LIVRE BLANC

La cybersécurité dans l'industrie agro-alimentaire

La réduction des risques selon CRITIS
siemens.com/industrialsecurity

SIEMENS

Le développement du numérique dans les entreprises et la mise en réseau de la plupart des secteurs d'activité génèrent un potentiel économique considérable. Aujourd'hui, plus de 20 milliards de dispositifs et de machines sont déjà connectés via Internet. D'ici 2030, ce nombre atteindra environ 500 milliards de dollars. Le numérique et la connectivité peuvent favoriser la croissance et un certain dynamisme, mais le développement de la connectivité crée également de nouvelles failles qu'il faut corriger rapidement et de manière cohérente.

Cela est également vrai pour les entreprises de l'industrie agro-alimentaire

En 2017, l'une des plus grandes entreprises du secteur agro-alimentaire au monde a été victime d'un ransomware ayant pris la forme d'un cheval de Troie. Le logiciel malveillant "Petya" a attaqué des systèmes informatiques dans le monde entier et verrouillé l'accès à leurs utilisateurs dans le but de leur extorquer une rançon. Selon les propres estimations de l'entreprise, la cyberattaque a entraîné une perte de revenus d'environ 140 millions de dollars. Il a fallu plusieurs jours pour que les systèmes les plus importants redeviennent opérationnels, et plusieurs semaines pour que les systèmes restants soient de nouveau utilisables.

Cet incident, ainsi que d'autres incidents similaires survenus au cours des dernières années, ont incité les législateurs de nombreux pays à adopter des règles et des réglementations relatives à la cybersécurité. Ces normes visent à protéger les infrastructures essentielles afin de garantir la sécurité de l'approvisionnement pour les citoyens de ces pays et la stabilité pour les pays eux-mêmes.

En Allemagne, par exemple, la loi "Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (loi sur le renforcement de la sécurité des systèmes informatiques = IT Security Act) est entrée en vigueur en juillet 2015. Cette loi impose aux exploitants d'infrastructures essentielles (CRITIS) de mettre en place certaines mesures. Le terme "opérateurs d'infrastructures critiques" désigne également les entreprises du secteur agro-alimentaire, dans la mesure où les cyberattaques dirigées contre cette industrie ne se contentent pas de perturber la production et de provoquer des pertes financières, elles peuvent aussi présenter des risques pour la santé.

La principale priorité est d'éviter les erreurs de fabrication et la manipulation de la production, et d'éviter une perte de réputation. L'adoption de mesures de sécurité appropriées n'est pas un luxe, c'est une nécessité.

Sommaire

1
Les législateurs réglementent la sécurité informatique dans le monde entier 4

2
Cybersécurité : un processus continu 5

3
Menaces : cibles des attaques et types de pirates informatiques 6

4
Cybersécurité : procédure étape par étape 7

5
Mesures de sécurité pour les usines 8

6
Mesures de sécurité pour les réseaux 8

7
Segmentation des réseaux 9

8
Accès à distance et postes extérieurs distribués 10

9
Exigences générales concernant les éléments de réseau 11

10
Contrôle d'accès : autorisation 12

11
Mesures liées à l'intégrité du système 13

12
Mesures relatives au personnel 14

13
Plan d'urgence et restauration 14

14
Vue d'ensemble 15

15
Terminologie et abréviations 16

Les législateurs réglementent la sécurité informatique dans le monde entier

Depuis juillet 2015, la loi allemande sur la sécurité informatique impose le signalement des incidents de sécurité affectant certaines infrastructures essentielles. Au fil du temps, les opérateurs CRITIS seront également tenus de se conformer à des normes minimales de cybersécurité. La mise en œuvre de ces normes s'appuie notamment sur les normes CEI 27001 et CEI 62443. Les fabricants de composants d'automatisation et de réseau, ainsi que les exploitants d'usines, doivent mettre en œuvre des mesures de cybersécurité de pointe. Le terme juridique "de pointe" est utilisé parce que l'expérience a montré que le développement technologique progresse plus vite que la législation. La technologie de pointe à un moment donné peut être déterminée sur la base des normes nationales ou internationales existantes, telles que DIN et IEC, ou sur la base des bonnes pratiques du secteur en question.

Technologie de pointe selon la norme CEI 62443

Les documents de la norme CEI 62443 sont organisés de la manière suivante :

- La norme CEI 62443-1 comprend la terminologie, les concepts, les cas d'utilisation et les modèles.
- La norme CEI 62443-2 s'adresse aux exploitants d'usines et décrit des activités telles que la mise en œuvre d'un système de gestion de la sécurité et de gestion des correctifs.
- La norme CEI 62443-3 décrit les technologies de sécurité pour les contrôleurs et les composants réseau.
- La norme CEI 62443-4 s'adresse aux fabricants et décrit des procédures permettant de protéger le processus de développement et d'autres activités.

Cette division des informations démontre que la cybersécurité est considérée comme un processus complet et que les normes de sécurité doivent être respectées au moment du développement des composants.

Aux États-Unis, la loi sur la modernisation de la sécurité alimentaire ("Food Safety Modernization Act", FSMA) de la FDA prévoit des normes similaires qui associent, entre autres, la surveillance, les possibilités d'intervention et la vérification des mesures de cybersécurité. En Grande-Bretagne, la norme PAS 96:2017 réglemente les mesures de sécurité et de prévention contre les attaques pour l'industrie agro-alimentaire.

Fondamentalement, ce que toutes les lois et normes ont en commun, c'est qu'elles sont composées d'un mélange de normes techniques, d'obligations de signalement des incidents et de surveillance du respect des normes.

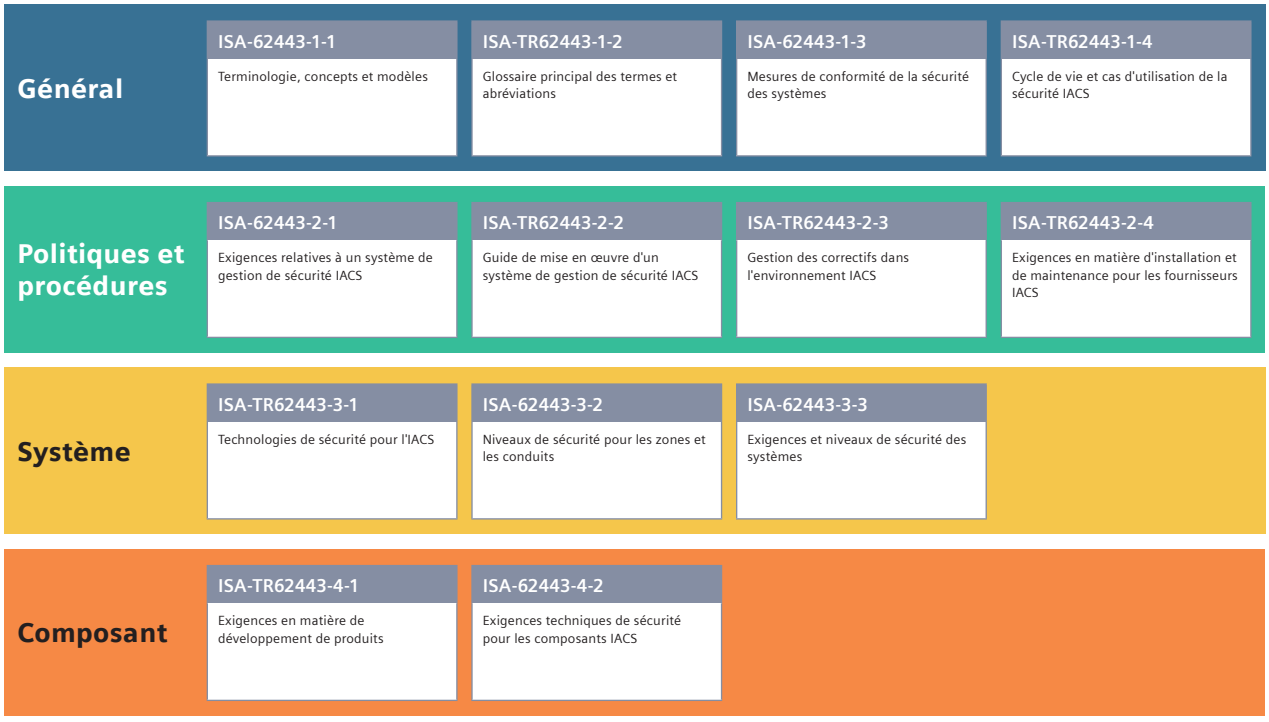

Schéma 1 : documents de la norme CEI 62443

Cybersécurité : un processus continu

Une protection efficace contre les cyberattaques n'est pas obtenue par une mise en œuvre ponctuelle de mesures de sécurité : il s'agit d'un processus continu.

Une fois l'analyse des risques (évaluation) d'un processus automatisé effectuée, des mesures doivent être mises en œuvre pour les réduire (implémentation). Ces mesures doivent faire l'objet d'un suivi, et la nécessité de les réviser en raison d'une évolution du scénario de menace doit être continuellement évaluée (gestion). Les mesures requises sont aussi variées que les risques évalués. En fonction du niveau d'automatisation, de la technologie utilisée et de la connectivité OT (technologies opérationnelles) et IT (technologies de l'information), les experts en sécurité développent des mécanismes de sécurité appropriés et adaptés à chaque entreprise et à ses processus.

L'exploitant de l'usine est toujours responsable de sa sécurité informatique. Même si l'exploitation de l'usine n'est pas totalement, ou n'est pas du tout, prise en charge par le personnel de l'entreprise en raison de la sous-traitance, l'exploitant de l'usine reste responsable. Les menaces liées à la sous-traitance doivent également être évaluées. Il est généralement recommandé que les employés suivent des formations de sensibilisation aux cyberattaques, afin qu'ils puissent réagir rapidement et de manière ciblée en cas d'urgence.

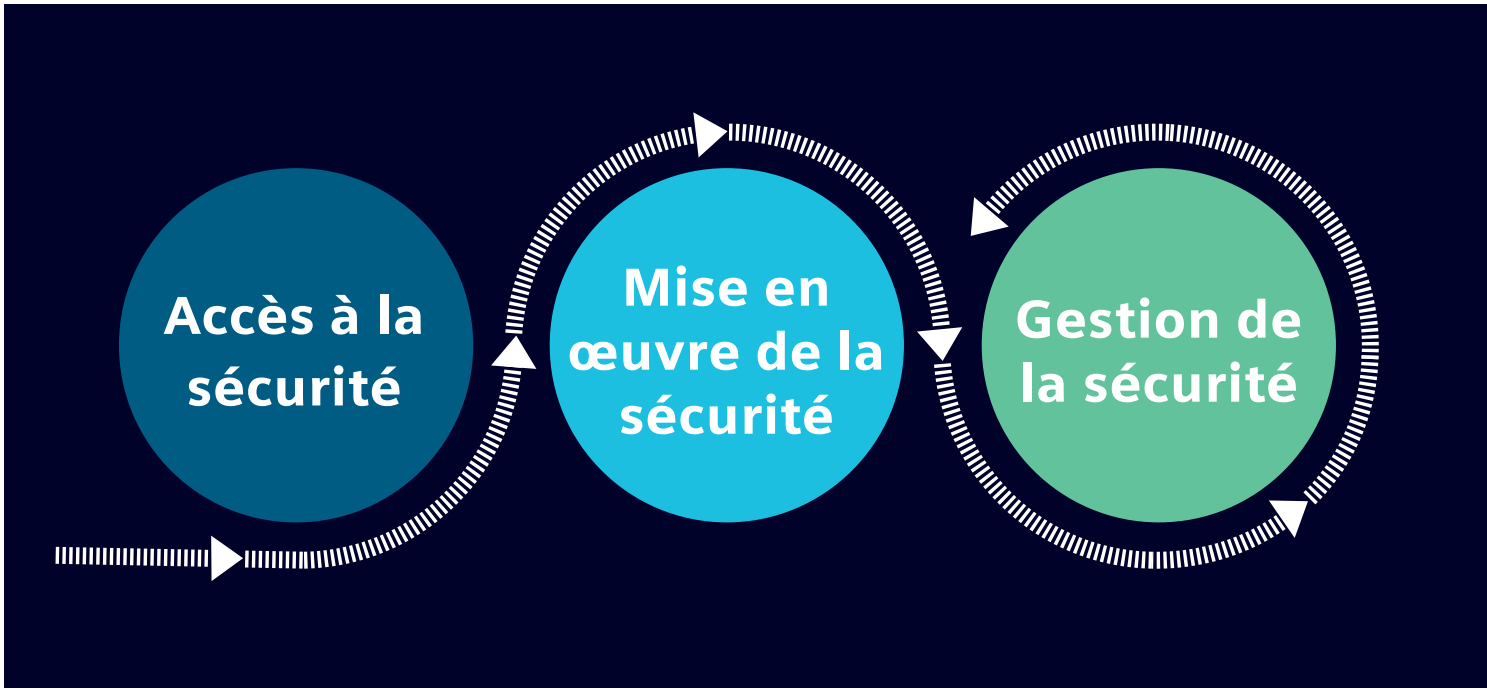

Schéma 2 : les trois phases de la sécurité IT/OT ou de la sécurité industrielle

Menaces : cibles des attaques et types de pirates informatiques

Quels sont les objectifs des pirates informatiques qui tentent de contourner les mesures de sécurité ? Les pirates se répartissent généralement en quatre catégories.

Les **pirates non spécialistes** ("script kiddies") recourent à des scripts complets disponibles sur Internet comme un moyen simple d'attaquer des vulnérabilités connues, "simplement parce qu'ils en ont la possibilité".

Les **pirates spécialistes** ("pirates informatiques") lancent des attaques plus complexes dans un but lucratif et, par exemple, afin d'extorquer des rançons pour déchiffrer des données.

L'**espionnage industriel** est généralement pratiqué par des personnes internes, qui utilisent leurs connaissances spécialisées pour dérober des données ou nuire à l'entreprise. Dans ce cas, des (anciens) employés ciblent une entreprise spécifique.

Les **attaques dirigées par un État** sont les plus dangereuses au niveau technique. Ces attaques exploitent généralement des failles jusqu'alors non identifiées et ont des objectifs variés : accéder à des données sensibles, manipuler des données, désorganiser des processus de fabrication, voire détruire des sections entières d'une usine. Outre le gain financier, leur motivation peut également être de déstabiliser un pays, par exemple en s'attaquant à l'approvisionnement alimentaire dudit pays.

Menaces

L'Office fédéral allemand des technologies de l'information (Bundesamt für Sicherheit in der Informationstechnik = BSI) a identifié les dix attaques les plus fréquentes lancées contre des installations industrielles (Statut : BSI-CS 029 | Version 2.0 du 11 juillet 2018) :

1. Utilisation non autorisée d'un accès de maintenance à distance qui permet un accès externe à des systèmes de contrôle industriel (ICS) souvent insuffisamment protégés.
2. Attaques en ligne via le service informatique d'un bureau, qui est généralement connecté à Internet et peut également établir une connexion au réseau de circuits intégrés.
3. Attaques ciblant des composants standard comme des systèmes d'exploitation, des serveurs d'application ou des bases de données qui recèlent généralement des erreurs et des failles que les attaquants peuvent exploiter. Ces composants peuvent également être déployés dans des systèmes de supervision informatique, ce qui augmente le risque.
4. Les attaques par déni de service sur les connexions réseau peuvent surcharger les systèmes et perturber la fonctionnalité du réseau du système de supervision informatique, ou du système de supervision informatique lui-même.
5. L'erreur humaine et le sabotage par des auteurs internes ou externes constituent une menace très importante. La négligence et l'erreur humaine menacent également la confidentialité et la disponibilité.
6. Des logiciels malveillants sont souvent introduits par le biais de dispositifs de stockage amovibles ou de composants informatiques mobiles appartenant à des employés externes (exemple : Stuxnet).
7. Les commandes de contrôle peuvent être facilement lues et importées, car la plupart des composants de contrôle communiquent via des protocoles en texte brut, ce qui signifie que leur communication n'est pas protégée.
8. Un accès non autorisé aux composants de réseau est possible si des personnes internes (ou des personne externes qui sont passées outre les mesures de sécurité) accèdent aux composants à l'aide de méthodes d'authentification et d'autorisation non sécurisées.
9. Les pirates informatiques peuvent manipuler les composants de réseau afin de mener des attaques de type "man-in-the-middle" ou de faciliter le "sniffing" (surveillance du trafic Internet en temps réel).
10. Le risque de défaillance résultant d'influences environnementales extrêmes ou de défauts techniques ne peut jamais être complètement éliminé, mais il peut être réduit, ainsi que les dommages qui en découlent, à l'aide de composants et de mesures de sécurité appropriés.

Cybersécurité : procédure étape par étape

La liste des menaces montre que des méthodes très différentes peuvent être utilisées pour lancer des attaques, et les processus doivent être protégés contre ce vaste éventail de menaces. La norme industrielle allemande et la norme CEI 62443 définissent un processus en plusieurs étapes pour la mise en œuvre de la cybersécurité.

1. La sélection d'objets permet d'enregistrer et de documenter tous les systèmes de l'usine, y compris les sous-systèmes et un plan du réseau.
2. Les menaces découlent d'une sélection de cas d'utilisation : par exemple, le fait qu'un système puisse être attaqué par le biais d'un accès de maintenance à distance.
3. L'évaluation des menaces identifie les menaces pour chaque cas d'utilisation : par exemple, l'accès à la maintenance à distance peut être utilisé par une personne non autorisée.
4. L'analyse des risques consiste à identifier les menaces potentielles sur la base d'une matrice de risques.

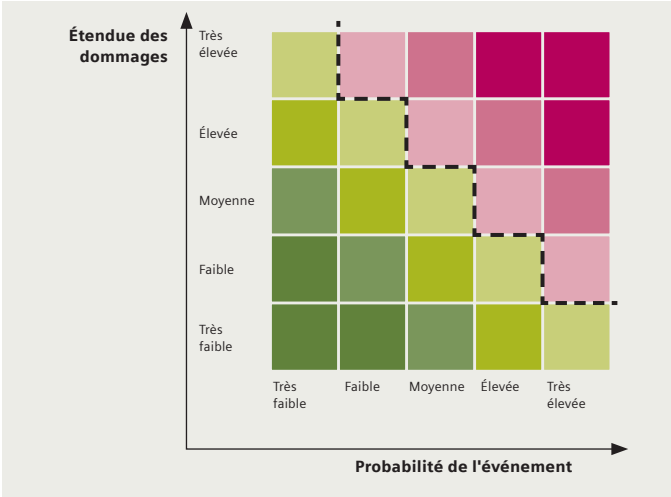

Schéma 3 : matrice des risques basée sur la norme BSI 200-3

Une menace dont la probabilité est élevée et dont l'étendue des dommages potentiels est également élevée apparaît dans la zone rouge, en haut à droite de la matrice (risque élevé). Une étendue des dommages et une probabilité faibles posent un faible risque et apparaissent dans la zone verte, en bas à gauche. La norme BSI 200-3 fournit une répartition exacte de l'étendue des dommages (degré auquel l'exploitation de l'usine est limitée), de la probabilité de la menace et du risque.

5. Un processus visant à déterminer les mesures nécessaires définit des options concrètes, qui sont décrites en détail dans la section suivante.
6. La mise en œuvre des mesures comprend l'échéancier et la planification organisationnelle de la mise en œuvre. Il s'agit également de définir les responsabilités et d'allouer clairement le budget pour la mise en œuvre des mesures.
7. Pour l'audit, les mesures doivent être vérifiées, la documentation de l'usine doit être complète et des listes de contrôle doivent être remplies. L'efficacité des mesures doit être vérifiée à intervalles réguliers. Si des failles sont détectées, par exemple en raison de l'évolution des risques ou de nouveaux types de logiciels malveillants, l'ensemble du processus doit être redémarré, en commençant par l'évaluation de la menace.

Concept de sécurité

Puisque les menaces diffèrent en termes de nature, qu'elles peuvent provenir de l'intérieur ou de l'extérieur, et que les pirates disposent de niveaux d'expertise différents, il est important de créer un concept de sécurité multicouche, afin d'élaborer un processus offrant la meilleure protection possible. Par exemple, même si le pare-feu a été violé parce que le pirate est entré en personne dans l'usine, des mécanismes de sécurité supplémentaires doivent protéger les terminaux.

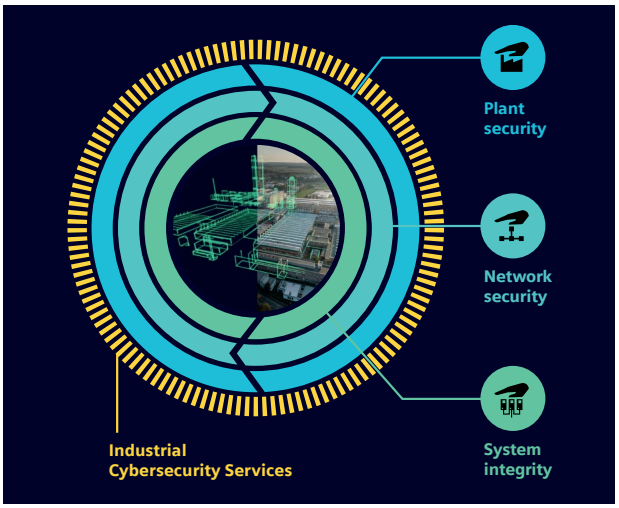

Schéma 4 : concept de sécurité de "Défense en profondeur"

Le schéma illustre un concept de sécurité multicouche qui définit la sécurité de l'usine, la sécurité du réseau et l'intégrité du système comme les trois couches essentielles d'une sécurité efficace.

Mesures de sécurité de l'usine

Les mesures organisationnelles comprennent toutes les mesures de protection physique de l'usine. En plus de la protection contre les effractions, elles doivent également inclure des procédures visant à protéger l'installation des influences environnementales.

Menaces
- Effraction/vandalisme
- Accès non autorisé
- Inondation
- Incendie
- Fumée/poussières/gaz corrosifs
- Foudre/surtension/CEM

Mesures organisationnelles
En fonction des menaces spécifiques, des mesures appropriées doivent être prises pour protéger l'usine. Une attention particulière est requise pour les postes extérieurs (par exemple, les entrepôts) qui sont généralement inoccupés et surveillés à distance depuis le centre de contrôle. Les postes extérieurs doivent être sécurisés contre les effractions et les portes et fenêtres doivent être protégées de manière appropriée.

Des capteurs fixés sur les portes et fenêtres peuvent notifier le contrôleur si celles-ci sont ouvertes et le contrôleur peut à son tour avertir le centre de contrôle. Une caméra IP peut permettre de détecter les intrus et de surveiller le bâtiment depuis le centre de contrôle.

Les différentes zones de production doivent également être séparées physiquement, au moyen d'un contrôle d'accès différencié. Par exemple, les composants critiques doivent être sécurisés dans une armoire de commande verrouillée (voir également page 14).

Les directives relatives aux mesures de protection liées à l'accès physique déterminent également les mesures de cybersécurité requises et la rigueur de ces mesures. Par exemple, dans les zones qui ne sont accessibles qu'à certaines personnes habilitées, il n'est pas nécessaire d'assurer un niveau de protection aussi élevé pour les interfaces d'accès au réseau et les systèmes d'automatisation que pour les zones accessibles au public.

Grâce à la certification de conformité à la norme CEI 27001, les entreprises peuvent réduire les risques liés à la sécurité de l'information, mieux se conformer aux réglementations et exigences de sécurité pertinentes et favoriser une culture de sécurité interne.

Mesures de sécurité du réseau

Le réseau doit être structuré en vue de résister au maximum aux attaques potentielles, tout en tenant compte des options d'accès, de la disponibilité et de la protection.

Options d'accès
En règle générale, les réseaux sont des systèmes ouverts dotés d'une connexion Internet. Pour la plupart des exploitants d'usines, l'accès externe à des fins de maintenance, de diagnostic, d'optimisation, de correctifs, de mises à jour et d'autres activités est devenu essentiel.

Disponibilité
Le processus automatisé, qui est commandé, par exemple, via le réseau à l'aide de la communication PROFINET, doit être exécuté indépendamment des interruptions de lignes individuelles. Les systèmes de surveillance du centre de contrôle doivent être en mesure de continuer à surveiller le processus même en cas de défaillance des différents routeurs.

Protection
Le processus doit être protégé contre tous les risques potentiels qui pourraient menacer le réseau, y compris les accès non autorisés, les logiciels malveillants et les attaques par déni de service. Tous les types de communication autres que les accès autorisés doivent être bloqués à l'aide de mesures appropriées.

La norme CEI 62443 impose les éléments suivants pour la protection du réseau :
- Segmentation de l'architecture réseau
- Isolement ou segmentation des composants à haut risque
- Blocage des communications inutiles
- Accès via des pare-feu

Segmentation du réseau

La segmentation du réseau à l'aide de pare-feu offre une protection contre les attaques provenant du réseau lui-même. Le réseau est divisé en groupes fonctionnels (par exemple, les réseaux de production, le réseau d'usine et le réseau des bureaux) et l'accès est contrôlé avec précision par des pare-feu.

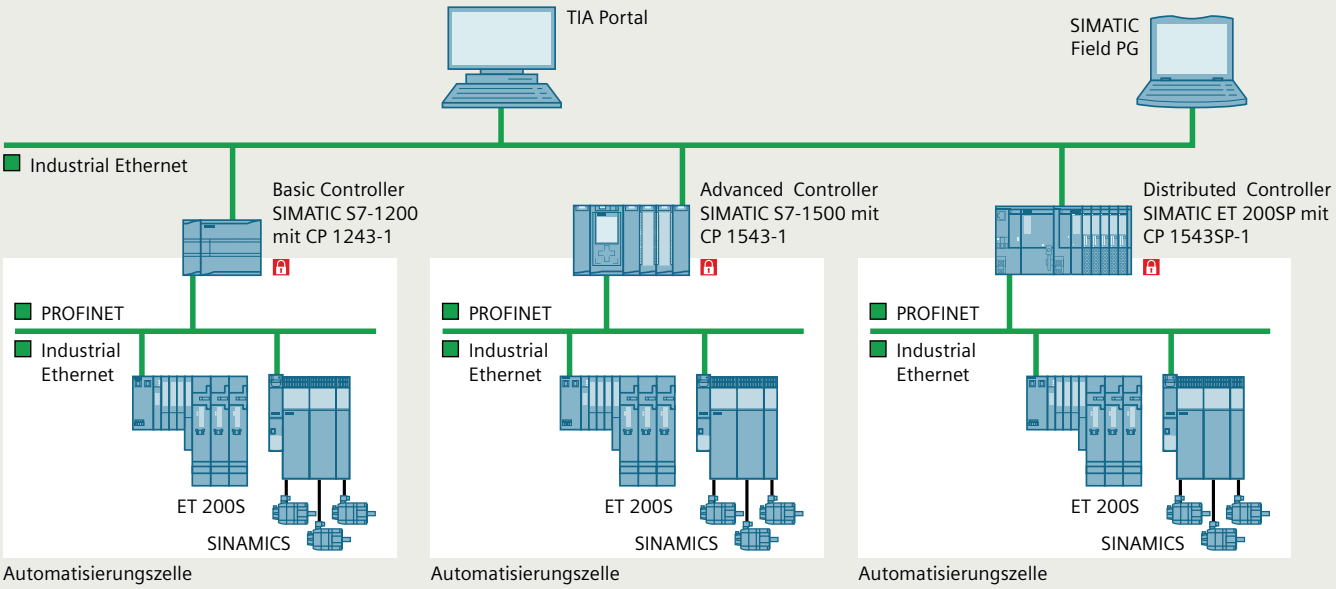

Schéma 5 : segmentation du réseau selon la norme CEI 62443-2-1

Zones démilitarisées (Demilitarisierte Zone, DMZ)
Le schéma 5 illustre une configuration réseau recommandée par la norme CEI 62443-2. Les cellules d'automatisation situées en bas sont regroupées en unités fonctionnelles et sont séparées du réseau de l'usine par un pare-feu. Le réseau de l'usine, qui se trouve au sommet, contient tous les dispositifs de niveau supérieur qui sont importants pour le fonctionnement de l'usine, comme le centre de contrôle et les serveurs. L'interface entre le réseau de l'usine et le réseau des bureaux est à nouveau séparée par un pare-feu. Une ou plusieurs zones démilitarisées (DMZ) peuvent y être mises en place. Dans une DMZ, les dispositifs des réseaux de niveau supérieur et inférieur ne communiquent pas directement entre eux. Ils communiquent plutôt par le biais d'un serveur qui, par exemple, récupère l'état de l'usine auprès des cellules d'automatisation et met ces informations à la disposition du réseau de niveau supérieur. Le réseau des bureaux est également protégé d'Internet par un ou plusieurs pare-feu.

Dans cet exemple, la configuration crée trois murs défensifs pour les cellules d'automatisation qui contrôlent le processus. Quant au réseau des bureaux, qui risque d'être affecté par les attaques plus fréquentes de logiciels malveillants (par exemple, sur des clés USB), il est séparé de la cellule d'automatisation par deux pare-feux. Plus un employé est proche de la cellule d'automatisation, plus il est important qu'il soit constamment sensibilisé aux enjeux de cybersécurité.

Accès à distance et postes extérieurs distribués

La connexion de postes extérieurs distribués constitue un défi particulier. Si ces postes doivent pouvoir fonctionner de manière autonome, il doit également être possible de les surveiller depuis le centre de contrôle. Le réseau d'un poste extérieur doit être protégé et l'accès au poste extérieur doit être sécurisé, même s'il est connecté via un réseau distinct ou la connexion propre à l'entreprise. Le poste extérieur peut être connecté par câble (comme ADSL ou SHDSL) ou par liaison radio (par exemple, LTE ou UMTS). Le modem doit contenir un pare-feu et être compatible avec un VPN.

Pour augmenter la sécurité, la connexion VPN peut être configurée pour l'accès à distance selon la norme CEI 62443, de sorte que le tunnel ne soit établi que lorsqu'un technicien sur site active le VPN au niveau du module.

Connexions sans fil via un réseau WLAN

Une attention particulière doit être accordée à la transmission sans fil via un réseau WLAN ou d'autres technologies similaires. Dans le cas d'une communication filaire, un attaquant doit se procurer un accès physique aux câbles ou aux composants du réseau pour lire les données ou en perturber le trafic. Avec la communication sans fil, les ondes radio sont réparties sur une plus grande surface, ce qui facilite les attaques.

Si un réseau WLAN est nécessaire dans la cellule d'automatisation, un réseau WLAN séparé doit être configuré pour l'automatisation. Le réseau WLAN dédié aux bureaux doit être exploité par le biais de différents points d'accès WLAN, afin de maintenir la segmentation du réseau.

Mesures organisationnelles pour un réseau WLAN

Le point d'accès doit être installé de manière à être inaccessible ou sécurisé dans une armoire de commande fermée, et les antennes WLAN doivent être installées à distance. Ces mesures empêcheront les intrus d'accéder physiquement au point d'accès. La fréquence WLAN doit également être sélectionnée avec soin, car d'autres applications utilisant la même fréquence peuvent interférer avec la transmission d'une manière similaire à celle des brouilleurs, voire la perturber complètement.

Mécanismes techniques de sécurité pour un réseau WLAN

Le chiffrement WPA2 est la technique de pointe actuelle. Les anciennes méthodes de chiffrement (WEP et WPA) ne doivent plus être utilisées, car elles ne sont pas sécurisées et sont faciles à déchiffrer. Le mot de passe et le SSID par défaut doivent être modifiés, et le SSID doit être masqué.

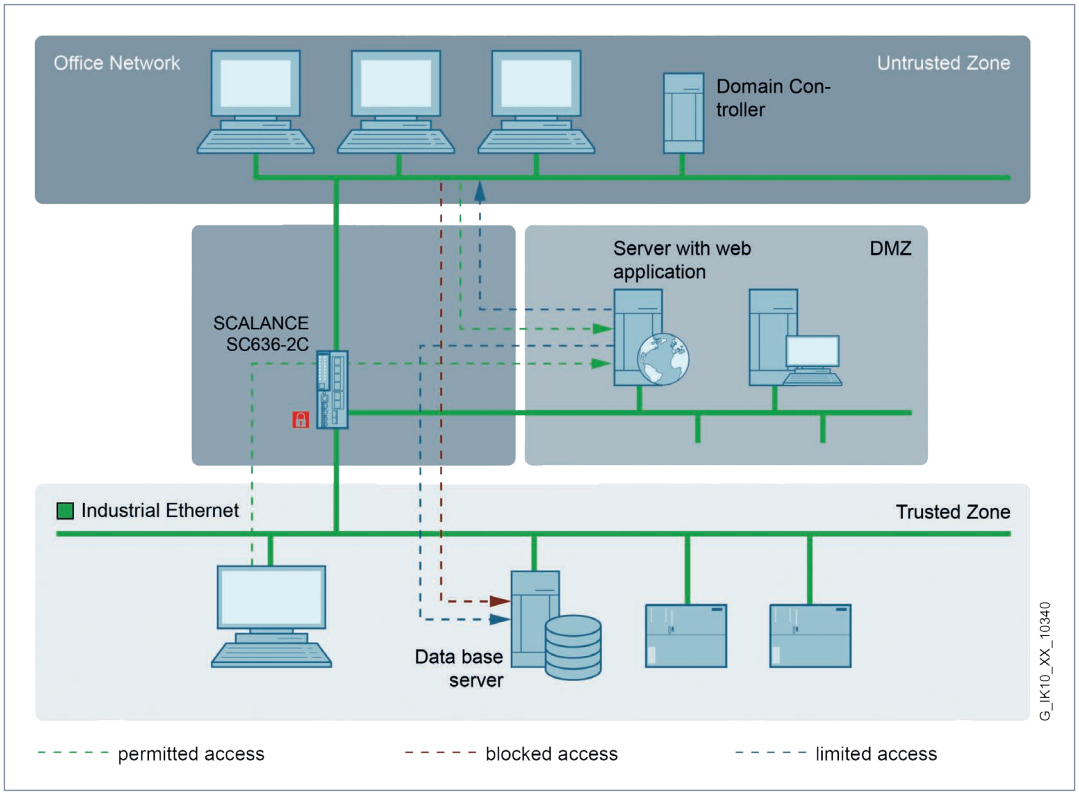

Schéma 6 : connexion d'un PC de service local via un port DMZ sur SCALANCE S615

Exigences générales pour les éléments de réseau

Selon la norme CEI 62443, la norme internationale pour la configuration et la gestion sécurisées des composants réseau recommande les spécifications et mécanismes de sécurité suivants pour la configuration et la protection des dispositifs.

Protection de l'accès et gestion des comptes
Pour protéger les composants du réseau contre les accès non autorisés, il doit être possible de gérer et, si nécessaire, de bloquer les comptes pour lesquels l'accès a été activé.
Les fonctionnalités suivantes doivent être prises en charge :

- Configuration des options d'accès
- Identification des utilisateurs/configuration permettant de rendre les utilisateurs identifiables au moyen de comptes
- Configuration/modification/annulation des comptes par le biais d'un gestionnaire central
- Documentation des comptes et des utilisateurs de comptes
- Suppression ou verrouillage des comptes inutilisés
- Vérification régulière des droits d'accès
- Modification des mots de passe par défaut

Les exigences en matière de protection de l'accès peuvent être mises en œuvre à l'aide de composants de gestion des utilisateurs (UMC). Avec les UMC, différents comptes utilisateurs sont créés sur un serveur central appelé serveur en anneau UMC. Les projets TIA Portal peuvent se servir de ces utilisateurs, et ces utilisateurs peuvent se voir accorder des droits d'accès aux composants et aux participants du réseau.

Contrôle d'accès : authentification
Lors de l'accès à un composant, il doit être possible d'identifier l'utilisateur qui y accède. L'authentification doit assurer les mécanismes suivants :

- Accès possible uniquement si l'utilisateur a été authentifié (ou s'il existe un contrôle d'accès suffisant)
- Mécanismes de sécurité renforcés pour l'accès administratif
- Enregistrement de tous les accès aux systèmes essentiels
- Identification de tous les utilisateurs de l'accès à distance
- Directives pour l'accès à distance, déconnexion automatique suite à une période d'inactivité
- Accès à distance verrouillé suite à des échecs de connexion répétés
- Réauthentification lors d'un accès à distance suite à une période d'inactivité
- Un mécanisme d'authentification doit également être mis en place pour la communication de tâche à tâche

Ces exigences concernent différents systèmes et doivent donc être prises en compte pour l'ensemble de l'usine. En ce qui concerne l'accès à distance, par exemple, les exigences peuvent être remplies par SINEMA Remote Connect car, entre autres, la déconnexion automatique suite à une période d'inactivité et le verrouillage d'une adresse IP après plusieurs tentatives de connexion infructueuses sont déjà mis en œuvre, et les accès à distance sont toujours enregistrés. Dans TIA Portal, les utilisateurs peuvent se voir accorder l'accès à un projet, ainsi qu'un accès distinct à la configuration de sécurité. Puisque la configuration de sécurité nécessite ses propres droits d'accès, l'exigence d'une sécurité supplémentaire pour l'accès administratif est également satisfaite.

Contrôle d'accès : autorisation

L'autorisation consiste à accorder des droits spécifiques à des utilisateurs préalablement authentifiés, par exemple l'accès à un composant. La norme CEI 62443 mentionne les points suivants en ce qui concerne l'autorisation :

- Méthode logique ou physique pour l'autorisation d'accès
- Accès basé sur les rôles au système ou aux informations
- Les droits d'accès aux dispositifs de sécurité doivent être distincts
- Plusieurs niveaux d'accès doivent être configurés pour les systèmes essentiels

Gestion du réseau
SNMP, qui est désormais pris en charge par toutes les interfaces réseau, peut être utilisé pour la gestion du réseau. SNMP peut être utilisé en conjonction avec le serveur SINEMA pour surveiller le réseau et les sections de l'usine connectées par le biais d'un VPN. Cela permet de gérer toutes les sections du réseau et de détecter plus rapidement les pannes.

Plan du réseau
Un plan du réseau physique, c'est-à-dire une vue topologique, est nécessaire pour documenter l'usine et montrer comment les participants sont interconnectés. Ce plan du réseau doit indiquer les adresses (IP et MAC), les connexions des ports et les sites de l'usine. Il peut être imprimé à partir de TIA Portal ou l'outil de planification de réseau SINETPLAN peut être utilisé.

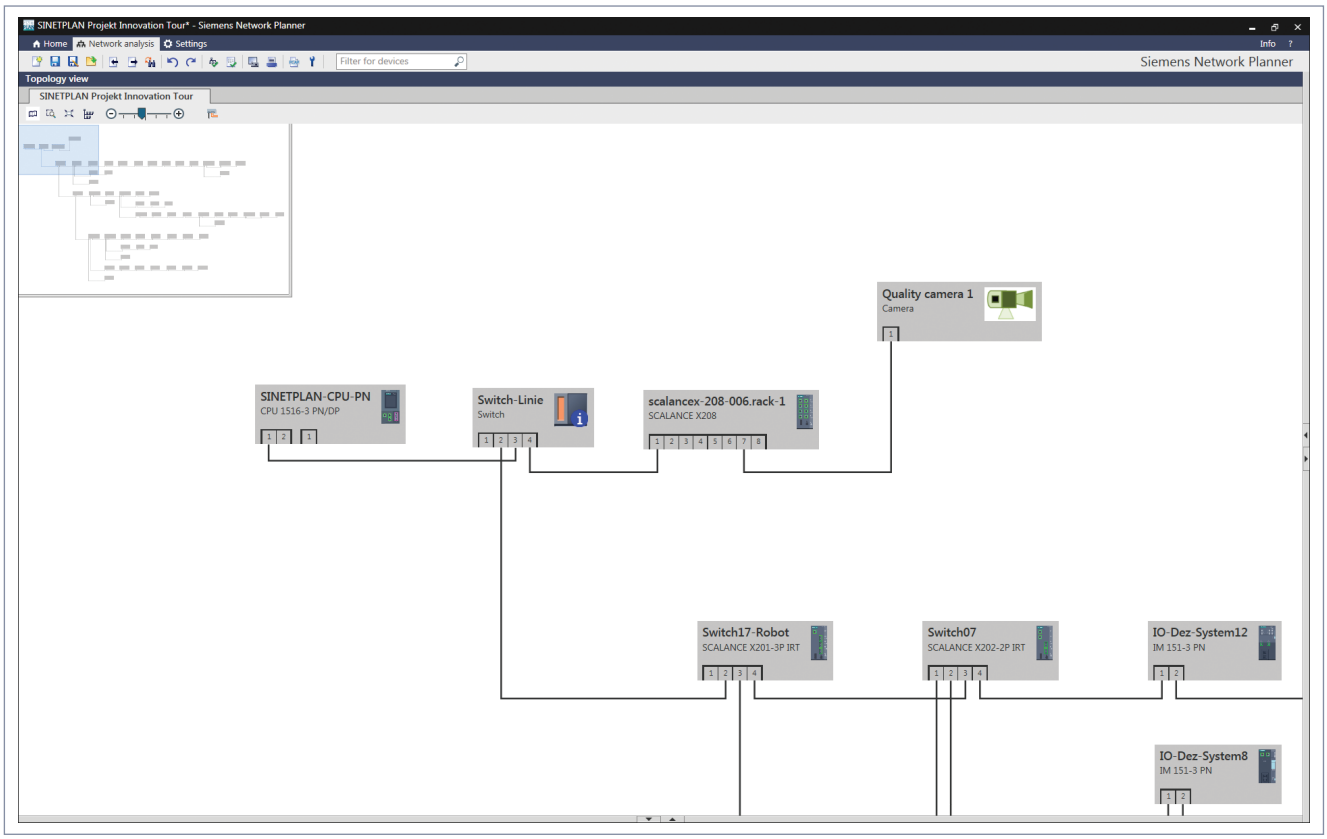

Schéma 7 : réseau topologique dans SINETPLAN

Mesures liées à l'intégrité du système

L'intégrité du système signifie que l'authenticité des données et des programmes d'un système sont garanties. Personne n'est autorisé à modifier le programme ou à altérer les données (que ce soit au sein du canal de communication ou du système), ou encore à copier le programme ou les données sans autorisation. L'expertise en matière de contrôle des procédés doit également être protégée.

Accès au programme
La programmation des contrôleurs (PLC) fait également partie de la cybersécurité, c'est pourquoi l'accès au projet et aux bureaux doit être protégé. Le projet peut généralement être protégé à l'aide du journal Windows. À partir de TIA Portal V15, l'ensemble du projet peut être chiffré. Cela signifie que le projet ne peut être ouvert qu'à l'aide d'un nom d'utilisateur et d'un mot de passe supplémentaires, ce qui garantit la sécurité lorsque plusieurs personnes travaillent simultanément sur le même projet.

Protection de l'accès au processeur
Différents mots de passe peuvent être configurés en fonction des différents niveaux d'accès au processeur, afin que seul le personnel qualifié dispose d'un accès complet.

Serveurs web
De plus en plus de solutions de contrôle ont recours à l'accès via des serveurs web, qui sont souvent également utilisés pour l'accès à distance. Dans ce cas, les serveurs web doivent également être entièrement protégés. HTTPS, la version sécurisée de HTTP, et est la solution recommandée. L'authentification et l'autorisation requises par la norme du secteur peuvent être obtenues en configurant différents utilisateurs et différents niveaux d'accès.

Communication sécurisée
Si le contrôleur communique en dehors de sa cellule sécurisée, cette communication doit être chiffrée. La technologie de pointe est actuellement le chiffrement TLS, qui peut être utilisé dans le contrôleur S7-1500 via OPC UA ou une connexion TCP.

Une autre option de chiffrement consiste à utiliser des pare-feu intégrés pour configurer une connexion VPN. Le tunnel VPN est établi entre les pare-feu, et la communication entre les cellules d'automatisation est transmise via le réseau de niveau supérieur sous une forme chiffrée et déchiffrée par le réseau cible.

Mesures de sécurité sur les PC industriels
Les PC utilisés dans un environnement industriel (IPC) nécessitent des mesures spéciales, car ils sont directement exposés à plusieurs menaces, notamment des dispositifs de stockage infectés, alors que les clés USB ne peuvent pas être directement connectées à un contrôleur. Les mesures suivantes servent à renforcer un IPC contre les attaques de cybersécurité.

Comptes utilisateurs
Il est conseillé de configurer des comptes administrateur et utilisateur. Seul l'administrateur est autorisé à modifier les paramètres de sécurité ou à (dés)installer des logiciels. L'utilisateur standard n'est pas en mesure d'exécuter ces fonctions, ce qui empêche l'installation de logiciels malveillants au cours des opérations normales.

Configuration des directives
À l'aide de la console de gestion Microsoft, des directives peuvent être établies pour l'utilisation des dispositifs de stockage et le contrôle du système, entre autres. Un document décrivant ces directives et la façon dont elles peuvent être établies est disponible en ligne à l'adresse suivante : support.industry.siemens.com/cs/ww/en/view/109475014

Filtre d'écriture amélioré (EWF)
Cette fonctionnalité est disponible sur les IPC SIMATIC : elle protège une partie du système de fichiers contre la modification des données en redirigeant l'accès en écriture vers la RAM. Lorsque l'IPC est redémarré, le système de fichiers revient à son état d'origine. Les logiciels malveillants introduits ne sont alors plus présents après un redémarrage.

Pare-feu
Les pare-feu standard (pare-feu Windows) offrent déjà une protection de base importante. Ils doivent absolument rester activés. À l'aide de règles appropriées, les pare-feu doivent être configurés de manière à ce que seules les données des utilisateurs puissent être communiquées et que toutes les autres communications soient bloquées.

Protection contre les virus
Les logiciels antivirus peuvent détecter les virus et les logiciels malveillants. Siemens utilise une installation McAfee pour son automatisation. Un serveur d'administration gère les clients antivirus sur les systèmes PC et fournit les signatures de virus les plus récentes. Le serveur de gestion peut également avertir le personnel de service par le biais d'alarmes envoyées par e-mail.

Produits certifiés CEI 62443
Les contrôleurs, PC et autres systèmes sélectionnés pour l'utilisation doivent contenir des mécanismes de sécurité et ils doivent avoir fait l'objet de tests pour en détecter les vulnérabilités. Ces tests sont standardisés : par exemple, un certificat Achilles indique que le système a subi des tests de charge et de vulnérabilité. Les fabricants peuvent également effectuer un développement de produits sécurisé pour garantir un haut niveau de qualité pour leurs produits. Le processus de développement de Siemens a été testé et a satisfait aux conditions du test CEI 62443-4 : siemens.com/press/PR2016080373DFEN

Mesures relatives au personnel

Les meilleures mesures de sécurité techniques et organisationnelles sont inutiles si les employés d'une entreprise font preuve de négligence. C'est pourquoi des formations et des définitions claires des domaines de responsabilité font partie intégrante de la cybersécurité. La norme CEI 62443 recommande que les nouveaux employés fassent l'objet d'une sélection afin de déterminer leur fiabilité et d'évaluer s'ils sont en mesure de s'acquitter de leurs responsabilités. La fiabilité du personnel existant doit également être évaluée. Le personnel externe peut également suivre des formations, mais il doit toujours être accompagné et supervisé par des employés formés de l'entreprise.

Responsabilité
La norme du secteur exige que les opérateurs d'infrastructures essentielles (CRITIS) désignent l'organisation UP KRITIS comme leur contact en matière de cybersécurité. Il est généralement recommandé qu'une personne ou un groupe soit responsable de la cybersécurité au sein de l'entreprise.

Formation
Des formations régulières doivent être proposées pour couvrir la manipulation correcte des systèmes installés, des dispositifs de stockage amovibles et des logiciels. Il est également recommandé de proposer une formation sur la manière de réagir aux incidents et à toutes les autres menaces potentielles. La norme du secteur exige explicitement que les administrateurs soient formés à la manipulation correcte des composants réseau afin veiller à ce que les configurations soient correctement effectuées.

Plan d'urgence et restauration

La norme du secteur exige que les entreprises disposent d'un concept permettant de gérer une urgence lorsqu'une menace est apparue et que le processus a été interrompu. Ce concept est également connu sous le nom de gestion de la continuité des activités. Il sert à répondre aux questions suivantes :

- Quel est le temps d'arrêt maximal acceptable ?
- Comment le processus peut-il continuer à fonctionner indépendamment du système/bureau de contrôle ?
- Dans quelle mesure d'autres sections de l'usine peuvent-elles compenser l'approvisionnement ?
- Comment le système concerné sera-t-il modifié ?
  - Par le biais de redondances
  - Par le biais d'une sauvegarde
- Comment éviter que cette défaillance ne se reproduise ?
  - Rapports
  - Optimisation

Siemens ProductCERT
Siemens dispose d'une équipe d'experts en sécurité qui sert de point de contact pour les clients et leurs experts en sécurité lorsqu'ils détectent une faille de sécurité. Cette équipe, appelée Product Computer Emergency Response Team (ProductCERT), évalue et analyse immédiatement les vulnérabilités de sécurité signalées.

Avis de sécurité Siemens
Siemens ProductCERT étudie tous les problèmes de sécurité signalés et publie des avis de sécurité concernant les vulnérabilités de sécurité validées qui impliquent directement les produits Siemens et nécessitent une mise à jour logicielle, une mise à niveau logicielle ou une autre action de la part de l'exploitant de l'usine. Tirez parti de cette source d'informations pour évaluer les effets d'une faille de sécurité. Siemens traite ouvertement ses propres vulnérabilités pour vous permettre de réagir avant que ces vulnérabilités ne vous affectent. Restez informé en vous abonnant à nos flux RSS : siemens.com/global/de/home/produkte/services/cert.html#Benachrichtigungen

Vue d'ensemble

Pour bénéficier d'une sécurité industrielle complète, il est nécessaire de prendre en compte tous les niveaux de protection. Les mesures de sécurité doivent être aussi variées que les risques potentiels. Une approche de bout en bout, ainsi que plusieurs lignes de défense, peuvent protéger les installations industrielles de manière fiable. Pour simplifier ce problème complexe auquel l'industrie doit faire face, Siemens propose un portefeuille de solutions personnalisées spécifiquement destinées à la sécurité des installations industrielles et des technologies opérationnelles.

Le schéma ci-dessous représente une architecture de réseau typique pour une usine de boissons non alcoolisées. Il indique les niveaux auxquels les mesures de sécurité décrites dans le présent document ont été mises en œuvre conformément aux recommandations de la norme CEI-62443.

Pourquoi Siemens ?
Siemens offre une base fiable pour des solutions d'automatisation sûres et innovantes.

Chez Siemens, nous :

- comprenons le numérique ;
- comprenons l'industrie agro-alimentaire ;
- comprenons la communication industrielle ;
- comprenons la sécurité industrielle ; et
- proposons des processus et des produits de sécurité éprouvés et certifiés

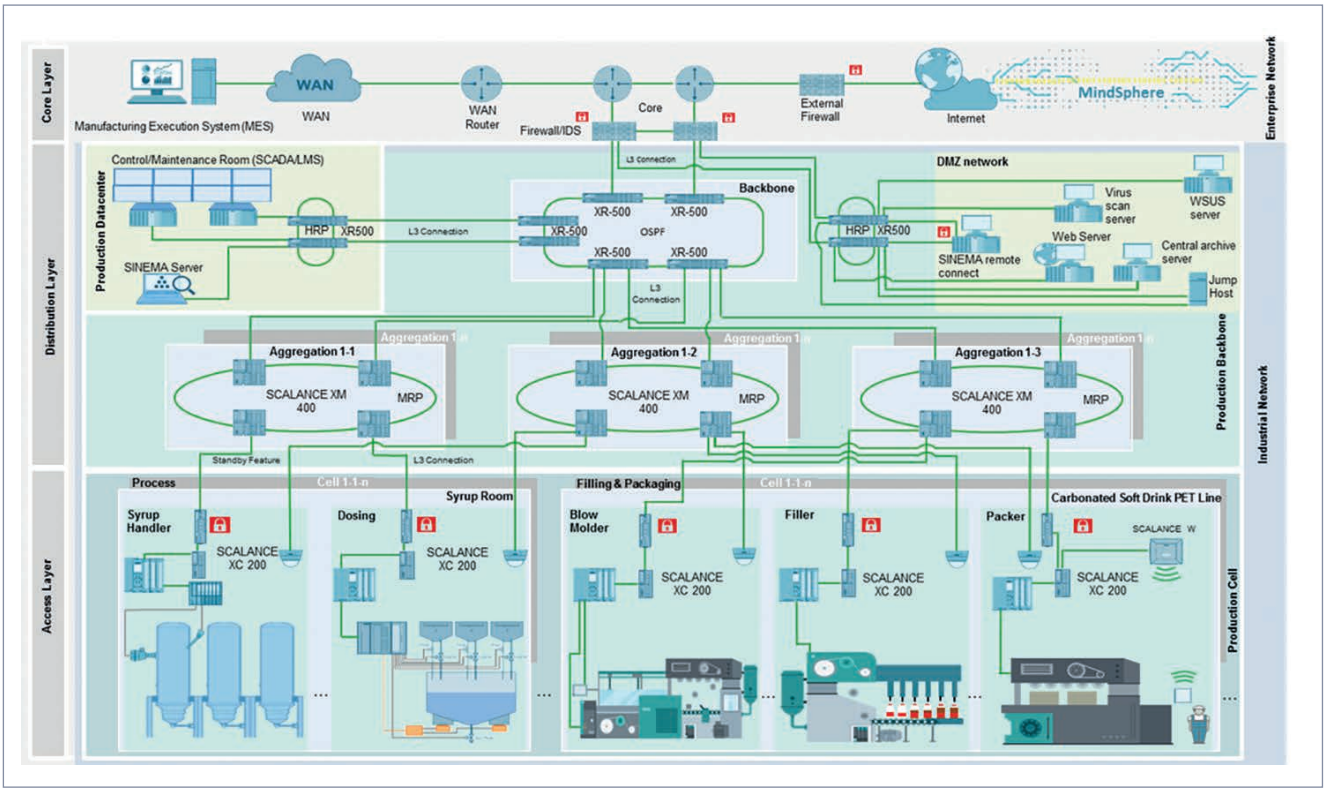

Schéma 8 : architecture réseau d'une usine de boissons non alcoolisées

Termes et abréviations

Authentification
La détection et l'identification d'un utilisateur ou (dans le cas d'usines en réseau) d'un autre système.

autorisation
Le droit d'accéder à un système ou à une section (logiciel) d'un système ou d'un programme.

Cybersécurité
Toutes les mesures techniques de protection d'une usine, y compris la protection du réseau, le renforcement du système et la surveillance des incidents.

Processus
Le processus de production proprement dit, par exemple la production du fromage ou l'embouteillage des boissons, qu'il s'agisse d'un processus discret ou continu.

Réseau privé virtuel (VPN)
Un VPN fournit une connexion chiffrée entre ses abonnés. On l'appelle aussi un groupe VPN. Un VPN s'assimile à un tunnel, par le biais duquel le trafic de données peut être envoyé dans les deux sens. Dans ce tunnel, le trafic de données est transmis sous une forme chiffrée et au bout du tunnel, c'est-à-dire sur l'autre dispositif VPN, il est livré sous une forme déchiffrée. Les terminaux n'ont pas besoin de prendre en charge le chiffrement, car celui-ci est effectué par les dispositifs VPN.

Publié par
Siemens SA

Industries numériques
Automatisation d'usine
Ventes secteur agro-alimentaire
Lindenplatz 2
20099 Hambourg
Allemagne

Pour de plus amples informations,
merci de prendre contact avec nous.
Adresse e-mail : fb.communications@siemens.com

Article N° VRFB-B10060-00-7600

Pour les États-Unis publié par
Siemens Industrie Inc.

100 Technology Drive
Alpharetta, GA 30005
États-Unis