SIEMENS

# SINUMERIK / SIMOTION / SINAMICS

# Motion Control Industrial Security

Manuel de configuration




02/2020
6FC5397-5EP40-6DA1

## Mentions légales

### Signalétique d'avertissement

Ce manuel donne des consignes que vous devez respecter pour votre propre sécurité et pour éviter des dommages matériels. Les avertissements servant à votre sécurité personnelle sont accompagnés d'un triangle de danger, les avertissements concernant uniquement des dommages matériels sont dépourvus de ce triangle. Les avertissements sont représentés ci-après par ordre décroissant de niveau de risque.

| ⚠ DANGER |
| --- |
| signifie que la non-application des mesures de sécurité appropriées **entraîne** la mort ou des blessures graves. |

| ⚠ ATTENTION |
| --- |
| signifie que la non-application des mesures de sécurité appropriées **peut entraîner** la mort ou des blessures graves. |

| ⚠ PRUDENCE |
| --- |
| signifie que la non-application des mesures de sécurité appropriées peut entraîner des blessures légères. |

| IMPORTANT |
| --- |
| signifie que la non-application des mesures de sécurité appropriées peut entraîner un dommage matériel. |

En présence de plusieurs niveaux de risque, c'est toujours l'avertissement correspondant au niveau le plus élevé qui est reproduit. Si un avertissement avec triangle de danger prévient des risques de dommages corporels, le même avertissement peut aussi contenir un avis de mise en garde contre des dommages matériels.

### Personnes qualifiées

L'appareil/le système décrit dans cette documentation ne doit être manipulé que par du **personnel qualifié** pour chaque tâche spécifique. La documentation relative à cette tâche doit être observée, en particulier les consignes de sécurité et avertissements. Les personnes qualifiées sont, en raison de leur formation et de leur expérience, en mesure de reconnaître les risques liés au maniement de ce produit / système et de les éviter.

### Utilisation des produits Siemens conforme à leur destination

Tenez compte des points suivants:

| ⚠ ATTENTION |
| --- |
| Les produits Siemens ne doivent être utilisés que pour les cas d'application prévus dans le catalogue et dans la documentation technique correspondante. S'ils sont utilisés en liaison avec des produits et composants d'autres marques, ceux-ci doivent être recommandés ou agréés par Siemens. Le fonctionnement correct et sûr des produits suppose un transport, un entreposage, une mise en place, un montage, une mise en service, une utilisation et une maintenance dans les règles de l'art. Il faut respecter les conditions d'environnement admissibles ainsi que les indications dans les documentations afférentes. |

### Marques de fabrique

Toutes les désignations repérées par ® sont des marques déposées de Siemens AG. Les autres désignations dans ce document peuvent être des marques dont l'utilisation par des tiers à leurs propres fins peut enfreindre les droits de leurs propriétaires respectifs.

### Exclusion de responsabilité

Nous avons vérifié la conformité du contenu du présent document avec le matériel et le logiciel qui y sont décrits. Ne pouvant toutefois exclure toute divergence, nous ne pouvons pas nous porter garants de la conformité intégrale. Si l'usage de ce manuel devait révéler des erreurs, nous en tiendrons compte et apporterons les corrections nécessaires dès la prochaine édition.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
ALLEMAGNE

Numéro de référence du document: 6FC5397-5EP40-6DA1
℗ 04/2020 Sous réserve de modifications

# Avant-propos

Sous ce lien (https://support.industry.siemens.com/cs/de/en/view/108464614), vous trouverez différentes informations pour :

- Commander la documentation/Vue d'ensemble des documents
- Télécharger des documents à partir de liens supplémentaires
- Utiliser la documentation en ligne (trouver des manuels/informations et y effectuer des recherches)

Pour toute question concernant la documentation technique (p. ex. suggestion, correction), envoyez un e-mail à cette adresse (mailto:docu.motioncontrol@siemens.com).

## mySupport/Documentation

Plus d'informations sur la documentation Siemens disponible et sur les possibilités de l'utiliser pour créer votre propre documentation machine, voir : lien (https://support.industry.siemens.com/My/ww/fr/documentation).

## Formation

Ce lien (https://www.siemens.com/sitrain) livre des informations sur SITRAIN, le programme de formations de Siemens pour les produits, systèmes et solutions d'entraînements et d'automatisation.

## FAQ

La Foire Aux Questions se trouve sur les pages Service&Support sous Support produit (https://support.industry.siemens.com/cs/de/en/ps/faq).

## SINUMERIK

Des informations relatives à SINUMERIK figurent à cette adresse (https://www.siemens.com/sinumerik).

## SIMOTION

Des informations relatives à SIMOTION figurent à cette adresse (https://www.siemens.com/simotion).

## SINAMICS

Des informations sur SINAMICS figurent à cette adresse (https://www.siemens.com/sinamics).

## Audience cible

La présente documentation s'adresse aux constructeurs de machines-outils/machines de production et plus particulièrement aux :

- Concepteurs
- Services informatique chez les clients finaux et les OEM

Pour la mise en œuvre des concepts de sécurité décrits, les connaissances suivantes sont supposées acquises :

- Administration des technologies informatiques du monde de la bureautique
- Configuration des produits SINUMERIK / SIMOTION / SINAMICS utilisés

## Utilisation

La documentation "Industrial Security" contient des recommandations et des informations pour la planification et la mise en place de systèmes ou d'installations. À ce titre, la documentation sert de manuel de référence et de guide. Cette documentation ne peut ni ne souhaite suggérer une sécurité à 100 %, car le scénario de menace est de nos jours beaucoup trop varié et complexe.

La présente documentation rassemble toutes les dispositions dont le respect est nécessaire pour la configuration de systèmes dans un environnement sécurisé. Elle vise à assister le fabricant de machines dans l'exploitation sécurisée de son automate ou de son installation. En tant qu'exploitant, vous êtes responsable de la mise en œuvre des mesures de sécurité.

## Remarque concernant le règlement général sur la protection des données

Siemens respecte les principes de la protection des données, en particulier l'impératif de minimisation des données (protection de la vie privée dès la conception). Pour ce produit, cela signifie :

Le produit ne traite/n'enregistre aucune donnée à caractère personnel mais uniquement des données techniques fonctionnelles (p. ex. horodatage). Si l'utilisateur relie ces données à d'autres données (p. ex. plannings d'équipes) ou s'il enregistre des données à caractère personnel sur le même support (p. ex. disque dur) et crée par là même un lien avec des personnes, il est tenu de garantir le respect des prescriptions en matière de protection des données.

## Technical Support

Si vous avez besoin de conseils techniques, vous trouverez sur Internet les coordonnées téléphoniques appropriées à l'adresse (https://support.industry.siemens.com/sc/ww/fr/sc/support-technique/oid2090) suivante, dans la zone "Contact".

Pour poser une question technique, utilisez le formulaire en ligne dans la zone de demande d'assistance "Support Request".

# Sommaire

# Consignes de sécurité élémentaires

# 1

## 1.1 Consignes de sécurité générales

**⚠ ATTENTION**

**Le non respect des consignes de sécurité et le manque de prise en compte des risques résiduels peuvent entraîner la mort**

Le non respect des consignes de sécurité et des remarques relatives aux risques résiduels dans la documentation du matériel peut conduire à des accidents susceptibles d'entraîner la mort ou de causer des blessures graves.

- Respecter les consignes de sécurité figurant dans la documentation du matériel.
- Tenir compte des risques résiduels pour l'évaluation des risques.

**⚠ ATTENTION**

**Danger de mort lié à des dysfonctionnements de la machine suite à un paramétrage incorrect ou modifié**

Un paramétrage incorrect ou modifié peut entraîner des dysfonctionnements sur les machines, susceptibles de provoquer des blessures, voire la mort.

- Protéger le paramétrage contre l'accès non autorisé.
- Prendre les mesures appropriées pour palier aux défauts éventuels (p. ex. un arrêt ou une coupure d'urgence).

## 1.2 Garantie et responsabilité pour les exemples d'application

Les exemples d'application sont sans engagement et n'ont aucune prétention d'exhaustivité concernant la configuration, les équipements et les éventualités de toutes sortes. Les exemples d'application ne constituent pas des solutions client spécifiques, mais ont uniquement pour objet d'apporter une aide dans la résolution de problèmes typiques.

L'utilisateur est seul responsable de la mise en œuvre des produits selon les règles de l'art. Les exemples d'application ne vous dispensent pas des obligations de précaution lors de l'utilisation, de l'installation, de l'exploitation et de la maintenance.

## 1.3 Note relative à la sécurité

Siemens commercialise des produits et solutions comprenant des fonctions de sécurité industrielle qui contribuent à une exploitation sûre des installations, systèmes, machines et réseaux.

Pour garantir la sécurité des installations, systèmes, machines et réseaux contre les cybermenaces, il est nécessaire de mettre en œuvre - et de maintenir en permanence - un concept de sécurité industrielle global et de pointe. Les produits et solutions de Siemens constituent une partie de ce concept.

Il incombe aux clients d'empêcher tout accès non autorisé à ses installations, systèmes, machines et réseaux. Ces systèmes, machines et composants doivent uniquement être connectés au réseau d'entreprise ou à Internet si et dans la mesure où cela est nécessaire et seulement si des mesures de protection adéquates (ex: pare-feu et/ou segmentation du réseau) ont été prises.

Pour plus d'informations sur les mesures de protection pouvant être mises en œuvre dans le domaine de la sécurité industrielle, rendez-vous sur https://www.siemens.com/industrialsecurity (https://www.siemens.com/industrialsecurity).

Les produits et solutions Siemens font l'objet de développements continus pour être encore plus sûrs. Siemens recommande vivement d'effectuer des mises à jour dès que celles-ci sont disponibles et d'utiliser la dernière version des produits. L'utilisation de versions qui ne sont plus prises en charge et la non-application des dernières mises à jour peut augmenter le risque de cybermenaces pour nos clients.

Pour être informé des mises à jour produit, abonnez-vous au flux RSS Siemens Industrial Security à l'adresse suivante:
https://www.siemens.com/industrialsecurity (https://new.siemens.com/global/en/products/services/cert.html#Subscriptions)

Plus d'informations, voir sur Internet :

Manuel de configuration Industrial Security (https://support.industry.siemens.com/cs/ww/fr/view/108862708/en)

**⚠ ATTENTION**

**États de fonctionnement non sûrs suite à une manipulation du logiciel**

Les manipulations des logiciels, p. ex. les virus, chevaux de Troie ou vers, peuvent provoquer des états de fonctionnement non sûrs de l'installation, susceptibles de causer la mort, des blessures graves et des dommages matériels.

- Les logiciels doivent être maintenus à jour.
- Intégrer les composants d'entraînement et d'automatisation dans un concept global de sécurité industrielle (Industrial Security) de l'installation ou de la machine selon l'état actuel de la technique.
- Tenir compte de tous les produits utilisés dans le système global de sécurité industrielle (Industrial Security).
- Il convient de protéger les données stockées sur les supports de mémoire amovibles contre les logiciels nuisibles avec les mesures de protection appropriées, par exemple avec un antivirus.
- Contrôler à l'issue de la mise en service toutes les fonctions relatives à la sécurité.
- Protéger l'entraînement contre toute modification non autorisée en activant la fonction variateur "Protection de savoir-faire".

# Qu'est-ce que la sécurité industrielle ? 2

## Définition de la sécurité industrielle

Par sécurité industrielle ou Industrial Security, on entend généralement toutes les mesures destinées à protéger les éléments suivants :

- Perte de confidentialité liée à un accès non autorisé aux données
- Perte d'intégrité suite à une manipulation des données
- Perte de disponibilité (p. ex. suite à une destruction de données ou un déni de service (DoS))

## Objectifs de Industrial Security

Les objectifs d'Industrial Security comprennent dans ce cadre :

- L'exploitation sans défaut et la garantie de la disponibilité des installations industrielles et des processus de production
- La prévention des risques que les cyberattaques font courir aux personnes et à la production
- La protection de la communication industrielle contre l'espionnage et la manipulation
- La protection des systèmes d'automatisation industrielle et de leurs constituants contre les accès non autorisés et la perte de données
- Un concept praticable et économique pour la protection des installations et appareils existants sans fonctions de sécurité propres
- L'utilisation de normes de sécurité industrielle existantes, ouvertes et éprouvées
- Le respect des prescriptions légales

La technologie d'automatisation et d'entraînement implique un concept de sécurité optimisé et adapté. Les mesures de sécurité ne doivent pas entraver ou mettre en danger la production.

# Pourquoi la sécurité industrielle est-elle si importante ? 3

## 3.1 Interconnexion et technologie sans fil

### Vue d'ensemble

Une multitude de tendances actuelles dans la technologie informatique affecte potentiellement la sécurité industrielle :

- Solutions de cloud computing
  Le nombre des connexions réseau augmente sans cesse au niveau mondial. Cette tendance a permis des innovations telles que le cloud computing et les applications connexes. L'essor du cloud computing s'accompagne de l'augmentation massive du nombre d'appareils mobiles tels que les téléphones portables et les tablettes.
- Technologie sans fil
  L'utilisation accrue d'appareils mobiles a été rendue possible par la disponibilité de réseaux cellulaires sur la quasi-totalité du territoire. De plus, l'utilisation du Wi-Fi est en constante augmentation.
- Accès à distance à des installations, des machines et des applications mobiles dans le monde entier
- Internet des objets / Internet of Things (IoT)
  Des millions d'appareils électroniques sont dotés de fonctions de connexion et communiquent via Internet, tels que p. ex. l'ordinateur de bord d'une voiture fournissant des informations de garantie au constructeur ou encore les compteurs d'eau électroniques transmettant les données de consommation par radio aux services de distribution.

Pour que tout ceci fonctionne sans accroc, du cloud computing jusqu'à l'Internet des objets, des infrastructures de réseau fiables sont nécessaires, protégées des attaques des logiciels malveillants et des pirates.

## 3.2 Failles de sécurité potentielles dans les entreprises

### Failles de sécurité ou points faibles possibles

La chaîne de sécurité d'une entreprise est tributaire de son maillon le plus faible. Des failles de sécurité peuvent exister à de nombreux endroits. La liste ci-après est loin d'être exhaustive :

- Collaborateurs / entreprises tierces
- Installations de production
- Infrastructure de réseau
- Centres de calcul / stations de travail PC
- Ordinateurs portables / tablettes
- Imprimantes
- Smartphones / Smartwatches
- Supports de données mobiles

Par conséquent, le traitement du problème de sécurité nécessite une approche globale, notamment des prescriptions et directives coordonnées qui couvrent tous les domaines : appareils, systèmes, procédés et employés.

Le sujet de la sécurité des données et de la protection d'accès (sécurité) prend aussi une importance grandissante dans l'environnement industriel. Les technologies suivantes impliquent des exigences accrues en matière de protection de l'installation industrielle :

- Mise en réseau croissante d'installations industrielles complètes
- Intégration verticale et mise en réseau des niveaux de l'entreprise
- Nouvelles technologies telles que la télémaintenance ou l'accès à distance

Les menaces sont multiples et les conséquences, profondes.

### Menaces possibles

Les menaces potentielles résultent de l'environnement industriel et touchent à la confidentialité, à l'intégrité et à la disponibilité. Les menaces sont par exemple les suivantes :

- Espionnage de données, recettes, etc.
- Sabotage des installations de production
- Arrêt des machines, par ex. en raison d'une attaque de virus ou d'un logiciel malveillant
- Manipulation des données ou du logiciel d'application
- Utilisation non autorisée de fonctions système

### Conséquences possibles d'un incident sécuritaire

- Perte de propriété intellectuelle
- Perte de production ou qualité de production réduite
- Image négative de l'entreprise et dommages économiques

- Incidences désastreuses sur l'environnement
- Dangers pour l'opérateur et pour la machine

# Mesures de sécurité au niveau de l'automatisation et des entraînements

# 4

La technologie d'automatisation et des entraînements de Siemens traite les aspects liés à la sécurité aux niveaux suivants :

- **Application Security** désigne des produits et des fonctions tenant compte des questions de sécurité industrielle dans l'environnement de l'automatisation, en particulier à l'égard de l'application et de sa fonction ainsi que des personnes œuvrant dans une installation d'automatisation. Le concept d'Industrial Security peut ainsi être aisément implémenté dans les procédés de fabrication.
- **Security-Support** apporte son soutien lors de l'analyse, la planification, l'implémentation, le contrôle et l'optimisation de la sécurité industrielle, fourni par des spécialistes du réseau, ainsi que son savoir-faire sectoriel. Ces services permettent d'atteindre le plus haut niveau possible de sécurité industrielle et de disponibilité de l'installation de production.
  Avec le service "Implement Security", Siemens propose une assistance complète du client : elle permet d'augmenter le niveau de sécurité des installations et des sites de production par la mise en œuvre de mesures de protection. Pour plus d'informations sur l'ensemble de la gamme de produits "Implement Security", voir sur Internet.

## Voir aussi

Mise en œuvre de la sécurité (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/implementation.html)

# 4.1 Mesures de sécurité

Avec le développement de la numérisation, le rôle d'une sécurité globale dans l'automatisation gagne encore en importance. La sécurité industrielle est donc un élément central de tous les produits pouvant être mis en réseau.

## Intégration de la sécurité dans les produits

En tant que fabricant de produits d'automatisation et d'entraînements, Siemens supporte l'exploitation sûre ce ces produits chez le client par l'**intégration de la sécurité dans les produits** :

- Toutes les mesures pour la technologie d'automatisation et d'entraînement sont consignées dans le **processus de gestion du cycle de vie des produits (PLM)**, lequel est certifié par le TÜV, sur la base de la norme CEI 62443-4-1.
- Les **analyses des menaces et des risques (TRA)** permettent de déceler et d'évaluer par voie analytique les risques d'attaques potentiels. Les menaces critiques identifiées sont converties dans le produit en fonctions de base indispensables, selon la devise "Security by Design".
- Siemens effectue périodiquement des **analyses de code** pour identifier et éliminer de manière précoce des erreurs possibles au cours du contrôle formel.
- Siemens a implémenté dans ses produits et dans ses procédés de fabrication des **mesures d'assurance de l'intégrité** afin de déceler toute modification de l'intégrité.
- Siemens contrôle en permanence des mesures de **durcissement** :
  - Les systèmes d'exploitation sont configurés de telle sorte que les **points d'attaque** (p. ex. ports de services inutilisés) soient **minimisés**.
  - Siemens **teste ses produits** pour identifier de manière précoce ses points faibles.
  - Siemens propose un service de **gestion ciblée des hotfixes/correctifs**.

## Sécurisation de l'infrastructure de développement et de la chaîne de fournisseurs

En tant que fabricant de produits d'automatisation et d'entraînements, Siemens supporte la sécurité d'exploitation de ces produits chez le client par la **sécurisation de l'infrastructure de développement et de la chaîne de fournisseurs** :

- Siemens ProductCERT (https://www.siemens.com/cert/en/cert-security-advisories.htm) (**C**yber **E**mergency **R**eadiness **T**eam) est le service centralisé pour les incidents relatifs à la sécurité dans l'environnement des produits et des solutions Siemens. Siemens ProductCERT supporte les services de développement avec des prestations de conseil et de maintenance. **ProductCERT** met à disposition des informations sur les menaces et points faibles actuels ainsi que sur les contre-mesures appropriées.
- La sécurité industrielle est une thématique complexe et dynamique exigeant une surveillance continue ainsi qu'une adaptation constante aux nouvelles mesures de sécurité. Pour plus d'informations sur la manière dont Siemens protège ses propres produits et solutions contre les cyberattaques et fait profiter l'industrie de ses compétences, voir sur Internet (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/always-active.html).

## Mise à disposition de correctifs, composants Security et services adaptés

En tant que fabricant de produits d'automatisation et d'entraînements, Siemens supporte la sécurité d'exploitation chez le client par une assistance directe des intégrateurs et des exploitants, en **mettant à disposition des correctifs, des composants Security et des services adaptés** :

- Pour la surveillance du risque résiduel, Siemens propose un **système SIEM**. SIEM signifie Security Information and Event Management et le terme s'est établi dans le domaine de la sécurité informatique. Les systèmes correspondants sont en mesure d'identifier des événements concernant la sécurité, de les évaluer et d'alarmer ensuite l'administrateur.

## 4.2 Siemens Industrial Holistic Security Concept

Siemens attache une grande importance à la protection de l'intégrité et à la garantie de la confidentialité des données traitées par ses propres produits. La propriété intellectuelle et le savoir-faire associé aux produits Siemens sont également au centre des préoccupations.

Pour atteindre cet objectif, Siemens applique le Siemens Industrial Holistic Security Concept (SI HSC) qui protège les départements de développement et les installations de production (voir le graphique ci-après). Ce concept met en œuvre des systèmes de sécurité à plusieurs niveaux et des améliorations fondamentales de la sécurité de l'infrastructure informatique. Parallèlement à cela, Siemens a amélioré les processus et sensibilisé le personnel à la sécurité par des formations. Ces mesures sont prises en continu et sont rendues visibles par les niveaux de sécurité atteints.

SI HSC profite également aux clients qui choisissent Siemens comme partenaire pour leurs solutions industrielles ou qui souhaitent s'aligner eux-mêmes sur ce concept. Les fournisseurs de Siemens sont également englobés dans les considérations de sécurité, dans la mesure où Siemens se base pour ses achats sur les mêmes normes de sécurité que pour la fabrication de ses propres produits.

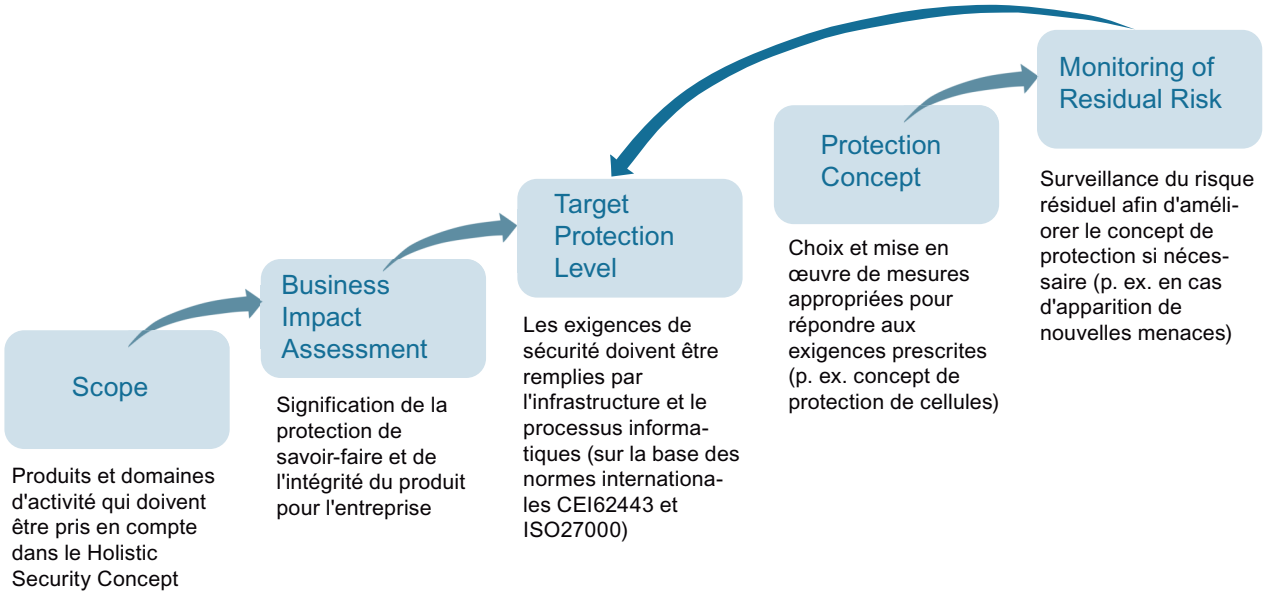



Figure 4-1 Processus de gestion de la sécurité SI HSC

### Plus d'informations

Pour plus d'informations sur le Siemens Industrial Holistic Security Concept, voir le site Always active (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/always-active.html).

## 4.3 Normes et prescriptions

Siemens respecte sur l'ensemble du processus de développement les normes et prescriptions suivantes en matière de sécurité industrielle :

- ISO 2700X : gestion des risques de sécurité de l'information
- CEI 62443 : sécurité des automatismes industriels et des systèmes de commande – sécurité dans les réseaux et les systèmes

**Plus d'informations** sur la certification et les normes dans le domaine de la sécurité industrielle, voir sur Internet (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/certification-standards.html).

# Gestion de la sécurité

# 5

## Le processus de gestion de la sécurité comme fondement

Protégez votre système et votre entreprise. Une gestion de la sécurité selon CEI 62443 et ISO 27001 constitue dans ce cadre le fondement pour une mise en œuvre réussie de la sécurité industrielle.

Le processus de gestion de la sécurité est représenté graphiquement ci-dessous :

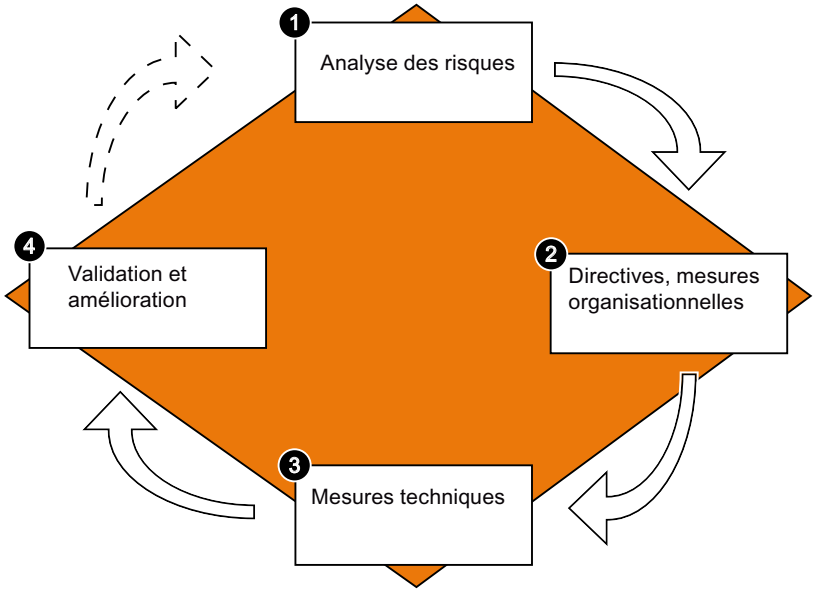



Figure 5-1 Processus de gestion de la sécurité

1. Procéder à une analyse des risques. Déterminer tous les risques potentiels et définir les contre-mesures permettant de réduire les risques à un niveau acceptable. Dans le détail, une analyse des risques comprend les étapes suivantes :
   - Identification des objets menacés
   - Analyse de la valeur et du risque de dommage
   - Analyse des menaces et des points faibles
   - Identification des mesures de sécurité existantes
   - Évaluation des risques
   - Évaluation des conséquences en termes de confidentialité, d'intégrité et de disponibilité
2. Définir des directives et introduire des mesures organisationnelles coordonnées. Pour cela, la conscience de l'importance de la sécurité industrielle doit être prise en charge à tous les niveaux de l'entreprise. Définir également des directives et des processus afin d'obtenir une démarche uniforme et d'encourager le respect du concept de sécurité industrielle défini.

3. Introduire des mesures techniques adaptées. Une liste des mesures générales utiles pour la protection de votre installation contre les menaces est fournie au chapitre Mesures générales de sécurité (Page 27). Les mesures recommandées dans le contexte SINUMERIK, SIMOTION et SINAMICS sont fournies au chapitre Mesures de sécurité spécifiques au produit (Page 47).
4. S'assurer au moyen d'un audit de sécurité que toutes les mesures ont été mises en œuvre et que celles-ci ont réellement éliminé ou réduit les risques identifiés.

**Remarque**

**Processus continu**

En raison des menaces de sécurité en constante évolution, **ce processus doit sans cesse être répété** afin de garantir la sécurité de votre installation. C'est pourquoi le processus de gestion de la sécurité doit être considéré comme un processus continu.

# Mesures générales de sécurité 6

Le chapitre suivant présente des mesures générales de sécurité que vous devez prendre pour protéger votre système contre les menaces.

Des mesures de sécurité supplémentaires spécifiques aux produits SINUMERIK, SIMOTION et SINAMICS sont présentées dans le chapitre Mesures de sécurité spécifiques au produit (Page 47).

# 6.1 Concept de défense en profondeur

La protection complète des installations industrielles contre les cyberattaques provenant aussi bien de l'intérieur que de l'extérieur impose une intervention simultanée à tous les niveaux – du niveau exploitation au niveau terrain, du contrôle d'accès à la protection contre la copie. Nous utilisons à cet effet une défense en profondeur par couches – "Defense in Depth" – comme concept général de protection selon la recommandation ISA99 / CEI 62443, la principale norme pour la sécurité dans l'automatisation industrielle.


Figure 6-1 Stratégie de défense en profondeur

**Plus d'informations** sur le concept de défense en profondeur et sur la planification d'un concept de protection pour les installations industrielles, voir Internet (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/planning.html).

## Couches de protection

Le modèle de défense en profondeur comprend trois couches :

- **Sécurité de l'installation**
  La "sécurité de l'installation" représente la couche extérieure. La sécurité de l'installation comprend des mesures de protection physique complètes, telles que les contrôles d'accès, qui doivent être coordonnées de manière étroite avec les mesures de protection de la sécurité informatique.
- **Sécurité des réseaux**
  Les mesures regroupées sous le mot-clé "sécurité des réseaux" constituent la pièce maîtresse des mesures de protection. Ce terme sous-entend la segmentation du réseau de l'installation avec communication limitée et sécurisée des sous-réseaux ("Secure Islands") ainsi que le contrôle des interfaces grâce à la mise en œuvre de systèmes pare-feu.
- **Intégrité du système**
  Le terme "Intégrité du système" englobe deux aspects de protection essentiels. Les systèmes sur base PC et le niveau de commande doivent être protégés contre les attaques. Il s'agit, par exemple, des mesures suivantes :
  - Mécanismes intégrés de protection d'accès aux composants d'automatisation afin d'empêcher des modifications non autorisées par le biais du système d'ingénierie ou pendant la maintenance.
  - Utilisation de logiciels antivirus et de listes blanches protégeant les systèmes PC contre les logiciels malveillants.
  - Procédés de maintenance et de mise à jour pour maintenir les systèmes d'automatisation à un niveau actualisé
    (p. ex. gestion des correctifs, mise à jour du firmware, etc.)

## 6.2 Sécurité de l'installation


Les lacunes dans la sécurité physique d'une entreprise permettent aux personnes non autorisées de pénétrer sur le site / dans le bâtiment de production, et d'endommager ou de modifier les installations de production, engendrant, le cas échéant, la perte d'informations confidentielles. Cela peut être empêché en protégeant en conséquence aussi bien le site de l'entreprise que les zones de production.

### 6.2.1 Protection physique des zones de production critiques

#### Sécurité de l'entreprise

La sécurité physique de l'entreprise peut être assurée par les mesures suivantes :

- Site de l'entreprise doté d'une enceinte surveillée
- Contrôle d'accès, serrures/lecteurs de carte et/ou personnel de sécurité
- Accompagnement des personnes étrangères à l'entreprise par un membre du personnel
- Formation du personnel aux procédures de sécurité de l'entreprise et application de ces procédures par tous les collaborateurs

#### Sécurité physique de la production

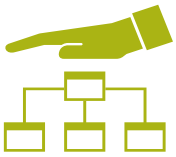
La sécurité physique de la production peut être assurée par les mesures suivantes :

- Contrôle d'accès séparé pour les zones critiques telles que les zones de production
- Intégration des constituants critiques dans des armoires / salles de commande sécurisées, avec possibilités de surveillance et d'alarme. Les armoires / salles de commande doivent être sécurisées avec des serrures à cylindre. Ne pas utiliser des serrures simples telles que les serrures universelles, à clé triangulaire ou carrée ou à panneton double.
- Planification des champs de liaison radio afin de limiter la portée du Wi-Fi et d'empêcher que ces liaisons puissent être captées à l'extérieur des zones définies (p. ex. hall de production).
- Des directives qui interdisent l'utilisation sur les systèmes de supports de données (p. ex. clés USB) et d'appareils IT (p. ex. ordinateurs portables) de constructeurs tiers, considérés comme étant non sécurisés.

## Plus d'informations

Plus d'informations sur les solutions de sécurité intégrées de Siemens, voir Page Siveillance (https://new.siemens.com/global/en/products/buildings/security/security-management.html).

# 6.3 Sécurité des réseaux




La sécurité des réseaux regroupe toutes les mesures de planification, d'exécution et de surveillance de la sécurité des réseaux. Cela inclut le contrôle de toutes les interfaces, par exemple entre le réseau du bureau et le réseau de l'installation ou l'accès à Internet pour la télémaintenance.

## 6.3.1 Segmentation des réseaux

### 6.3.1.1 Séparation des réseaux de production et de bureautique

Une mesure de sécurité importante pour une installation d'automatisation ou d'entraînement est la séparation stricte entre les réseaux de production et les autres réseaux de l'entreprise. Cette séparation crée des zones de protection pour les réseaux de production.

**Remarque**

Les produits décrits dans ce manuel ne doivent être utilisés que dans des zones de protection définies.

#### Séparation au moyen d'un système de pare-feu

Dans le cas le plus simple, la séparation est réalisée au moyen d'un seul système de pare-feu qui contrôle et réglemente la communication entre les réseaux.

Voir aussi Segmentation des réseaux avec SCALANCE S (Page 33)

#### Séparation au moyen d'un réseau DMZ

Pour la variante plus sûre, le couplage est effectué au moyen d'un réseau DMZ distinct. Dans ce cas, la communication directe entre les réseaux de production et ceux de l'entreprise est empêchée entièrement et la communication ne s'effectue que de manière indirecte à travers des serveurs dans le réseau DMZ.

**Remarque**

Il convient également de cloisonner les réseaux de production dans des cellules d'automatisation distinctes afin de protéger les mécanismes de communication critiques.

### Mesures générales de sécurité

Même à l'intérieur des zones de protection, il convient d'observer les mesures générales de sécurité p. ex. du chapitre Durcissement (Page 37).

#### 6.3.1.2 Segmentation des réseaux avec SCALANCE S

Afin de répondre aux exigences en matière de protection et de segmentation des réseaux, Siemens propose les Security Modules SCALANCE S. Plus d'informations sur SIEMENS SCALANCE S, voir sur Internet (https://siemens.com/scalance-s).

### Security Modules SCALANCE S

Les Security Modules SCALANCE S avec Security Integrated offrent les fonctionnalités suivantes :

- Pare-feu Stateful Inspection
  Afin d'assurer un contrôle et une journalisation spécifiques à l'utilisateur, il est possible de définir des règles de pare-feu dont la validité est limitée à certains utilisateurs.
- VPN via IPsec (cryptage des données et authentification)
  Cette fonction crée une liaison tunnellisée, protégée entre les utilisateurs authentifiés, dont les données ne peuvent être interceptées ou manipulées. L'aspect le plus important est la protection contre les accès externes via Internet.
- NAT/NAPT (translation d'adresses)
- Fonctionnalité routeur (PPPoE, DDNS) pour l'accès large bande à Internet (DSL, câble)
- SCALANCE S623 avec port VPN (DMZ) supplémentaire permet la connexion sécurisée d'un autre réseau à des fins de service ou de télémaintenance. S623 autorise en outre la connexion sécurisée et redondante de réseaux de niveau inférieur via des routeurs et systèmes pare-feu redondants.
- SCALANCE S615 dispose de cinq ports Ethernet permettant de protéger différentes topologies de réseau à l'aide de pare-feu ou de VPN (IPsec et OpenVPN) et de mettre en œuvre des concepts de sécurité en toute flexibilité.

### Condition

| IMPORTANT |
| --- |
| **Utilisation abusive des données**<br>De longues distances entre l'appareil à protéger et les Security Modules en amont peuvent favoriser une utilisation abusive des données.<br>• Noter qu'il convient d'installer les Security Modules en amont, comme SCALANCE S, près de l'appareil à protéger dans une armoire électrique verrouillée. Cela permet de s'assurer que personne ne puisse manipuler les données sans qu'on s'en aperçoive. |

## Principe

L'exemple d'application suivant montre la segmentation de cellules à l'aide de plusieurs modules SCALANCE S installés en amont des cellules d'automatisation. Le pare-feu de SCALANCE S permet de filtrer et contrôler l'échange de données entre les appareils à l'intérieur des cellules d'automatisation. L'échange de données entre les cellules peut être crypté et authentifié si nécessaire. Pour l'accès client entre PC et cellules, SOFTNET Security Client, un logiciel client VPN pour PC, permet de créer des canaux sécurisés.

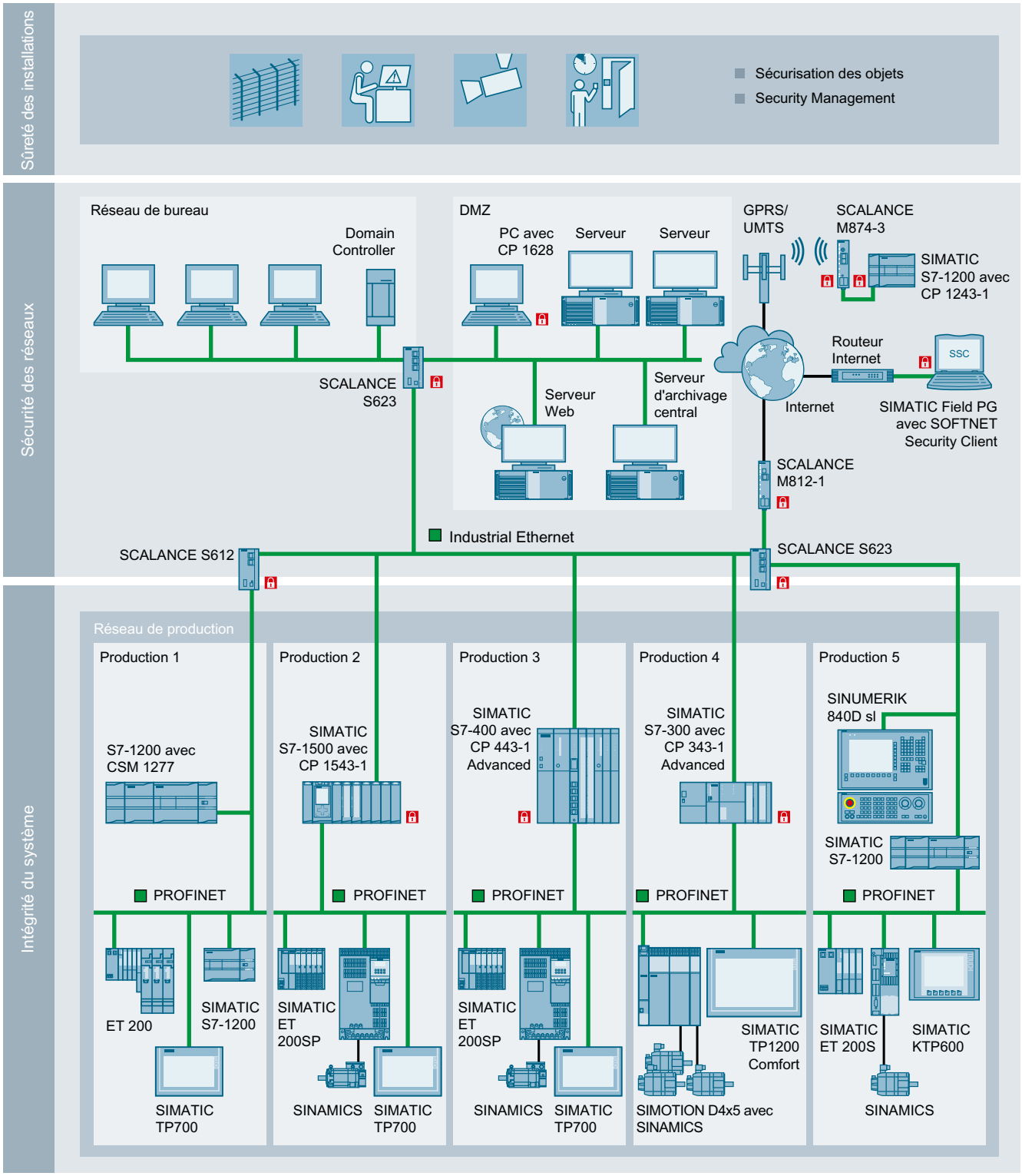



Figure 6-2 Exemple d'application SCALANCE S

### Accès VPN

**Remarque**

Noter qu'un accès VPN doit systématiquement s'effectuer avec un Security Module SCALANCE S.

## 6.3.2 Sécurité cloud

Les applications cloud sont de plus en plus répandues et la signification du cloud pour l'avenir ne cesse de croître ; la thématique de la sécurité dans le cloud est donc particulièrement importante et va continuer à gagner en importance.

Les adresses suivantes vous permettent de vous informer sur les moyens de sécuriser votre système dans l'environnement cloud. Elles fournissent des informations sur les exigences en vigueur et permettent de se familiariser avec les mesures éprouvées et les bonnes pratiques.

### Plus d'informations

- Companion Guide for Cloud - CIS Organisation (https://www.cisecurity.org/press-release/cis-controls-companion-guide-for-cloud-now-available/)
- Questionnaire Cloud Security - CSA Organisation (https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-0-1/)

# 6.4 Intégrité du système

Intégrité du système

Par intégrité du système, on entend la "complétude" et l'"exactitude" des données ou le comportement correct du système. Les mesures suivantes de protection de l'intégrité du système visent à garantir que les données / la fonctionnalité du système ne sont pas manipulées sans autorisation et que les manipulations sont détectées.

## 6.4.1 Durcissement

### 6.4.1.1 Services et ports

Les services et les ports activés présentent un risque. Pour minimiser les risques, seuls les services requis doivent être activés sur les composants d'automatisation. Tous les services activés (en particulier serveur web, FTP, télémaintenance, etc.) doivent être pris en compte dans le concept de sécurité.

Une description de tous les ports utilisés est fournie dans les manuels ou descriptions fonctionnelles des différents produits.

### 6.4.1.2 Comptes utilisateur

Chaque compte utilisateur actif permet un accès au système et constitue ainsi un risque potentiel. Par conséquent, prenez les mesures de sécurité suivantes :

- Réduction du nombre de comptes utilisateur configurés/activés au strict minimum
- Utilisation de données d'accès sûres pour les comptes existants. Attribution d'un mot de passe sûr.
- Contrôle régulier en particulier des comptes utilisateur configurés en local
- Modification fréquente et régulière des mots de passe

#### 6.4.1.3 PC/ordinateurs portables et appareils mobiles dans l'environnement industriel

Les équipements terminaux utilisés dans l'environnement industriel (PC, ordinateurs portables et appareils mobiles) doivent correspondre aux exigences de sécurité en vigueur. Par conséquent, il convient de prendre les mesures de suivantes :

- Le terminal mobile utilisé est installé, administré, périodiquement contrôlé et doté des correctifs actuels par les services appropriés, ce qui permet de le maintenir dans l'état actuel de la technique. Ceci signifie également que le logiciel et les systèmes d'exploitation installés sont ceux qui sont supportés par le fabricant.
- Le terminal utilisé doit héberger un antivirus adapté au système d'exploitation installé. Pour cela, il convient d'actualiser régulièrement les signatures de virus et le logiciel. Ou, à titre d'alternative, travailler avec la méthode Liste blanche (Page 42).
- Activer sur le terminal utilisé un pare-feu avec les réglages appropriés.
- Utiliser sur le terminal une configuration sans droits d'administrateur.
- Crypter tous les disques durs ou mémoires de masse (p. ex. eMMC ou SSD) du terminal afin de protéger les données sensibles des accès non autorisés.
- Ne pas utiliser le terminal pour d'autres tâches, p. ex. dans le réseau de bureautique. Ceci relève de la séparation des réseaux traitée au chapitre "Séparation des réseaux de production et de bureautique (Page 32)".
- Sécuriser les terminaux contre le vol avec une serrure physique (p. ex. verrou Kensington) ou ne pas les laisser sans surveillance.
- Si les terminaux sécurisés doivent être laissés sur le poste de travail, activer systématiquement le mode verrouillé du système d'exploitation, ce qui empêche l'accès au terminal et la lecture du contenu de l'écran.
- Créer des comptes utilisateur (Page 37) pour les droits d'accès.
- Sécuriser au moyen de mesures appropriées les interfaces non utilisées (p. ex. USB, réseau, etc.) contre l'accès non autorisé. Il est possible d'utiliser des verrous de port USB du commerce ou des mesures logicielles correspondantes.

### 6.4.1.4 Stockage des données

**Remarque**

Il incombe à chacun de veiller, sous sa propre responsabilité, au stockage sécurisé de ses données sur son PC.

Les mesures suivantes sont applicables :

- Identifier les documents systématiquement selon des niveaux de confidentialité en introduisant un classement des documents.
- Protéger les emplacements de stockage cryptés tels que les points de partage contre les manipulations.
- Ne stocker des données confidentielles ou nécessitant une sécurisation sur le PC / les systèmes ou le réseau que si cela est absolument nécessaire et uniquement sous forme cryptée.
  Les données à sécuriser sont les données sensibles telles qu'archives, mots de passe ou fichiers exécutables (*.exe).
- Effectuer périodiquement des sauvegardes des données à sécuriser et les protéger contre la perte et la manipulation.

### 6.4.1.5 Transport des données

**Remarque**

Appliquer les mesures suivantes lors du transport de données :

- Lors de l'envoi par e-mail de données confidentielles et/ou nécessitant une sécurisation, crypter systématiquement ces e-mails.
- Lors du transport de données confidentielles ou nécessitant une sécurisation sur un support de données (clé USB, disque dur, etc.) veiller à utiliser un support de données sûr. Les supports de données doivent être contrôlés périodiquement par des antivirus. N'enregistrer les données que sous forme cryptée, même sur des supports de données locaux.

Ces mesures s'appliquent en particulier aux données sensibles telles qu'archives, mots de passe ou fichiers exécutables (*.exe).

### 6.4.1.6 Mots de passe

| IMPORTANT |
| --- |
| **Utilisation abusive des données due à un mot de passe faible**<br>L'attribution de mots de passe faibles peut faciliter une utilisation abusive des données. Des mots de passe faibles sont faciles à deviner ou à décrypter.<br>• Modifier par conséquent toujours les mots de passe par défaut pendant la mise en service et les modifier périodiquement selon un intervalle de temps défini.<br>• Modifier également les mots de passe pour les fonctions que vous n'utilisez pas personnellement, afin d'éviter une utilisation abusive de ces fonctions.<br>• Garder les mots de passe secrets et s'assurer que seules des personnes autorisées ont accès aux différents mots de passe. |

**Remarque**

**Mots de passe sécurisés**

Les règles suivantes doivent être respectées lors de l'attribution de nouveaux mots de passe :

- Lors de l'attribution de nouveaux mots de passe, veiller à ne jamais attribuer de mots de passe faciles à deviner, comme des mots simples, des suites de touches sur le clavier faciles à deviner, etc.
- Les mots de passe doivent toujours comprendre une combinaison de majuscules et de minuscules, ainsi que des chiffres et des caractères spéciaux. Les codes PIN doivent être composés d'une suite aléatoire de chiffres.
- Lors de l'attribution de mots de passe, veiller à respecter les prescriptions en vigueur de l'entreprise, p. ex. des stratégies de mot de passe spécifiques à l'entreprise.
- Attribuer des mots de passe de la longueur minimale exigée selon les prescriptions en vigueur de l'entreprise.
- Dans la mesure du possible et si les systèmes informatiques et le logiciel le permettent, le choix des caractères composant un mot de passe doit toujours obéir à la complexité la plus élevée.

Pour vous aider à gérer vos mots de passe, vous pouvez utiliser un gestionnaire de mots de passe. Ce type de programme permet d'enregistrer les mots de passe et codes secrets de manière chiffrée, de les gérer et de créer des mots de passe sécurisés.

**Plus d'informations** sur l'attribution de mots de passe sécurisés, voir le chapitre "Références (Page 109)".

### 6.4.1.7 Notifications sur la sécurité des produits

**Remarque**

**Respecter les notifications sur la sécurité des produits**

Les menaces prennent de nombreux aspects et changent constamment. Il convient par conséquent de se tenir informé régulièrement par le biais de l'assistance technique Industry Online Support (https://support.industry.siemens.com/sc/ww/fr/sc/support-technique/oid2090) de l'existence de nouvelle notifications de sécurité relatives aux produits utilisés. Suivre les instructions des notifications de sécurité produit.

### 6.4.1.8 Antivirus

Un logiciel antivirus, ou antivirus, est un logiciel destiné à détecter, bloquer et le cas échéant éliminer les virus, vers et chevaux de Troie informatiques connus.

Par principe, les antivirus ne sont capables de détecter que des logiciels malveillants connus (virus, vers, chevaux de Troie, etc.) et n'offrent donc pas une protection contre tous les virus et vers. Ainsi les antivirus peuvent être uniquement considérés comme des mesures de précaution complémentaires aux mesures de protection générales.

La mise en œuvre d'un logiciel antivirus ne doit pas entraver la production d'une installation. Au final, cela implique que même un ordinateur infecté par un virus ne doit pas être arrêté immédiatement et automatiquement si cela se traduirait par une perte du contrôle sur le processus de production.

| IMPORTANT |
| --- |
| **Utilisation abusive des données avec les antivirus en ligne**<br>En cas d'utilisation d'un antivirus en ligne, des données confidentielles ou nécessitant une sécurisation peuvent tomber entre de mauvaises mains ou faire l'objet d'une utilisation abusive.<br>• C'est pourquoi il convient de ne pas contrôler des données confidentielles ou nécessitant une sécurisation à l'aide d'un logiciel antivirus en ligne. |

**Remarque**

**Mise à jour des logiciels antivirus**

Veiller à ce que la base de données du logiciel antivirus soit systématiquement à jour.

**Remarque**

**Pas d'installation simultanée de plusieurs logiciels antivirus**

L'installation simultanée de plusieurs logiciels antivirus sur un même système doit être systématiquement évitée.

**Remarque**

**Fonctionnement dans le réseau local**

Utiliser systématiquement un antivirus même en cas de connexion locale avec le réseau de l'installation.

#### 6.4.1.9 Liste blanche

Le principe de la liste blanche consiste à se méfier de toutes les applications, à l'exception de celles qui ont été classées comme applications de confiance lors d'un contrôle. Autrement dit, une liste positive (liste blanche) est tenue à jour. Cette liste positive contient toutes les applications classées comme fiables et pouvant par conséquent être exécutées sur vos systèmes PC.

Les mécanismes de liste blanche offrent une protection supplémentaire / alternative contre les applications indésirables ou les logiciels malveillants ainsi que les modifications non autorisées des applications installées ou des fichiers exécutables (.exe, .dll).

Observer les Consignes spécifiques au produit (Page 47) correspondantes recommandant l'utilisation de logiciels antivirus et/ou de listes blanches.

### 6.4.2 Gestion des correctifs

#### WSUS

Pour les systèmes Windows actuels, Microsoft propose la fonctionnalité système **WSUS** (Windows Server Update Services). WSUS aide les administrateurs à appliquer les mises à jour Microsoft sur des réseaux locaux très étendus. WSUS télécharge automatiquement sur Internet les packages de mise à jour (Microsoft Update) et les met à disposition des clients Windows pour l'installation.

Ce processus entièrement automatisé garantit que les dernières mises à jour de sécurité de Microsoft sont toujours disponibles sur les clients Siemens.

| IMPORTANT |
| --- |
| **Failles de sécurité des systèmes d'exploitation obsolètes**<br>Noter que Microsoft ne met plus automatiquement à disposition de mises à jour de sécurité, hotfixes, etc. pour les systèmes d'exploitation obsolètes < Windows 10. Des failles de sécurité dangereuses sont donc possibles dans vos systèmes d'exploitation.<br>• Il convient donc, si possible, de toujours installer la version la plus récente de votre système d'exploitation.<br>• Si votre système d'exploitation est plus ancien, des mesures complémentaires appropriées (p. ex. tenue d'une liste blanche) doivent être prises pour le protéger. |

**Remarque**

**Avant l'installation de mises à jour de Microsoft, observer les points suivants :**

- Sauvegarder l'état du système **avant la mise à jour** en vue d'un éventuel repli nécessaire. La compatibilité de la mise à jour avec la configuration individuelle de l'installation relève de la responsabilité du client.
- Ne jamais se connecter directement au serveur WSUS sur Internet ! Veiller à un environnement sécurisé et installer une couche intermédiaire (p. ex. réseau DMZ, pare-feu, modules SCALANCE S, etc.)

#### 6.4.2.1 Logiciel produit

**Remarque**

Un logiciel produit de version plus ancienne représente également une surface d'attaque potentielle.

- Il convient donc d'installer systématiquement la version la plus récente disponible du logiciel produit.

### 6.4.3 Intégrité des données

Par intégrité des données, on entend l'exactitude et la complétude des données et le fonctionnement correct des systèmes. La garantie de l'intégrité des données est un objectif essentiel de la sécurité de l'information. La protection de l'intégrité ne doit pas être confondue avec la protection de la confidentialité.

| IMPORTANT |
| --- |
| **Corruption des données et dysfonctionnement du système qui en résulte**<br>Des données telles que des archives ou des programmes provenant de sources externes peuvent être chargées sur les systèmes d'automatisation ou d'entraînement ainsi que sur les composants de commande. Ces données influencent le comportement de ces systèmes et doivent donc être protégées contre une modification non autorisée.<br>De même, des données telles que des archives, des programmes et des applications OA peuvent être enregistrées et archivées. Les systèmes ne fournissent actuellement aucune possibilité de garantir l'intégrité des programmes, archives et applications OA.<br>L'utilisateur doit donc prendre ses propres mesures pour garantir l'intégrité de ses archives, applications OA ou autres données stockées :<br>• Utiliser le Siemens Industrial Holistic Security Concept.<br>• Utiliser les signatures numériques pour la protection des données.<br>• Veiller à une protection d'accès suffisante :<br>– Restreindre les droits d'accès en conséquence, p. ex. sur les lieux de stockage des données/points de partage.<br>– Ne pas envoyer d'e-mails non cryptés/non signés |

### 6.4.4 Élimination

Les produits doivent être éliminés conformément aux prescriptions nationales en vigueur. Les produits décrits dans ce manuel sont pour une large part recyclables grâce à leurs équipements à faible teneur en polluants. S'adresser à une entreprise spécialisée dans la mise au rebut pour un recyclage et une mise au rebut de l'appareil qui soient respectueux de l'environnement.

| IMPORTANT |
| --- |
| **Utilisation abusive des données due à un effacement de données non sûr**<br>Un effacement des données incomplet ou non sûr sur les cartes mémoires ou les disques durs des produits peut être à l'origine d'une utilisation abusive des données des programmes pièce, archives, etc. par des tiers.<br>• Veiller par conséquent à effacer de manière sûre tous les supports de mémoire utilisés **avant l'élimination du produit** :<br>• Il existe des programmes permettant de vider/formater les supports de mémoire. Ou s'adresser à un prestataire de services d'élimination certifié qui se chargera de cette tâche. |

Respecter aussi les consignes relatives à l'élimination du produit du chapitre Mesures de sécurité spécifiques au produit (Page 47).

# Mesures de sécurité spécifiques au produit 7

Ce chapitre contient des mesures de sécurité supplémentaires spécifiques aux produits SINUMERIK, logiciel de gestion CNC Shopfloor Management, SIMOTION, SINAMICS et SIMOCRANE.

# 7.1 SINUMERIK

Le chapitre suivant fournit une vue d'ensemble des mesures de sécurité à prendre pour protéger une commande SINUMERIK contre les menaces. Des descriptions et procédures détaillées sont fournies dans la documentation SINUMERIK correspondante indiquée.

De nombreux produits (SINUMERIK, SIMOTION, SINAMICS) contiennent OpenSSL. Pour ces produits :

- Ce produit comprend un logiciel (https://www.openssl.org/) développé par le projet OpenSSL pour une utilisation dans la boîte à outils OpenSSL.
- Ce produit comprend un logiciel (mailto:eay@cryptsoft.com) cryptographique créé par Eric Young.
- Ce produit comprend un logiciel (mailto:eay@cryptsoft.com) développé par Eric Young.

## 7.1.1 Pare-feu et mise en réseau

### Structure de mise en réseau NCU/PCU

Le graphique suivant illustre la mise en réseau de la commande (NCU) et de l'IPC. La mise en réseau dans le réseau d'entreprise doit s'effectuer via X130 sur la NCU et eth1 sur l'IPC. Ces deux interfaces sont protégées contre les accès non autorisés à l'aide d'un pare-feu.

La NCU contient une fonctionnalité de filtrage de paquets (pare-feu) ; la connexion au réseau d'entreprise est filtrée par ce pare-feu. Ce pare-feu intégré est préconfiguré avec des réglages optimisés pour la communication entrante et sortante. Le pare-feu est réglé de manière à bloquer tout accès au réseau en aval et à détecter, bloquer et empêcher des tentatives répétées de connexion d'une adresse IP définie. La commande est ainsi protégée des attaques dites par force brute.

L'IPC est doté de la fonction pare-feu par la fonctionnalité Windows.

| IMPORTANT |
| --- |
| **Utilisation abusive des données via une interface non protégée**<br>L'interface X120 de la NCU et l'interface eth2 de l'IPC n'étant pas protégées par un pare-feu, il existe un risque d'utilisation abusive des données. L'interface fournit uniquement une possibilité de raccordement pour le réseau local de l'installation.<br>• Par conséquent, il ne faut jamais connecter ce réseau local au réseau de l'entreprise ou à Internet. |

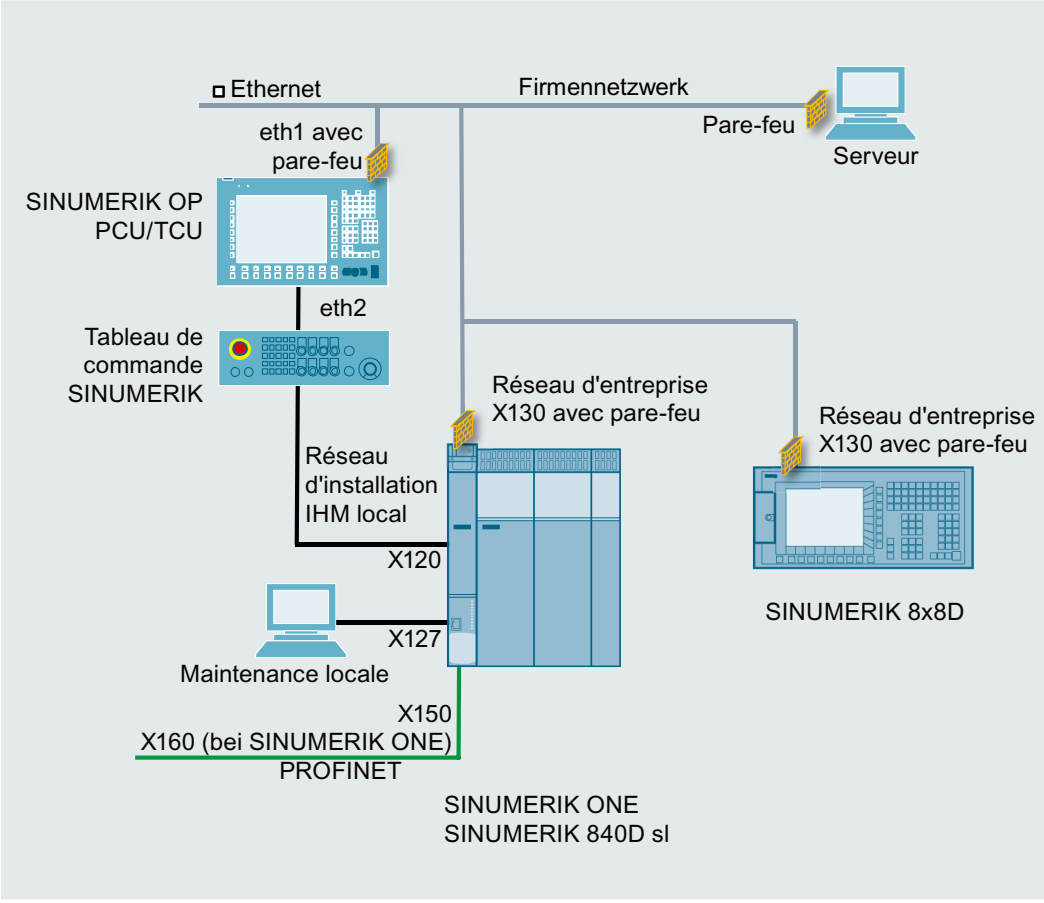



Figure 7-1 Mise en réseau NCU/IPC

## Réglages du pare-feu

L'interface Ethernet X130 de la NCU et l'interface eth1 de l'IPC sont protégées par un pare-feu pour des raisons de sécurité. Lorsque certains programmes doivent accéder à un port pour la communication, il est possible d'activer ou désactiver le pare-feu avec SINUMERIK Operate. Des ports supplémentaires peuvent être validés séparément.

Le pare-feu peut également être configuré via "basesys.ini"

## Plus d'informations

Plus d'informations sur la configuration du pare-feu et sur les réglages par défaut, voir les manuels suivants :

- SINUMERIK Operate (IM9) (https://support.industry.siemens.com/cs/de/en/view/109777907)
- Manuel de diagnostic (808D) (https://support.industry.siemens.com/cs/de/en/view/109763685)

## 7.1.2 Protection physique de la NCU

**IMPORTANT**

**Utilisation abusive, manipulation et vol**

Les modules tels que la NCU sont des matériels ouverts. Sans protection, il existe un risque d'utilisation abusive par du personnel non autorisé, de manipulation ou de vol de données (p. ex. carte CompactFlash).

- Monter par conséquent les NCU dans des boîtiers et des armoires électriques fermées à clé ou dans des locaux électriques. L'accès aux boîtiers, aux armoires ou aux locaux de service électriques ne doit être possible que pour du personnel qualifié ou autorisé. Pour plus d'informations sur les serrures autorisées, voir le chapitre "Protection physique des zones de production critiques (Page 30)".
- **Plus d'informations** sur le montage en armoire des NCU, voir le Manuel de l'appareil SINUMERIK 840D sl NCU 7x0.3 PN (https://support.industry.siemens.com/cs/de/en/view/99922219) ou les manuels correspondants de SINUMERIK ONE : "NCU1750" et "NCU1760".

## 7.1.3 Tableaux de commande machine SINUMERIK (TCM/MPP)

Des tableaux de commande (**T**ableau de **C**ommande **M**achine et **M**achine **P**ush Button **P**anels) sont disponibles pour la commande conviviale des fonctions machine de SINUMERIK.

**Remarque**

Utiliser les tableaux de commande machine (TCM/MPP) exclusivement sur le réseau de machine local, interne, et les sécuriser contre les accès par des tiers.

**Remarque**

**Mise à jour du firmware**

Pour la mise à jour du firmware des TCM/MPP/PP72-48 ou pour un diagnostic des modules (port 3845), contacter le Siemens Service&Support (https://support.industry.siemens.com/sc/ww/en/sc/2090).

### Voir aussi

Mots de passe (Page 40)

## 7.1.4 Durcissement

### 7.1.4.1 Désactiver les interfaces matérielles

#### Désactiver des interfaces

| Mesure | Description |
|---|---|
| Activer/désactiver les interfaces Ethernet dans le BIOS de la PCU. | Il est possible d'activer ou désactiver les interfaces Ethernet dans le BIOS de la PCU.<br>Pour plus d'informations à ce sujet, voir Manuel de mise en service logiciel de base PCU (IM8) (https://support.industry.siemens.com/cs/de/de/view/109748542/fr), chapitre "Réglages du BIOS". |
| Activer/désactiver les interfaces USB | Pour empêcher que des logiciels malveillants ne pénètrent dans la commande ou dans le réseau d'installation via les interfaces USB, vous pouvez désactiver les interfaces USB de la NCU. Utiliser pour cela la commande de maintenance "sc_usb disable". Entrer la commande sur le Service Desktop, dans la boîte de dialogue "Run" ou dans l'invite de commande. Utiliser cette fonction pour rendre le système plus sûr et pour le protéger contre les manipulations indésirables et les logiciels malveillants.<br>**Plus d'informations**, voir le Manuel de mise en service logiciel de base PCU (IM8) (https://support.industry.siemens.com/cs/de/de/view/109748542/fr), chapitre "Procédure de désactivation des interfaces USB". |

### Désactiver les ports

| Mesure | Description |
|---|---|
| Désactiver un port PROFINET sur l'AP SINUMERIK 840D sl | Un port de l'interface PROFINET d'un AP SINUMERIK peut être désactivé dans STEP 7 HW-Config (X150). Le port est activé par défaut. L'AP SINUMERIK n'est pas accessible par un port désactivé de l'interface PROFINET.<br>**Plus d'informations**, voir le Manuel de l'appareil SIMATIC S7-300 CPU 31xC et CPU 31x : Caractéristiques techniques (https://support.industry.siemens.com/cs/de/en/view/12996906/fr), chapitre "Configurer les propriétés du port".<br>**Pas de fonction de communication.**<br>Tenir compte du fait qu'aucune fonction de communication, comme par exemple les fonctions de console de programmation/pupitre opérateur, la communication IE ouverte ou la communication S7 (PROFINET I/O), n'est possible par un port désactivé. |
| Désactiver un port PROFINET sur l'AP SINUMERIK ONE | Le port PROFINET peut être désactivé dans TIA Portal sous "Configuration de l'appareil". Sélectionner l'AP et passer dans le menu "Général > Interface PROFINET > Options étendues > Port > Options de port". Décocher la case "Activer ce port pour l'utilisation."<br>**Plus d'informations**, voir l'aide en ligne de TIA Portal. |
| Désactiver le port PROFINET du commutateur SCALANCE X (possible à partir de la série X200) | Pour un fonctionnement sûr, un seul point d'accès au réseau doit être défini pour le diagnostic / la maintenance. Tous les autres ports sur les commandes, périphériques ou commutateurs (Scalance X) doivent être désactivés. Cela permet d'empêcher les accès non autorisés.<br>**Plus d'informations**, voir le Manuel de configuration SIMATIC NET : Commutateurs Industrial Ethernet SCALANCE X-200 (https://support.industry.siemens.com/cs/de/en/view/109757352/fr), chapitre "Ports". |

### 7.1.4.2 Services de communication et numéros de port utilisés

SINUMERIK prend en charge certains protocoles de communication. Les paramètres d'adresse, la couche de communication appropriée ainsi que le rôle et le sens de communication sont indiqués pour chaque protocole.

Ces informations permettent d'adapter les mesures de sécurité nécessaires pour la protection du système d'automatisation aux protocoles utilisés (p. ex. pare-feu).

**Plus d'informations**, voir l'information produit "Liste des ports SINUMERIK" (en préparation).

**Remarque**

**Durcissement du système pour les solutions logicielles**

En cas d'utilisation du logiciel SINUMERIK Integrate et d'autres applications PC, telles que Create MyConfig (CMC) ou Access MyMachine (AMM), veiller à ce que le PC sur lequel est exploité le logiciel satisfasse aux dernières exigences de sécurité industrielle.

Il s'agit p. ex. des exigences suivantes :

- Mises à jour de sécurité Microsoft actuelles
- Logiciel antivirus actuel
- Pare-feu activé, etc.

Plus d'informations, voir le chapitre Intégrité du système (Page 37).

#### 7.1.4.3 Secure Boot avec SINUMERIK ONE

**Remarque**

**Uniquement logiciels signés**

Les NCU SINUMERIK ONE disposent d'une procédure d'amorçage sécurisée (Secure Boot) qui garantit que seuls des logiciels signés de Siemens peuvent être chargés sur la NCU. Ceci s'applique aussi bien aux versions du logiciel GIV de la commande qu'à tout autre logiciel (p. ex. SINAMICS TEC). Si un fichier *.tgz est chargé et qu'il ne s'accompagne pas d'un fichier *.sig, la NCU ne démarre pas.

Dans cette situation, aucun accès à la commande n'est possible par aucune interface. Le logiciel installé auparavant ne peut pas être supprimé.

### 7.1.5 Protection antivirus

Compte tenu de la durée de vie d'une machine-outil, l'utilisation d'un logiciel antivirus n'est pas pertinente.

Cela s'explique par les raisons suivantes :

- **Mise à jour continue du fichier de signatures nécessaire**
  La protection d'un logiciel antivirus ne vaut que par l'actualité de ses signatures de virus. Une mise à jour sans connexion directe à Internet n'est pas possible dans le quotidien de production de la machine.
- **Les signatures modifiées ainsi que les scans antivirus en arrière-plan influencent les temps d'exécution de la commande**
  Les scans exécutés en arrière-plan peuvent influencer la charge du système et donc le comportement système de la machine. La durée d'un scan est d'autant plus longue que la liste de signatures est plus longue et l'influence augmente donc avec l'âge de la machine.
- **Périodes de support courtes**
  En règle générale, les mises à jour et les signatures d'un logiciel antivirus sont mises à disposition au maximum jusqu'à la fin du support du système d'exploitation. La durée de vie d'une machine-outil est toutefois bien supérieure à la durée de vie d'un système d'exploitation Windows. La protection devient donc sans effet contre de nouvelles menaces avec le temps.
- **Effets imprévisibles sur la fonctionnalité de la machine**
  Une mise à jour des signatures de virus peut entraîner dans certaines conditions la détection par le logiciel antivirus de fonctions systèmes voulues comme étant des opérations suspectes ; dans ce cas, l'antivirus empêche l'exécution de ces fonctions, ce qui a des conséquences imprévisibles sur la commande de la machine.

### Arguments pour la liste blanche

L'utilisation d'une liste blanche pour la protection d'un IPC sur base Windows dans le système SINUMERIK est pertinente pour les raisons suivantes :

- La liste blanche n'a pas besoin de mise à jour pour une protection continue de la machine.
- La liste blanche ne perd pas son effet protecteur sur la durée de vie de la machine (exception faite des progrès techniques).
- La liste blanche assure également une protection contre les logiciels malveillants qui ne sont pas encore connus par un antivirus.

**Remarque**

**Mesures de protection contre les virus dans l'environnement CNC**

Prendre toutes les mesures nécessaires pour la protection contre les virus dans l'environnement de la commande CNC. Cela comprend également une gestion conséquente des supports de données, clés USB et connexions réseau, ainsi que des mesures de précaution lors de l'enregistrement de données et de l'installation de logiciels, etc.

### Voir aussi

Signatures de virus (https://support.industry.siemens.com/cs/ww/fr/view/19577116/en)

## 7.1.5.1 Liste blanche

### Exemple d'application SINUMERIK

L'exemple du logiciel McAfee Application Control décrit comment réaliser un "durcissement" de la SINUMERIK PCU 50 avec Windows XP. Le logiciel soumis à licence peut être utilisé avec la PCU 50 en tant que variante autonome (Solidifier/Solidcore). Le logiciel de liste blanche provient directement du fabricant.

Une description détaillée de cette application est disponible sur Internet (https://support.industry.siemens.com/cs/ww/fr/view/89027076/en).

#### 7.1.5.2 Protection contre les virus/carte mémoire

Pour tous les appareils SINUMERIK disposant d'une carte mémoire, il convient de prendre des précautions particulières afin d'éviter que des logiciels malveillants ne pénètrent dans cette carte mémoire.

**⚠ ATTENTION**

**Danger de mort en raison de logiciels manipulés lors de l'utilisation de supports de mémoire amovibles**

L'archivage de fichiers sur des supports de mémoire amovibles présente un risque élevé d'infection, p. ex. par des virus ou des logiciels malveillants. Un paramétrage incorrect peut entraîner des dysfonctionnements sur les machines, susceptibles de provoquer des blessures, voire la mort.

- Protéger les fichiers du support de mémoire amovible contre les logiciels malveillants par les mesures de protection appropriées, p. ex. un logiciel antivirus.

### 7.1.6 Mises à jour de sécurité / gestion des correctifs

Pour des raisons d'organisation, il n'est pas possible de mettre à disposition la version la plus récente des correctifs de sécurité de Windows lors de la livraison de la **PCU /** de l'**IPC**.

Les SINUMERIK IPC sur base Windows 10 sont livrés avec la variante LTSB 2016. Cette variante de Windows, en plus d'un support prolongé, offre la possibilité de charger les correctifs de manière ciblée et n'impose pas de mise à jour.

Installer sans délai les mises à jour de sécurité actuelles sur les appareils sur base Windows. Ne pas installer ces mises à jour pendant le fonctionnement de la machine. Utiliser à cet effet un serveur WSUS local (voir chapitre Concept de défense en profondeur (Page 28)).

**Remarque**

**Avant l'installation de mises à jour de Microsoft, observer les points suivants :**

- Sauvegarder l'état du système **avant la mise à jour** en vue d'un éventuel repli nécessaire. La compatibilité de la mise à jour avec la configuration individuelle de l'installation relève de la responsabilité du client.
- Ne jamais se connecter directement au serveur WSUS sur Internet ! Veiller à un environnement sécurisé et installer une couche intermédiaire (p. ex. réseau DMZ, pare-feu, modules SCALANCE S, etc.).

Une mise à jour périodique du système d'exploitation Windows d'un IPC faisant partie intégrante d'une machine est cependant difficile à réaliser dans la pratique ; par ailleurs, au plus tard après la fin du support, aucune mise à jour n'est plus disponible ; c'est pourquoi il convient d'assurer une protection de l'IPC selon le concept de défense en profondeur (Page 28), p. ex. avec un routeur de sécurité, ainsi qu'en utilisant une solution de liste blanche.

D'éventuelles failles de sécurité de la **NCU** sont également prises en compte ou éliminées dans la version actuelle du logiciel CNC.

**Remarque**

**Disponibilité**

La disponibilité des mises à jour de sécurité Microsoft est publiée dans les bulletins de sécurité Microsoft. L'utilisation des mises à jour de sécurité relève entièrement de l'appréciation et de la responsabilité du client. Elle peut s'effectuer sur la base de l'évaluation de "l'indice de gravité maximal" figurant dans le bulletin de sécurité Microsoft. Microsoft publie les informations relatives aux mises à jour de sécurité pour la PCU et les liens de téléchargement sur Internet (https://docs.microsoft.com/fr-fr/security-updates/).

## Voir aussi

Gestion des correctifs (Page 42)

## 7.1.7 Gestion des comptes

### 7.1.7.1 Définition des niveaux d'accès

#### Accès aux fonctions et aux paramètres machine

Le système d'accès définit l'accès aux fonctions et aux zones de données. On distingue les niveaux d'accès de 1 à 7, 1 étant le niveau le plus élevé et 7 le niveau le plus bas. Les niveaux d'accès 1 à 3 sont verrouillés par un mot de passe et les niveaux 4 à 7 par la position du commutateur à clé.

| Niveaux d'accès | Verrouillage par | Groupe fonctionnel | Classe de données |
|---|---|---|---|
| 1 | Mot de passe : SUNRISE | Constructeur de machines | Manufacturer (M) |
| 2 | Mot de passe : EVENING | Maintenance | Individual (I) |
| 3 | Mot de passe : CUSTOMER | Utilisateur | User (U) |
| 4 | Commutateur à clé, position 3 | Programmeur, régleur | User (U) |
| 5 | Commutateur à clé, position 2 | Opérateur qualifié | User (U) |
| 6 | Commutateur à clé, position 1 | Opérateur formé | User (U) |
| 7 | Commutateur à clé, position 0 | Opérateur semi-qualifié | User (U) |

## Mots de passe Linux / NCK

| Niveau | Nom d'utilisateur | UID |
|---|---|---|
| 1 | manufact | 102 |
| 2 | service | 103 |
| 3 | user | 104 |
| 4 | operator3 | 105 |
| 5 | operator2 | 106 |
| 6 | operator1 | 107 |
| 7 | operator | 108 |

Pour chaque utilisateur mentionné, il existe aussi un groupe Unix de même nom (et de même GID pour chaque UID). Tous les utilisateurs sont systématiquement membres de leur propre groupe et de tous les groupes de niveau "inférieur". Par exemple "operator2" est membre des groupes "operator2", "operator1" et "operator". Ces groupes régissent principalement les droits d'accès aux données.

**IMPORTANT**

**Utilisation abusive des données due à des mots de passe faibles**

L'attribution de mots de passe faibles peut faciliter une utilisation abusive des données. Les mots de passe faibles sont faciles à pirater.

Pour simplifier la mise en service, les mots de passe mémorisés sont prérenseignés.

- Lors de la mise en service, modifier systématiquement les mots de passe par défaut prérenseignés.
- Changer les mots de passe à intervalles réguliers.
- Pour logiciel CNC <V4.8 : modifier aussi le mot de passe Linux pendant la mise en service, en plus des mots de passe SINUMERIK Operate. Plus d'informations, voir le manuel de mise en service "Système d'exploitation NCU".
- Sur SINUMERIK ONE, un avertissement est affiché en permanence tant que les mots de passe n'ont pas été modifiés.

Plus d'informations sur l'attribution de mots de passe sécurisés, voir le chapitre Mots de passe (Page 40).

**Remarque**

**Modification de mot de passe entre SINUMERIK Operate et Linux**

Les niveaux d'accès pour SINUMERIK Operate et Linux sont fusionnés à partir de la version du logiciel 4.8 SP3 (840D sl/828D) et de la version du logiciel 6.13 (SINUMERIK ONE). La modification d'un mot de passe pour SINUMERIK Operate modifie simultanément le mot de passe correspondant dans Linux et réciproquement. Tenir compte du comportement suivant :

- En cas d'effacement général de la CN, aucun mot de passe n'est réinitialisé à sa valeur par défaut.
- Après une mise à niveau logicielle, les mots de passe pour SINUMERIK Operate restent valables pour la CN.
- Un mot de passe modifié une fois ne peut plus être réinitialisé à la valeur de livraison.
- Lors d'une nouvelle mise en service du système avec Restore [-full] (option de menu dans le Emergency Boot System "Recover system from USB memory stick (reformat CF card)"), la carte CompactFlash est formatée et le système est rétabli dans l'état de livraison. Les mots de passe ne sont pas contenus dans l'archive SINUMERIK. Après un Restore [-full], il faut donc systématiquement modifier les mots de passe par défaut et les remplacer par des mots de passe personnels.

### 7.1.7.2 Mot de passe Safety Integrated

En général, les données de mise en service sont protégées dans SINUMERIK Operate avec différents niveaux d'accès. Le paramétrage d'entraînement de sécurité est en outre protégé par le mot de passe Safety Integrated. Ce mot de passe est enregistré dans les données d'entraînement elles-mêmes, de sorte que seules les personnes autorisées connaissant le mot de passe peuvent modifier ces dernières.

**Remarque**

**Le mot de passe SINAMICS Safety doit être utilisé pour SINUMERIK Safety**

L'attribution du mot de passe Safety Integrated au moyen d'un masque SINUMERIK Operate est prise en charge à partir de V4.8 SP2 HF1. L'attribution du mot de passe Safety Integrated est également supportée par un masque de l'outil de mise en service SINUMERIK ONE Commissioning Tool.

- Définir dans tous les cas un mot de passe Safety afin d'éviter que les paramètres ne puissent être modifiés au moyen du logiciel de configuration externe Starter ou du logiciel de mise en service SINAMICS Startdrive.

**Plus d'informations**, voir le manuel de mise en service Safety Integrated plus.

## Voir aussi

Manuel de mise en service SINUMERIK 840Dsl Safety Integrated plus (https://support.industry.siemens.com/cs/de/en/view/109777982/fr)

### Plus d'informations

**Plus d'informations** sur la procédure de modification des mots de passe des niveaux d'accès, ainsi que sur les niveaux d'accès pour les programmes et les touches logicielles et les droits d'accès aux fichiers, voir le manuel "Manuel de mise en service SINUMERIK Operate (IM9) (https://support.industry.siemens.com/cs/ww/en/view/109769186), chapitre "Paramètres généraux > Niveaux de protection".

## 7.1.7.3 Fonction de verrouillage CNC

La "fonction de verrouillage CNC" permet d'activer une date de verrouillage dans la commande, à l'aide d'un fichier crypté généré avec l'application SINUMERIK Integrate Access MyMachine (AMM). Il est ainsi possible de limiter l'utilisation de la machine à la durée s'achevant à la date de verrouillage. En cas de dépassement de la date de verrouillage, la fonction NC-Start de la commande est bloquée.

La fonction de verrouillage CNC prend en charge le modèle commercial avec utilisation limitée dans le temps. La protection vise à empêcher une utilisation non autorisée au-delà de la période de temps paramétrée.

**Remarque**

**Uniquement pour SINUMERIK 828D**

Noter que la fonction de verrouillage CNC n'est disponible que sur la commande SINUMERIK 828D.

**Plus d'informations** sur la fonction de verrouillage CNC et la génération du fichier Lockset crypté, voir sous :

- Manuel d'utilisation SINUMERIK Integrate Access MyMachine /P2P (PC) (https://support.industry.siemens.com/cs/de/en/view/109770206)
- Description fonctionnelle "AP", chapitre "P4 : AP pour SINUMERIK 828D > Fonction de verrouillage CNC"

## 7.1.7.4 Supprimer la clé SSH préinstallée

### Cas d'application

La suppression de la clé SSH préinstallée par Siemens permet de réduire le risque d'utilisation abusive des données. Cependant, pour pouvoir continuer à accéder au système avec des droits suffisants, il est possible de définir et d'installer des clés SSH personnelles.

### Commande de maintenance

La commande de maintenance 'sc' est un outil permettant d'effectuer différentes tâches de maintenance sur une SINUMERIK NCU.

| | |
|---|---|
| Syntaxe : | sc clear preinstalled-keys |
| Noms alternatifs : | --- |
| Niveau d'habilitation | service |

Cette commande supprime toutes les clés SSH préinstallées par Siemens sur la commande. En cas d'appel à partir du système de maintenance, les clés sur la carte CompactFlash sont concernées, et non les clés SSH sur le système de maintenance lui-même.

### Plus d'informations

Plus d'informations, voir le Manuel de mise en service du logiciel de base et du logiciel de commande (https://support.industry.siemens.com/cs/de/en/view/109777905).

## 7.1.7.5 Serveur web AP

À l'état de livraison, l'AP n'a aucun mot de passe et le serveur web de l'AP n'est pas activé.

**Remarque**

- En cas d'activation du serveur web de l'AP dans le projet S7, il faut définir un utilisateur correspondant et un mot de passe associé pour le serveur web de l'AP. Attribuer un mot de passe sécurisé. Observer les consignes du chapitre Mots de passe (Page 40) pour l'attribution du mot de passe.
- Pour assurer la confidentialité et l'intégrité dans la communication, utiliser exclusivement le protocole HTTPS.

### Plus d'informations

Plus d'informations sur le serveur web de l'AP, voir le Description fonctionnelle S7-1500, ET 200SP, ET200pro Webserver (https://support.industry.siemens.com/cs/ww/fr/view/59193560).

### 7.1.7.6 Niveaux d'accès des touches logicielles

L'OEM et l'utilisateur peuvent désactiver l'affichage et l'utilisation de certaines touches logicielles afin d'adapter le logiciel de commande aux fonctions requises, de façon aussi claire et ciblée que possible. L'étendue fonctionnelle du système s'en trouve limitée afin d'empêcher l'accès à certaines fonctions du logiciel de commande ou de réduire les risques d'erreur de manipulation.

**Remarque**

**Applicabilité des niveaux d'accès modifiés pour les touches logicielles**

Le réglage de certains niveaux d'accès pour les touches logicielles d'une PCU agit uniquement sur les touches logicielles correspondantes de la PCU. Pour convertir les droits d'accès sur la NCU, le constructeur comme l'utilisateur doivent utiliser les mécanismes appropriés et définir les autorisations en conséquence.

**Plus d'informations**, voir le Manuel de mise en service SINUMERIK Operate (IM9) (https://support.industry.siemens.com/cs/ww/en/view/109769186), chapitre "Niveaux d'accès pour les programmes".

### 7.1.7.7 Protection d'accès BIOS et AMT

Pour empêcher l'accès non autorisé au BIOS de la PCU 50 et des SIMATIC IPC, définir un mot de passe BIOS sûr. (Voir chapitre Mots de passe (Page 40))

#### Plus d'informations

**Plus d'informations** sur les réglages du BIOS de la PCU 50, voir le Manuel de mise en service logiciel de base PCU (IM8) (https://support.industry.siemens.com/cs/de/de/view/109748542/fr).

#### Définir un mot de passe pour AMT (Intel® Active Management Technology)

La fonction Active Management Technology (AMT) sert à la gestion à distance de la PCU. Des mesures de protection appropriées (p. ex. la segmentation du réseau) doivent être prises pour la gestion à distance, afin de garantir le fonctionnement sécurisé de l'installation.

Pour des raisons de sécurité, AMT est désactivé à la livraison de la PCU. Lors de la première activation d'AMT dans les paramètres du BIOS, attribuer un mot de passe sûr afin d'éviter une utilisation abusive de la gestion à distance.

Plus d'informations sur la fonction AMT de la PCU et sur la procédure de modification du mot de passe, voir sur Internet (https://support.industry.siemens.com/cs/de/en/view/52310936).

#### 7.1.7.8 Protection par mot de passe pour Create MyConfig (CMC)

| IMPORTANT |
| --- |
| **Utilisation abusive des données due à des droits d'accès incorrects**<br>Les données d'accès telles que les mots de passe préconfigurés pour l'accès à la commande peuvent faire l'objet d'un vol ou d'une utilisation abusive.<br>• Mettre en place des mesures organisationnelles garantissant que seules des personnes autorisées ont accès à ces fichiers. |

**Remarque**

**Protection par mot de passe pour les fichiers externes liés**

Les mécanismes de protection (protection par mot de passe) intégrés dans CMC ne s'appliquent pas aux fichiers externes liés qui sont intégrés dans le contexte de CMC.

**Remarque**

**Sécuriser les packages CMC contre la réimportation**

Noter que les packages CMC doivent être protégés contre la réimportation par mot de passe.

- Créer systématiquement un mot de passe contre la réimportation au moment de l'attribution d'un mot de passe pour un nouveau projet.

### 7.1.8 Protection de savoir-faire

Les fonctionnalités suivantes offrent une protection du savoir technologique et une protection contre l'accès non autorisé aux commandes SINUMERIK :

#### 7.1.8.1 SINUMERIK Integrate Lock MyCycles

La fonctionnalité "SINUMERIK Integrate Lock MyCycles" (protection des cycles) permet de crypter des cycles puis de les stocker dans la commande sous une forme protégée. Le cryptage des cycles s'effectue en dehors de la commande avec le programme SINUMERIK Integrate Access MyMachine/P2P.

Pour les cycles disposant de la protection de cycle, l'exécution dans la CN s'effectue sans restriction.

Toute tentative de visualiser les cycles disposant de la protection de cycle est bloquée afin de protéger le savoir-faire du constructeur.

Cette option logicielle est disponible pour les commandes SINUMERIK 808D, 828D et 840D sl.

Un exemple d'application de la protection des cycles pour SINUMERIK est disponible sur Internet (https://support.industry.siemens.com/cs/ww/fr/view/109474775/en).

### Plus d'informations

**Plus d'informations** sur la protection des cycles, voir le Manuel d'utilisation SINUMERIK Access MyMachine /P2P (PC) (https://support.industry.siemens.com/cs/ww/en/view/109770206).

## 7.1.8.2 SINUMERIK Integrate Lock MyPLC

Grâce aux propriétés de bloc, vous pouvez protéger les blocs créés dans l'AP SIMATIC entre autres contre les modifications non autorisées.

Les propriétés de bloc doivent être modifiées lorsque le bloc est ouvert. Outre les propriétés modifiables, la boîte de dialogue correspondante affiche également des données pour votre information : celles-ci ne peuvent pas être modifiées.

Un bloc compilé avec cette option ne permet pas de visualiser la partie instructions. L'interface du bloc peut être visualisée mais pas modifiée.

### Plus d'informations

Plus d'informations sur la protection des blocs, voir le Manuel de programmation et d'utilisation SIMATIC Programmer avec STEP 7 (https://support.industry.siemens.com/cs/de/de/view/109751825/fr), chapitre "Propriétés de bloc".

**Remarque**

Le CP intégré dans la SINUMERIK 840D sl ne prend pas en charge l'option "Protection d'accès/niveau de protection".

### Cryptage des blocs

À partir de STEP 7 version 5.5 SP3 et du logiciel système CNC V4.5 SP2 pour 840D sl/ 840D ou V6.13 pour SINUMERIK ONE, il est possible de créer, pour les fonctions et blocs fonctionnels, une protection de blocs cryptée pour la vue hors ligne et en ligne. Cette fonction permet de crypter vos blocs fonctionnels et de protéger le code de bloc fonctionnel contre tout accès non autorisé.

Pour SINUMERIK, il faut sélectionner lors du cryptage l'option "SINUMERIK" et en plus, le cas échéant, SIMATIC.

Une procédure détaillée sur la manière de crypter les blocs est disponible sur Internet (https://support.automation.siemens.com/WW/view/fr/45632073).

### 7.1.8.3 OPC UA

OPC UA (Unified Architecture) est un protocole de communication industrielle standardisé pour l'accès aux données des commandes, p. ex. par des systèmes de conduite. L'option logicielle SINUMERIK Integrate Access MyMachine /OPC UA, permet de lire et d'écrire des variables d'une SINUMERIK 840D sl, d'une SINUMERIK 828D ou d'une SINUMERIK ONE par le biais de ce protocole de communication.

| IMPORTANT |
| --- |
| **Utilisation abusive des données due à une connexion au client non sécurisée**<br>Une connexion non cryptée au client OPC UA entraîne un risque d'utilisation abusive des données.<br>• Crypter systématiquement la liaison au client OPC UA.<br>• Pour plus d'informations sur le cryptage de la liaison de données, voir le Manuel de configuration SINUMERIK Access MyMachine /OPC UA (https://support.industry.siemens.com/cs/de/de/view/109777871/fr). |

| IMPORTANT |
| --- |
| **Utilisation abusive des données due à une gestion des utilisateurs / des droits d'accès incorrecte**<br>Une gestion des utilisateurs incorrecte et une attribution erronée des droits d'accès peuvent entraîner un risque considérable pour la sécurité. Des utilisateurs risquent d'avoir accès à des données ou des actions pour lesquelles ils n'ont pas d'autorisation.<br>• Sélectionner soigneusement les utilisateurs et les droits qui leurs sont attribués. Il est de la responsabilité de l'administrateur d'assurer une gestion des utilisateurs et une attribution des droits appropriées. |

**Remarque**

**Sélectionner un mot de passe sûr**

Définir systématiquement un mot de passe sûr pour la connexion au client OPC UA ! Plus d'informations sur le choix d'un mot de passe sûr, voir le chapitre Mots de passe (Page 40).

### 7.1.8.4 Gestion des utilisateurs dans TIA Portal

TIA Portal offre la possibilité d'utiliser une gestion des utilisateurs pour les projets. Cela permet de protéger ces derniers de toute modification accidentelle ou non autorisée. Pour activer la gestion des utilisateurs, un utilisateur configure la protection du projet. Cet utilisateur devient alors l'administrateur de projet. Après l'activation de la protection du projet, seuls les utilisateurs autorisés peuvent ouvrir le projet et travailler sur celui-ci. Tenir compte du fait que la protection du projet ne peut pas être annulée.

La gestion des utilisateurs dans TIA Portal est disponible pour les commandes SINUMERIK 840D sl et SINUMERIK ONE.

### UMC - User Management Component

Il est également possible d'installer le pack logiciel "User Management Component UMC" sur un ou plusieurs ordinateurs ; il met à disposition une gestion centrale des utilisateurs.

### Plus d'informations

Plus d'informations sur la gestion des utilisateurs sécurisée, voir l'aide en ligne de TIA Portal.

#### 7.1.8.5 SIMATIC Logon

### Gestion des utilisateurs et traçabilité

Le pack optionnel SIMATIC Logon sert à instaurer des droits d'accès pour les projets et les bibliothèques dans STEP 7. Ces projets ne sont alors accessibles qu'à un groupe de personnes autorisées. SIMATIC Logon est utilisable en combinaison avec SINUMERIK STEP 7.

Pour plus d'informations, voir le chapitre Contrôle d'accès sécurisé avec SIMATIC Logon (Page 80).

## 7.1.9 Sauvegarde des données

Dans la SINUMERIK, il existe différentes formes d'archive et différentes méthodes d'archivage pour les différents composants.

### Moment de sauvegarde des données

Procéder à une sauvegarde des données dans les cas suivants :

- Après une mise en service
- Modification de paramètres spécifiques à la machine
- Après le remplacement d'un composant matériel
- Avant et après une mise à niveau logicielle
- Avant l'activation de paramètres machine de configuration de la mémoire

**Plus d'informations**, voir les manuels suivants :

- Manuel de mise en service SINUMERIK 840Dsl Mise en service CNC (https://support.industry.siemens.com/cs/ww/en/view/109777906)
- Manuel de mise en œuvre SINUMERIK ONE Nouvelle installation et mise à niveau

Observer les consignes générales sur le stockage sécurisé des données d'archivage au chapitre Stockage des données (Page 39).

| IMPORTANT |
| --- |
| **Utilisation abusive de données confidentielles sur la commande**<br>Il existe un risque d'utilisation abusive de données confidentielles sur la commande<br>• Éviter par conséquent de charger des données confidentielles sur la commande (p. ex. avec le logiciel "SINUMERIK Integrate Access MyMachine/P2P").<br>• Stocker les données confidentielles localement uniquement sous forme cryptée ou les stocker dans un emplacement de mémoire crypté sur le réseau. |

### 7.1.10 Élimination

| IMPORTANT |
| --- |
| **Utilisation abusive des données due à un effacement de données non sûr**<br>Un effacement des données incomplet ou non sûr sur les cartes mémoires ou les disques durs des produits peut être à l'origine d'une utilisation abusive des données des programmes pièce, archives, etc. par des tiers.<br>• Veiller par conséquent à effacer de manière sûre tous les supports de mémoire utilisés **avant l'élimination du produit** :<br>• Il existe des programmes permettant de vider/formater les supports de mémoire. Ou s'adresser à un prestataire de services d'élimination certifié qui se chargera de cette tâche. |

## 7.2 Logiciel CNC Shopfloor Management

Le chapitre suivant fournit une vue d'ensemble des mesures de sécurité à prendre pour protéger les produits du logiciel CNC Shopfloor Management contre les menaces. Des descriptions et procédures détaillées sont fournies dans la documentation du logiciel CNC Shopfloor Management correspondante indiquée.

### 7.2.1 Vue d'ensemble du système

Avec les 3 niveaux "In Cloud", "In Line" et "In Machine", une architecture IT durable a été mise au point avec CNC Shopfloor Management Software. Ces niveaux correspondent aux 3 plateformes "MindSphere", "SINUMERIK Integrate" et "SINUMERIK/SINUMERIK Edge" avec de nombreuses fonctionnalités sur mesure, du terrain jusqu'au cloud.

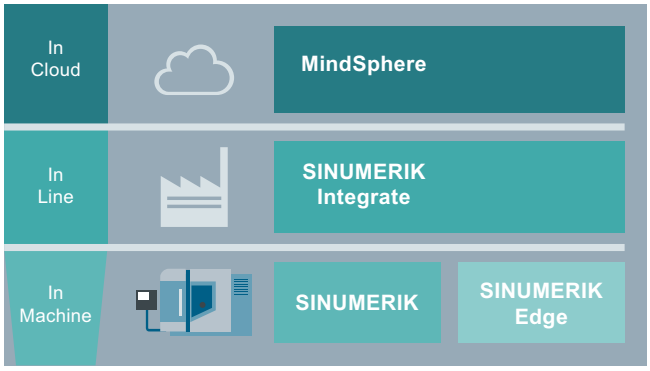



Figure 7-2 Logiciel CNC Shopfloor Management

### 7.2.2 Applications cloud (In Cloud)

MindSphere offre une sécurité conforme à l'état de la technique aussi bien lors de la collecte des données sur site que lors de la transmission vers le cloud et du stockage dans le cloud.

L'environnement de sécurité se base sur les principes de normes industrielles telles que CEI 62443, International Organization for Standardization (ISO)/CEI 27001, et de l'Office fédéral allemand pour la sécurité en matière de technologies de l'information (BSI) ainsi que sur les recommandations des autorités concernant le traitement des données en environnement cloud.

Conformément aux pratiques de communication industrielle éprouvées, toute communication entre le client et MindSphere via des points terminaux publics est protégée par TLS V1.2. Des certificats x509 fiables du Siemens Trust Center sont utilisés, qui satisfont aux exigences de l'Institut européen des normes de communication (European Telecommunications Standards Institute, ETSI) et du Forum CA/B (Certification Authority Browser Forum).

Plus d'informations sur le cryptage en liaison avec MindSphere, voir Livre blanc Mindsphere (https://www.plm.automation.siemens.com/global/fr/topic/mindsphere-whitepaper/28842).

Les données enregistrées sont toujours sauvegardées sur des serveurs haute performance dans les centres de calcul des fournisseurs d'infrastructure de Siemens. Tous les centres de

calcul répondent aux normes les plus exigeantes en matière de sécurité et sont protégés contre les cybermenaces. En tant que fournisseurs commerciaux d'un Cloud-IaaS (Infrastructure as a Service), ils offrent des normes de sécurité plus élevées que les équipements privés locaux de stockage des données. Les centres de calcul sont exploités conformément aux meilleures pratiques du secteur.

En tant que couche de sécurité supplémentaire, tous les partenaires d'infrastructure cloud doivent appliquer des mesures de sécurité locales telles que les badges d'identité électroniques avec photo, la gestion d'accès pour titulaires de carte, la biométrie, la surveillance vidéo numérique avec enregistrement et alarmes.

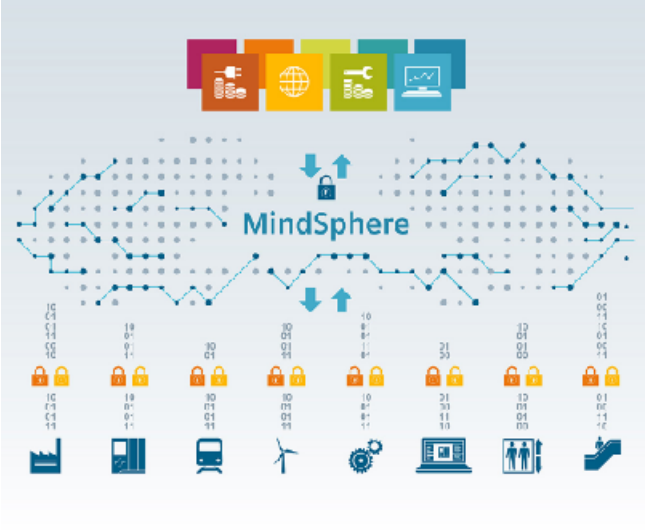



Figure 7-3 MindSphere

### 7.2.2.1 Manage MyMachines /Remote

#### Mesures de sécurité et durcissement du système

**Remarque**

L'utilisateur de Manage MyMachines /Remote doit toujours s'assurer que le produit est exploité avec les versions les plus récentes du client SINUMERIK Integrate et des clients Manage MyMachines /Remote Service Engineer et Machine Operator. Respecter en outre les directives de sécurité industrielle fournies aux paragraphes 1.3 et 2.3 de la Description fonctionnelle de Manage MyMachines /Remote (https://support.industry.siemens.com/cs/ww/en/view/109759394).

La connexion des commandes SINUMERIK à MindSphere via "TLS 1.2 /HTTPS" répond aux normes de sécurité les plus élevées.

La confirmation automatique de l'identité de la machine en utilisant le jeton mis à disposition par MindSphere pour l'intégration (onboarding) de la machine garantit que la session à distance accède à la bonne machine.

### Élimination

Pour supprimer intégralement une installation de Manage MyMachines /Remote, il convient de s'assurer que tous les logiciels et certificats ont été correctement supprimés de l'appareil Windows ou du système de commande SINUMERIK, y compris des systèmes de sauvegarde. Les données resteront disponibles dans MindSphere, sauf en cas de fermeture du locataire.

Plus d'informations sur la procédure d'élimination, voir la Description fonctionnelle Manage MyMachines /Remote (https://support.industry.siemens.com/cs/ww/en/view/109759394).

Plus d'informations sur les concepts généraux de l'accès à distance sécurisé aux installations industrielles, voir les documents suivants :

- cRSP IT Security Concept (https://support.industry.siemens.com/cs/ww/en/view/109759394)
- Siemens common Remote Service Platform (cRSP) (https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&id1=A6V11272777)

### Voir aussi

cRSP IT Security Concept (https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&id1=A6V11272775)

## 7.2.3 Applications PC / Serveur / Desktop (In Line)

### 7.2.3.1 SINUMERIK Integrate 4.1

### Accès aux ressources du serveur SINUMERIK Integrate

**Remarque**

**Accès aux ressources du serveur SINUMERIK Integrate**

L'accès en écriture et en lecture au système de fichiers et aux ressources du système d'exploitation (en particulier à la base de registre Windows) du serveur SINUMERIK Integrate est uniquement autorisé aux utilisateurs disposant de droits d'administrateur. S'assurer que ces comptes d'administrateur sont protégés par des mots de passe suffisamment sûrs.

| IMPORTANT |
| --- |
| **Manipulation possible des données**<br>Le risque existe qu'un pirate parvienne à accéder au système de fichiers du serveur SINUMERIK Integrate ou des différents clients SINUMERIK Integrate via le réseau de production/ de machine (Intranet). Le pirate peut alors manipuler différentes parties du système (p. ex. contenus de la base de données). Le pirate peut modifier par exemple des données d'outil, des programmes CN, des archives de machine ou la structure de l'installation. SINUMERIK Integrate n'est pas en mesure de parer cette forme d'attaque.<br>• En tant qu'exploitant du réseau de machines, prendre des mesures pour la sécurité industrielle du réseau de production/de machine. |

## Utilisation d'interfaces de programmation ouvertes

| IMPORTANT |
| --- |
| **Utilisation abusive des données lors de l'utilisation d'interfaces de programmation ouvertes**<br>Un risque d'utilisation abusive des données existe lors de l'utilisation d'interfaces de programmation ouvertes<br>• Lors de l'utilisation d'interfaces de programmation ouvertes, n'utiliser que des clients communicant avec le serveur SINUMERIK Integrate au minimum via des voies de communication "TLS 1.2 /https".<br>• Noter que la version TLS correspondante n'est pas prise en charge pour tous les systèmes d'exploitation. |

## Durcissement

Par durcissement, on entend l'élimination de tous les composants logiciels et de toutes les fonctions qui ne sont pas impérativement nécessaires pour la réalisation des tâches prévues par l'application souhaitée.

**Durcissement de logiciels de fabricants tiers Microsoft™ Internet Information Server, Microsoft™ SQL Server, navigateurs (Microsoft™ Internet Explorer, Mozilla Firefox)**

SINUMERIK Integrate a besoin de logiciels de fabricants tiers : entre autres, des produits Microsoft™ Internet Information Server, Microsoft™ SQL Server et divers navigateurs. Ces derniers doivent être durcis selon l'état actuel de la technique. Limiter notamment l'accès à Microsoft™ SQL Server sur l'hôte local et sécuriser l'accès avec un mot de passe. Crypter l'accès à la base de données. De plus, il convient d'utiliser uniquement des navigateurs actuels pour la communication avec le serveur SINUMERIK Integrate. En cas d'utilisation de navigateurs obsolètes (SSL au lieu de TLS), il n'est pas possible de garantir une communication sécurisée.

**Durcissement de produits touchant à SINUMERIK Integrate : p. ex. dispositif de préréglage d'outil, Teamcenter, AUVESY™ VersionDog**

SINUMERIK Integrate communique avec des produits logiciels tels que les dispositifs de préréglage d'outil, Teamcenter ou VersionDog. Ces derniers doivent être durcis selon l'état

actuel de la technique, afin qu'aucune répercussion négative ne puisse avoir lieu via cette voie de communication.

### Échange de fichiers de réseau via des lecteurs communs

**Remarque**

**Échange de fichiers de réseau via des lecteurs communs (Server Message Block ou SMB)**

En cas d'utilisation de SMB pour l'échange de fichiers avec des fonctions SINUMERIK Integrate, utiliser des mécanismes d'authentification standard (nom d'utilisateur/ mot de passe). Limiter en outre les accès des différents utilisateurs en fonction de leurs droits. Le stockage de données sur des lecteurs communs doit être réduit au minimum indispensable.

### Sauvegarde des données

Pour la sauvegarde des données sur les machines-outils, voir le chapitre "Sauvegarde des données (Page 65)". Sauvegarder en plus la page serveur. Les données à sauvegarder sont la configuration et les contenus de la base de données Microsoft SQL Server, du serveur SINUMERIK Integrate et des applications SINUMERIK Integrate suivantes :

- MMT
- SFT RM
- MMP
- AMC
- AMP

Réaliser une sauvegarde des données dans les cas suivants :

- Après une mise en service
- En cas de modification de la configuration matérielle
- Après un remplacement de matériel
- Avant et après une mise à niveau logicielle

### Sécurité de communication des applications SINUMERIK Integrate

La communication entre le serveur SINUMERIK Integrate et les différentes formes de client (telles que MMT ou les navigateurs) est préconfigurée avec HTTP. Il est recommandé de recourir à l'assistance de techniciens de SAV formés pour la configuration nécessaire, en particulier pour SINUMERIK Integrate. Changer la communication dans la mesure du possible pour HTTPS, qui nécessite son propre certificat. Il convient de noter que toutes les combinaisons client/serveur ne permettent pas HTTPS.

## 7.2.3.2 Mode cloud

Si les applications AMM et AMC sont utilisées en mode cloud, l'exploitant Siemens AG assure la sécurité du serveur SINUMERIK Integrate. Le client doit uniquement protéger l'infrastructure côté machine.

## Pare-feu du réseau de machine

Contrairement au mode autonome, une liaison au serveur cloud en dehors du réseau de machine et d'entreprise est nécessaire pour les applications AMM et AMC de SINUMERIK Integrate. Les pare-feu correspondants doivent débloquer les ports requis. Toutefois, il convient de ne pas ouvrir d'autres ports que ces ports requis. Plus d'informations sur les réglages de pare-feu nécessaires, voir le Manuel de mise en œuvre SINUMERIK Integrate, chapitre "Configuration système requise".

## Hameçonnage de mots de passe

Des "hameçonneurs (phishers)" pourraient tenter de se procurer les données de connexion qui leur permettraient d'exécuter des actions dans SINUMERIK Integrate en se faisant passer pour l'utilisateur. Les cybercriminels pourraient par exemple falsifier des e-mails ou des sites Internet de Siemens afin de soutirer des informations confidentielles aux utilisateurs de SINUMERIK Integrate. Dans ce cas, les utilisateurs sont p. ex. priés de saisir leurs données d'accès à leur organisation SINUMERIK Integrate dans un formulaire et de les envoyer.

**Remarque**

**Tenir compte des points suivants en cas d'e-mail suspect :**

- Rester prudent en cas de réception d'e-mails d'expéditeurs inconnus, en particulier lorsque ces e-mails contiennent des liens et des pièces jointes. Ne jamais ouvrir des pièces jointes suspectes ni cliquer sur les liens contenus dans l'e-mail.
- Vérifier soigneusement l'adresse e-mail complète de l'expéditeur.
- Vérifier l'intégrité des liens inclus dans l'e-mail (p. ex. en déplaçant le pointeur de la souris sur le lien). Des indices typiques sont des fautes d'orthographe ou des noms de société trompeurs contenus dans les liens.
- Utiliser des signatures numériques dans les e-mails.
- En cas de doute, ne jamais transmettre d'informations confidentielles.

## Traitement des informations confidentielles

La voie de transmission entre le pare-feu de l'entreprise et le serveur SINUMERIK Integrate est protégée contre les accès malveillants par le protocole de communication sécurisé (TLS). Les tiers ne peuvent ni espionner ni modifier les informations transmises. Respecter par ailleurs les directives spécifiques à l'entreprise lors de la transmission d'informations confidentielles par AMM et AMC.

## 7.2.4 Applications à proximité de la commande (In Machine, SINUMERIK Edge)

### 7.2.4.1 SINUMERIK Edge

#### Vue d'ensemble

SINUMERIK Edge est un périphérique Edge commandé à distance qui, dans une architecture IoT/OT étendue, sert à la fois de passerelle de terrain et de nœud de calcul pour des travaux utilisateur (User Workloads) quelconques. SINUMERIK Edge autorise ainsi un flux de traitement des données et des informations vertical entre toutes les couches :

- In Machine
- In Line et
- In Cloud

Ceci comprend également la mémorisation temporaire ou permanente des données de processus. Il appartient donc à SINUMERIK Edge d'empêcher, par son architecture de sécurité, toute régression/érosion de la sécurité du réseau existante et du niveau de protection des données. Là aussi, une assistance organisationnelle est nécessaire pour éviter de neutraliser les différents mécanismes de protection de SINUMERIK Edge.

#### Fonctions de sécurité et mesures de sécurité

SINUMERIK Edge est équipé de 2 connecteurs de réseau physiques (RJ45) qui, selon le manuel, doivent être utilisés pour la connexion au niveau In Machine et au niveau In Line. S'assurer que l'affectation des ports est correcte en considérant les raisons suivantes :

- Pour le réseau "In Machine", on suppose une communication en grande partie non protégée.
- Pour le réseau "In Machine", aucune connectivité non contrôlée avec des réseaux de niveau supérieur (In Line, In Cloud) n'est possible.

SINUMERIK Edge garantit, grâce à une architecture de réseau à plusieurs couches, une isolation des deux réseaux qui n'est franchie que par un flux de données défini par l'application. Grâce à l'utilisation de la technologie de conteneurs, d'autres mécanismes d'isolation de la charge de travail (workload) (application Edge) existent en ce qui concerne le réseau, la mémoire et les ressources CPU.

La communication de SINUMERIK Edge en direction "In Cloud" et "In Line" s'effectue systématiquement via un canal crypté de bout en bout (TLS 1.3). L'intégration dans une chaîne de confiance (trust chain) basée sur une infrastructure à clés publiques (PKI) est prise en charge en complément. Ceci permet de garantir une transmission de confiance ainsi qu'une restriction aux seuls partenaires de communication autorisés. Une autorisation basée sur le client avec des certificats client est possible pour l'échange de données In Line dans les environnements avec des exigences de sécurité particulièrement élevées.

L'échange initial des certificats requis pour la communication de sécurité entre le système de gestion Edge (MindSphere / In Cloud) et SINUMERIK Edge (In Line) est effectué pendant la procédure d'intégration (appelée onboarding). La procédure d'onboarding contient l'échange d'un secret partagé ("shared secret") qui lie un périphérique logique (MindSphere Asset) à un périphérique physique (SINUMERIK Edge). Cet échange n'ayant pas lieu via la même

infrastructure de communication, une compromission peut être exclue dès la procédure d'onboarding. Un autre aspect de l'onboarding est l'intégration des services IoT MindSphere (Timeseries Store, FileStore, Fleetmanager, …) dans les locataires MindSphere corrects. La plateforme SINUMERIK Edge garantit en outre qu'à aucun moment il n'est possible d'établir un flux de données dans un locataire ou un actif non prévu à cet effet.

**Remarque**

Un locataire MindSphere et un compte MindAccess valide (au moins IoT value plan S) sont nécessaires pour l'utilisation de SINUMERIK Edge.

SINUME

RIK Edge communique exclusivement via des liaisons sortantes ("outgoing"). Ceci signifie qu'aucune exposition de SINUMERIK Edge n'est nécessaire dans les niveaux In Line ou In Cloud. En fait, ce scénario n'est pas recommandé. Indépendamment de cette configuration, l'accessibilité des points terminaux MindSphere par SINUMERIK Edge doit être assurée temporairement. Ceci concerne l'onboarding, la mise à jour du firmware et l'installation/ désinstallation des applications Edge.  SINUMERIK Edge permet aux applications (Industrial App) non seulement de mettre des données à disposition In Cloud par une voie contrôlée, mais surtout de mettre à disposition des interfaces utilisateur et/ou des interfaces (API) en vue d'autoriser de nouveaux flux de travail (In Line) ou de compléter des flux de travail existants. Pour cela, les applications mettent à disposition leurs propres gestions des utilisateurs et des accès. Les consignes de sécurité correspondantes figurent dans la documentation considérée.

La communication entre SINUMERIK Edge et SINUMERIK s'effectue uniquement via le réseau "In Machine" et est cryptée selon le protocole correspondant. Les mécanismes d'autorisation varient cependant en fonction du protocole utilisé. Les mécanismes de protection de certains protocoles étant faibles, il importe dans ces cas de respecter des stratégies de mot de passe adéquates et de s'assurer par des mesures organisationnelles que les mots de passe ne sont jamais enregistrés (ou seulement dans des cas impératifs).

SINUMERIK Edge est également protégé par les fonctions suivantes contre des manipulations indésirables ou contre un affaiblissement de la sécurité tant au niveau firmware qu'au niveau application :

- Measured / Secured-Boot
- Full Disk Encryption
- Rootless Access

Afin de garantir un niveau de sécurité élevé de SINUMERIK Edge sur le long terme, le firmware est continuellement développé et durci. Ceci est nécessaire pour s'adapter aux menaces contre la cybersécurité qui ne cessent de se renforcer. Un mécanisme de mise à jour est disponible à cet effet, en tant que partie intégrante du firmware de SINUMERIK Edge ; ce mécanisme fait partie de la stratégie de sécurité et est intégré en tant que tel dans le processus informatique.

# 7.3 SIMOTION

## Mesures de sécurité SIMOTION

Le chapitre suivant fournit une vue d'ensemble des mesures de sécurité industrielle pour SIMOTION (Motion Control), à prendre pour protéger une installation contre les menaces.

### Fonctions de sécurité

- La commande contient de manière standard uniquement du code compilé. Aucun chargement et aucune réingénierie ne sont donc possibles.
- Aucune modification de la configuration n'est possible sans le projet d'ingénierie correspondant
- Protection de savoir-faire pour les programmes source avec mot de passe et cryptage
- Protection applicative contre la copie de la configuration sur le système de commande
- Détection de manipulations du code source avec le système d'ingénierie SIMOTION SCOUT
- Activation/désactivation de fonctions non utilisées (serveur web, serveur OPC UA, ports, etc.)
- Utilisation de SIMATIC Logon pour l'accès à un projet uniquement avec les droits correspondants
- Antivirus et mises à jour de sécurité pour commandes sur base PC SIMOTION (SIMOTION P)

L'installation de production est généralement divisée en différents segments de réseau. Des composants équipés des fonctions de sécurité nécessaires sont placés en amont de ces segments. Dans la vue d'ensemble graphique, ces composants sont représentés avec un symbole de cadenas.

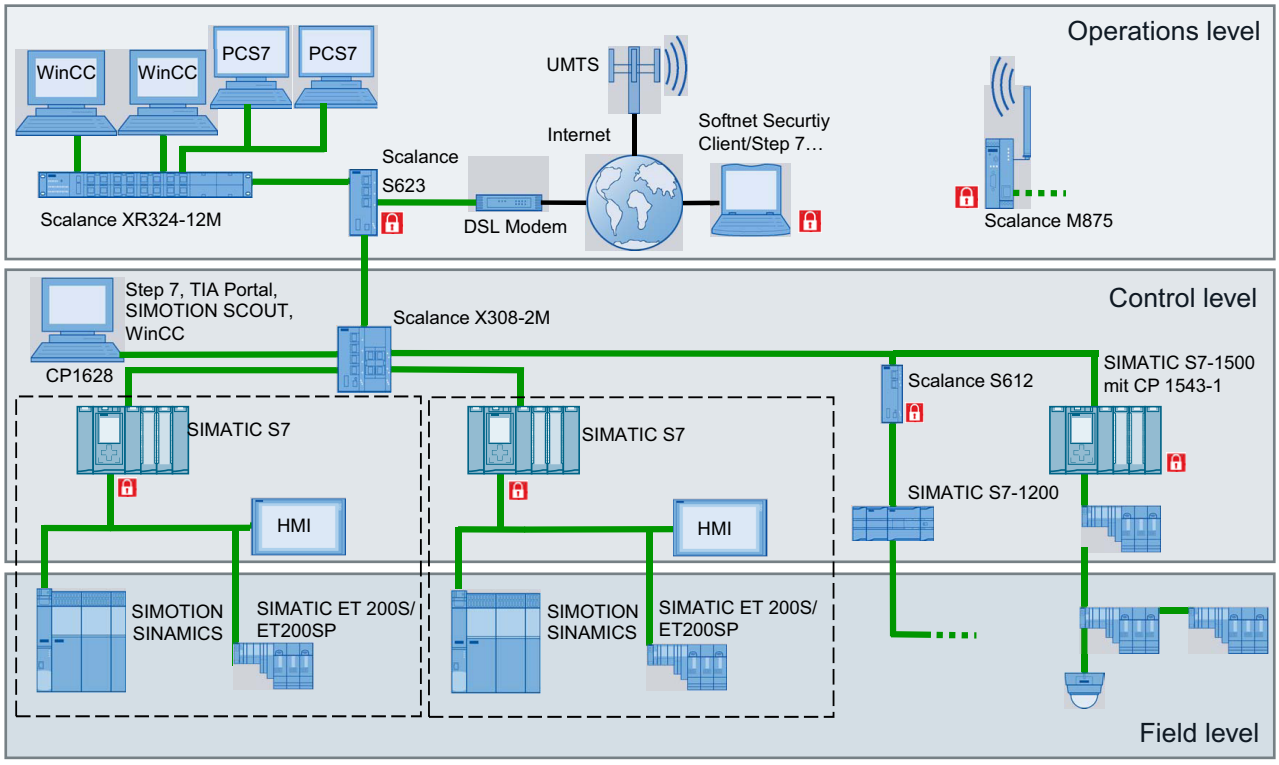



Figure 7-4 Représentation d'une installation de production type avec des zones sécurisées

## Voir aussi

Des descriptions détaillées et procédures supplémentaires sont fournies dans la documentation SIMOTION correspondante.

De nombreux produits (SINUMERIK, SIMOTION, SINAMICS) contiennent OpenSSL. Pour ces produits :

- Ce produit comprend un logiciel (https://www.openssl.org/) développé par le projet OpenSSL pour une utilisation dans la boîte à outils OpenSSL.
- Ce produit comprend un logiciel (mailto:eay@cryptsoft.com) cryptographique créé par Eric Young.
- Ce produit comprend un logiciel (mailto:eay@cryptsoft.com) développé par Eric Young.

## 7.3.1 Durcissement

### 7.3.1.1 Sécurité des ports

#### Désactivation des ports matériels

Pour les appareils SIMOTION à partir de la version 4.4, il est possible de désactiver (état **Disable**) des ports matériels individuels des interfaces PROFINET (p. ex. ports de l'interface X150) dans le système d'ingénierie (HW Config). Ceci empêche la connexion illicite d'appareils et augmente la sécurité en ce qui concerne l'accès au système par des tiers. Il convient donc de désactiver les ports non utilisés.

**Remarque**

Il n'est plus possible d'accéder à un appareil SIMOTION par un port matériel désactivé d'une interface PROFINET.

Le système d'ingénierie et la pile PN garantissent qu'au moins un port par interface n'est pas mis sur **Disable**, afin d'éviter que l'utilisateur n'exclue son propre accès. Le réglage par défaut est **Automatic settings**.

#### Plus d'informations

Plus d'informations sur les ports logiques Ethernet utilisés et sur les protocoles pour SIMOTION, voir le Manuel système Communication avec SIMOTION (https://support.industry.siemens.com/cs/de/en/view/109767623/fr), chapitre "Services utilisés".

### 7.3.1.2 Antivirus, correctifs de sécurité Windows SIMOTION P

#### Informations générales sur les logiciels antivirus

Dès qu'un PC industriel est connecté via un réseau interne de l'entreprise ou par liaison directe avec l'Internet, l'ordinateur court le risque d'être infecté par un virus. Cependant, les logiciels malveillants peuvent s'introduire dans les systèmes non seulement par Internet/Intranet, mais également via des supports de données amovibles tels que les clés USB connectées aux systèmes pour la sauvegarde des données.

### Logiciel antivirus SIMOTION P320

Un logiciel antivirus tournant sous un système d'exploitation Microsoft Windows, tel qu'on le trouve sur un grand nombre d'ordinateurs personnels ou de bureau, affecte profondément le fonctionnement du système. Il existe par exemple des processus tels que les analyses en temps réel ou les analyses de système périodiques. De telles opérations peuvent engendrer des pertes de performance du système, et ainsi du logiciel Runtime SIMOTION. Le logiciel Runtime SIMOTION s'exécute dans un environnement temps réel, mais il est toutefois dépendant des ressources système présentes.

**Remarque**

En raison de la baisse des performances, l'installation et l'utilisation d'un logiciel antivirus standard pendant le fonctionnement d'un système SIMOTION P320 ne sont pas autorisées.

### Utilisation d'un logiciel antivirus

Un logiciel antivirus standard ne pouvant être utilisé pour SIMOTION P320, une procédure alternative passe par l'installation du logiciel antivirus dans le système d'exploitation Windows PE amorçable séparément. Celui-ci est démarré à partir d'un CD ou d'une clé USB et exécute l'analyse des virus.

**Remarque**

**FAQ portail Service&Support**

Plus d'informations sur l'utilisation d'un logiciel antivirus sur une SIMOTION P320, voir la FAQ "Comment utiliser un logiciel antivirus sur une SIMOTION P3x0 ?" (https://support.industry.siemens.com/cs/ww/fr/view/59381507/en). Ce document peut être téléchargé sur le portail Service&Support.

## 7.3.2 Archivage sécurisé du projet

### Archivage des données de projet dans SIMOTION SCOUT

L'ensemble des données, des configurations et des programmes est archivé dans le projet. Dans un projet, seuls les programmes et les bibliothèques peuvent être archivés sous forme cryptée par le biais de la protection de savoir-faire. Pour protéger l'ensemble du projet, il convient de protéger les données de projet avec des solutions bureautiques courantes, p. ex. archives protégées par mot de passe ou disques durs cryptés.

### Structure de fichiers

Les données de projet de SIMOTION SCOUT peuvent exister dans les variantes suivantes.

**Données d'ingénierie (ES)**

- Archivage standard : structure de fichiers dans l'arborescence du projet
  Objets STEP 7/TIA Portal et SIMOTION SCOUT dans le répertoire du projet. Ils sont sans protection et peuvent être édités par chacun en l'absence de protection de savoir-faire pour les programmes et les bibliothèques ou de cryptage de fichiers externe. Dans ce contexte, on entend par programmes des unités pouvant contenir des programmes, des blocs fonctionnels et des fonctions.
- Données XML
  Données de projet générées par exportation/importation XML. La protection de savoir-faire reste appliquée.

**Données Runtime (RT) - données sur carte CF**

- Archive ZIP du projet SIMOTION (non binaire).
  L'archive du projet est stockée sur la carte mémoire de la commande SIMOTION correspondante (CFAST, carte CF, MMC). L'archive peut être transférée p. ex. par SIMOTION SCOUT ou par des voies standard (transfert FTP).
- Données binaires (comprimées, non comprimées)
  Les données binaires contiennent le projet exécutable compilé avec les configurations et les applications.
  Sans le projet SIMOTION SCOUT, il n'est pas possible d'effectuer des modifications au runtime, car le projet est stocké sur la commande SIMOTION sous forme de données binaires.

Le graphique suivant montre un exemple d'archivage possible des données du projet avec la représentation des données protégées.

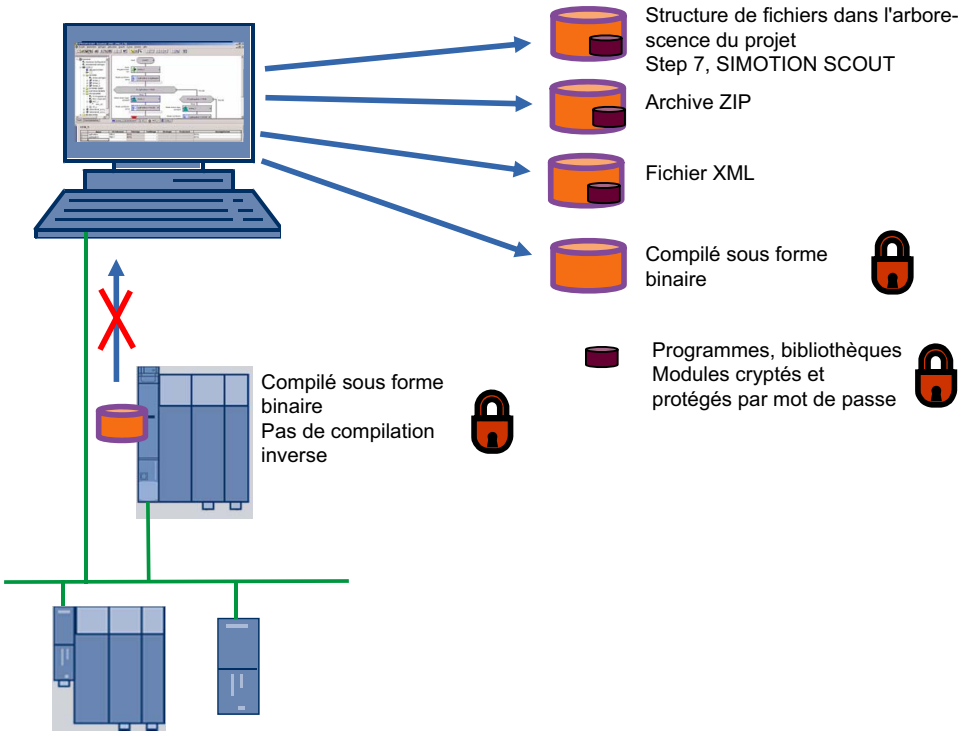



Figure 7-5 Archivage des données de projet dans SIMOTION SCOUT

## 7.3.3 Protection de savoir-faire

### 7.3.3.1 Contrôle d'accès sécurisé avec SIMATIC Logon

#### Gestion des utilisateurs et traçabilité

Le pack optionnel SIMATIC Logon sert à instaurer des droits d'accès pour les projets et les bibliothèques dans STEP 7. Ces projets ne sont alors accessibles qu'à un groupe de personnes autorisées. SIMATIC Logon est utilisable en combinaison avec SIMOTION SCOUT.

**SIMATIC Logon prend en charge les fonctions suivantes :**

- Affectation d'autorisations individuelles à des utilisateurs ou des groupes d'utilisateurs les autorisant à exécuter des actions précises (p. ex. lecture, écriture, transfert de blocs).
- Journalisation des activités en ligne et des procédures de connexion à l'ordinateur. Les accès au projet et les modifications du projet sont traçables.
- Affectation d'autorisations limitées dans le temps pour les utilisateurs/groupes d'utilisateurs.
- Politiques d'expiration de mot de passe

**Journal des modifications**

Les modifications peuvent être journalisées lorsque la protection d'accès est activée. Ce journal contient par exemple :

- l'activation
- la désactivation
- la configuration de la protection d'accès et du journal des modifications
- l'ouverture et la fermeture de projets et bibliothèques, y compris le chargement dans le système cible et les activités de modification de l'état de fonctionnement.

### 7.3.3.2 Protection de savoir-faire dans l'ingénierie

#### Types de protection de savoir-faire

La protection du savoir-faire dans SIMOTION SCOUT empêche la visualisation et la modification non autorisées de vos programmes. Plusieurs connexions (login) sont possibles. La connexion standard pour une session d'ingénierie est configurable.

Il existe deux types de protection du savoir-faire :

- Protection de savoir-faire des programmes et bibliothèques
- Protection du savoir-faire pour les groupes d'entraînement (à partir de SINAMICS V4.5)

Saisir un login et un mot de passe sous **Projet -> Protection de savoir-faire**. La commande de menu **Activer** permet alors d'activer la protection de savoir-faire pour le programme. Les programmes contenus dans le projet sont encore visibles pour l'utilisateur lors de cette session, mais les noms de programmes sont représentés avec un cadenas.

## Programmes et bibliothèques

La protection du savoir-faire est destinée à protéger les programmes et bibliothèques de votre projet. Lorsqu'elle est activée, la protection du savoir-faire évite l'affichage et la modification non autorisés de vos programmes. La protection du savoir-faire est activable pour des programmes individuels ou pour tous les programmes d'un projet.

Plusieurs niveaux de protection d'accès et de cryptage sont possibles pour les types d'objets suivants :

- Programmes (Units in Structured Text (ST), Motion Control Chart (MCC) et CONT/LOG contenant des programmes, des blocs fonctionnels et des fonctions)
- Diagrammes Drive Control Chart (DCC)
- Bibliothèques

**Pour le cryptage, il existe trois niveaux de sécurité au choix :**

- **Standard**
  Accès avec login utilisateur et mot de passe (rétrocompatible avec les versions antérieures à V4.2)
- **Moyen**
  Codage amélioré du mot de passe (nouveau procédé, pas de rétrocompatibilité sans connaissance du mot de passe).
  Les programmes et les bibliothèques peuvent être recompilés à tout moment, même sans connaissance du mot de passe.
- **Élevé** (uniquement pour sources ST dans les bibliothèques)
  Compilation possible uniquement après saisie du mot de passe.
  Des bibliothèques protégées peuvent aussi être utilisées sans connaissance du mot de passe après une exportation, car dans ce cas le résultat de la compilation est également exporté.
  - **Une exportation sans textes sources est possible en outre lors de l'exportation de bibliothèques**
    Protection maximale Suppression complète des textes sources dans l'ingénierie lors de l'exportation.
    L'exportation contient uniquement le résultat de la compilation (pas de nouvelle compilation possible).

Les interfaces de bloc sont toujours visibles.

## Entraînement dans SIMOTION SCOUT

La protection du savoir-faire pour les entraînements est uniquement valide en ligne et sert à protéger la propriété intellectuelle, en particulier le savoir-faire des constructeurs de machines contre toute utilisation ou reproduction illicite de leurs produits.

Pour une description détaillée, voir au chapitre Protection de savoir-faire (Page 90).

### 7.3.3.3 Protection contre la copie de la configuration sur le système de commande

#### Protection contre la copie de projets SIMOTION

Des mesures applicatives permettent de relier la configuration à la carte mémoire ou à la commande. Une duplication illicite de la configuration est ainsi empêchée.

Des fonctions système permettent d'interroger le numéro de série de la CPU, de la carte mémoire et des composants DRIVE-CLiQ dans l'application. Le constructeur de machines est ainsi à même de créer un bloc avec un algorithme de cryptage qui, pendant l'exécution, forme une clé à partir du numéro de série actuellement monté et le compare à une clé machine. Chaque configuration de machine possède sa propre clé machine générée par le constructeur et consignée dans l'application, mais qui peut également être saisie par le client final p. ex. sur un appareil IHM, notamment en cas de maintenance.

Dans le cadre d'accords spécifiques, il est également possible de réaliser une protection de savoir-faire et contre la copie étendue par un pack technologique SIMOTION OpenArchitecture.

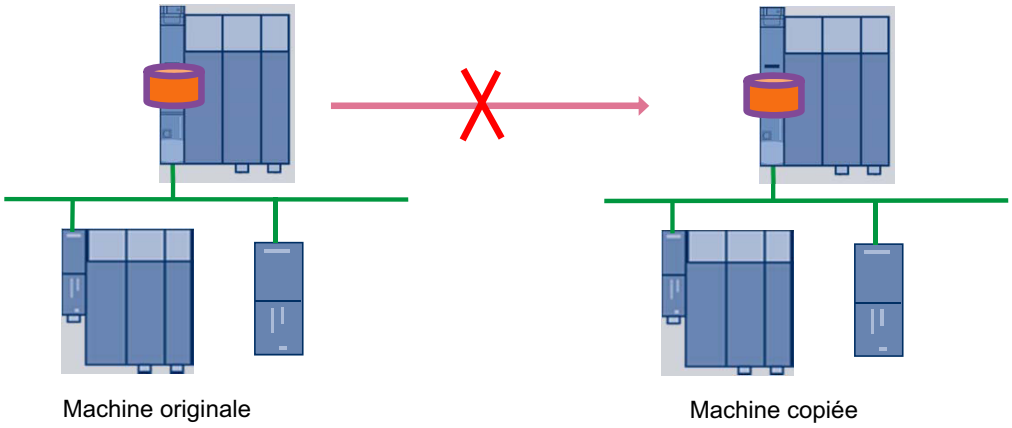



Figure 7-6 Protection contre la copie de projets SIMOTION SCOUT binaires

## 7.3.4 Comparaison hors ligne/en ligne

#### Comparaison de projets

La fonction SIMOTION SCOUT/STARTER **Comparaison de projet** (lancement avec le bouton **Lancer la comparaison d'objets**) permet de comparer des objets à l'intérieur d'un projet, ou à ceux d'autres projets (en ligne ou hors ligne).

La comparaison hors ligne/en ligne permet de détecter en détail les manipulations ultérieures des données du projet sur l'installation, par rapport aux données d'ingénierie sauvegardées. Des accès par des tiers sont ainsi détectés dans le système.

**Les comparaisons suivantes sont possibles :**

- Objet hors ligne avec objet hors ligne d'un même projet
- Objet hors ligne avec objet hors ligne d'un autre projet
- Objet hors ligne avec objet en ligne

La comparaison de projets dans SIMOTION SCOUT contient tous les objets d'un projet, tels que les appareils SIMOTION, groupes d'entraînements, bibliothèques, les programmes (Units), E/S, ainsi que la configuration du système d'exécution.

La comparaison hors ligne/en ligne fournit une aide en cas de maintenance ou pour la détection des modifications des données du projet.

Il se peut, par exemple, que des incohérences entre votre projet dans SIMOTION SCOUT et le projet qui est chargé dans le système cible soient signalées lors du passage en mode en ligne dans le navigateur de projet.

**Ces incohérences peuvent par exemple avoir les causes suivantes :**

- un programme a été modifié
- le résultat de compilation d'un programme est différent
- les variables d'appareil globales présentent des différences
- le système exécutif a été modifié
- la configuration matérielle a changé
- une bibliothèque a été modifiée
- une donnée de configuration d'un axe a été modifiée

La comparaison d'objets permet de déterminer les différences et d'effectuer un transfert de données le cas échéant pour éliminer les différences.

### Comparaison hors ligne/en ligne détaillée

Une comparaison de projets complète permet de déterminer de manière ciblée des différences entre le projet en ligne et le projet hors ligne. En cas de différences, il est possible de déterminer les modifications/manipulations du code source jusqu'au niveau de la ligne de code, dans la mesure où les données supplémentaires (informations source) ont été archivées dans le système cible lors du chargement. Ceci est possible aussi pour les langages de programmation CONT/LOG et MCC.

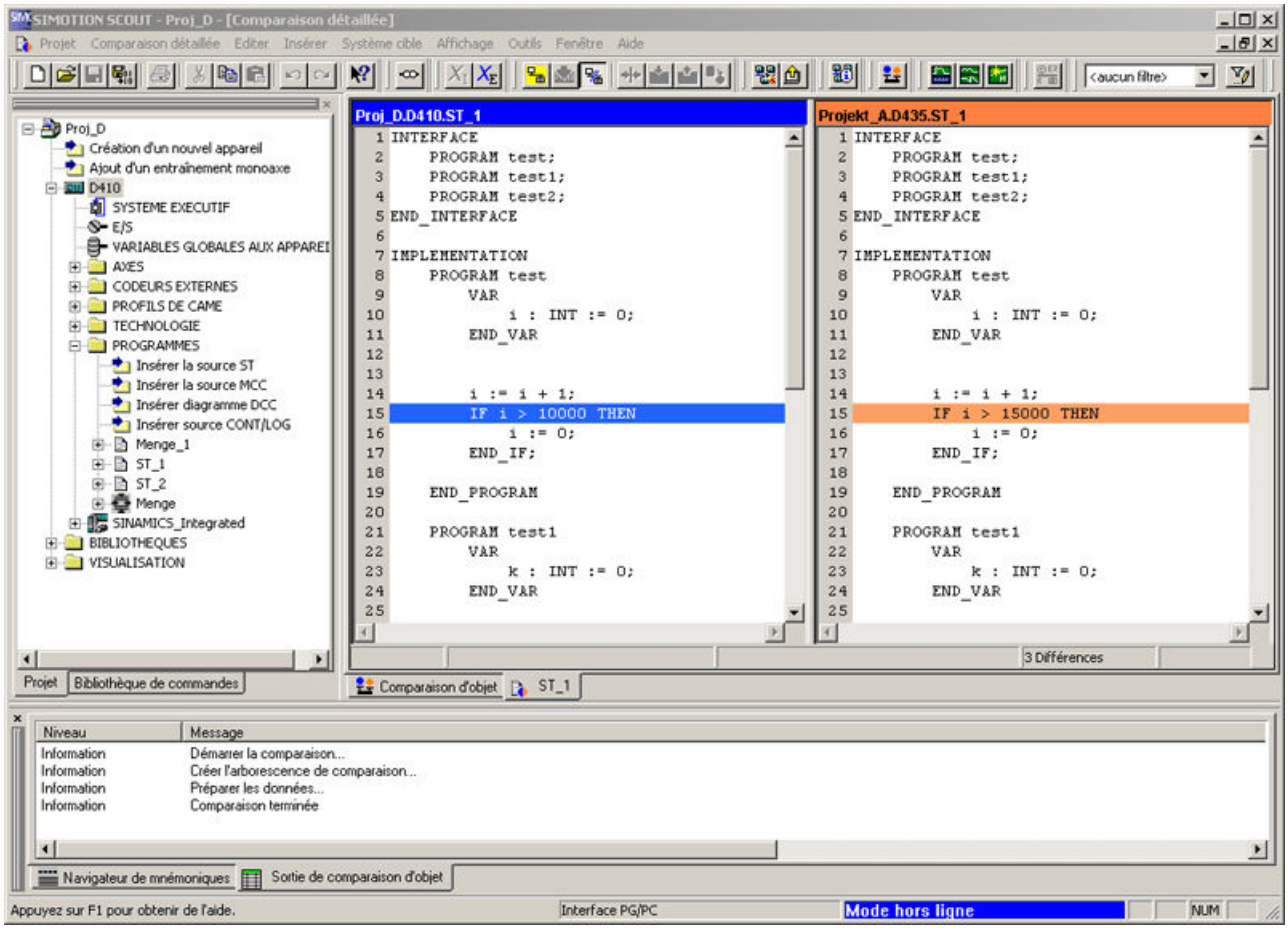



Figure 7-7 Exemple de comparaison détaillée ST

## 7.3.5 Serveur web SIMOTION IT

### Introduction

Les appareils SIMOTION possèdent des pages de diagnostic standard préconfigurées via un serveur web. Ces pages peuvent être affichées via Ethernet avec un navigateur courant. Par ailleurs, vous pouvez créer vos propres pages HTML avec des informations de maintenance et de diagnostic. Le serveur web peut être désactivé. Lorsque le serveur web est activé, le concept de sécurité intégré et la gestion des utilisateurs garantissent un fonctionnement sécurisé de l'installation.

## Désactivation/activation du serveur web

Le serveur web avec toutes les fonctions et services peut être activé ou désactivé dans le projet SIMOTION SCOUT ou SIMOTION SCOUT TIA, sous la configuration matérielle de la commande. Il est possible d'activer ou de désactiver des fonctions individuelles.

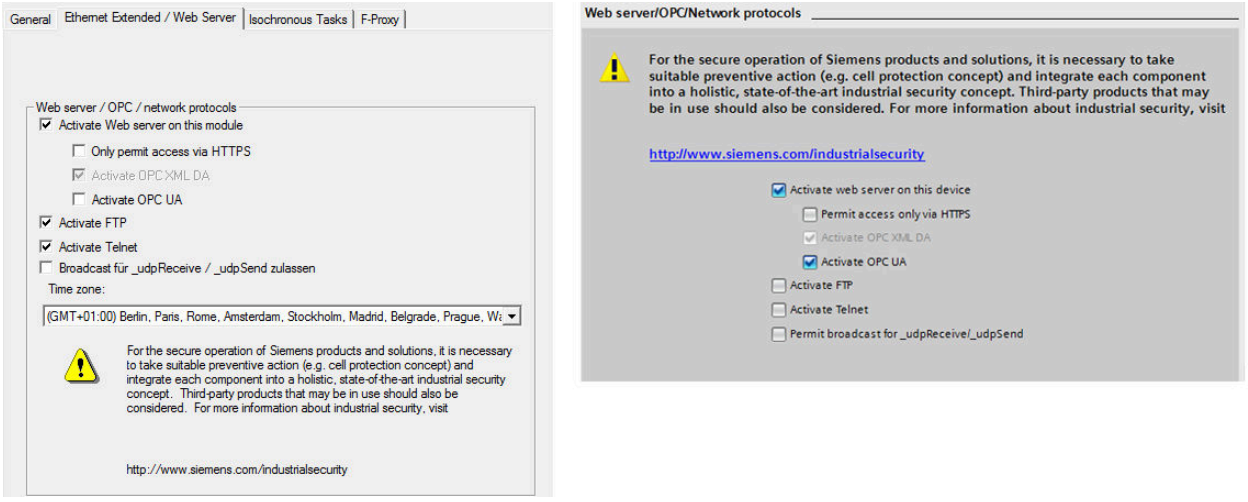



Figure 7-8 **Activation de fonctions serveur web SIMOTION IT dans SIMOTION SCOUT ou SIMOTION SCOUT TIA**

**Remarque**

Lors de l'activation du serveur web, il faut créer une gestion des utilisateurs avec un accès des utilisateurs protégé par mot de passe.

## Concept de sécurité des accès HTTP/S, FTP et Telnet au serveur web

À partir de la version V4.4, l'accès au serveur web SIMOTION IT est protégé par un concept de sécurité à plusieurs niveaux.

L'état de sécurité du serveur web est indiqué par le niveau de sécurité sur la page web. Ce niveau de sécurité peut prendre l'une des trois valeurs suivantes : Low, Normal, High

### Security Level Low

Dans l'état à la livraison, l'appareil contient une base de données des utilisateurs vide. Aucun projet n'est encore disponible. Le niveau de sécurité est faible pour permettre la configuration de l'appareil.

- Dans cet état, l'accès au serveur web est possible en tant qu'utilisateur anonyme, ce qui permet d'utiliser des fonctions telles que les mises à jour de projet et du firmware ou OPC XML.
- Les accès FTP et Telnet sont également ouverts.
- Il est possible de saisir de nouveaux utilisateurs dans la base de données des utilisateurs vide.

#### Security Level Normal

La commande comprend une base de données des utilisateurs. Un projet est disponible sur la commande et HTTP, HTTPS, FTP ainsi que Telnet sont activés dans la configuration matérielle.

- Une authentification avec un nom d'utilisateur et un mot de passe est nécessaire pour l'accès aux pages web intégrant des contenus sensibles (par exemple, mise à jour de firmware, table des surveillances, etc.), FTP et Telnet.

Dès qu'un projet est chargé dans la commande, le niveau de sécurité normal est actif, le cas échéant avec une base de données des utilisateurs vide. Les pages standard restent visibles. L'accès à toutes les autres pages web, qui exigent une authentification, n'est pas possible.

#### Security Level High

Sécurité élevée avec protection d'accès maximale :

- Les services HTTP, HTTPS, FTP et Telnet ont été désactivés dans la configuration matérielle par le projet. Un accès Ethernet par les ports respectifs des services n'est alors plus possible. Le serveur web ne peut pas être utilisé.

### Gestion des utilisateurs

SIMOTION IT utilise une base de données des utilisateurs pour sécuriser l'accès à un appareil. La base de données des utilisateurs contient les groupes avec les utilisateurs associés. Il est possible d'affecter aux groupes d'utilisateurs définis des droits d'accès aux différentes pages web du serveur web.  L'accès au serveur web s'effectue après l'authentification.

#### Authentification

- Il existe des utilisateurs (USER).
- Chaque utilisateur a un mot de passe. Ce dernier est crypté.
- Les utilisateurs appartiennent à des groupes (GROUP).
- En fonction des groupes, les pages Web, les répertoires et les applications sont protégés par des zones sécurisées.
- Seuls les utilisateurs faisant partie d'une zone sécurisée ont accès aux pages ainsi protégées.
- Chaque zone sécurisée est associée à un groupe d'utilisateurs autorisés à y accéder.
- Un utilisateur peut faire partie de différents groupes.

### Transmission cryptée des données

Les accès au serveur web sont possibles par HTTP ou par HTTPS. Le protocole SSL (Secure Socket Layer) dans HTTPS permet de réaliser une transmission cryptée des données entre un client (navigateur) et la commande SIMOTION (serveur web). Pour des raisons de sécurité, il est possible de forcer la transmission sécurisée en désactivant le port HTTP.

La variante de communication cryptée entre le navigateur et le serveur web via HTTPS présuppose la création et l'installation de certificats. Dans l'état à la livraison, un appareil contient un certificat racine standard et une clé privée pour le serveur Web sous la forme d'un

fichier. Ces fichiers doivent être remplacés par des fichiers personnalisés de manière à renforcer la sécurité de l'accès HTTPS à l'appareil.

#### Fichiers de clé

- État à la livraison
  Pour permettre d'accéder à la commande SIMOTION par HTTPS dans l'état à la livraison des pages standard de diagnostic SIMOTION IT, un certificat racine et une clé privée sont fournis sous la forme d'un fichier sur l'appareil.
- Créer son propre certificat SSL
  L'outil Perl et le script Perl fourni (cert.pl) permettent de générer et de concaténer en packs de chargement les certificats requis pour les installations client (sites).

Il existe deux possibilités pour obtenir son propre certificat de serveur (certificat SSL) :

- Génération d'un certificat racine (auto-signé) et d'une clé privée au moyen d'un logiciel dédié.
- Achat d'un certificat de serveur auprès d'une autorité de certification (Certificate Authority).

#### Importation d'un certificat SSL dans le navigateur

Si vous utilisez le protocole SSL avec votre propre autorité de certification, vous devez préparer vos PC afin qu'ils communiquent avec la commande SIMOTION. Pour cela, vous devez enregistrer le certificat racine dans la liste des certificats de votre navigateur.

### Plus d'informations

Plus d'informations sur le serveur web SIMOTION IT, voir les documents suivants :

- Manuel de diagnostic SIMOTION IT Diagnostic et configuration (https://support.industry.siemens.com/cs/de/de/view/109767636/fr)
- Manuel de programmation SIMOTION IT OPC UA (https://support.industry.siemens.com/cs/de/en/view/109767638/fr)
- AUTOHOTSPOT
- Manuel de programmation SIMOTION IT Machine virtuelle et servlets (https://support.industry.siemens.com/cs/de/en/view/109767639/fr)

### Voir aussi

Manuel de programmation SIMOTION IT Programmation et services Web (https://support.industry.siemens.com/cs/de/en/view/109767637/fr)

## 7.3.6 Serveur OPC UA

### Introduction

SIMOTION a implémenté un serveur OPC UA avec DA (Data Access).

Le codage binaire OPC UA est pris en charge. L'accès à un client OPC UA quelconque peut être protégé par une authentification et une transmission de données cryptée.

## Configuration

**Remarque**

Avant la connexion au serveur OPC UA, veiller à un environnement sécurisé et installer une couche intermédiaire sur base matérielle (p. ex. réseau DMZ, pare-feu, modules SCALANCE S, etc.).

Le serveur OPC UA peut être activé ou désactivé avec HW-Config dans TIA Portal ou Step 7.

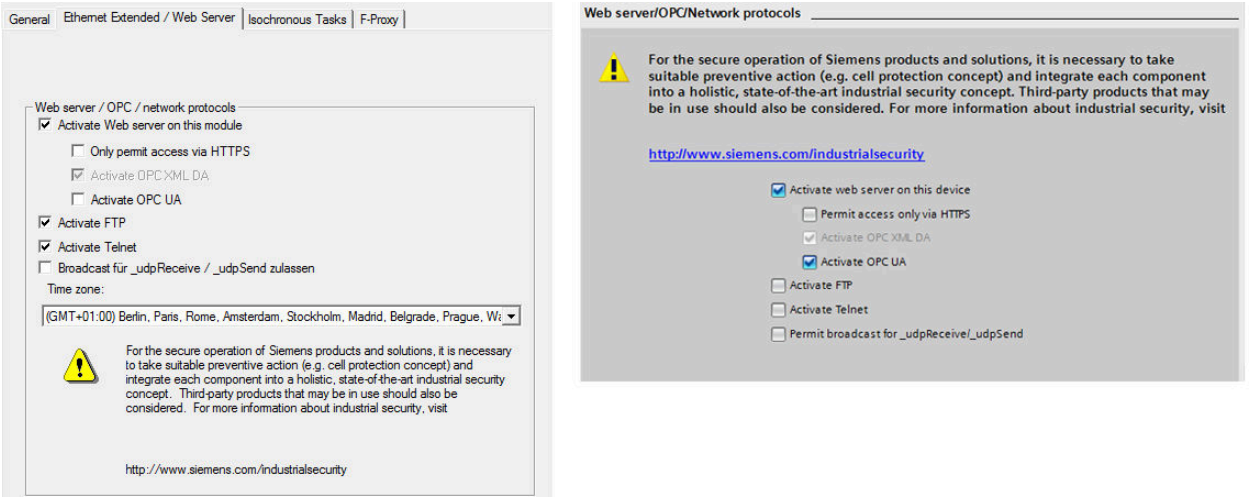



Figure 7-9 Activation de fonctions serveur web SIMOTION IT dans SIMOTION SCOUT ou SIMOTION SCOUT TIA

Des réglages supplémentaires sont possibles dans les masques de configuration du serveur web SIMOTION IT :

- Validation de l'interface Ethernet et du port correspondant de SIMOTION pour l'accès OPC UA.
- Définition du nom d'utilisateur, du mot de passe et du groupe d'utilisateurs dans le cadre de la gestion des utilisateurs du serveur web SIMOTION IT.
- Utilisation des certificats pour la transmission de données cryptées.

## Plus d'informations

Plus d'informations sur le serveur OPC-UA, voir le Manuel de programmation SIMOTION IT OPC UA (https://support.industry.siemens.com/cs/de/en/view/109767638/fr).

## 7.3.7 Élimination

| IMPORTANT |
| --- |
| **Utilisation abusive des données**<br>Une élimination non sûre des supports de mémoire (carte CF/CFast/SSD) peut être à l'origine d'une utilisation abusive des données de programmes pièce, d'archive, etc. par des tiers.<br>• Veiller par conséquent à effacer de manière sûre les supports de mémoire utilisés avant l'élimination du produit.<br>Utiliser pour cela des programmes permettant de vider/formater le support de mémoire de manière sûre. |

# 7.4 SINAMICS

Le chapitre suivant fournit une vue d'ensemble des mesures de sécurité industrielle pour SINAMICS à prendre pour protéger un variateur contre les menaces. Il traite également de questions pour lesquelles il convient de tenir particulièrement compte de la sécurité industrielle :

- Protection en écriture et protection de savoir-faire
- Paramètres : niveaux d'accès
- Manipulation de la carte mémoire
- Remarque relative à Safety Integrated
- Services de communication et numéros de port utilisés
- Serveur web
- Remarques concernant des interfaces
- SINAMICS Startdrive et STARTER
- SINAMICS Drive Control Chart (DCC)

Des descriptions et procédures détaillées sont fournies dans la documentation SINAMICS correspondante indiquée.

De nombreux produits (SINUMERIK, SIMOTION, SINAMICS) contiennent OpenSSL. Pour ces produits :

- Ce produit comprend un logiciel (https://www.openssl.org/) développé par le projet OpenSSL pour une utilisation dans la boîte à outils OpenSSL.
- Ce produit comprend un logiciel (mailto:eay@cryptsoft.com) cryptographique créé par Eric Young.
- Ce produit comprend un logiciel (mailto:eay@cryptsoft.com) développé par Eric Young.

## 7.4.1 Sécurité des réseaux

**Remarque**

Les produits SINAMICS ne doivent être utilisés que dans un réseau sécurisé et digne de confiance. Pour cela, respecter les indications du chapitre "Segmentation des réseaux (Page 32)".

## 7.4.2 Protection de savoir-faire

Certains variateurs SINAMICS offrent la fonction "protection de savoir-faire" : la protection du savoir-faire sert à protéger la propriété intellectuelle, en particulier le savoir-faire des constructeurs de machines contre toute utilisation ou reproduction illicite de leurs produits.

### Effet

Les paramètres de réglage qui ne sont pas compris dans une liste d'exception ne sont accessibles ni en lecture, ni en écriture.

### Exceptions

- La protection de savoir-faire ne s'applique pas aux paramètres dotés des attributs suivants :
  - KHP_WRITE_NO_LOCK
    - Ces paramètres sont exclus de la protection de savoir-faire et peuvent donc être écrits malgré la protection de savoir-faire.
    - Une liste de ces paramètres se trouve dans les Tables de paramètres du produit correspondant.
    - Ces paramètres ne sont pas compris dans la liste d'exceptions.
  - KHP_ACTIVE_READ
    - Ces paramètres sont accessibles en lecture même lorsque la protection en écriture est activée, mais ne sont pas accessibles en écriture.
    - Une liste de ces paramètres se trouve dans les Tables de paramètres du produit correspondant.
    - Ces paramètres ne sont pas compris dans la liste d'exceptions.
- La protection de savoir-faire n'empêche pas l'exécution de certaines fonctions :
  - Entre autres, la fonction "Restaurer les réglages d'usine" est exécutable malgré la protection de savoir-faire.
  - Une liste exhaustive des fonctions exécutables est fournie dans les documents indiqués ci-après.

### Plus d'informations

Plus d'informations à ce sujet, voir les documents suivants :

- SINAMICS S120 Description fonctionnelle Fonctions d'entraînement (https://support.industry.siemens.com/cs/de/en/view/109763287/fr)
  Chapitre "Protection de savoir-faire"
- Instructions de service SINAMICS G110M (https://support.industry.siemens.com/cs/de/en/view/109757594/fr)
  Chapitre "Protection de savoir-faire"
- Instructions de service SINAMICS G120
  Chapitre "Protection de savoir-faire"
- SINAMICS S et SINAMICS G Tables de paramètres
  Chapitre "Paramètres pour la protection en écriture et la protection de savoir-faire"
- Instructions de service SINAMICS G130, G150 et S150
  Chapitre "Protection de savoir-faire"

### 7.4.3 Paramètres : niveaux d'accès et mot de passe

Pour les appareils des séries G110M, G120, G130, G150, S110, S120 et S150, les paramètres SINAMICS sont classés dans les niveaux d'accès 0 à 4. Les niveaux d'accès permettent de définir quel utilisateur ou quel appareil d'entrées/sorties est autorisé à traiter les différents paramètres :

- Le paramètre p0003 définit p. ex. quels niveaux d'accès sont sélectionnables avec le BOP ou l'IOP.
- Les paramètres du niveau d'accès 4 sont protégés par un mot de passe jusqu'à SINAMICS RT V4.9 et uniquement visibles pour les experts.

Le niveau d'accès dans lequel le paramètre peut être affiché et modifié est indiqué dans SINAMICS S et SINAMICS G Tables de paramètres.

#### Plus d'informations

Pour plus d'informations à ce sujet, voir les documents suivants :

- SINAMICS S120 Description fonctionnelle Fonctions d'entraînement (https://support.industry.siemens.com/cs/de/en/view/109771805/fr)
  Chapitre "Paramètres"
- Description fonctionnelle SINAMICS S120 Safety Integrated (https://support.industry.siemens.com/cs/de/en/view/109771806/fr)
  Chapitre "Utilisation du mot de passe Safety"
- SINAMICS G110M Tables de paramètres
  Chapitre "Vue d'ensemble des paramètres"
- SINAMICS G120 Instructions de service
  Chapitre "Paramètres"
- SINAMICS S et SINAMICS G Tables de paramètres
  Chapitre "Explications au sujet de la table de paramètres"
- Instructions de service SINAMICS G130, G150 et S150
  Chapitre "Paramètres"

### 7.4.4 Manipulation de la carte mémoire

Pour tous les appareils SINAMICS disposant d'une carte mémoire, il convient de prendre des précautions particulières lors de la manipulation de la carte mémoire afin d'éviter que des logiciels malveillants ou des paramétrages incorrects ne soient introduits sur les différents PC de mise en service ou variateurs.

**⚠ ATTENTION**

**Danger de mort en raison de logiciels manipulés lors de l'utilisation de supports de mémoire amovibles**

L'archivage de fichiers sur des supports de mémoire amovibles présente un risque élevé d'infection des PC de mise en service, p. ex. par des virus ou des logiciels malveillants. Un paramétrage incorrect peut entraîner des dysfonctionnements sur les machines, susceptibles de provoquer des blessures, voire la mort.

- Protéger les fichiers du support de mémoire amovible contre les logiciels malveillants par les mesures de protection appropriées, p. ex. un logiciel antivirus.

**⚠ ATTENTION**

**Danger de mort en raison de logiciels manipulés lors de l'utilisation de supports de mémoire amovibles**

L'enregistrement du paramétrage (paramétrage Safety Integrated inclus) sur des supports de mémoire comporte un risque d'écraser le paramétrage d'origine (avec Safety Integrated) p. ex. avec la carte mémoire d'un autre entraînement sans Safety Integrated. Un paramétrage incorrect peut entraîner des dysfonctionnements sur les machines, susceptibles de provoquer des blessures, voire la mort.

- S'assurer d'utiliser la seule la carte mémoire appartenant au variateur considéré.
- S'assurer que l'accès aux boîtiers, aux armoires ou aux locaux de service électriques n'est possible que pour du personnel qualifié ou autorisé.

### 7.4.5 Safety Integrated

Afin de réellement réduire le risque pour les machines et les installations grâce à la mise en œuvre de fonctions Safety Integrated, l'utilisation des fonctions Safety Integrated exige une attention particulière, pour tous les appareils SINAMICS disposant de ces fonctions.

**⚠ DANGER**

**Mouvement de machine intempestif dû à des fonctions de sécurité inactives**

Des fonctions de sécurité inactives ou non adaptées peuvent déclencher des mouvements intempestifs des machines qui risquent de causer des blessures graves ou la mort.

- Tenir compte, avant la mise en service, des informations contenues dans la documentation produit correspondante.
- Effectuer, pour les fonctions conditionnant la sécurité, une évaluation de la sécurité de l'ensemble du système, y compris de tous les constituants de sécurité.
- S'assurer par un paramétrage adéquat que les fonctions de sécurité sont adaptées aux tâches d'entraînement et d'automatisation et qu'elles sont activées.
- Effectuer un test des fonctions.
- N'exploiter l'installation en production qu'après s'être assuré de l'exécution correcte des fonctions conditionnant la sécurité.

**Remarque**

**Importantes consignes de sécurité relatives aux fonctions Safety Integrated**

Lorsque les fonctions Safety Integrated sont utilisées, il convient de tenir compte des consignes de sécurité indiquées dans les manuels Safety Integrated.

### 7.4.6 Services de communication et numéros de port utilisés

Les variateurs SINAMICS prennent en charge certains protocoles de communication. Les paramètres d'adresse, la couche de communication appropriée ainsi que le rôle et le sens de communication sont décisifs pour chaque protocole. Ces informations permettent d'adapter les mesures de sécurité requises pour la protection du système d'automatisation aux protocoles utilisés (p. ex. pare-feu). Les mesures de sécurité décrites ici se limitent aux réseaux Ethernet et PROFINET.

Pour plus d'informations à ce sujet, voir les documents suivants :

- SINAMICS S120
  - À partir de la version 5.2 du firmware
    SINAMICS S120 Description fonctionnelle Communication (https://support.industry.siemens.com/cs/ww/fr/view/109771803)
  - Versions de firmware antérieures
    SINAMICS S120 Description fonctionnelle Fonctions d'entraînement (https://support.industry.siemens.com/cs/de/en/view/109771805/fr)
  - Respectivement : chapitre "Services de communication et numéros de port utilisés"
- SINAMICS G Description fonctionnelle Bus de terrain (https://support.industry.siemens.com/cs/ww/de/view/109757336/en)
  Chapitre "Protocoles Ethernet et PROFINET utilisés"
- Instructions de service SINAMICS G130, G150 et S150
  chapitre "Services de communication et numéros de port utilisés"

## 7.4.7 Serveur web intégré

Le serveur web SINAMICS fournit des informations sur un appareil SINAMICS par l'intermédiaire de ses pages web. L'accès s'effectue via un navigateur Internet.

### Transmission de données

Outre la transmission (HTTP) normale (non sécurisée), le serveur web prend aussi en charge la transmission sécurisée (HTTPS). Le réglage recommandé est la transmission sécurisée (HTTPS).

**Remarque**

**Smart Access Module**

Le serveur web du Smart Access Module ne prend pas en charge la transmission sécurisée (HTTPS). À titre d'alternative, il est possible d'utiliser une transmission WLAN cryptée.

En indiquant "HTTP://" ou "HTTPS://" devant l'adresse de l'entraînement, vous pouvez décider vous-même d'accéder aux données par une transmission normale ou sécurisée.

Pour des raisons de sécurité, il est possible de forcer la transmission sécurisée en désactivant le port http.

### Droits d'accès

Les mécanismes normaux de protection de SINAMICS, y compris la protection par mot de passe, s'appliquent également à l'accès via le serveur web. D'autres mécanismes de protection ont été implémentés spécialement pour le serveur web. Selon la fonction, différentes options d'accès sont définies pour différents utilisateurs. Les listes de paramètres sont protégées de manière à ce que là aussi seuls les utilisateurs ayant les droits correspondants puissent accéder aux données ou les modifier.

### Plus d'informations

Pour plus d'informations à ce sujet (p. ex. les navigateurs Internet pris en charge), voir les documents suivants :

- SINAMICS S120 Description fonctionnelle Fonctions d'entraînement (https://support.industry.siemens.com/cs/de/en/view/109763287/fr)
  Chapitre "Serveur web"
- Instructions de service SINAMICS S210 (https://support.industry.siemens.com/cs/ww/fr/view/109771824)
- Instructions de service SINAMICS V20 (https://support.industry.siemens.com/cs/de/de/view/109768394/fr)
- SINAMICS G120 Instructions de service Smart Access (https://support.industry.siemens.com/cs/ww/fr/view/109771299)
- Instructions de service SINAMICS G130, G150 et S150

## 7.4.7.1 Certificats pour la transmission sécurisée des données

### Sécurisation de l'accès HTTPS

Le protocole "Transport Layer Security" (TLS) garantit une transmission cryptée des données entre un client et l'entraînement SINAMICS. Les accès du navigateur à l'entraînement via HTTPS sont basés sur le protocole "Transport Layer Security".

La variante de communication cryptée entre le navigateur et le serveur web via HTTPS présuppose la création et l'installation de certificats (configuration par défaut, propres certificats ou certificat de serveur d'une autorité de certification).

### TLS

Transport Layer Security (TLS V1.2 ou "sécurité de la couche transport ") est un protocole de cryptage hybride pour la transmission de données sécurisée sur Internet.

### Fichiers de clé

Pour le procédé de cryptage à la base du protocole Transport Layer Security, 2 fichiers de clé sont nécessaires (un certificat public et une clé privée).

#### Traitement de certificats

Pour permettre d'accéder à l'entraînement SINAMICS via HTTPS dans l'état dans lequel ce dernier est livré, le certificat standard et la clé nécessaires sont générés sur l'entraînement. Par conséquent, le certificat de firmware doit uniquement être utilisé sur les réseaux sécurisés (p. ex. PROFINET au-dessous d'un AP) ou pour les liaisons point à point directes à l'interface de maintenance X127.

Il convient d'utiliser un certificat validé par une autorité de certification externe à la place. Pour plus d'informations sur la procédure, voir les documents mentionnés ci-après.

### Plus d'informations

Pour plus d'informations à ce sujet, voir les documents suivants :

- SINAMICS S120 Description fonctionnelle Fonctions d'entraînement (https://support.industry.siemens.com/cs/de/en/view/109771805/fr)
  Chapitre "Certificats pour la transmission sécurisée des données"
- Instructions de service SINAMICS G130, G150 et S150

## 7.4.8 Remarques concernant des interfaces

### X127 LAN (Ethernet)

L'interface Ethernet X127 est prévue pour la mise en service et le diagnostic et doit par conséquent être toujours accessible. Tenir compte des restrictions suivantes pour l'interface X127 :

- Seul un accès local est autorisé
- Aucune mise en réseau n'est autorisée, à l'exception d'une mise en réseau locale dans l'armoire électrique fermée

Si un accès à distance à l'armoire électrique est nécessaire, des mesures de sécurité supplémentaires doivent alors être prises pour exclure tout emploi abusif du fait d'un sabotage ou d'une manipulation non qualifiée des données et toute interception de données confidentielles.

### Interface série X140 (RS232)

Via l'interface série X140, il est possible de raccorder un pupitre opérateur externe pour la commande ou le paramétrage.

| IMPORTANT |
| --- |
| **Accès aux variateurs réservé au personnel autorisé**<br>Les lacunes dans la sécurité physique d'une entreprise permettent aux personnes non autorisées d'endommager ou de modifier les installations de production, et également de causer, le cas échéant, la perte ou la modification d'informations confidentielles. Pour éviter cela, il convient de protéger en conséquence le site de l'entreprise et les zones de production.<br>• Pour les consignes relatives aux mesures de protection appropriées, voir le chapitre "Protection physique des zones de production critiques (Page 30)". |

### X150 LAN (Ethernet)

Le réseau auquel l'interface X150 est reliée doit être séparé du reste du réseau de l'installation selon le concept de défense en profondeur (voir le chapitre "Mesures générales de sécurité (Page 27)"). L'accès aux câbles et aux éventuelles connexions ouvertes doit se faire de manière protégée comme dans une armoire électrique.

### X1400 LAN (Ethernet)

Le réseau auquel l'interface X1400 est reliée doit être séparé du reste du réseau de l'installation selon le concept de défense en profondeur (voir le chapitre "Mesures générales de sécurité (Page 27)"). L'accès aux câbles et aux éventuelles connexions ouvertes doit se faire de manière protégée comme dans une armoire électrique.

### Plus d'informations

Pour plus d'informations à ce sujet, voir les documents suivants :

- SINAMICS S120
  - Manuel de l'appareil SINAMICS S120 Control Units et composants systèmes complémentaires (https://support.industry.siemens.com/cs/de/en/view/109763286/fr) Chapitres relatifs aux interfaces
  - À partir de la version 5.2 du firmware : Description fonctionnelle SINAMICS S120 Communication (https://support.industry.siemens.com/cs/ww/fr/view/109771803)
  - Versions de firmware antérieures : Description fonctionnelle SINAMICS S120 Fonctions d'entraînement (https://support.industry.siemens.com/cs/de/en/view/109763287/fr)
- SINAMICS G et SINAMICS S Instructions de service
- Instructions de service SINAMICS V90

## 7.4.9 Élimination

| IMPORTANT |
| --- |
| **Utilisation abusive des données due à une élimination non sûre du produit**<br>Une élimination non sûre du produit peut être à l'origine d'une utilisation abusive des données de paramétrage par des tiers.<br>• Réinitialiser par conséquent tous les paramètres au réglage d'usine sur tous les produits avant leur élimination.<br>Pour plus d'informations sur la restauration des réglages d'usine, voir la description fonctionnelle ou les instructions de service du produit concerné. |

| IMPORTANT |
| --- |
| **Utilisation abusive des données due à une élimination non sûre de la carte mémoire**<br>Une élimination non sûre de la carte mémoire peut être à l'origine d'une utilisation abusive des données, etc. par des tiers. La carte mémoire héberge entre autres les sauvegardes de données nécessaires au fonctionnement du variateur.<br>• Veiller par conséquent à effacer de manière sûre la carte mémoire avant l'élimination du produit. Il existe des programmes permettant de vider/formater la carte mémoire de manière sûre.<br>• Ceci concerne tous les produits équipés d'une carte mémoire. |

**Remarque**

**Supprimer les certificats définis par l'utilisateur**

Veiller à ce que tous les certificats définis par l'utilisateur soient supprimés de manière sûre avant l'élimination d'un produit SINAMICS. Les certificats de l'utilisateur peuvent permettre à un cybercriminel d'accéder à la transmission de données sécurisée.

- Produits avec carte mémoire
  - Supprimer les fichiers SINAMICS.key et SINAMICS.crt du répertoire OEM\SINAMICS \WEB\WEBCONF\CERT sur la carte mémoire.
- Produits avec carte mémoire optionnelle (p. ex. SINAMICS S210)
  - Générer des fichiers vides ("SINAMICS.key" et "SINAMICS.crt") avec les noms correspondants.
  - Copier ces fichiers sur la carte mémoire.
  - Insérer la carte mémoire dans le variateur.
  - Redémarrer le variateur.
  - À titre d'alternative, si aucune donnée de la carte mémoire n'est plus nécessaire : reformater la carte mémoire.

Plus d'informations, voir la description fonctionnelle ou les instructions de service du produit concerné.

## 7.4.10 SINAMICS Startdrive et STARTER

### 7.4.10.1 Danger de mort lié à des dysfonctionnements de la machine suite à un paramétrage incorrect ou modifié

**⚠ ATTENTION**

**Danger de mort lié à des dysfonctionnements de la machine suite à un paramétrage incorrect ou modifié**

Un paramétrage incorrect ou modifié peut entraîner des dysfonctionnements sur les machines, susceptibles de provoquer des blessures, voire la mort.

- Protéger les paramètres contre l'accès non autorisé.
- Prendre les mesures appropriées pour remédier aux dysfonctionnements éventuels (p. ex. un arrêt ou une coupure d'urgence).

### 7.4.10.2 SINAMICS Startdrive

#### Startdrive dans TIA Portal

SINAMICS Startdrive est un pack optionnel de TIA Portal permettant la mise en service des entraînements SINAMICS. En ce qui concerne Industrial Security, il convient de tenir compte des prescriptions pour les entraînements SINAMICS et pour TIA Portal.

En plus de la mise en service d'entraînements individuels, Startdrive permet de configurer des entraînements connectés à des automates SIMATIC tels que S7-1500. Pour plus d'informations sur l'utilisation des automates SIMATIC, voir l'aide en ligne de TIA Portal sous "Configuration de réseaux".

#### Ordinateur de mise en service

Veiller à la sécurité de l'ordinateur de mise en service. Respecter pour cela les Mesures de sécurité (Page 27) générales.

#### Protection de savoir-faire des appareils

- La fonction de "Protection de savoir-faire" permet de protéger le paramétrage de l'entraînement contre les accès non autorisés.
- Cette fonction est seulement disponible en ligne.
- La protection de savoir-faire des appareils est prise en charge à partir de Startdrive V16.

### Fonctions de sécurité

- Activation/désactivation de fonctions non utilisées (serveur web, ports)
- Protection d'écriture pour le paramétrage (la lecture des paramètres p est possible, mais pas l'écriture), assurant la protection contre les modifications involontaires du paramétrage (uniquement disponible en ligne).

### Protection des fichiers de sauvegarde dans le système de fichiers Windows

Les fichiers de sauvegarde de diagrammes ou de projets générés avec les outils de Windows doivent également être protégés contre les accès non autorisés à l'aide d'outils Windows, au moyen de mots de passe sûrs. Le projet Startdrive est lui-même protégé contre les atteintes à l'intégré.

### Scripting (Openness)

Les scripts (Openness) servent à l'automatisation de séquences dans Startdrive. Ces scripts doivent être testés avant leur utilisation sur la machine.

**⚠ ATTENTION**

**Danger dû à des configurations incorrectes d'opérations automatisées**

Le scripting permet d'automatiser considérablement les opérations manuelles dans l'outil Startdrive et de réduire le temps nécessaire à la configuration répétée des projets et des tâches.

Les auteurs et les utilisateurs de scripts sont responsables des opérations qui sont automatisées dans le scripting.

Les erreurs de configuration qui ne sont pas détectées par des tests peuvent provoquer des blessures graves, voire mortelles.

- Les nouveaux scripts et les scripts modifiés doivent toujours être testés pour être vérifiés et validés.
- Avant d'exécuter un script, vérifier que son contenu est correct. Vérifier et valider les résultats de l'exécution du script en effectuant des tests sur la machine.

Les scripts, de même que les diagrammes DCC peuvent être protégés par la protection de savoir-faire.

## 7.4.10.3 SINAMICS STARTER

### Mise en service d'entraînements avec STARTER

STARTER permet la mise en service d'entraînements des familles MICROMASTER et SINAMICS. SIMOTION SCOUT intègre une version de STARTER. Pour plus d'informations sur SIMOTION SCOUT, voir "SIMOTION (Page 75)".

### Ordinateur de mise en service

Veiller à la sécurité de l'ordinateur de mise en service. Respecter pour cela les Mesures de sécurité (Page 27) générales.

### Protection des fichiers de sauvegarde dans le système de fichiers Windows

Les fichiers de sauvegarde de diagrammes ou de projets générés avec les outils de Windows doivent également être protégés contre les accès non autorisés à l'aide d'outils Windows, au moyen de mots de passe sûrs.

### Fonctions de sécurité

- Protection de savoir-faire pour le paramétrage, les scripts, les diagrammes DCC et les bibliothèques DCC avec mot de passe et cryptage
- Protection contre la copie de la configuration sur l'entraînement. Le projet peut être ouvert uniquement avec la carte d'origine.
- Détection de manipulations de paramètres avec STARTER grâce à la comparaison de projets, voir aussi "Comparaison hors ligne/en ligne (Page 82)"
- Activation/désactivation de fonctions non utilisées (serveur web, ports), voir aussi "Serveur web intégré (Page 95)"
- Protection d'écriture pour le paramétrage (la lecture des paramètres p est possible mais pas l'écriture), assurant la protection contre les modifications involontaires du paramétrage (uniquement disponible en ligne).

### Protection de savoir-faire pour entraînements

En plus de la protection de savoir-faire pour les diagrammes DCC, les bibliothèques DCC et les scripts, la fonction de "Protection de savoir-faire" de l'entraînement permet de protéger le paramétrage de l'entraînement contre les accès non autorisés. Cette fonction est seulement disponible en ligne. Voir aussi "Protection de savoir-faire (Page 90)".

### Scripting

Les scripts servent à l'automatisation de séquences dans STARTER. Ces scripts doivent être testés avant leur utilisation sur la machine.

**⚠ ATTENTION**

**Danger dû à des configurations incorrectes d'opérations automatisées**

Le scripting permet d'automatiser considérablement les opérations manuelles dans les outils STARTER/SCOUT et de réduire le temps nécessaire à la configuration répétée des projets et des tâches.

Les auteurs et les utilisateurs de scripts sont responsables des opérations qui sont automatisées dans le scripting.

Les erreurs de configuration qui ne sont pas détectées par des tests peuvent provoquer des blessures graves, voire mortelles.

- Les nouveaux scripts et les scripts modifiés doivent toujours être testés pour être vérifiés et validés.
- Avant d'exécuter un script, vérifier que son contenu est correct. Vérifier et valider les résultats de l'exécution du script en effectuant des tests sur la machine.

Les scripts, de même que les diagrammes DCC peuvent être protégés par la protection de savoir-faire.

## 7.4.11 SINAMICS Drive Control Chart (DCC)

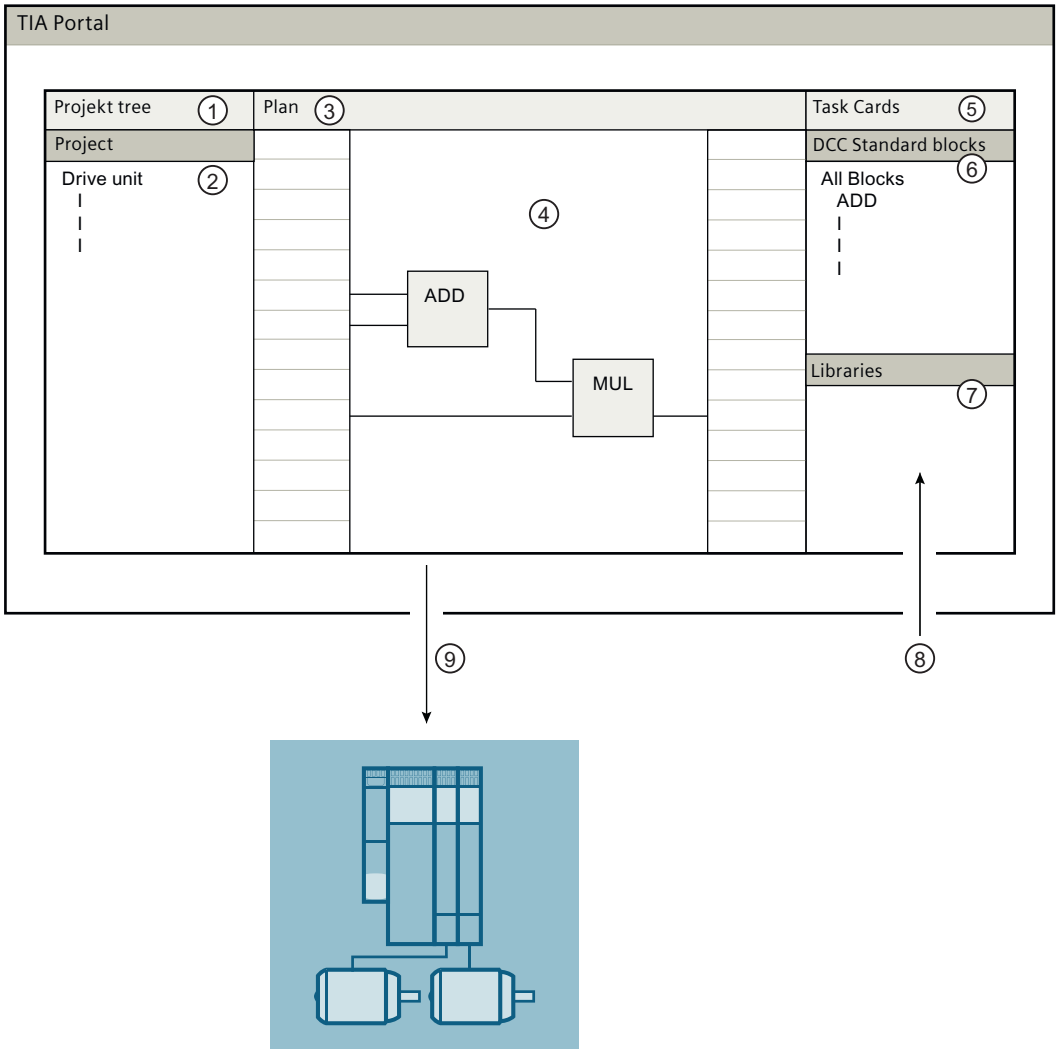
### 7.4.11.1 Industrial Security avec SINAMICS DCC

### Vue d'ensemble

SINAMICS Drive Control Chart (DCC) offre une option technologique modulaire et échelonnable qui a été développée principalement pour les tâches continues de régulation et de commande à proximité des entraînements.

L'éditeur de Drive Control Chart, basé sur CFC, permet de configurer graphiquement les fonctions technologiques avec DCC pour entraînements SINAMICS.

- Startdrive
  La figure suivante illustre le flux des données de configuration dans le cadre de la configuration avec SINAMICS DCC :




① Chargement
② Importation de bibliothèques DCB

Figure 7-10 Flux des données de configuration : TIA-DCC

- STARTER
  La figure suivante illustre le flux des données de configuration dans le cadre de la configuration avec SINAMICS DCC et les possibilités de protection des sources DCC configurées/programmées :

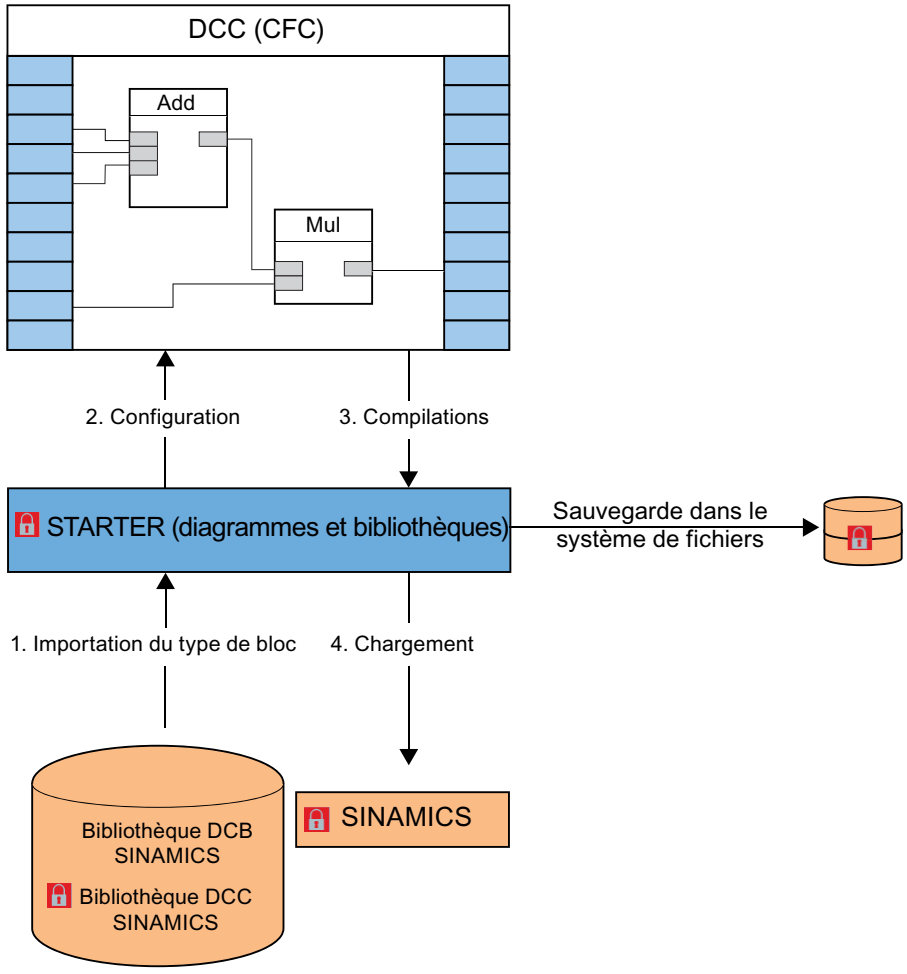



Figure 7-11 Flux des données de configuration : Exemple pour DCC Classic V2.1 ... V3.4 (STARTER)

## Startdrive : Package optionnel DCC

Tenir compte des particularités suivantes pour Startdrive :

- DCC n'offre pas de sauvegarde dans le système de fichiers.
- Les bibliothèques DCB utilisées sont chargées implicitement dans l'appareil cible avec le projet.
- DCC n'offre pas de protection de savoir-faire pour les diagrammes.

## Ordinateur de mise en service

Veiller à la sécurité de l'ordinateur de mise en service. Respecter pour cela les Mesures de sécurité (Page 27) générales.

### Utilisation de la protection de savoir-faire

Les diagrammes DCC, bibliothèques DCC et fichiers de sauvegarde sont très exposés à la manipulation des données. Il convient par conséquent d'utiliser la protection de savoir-faire dans STARTER, la protection d'écriture pour les entraînements et la protection de savoir-faire pour les diagrammes DCC et les bibliothèques DCC, voir aussi Utiliser la protection de savoir-faire et la protection en écriture (Page 106).

Pour plus d'informations sur la protection de savoir-faire, voir aussi le manuel de programmation et d'utilisation "Motion Control SINAMICS/SIMOTION Description de l'éditeur DCC".

### Protection des fichiers de sauvegarde dans le système de fichiers Windows

Les fichiers de sauvegarde de diagrammes ou de projets générés avec les outils de Windows doivent également être protégés contre les accès non autorisés à l'aide d'outils Windows, au moyen de mots de passe sûrs.

### Respecter les consignes relatives à SINAMICS et au système d'ingénierie

Respecter également les consignes Industrial Security s'appliquant aux entraînements SINAMICS et aux systèmes d'ingénierie utilisés pour la mise en service des entraînements SINAMICS. Les consignes relatives à la sécurité des réseaux sont particulièrement importantes, voir aussi Sécurité des réseaux (Page 32).

## 7.4.11.2 Utiliser la protection de savoir-faire et la protection en écriture

### Empêcher les modifications illicites avec la protection de savoir-faire

**⚠ ATTENTION**

**Danger de mort en cas de manipulation des diagrammes DCC et des bibliothèques DCC**

L'utilisation de diagrammes DCC et bibliothèques DCC qui ne sont pas protégés présente un risque en matière de manipulation de diagrammes DCC, bibliothèques DCC et fichiers de sauvegarde.

- Protéger les diagrammes DCC et les bibliothèques DCC importants via "Protection de savoir-faire pour programmes" ou "Protection de savoir-faire pour groupes d'entraînement" dans SCOUT ou STARTER. Attribuer un mot de passe efficace afin d'empêcher toute manipulation.
- C'est pourquoi, pour "Protection de savoir-faire pour programmes" ou "Protection de savoir-faire pour groupes d'entraînement", utiliser des mots de passe d'au moins 8 caractères comportant des majuscules et des minuscules, des chiffres et des caractères spéciaux.
- Faites en sorte que seules les personnes autorisées aient accès aux mots de passe.
- Protégez les fichiers de sauvegarde sur votre système de fichiers avec une protection en écriture.

## 7.4.12 SINAMICS Smart Access Module

Le Smart Access Module optionnel représente une solution intelligente pour la mise en service du variateur SINAMICS V20 ou G120.

Le Smart Access Module est un module serveur web avec connectivité WLAN intégrée. Il permet l'accès basé sur le web au variateur à partir d'un appareil connecté (PC courant avec adaptateur WLAN, tablette ou smartphone). Il est uniquement prévu pour la mise en service et ne doit pas rester connecté durablement au variateur.

| IMPORTANT |
| --- |
| **WLAN : modification du mot de passe par défaut**<br>L'utilisation abusive des mots de passe peut également constituer un risque de sécurité considérable. Un paramétrage incorrect ou modifié peut entraîner des dysfonctionnements sur les machines, susceptibles de provoquer des blessures, voire la mort.<br>• Modifier le mot de passe par défaut du module dès la première connexion au Smart Access Module.<br>• Attribuer un mot de passe sécurisé. Des consignes à ce sujet sont disponibles dans les instructions de service du variateur considéré. |

| IMPORTANT |
| --- |
| **Accès non autorisé au variateur via le SINAMICS Smart Access Module.**<br>Un accès non autorisé au variateur via le Smart Access Module par des cybercriminels peut entraîner des interruptions du processus et, de ce fait, des dommages matériels ou des blessures corporelles.<br>• Avant de se connecter aux pages web, contrôler la LED d'état sur le Smart Access Module. Si la LED d'état est allumée en vert ou clignote en vert, un accès non autorisé a pu se produire : effectuer une mise hors/sous tension du SINAMICS Smart Access Module afin de renouveler la connexion LAN. |

Pour plus d'informations à ce sujet, voir les documents suivants :

- Instructions de service Variateur SINAMICS V20 (https://support.industry.siemens.com/cs/de/en/view/109773836/fr)
- Instructions de service SINAMICS G120 Smart Access (https://support.industry.siemens.com/cs/ww/fr/view/109771299)

## 7.5 SIMOCRANE

Disponibilité, productivité et sécurité sont des facteurs décisifs dans les applications d'appareils de levage. Les produits SIMOCRANE étant basés sur des produits SIMOTION et SINAMICS, respecter les mesures de durcissement spécifiques à ces produits indiquées aux chapitres SIMOTION (Page 75) et SINAMICS (Page 90).

# Références

A

## Informations générales

Vous trouverez des **informations générales** complémentaires sur Industrial Security sur Internet :

- Industrial Security (https://www.siemens.com/industrialsecurity)
- Cybersécurité (https://new.siemens.com/global/en/company/topic-areas/cybersecurity.html)
- Planification de la sécurité (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/planning.html)
- Mise en œuvre de la sécurité (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/implementation.html)
- Always active (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/always-active.html)
- Certifications et normes (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/certification-standards.html)
- Livres blancs et téléchargements (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/downloads.html)

## Mots de passe sécurisés

**Plus d'informations** sur l'attribution de mots de passe sécurisés, voir aux adresses suivantes :

- Office fédéral allemand de la sécurité des technologies de l'information (BSI) (https://support.industry.siemens.com/cs/de/de/view/109757594/fr) (uniquement en allemand)
- European Network and Information Security Agency (enisa). (https://www.enisa.europa.eu/media/news-items/basic-security-practices-regarding-passwords-and-online-identities)
- National Institute of Standards and Technology (NIST) (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf)

## Pages web des produits

Pour plus d'informations spécifiques aux produits sur Industrial Security, voir les **pages web des différents produits** :

- SINUMERIK : Page d'accueil SINUMERIK (https://www.siemens.com/sinumerik)
- SIMOTION : Page d'accueil SIMOTION (https://www.siemens.com/simotion)
- SINAMICS : Page d'accueil SINAMICS (https://www.siemens.com/sinamics)

## Manuels spécifiques aux produits

Les **manuels spécifiques** des différents produits sont disponibles sur Internet :

- Manuel de l'appareil "SINUMERIK 840D sl NCU 7x0.3 PN" (https://support.industry.siemens.com/cs/de/en/view/99922219)
- Manuel de mise en service "Mise en service CNC : CN, AP, entraînement" (https://support.industry.siemens.com/cs/ww/en/view/109777906)
- Manuel de mise en service "SINUMERIK 840D sl Système d'exploitation NCU (IM7)" (https://support.industry.siemens.com/cs/ww/fr/view/109777905/en)
- Manuel de mise en service "SINUMERIK 840D sl Logiciel de base et HMI sl" (https://support.industry.siemens.com/cs/de/en/view/109254363/fr)
- Manuel de mise en service SINUMERIK 840Dsl Safety Integrated plus (https://support.industry.siemens.com/cs/de/en/view/109777982/fr)
- Manuel de mise en service "SINUMERIK Operate (IM9)" (https://support.industry.siemens.com/cs/ww/en/view/109769186)
- Manuel de mise en service logiciel de base PCU (IM8) (https://support.industry.siemens.com/cs/de/de/view/109748542/fr)
- Manuel de mise en service "Logiciel de base PCU (IM10)" (https://support.industry.siemens.com/cs/de/en/view/109769185)
- Manuel d'utilisation SINUMERIK Access MyMachine /P2P (PC) (https://support.industry.siemens.com/cs/ww/en/view/109770206)
- Manuel de configuration SINUMERIK Access MyMachine /OPC UA (https://support.industry.siemens.com/cs/de/de/view/109777871/fr)
- Description fonctionnelle Manage MyMachines /Remote (https://support.industry.siemens.com/cs/ww/en/view/109759394)
- Manuel de diagnostic 808D (https://support.industry.siemens.com/cs/de/en/view/109763685)
- Manuel de programmation SIMOTION IT Programmation et services Web (https://support.industry.siemens.com/cs/de/en/view/109767637/fr)
- Manuel de diagnostic SIMOTION IT Diagnostic et configuration (https://support.industry.siemens.com/cs/de/de/view/109767636/fr)
- Manuel de programmation SIMOTION IT Machine virtuelle et servlets (https://support.industry.siemens.com/cs/de/en/view/109767639/fr)
- Manuel de programmation SIMOTION IT OPC UA (https://support.industry.siemens.com/cs/de/en/view/109767638/fr)
- BA_G110M (https://support.industry.siemens.com/cs/de/de/view/109757594/fr)
- Manuel système Communication avec SIMOTION (https://support.industry.siemens.com/cs/de/en/view/109767623/fr)
- SINAMICS S120 Description fonctionnelle Fonctions d'entraînement (https://support.industry.siemens.com/cs/de/en/view/109771805/fr)
- Manuel de l'appareil SINAMICS S120 Control Units et composants systèmes complémentaires (https://support.industry.siemens.com/cs/de/en/view/109771804/fr)

- Description fonctionnelle SINAMICS S120 Safety Integrated (https://support.industry.siemens.com/cs/de/en/view/109771806/fr)
- Description fonctionnelle SINAMICS S120 Communication (https://support.industry.siemens.com/cs/ww/fr/view/109771803)
- Tables de paramètres SINAMICS S120/S150 (https://support.industry.siemens.com/cs/de/en/view/109763271/fr)
- Instructions de service G110M (https://support.industry.siemens.com/cs/de/de/view/109757594/fr)
- Instructions de service G120 (https://support.industry.siemens.com/cs/ww/fr/view/109771299)
- Description fonctionnelle SINAMICS G Bus de terrain (https://support.industry.siemens.com/cs/ww/de/view/109757336/en)
- Instructions de service S210 (https://support.industry.siemens.com/cs/ww/fr/view/109771824)
- Instructions de service V20 (https://support.industry.siemens.com/cs/de/en/view/109773836)
- Description fonctionnelle S7-1500, ET 200SP, ET200pro Webserver (https://support.industry.siemens.com/cs/ww/fr/view/59193560)
- Manuel de programmation et d'utilisation SIMATIC Programmer avec STEP 7 (https://support.industry.siemens.com/cs/de/de/view/109751825/fr)
- Manuel de l'appareil SIMATIC S7-300 CPU 31xC et CPU 31x : Caractéristiques techniques (https://support.industry.siemens.com/cs/de/en/view/12996906/fr)
- Manuel de configuration SIMATIC NET : Commutateurs Industrial Ethernet SCALANCE X-200 (https://support.industry.siemens.com/cs/de/en/view/109757352/fr)

## Voir aussi

Implement Security (https://www.industry.siemens.com/services/global/en/portfolio/plant-data-services/industrial_security)

Manuel de mise en service Safety Integrated plus (https://support.industry.siemens.com/cs/de/en/view/109777982/fr)

Recommandations du BSI en matière de mots de passe (https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html)

# Glossaire

### Accès à distance

Utilisation de systèmes situés dans le périmètre de la zone de sécurité et auxquels on accède à partir d'un autre lieu géographique avec les mêmes droits que si les systèmes se trouvaient physiquement sur ce lieu.

### AMC

Abréviation de SINUMERIK Integrate Analyze MyCondition

### AMD

Abréviation de SINUMERIK Integrate Access MyData

### AMM

Abréviation de SINUMERIK Integrate Access MyMachine

### AMP

Abréviation de SINUMERIK Integrate Analyze MyPerformance

### AMT

Abréviation de Intel® Active Management Technology

### Analyse des menaces et des risques (TRA)

L'analyse des menaces et des risques est une méthode standardisée de Siemens utilisable pour les activités de produit, de solutions et de services, dans les projets de développement de produit, d'ingénierie ou de maintenance. La méthode vise à aider les participants au projet à détecter les points faibles et failles de sécurité typiques, à analyser les menaces susceptibles d'utiliser ces faiblesses et failles et d'évaluer les risques qui en découlent.

### Attaque

Tentative de détruire une ressource, de la priver de sa protection, de la modifier, de la désactiver, de la voler, d'y accéder sans autorisation ou de l'utiliser de manière non autorisée.

### Authentification

Vérification de l'identité d'un utilisateur, processus ou appareil, souvent une condition pour autoriser l'accès à des ressources dans un système informatique.

### Autorisation

Le droit accordé à une entité de système d'accéder à une ressource système.

### Cloud computing

Par cloud computing, on entend la sauvegarde de données dans un centre de calcul distant, mais également l'exécution de programmes qui ne sont pas installés sur l'ordinateur local mais dans un nuage (métaphorique), ou cloud en anglais.

### Commutateur

Composant de réseau pour la connexion de plusieurs équipements terminaux ou segments de réseau dans un réseau local (LAN).

### Confidentialité

Le fait, pour des informations, de ne pas être rendues disponibles ni divulguées à des personnes, des entités ou des processus non autorisés.

### Cybersécurité

La cybersécurité désigne les pratiques de défense des ordinateurs, serveurs, appareils mobiles, systèmes électroniques, réseaux et données contre des attaques malveillantes. Elle comprend également la sécurité des technologies de l'information et des informations électroniques. Le terme s'entend dans un sens large et englobe tout, de la sécurité informatique jusqu'à la formation des utilisateurs finaux en passant par la restauration après un incident (disaster recovery).

### Défense en profondeur (Defense in Depth)

Réalisation de plusieurs mécanismes de sécurité, notamment avec une structure en couches, dans l'optique de freiner voir d'empêcher totalement les attaques.

### Déni de service (Denial of Service, DoS)

Le déni de service, ou DoS (en anglais Denial of Service), désigne en informatique la non-disponibilité d'un service qui devrait être disponible. Bien qu'il puisse exister diverses causes à la non-disponibilité, on parle généralement de DoS comme de la conséquence d'une surcharge de systèmes d'infrastructure. Celle-ci peut être causée par des surcharges non intentionnelles mais également par une attaque délibérée sur un serveur, un ordinateur ou d'autres composants d'un réseau de données.

### Disponibilité

Capacité d'être accessible et utilisable à la demande par une entité autorisée.

## DMZ

Une zone démilitarisée, ou DMZ (en anglais, demilitarized zone) est un sous-réseau séparé qui isole le réseau local (LAN) d'Internet par des routeurs pare-feu (A et B). Ces routeurs pare-feu sont configurés de manière à rejeter les paquets de données pour lesquels il n'existait pas de paquets de données préalables. Ainsi, si un paquet de données est envoyé au serveur depuis l'Internet, il sera rejeté par le routeur pare-feu A. Si un pirate obtient malgré tout un accès à un serveur dans la DMZ et veut envoyer des paquets de données dans le LAN à des fins d'espionnage ou de piratage, ces paquets seront rejetés par le routeur pare-feu B.

## Durcissement

Démarche consistant à augmenter la sécurité d'un système en réduisant la surface d'attaque.

## Faille de sécurité ou vulnérabilité

Faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système. Elle est généralement la conséquence d'erreurs de programmation ou de faiblesses dans la conception du système.

Point faible d'une ressource ou d'un élément de commande pouvant être exploitée par une ou plusieurs menaces.

## Force brute

Pour de nombreux problèmes en informatique, il n'existe pas d'algorithme efficace. L'approche la plus naturelle et la plus simple d'une solution algorithmique à un problème consiste à considérer toutes les solutions possibles jusqu'à trouver la solution correcte. Cette méthode est appelée "recherche par force brute" (anglais : brute-force search). La méthode de force brute est par exemple utilisée pour casser (ou "craquer") un mot de passe. Les mots de passe sont souvent cryptés à l'aide de fonctions de hachage cryptographiques. Un calcul direct du mot de passe à partir de la valeur de hachage est pratiquement impossible. Un cracker peut toutefois calculer les valeurs de hachage de nombreux mots de passe. Si une valeur correspond à la valeur du mot de passe défini, il a découvert le mot de passe (ou un autre mot de passe correspondant par hasard). Force brute signifie donc ici essayer simplement des mots de passe possibles.

## Gestion des correctifs

Domaine de la gestion système comprenant les tâches d'obtenir, tester et installer plusieurs correctifs (modifications du code) pour un système informatique administré ou dans un tel système. Il s'agit également d'un sous-processus de la gestion des failles de sécurité (Security Vulnerability Management) qui a notamment pour tâche d'éliminer et de circonscrire les failles de sécurité des produits Siemens à l'aide de corrections du logiciel.

## Hameçonnage (phishing)

L'hameçonnage ou phishing désigne le risque de la "pêche aux mots de passe à l'aide de leurres" dans des e-mails, avec des liens falsifiés ou des messages (p. ex. SMS). À l'aide d'e-mails et de sites Internet d'apparence sérieuse ou officielle, les "hameçonneurs (phishers)" essayent d'accéder aux données. Ils utilisent pour cela des points faibles p. ex. dans le

système d'exploitation ou le navigateur Internet par lesquels ils infiltrent des logiciels malveillants.

### IANA

L'**I**nternet **A**ssigned **N**umbers **A**uthority (**IANA**) est un département de l'ICANN responsable de l'allocation des noms et numéros attribués dans l'Internet, notamment des adresses IP. Il s'agit d'une des plus anciennes institutions de l'Internet.

### Incident

Un ou plusieurs événements indésirables ou inattendus qui compromettent les opérations liées à l'activité de l'organisme et menacent la sécurité de l'information. Les causes d'un incident peuvent être des failles de sécurité, des configurations incorrectes ou un comportement erroné, ainsi que leur exploitation.

### Industrial Security

Mesures visant à augmenter les normes de sécurité industrielle d'une installation. Celles-ci assurent la protection contre l'accès non autorisé aux systèmes de conduite, automates industriels et systèmes sur base PC de l'installation ainsi que contre les cyberattaques.

### Intégrité

Propriété garantissant l'exactitude et la complétude de ressources.

### Internet des objets / Internet of Things (IoT)

Terme générique désignant des technologies d'une infrastructure globale de la société de l'information permettant d'interconnecter entre eux des objets physiques et virtuels et de les faire collaborer grâce aux techniques d'information et de communication.

### IPsec (Internet Protocol Security)

IPsec est une extension du protocole Internet (IP) par des mécanismes de cryptage et d'authentification. Le protocole Internet est ainsi capable de transporter des paquets IP sécurisés par cryptographie sur des réseaux publics non sécurisés.

### Logiciel malveillant, maliciel (malware)

Logiciel malveillant est un terme générique désignant des programmes développés pour porter préjudice aux utilisateurs. Il existe de nombreux types de logiciels malveillants, tels que les virus, les chevaux de Troie, les rootkits, les spywares (logiciels espions).

### Menace

Cause potentielle d'incident, qui peut résulter en un dommage au système ou à l'organisation.

### MMP

Abréviation de SINUMERIK Integrate Manage MyPrograms

### MMT

Abréviation de SINUMERIK Integrate Manage MyTools

### NAT (Network Address Translation)

NAT est une procédure utilisée dans les routeurs IP qui connectent les réseaux locaux à l'Internet. Étant donné que les accès Internet ne disposent en général que d'une seule adresse IP (IPv4), toutes les autres stations du réseau local doivent se contenter d'une adresse IP privée. Les adresses IP privées peuvent être utilisées plusieurs fois, mais n'ont aucune validité dans les réseaux publics. Des stations possédant une adresse IP privée ne peuvent donc pas communiquer avec des stations situées en dehors du réseau privé. Afin que tous les ordinateurs ayant un accès avec adresse IP privée puissent malgré tout accéder à l'Internet, le routeur d'accès à Internet doit remplacer, dans tous les paquets de données sortants, l'adresse IP des stations locales par sa propre adresse IP publique. Afin que les paquets de données entrants puissent être affectés à la station concernée, le routeur stocke les connexions TCP actuelles dans une table. Le routeur NAT mémorise l'affectation des paquets de données aux connexions TCP. Cette procédure est appelée NAT (Network Address Translation).

### NCU

Unité de commande centrale d'une commande CNC pour CN, IHM, AP et régulation.

### OpenVPN

OpenVPN est un programme servant à établir un réseau privé virtuel (virtual private network, VPN) via une connexion TLS cryptée. Les bibliothèques du programme Open SSL sont utilisées pour le cryptage. OpenVPN utilise au choix UDP ou TCP pour le transport.

### Pare-feu

Appareil de liaison entre des réseaux qui restreint l'échange de données entre les deux réseaux reliés.

### PCU

PC industriel à haut degré d'intégration pour interface utilisateur ou logiciel système et interface utilisateur d'une CNC.

### Pirate informatique (hacker)

Personne impliquée dans des activités délibérées de piratage informatique (hacking). Les motivations de ces activités peuvent être malveillantes ou non malveillantes, ou se maintenir dans des limites éthiques et juridiques acceptables.

### SCADA

Par **S**upervisory **C**ontrol **a**nd **D**ata **A**cquisition (**SCADA**), on entend la supervision et la commande de processus techniques à l'aide d'un système informatique.

### Sécurité (Security)

Préservation de la confidentialité, de l'intégrité et de la disponibilité d'un produit, d'une solution ou de services.

### Sécurité de l'information

Préservation de la confidentialité, de l'intégrité et de la disponibilité des informations.

### Signature de virus

Désignation de la base de données utilisée par les antivirus et contenant la structure schématique et spécifique au code de tous les virus connus. Il s'agit généralement d'un fichier utilisé et traité par l'antivirus. Les schémas contenus dans le fichier sont utilisés pour la détection de virus ; les fichiers à contrôler sont comparés à ces schémas.

### Surface d'attaque

Somme totale des vulnérabilités d'un système accessibles à un pirate.

### Système SIEM

SIEM signifie Security Information and Event Management et le terme s'est établi dans le domaine de la sécurité informatique. Les systèmes correspondants sont en mesure d'identifier des événements concernant la sécurité, de les évaluer et d'alarmer ensuite l'administrateur.

### TLS

Transport Layer Security (TLS V1.2 ou "sécurité de la couche transport ") est un protocole de cryptage hybride pour la transmission de données sécurisée sur Internet.

### VPN (Virtual Private Network)

Une connexion cryptée d'ordinateurs ou de réseaux via l'Internet. Elle permet l'échange de données confidentielles sur des réseaux publics.

### WSUS (Windows Server Update Services)

Windows Server Update Services (WSUS) est le composant logiciel de Microsoft Windows Server depuis la version 2003 qui est responsable des correctifs et des mises à jour. Il s'agit de la version succédant au composant logiciel Software Update Services.

# Index

## T



## U



## V



## W

## X



## Z