SIEMENS

Ingenuity for life*

Simatic magazine

Le magazine des produits d'automatisme et d'entraînement

N° 66 octobre 2016

Spécial Cybersécurité

*L'ingéniosité au service de la vie

siemens.fr

Sommaire

Siemens S.A.S. - Divisions DF & PD
Tél. : 01 85 57 00 00

Siemens S.A.S. Divisions DF&PD
40 avenue des Fruitiers 93527 Saint-Denis Cedex
Tél : 01 85 57 00 00

Rédactrice en chef : Fabienne Fremaux

Rédacteurs : Antoine Coutant, François Gérin, Pierre Etcheberry, Jean-Christophe Mathieu, Laurent Mismacque, Franck Noyaret, Isabelle Stoltz.

Directeur de la publication : Vincent Jauneau

Photos : Siemens SAS, Siemens AG

Tirage : 700 exemplaires

Marques de fabrique : SIMATIC

Siemens, acteur engagé contre les cybermenaces

En France, pas moins d'une vingtaine de cyberattaques d'envergure ont été recensées durant l'année 2015. Organisés et rigoureux, les pirates informatiques pénètrent les réseaux des piliers de l'économie de notre pays, friands des branches phares de l'énergie, des transports, des télécoms, des finances et de l'industrie.

Pour lutter contre cette menace sournoise, la France est désormais dotée d'un arsenal réglementaire, destiné à protéger ses infrastructures vitales. En témoigne l'article 22 de la loi de programmation militaire (cf. page 19) qui prévoit l'adoption de mesures de renforcement de la sécurité des opérateurs d'importances vitales et confère à l'ANSSI* de nouvelles prérogatives.

Acteur engagé dans la protection des systèmes sensibles, Siemens, qui vient de faire certifier 7 de ses sites de développement pour les produits des divisions Digital Factory & Process Industries and Drive, sur la base de la norme internationale IEC 62443-4-1, se démarque en tant que premier équipementier à avoir obtenu la certification et la qualification de sécurité émanant de l'ANSSI pour son automate SIMATIC S7-1500 (cf. page 4). Son commutateur industriel Ethernet Scalance XM400 a, quant à lui, obtenu la certification (cf. page 23).

Bien que proposant des produits dont le niveau de sécurité ne cesse de croître, Siemens s'évertue, en outre, à les mettre en service et à les maintenir dans des conditions de sécurité elles aussi en progression constante via des équipes formées et compétentes. Pour ce faire, la filiale française du géant allemand se base sur le référentiel de l'ANSSI concernant les prestataires d'intégration et de maintenance pour les systèmes industriels ; garantie d'un niveau de compétences particulièrement élevé.

Produits sécurisés, alliés à des mesures de mise en service et de maintenance optimisées, permettent à Siemens de s'imposer comme référent auprès des industriels soucieux de préparer sereinement l'homologation de leurs installations industrielles.

L'Industrie 4.0, un autre défi majeur que Siemens a déjà en grande partie relevé, et qui va générer un volume colossal de données, dont on estime encore difficilement la valeur réelle, est une proie de choix pour tout acteur malveillant. La collecte des données sur les installations, leur analyse ou leur exploitation sont autant d'étapes où l'exposition doit être réduite au minimum afin que les avantages envisagés ne se transforment en vulnérabilités.

A partir de ce constat, est-il encore bien utile de rappeler qu'on ne peut envisager de sereine 4ème révolution industrielle sans prise en compte de la cybersécurité ?

Alain Greffier
Directeur des BU Factory Automation et Control Products Usine du Futur

** Agence Nationale de Sécurité des Systèmes Informatiques*

> ***Retrouvez l'offre Siemens sur les salons ALL4PACK (Hall 5A – Stand 5AD049), du 14 au 17 novembre, et SMART INDUSTRIES, du 06 au 09 décembre, au Parc des Expositions de Paris Nord II Villepinte.***

emballage & manutention become / deviennent all4pack Paris
THE GLOBAL MARKETPLACE FOR PACKAGING | PROCESSING | PRINTING | HANDLING
14-17 NOV 2016 - PARIS NORD VILLEPINTE - FRANCE

SMART 2016 INDUSTRIES

SIMATIC S7-1500*
Premier automate Siemens à obtenir la certification et la qualification ANSSI

Avec son automate SIMATIC S7-1500, Siemens est devenu le premier équipementier pour systèmes industriels à obtenir une certification et une qualification de sécurité délivrées par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Cette qualification constitue une attestation d'un plus haut niveau de sécurité et de confiance pour les opérateurs d'importance vitale, les incitant à opter pour notre produit, recommandé à l'achat par l'ANSSI pour les besoins de l'Etat français, qui garantira une protection optimale de leurs infrastructures contre la cybermenace. »

La Certification de Sécurité de Premier Niveau (CSPN) prononcée par l'ANSSI le 25 avril 2016 (certificat ANSSI-CSPN-2016-5) atteste du niveau de sécurité offert à cejour par l'automate SIMATIC S7-1500 de Siemens. Soumis à une série de tests visant, d'une part, à éprouver ses fonctions de sécurité, et d'autre part, à rechercher des vulnérabilités, l'automate SIMATIC S7-1500 a démontré sa capacité à fournir un niveau plus élevé de confidentialité, de disponibilité et d'intégrité des installations qu'il équipe.
La qualification, prononcée le 10 mai 2016, atteste de la pertinence des fonctions évaluées pour les besoins de la sécurité nationale et de la confiance résultant des processus de développement au sein de Siemens. Elle précise les conditions d'emploi permettant notamment au produit de contribuer à la protection des infrastructures vitales.
L'ANSSI est la seule autorité apte à délivrer en France la certification et la qualification pour la sécurité des produits des systèmes industriels.
Grâce au concept « Security Integrated » de Siemens, les fonctions de sécurité de l'automate programmable SIMATIC S7-1500 concernées par ces labels sont notamment :

- la protection de la lecture et de la modification des blocs de programme par des personnes non autorisées ;
- la protection contre la copie du programme utilisateur ;
- la protection de l'automate contre la modification des données transmises (données

ingénierie pour la configuration et le programme utilisateur) ;
- la gestion des droits d'utilisateur : des droits d'accès distincts peuvent être attribués à différents utilisateurs grâce à plusieurs niveaux d'autorisation ;
- la protection du micrologiciel (firmware) contre une mise à jour frauduleuse.

Selon Vincent Jauneau, directeur des divisions Digital Factory et Process Industries and Drives chez Siemens France : *« Ce processus de certification et de qualification permet aux utilisateurs de renforcer la sécurité de leurs systèmes industriels et d'appréhender sereinement l'homologation de sécurité de leurs installations ».*

** Pour plus d'informations sur la cible de sécurité du SIMATIC S7-1518-4 et le rapport de certification, consultez le site de l'ANSSI : http://ssi.gouv.fr/certification_cspn/simatic-s7-1518-4-version-du-micrologiciel-1-83/*

La puissance sous TIA Portal en toute sécurité - SIMATIC S7-1500– Système innovant pour une productivité accrue

- Ingénierie intuitive et efficace
- Diagnostic système intégré
- Safety Intégrated (sécurité machine)
- Fonctions technologiques intégrées (motion, PID, Trace..)
- Security Integrated

Le concept Security Integrated pour le SIMATIC S7-1500 s'étend de la protection des blocs à la vérification de l'intégrité de la communication. Il permet à l'utilisateur de sécuriser ses applications.

Les fonctions intégrées pour la protection du savoir-faire permettent, par exemple, d'empêcher la reproduction des machines en interdisant les accès et les modifications non autorisés. La protection contre la copie consiste au verrouillage des blocs associé au numéro de série de la carte SD ou de la CPU.

La protection contre l'accès permet de protéger l'application contre toute modification non autorisée de la configuration. Des droits d'accès distincts peuvent être attribués à différents groupes d'utilisateurs grâce à divers niveaux d'autorisation. Des mécanismes spéciaux permettent enfin de détecter toute modification des données d'ingénierie afin de protéger, par exemple, les données transmises à l'automate contre les manipulations non autorisées.

L'utilisation d'un CP Ethernet (CP 1543-1) permet à l'utilisateur une protection d'accès supplémentaire par un pare-feu ou la possibilité d'établir des liaisons VPN.

CP 1543-1

TIA PORTAL V14
Un tremplin au service de l'industrie du futur

Avec la version V14, TIA Portal entre véritablement dans l'ère du numérique grâce à de nombreux atouts supplémentaires. Totally Integrated Automation couvre le plus large spectre de fonctionnalités connu à ce jour, sous un moteur unique alliant conception et gestion de production. Offre globale et cohérente, TIA Portal V14 mixe naturellement l'univers du numérique et l'environnement matériel.

Il y a 5 ans, lorsque TIA Portal est venu bousculer un univers composé de multiples ateliers logiciels, Siemens a introduit une vision globale des projets sur la base d'une interface unique et d'une base de données centrale. Depuis, TIA Portal n'a cessé d'évoluer afin de suivre la stratégie de développement dans laquelle s'est engagé Siemens depuis le début des années 2000. A lui seul, le slogan « Total Integrated Automation » résume bien cette stratégie. Cela explique aussi pourquoi, très tôt, Siemens a acquis et intégré de nombreux savoir-faire complémentaires à son métier initial.
Aujourd'hui, l'évolution de TIA Portal marque une étape concrète et donne du sens à plus d'une décennie de développements. Sa particularité ? TIA Portal V14 s'inscrit pleinement dans une thématique chère à Siemens : l'industrie du futur et le partage de données numériques. Sans aucun doute, TIA Portal V14 sera la star du salon Smart Industries 2016 auquel participera Siemens du 6 au 9 décembre à Paris Nord Villepinte.

Accès complet à l'automatisation numérique

TIA Portal V14 donne à présent un accès total à l'automatisation numérique sous tous ses aspects : ingénierie intégrée, planification numérique, PLM, MES...
En d'autres termes, il permet de concevoir les équipements, mais aussi de suivre la fabrication des produits jusqu'à la livraison chez le client.
TIA Portal s'interface à présent à Plant Simulation afin d'étudier précisément un projet en phase d'investissement. L'interfaçage avec NX permet aux fabricants de machines d'optimiser les phases de conception, tandis que Process Simulate donne à l'intégrateur comme à l'exploitant, les moyens de simuler les cellules robotisées. TIA Portal V14 est bien en capacité de présenter le jumeau numérique d'une machine et de le faire vivre en condition réelle de fabrication.
Dans le contexte de l'usine du futur, Siemens est actuellement le seul acteur au monde à présenter une offre complète couvrant toutes les étapes de conception et de fabrication allant du PLM au produit.

Constructeurs de machines et intégrateurs peuvent en bénéficier avec pour objectif :

- d'accélérer la mise sur le marché des produits grâce aux outils de simulation ;
- d'accroitre la productivité à l'aide des possibilités de diagnostic et des fonctions de gestion de l'énergie ;
- de bénéficier d'une plus grande flexibilité, bénéfice d'une collaboration plus efficace entre équipes.

Simulation multi automates

Les capacités de simulation offertes par TIA Portal V14 sont la conséquence d'une parfaite maîtrise des flux numériques. L'outil PLCSIM Advanced autorise la simulation non pas d'un automate, mais d'une installation complète mettant en jeu plusieurs automates. Le concepteur, tout comme l'exploitant, accèdent ainsi à un parfait jumeau numérique de l'installation.

Base de données vraiment unique

Pour sa part, l'outil Teamcenter (offre PLM) permet d'intégrer la totalité des fichiers dans une seule et unique base de données. Jusqu'alors, seules les données électriques et mécaniques étaient concernées. A présent, avec TIA Portal V14, les données liées aux automatismes peuvent aussi intégrer cette base de données unique.

La souplesse du cloud

Avec le TIA Portal Cloud Connector, le concepteur ou l'exploitant peuvent intervenir à distance sur la machine il suffit de lancer TIA Portal V14 hébergé sur le cloud privé de l'utilisateur. Il n'est plus nécessaire d'avoir TIA Portal installé sur son terminal.

Un outil unique pour approches multiples

TIA Portal tient ses promesses : au fil des versions, il intègre l'ensemble des composants techniques d'un projet d'automatisme : sécurité, sûreté, contrôle, IHM, entraînements, entrées/sorties déportées, contrôle de mouvement et distribution de puissance. Une interface unique permet de gérer les particularités de chaque composant, dans une base de données optimisée. De quoi réduire les temps d'ingénierie.

Travail collaboratif amélioré

Jusqu'alors, un projet pouvait être partagé, mais selon un schéma correspondant à un développeur par automate. A présent, avec TIA Portal Multiuser, plusieurs utilisateurs peuvent accéder à un même automate sur TIA Portal, améliorant ainsi les possibilités de travail collaboratif.

Diagnostic plus efficace

Complémentaire au diagnostic système, l'outil de diagnostic Prodiag permet de déceler des défauts process et d'identifier des erreurs au niveau de la machine ou de l'usine, afin de rapidement les corriger.

Génération automatique de code

Programmer les vues sur les pupitres prend un temps non négligeable en phase de conception. Avec l'option logicielle SiVarc sous TIA Portal, Siemens propose de générer automatiquement les interfaces homme/machine à partir du code automate. L'imagerie est alors directement attachée à la programmation de l'automate. A ce titre, l'interface TIA Portal Openness met à disposition des développeurs, les librairies permettant d'automatiser la conception des machines.

Fluidité et transparence de l'information

De façon native, TIA Portal permet d'accéder aux informations et au contrôle de la machine à tous les niveaux de l'entreprise, sur smartphone ou tablette, localement ou à distance. Des codes d'accès, et pour l'utilisation à distance le recours à un tunnel VPN, assurent la sécurisation des données et la cybersécurité des échanges.

Gestion de l'énergie

TIA Portal intègre le module SIMATIC Energy Suite grâce auquel il est possible de générer automatiquement le code automate de gestion des capteurs impliqués dans la mesure des paramètres énergétiques. L'outil délivre ensuite l'analyse énergétique de la machine. Energy Manager PRO assure pour sa part la visualisation des données énergétiques au niveau du SCADA. Ces outils facilitent l'application de la norme ISO 50001 en matière de transparence énergétique.

Une communication ouverte avec OPC UA

Nouveau standard de communication dans le monde des automatismes, OPC UA facilite l'intégration verticale vers le MES et l'ERP. Basé sur Ethernet TCP/IP, ce protocole universel non propriétaire est désormais implémenté sur les CPU SIMATIC S7-1500. Ainsi pourvues de ce protocole, les CPU deviendront de véritables objets connectés. TIA Portal V14 fournit maintenant toutes les fonctionnalités permettant de mettre en œuvre un serveur OPC UA de SIMATIC. Rappelons qu'OPC UA fait l'objet de liaisons chiffrées assurant l'intégrité des données lors des échanges.

Une télémaintenance rapide et sécurisée

Pour accroître la disponibilité des installations industrielles toujours plus complexes, les entreprises font de plus en plus le choix de la télémaintenance. La gestion centralisée assure des temps de réponse courts et l'intervention rapide d'un personnel qualifié dans le monde entier.

L'accès à distance est possible via un réseau local, mobile, DSL ou SHDSL

Disponibilité élevée et temps d'arrêt réduits : ces deux facteurs sont essentiels pour les sites de production d'une entreprise, souvent répartis aux quatre coins du monde. Le défi est encore plus grand pour les sites de moindre envergure ne disposant pas sur place d'un personnel technique qualifié. Pour garantir là aussi une disponibilité élevée des machines et des installations industrielles, la meilleure solution consiste à faire appel à une assistance rapide et économique via un accès à distance. Aujourd'hui, les installations réparties sur plusieurs sites peuvent en effet bénéficier d'une télémaintenance fiable et sécurisée via une communication IP utilisant des connexions DSL, des réseaux mobiles ou des lignes privées. Outre des routeurs industriels parfaitement adaptés aux besoins des automaticiens, Siemens offre, avec sa plateforme Sinema Remote Connect, une application serveur permettant de gérer simplement les réseaux distants.

Gestion centralisée des points terminaux

La télémaintenance doit être simple à utiliser et sécurisée. Elle repose sur un logiciel spécial faisant office de plateforme de gestion centralisée. Celui-ci regroupe les configurations, les groupes, permet de configurer et de gérer intuitivement les points d'accès à l'échelle mondiale. On sait ainsi à tout moment qui communique avec qui. Les clés et les certificats

des connexions pour les tunnels VPN (réseaux privés virtuels) sont faciles à gérer et à maintenir à jour. L'enregistrement des journaux, les sauvegardes et les mises à jour du firmware des routeurs s'effectuent également via la plateforme de gestion. Des routeurs assurent la mise en réseau des installations et des utilisateurs via des connexions VPN sécurisées.
Sinema Remote Connect permet de configurer les réseaux, les points terminaux et les connexions OpenVPN via une interface utilisateur claire. Le système est fourni sous forme de « software appliance » (boîtier applicatif) et peut être exploité soit par le constructeur de machines/l'équipementier OEM lui-même, soit par un partenaire de confiance. Il est possible d'utiliser comme plateforme un matériel dédié ou un environnement virtuel.
Une fois installé, le système basé sur Linux offre une interface web à laquelle de nombreux navigateurs courants peuvent accéder et qui permet de configurer de manière intuitive une liaison sécurisée entre les terminaux et le serveur. La liaison entre les terminaux et le serveur est assurée via un routeur industriel, comme le Scalance M876-4 LTE. Pour lancer l'échange des certificats nécessaires à la connexion VPN, il suffit d'entrer l'adresse du serveur et les données utilisateur du Scalance M876-4 LTE. Cet échange s'opère via une connexion https sécurisée.
La configuration d'autres appareils et leur affectation à des groupes avec les droits de communication correspondants s'effectuent de manière tout aussi simple. Cela permet d'établir un réseau de machines et d'installations communiquant via un serveur centralisé et dont l'accès est sécurisé. Dans cette configuration, la connexion est toujours activée à partir de la machine, c'est-à-dire du routeur industriel. Sur le terrain, l'opérateur de l'installation garde ainsi toujours la main sur la connexion de sa machine avec Internet et le serveur Sinema Remote Connect.

Accès à distance sécurisé des techniciens de maintenance

Les techniciens de maintenance doivent également disposer d'un accès sécurisé aux différentes machines et installations. Grâce à une gestion claire des droits et autorisations à partir d'un site centralisé, le travail de configuration est réduit au minimum ainsi que les temps de réaction en cas de demandes d'accès à distance. Les utilisateurs peuvent être configurés et gérés de manière aussi simple que des appareils au sein de l'interface web du serveur. Ils peuvent être affectés à différents groupes avec des droits de communication définis. L'accès des utilisateurs s'effectue de manière sécurisée via un client OpenVPN. La solution la plus simple consiste à utiliser le client Sinema Remote Connect fourni avec le pack de base.
Autre point fort : la fonction annuaire qui simplifie considérablement l'établissement de connexions sécurisées avec les machines de série grâce à l'activation du Network Address Translation 1:1 (NAT statique). Les installations possédant la même configuration IP côté machines sont ainsi clairement identifiées. Après s'être identifiés sur le serveur et avoir établi une connexion OpenVPN avec la machine, les utilisateurs peuvent utiliser les outils courants comme le TIA Portal pour effectuer des diagnostics système, des opérations de maintenance, de service ou de dépannage sur l'installation. Grâce au tunnel sécurisé, les modifications ne sont possibles que sur les installations disposant des droits d'accès adéquats.
Les constructeurs de machines ont également la possibilité de mettre à jour eux-mêmes les points terminaux via le serveur Sinema Remote Connect. Il leur suffit de charger la nouvelle version du firmware sur le serveur et de la transférer aux appareils Scalance. Les paramétrages et les données de configuration sont conservés et le routeur Scalance se reconnecte automatiquement avec le serveur à l'issue de la mise à jour.
Dans les grandes entreprises, où la politique de sécurité interdit l'accès direct aux machines et aux installations, Sinema Remote Connect peut être installé directement dans le centre de traitement des données du client final. Le service IT attribue alors lui-même les droits aux techniciens de maintenance, conservant ainsi à tout moment une transparence totale sur l'ensemble des personnes intervenant sur le réseau de l'entreprise.
En cas de défaillance du routeur industriel Scalance, la cartouche Key-Plug simplifie le remplacement de l'appareil. Ce support de licence et de mémoire permet en effet de sauvegarder la configuration courante. En cas de panne, le technicien présent sur le site n'a plus qu'à remplacer l'appareil et à brancher la cartouche Key-Plug.

Certification du concept de sécurité appliqué au processus de développement des produits d'automatisation Siemens

L'organisme de certification allemand TÜV SÜD certifie sur la base de la norme IEC 62443 le concept de sécurité Siemens appliqué au processus de développement des produits d'automatisation. Siemens est la première entreprise au monde dont le processus de développement est certifié TÜV SÜD sur la base de la norme IEC 62443-4-1, la sécurité du développement des produits étant une composante essentielle du concept de défense en profondeur (« Defense in Depth »).

Siemens est la première entreprise à obtenir la certification TÜV SÜD basée sur la norme IEC 62443-4-1 pour ses processus de développement des produits d'automatisation et d'entraînement, y compris des logiciels industriels. Au sein de Siemens, il s'agit d'un processus de développement transverse qui implique plusieurs domaines d'activité de l'entreprise. Ainsi, sept centres de développement Siemens ont été certifiés en Allemagne. Ces sites développent notamment des automates programmables industriels SIMATIC S7, des PC industriels de la gamme SIMATIC, des pupitres opérateur SIMATIC HMI (interfaces homme-machine) pour le contrôle-commande, des systèmes d'entraînement SINAMICS ainsi que la plateforme d'ingénierie TIA (Totally Integrated Automation) Portal. La série de normes internationales IEC 62443 définit les mesures de sécurité pour les systèmes d'automatisation industriels, la Partie 4-1 de la norme décrivant les exigences relatives au processus de développement mis en œuvre par les fabricants.

Le certificat TÜV SÜD se fonde sur la norme IEC 62443-4-1 (Secure Product Development Lifecycle Requirements, Draft 3 Edition 10, 01.2016).

Cette norme comprend des exigences relatives à la sécurité. Elle définit notamment les capacités et l'expertise requises en matière de cyber-sécurité, la sécurité des composants fabriqués par des tiers, la qualité des processus industriels et l'assurance de la qualité, la sécurité de l'architecture et de la conception, ainsi que la gestion des points de vigilance, des mises à jour, des correctifs et des modifications de sécurité.

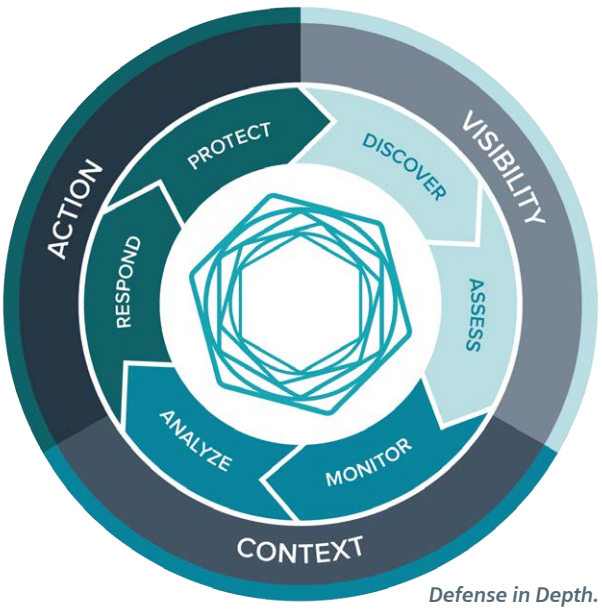
Acteur majeur dans le domaine des équipements d'automatisme et des logiciels industriels, Siemens veille à l'amélioration continue de ses produits et de ses solutions en matière de sécurité industrielle. La certification TÜV SÜD basée sur la norme IEC 62443-4-1 s'inscrit dans cette optique. Cette certification permet de documenter l'approche « Security by Design » de Siemens pour les produits d'automatisation et offre aux intégrateurs comme aux opérateurs une vision claire des mesures de sécurité pour les systèmes d'information. Ainsi intégrateurs et opérateurs peuvent concevoir et exploiter des installations d'automatisation qui font appel à la technologie Siemens et mettent en œuvre le concept de sécurité en profondeur.

« Defense in Depth »

Afin de protéger les installations industrielles contre les cyberattaques internes et externes, tous les niveaux doivent être sécurisés simultanément, de la gestion de l'entreprise au niveau terrain, du contrôle d'accès à la protection contre la copie des données. C'est pourquoi Siemens propose un concept de défense en profondeur – « Defense in Depth » – pour couvrir tous les niveaux. Ce concept est conforme aux recommandations de la série de normes IEC 62443, principale norme relative à la sur la cybersécurité industrielle.

Siemens devient ainsi la première entreprise à obtenir la certification TÜV SÜD selon la norme CEI 62443-4-1 pour son processus de développement des produits d'automatisation et d'entraînement, y compris des logiciels industriels. Au sein de Siemens, il s'agit d'un processus de développement transversal qui implique plusieurs domaines d'activité de l'entreprise. Sept centres de développement Siemens ont été certifiés en Allemagne.

www.siemens.com/industrialsecurity



Defense in Depth.

GPI 2017
Un Grand Prix de l'Innovation sous le signe de l'intelligence des données

Le Grand Prix de l'Innovation (GPI) organisé par Siemens a pour objectif d'encourager les étudiants des écoles d'ingénieurs ayant un projet de création d'entreprise technologique innovante. Les étudiants dont les projets auront été sélectionnés seront accueillis en stage de fin d'études, pour une durée de 6 mois, au sein des équipes techniques et business de la Division Digital Factory de Siemens France. L'édition GPI 2017 met l'accent sur la valorisation des données au cœur de l'Usine du Futur, illustrée par le nouveau concept « Mindsphere », le « cloud » Siemens pour l'industrie.

Le plan « Industrie du Futur » constitue un enjeu considérable pour l'industrie française, mobilisant nombre d'acteurs importants. La numérisation révolutionne l'économie de notre pays en offrant aux industriels la capacité de concevoir plus efficacement leurs produits et outils de production, puis de planifier, ordonnancer et réaliser celle-ci avec des performances accrues en matière d'efficacité énergétique, de qualité et de souplesse opérationnelle. Ces performances sont apportées par une collecte permanente, une sauvegarde sécurisée et l'analyse intelligente des données utiles. Les données ainsi traitées doivent être également protégées de toute cyberattaque pour réduire les risques, à savoir prise de contrôle intempestive sur ces processus, propriété intellectuelle, etc.

Grâce à l'apport des outils de modélisation et de simulation du produit ainsi que du moyen de production (monde virtuel) et de l'analyse de ces données (monde réel), ce concept de

DATES À RETENIR :

- **10 janvier 2017 : date limite de soumission des projets.**
- **17 janvier 2017 : présélection des projets.**
- **17 janvier 2017 : date limite de candidature à l'offre de stage de fin d'études au sein de Siemens.**
- **Fin janvier 2017 : Innovation Day avec le jury du GPI.**

jumeau numérique permet de comparer les modèles virtuels et réels de l'outil de production et de réaliser la maintenance prédictive des équipements et leur optimisation (consommation énergétique, disponibilité, etc.)
Cette intelligence des données permet également de révolutionner les modèles de fabrication en apportant aux industriels de nouveaux services à forte valeur ajoutée.
La valorisation de ces données a donné naissance au concept de « MindSphere », le « cloud Siemens» pour l'industrie.

Dans cet esprit, les projets que les candidats développeront devront impérativement traiter un des thèmes suivants :

- La maintenance prédictive, à partir des données de production, permettant d'éviter toute panne éventuelle et d'intervenir à distance sur la machine.
- L'efficacité énergétique industrielle, à partir des données de consommation énergétique.
- L'optimisation des ressources, et pilotage en ligne de machines, réparties dans les chaînes d'un industriel.
- La cybersécurité des systèmes industriels, destinée à sécuriser transactions et informations de production.
- L'avatar d'un expert distant, destiné à assister les opérateurs sur site, lors de réception, mise en service ou maintien en condition opérationnelle d'installations industrielles avec des protocoles précis et efficaces ; celui-ci garantissant la remise en état des installations dans les meilleurs délais via l'utilisation de la simulation et de la visualisation 2D ou 3D.

VOUS ÊTES INTÉRESSÉ ET SOUHAITEZ PARTICIPER :

Envoyez-nous vos projets originaux et innovants. Pour ce faire, transmettez-nous votre dossier avec les pièces suivantes :

- **Un dossier de 5 pages maximum à remplir directement sur le site : www.siemens.fr/grandprixinnovation décrivant le projet autour de la thématique de l'intelligence des données dans l'Industrie du Futur en détaillant les perspectives économiques, technologiques et organisationnelles du projet (notamment données économiques et de marché prévisionnelles, points clés technologiques, conception et cycle de vie, valeur ajoutée, ressources nécessaires, planning…).,.**
- **Les Curriculum Vitae et lettres de motivation des membres de l'équipe projet, afin de postuler à l'offre de stage au sein de Siemens, à déposer directement via le site Carrière**
- **Une lettre de recommandation émanant d'un enseignant (optionnelle).**

Le dossier complet devra être rédigé en français et transmis avant le 10 janvier 2017.

Un comité composé d'experts techniques et de professionnels Siemens examinera les projets reçus. Il sélectionnera les équipes finalistes qui viendront présenter leur projet devant le jury du Grand Prix de l'Innovation lors de la journée Siemens Industrie Innovation Day, à Paris, fin janvier 2017.
Le Grand Prix de l'Innovation est ouvert aux étudiants de dernière année d'écoles d'ingénieurs françaises, master pro technologique ou scientifique. Les projets peuvent être réalisés en binôme.

Un nouveau réseau sécurise la production

Sur son site de Fürth, Siemens a sécurisé et optimisé sa production grâce à l'utilisation de composants réseau adaptés au milieu industriel, issues de son portefeuille de produits. De surcroit orienté process, segmenté en VLAN et avec du routage au niveau 3, l'ensemble des procédures rendent le réseau particulièrement performant, disponible , flexible et sûr.

Dans le nouvel atelier de production du site de Fürth, Siemens fabrique du matériel électronique en petites et moyennes séries avec une flexibilité maximale.

Jusqu'ici réparties, les installations de production du site de Fürth ont été regroupées dans un nouvel atelier de fabrication et intégrées dans les processus de production et les processus opérationnels de l'entreprise. Depuis mars 2014, des produits en moyennes et petites séries ainsi que des pièces unitaires sont fabriqués sur le site. La gamme s'étend de la carte électronique à l'automate industriel complexe destiné aux applications les plus diverses, en passant par les modules pour API.
La solution réseau étendue, qui fait appel à des composantes de la gamme de produits Scalance, a été développée, planifiée et mise en œuvre dans le cadre d'une étroite collaboration entre Siemens Global Services Information Technology, le service IT du site, le fournisseur de services IT et le partenaire Siemens Atos Allemagne. Les experts réseau de l'activité Industrial Communication de Siemens ont également apporté leur soutien et ont fourni des conseils en matière de réseau industriel. Répondant aux exigences de disponibilité et de sécurité des données les plus sévères, les experts ont développé un concept de réseau garantissant une mise en réseau sécurisée des environnements de production et bureautiques.

Des tâches et des exigences complexes

Plus de 100 systèmes IT du niveau production de l'usine devaient être interconnectés en réseau avec les serveurs centraux du centre de données Siemens. Ce réseau sert à distribuer les ordres de travail à des machines et des installations fonctionnant en partie 24 heures sur 24 en trois équipes, les instructions de travail aux opérateurs ainsi que des mises à jour logicielles et les micro-logiciels aux automates. Tous les processus impliquant un échange de données interactif entre terminaux et serveurs exigent une disponibilité et une efficacité accrues afin

de permettre un suivi des différentes étapes. Certaines activités nécessitent en outre des autorisations de la part d'un poste central. Tout cela suppose une fiabilité maximale de la communication ainsi que la prise en compte de critères de sécurité IT extrêmement sévères. Pour éviter les défaillances, le réseau de production du nouvel atelier devait être découplé du reste du site et subdivisé en segments logiques axés sur les différents processus de production. Pour assurer la sécurité du réseau, des pare-feu ont notamment été utilisés dans une architecture de niveau 3, mais aussi des restrictions d'accès via des listes de contrôle d'accès (ACL).

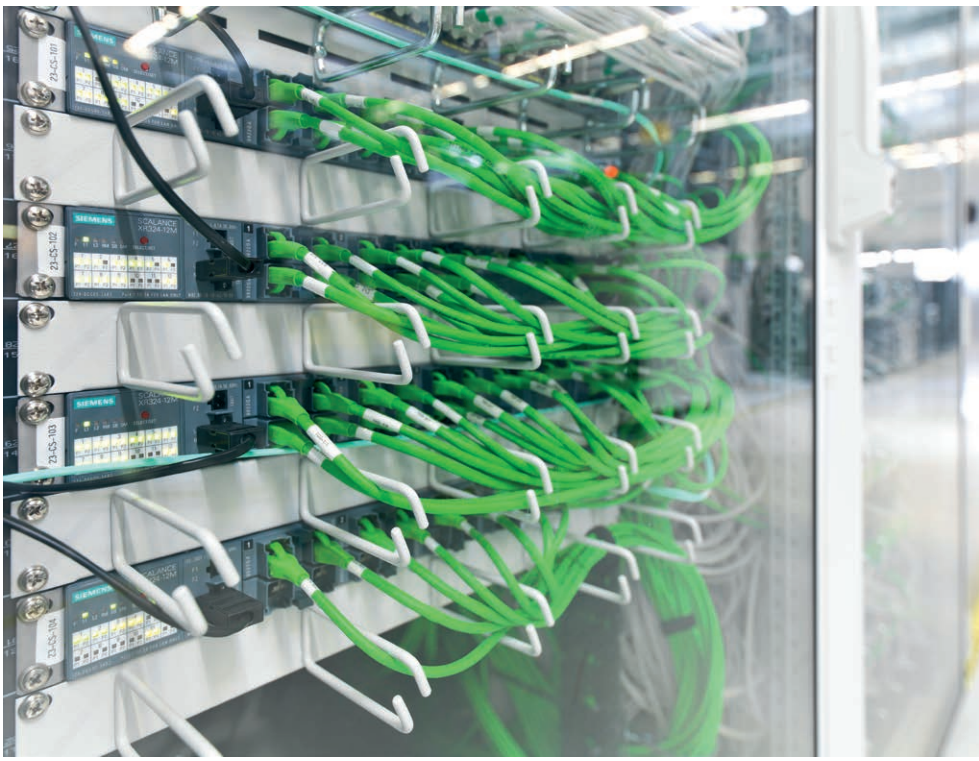
De nouvelles structures de réseau pour une production efficace

Le réseau de communication du site de Fürth est structuré en trois couches : cœur, distribution et accès. En plus des routeurs de cœur déjà présents au sein du réseau local du site et des pare-feu matériels déjà disponibles, on a installé au niveau distribution deux commutateurs Scalance XR528-6M séparés physiquement entre eux. Connectés entre eux via des anneaux fibre optique redondants de 10 Gbit, ils constituent l'épine dorsale extensible de la production. Si l'un des appareils tombe en panne, l'autre prend le relais. Les pare-feu matériels séparent et régulent les accès entre la production et le reste du réseau. La communication des réseaux locaux virtuels (VLAN) de la production est également contrôlée par les pare-feu. Neuf commutateurs Scalance XR324-12M dotés de plusieurs ports au niveau accès sont connectés de manière redondante aux commutateurs Scalance du niveau distribution. Ils sont répartis sur plusieurs armoires de la zone de production et combinés en anneaux redondants. Les terminaux de la production regroupés en VLAN sont connectés à ces anneaux redondants via des panneaux de brassage. Un câblage de catégorie 6 permet de réaliser une liaison Ethernet gigabit continue dans le panneau.

Segmentation de la production

Le VLAN d'origine, qui comptait quelque 150 stations raccordées, n'était pas segmenté. Tout problème au niveau de la communication de la couche 2 risquait donc d'affecter les niveaux supérieurs. Le réseau n'étant pas redondant, la défaillance de certains composants pouvait provoquer des arrêts relativement longs. L'utilisation de commutateurs Scalance a permis de séparer le réseau production du nouvel atelier du reste du site et de le segmenter en fonction des exigences de la production. On compte désormais une vingtaine de VLAN plus petits gérant chacun un maximum de 11 stations. Cela accroît la bande passante des segments et donc les vitesses de transmission. En cas de défaillance ou d'attaque, les conséquences sont désormais limitées à un nombre minime d'appareils. L'interaction des pare-feu matériels et des listes de contrôle d'accès (ACL) offre une protection maximale contre les accès non autorisés.

Grâce à une bonne préparation et à la migration réalisée en amont, l'équipe chargée du projet a pu restructurer et tester les différentes stations raccordées dans les délais de maintenance impartis. Le service n'a pratiquement pas été affecté par ces opérations. Même au terme des tests de fonctionnement, Atos continuera à suivre la solution complète mise en œuvre sur le site de Fürth dans le cadre d'un contrat de Full Managed Services. Une équipe de spécialistes accessible 24 heures sur 24 garantit en outre la disponibilité permanente du réseau. *« Nous sommes très satisfaits du déroulement du projet ainsi que de la stabilité, de la disponibilité et de l'efficacité au quotidien de la nouvelle infrastructure »*, s'est félicité Lorenz Rappl, responsable de la production à Fürth.



Couplés de manière redondante au niveau distribution, les commutateurs performants Scalance XR324-12M relient en toute sécurité une vingtaine de VLAN aux serveurs de données.

Cybersécurité des installations existantes : il n'est pas trop tard !

Il existe aujourd'hui des solutions permettant aux installations existantes de talonner les équipements neufs quant à leur performance en matière de cybersécurité. Même obsolètes, les composants d'une installation industrielle peuvent bénéficier de briques de protection et autres pare-feu efficaces, sans compter sur les mesures organisationnelles et les processus opératoires à mettre en œuvre. Rien n'est perdu, mais il faut pour cela passer à l'acte !

Aujourd'hui, les acteurs de l'industrie prennent conscience que leurs systèmes automatisés de contrôle des procédés industriels (automatismes, régulation, robotique…) peuvent être les cibles de cyberattaques ou encore les victimes de négligences internes. Si la cybersécurité des installations neuves intègre de façon native une stratégie de protection contre les actions malveillantes et certaines conduites peu scrupuleuses, les installations existantes en revanche doivent faire l'objet d'une attention toute particulière. Dans tous les cas, rappelons que le risque zéro n'existe pas.

Y a-t-il un pilote à bord ?

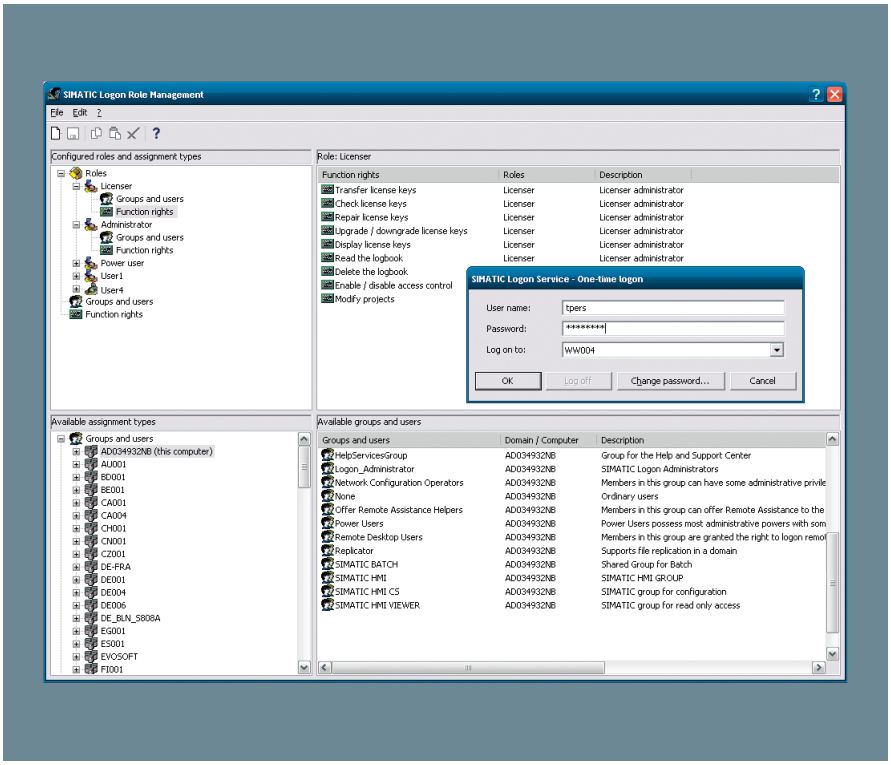
L'étape de prise de conscience étant franchie, quelle stratégie mettre en œuvre ? L'expérience montre que plus de 70 % des actions à conduire sont de type organisationnel. Cela signifie que la partie matérielle ou logicielle n'occupe que 20 à 30 % du programme à déployer.

La première étape ? Les rôles et responsabilités en matière de cybersécurité des installations industrielles doivent être clairement établis au sein de l'entreprise. Si ce n'est pas le cas, il convient de nommer le ou les responsable(s). Cette charge incombe généralement aux spécialistes internes de la sécurité informatique ou de la sécurité du site. Dans ce cas, il est nécessaire de largement coopérer avec les équipes industrielles.

Le responsable « cybersécurité des équi-

GESTION DES IDENTITÉS

Intégrée dans la gestion des utilisateurs Windows, SIMATIC Logon assure la gestion centralisée de tous les utilisateurs de l'installation. Cet outil offre un grand nombre de mécanismes de sécurité aussi bien côté administrateur que côté utilisateur. L'utilisateur est identifié de manière univoque par un identifiant appelé User ID, le nom d'utilisateur et son mot de passe. Des fonctions telles que le vieillissement du mot de passe, la déconnexion automatique après un temps prédéfini ainsi que l'interdiction d'accès après plusieurs saisies d'un mot de passe erroné garantissent une sécurité maximale. En outre, l'administrateur peut créer ou supprimer des utilisateurs en ligne pour toute l'installation et quelle que soit l'application.



pements industriels » a pour mission de faire cohabiter différentes métiers et d'animer des équipes pluridisciplinaires : spécialistes de la sécurité informatique, analystes des données, automaticiens, juristes...

Quelle stratégie ?

Afin de mettre un maximum d'atouts de son côté, il convient de s'inspirer des bonnes pratiques issues des technologies de l'information et de les adapter au contexte industriel. A commencer par les règles comportementales. En d'autres termes, il s'agit de bannir le passage des clés USB de serveur en serveur ou encore de gérer les autorisations et l'usage des équipements qui doivent se connecter sur site (besoins de maintenance, de mise à jour, de paramétrage...). Processus opératoires et bon sens doivent rester des règles à appliquer par tous et guider pourquoi pas la rédaction d'une charte interne.

Dresser un état des lieux

Pour savoir quels sont les équipements à protéger, un inventaire est indispensable, véritable cartographie exhaustive des installations matérielles et des logiciels en place. Sur cette base, les experts Siemens pourront lister les vulnérabilités connues, relatives à chaque équipement ou logiciel. Cette mission visant à répertorier et à instruire un état des lieux et des points faibles, peut faire l'objet d'une prestation clé en main réalisée par Siemens.

SE FORMER À LA CYBERSÉCURITÉ

Siemens propose de former ses clients à la cybersécurité et au bon sens concernant le parc des équipements d'automatisme et d'informatique industrielle. Il existe aussi au catalogue une formation à la gestion de crise pour apprendre à réagir et à se poser les bonnes questions...
Ces formations s'adressent notamment aux intégrateurs, eux-mêmes au contact de très nombreuses installations et en premier lieu garants des bonnes pratiques auprès de leurs clients.

Quels équipements protéger ?

Vient ensuite l'étape d'audit, liée à l'architecture et à la configuration de l'installation d'automatisme. Cette phase d'approche vise à mieux comprendre quels sont les risques et les menaces les plus vraisemblables auxquels l'industrie doit faire face. Cela détermine plus précisément les enjeux, et permet de mettre en avant les équipements à protéger en priorité. Là encore, l'audit incite à prendre majoritairement des résolutions organisationnelles.

Comment se protéger ?

- La première étape consiste à isoler les systèmes industriels du reste des installations informatiques. Cette action doit être effectuée au plus tôt. Il s'agit de mettre en œuvre des solutions de protection périmétrique, véritables fortifications autour de l'outil industriel. Cette défense en profondeur s'appuie d'abord sur un pare-feu, en lien éventuellement avec des diodes informatiques. En complément, des sondes de détection d'intrusion permettent d'observer les éventuelles attaques...

3 NIVEAUX DE CYBERSÉCURITÉ

Définis par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), 3 classes de cybersécurité permettent de classer les installations industrielles en fonction de leurs besoins de sécurité : classes 1 (risque faible), classe 2 (risque significatif) et classe 3 (risque critique). Voir le guide ANSSI : « La cybersécurité des systèmes industriels – Méthode de classification et mesures principales ».

- En complément, la seconde étape consiste à séparer les installations les unes des autres en fonction de leur aspect critique, afin d'éviter la propagation d'un éventuel problème. Dans un autre domaine, cette stratégie s'apparente aux coupes effectuées entre parcelles boisées, dans les régions les plus sensibles au feu de forêt.

Ne rien négliger !

Les installations anciennes, par exemple dotées d'automates SIMATIC S7 ou de pupitres, ne doivent pas négliger les protections par mots de passe. Ajouter au châssis de l'automate un coupleur de communication avec son pare-feu natif est également un bon réflexe. Pour les automates SIMATIC S7-300 et S7-400 sont d'ailleurs disponibles les coupleurs de communication de nouvelle génération sous protocole OPC UA, embarquant de façon native les fonctions de sécurité.

Les systèmes très anciens non reliés à un réseau global (automates, pupitres, ordinateurs en production...) sont-ils à l'abri des attaques ? Non, car ils présentent toujours un risque de contamination lors d'une mise à jours du programme ou du logiciel, avec une clé USB ou un ordinateur extérieur... C'est pourquoi, même dans ce cas, il est impératif de vérifier de la façon la plus stricte l'intégrité de la clé USB qui sera utilisée, à l'aide d'un outil spécifique. De la même façon, avant raccordement, il faut interroger l'intégrateur de passage sur site quant à la protection de son ordinateur.

Les switchs sont aussi des portes d'entrée par défaut vulnérables. Il convient alors de verrouiller les ports non utilisés, voire d'y placer des verrous physiques.

Au-delà de la gestion des accès par mots de passe, éviter les connexions indésirables en interne, passe aussi par le contrôle physique des accès aux équipements. Changer les clés des armoires et des coffrets critiques peut être une bonne chose. Placer sous alarmes les armoires électriques permet de savoir ou et quand une action à pu se produire.

LA DÉFENSE EN PROFONDEUR

Contre les cyber-attaques internes et externes, la sécurité doit être assurée simultanément à tous les niveaux. Cette approche, communément appelée « défense en profondeur » est conforme aux recommandations de la norme ISA99 / CEI 62443, la norme de référence en matière de cybersécurité des applications industrielles.

- **Sécurité du site - Sécuriser l'accès physique aux composants critiques grâce à l'utilisation cohérente de mécanismes de sécurité pour protéger les installations.**
- **Sécurité des réseaux - La communication industrielle est un facteur clé de la réussite des entreprises, à condition que les réseaux soient sécurisés.**
- **Intégrité des systèmes - Assurer l'intégrité des systèmes grâce à des fonctions de protection dédiées.**

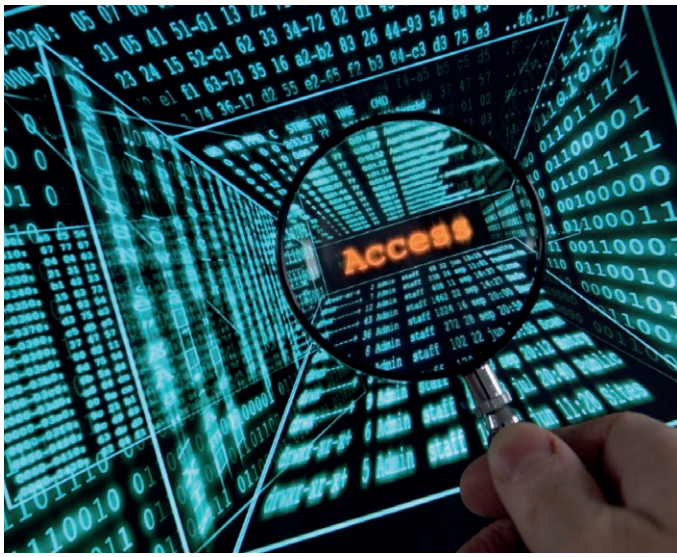
En Bref, l'ANSSI ses missions et contexte réglementaire

Initialement perçue comme un scénario catastrophe cher à la science fiction, la cybermenace a désormais envahi nos villes, nos entreprises et même nos foyers. D'imaginaire, elle est aujourd'hui on ne peut plus concrète. Pour lutter contre ce fléau, dont les acteurs insidieux et inventifs font montre de techniques de plus en plus perfectionnées, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a été créée en 2009. Rattachée au Secrétaire général de la défense et de la sécurité nationale (SGDSN), l'ANSSI se fait le garant de la sécurité et de la cyber défense en France. L'enjeu est stratégique mais également économique puisqu'il est désormais indispensable pour les entreprises de préserver compétences, savoir-faire et avantages concurrentiels.

Outre ses fonctions de veille, de détection, d'alerte et de réaction aux attaques informatiques, l'ANSSI a également pour vocation la promotion des technologies, des produits et services de confiance, des systèmes et des savoir-faire nationaux auprès des experts et du grand public. Information et conseil, formation et labellisation de produits et prestataires de confiance figurent également sur la feuille de route de l'ANSSI et plus largement, dans la stratégie nationale pour la sécurité du numérique présentée en octobre 2015 par le Premier Ministre. L'Agence apporte expertise et assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV). Ceux-ci évoluent dans des secteurs d'activités ayant trait à la production et à la distribution de biens ou de services jugés indispensables : satisfaction des besoins essentiels pour la vie des populations, exercice de l'autorité de l'Etat, fonctionnement de l'économie, maintien du potentiel de défense, sécurité de la Nation.

Les opérateurs d'importance vitale vis-à-vis de la loi de programmation militaire

Promulguée le 18 décembre 2013, cette législation fait suite aux orientations fixées par le Livre blanc sur la défense et la sécurité nationale 2013. Son article 22 prévoit l'adoption de mesures de renforcement de la sécurité des opérateurs d'importance vitale et confère à l'ANSSI de nouvelles prérogatives : l'agence, au nom du Premier Ministre pourra imposer aux OIV des mesures de sécurité et des contrôles de leurs systèmes d'information les plus critiques.



Face à l'augmentation des attaques informatiques, l'ANSSI a pour mission d'accompagner les opérateurs d'importance vitale dans la sécurisation de leurs systèmes d'information sensibles

Depuis le 1er juillet 2016, les arrêtés sectoriels, précisant les mesures à mettre en œuvre pour chaque secteur d'importance vitale commencent à rentrer en vigueur. Aussi, afin de garantir un niveau de sécurité maximale, l'ANSSI recommande certains produits au préalablement qualifiés par ses soins. Délivrée par l'ANSSI, la qualification, permet d'attester d'un certain niveau de sécurité et de confiance dans les produits et les prestataires de service listés respectivement dans le catalogue des produits qualifiés et celui des prestataires de service qualifiés. La qualification offre donc des garanties de sécurité et de confiance aux acheteurs de produits ou de prestations de service.

Automate S7-1518 et commutateur industriel XM400 : les « cyber fruits » Siemens à consommer sereinement et sans modération

En mai 2016, notre automate SIMATIC S7-1518 a obtenu une qualification de sécurité délivrée par l'ANSSI, élevant Siemens au rang de tout premier équipementier à obtenir une certification et une qualification pour un équipement de systèmes industriels. Notre produit phare devait être suivi de près par le commutateur industriel Ethernet Scalance XM400, certifié en juillet. Retrouvez nos deux « protégés » en pages 4 et 23 de notre magazine.

Depuis 2013, Siemens a participé à l'ensemble des groupes de travail menés par l'ANSSI sur la cyber sécurité des systèmes industriels. Cela contribue activement à créer un écosystème de confiance pour ces systèmes dont certains sont d'importance vitale pour la nation.

Nous vous invitons à parcourir les documents auxquels nous avons contribués :
www.ssi.gouv.fr/entreprise/bonnes-pratiques/systemes-industriels/

Jean-Christophe Mathieu

SECLAB, SENTRYO, WALLIX
Les trois mousquetaires au service de sa majesté Cybersécurité

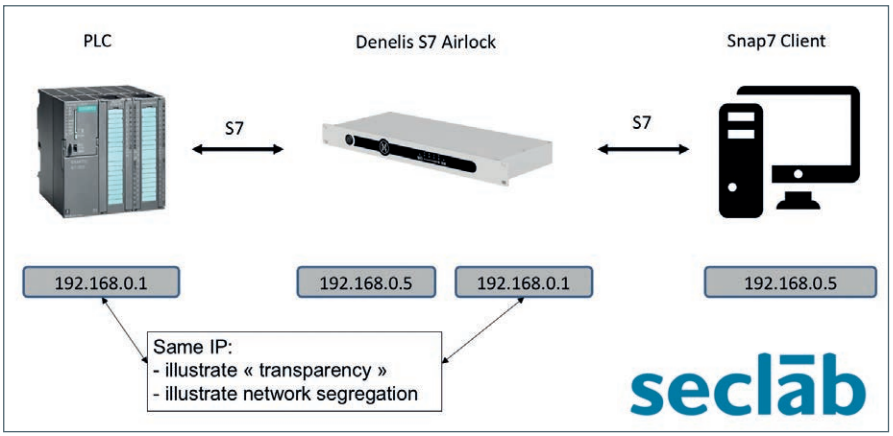
Assurant la protection des réseaux et systèmes industriels critiques ou spécialisées dans la gestion des accès à privilèges, ces sociétés, dynamiques et innovantes, proposent des solutions dédiées pour lutter contre la cybermenace qui viennent à point nommé compléter l'offre Siemens.
Nous vous proposons de faire plus ample connaissance avec nos 3 expertes au cœur de ces 3 pages.

SECLAB

Fondé en 2011, Seclab protège les systèmes sensibles contre les cyberattaques sophistiquées via réseau ou USB. Ses solutions reposent sur des technologies uniques d'Airgap de Nouvelle Génération, brevetées et certifiées ANSSI qui implémentent une approche de défense en profondeur dans l'électronique.

Les produits ont été conçus historiquement au sein d'EDF pour répondre aux enjeux particuliers des systèmes industriels critiques. Ils sont par extension adaptés aux besoins des opérateurs d'importances vitales pour les infrastructures industrielles critiques des secteurs énergie, transports, traitement et distribution de l'eau, etc. Ces besoins se retrouvent également dans le cadre d'infrastructures sensibles telles que la finance, la santé et les télécoms.

A partir du constat que la sécurité logicielle est largement insuffisante pour les systèmes critiques, l'offre se base sur une combinaison de software et hardware permettant de garantir des propriétés de sécurité de manière déterministe avec une logique câblée.
Ainsi, Seclab rend possible des communications entre systèmes isolés avec un cloisonnement physique unidirectionnel ou bidirectionnel, tout en facilitant leur intégration dans les systèmes existants et futurs.
Siemens et Seclab ont initié une collaboration afin d'assurer une compatibilité et complémentarité entre leurs offres : support des protocoles majeurs utilisés sur le terrain, renforcement de la chaine de confiance de distribution de mises à jour.



Concrètement, les solutions de Seclab associées à Siemens permettent de répondre au besoin de remontée d'informations nécessaires à la supervision, de cloisonner strictement des domaines en les immunisant contre les attaques réseaux et de simplifier les architectures existantes en minimisant l'exploitation.

Ainsi, elles contribuent aux enjeux suivants :

- répondre aux enjeux de sécurité opérationnelle.
- optimiser la performance des procédés industriels.
- se conformer aux réglementations et standards de sécurité renforcée.

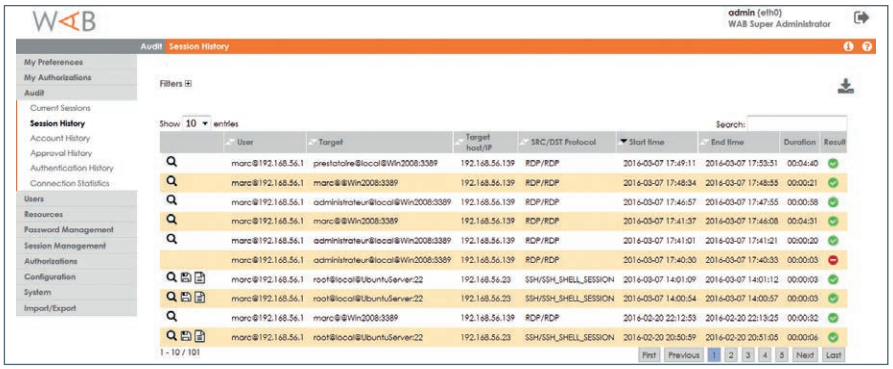
La société est basée à Montpellier (France) avec un bureau à San Francisco (Etats-Unis). **www.seclab-solutions.com**

WALLIX

Spécialiste de la cybersécurité et expert dans la gestion des accès des utilisateurs à privilèges, Wallix accompagne Siemens avec son offre dédiée aux Systèmes de Contrôles Industriels et SCADA SIMATIC. La plateforme WALLIX Admin Bastion (WAB Suite) permet de contrôler, tracer et gérer les accès des utilisateurs internes et externes au réseau de technologie opérationnelle. Les SCI sont extrêmement vulnérables aux menaces dont certaines peuvent avoir des conséquences vitales sur le marché des opérateurs d'infrastructures industrielles (OIV).

WALLIX Admin Bastion est aujourd'hui la seule solution de gestion des accès à privilèges (Privileged Access Management : PAM) qui soit totalement certifiée CSPN par l'ANSSI. Pour optimiser la cyber sécurité des industriels, voici ce que propose notre plateforme logicielle :

- **Sécuriser et contrôler les sessions et les accès à distance :** par la surveillance, l'authentification et la sécurité des utilisateurs qui accèdent au réseau SCI, la délégation d'autorisation d'accès via un workflow paramétrable, des alertes en temps réel en cas d'action inappropriée ou selon des plannings prédéfinis.
- **Suivre les exigences des politiques de sécurité ou règlement de gestion des mots de passe de la console d'administration SCI :** le durcissement des mots de passe pour accéder aux équipements industriels, la génération et la sécurité dans un coffre-fort certifié (cacher, dévoiler, changer ou pérenniser les mots de passe).Tracer les connexions et auditer les actions réalisées : le monitoring des connexions et des équipements administrés, la visualisation dans une console web du contenu des connexions actives et le reporting des actions associées.
- **Passer d'une politique de gestion du risque à une démarche de confiance numérique :** en laissant aux collaborateurs internes et tiers privilégiés les moyens de se focaliser sur les usages et obligations de leurs métiers, dans un environnement sécurisé et conforme aux obligations réglementaires qui pèsent sur l'entreprise.
- **Gagner en agilité, productivité et performance** en mettant en œuvre une solution de gouvernance des accès performante, peu contraignante et à même de faire gagner du temps aux utilisateurs dans leur activité.



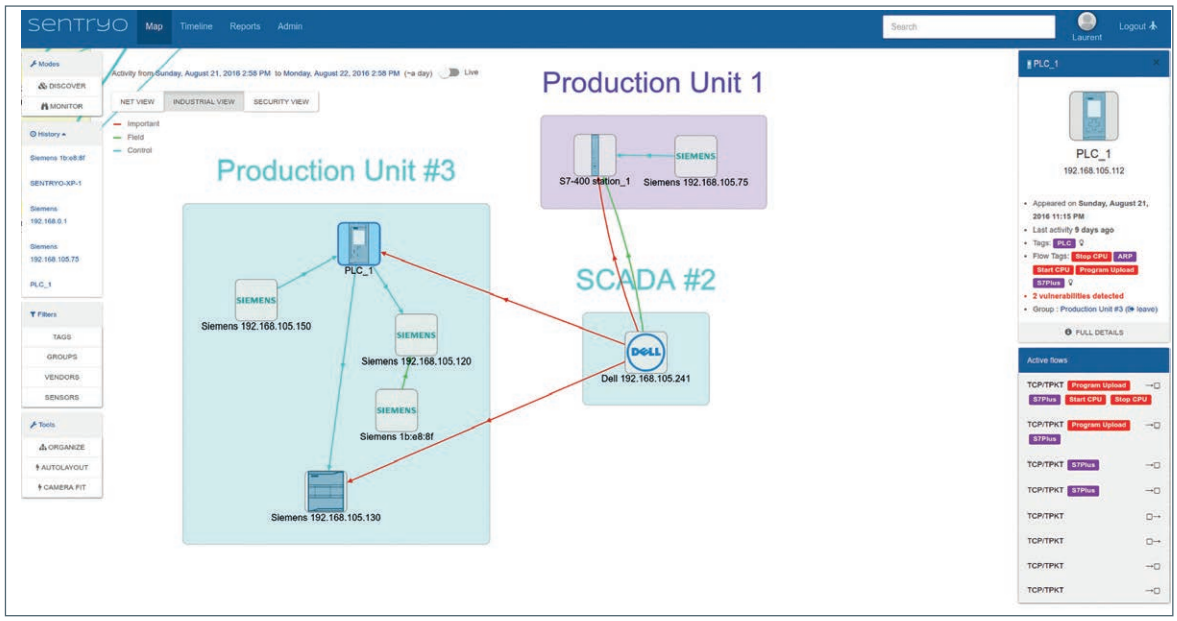
WALLIX est en entreprise côtée en bourse présente dans plus de 25 pays via son réseau de plus de 90 partenaires. Suivez-nous sur les réseaux sociaux **@Wallixcom**, **@Wallixfr** et consultez notre blog et site web **www.wallix.com**

WALLIX
TRACE, AUDIT & TRUST

SENTRYO

Sentryo est un éditeur de solutions de cybersécurité - hardware/software - pionnier de la protection des réseaux M2M et des systèmes industriels critiques.
L'évolution inévitable des systèmes industriels et des réseaux qui contrôlent notre monde physique vers plus d'ouverture et d'intelligence les expose de plus en plus aux cybermenaces. Les solutions de cybersécurité issue de l'IT ne sont pas adaptées aux contraintes du monde industriel.

Description de la solution :
ICS CyberVision est conçu pour protéger les réseaux industriels critiques. La solution permet de connaître et monitorer le réseau, prévenant ainsi les risques de compromission. Cela inclut un inventaire des éléments du réseau, une carte de tous les flux de communication et un zoom sur les vulnérabilités. ICS CyberVision s'appuie sur les techniques de machine learning pour construire un modèle du système lui permettant ainsi de détecter chaque événement anormal.



La solution Sentryo ICS CyberVision surveille le réseau, détecte les comportements anormaux et facilite la réaction aux incidents.
A l'inverse des solutions IT, Sentryo ICS CyberVision est complètement passive, condition déterminante pour des réseaux critiques. Conçue pour être utilisée par les automaticiens, ICS CyberVision permet une collaboration OT/IT et un monitoring complet de la situation, ce qui permet de conserver une longueur d'avance sur la menace.
Sentryo s'adresse aux entreprises des secteurs de l'énergie, du transport ou de l'environnement qui opèrent des infrastructures critiques comme aux entreprises industrielles du secteur manufacturier qui relèvent le défi « Industry 4.0 » Elle est idéalement placée pour répondre aux enjeux de cyber sécurité de l'Internet des objets professionnels. La société a démarré simultanément en France et en Allemagne.
En Février 2016, Sentryo lève 3M € auprès d'investisseurs privés européens pour poursuivre son développement à l'international.

Enfin, ICS CyberVision facilite la réponse à incident en regroupant toutes les informations utiles à une enquête forensic.
ICS CyberVision est complémentaire avec l'offre Siemens qui offre un niveau de protection élevé des automates, permet de filtrer les messages et de chiffrer les communications. ICS CyberVision complète cette offre avec une capacité de détection et d'identification des opérations malveillantes.
www.sentryo.net/fr/blog

L'ANSSI certifie le commutateur industriel Ethernet Scalance XM400* de Siemens

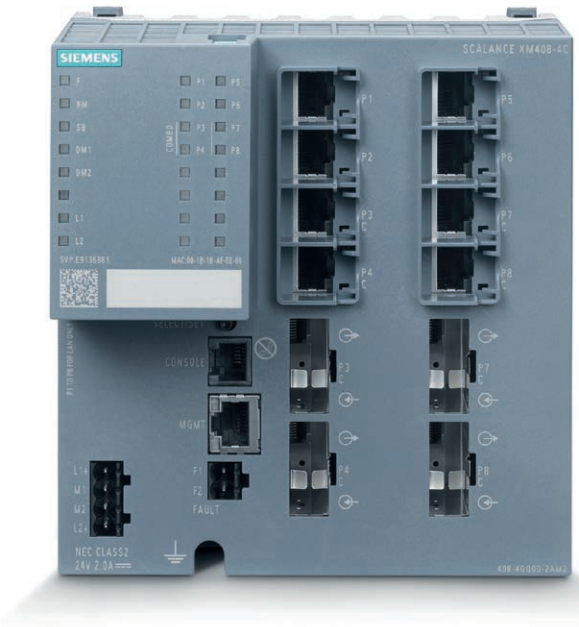
Après l'automate programmable SIMATIC S7-1500, Siemens est une nouvelle fois le premier industriel à obtenir la certification pour un équipement avec cette fois-ci le commutateur industriel Ethernet Scalance XM400. Cette certification de sécurité est délivrée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), seule autorité apte à délivrer en France la certification pour la sécurité des produits des systèmes industriels.

Le commutateur constitue un équipement clé de ces réseaux. La certification du Scalance XM400 de Siemens apporte aujourd'hui aux utilisateurs le niveau de protection indispensable à la sécurité de leurs systèmes industriels.
La Certification de Sécurité de Premier Niveau (CSPN) prononcée par l'ANSSI le 13 juin 2016 (certificat ANSSI-CSPN-2016-09) atteste du niveau de sécurité offert à ce jour par le commutateur Scalance XM400 de Siemens. Soumis à une série de tests visant, d'une part, à éprouver ses fonctions de sécurité, et d'autre part, à rechercher des vulnérabilités, le commutateur Ethernet Scalance XM400 a démontré sa capacité à fournir un niveau plus élevé de confidentialité, de disponibilité et d'intégrité des installations qu'il équipe.

Grâce au concept « Security Integrated » de Siemens, le commutateur industriel Ethernet Scalance XM400 propose nombre de fonctions de sécurité qui ont justifié ce label

- le cloisonnement logique (à l'aide de VLAN par exemple) ;
- la gestion des ports de communication : possibilité de désactiver les ports inutilisés ;
- le filtrage par adresse MAC : créer une liste blanche d'adresse pour chaque interface Ethernet ;
- l'authentification des terminaux connectés grâce au protocole IEEE 802.1x par exemple ;
- la protection du micrologiciel (firmware) contre une mise à jour frauduleuse ;
- la protection de la corruption de la configuration ;
- la journalisation locale et distante des évènements d'administration et de sécurité ;

« *Cette reconnaissance confirme Siemens dans son rôle de partenaire de référence pour répondre aux enjeux de la digitalisation et de la cybersécurité de ses clients. Elle constitue une nouvelle étape dans notre volonté d'apporter une offre complète de produits d'automatismes sécurisés à tous les niveaux* » déclare Vincent Jauneau, directeur des Divisions Digital Factory et Process Industries and Drives chez Siemens France.



** Pour plus d'informations sur la cible de sécurité du swtich Scalance XM400 et le rapport de certification, consultez le site de l'ANSSI : http://www.ssi.gouv.fr/entreprise/certification_cspn/scalance-xm408-8c/*

SCALANCE XM400, LES AVANTAGES EN BREF :

- **XM 400 Switch modulaire 24 ports.**
- **Ports Combo hybride Cuivre et SFP.**
- **Activation des fonctions de niveau 3 par KEY PLUG**
- **Port Extender PE408 : huit ports RJ45 supplémentaires**
- **Port Extender PE400-8SFP : huit logements SFP supplémentaires**
- **Port Extender PE408PoE : huit ports RJ45 supplémentaires avec PoE selon IEEE 802.3at Type 2.**

MindSphere : le cloud Siemens pour collecter, analyser et mettre à disposition les données pour un pilotage et une optimisation de la production

Opérationnelle pour tous les utilisateurs de solutions Siemens, la plateforme Siemens Cloud for Industry s'ouvre également à tous les équipements sous standard OPC UA. Issu d'un partenariat entre Siemens et SAP, cette plateforme s'appuie sur l'outil universel MindSphere. Ce véritable écosystème IT collecte les données pour créer de la valeur ajoutée, au service des fabricants de machines, des intégrateurs et de leurs clients finaux.

Maîtrisé depuis plusieurs années par les grands noms de l'informatique de gestion, les données en masse couvrent aujourd'hui la plupart des applications IT au service du secteur tertiaire et du grand public. Dans l'industrie, qu'il s'agisse du manufacturier ou du process, il existe un grand nombre de données issues de capteurs répartis. Ces données permettent aujourd'hui une gestion prédictive des équipements, bien plus pertinente que la traditionnelle maintenance curative ou même préventive. Sur la base d'une analyse des dérives, le «condition monitoring» permet de maîtriser les coûts de maintenance. De la même manière, les objectifs de réduction des temps de cycle ou de personnalisation de la production nécessitent l'analyse fine des données issues des machines. Il restait à partager ces données de façon optimale et sécurisée pour un maximum d'applications...

Un système cloud pour l'industrie

L'usage d'un cloud dédié à l'industrie donne toute latitude pour enrichir des tableaux de bord ou comparer entre eux plusieurs sites (benchmarking). Chez Siemens, le cloud s'appelle MindSphere. Lancée il y a un an, cette offre dépend de la business unit Digital Factory - Product Life Cycle Management - Plant Data Services (voir encadré). MindSphere est plug and play et collecte les données de production transmises par les clients de Siemens.

Elément de différentiation

Fabricants de machines et intégrateurs peuvent utiliser MindSphere sur leurs équipements existants, avec une plateforme de développement Fleet Manager et Visual Analyser. Les services apportés par le cloud représentent un élément de différentiation notoire et la perspective de faire évoluer les performances de la machine dans le cadre d'un suivi permanent ou régulier.

De son coté, l'exploitant de l'équipement accède au tableau de bord souhaité avec Visual Analyser ou s'appuie sur les services de partenaires pour accéder à ses données sur ordinateur ou sur smartphone via des applications. Les données à disposition permettent une analyse pointue

PLANT DATA SERVICES FAIT PLACE À DF PL DS

La nouvelle business unit Digital Factory Product Life Cycle Management Plant Data Services (DF PL DS) est officiellement entrée en activité en France le 1er octobre 2016. Cette organisation est un signe fort envoyé par Siemens sur la question du Big Data industriel. La nouvelle organisation a été testée pendant 18 mois en Allemagne et dans plusieurs pays pilotes avant d'être généralisée au niveau des différentes filiales.
L'intérêt ? S'ouvrir à de nouvelles compétences et à de nouveaux métiers à l'ère du numérique et de l'optimisation permanente de la production.

de l'état des machines et une amélioration de la production.

Ouverture à la valeur ajoutée

Les données collectées dans le cloud peuvent ensuite être utilisées dans un tableau de bord, tel que Visual Analyzer, pour répondre aux besoins quotidiens de l'industriel. Ces données peuvent aussi servir d'autres besoins, comme en recherche et développement. Avec son cloud, Siemens s'inscrit en effet dans une dynamique portée par des partenaires spécialistes des algorithmes et de la re-contextualisation de données. Une stratégie qui ouvre la voie à toute une série de travaux collaboratifs avec des écoles d'ingénieurs et des partenaires universitaires.

Gestion sécurisée des données

Concrètement, la technologie MindSphere réside dans MindConnect Nano, un PC industriel compact qui lui est dédié (voir encadré). La configuration s'effectue à l'aide de l'atelier logiciel Fleet Manager. En aval, MindConnect Nano tisse un lien Ethernet pour collecter les données via les automates. En amont, les données sont échangées avec une liaison Internet. Déconnectées de toute signification réelle relative aux machines et au process desquels elles sont extraites, les données transitent de façon chiffrée entre la box et le cloud. Seul le logiciel Fleet Manager, via l'identifiant utilisé, permet de donner leur sens réel aux données.
C'est à l'exploitant, via son service informatique, de déclarer les machines sur lesquelles il souhaite une lecture des données, et de fournir les droits d'accès nécessaires. Il garde en permanence la main sur l'extraction des données vers l'extérieur de son site. D'autres plateformes seront bientôt disponibles sur base S7 1500, S71200, SINUMERIK.

Un mécanisme sous OPC UA

MindSphere est en capacité de collecter les données issues des équipements SIMATIC S7 (S7 300 -400- 1500- 1200), mais aussi de l'ensemble des équipements répondant au standard OPC UA. Ce protocole est notamment reconnu pour ses qualités de gestion sécurisée des données. Si besoin, un automate concentrateur SIMATIC S7 peut jouer le rôle de passerelle intermédiaire en charge de collecter les données.

Une technologie SAP

Le cloud mis en œuvre par Siemens au travers de MindSphere s'appuie sur une technologie de développement identique à celle de la plateforme SAP Hana Cloud Platform, totalement ouverte à la technologie des objets connectés (smartphone, tablettes et autres équipements mobiles). Le stockage des données s'effectue sous technologie SAP Server, sur des serveurs informatiques gérés par Siemens.

Autre services de Plant Data Services

Une multitude de fonctionnalités permet de suivre le comportement des machines. Des modules complémentaires sont proposés :

- **Energy Analytics :** ce tableau de bord dédié aux consommations d'énergie présente une analyse pertinente pour les besoins des exploitants ;
- **Control Performance Analytics :** ce module permet la remontée et l'analyse des boucles de régulation dans le but d'en optimiser le paramétrage.;
- **Plant Security Services :** ce module est capable de minimiser les risques d'intrusion sur un réseau et de mettre en place des audits.
- **Drive Train Analytics :** Gére en ligne la surveillance, le diagnostic, propose une visualisation et le reporting pour des variateurs et moteurs.
- **Fleet manager for Machine Tools :** Gére en ligne la surveillance, le diagnostic, propose une visualisation et le reporting des machines-outils équipés SINUMERIK.

MINDCONNECT NANO GÈRE LA COLLECTE DES DONNÉES

MindConnect Nano est un PC industriel préconfiguré grâce auquel la machine est connectée au cloud via MindSphere. Son rôle ? Collecter les données issues du terrain et les transmettre à la plateforme cloud MindSphere. MindConnect assure la transmission chiffrée au travers d'une connexion Internet sécurisée. Sur les machines à commande numérique, MindSphere s'intègre directement dans les unités SINUMERIK, sans nécessité l'usage de MindConnect Nano.

AMOSSYS, notre expert en évaluations de sécurité CSPN

Dans le cadre des travaux portant sur la cybersécurité des systèmes industriels dirigés par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), Siemens a choisi de faire confiance au Centre d'Évaluation de la Sécurité des Technologies de l'Information (CESTI) AMOSSYS afin de réaliser les évaluations CSPN des produits suivants : SIMATIC S7 1518-4 Version du micrologiciel 1.83 (automate programmable industriel) et SCALANCE XM408-8C (commutateur industriel).

Une évaluation CSPN - Certification de Sécurité de Premier Niveau - est un schéma promu par le centre de certification français de l'ANSSI qui s'appuie sur des critères, une méthodologie et un processus élaborés par l'ANSSI.

La mise en place de ce schéma d'évaluation dont la phase expérimentale s'est tenue durant trois ans (2008 à 2011) est issue du constat suivant :

- Une offre assez limitée de produits SSI dont la qualité a été attestée ;
- Une absence de certification portant sur des logiciels libres ;
- Des coûts et des délais d'évaluation peu ou pas adaptés au marché des produits SSI civils ;
- Des produits de sécurité avec des mécanismes de base de plus en plus complexes et hétérogènes, souvent hors de portée du cadre normatif et de plus en plus souvent intégrés au système d'exploitation ou à l'environnement opérationnel.

AMOSSYS est une société française de conseil et d'expertise en Cybersécurité. Évaluation de produits de sécurité, recherche et développement, logiciels innovants sur mesure, audit, conseil, forensic... AMOSSYS intervient sur l'ensemble des problématiques de cybersécurité et accompagne les entreprises de toute taille et de tout secteur d'activité dans la sécurisation et la défense de leurs systèmes d'Information.
Gage de la qualité de ses prestations, AMOSSYS bénéficie par ailleurs de la reconnaissance des plus hautes instances étatiques françaises : Centre d'Evaluation de la sécurité des Technologies de l'Information (CESTI) agréé par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Prestataire d'Audit de la Sécurité des Systèmes d'Information qualifié par l'ANSSI et certificateur de jeux en ligne.

La mise en place du schéma CSPN répond donc à des besoins liés au marché de l'évaluation de produits de sécurité civils (temps contraint adapté au versionnage des produits, coûts optimisés) et répond à des besoins purement techniques tels que privilégier l'expertise technique à la complétude méthodologique.
Le certificat CSPN d'un produit permet ainsi de valider que ce dernier a subi avec succès des tests fonctionnels et résiste aux vulnérabilités connues pour le type de service de sécurité qu'il fournit.
Ce schéma, délivré par le centre de certification de l'ANSSI sur la base d'une évaluation réalisée par un laboratoire agréé, est éprouvé et robuste.

L'évaluation d'un produit selon le schéma CSPN nécessite par ailleurs plusieurs étapes.

Il faut tout d'abord s'assurer que les services de sécurité annoncés par une cible d'évaluation soient effectivement rendus. Des analyses sont ensuite menées pour s'assurer de la robustesse d'une cible d'évaluation. Ce type d'évaluation permet d'obtenir des résultats fiables en temps contraint.
Avant de réaliser les évaluations, Siemens et AMOSSYS ont ainsi collaboré ensemble pour rédiger les cibles de sécurité. Le cœur d'une cible de sécurité est la partie relative à l'étude du problème de sécurité et s'articule autour des utilisateurs, biens sensibles, menaces, hypothèses et fonctions de sécurité. Le travail réalisé au titre de cette phase est déterminant pour la suite de l'évaluation car il permet, notamment dans un document autoporteur, de fixer les conditions d'emploi du produit ainsi que les hypothèses sur l'environnement.
Une fois les cibles de sécurité rédigées et validées par l'ANSSI, le CESTI AMOSSYS a entrepris la démarche d'évaluation selon ces principales étapes :

- installation du produit à évaluer (avec l'assistance de Siemens)
- analyse de la conformité (analyse de la documentation, tests des fonctions de sécurité sous l'angle de la conformité)
- analyse de la résistance des mécanismes et fonctions de sécurité ainsi que l'analyse des vulnérabilités intrinsèques, de construction, d'exploitation, etc.

À titre illustratif, et de façon non exhaustive, le CESTI AMOSSYS a réalisé pour l'automate programmable industriel des tests de fuzzing, analysé la résistance du produit face à des dénis de service, analysé la résistance des protocoles gérés par l'automate, analysé les mises à jour et réalisé des tests sur le TIA Portal (outil permettant de gérer à distance l'automate).
Les évaluations réalisées par le CESTI AMOSSYS n'ont mis en lumière aucune vulnérabilité critique sur chacun des produits évalués. L'ANSSI a ainsi délivré les certificats CSPN pour l'automate SIMATIC S7 1518-4 le 25 avril 2016 et pour le commutateur XM408-8C le 13 juin 2016.

Antoine Coutant

Depuis 16 ans, Antoine COUTANT travaille dans le domaine de la sécurité informatique (cryptographie, SSI, développements logiciels, ...). Il a commencé sa carrière au Ministère de la Défense dans un laboratoire de R&D en cryptanalyse. De 2008 à 2011, il fut ingénieur sécurité au CESTI d'Orange Business Services (ex Silicomp-AQL) en tant qu'évaluateur Critères Communs et CSPN. Dans ce laboratoire, il a également dirigé le laboratoire cryptologie et R&D du CESTI. Depuis juin 2011, Antoine est le responsable technique du CESTI d'AMOSSYS et il dirige actuellement l'ensemble des activités d'AMOSSYS (audit, conseil, évaluation, R&D, CERT, logiciels innovants).

SIEMENS
Ingenuity for life

*L'ingéniosité au service de la vie

Votre portail vers l'automatisation dans l'entreprise numérique

Totally Integrated Automation Portal

Que vous soyez constructeur de machines ou exploitant - à l'aide d'outils de simulation vous réduirez le temps de mise sur le marche de vos produits. Vous gagnerez en efficacité dans la production grâce à des fonctions supplémentaires de diagnostic et de gestion de l'énergie. La connexion au niveau de gestion de l'entreprise augmente votre flexibilité. Profitez de ces avantages et de bien d'autres encore dans TIA Portal. C'est plus qu'un environnement d'ingénierie – c'est le portail idéal vers l'automatisation dans l'entreprise numérique.

siemens.com/tia-portal