Sûreté

PILZ
THE SPIRIT OF SAFETY

Livre blanc

Exclusion de la garantie

Nous avons composé notre livre blanc avec beaucoup de soin. Il contient des informations sur notre entreprise et sur nos produits. Toutes les informations sont données conformément à l'état actuel de la technique et en notre âme et conscience. Toutefois, nous déclinons toute responsabilité sur la conformité et l'intégralité des informations données, dans la mesure où l'on ne nous reproche pas des négligences grossières, car, malgré tout le soin apporté, une erreur est toujours possible. En particulier, les données n'ont pas la valeur juridique de garanties ou de propriétés garanties. Nous acceptons volontiers toute suggestion relative aux éventuelles erreurs.

Droits d'auteurs

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern,
Allemagne

1re édition

Aperçu

En raison de la digitalisation des usines, les installations sont de plus en plus connectées en réseau. Cette évolution accroît également le risque d'espionnage ou de détournement de données stratégiques. Auparavant, dans le secteur des automatismes, les communications s'effectuaient principalement via des bus de terrain CAN et propriétaires, autrement dit des protocoles spécifiques au fabricant. Pour occasionner des dégâts, une personne malveillante devait pénétrer à l'intérieur du site de production ou s'attaquer à un ordinateur via une ligne téléphonique équipée d'un modem. Or, ces protocoles étant de plus en plus souvent remplacés par les protocoles Ethernet et IP, des attaques peuvent désormais également être perpétrées via internet.

Les motifs sont multiples : projets terroristes, espionnage industriel, sabotage d'installations, voire demandes de rançon. La tâche des assaillants est facilitée par le fait que le secteur des automatismes emploie de plus en plus fréquemment des logiciels open source et des composants logiciels grand public. Mais ces ressources comportent des failles connues des auteurs des attaques. Par conséquent, la sûreté, et donc la protection des données, fait l'objet d'une attention croissante.

Néanmoins, l'expérience montre que cette nécessité n'est pas encore parfaitement comprise de tous. Pour y remédier, le présent livre blanc explique les principaux aspects de la sûreté et présente les solutions qui ont fait leurs preuves sur le terrain. Son but est d'aider, par exemple, les fabricants de machines, les concepteurs d'installations, les installateurs et les opérateurs de maintenance à identifier le rôle joué par leurs produits ou services dans les stratégies de sûreté de leurs clients, ainsi que les points auxquels ils doivent prêter attention. La question de la sécurité fonctionnelle est également abordée. En effet, la sûreté et la sécurité sont deux aspects d'une même problématique et constituent à ce titre la clé de la sécurisation des processus de fabrication.

Sommaire

1. Sûreté et sécurité 5
1.1. Définition 5
1.2. Interactions 5

2. Importance de la sûreté dans l'automatisation 6
2.1. Objectifs 6
2.2. Bien plus que la sécurité informatique 6
2.3. Conséquences sur le cycle de vie des installations 7

3. Les différentes formes de menaces 7
3.1. Attaques externes 7
3.2. Attaques internes 8
3.3. Violations accidentelles de la sûreté 8

4. Appréciation de la sûreté 9
4.1. Principes normatifs 9
4.2. Analyse des phénomènes dangereux 10
4.3. Contre-mesures 11

5. Mise en œuvre de stratégies de sûreté 12
5.1. Pare-feu 12
5.2. Segmentation du réseau 13
5.3. Defense In Depth 14
5.4. Mesures organisationnelles 15
5.5. Formations 15

6. Résumé et perspectives 16

Glossaire 17

Répertoire des illustrations 19

1. Sûreté et sécurité

1.1. Définition

Auparavant, la sûreté relevait presque exclusivement du domaine de l'informatique classique (IT). Aujourd'hui, en revanche, l'univers de l'informatique et le monde des automatismes sont toujours plus dépendants l'un de l'autre. Par conséquent, le degré d'interconnexion des installations de fabrication et l'utilisation de protocoles standard tels qu'Ethernet pour le transfert physique des données ne cessent de croître. Par ailleurs, les protocoles standardisés tels qu'OPC UA permettent d'accéder aux systèmes de commande via les systèmes informatiques : la communication de données est encore plus ouverte.
Dans le domaine des automatismes, la notion de sûreté désigne avant tout la protection des machines et des installations contre un accès non autorisé depuis l'extérieur, ainsi que la protection des données sensibles contre la falsification, la perte ou l'accès non autorisé au niveau interne. Les menaces proviennent du cybermonde, dont font partie internet ainsi que l'ensemble des technologies d'information et de communication modernes. Elles commencent au niveau du contrôle des accès à la porte de l'usine et vont jusqu'à la protection contre les attaques des hackers. Cependant, comme l'explique Ralph Langner, expert allemand en sécurité informatique, ce ne sont pas toujours les « méchants » qui provoquent des dégâts. En effet, de nombreuses violations de la sûreté ont lieu sans intention malveillante, notamment via des erreurs de manipulation des employés et collaborateurs.
Le terme « sécurité » désigne la sécurité fonctionnelle des installations, et donc la protection de l'homme et de l'environnement contre les menaces prévisibles pouvant provenir des machines. Les risques résiduels, qui sont toujours plus ou moins présents, ne doivent pas dépasser des valeurs raisonnables. Pour garantir cette protection, des composants tels que des relais de sécurité et des capteurs de sécurité sont notamment mis en place. En cas de problème, leur rôle consiste à veiller à ce que la machine passe à un état de sécurité ne posant aucun danger pour l'homme, la machine et l'environnement.
Une fois que la sécurité fonctionnelle d'une machine était homologuée et déclarée conforme aux indications de la directive Machines, les utilisateurs de l'installation n'avaient plus à se soucier de la sécurité tant qu'aucune modification essentielle n'était apportée à la machine par la suite. Cette époque est désormais révolue. En effet, en raison des menaces issues du cybermonde, la sûreté est devenue un élément indissociable de la sécurité.

1.2. Interactions

Les processus de fabrication pouvant être interrompus par les fonctions de sécurité, les techniciens cherchent souvent à contourner ce problème de manière illicite, une situation que des mesures mécaniques, principalement, permettaient d'empêcher jusqu'ici. L'utilisation de vis scellées empêchant de retirer facilement les capteurs de sécurité est un exemple de ce type de mesures. Aujourd'hui, il est toutefois possible de procéder à de tels contournements via le réseau. Par exemple, lorsqu'une machine passe à l'état de sécurité en raison d'une barrière immatérielle, son programme peut être modifié de sorte que les données correspondantes ne soient pas plus analysées. La fonction protectrice est alors désactivée et la machine continue de fonctionner dans des situations dangereuses.
À l'opposé, les mécanismes de sécurité peuvent également être utilisés pour bloquer les machines de manière ciblée via le réseau. Pour cela, il suffit d'interrompre la communication des données. En effet, les mécanismes de sécurité vérifient de manière cyclique si l'abonné du

réseau est encore actif à l'autre extrémité de la connexion. En l'absence de réponse, la machine s'arrête. Les attaques DoS déjà mentionnées sont un autre moyen de bloquer les machines en provoquant une surcharge du réseau.
Les processus de fabrication ne sont toutefois pas les seuls à pouvoir être compromis via le réseau. D'autres dangers menacent également. Les mécanismes de sécurité qui contrôlent si l'entraînement d'une machine est activé ou non constituent un point d'entrée pour les personnes malveillantes. Lorsque ces mécanismes sont modifiés de sorte que l'entraînement fonctionne en continu, dans le pire scénario, une machine peut être détruite. C'est pourquoi la protection des biens d'investissements coûteux, tels que les éoliennes, est souvent doublée, voire triplée.

2. Importance de la sûreté dans l'automatisation

2.1. Objectifs

Dans le cadre des approches telles que l'Industrie 4.0, pour lesquelles la mise en réseau revêt une importance capitale, les menaces issues du cybermonde représentent un sérieux problème pour les entreprises de production. Certes, en principe, il est possible de protéger tous les processus informatiques, mais cette opération est complexe et coûteuse. C'est pourquoi il convient tout d'abord de déterminer les risques réels. En effet, une stratégie de sûreté doit toujours mettre en balance les coûts et l'utilité pour la productivité d'une entreprise.
La sûreté a pour objectif de garantir la disponibilité du réseau et des appareils, ainsi que l'intégrité et la confidentialité des données. Pour cela, les systèmes de commande diffusés doivent par exemple être protégés contre les attaques de type DoS, ainsi que contre les erreurs de manipulation et les défaillances des appareils et des logiciels. Pour interrompre les processus de fabrication, une autre possibilité consiste à détourner la transmission ou le stockage des données. C'est pourquoi l'intégrité de ces dernières est importante. De plus, la violation de la confidentialité des données peut avoir de lourdes conséquences, notamment en cas d'espionnage du programme utilisateur d'une machine dans le but de le recréer.

2.2. Bien plus que la sécurité informatique

Pour pouvoir contrer de manière flexible les scénarios de menace les plus divers, les stratégies de sûreté actuellement mises en œuvre intègrent plusieurs couches de protection. Le cœur de cette approche est constitué des composants d'automatismes. Vient ensuite le réseau via lequel ces composants peuvent communiquer les uns avec les autres ou avec un système ERP (Enterprise Resource Planning). La couche supérieure est constituée de l'usine qui est protégée de l'extérieur par un concept de pare-feu.
Toutefois, ces concepts ne suffisent pas à protéger intégralement les installations. En effet, comme nous l'avons déjà évoqué, les menaces peuvent également provenir de l'intérieur. Par conséquent, la protection physique contre l'accès illégitime aux appareils en réseau, tels que les pare-feu et les switchs, constitue la base de toute stratégie de sûreté. Pour éviter que ces appareils fassent l'objet de fraudes sur site, il faut absolument qu'ils ne soient pas en libre accès. Une mesure simple mais efficace peut par exemple consister à installer les appareils en réseau dans des armoires électriques ou des coffrets de distribution fermant à clé. Cela permet également de réduire le risque d'erreurs de maniement de la part du personnel non autorisé.

2.3. Conséquences sur le cycle de vie des installations

Les installations peuvent avoir un cycle de vie de 20 ans, voire plus. Jusqu'ici, elles étaient exploitées selon l'adage qui veut qu'« on ne change pas un système qui marche ». De fait, lorsqu'un mécanisme de sécurité devait être mis à jour, les systèmes de commande étaient normalement remplacés par un nouveau modèle du même type, car la sécurité fonctionnelle est garantie tant qu'aucune modification substantielle n'est apportée à la machine. Cette sécurité repose sur des modèles d'erreurs statistiques qui indiquent avec quelle probabilité un événement dommageable risque de survenir. En conséquence, quasiment aucune modification n'est apportée au fil du temps.
La sûreté, en revanche, est une « cible mouvante ». Contrairement à la sécurité, il ne s'agit pas de savoir, par exemple, que la probabilité d'une panne est de 1 sur 100 000, mais au contraire que le rapport peut être de 1:1 dès lors qu'une personne malveillante s'immisce dans un réseau. Par ailleurs, des méthodes toujours plus intelligentes sont élaborées pour contourner les mesures de défense, et les algorithmes jugés sûrs jusqu'ici ne le sont soudain plus du tout. Il y a quelques années de cela, l'utilisation de la norme Data Encryption Standard (DES) était une pratique courante. Aujourd'hui, le BSI (Bundesamt für Sicherheit in der Informationstechnik, office fédéral allemand pour la sécurité informatique) recommande de ne plus l'utiliser. L'algorithme de hachage MD5 a connu peu ou prou le même sort. De plus, avec les ordinateurs quantiques, il sera très prochainement possible de calculer les clés cryptographiques en seulement quelques minutes ou secondes, une opération qui prendrait une éternité avec les ordinateurs actuels.
La sûreté n'étant pas une grandeur physique, mais une cible mouvante, les mesures prises pour contrer les cybermenaces doivent être mises à jour en permanence. Cette responsabilité incombe en premier lieu aux exploitants des installations, pour qui la protection des données est également synonyme de protection des investissements. Grâce à une stratégie de sûreté efficace, ils peuvent en outre utiliser leurs installations plus longtemps qu'auparavant. À l'autre bout de la chaîne, les fabricants de machines et de composants sont contraints d'informer immédiatement les exploitants de tout nouveau problème de sécurité et de mettre à leur disposition les mises à jour requises pour les logiciels de leurs appareils afin de résoudre les failles. Toutefois, cela exige que les deux parties collaborent étroitement sur l'ensemble du cycle de vie des produits.

3. Les différentes formes de menaces

3.1. Attaques externes

Les réseaux d'automatismes basés sur Ethernet sont exposés à de nombreux scénarios de menaces qu'il est toutefois possible de catégoriser en fonction de leur point de départ. En effet, fondamentalement, il existe uniquement des attaques externes et internes ainsi que des violations de sûreté accidentelles dont les motifs varient.
Lorsque les réseaux sont attaqués depuis l'extérieur, l'intention sous-jacente est généralement malveillante. Les sabotages d'installations en font par exemple partie. Les conséquences éventuelles peuvent être illustrées par un exemple qui a certes été publié, mais sans citer de nom : après une attaque réussie menée contre un haut-fourneau en Allemagne, il a fallu détruire ce dernier, car les masses en fusion avaient durci.

L’espionnage industriel est un autre scénario de menace pouvant avoir des conséquences négatives. Lorsque des informations relatives aux produits ou au savoir-faire de la production sont espionnées, la compétitivité d’une entreprise peut être compromise. Cela vaut également lorsque des données financières confidentielles concernant des clients, des appels d’offres ou des commandes sont dérobées.
Pour récupérer les mots de passe et les données d’accès, les assaillants créent de faux sites internet et de faux e-mails ressemblant à s’y méprendre aux vrais. C’est ce qu’on appelle le phishing, ou hameçonnage. Lorsque les destinataires ne sont pas vigilants, la tâche est aisée pour les personnes malveillantes. C’est pourquoi il est important que les entreprises sensibilisent leurs employés au thème de la sûreté et mettent en place des directives devant être suivies par tous.
Ces derniers temps, les attaques perpétrées pour des motifs criminels sont de plus en plus fréquentes. La méthode de prédilection actuelle est un logiciel de rançon (ransomware) envoyé par e-mail pouvant se dissimuler dans des fichiers Word, PowerPoint ou Excel. Lorsqu’un destinataire ouvre ces fichiers, tous les fichiers présents sur l’ordinateur sont chiffrés. Par ailleurs, le malware peut se propager sur les autres appareils du réseau. La seule possibilité de récupérer les données consiste à payer une rançon.

3.2. Attaques internes

Bien que les attaques provenant de l’extérieur fassent toujours la une des journaux, les attaques internes sont tout aussi dangereuses. Dans ce cas, les stratégies de sûreté peuvent être contournées au sens propre du terme. Les intentions des assaillants sont plus ou moins les mêmes que pour les attaques externes : seule la procédure est différente.
Une possibilité consiste pour les assaillants à pénétrer dans l’entreprise et y rechercher une prise Ethernet libre afin de propager leur malware sur le réseau. Pour cela, une petite clé USB échappant au contrôle à la porte de l’usine suffit.
Bien plus souvent, les assaillants profitent toutefois du fait qu’en matière de sûreté, l’humain est le maillon le plus faible de la chaîne. L’ingénierie sociale est un exemple de méthode efficace pour tromper le personnel.
Elle consiste à gagner la confiance des employés et ainsi à les utiliser en tant qu’outils volontaires, pour ainsi dire. Elle nécessite au préalable des recherches approfondies, par exemple sur le site internet de l’entreprise où les noms et les fonctions des employés sont souvent disponibles. Le plus souvent, pour être considéré comme un membre de l’entreprise, il suffit même qu’un assaillant dise à un collaborateur qu’il a discuté avec le collègue X et que ce dernier lui a conseillé de s’adresser à lui.

3.3. Violations accidentelles de la sûreté

Cependant, la plupart des cyberincidents résultent non pas d’attaques internes ou externes, mais d’actes involontaires. Les conséquences peuvent être tout aussi graves que pour les deux autres types de scénarios de menace et peuvent notamment conduire à la défaillance de réseaux ou à la diffusion d’informations sensibles. Les principales raisons en sont des appareils incorrectement configurés et de mauvaises manipulations.
Par conséquent, les employés de la production, qui ne sont normalement pas experts en informatique, doivent être formés. Par ailleurs, les réseaux peuvent être configurés de telle sorte que les conséquences d’une mauvaise configuration ou manipulation des appareils soient limitées au moyen d’une segmentation, autrement dit une division en sous-réseaux, ainsi que par la mise en place de différents mécanismes de sûreté.

4. Appréciation de la sûreté

4.1. Principes normatifs

Dans l'informatique classique, la sûreté tient un rôle central depuis longtemps. Pour cette raison, il existe de nombreuses normes, telles que la série ISO/CEI 27000 « Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Vue d'ensemble et vocabulaire (ISO/CEI 27000:2016). Toutefois, leurs exigences ne peuvent pas être facilement transposées aux automatismes. En effet, dans l'univers des automatismes, la disponibilité des données est une priorité et une condition préalable essentielle au bon déroulement des processus de fabrication, tandis que pour l'informatique, c'est la confidentialité des données qui prime.
Afin de garantir des solutions de sûreté efficaces pour les automatismes, différentes organisations ont commencé à élaborer des normes correspondantes. Néanmoins, elles ne décrivent que des aspects spécifiques et limités, tels que la distinction entre la sûreté et la sécurité. De plus, elles n'existent ni sous la forme d'ébauches, ni sous la forme de normes officielles. Il s'agit donc plutôt de références techniques.
A contrario, avec la CEI 62443 « Réseaux de communication industriels – Sécurité des systèmes d'automatisation et de commande industriels », nous disposons d'une série de normes qui ont été en partie adoptées et qui traitent globalement de la sûreté informatique des automatismes. L'étendue des thèmes abordés va de l'analyse des phénomènes dangereux aux meilleures pratiques en passant par le développement sécurisé des produits (Security by

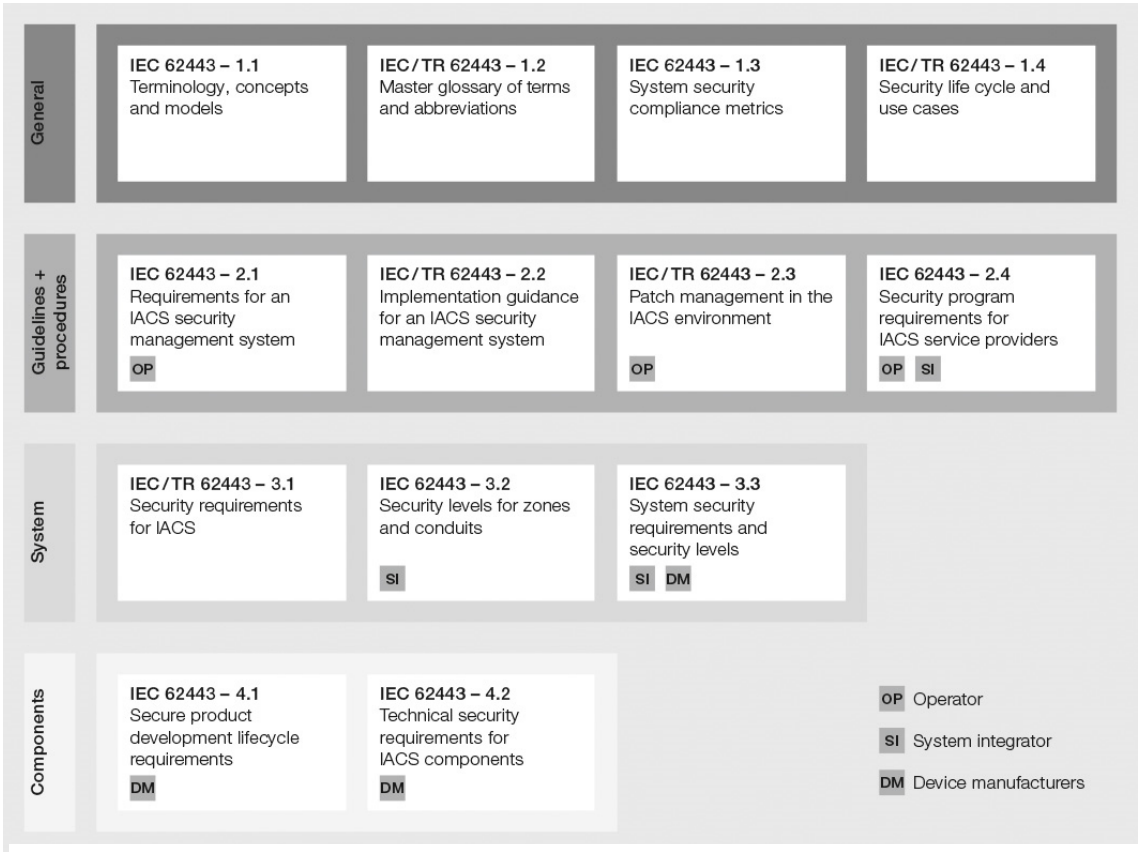


Illustration 1 : Norme CEI 62443

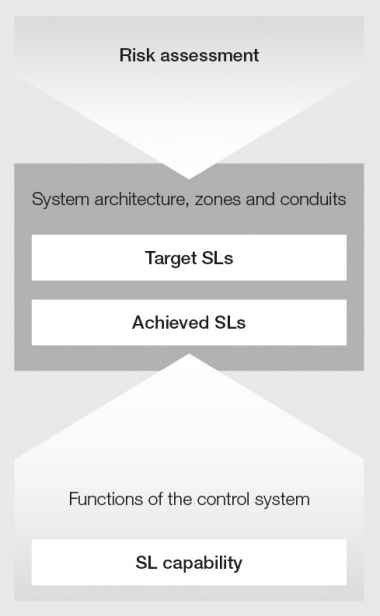
Design). Ainsi, la CEI 62443 propose aux exploitants d'installations et fabricants d'appareils les meilleures directives du moment pour une mise en œuvre efficace de la sûreté.
L'« ICS Security Kompendium » de l'office fédéral allemand pour la sécurité informatique s'adresse tout particulièrement aux exploitants de systèmes de commande industriels. Il explique aussi bien les principes fondamentaux que les exigences spécifiques et les normes applicables. D'autre part, il présente des mesures adaptées et les moyens de les mettre en œuvre.
Tandis que la CEI 62443 et l'« ICS Security Kompendium » s'adressent principalement aux experts, la directive VDI/VDE 2182 permet d'aborder plus simplement cette thématique en comparaison. Par ailleurs, différentes entreprises du secteur des automatismes ont publié des écrits qui atteignent parfois le volume d'un livre. En raison de la complexité de la sûreté industrielle, il est assurément recommandé de faire appel à des spécialistes extérieurs, au plus tard au stade de la mise en œuvre.

4.2. Analyse des phénomènes dangereux

Comme toute autre stratégie, une stratégie de sûreté commence par un état des lieux. Autrement dit, les exploitants d'installations doivent tout d'abord se faire une idée des menaces

Illustration 2 : Les différentes étapes de l'analyse des phénomènes dangereux

auxquelles ils sont exposés, ainsi que des valeurs de l'entreprise qu'ils souhaitent protéger en priorité. La deuxième étape consiste à définir cinq niveaux de sûreté conformément à la norme CEI 62443 sur une échelle allant de 0 (absence de risque) à 5 (risque extrême), ainsi que les différentes exigences qui s'appliquent à chacun d'entre eux. Néanmoins, la norme n'explique pas comment procéder concrètement.



Security Level	Protection
SL 0	No protection
SL 1	Protection against casual or coincidental violation
SL 2	Protection against intentional violation using simple means
SL 3	Protection against intentional violation using sophisticated means
SL 4	Protection against intentional violation using sophisticated means with extended resources

Illustration 3 : Évaluation du risque

Une règle empirique veut que tous les appareils dotés d'une connexion Ethernet soient considérés à risque. En effet, ils peuvent servir de porte d'entrée pour les attaques provenant de l'extérieur et de l'intérieur, ou de point de départ pour des violations accidentelles de la sûreté. En outre, lorsque des systèmes d'exploitation courants sont installés sur ces appareils, le risque augmente, surtout lorsqu'aucune mise à jour de sécurité n'est plus proposée pour ces derniers. Afin de déterminer comment ces systèmes peuvent être attaqués et quels malwares sont utilisés pour ce faire, une recherche sur internet suffit souvent.
Néanmoins, une analyse des phénomènes dangereux n'est qu'un « instantané » de la situation à un instant T. De nouvelles menaces peuvent survenir à tout moment et il convient alors de les intégrer. Alors que les processeurs étaient considérés comme non-critiques jusqu'ici, récemment, des failles de sécurité ont été détectées. Regroupées sous les appellations « Meltdown » et « Spectre », elles rendent de nombreux PC vulnérables aux attaques. Par conséquent, les systèmes API (systèmes de commande programmables par logiciel) sont également dans le viseur des assaillants. En bref : la sûreté est un processus de longue haleine.

4.3. Contre-mesures

Une fois les valeurs d'entreprise à protéger identifiées et priorisées (une attaque réussie contre un système de commande a normalement des conséquences plus lourdes qu'une attaque contre un outil de visualisation), il convient de décider des moyens à mettre en œuvre pour contrer ces menaces.

La voie royale consiste à empêcher les attaques et les violations accidentelles de la sûreté en les anticipant. En raison de la complexité et de la dynamique du sujet, ce n'est toutefois pas toujours réalisable. En effet, même si les spécialistes recherchent en permanence d'éventuelles failles dans le réseau, il n'existe aucune assurance couvrant toutes les éventualités.
Par conséquent, il faut identifier immédiatement les problèmes de sûreté et les gérer sans attendre. Pour cela, il est possible, entre autres choses, de consigner dans un journal tous les événements survenant sur le réseau (Event Logging) et de les analyser. Cela permet notamment de déterminer à quel moment précis un appareil donné a été attaqué. Par exemple, si des opérations de maintenance ont été effectuées à une heure inhabituelle, tous les signaux d'alerte doivent être au rouge.
Lorsque l'attaque a réussi ou que la protection des données a déjà été compromise par accident, le problème doit être réglé aussi vite que possible et sa cause doit être analysée en détail afin qu'il ne se reproduise pas à l'avenir.

5. Mise en œuvre de stratégies de sûreté

5.1. Pare-feu

La protection du réseau au moyen d'appareils spécifiques est une mesure permettant de mettre en œuvre des stratégies de sûreté. Bien que les routeurs et les switchs puissent également protéger les mécanismes de sécurité, les pare-feu jouent toujours encore un rôle central. Il s'agit de solutions logicielles ou de dispositifs (association de matériel et de logiciel) qui surveillent l'ensemble des flux de données au moyen de règles définies individuellement et de fonctions telles que l'inspection des paquets en profondeur (Deep Packet Inspection ou DPI) ou la détection des intrusions.
Les pare-feu nécessitant habituellement une configuration complexe, des compétences informatiques étendues sont nécessaires. Or, celles-ci font souvent défaut dans le domaine de la production. C'est pourquoi Pilz a développé, avec son SecurityBridge, un pare-feu adapté à l'industrie qui peut être mis en service facilement grâce à des préréglages propres à l'application sur le principe du Plug and Play. Avec lui, non seulement les systèmes de commande de Pilz sont protégés des attaques et des accès non autorisés, mais les données du process sont également transférées avec une latence réduite.
Toutefois, les appareils de sûreté les plus efficaces ne servent pas à grand-chose s'ils n'ont pas été développés de manière sûre dès le début et si cet aspect est négligé sur l'ensemble du cycle de vie. Dans ce domaine, le mot d'ordre est « Secure by Design » (sûr par conception). En effet, les processeurs peuvent ne plus être sûrs du jour au lendemain, comme le montre l'exemple de Meltdown et de Spectre. Qui plus est, il est parfaitement possible d'infiltrer un malware dans un processus de fabrication afin qu'il soit installé dans les produits et serve ensuite de porte dérobée pour des attaques. Pour couper court à ce type de scénario, les fabricants doivent surveiller le cybermonde en permanence à la recherche de nouvelles menaces et, si nécessaire, intégrer le plus rapidement possible des mécanismes de sécurité supplémentaires dans leurs appareils et mettre à disposition des correctifs (mises à jour de sécurité).

5.2. Segmentation du réseau

Classiquement, les pare-feu sont installés à la jonction entre un réseau sécurisé et un réseau non sécurisé, par exemple entre un intranet et internet. Cette protection dite « périmétrique » se heurte toutefois rapidement à ses limites, lorsqu'il s'agit d'empêcher qu'un malware se propage sur l'ensemble du réseau telle une épidémie et paralyse ce dernier tout comme les installations connectées.
C'est pourquoi la norme CEI 62443 prévoit de subdiviser les réseaux selon le modèle des « zones et conduits ».

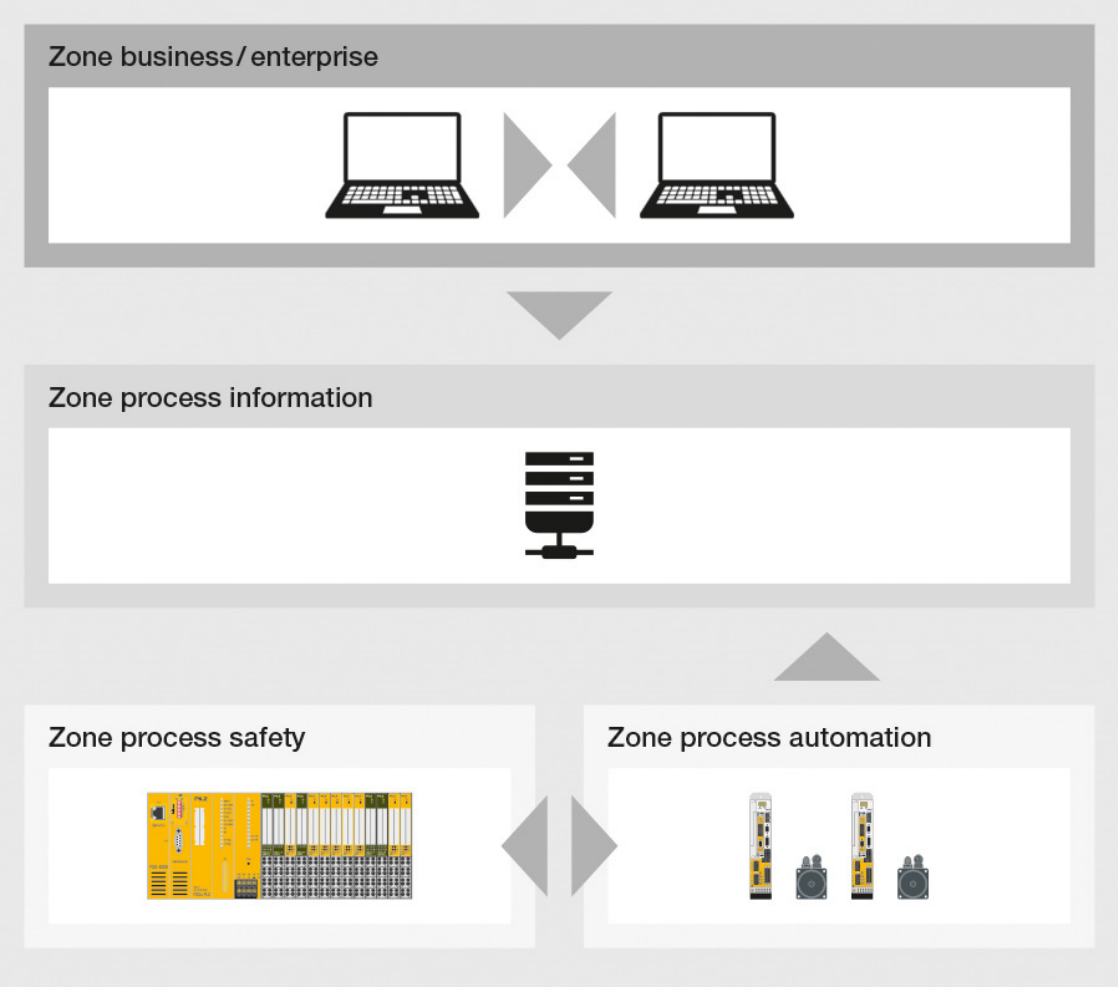


Illustration 4 : Modèle des zones et conduits

Selon ce principe, il est par exemple possible de séparer le réseau de gestion du réseau de production. Si nécessaire, ce réseau peut aussi être segmenté jusqu'à créer des cellules de production individuelles. Tout d'abord, il convient d'identifier des zones dans lesquelles les appareils présentent des exigences de sûreté similaires, puis de les isoler les unes des autres au moyen de pare-feu ou de routeurs sécurisés. Ainsi, seuls les appareils qui y sont autorisés peuvent envoyer et recevoir des données via les conduits entre les zones.
L'exemple suivant illustre ce que cela signifie dans la pratique : les violations accidentelles de la sûreté sont souvent causées par des appareils incorrectement configurés. Les conséquences peuvent être une transmission de données, ou ce qu'on appelle une « tempête de réseau », qui

risque de compromettre d'autres appareils. En revanche, lorsque les réseaux sont segmentés en sous-réseaux protégés, seuls les appareils situés dans la zone dans laquelle le problème s'est produit sont touchés. Cela vaut également pour les conséquences des attaques internes accidentelles ou délibérées.

5.3. Defense In Depth

Pour compliquer autant que possible la tâche des assaillants, le modèle des « zones et conduits » peut également servir d'élément central pour une protection approfondie (Defense In Depth) du réseau. Ce principe, appliqué lors de la construction des fortifications, implique de dresser en permanence de nouveaux obstacles sur le chemin des assaillants. Ainsi, au Moyen-Âge, certains châteaux forts étaient protégés par des douves, des trappes, des ponts-levis, des tours et plusieurs murs d'enceinte.
Les zones et les conduits d'un réseau correspondent aux portes d'un château fort. Les murs et les autres obstacles sont représentés par les pare-feu et les routeurs sécurisés qui protègent les différents mécanismes de sûreté. En font par exemple partie un contrôle d'accès conforme à la norme IEEE 802.1x et des listes de contrôle d'accès qui bloquent les appareils et protocoles inconnus. Par ailleurs, il existe des mécanismes qui déclenchent des alarmes en cas d'activités réseau suspectes ou qui détectent l'envoi de paquets IP avec des adresses d'expéditeur falsifiées (usurpation d'IP).

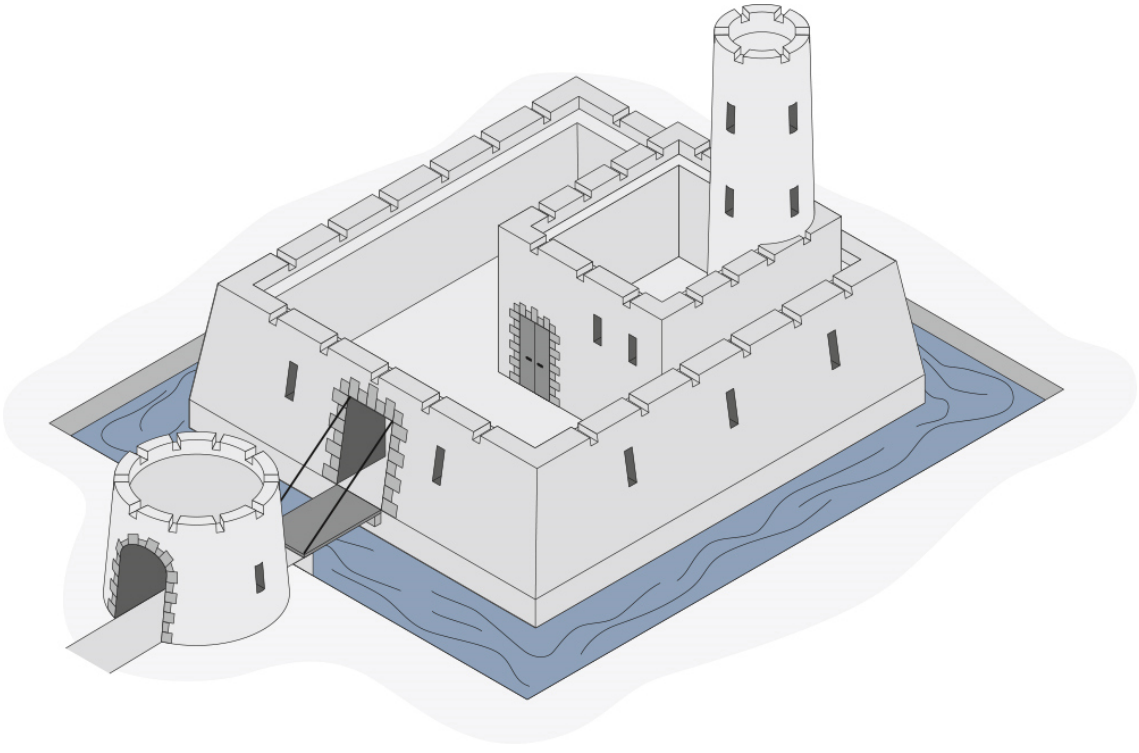


Illustration 5 : Château fort illustrant les différents niveaux de défense

Ce procédé permet de s'assurer qu'une méthode d'attaque seule ne puisse pas « réussir ». Pour s'immiscer plus profondément dans le réseau, un assaillant doit venir à bout de couches de protection qui se superposent. Et quand bien même il parviendrait à accéder au sous-réseau d'une cellule de production, il lui serait presque impossible d'attaquer des cibles situées dans les sous-réseaux voisins.

5.4. Mesures organisationnelles

Comme nous l'avons déjà évoqué, la protection des entreprises de production contre les menaces en provenance du cybermonde dépend toujours d'un équilibre entre les coûts et l'utilité. Par exemple, en Allemagne, conformément à la loi sur la sécurité informatique, seuls les exploitants d'infrastructures d'utilité publique, tels que les secteurs de l'énergie, des transports et de la santé, sont contraints de respecter ces mesures. Dans d'autres pays, il existe des directives légales comparables, notamment aux États-Unis pour la protection des réseaux électriques.
Étant donné le nombre important de menaces, de nombreux arguments plaident en faveur d'une protection des installations à la fois contre les violations délibérées et accidentelles de la sûreté. Mais, pour cela, des concepts de pare-feu sophistiqués ne suffisent pas à eux seuls. L'ensemble de la société doit pour ainsi dire intégrer le principe de la sûreté. De plus, il faut mettre en place des directives valables non seulement pour tous les employés, mais également pour les partenaires tels que les fabricants d'appareils et les prestataires de services.
Par ailleurs, il est important que les spécialistes de l'informatique et des automatismes travaillent main dans la main afin de se familiariser avec les différentes exigences et méthodes de travail des uns et des autres. Enfin, il convient de mettre en place une organisation dont les membres sont responsables de la protection des données de production, ainsi que de son amélioration continue. Dans l'idéal, cette organisation doit être dirigée par un responsable de la sûreté appartenant au niveau hiérarchique le plus élevé ou, au minimum, qui en dépend directement.

5.5. Formations

« Ceux qui cessent de s'améliorer cessent également d'être bons ». Telle est l'une des clés du succès que les entreprises devraient aussi appliquer en matière de sûreté. Des formations régulières permettant par exemple de sensibiliser davantage les employés sont l'une des possibilités pour y arriver. Les autres sources de connaissances peuvent être des informations sur les menaces actuelles ou des instructions sur les moyens à mettre en œuvre pour combler certaines failles de sécurité. Ce n'est qu'en améliorant les compétences en matière de sûreté qu'il est possible d'éviter que les employés prennent de mauvaises décisions en raison d'un manque de qualifications.
De nombreux prestataires proposent des formations à la sûreté. Les formations de Pilz, dispensées à notre siège d'Ostfildern près de Stuttgart et sur le site du client ou, dans un format plus condensé, sous forme de webinaires, s'adressent en particulier aux constructeurs de machines et aux concepteurs d'installations. Elles offrent une vue d'ensemble élémentaire et expliquent comment identifier et minimiser les risques. L'éventail de thèmes abordés va de l'architecture réseau à l'authentification des abonnés du réseau en passant par le chiffrement des données et la sécurisation de la maintenance à distance.

6. Résumé et perspectives

Pour atteindre un niveau de sûreté optimal, il convient avant tout de connaître précisément l'architecture du réseau ainsi que les protocoles de communication et le type de flux de données. En effet, c'est à ce prix qu'il est possible de contrer les attaques externes et internes, qu'elles soient délibérées ou accidentelles.
Autrefois, le thème de la sûreté relevait exclusivement de l'informatique classique. Depuis que, dans le sillage de l'Industrie 4.0, les installations de fabrication utilisent de façon accrue des produits grand public et des systèmes d'exploitation complexes, le secteur des automatismes doit également se pencher sur cette question. Les normes issues de l'informatique ne pouvant pas être appliquées à la lettre, de nouvelles normes sont apparues, parmi lesquelles la CEI 62443, qui est la plus importante. Celle-ci détermine comment développer et mettre en œuvre pas à pas une stratégie de sûreté complète pour le secteur industriel.
Parallèlement, ces stratégies doivent aussi intégrer la sécurité, car leurs fonctions ne peuvent être garanties que lorsque les données correspondantes sont transférées en toute fiabilité. En effet, les menaces pesant sur la sûreté évoluent en permanence, tout comme les contre-mesures. Par conséquent, bien que ces deux aspects des automatismes demeurent indépendants, ils doivent être étroitement adaptés l'un à l'autre. La bonne nouvelle, c'est que ceux qui sont familiarisés avec la sécurité auront des facilités avec la sûreté, car les procédures se ressemblent.

Glossaire

Liste de contrôle d'accès	Une liste de contrôle d'accès (Control Access List) détermine dans quelle mesure les individus, les ordinateurs ou les réseaux peuvent accéder aux routeurs ou aux switchs, et via quels services. L'accès peut être défini pour des ordinateurs ou des réseaux spécifiques et pour la méthode d'accès associée.
Tempête de réseau	Une tempête de réseau ou tempête de diffusion (broadcast storm) désigne l'accumulation d'une importante quantité de trafic de diffusion au sein d'un réseau informatique qui se solde par l'impossibilité d'établir de nouvelles connexions au réseau et l'interruption des connexions en cours. Une tempête de réseau peut survenir en raison d'une attaque, d'une mauvaise configuration ou d'une conception incorrecte du réseau.
Inspection des paquets en profondeur	L'inspection des paquets en profondeur (Deep Packet Inspection) désigne une procédure réseau qui consiste à surveiller et à filtrer les paquets de données. Elle permet notamment de lutter contre les courriers indésirables. De plus, l'inspection des paquets en profondeur peut être mise en œuvre pour contrôler les surcharges et réduire le flux de données.
DES (Data Encryption Standard)	La norme Data Encryption Standard ou DES est une procédure de chiffrement symétrique standardisée.
Système de détection des intrusions	La détection des intrusions permet de repérer précocement les attaques dirigées contre un système ou un réseau informatique afin de prendre rapidement des contre-mesures.
Usurpation d'IP	L'usurpation d'IP (IP Spoofing) désigne, sur les réseaux informatiques, la falsification des adresses IP des expéditeurs dans les paquets IP afin d'endosser une fausse identité auprès du système informatique attaqué. Chaque paquet IP contient l'adresse de son expéditeur dans ses données d'en-tête. Un assaillant peut falsifier cette adresse d'expédition dans les données d'en-tête de façon à faire croire que le paquet a été envoyé depuis un autre ordinateur. De nombreux protocoles de la famille TCP/IP peuvent uniquement être authentifiés à l'aide d'une adresse IP. Lorsque celle-ci est usurpée, les mesures de réduction des risques, telles que l'authentification basée sur l'adresse IP, peuvent être contournées sur le réseau. L'usurpation d'IP n'est qu'un type d'usurpation parmi d'autres. De nos jours, le terme « usurpation » désigne toutes les méthodes consistant à contourner les procédures d'authentification et d'identification qui permettent habituellement d'utiliser des adresses ou des noms d'hôte fiables dans les protocoles réseau.

Algorithme de hachage MD5	L'algorithme MD5 (Message Digest Algorithm 5) appartient au groupe des fonctions mathématiques unidirectionnelles. Cela signifie qu'il est très difficile de déduire le paramètre d'entrée à partir du résultat. L'algorithme MD5 permet de représenter une libre quantité de données d'entrées au moyen d'une valeur de 128 bits. Avec un algorithme de hachage, en principe, il est extrêmement difficile de trouver deux documents d'entrée renvoyant la même valeur de résultat (collision). Récemment, dans cet algorithme, des failles permettant à un assaillant de générer des collisions ont été identifiées.
Meltdown et Spectre	Meltdown et Spectre sont des failles de sécurité détectées dans des microprocesseurs qui permettent un accès non autorisé à la mémoire des process externes.
Norme réseau IEEE 802.1x	IEEE 802.1x est une norme réseau utilisée pour l'authentification des utilisateurs sur les réseaux IEEE-802. Cette norme fonctionne comme une instance de contrôle qui vérifie l'identité de l'utilisateur avant de l'autoriser à accéder au réseau LAN ou WLAN.
Objectif de sûreté : l'intégrité	Dans le cadre des données, l'intégrité garantit que les données et le fonctionnement d'un système sont toujours corrects. Lorsque l'intégralité est garantie, les modifications non autorisées ou passées inaperçues sont immédiatement détectées et exclues.
Segmentation des réseaux	La segmentation désigne la subdivision d'un réseau en entités plus petites. Ces entités sont alors couplées à des pare-feu ou d'autres appareils permettant de limiter la communication. Cette technique permet de limiter les conséquences des tempêtes de réseau ou d'autres événements « accidentels », ainsi que les conséquences des attaques.

Répertoire des illustrations

Illustration 1 : Norme CEI 62443 9
Illustration 2 : Les différentes étapes de l’analyse des phénomènes dangereux 10
Illustration 3 : Évaluation du risque 11
Illustration 4 : Modèle des zones et conduits 13
Illustration 5 : Château fort illustrant les différents niveaux de défense 14

Nous sommes représentés au niveau international. Pour plus de renseignements, consultez notre site internet
www.pilz.com ou prenez contact avec notre maison mère.

Maison mère : Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Allemagne
Téléphone : +49 711 3409-0, fax : +49 711 3409-133, e-mail : info@pilz.com, internet : www.pilz.com

PILZ
THE SPIRIT OF SAFETY