	Gestion d’une base de données recensant tous les éléments de pilotage, des systèmes périphériques aux terminaux «normaux»
Justification	Une protection efficace et concrète n'est possible qu'en connaissant les éléments à protéger et ceux dignes de confiance.
Conseils pratiques	Il existe différents moyens techniques permettant d’atteindre cet objectif. Pour obtenir un premier aperçu, utilisez un outil d'inventaire de réseau. Faites toutefois preuve d'une grande prudence en cas d'analyse active: beaucoup de SCI ne sont pas prévus pour supporter un trafic réseau inattendu, ce qui risque de provoquer un dysfonctionnement. Mettez en place une alarme qui se déclenche lorsque des appareils inconnus se connectent au réseau. Il est possible d'utiliser à cet effet les adresses MAC des appareils. Même s’il est facile de falsifier une adresse MAC, une telle mesure est néanmoins très efficace pour détecter des appareils étrangers.

3.2 Utilisation des logiciels

Mesure	Gestion d’une base de données recensant tous les éléments logiciels. C’est d’ailleurs la base d’une bonne gestion des correctifs de sécurité (*patchs*), des mises à jour et du cycle de vie. Il convient d’utiliser, autant que faire se peut, une liste blanche sur tous les appareils sensibles afin d'y exécuter uniquement des logiciels connus.
Justification	La base de données des ressources logicielles est le fondement de la gestion des changements, des correctifs et des

	mises à jour. De nombreuses intrusions – notamment les attaques ciblées – utilisent des systèmes peu protégés ayant des droits élevés, tels que les appareils des administrateurs ou des développeurs. Entraver cette possibilité d'attaque compliquera sensiblement la tâche aux cybercriminels. De façon générale, la gestion du cycle de vie des SCI est cruciale en raison de leur très longue durée de vie.
Conseils pratiques	Vous pouvez vous faciliter la création d'une base de données en utilisant des logiciels prévus à cet effet (*software inventory tools*). La gestion des correctifs est très délicate pour les SCI et ne peut souvent se faire qu'en collaboration avec le fournisseur (pour des questions de garantie), ce qui engendre généralement de longues périodes de vulnérabilité du système. Réduisez les risques liés aux logiciels en créant une liste blanche des applications exécutables. La grande majorité des intrusions commencent par l'exécution d'un logiciel sur la machine attaquée. Avec une liste blanche, seule l'exécution de programmes approuvés est autorisée.

3.3 Configuration sécurisée

Mesure	Configuration sécurisée
Justification	Les cybercriminels tirent souvent parti des mots de passe faibles ou des mots de passe par défaut.
Conseils pratiques	Vos interfaces d'administration ne devraient jamais être directement accessibles par Internet. Si cela s'avère toutefois nécessaire, imposez une restriction des adresses IP autorisées. Conformez-vous strictement aux instructions de sécurité et de durcissement (*hardening*) des systèmes émises par le fabricant. Utilisez la possibilité, si existante, de signer les logiciels et de déclencher une alarme en cas de modification des logiciels utilisés. De même, assurez-vous qu'aucun mot de passe faible ou mot de passe par défaut n'est utilisé dans vos configurations.

3.4 Architecture réseau robuste

Mesure	Segmentation de l'architecture réseau avec cloisonnement des zones

Justification	Les SCI devraient fonctionner si possible dans des zones cloisonnées, sans accès direct à Internet, afin de réduire au maximum la vulnérabilité aux attaques et compliquer considérablement le passage de la barrière restante. Le réseau des machines de bureau et celui des SCI devraient être complètement séparés. Si cela n'est pas possible, un concept de zones adéquat doit gérer la communication interzone.
Conseils pratiques	Si des éléments doivent être accessibles par Internet, protégez dûment leur accès. Nous vous recommandons d'utiliser les technologies VPN avec authentification à deux facteurs (par ex. un jeton avec mot de passe à usage unique et NIP). De plus, n'autorisez que certaines adresses IP et uniquement à des fins de maintenance. Il en va de même pour la segmentation interne: s'il est nécessaire d'accéder au réseau du SCI depuis le réseau «normal», désignez un moyen prévu à cet effet et mettez en place une authentification et une surveillance. Surveillez les réseaux à l'aide de systèmes spécifiques de détection des intrusions reposant sur des protocoles réseau SCI. Établissez dans la mesure du possible des protocoles réseau sous forme cryptée. Si une telle solution n'existe pas, le trafic réseau peut être acheminé à travers un tunnel. Utilisez toujours le protocole SSL/TLS, notamment pour l'accès aux interfaces d'administration sur le Web. S'il est nécessaire de transmettre régulièrement des données de l'environnement de production au réseau de machines de bureau (par ex. pour des statistiques), l'acheminement peut se faire via un isolateur optique de données (*data diode*) qui ne permet la communication que dans un sens. Cette solution permet d'éviter que du code malveillant ne se propage par ce canal, du réseau des machines de bureau aux systèmes de contrôle.

3.5 Protection à plusieurs niveaux contre les maliciels

Mesure	Protection à plusieurs niveaux contre les maliciels
Justification	Les SCI utilisant des systèmes d'exploitation répandus sur le marché sont exposés aux attaques de maliciels, en particulier car ils doivent souvent être maintenus à un niveau de correctifs antérieur (en raison des prescriptions du fabricant, de la validation ou de la sécurité de la production). Bien souvent, un maliciel est utilisé pour prendre le contrôle de systèmes auxiliaires, de machines servant à l'administration du réseau ou de serveurs de bases de données eux-mêmes reliés aux SCI. Les anciennes plateformes SCI utilisant des systèmes d'exploitation Windows sont particulièrement exposées aux attaques de maliciels.

Conseils pratiques	Globalement, une bonne protection contre les maliciels est essentielle au fonctionnement correct de tout SCI. Il n'est bien souvent ni possible ni judicieux d'installer des solutions de protection contre les maliciels sur des infrastructures SCI critiques. Par contre, veillez à ce que les machines servant à l'administration ainsi que les serveurs Windows «normaux» disposent d'une solution de protection antivirus à jour. Mettez en place une protection contre les maliciels à plusieurs niveaux pour que les logiciels non détectés à un niveau puissent l'être à un autre niveau. Surveillez également les flux de données suspects sur le réseau, qui pourraient indiquer une infection par un maliciel. Nous vous recommandons de veiller à ce qu'aucun système concerné ne soit directement relié à Internet et d'autoriser uniquement des liaisons point à point via un serveur proxy.

3.6 Authentification et autorisation

Mesure	Authentification et autorisation sécurisées de toutes les personnes et de tous les systèmes concernés
Justification	L'authentification et l'octroi des droits revêtent une grande importance. En effet, les cybercriminels peuvent très rapidement et très facilement exploiter les lacunes dans ce domaine.
Conseils pratiques	Exigez là où c'est possible une authentification et octroyez le minimum de droits d'accès en matière d'autorisation. Divers SCI ou protocoles SCI ne supportent qu'une authentification rudimentaire, voire aucune. Le cas échéant, prenez des mesures compensatoires, exigez par exemple une authentification à l'entrée du réseau du SCI. Assurez-vous qu'aucun compte d'utilisateur standard avec le mot de passe par défaut n'existe. Choisissez des mots de passe aussi forts que possible et mettez en place une authentification à deux facteurs pour les interfaces d'administration exposées. N'octroyez aux utilisateurs – notamment aux entreprises chargées de la maintenance – que les droits dont ils ont réellement besoin pour exécuter leur tâche.

3.7 Analyse centralisée des fichiers journaux

Mesure	Regroupement, analyse et conservation centralisés des fichiers journaux (*logs*) de tous les systèmes
Justification	Ce n'est qu'en regroupant tous les fichiers journaux qu'il est possible de comprendre les liens entre des événements isolés et d'identifier les cyberattaques.
Conseils pratiques	Déterminez les événements à consigner pour chaque classe de systèmes, qu'il s'agisse d'un SCI, d'une machine servant à l'administration ou d'un système périphérique. Conservez les données enregistrées le plus longtemps possible. Ce n'est parfois que des mois ou des années plus tard que l'on découvre des attaques fructueuses qui ne s'expliquent souvent qu'à l'aide des fichiers journaux. Définissez une base de référence pour les événements liés à un fonctionnement normal et sans incident. Analysez toujours les écarts, les erreurs et les comportements inattendus.

3.8 Protection physique

Mesure	Protection des SCI et des systèmes périphériques qui y sont directement ou indirectement reliés contre tout accès physique non autorisé
Justification	En règle générale, le degré de protection des SCI contre les intrusions physiques est très élevé. Il faut toutefois aussi tenir compte des systèmes périphériques, des postes d'accès à distance pour la maintenance ainsi que des autres installations gérées à distance, car l'accès physique à un raccordement permet généralement de contourner les mesures de sécurité adoptées au niveau du réseau.
Conseils pratiques	Étendez la recherche de failles dans la protection physique des SCI en place aux systèmes périphériques, aux systèmes d'administration et aux éventuels systèmes à distance. Toute interface physique offre un accès facilité au réseau.

3.9 Procédures de sauvegarde et de restauration de fichiers

Mesure	Mise en place et tests réguliers des procédures de sauvegarde et de restauration de fichiers autant pour les SCI proprement dits que pour les systèmes périphériques qui y sont reliés, et contrôles réguliers de l'intégrité des fichiers de sauvegarde
Justification	Les sauvegardes sont rarement testées. En cas d'incident, on dispose certes de fichiers de sauvegarde, mais ces derniers risquent d'être illisibles ou difficilement utilisables.
Conseils pratiques	Stockez les sauvegardes en lieu sûr, à distance du système dont elles proviennent. Sauvegardez non seulement les données, mais aussi les fichiers de configuration. Testez la récupération des sauvegardes au moins une fois par an, de préférence tous les six mois. Contrôlez régulièrement l'intégrité des fichiers de sauvegarde. Pour ce faire, calculez et conservez les valeurs de hachage cryptographique de chacun d'eux.

3.10 Processus de gestion des incidents de sécurité

Mesure	Définition de processus bien rodés et prêts à l'emploi en cas d'incident, portant sur la prévention, la détection et la réaction
Justification	En cas d'incident, une réaction correcte et décidée permet en général de limiter fortement les dommages.
Conseils pratiques	Intégrez les SCI au processus normal de gestion des incidents de sécurité informatique. Analysez toujours un comportement inexplicable d'un SCI, car il est parfois impossible d'identifier au premier coup d'œil un incident de sécurité. Dans le but d'une amélioration constante de la sécurité, analysez toujours les causes des incidents de sécurité et définissez les mesures à prendre pour éviter que de tels incidents ne se reproduisent.

3.11 Mise en place d'une culture de la sécurité

Mesure	Mise en place d’une culture de la sécurité spécifiant les responsabilités et les processus
Justification	La sécurité doit être prise en compte dans tous les processus opérationnels. Les mesures requises et les risques existants doivent faire l'objet d'un rapport à transmettre directement et fidèlement à la direction qui doit être informée des risques particuliers et des propriétés des systèmes de contrôle industriels.
Conseils pratiques	Intégrez les processus de sécurité aux processus opérationnels courants et aux cycles de contrôle usuels. Procédez à des contrôles réguliers, tant techniques qu’organisationnels, du bon fonctionnement et de la réalisation des objectifs. Là où cela est nécessaire, prévoyez et mettez en œuvre des améliorations. Désignez un acteur aussi indépendant que possible et accordez-lui les ressources et les compétences nécessaires, afin qu’il procède aux contrôles requis et en communique les résultats à la direction. La responsabilité en matière de sécurité incombe toujours à la direction.