Cybersécurité des systèmes industriels

Synthèses – Comment se protéger

Siemens Digital Industries | 2021

SIEMENS

Quelques décennies d'Histoire: du relais à l'automate

Software

Hardware

Du Germanium au Silicium

Wiring

PLC

TIA

SIMATIC STEP 7
SIMATIC WinCC
SIMATIC WinCC flexible

SIMATIC IT

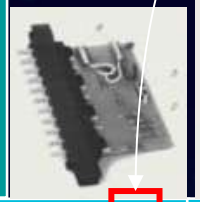
TIA Portal with
STEP 7
WinCC
Safety

STUXnet

TIA Portal

S7-1200

S7-1500 plus
TIA Portal



SIMATIC G	SIMATIC S3	SIMATIC S5	SIMATIC S7 200-300-400 SIMATIC S7 1200-1500 avec TIA Portal
1958	1973	1979	1995 1996 2012 2009 2010 2020…

SIEMENS

Sensibiliser et former mes équipes aux risques cyber
Pour sécuriser le « maillon le plus faible » de la chaine

Situations quotidiennes typiques

Exemple de scénario

"Que se passerait-il si un dispositif de contrôle apparemment sans importance était manipulé de telle manière qu'une recette de produit était modifiée et que le produit en résultant rendait les gens malades?"

Test des connaissances

Formation Cybersécurité des systèmes industriels (DI-CYBER)

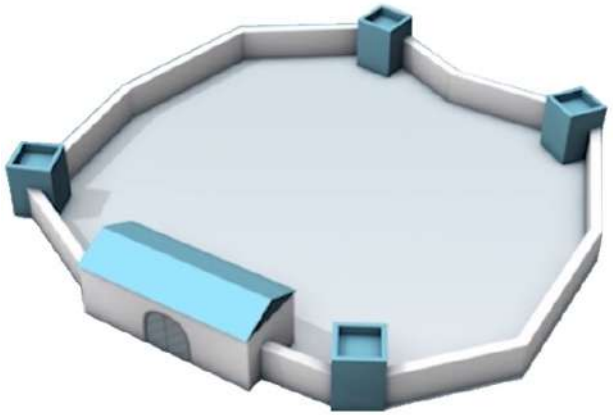
Labelisée (2019)

SIEMENS

Protéger la production – mais comment?
La solution: avec le concept de Défense en Profondeur

Mur

- Un seul niveau de défense
- Facile à faire tomber – une seule attaque avec succès peut suffire



Un seul niveau de défense ne fournit pas une protection suffisante!

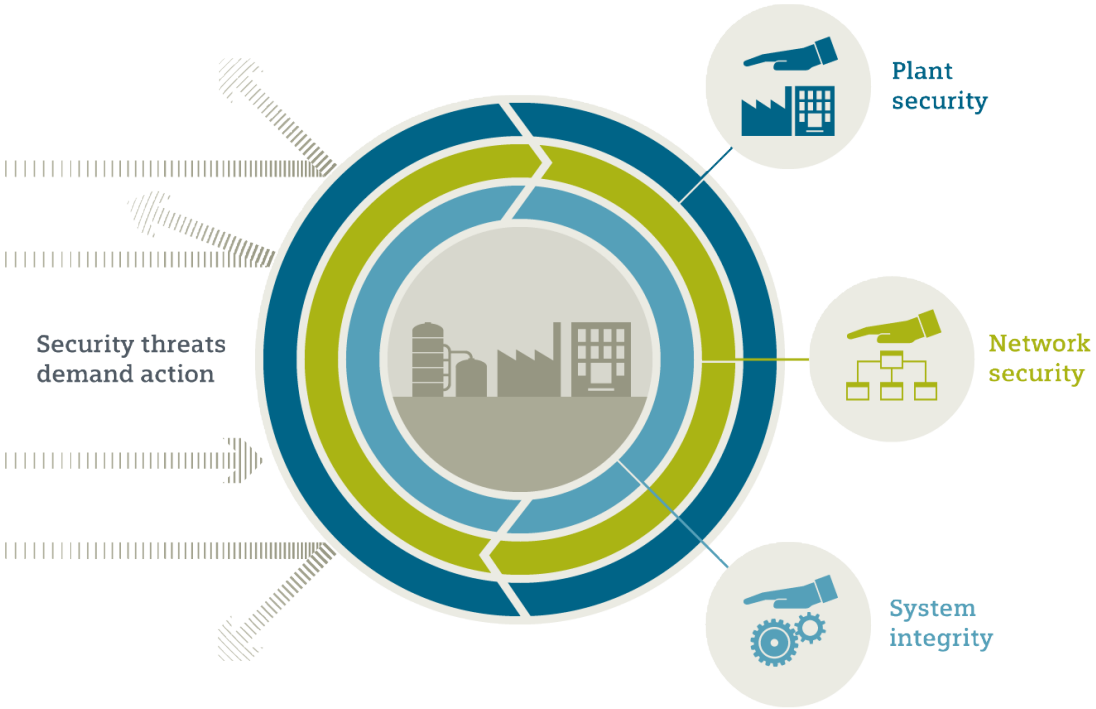
Défense en profondeur

- Des niveaux de sécurité multiples et indépendants
- Difficile à faire tomber – l'attaquant doit investir énormément de temps, d'efforts et de savoir-faire pour avoir une chance de réussir

SIEMENS

Sécurité des Systèmes Industriels

Le concept de sécurité de Siemens – “La Défense en Profondeur”



L’offre produit et Système de Siemens intègre la sécurité industrielle

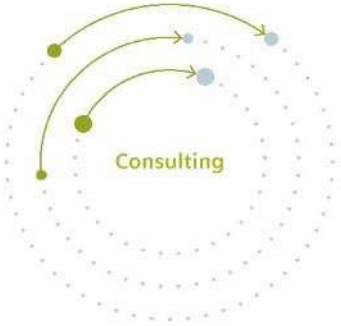
Protection de la connaissance et protection contre la copie

Authentification et gestion des droits utilisateurs

Firewall and VPN (Virtual Private Network)

Durcissement des systèmes, supervision et détection des anomalies

Siemens Industrial Security Services



SIEMENS

L’analyse de risques et vulnérabilités + La cartographie des assets industriels

Le point de départ pour prioriser et connaitre les mesures spécifiques à mettre en place

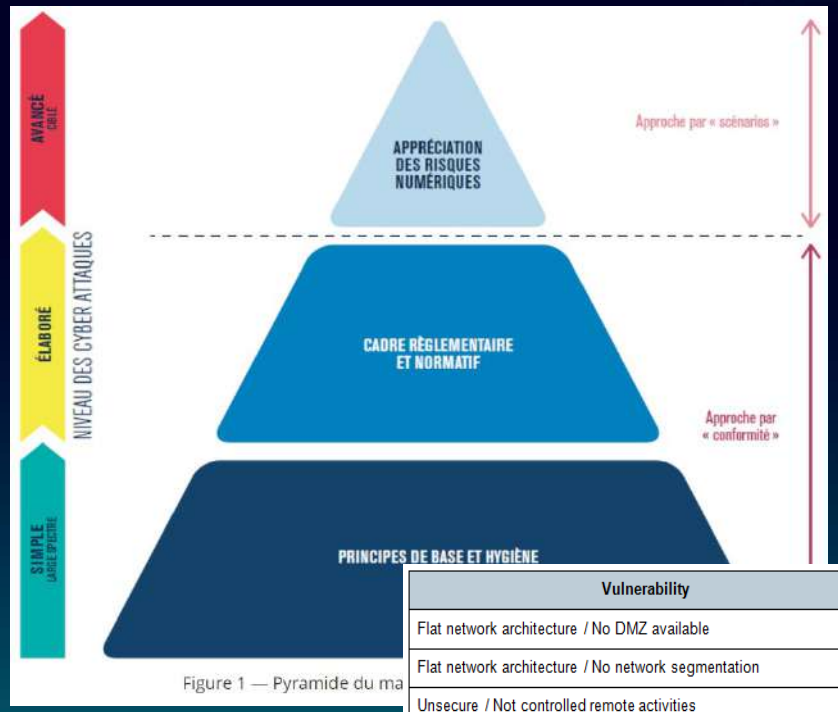


Figure 1 — Pyramide du ma

			Gravité				
			Mineure	Significative	Sévère	Critique	Catastrophique
Probabilité	Fréquent	A					
	Probable	B					
	Peu probable	C					
	Rare	D					
	Extrêmement rare	E					

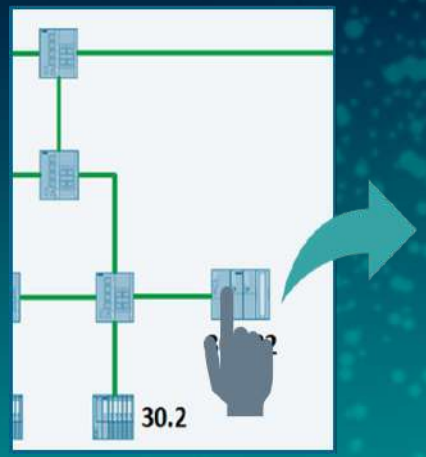
	Risque inacceptable, mesures indispensables de réduction du risque
	Risque à surveiller, mesures adaptées de réduction du risque
	Risque acceptable

set-revue.fr

Vulnerability	Risk Score
Flat network architecture / No DMZ available	8,1
Flat network architecture / No network segmentation	8,1
Unsecure / Not controlled remote activities	7,4
No system hardening / Unneeded applications and services installed	7,1
Unpatched operating systems	6,8
Obsolete anti-virus database	6,6
Windows firewall not active	5,6
Uncontrolled USB interfaces	4,8

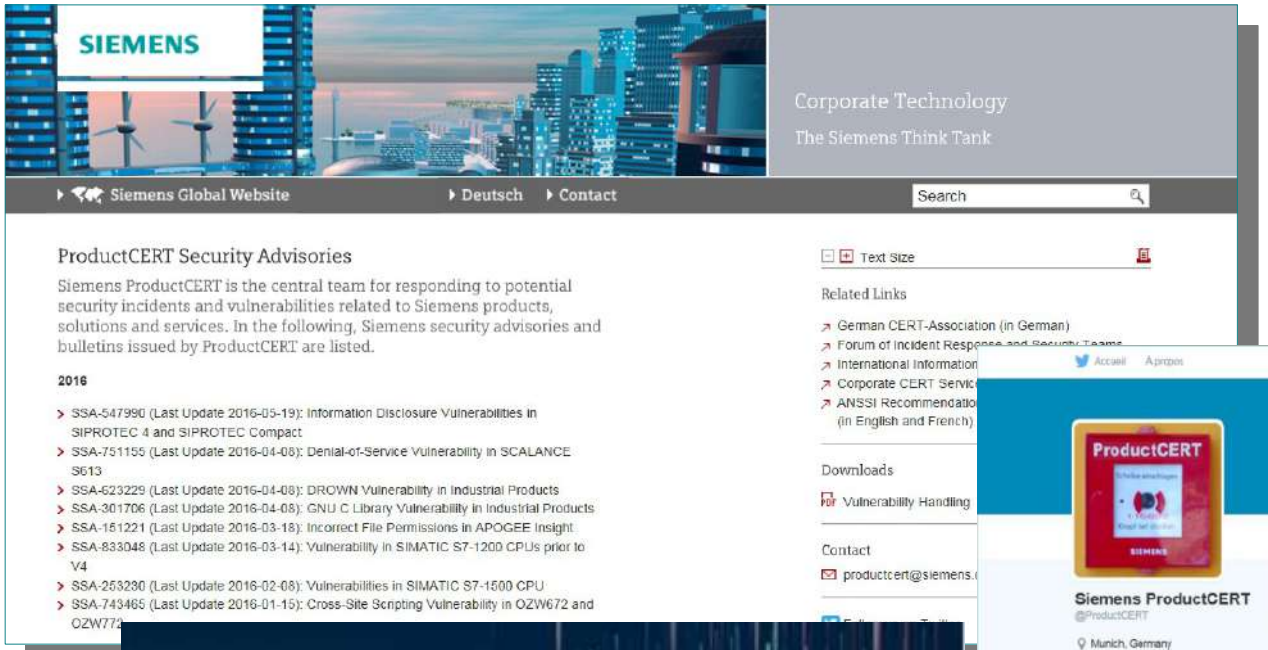
Table 1: Risk Scoring (direct risks) according to CVSS

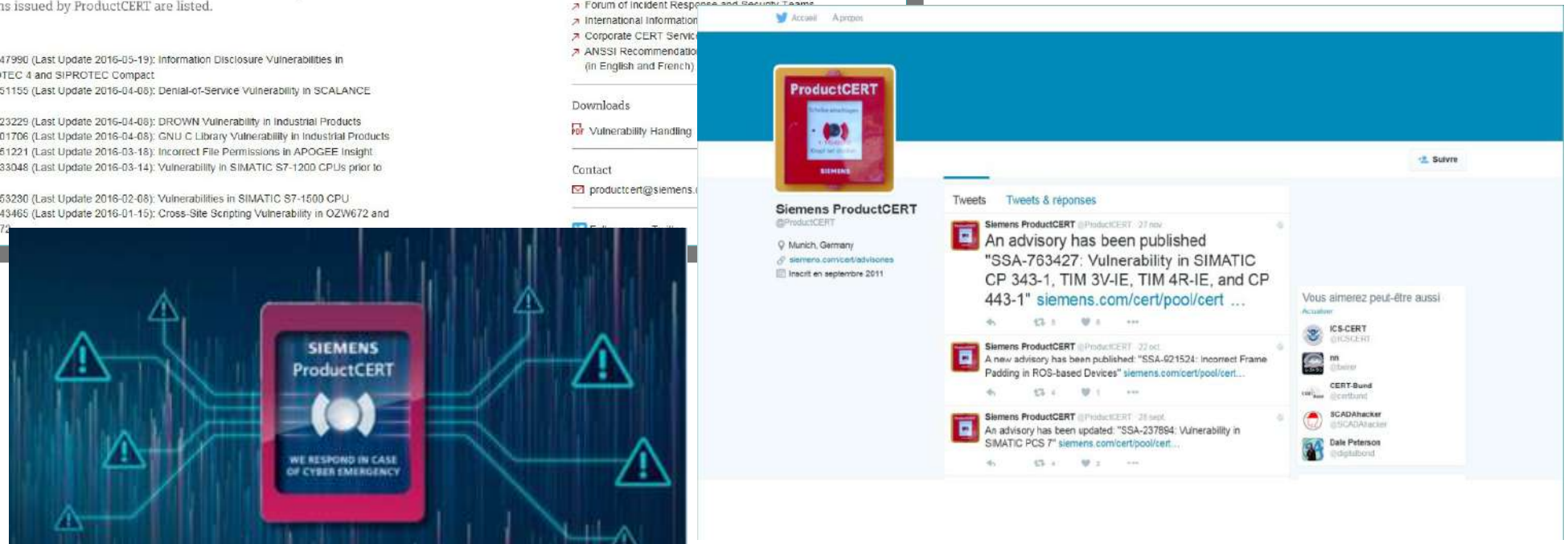
- Red [7,5-10] – Unacceptable risk; Urgent action is necessary
- Orange [5-7,5] – Unacceptable risk; Action is required
- Yellow [2,5-5] – Acceptable risk; Subject to management approval
- Green [0-2,5] – Acceptable risk; No action required



SIEMENS

Gérer les vulnérabilités de ses équipements
Le Computer Emergency Response Team (CERT)





Suivez-nous sur Twitter ou via notre flux RSS

SIEMENS

Certification de Sécurité de 1er Niveau (CSPN)

Printemps 2016 – les 2 premiers lauréats des systèmes industriels suivi par la qualification de la gamme complète des S7-1500 en 2017

Simatic S7-1518

Certifié et Qualifié (Avril 2016)

Scalance XM408

Certifié (Juin 2016)

Famille Simatic S7-1500

20 produits qualifiés (2017 puis 2019)

Simatic S7-1513R & S7-1515F

Qualifié (Octobre 2020)

Simatic S7-1517H

Qualifié (Octobre 2020)

Formation Cybersécurité des systèmes industriels (DI-CYBER)

Labelisée (2019)

Certification et Qualification
Rappel (extrait site ANSSI)

SIEMENS
Ingenuity for life

La qualification

Elle permet d'attester d'un certain niveau de sécurité et de confiance dans les produits listés dans le catalogue des produits qualifiés. La qualification offre donc des garanties de sécurité et de confiance aux acheteurs de produits. Le recours à des produits qualifiés est parfois imposé par le cadre légal ou réglementaire : protection des opérateurs d'importance vitale…
Dans tous les cas, si un produit qualifié offre les fonctions attendues par l'acheteur, il est recommandé d'y recourir en priorité, et ce même si l'acheteur n'est soumis à aucun texte légal ou réglementaire l'y obligeant.

http://www.ssi.gouv.fr/administration/qualifications

La certification

Elle permet d'attester par une tierce partie indépendante et impartiale qu'un produit atteint, à un instant donné, un niveau de résistance à un niveau d'attaques donné : en France, quel que soit le type d'évaluation, la certification s'appuie sur des vérifications de conformité, sur des tests d'intrusion pour déterminer le niveau de sécurité réellement atteint par le produit.

http://www.ssi.gouv.fr/administration/produits-certifies/cspn/

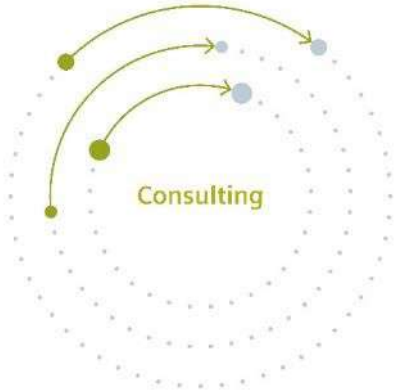
Point primordial…

SIEMENS
Ingenuity for life

A ce jour, …

Les CPUs de la Division Digital Industries de Siemens France sont les seules sur le marché français à être qualifiées par l'ANSSI !

Sécurité des systèmes industriels
Une offre de protection complète



Evaluation de la sécurité

Evaluation agnostique du statut de sécurité actuel d'un environnement industriel

- Accompagnement des OIV à l'homologation
- Check de la sécurité Industrielle
- Evaluation IEC 62443
- Evaluation ISO 27001
- Evaluation des Risques & Vulnérabilités
- Consulting sur la Sécurité Industrielle
- Scanning Services
- Cartographie de l'architecture industrielle

Implémentation de la sécurité

Diminution des risques à travers l'implémentation de mesures de sécurité

- Formations et sensibilisation à la Cybersécurité des Systèmes Industriels
- Pare Feux Nouvelle Génération
- Liste Blanche
- Anti Virus
- Sauvegarde et Restauration
- Station de décontamination

Gestion de la sécurité

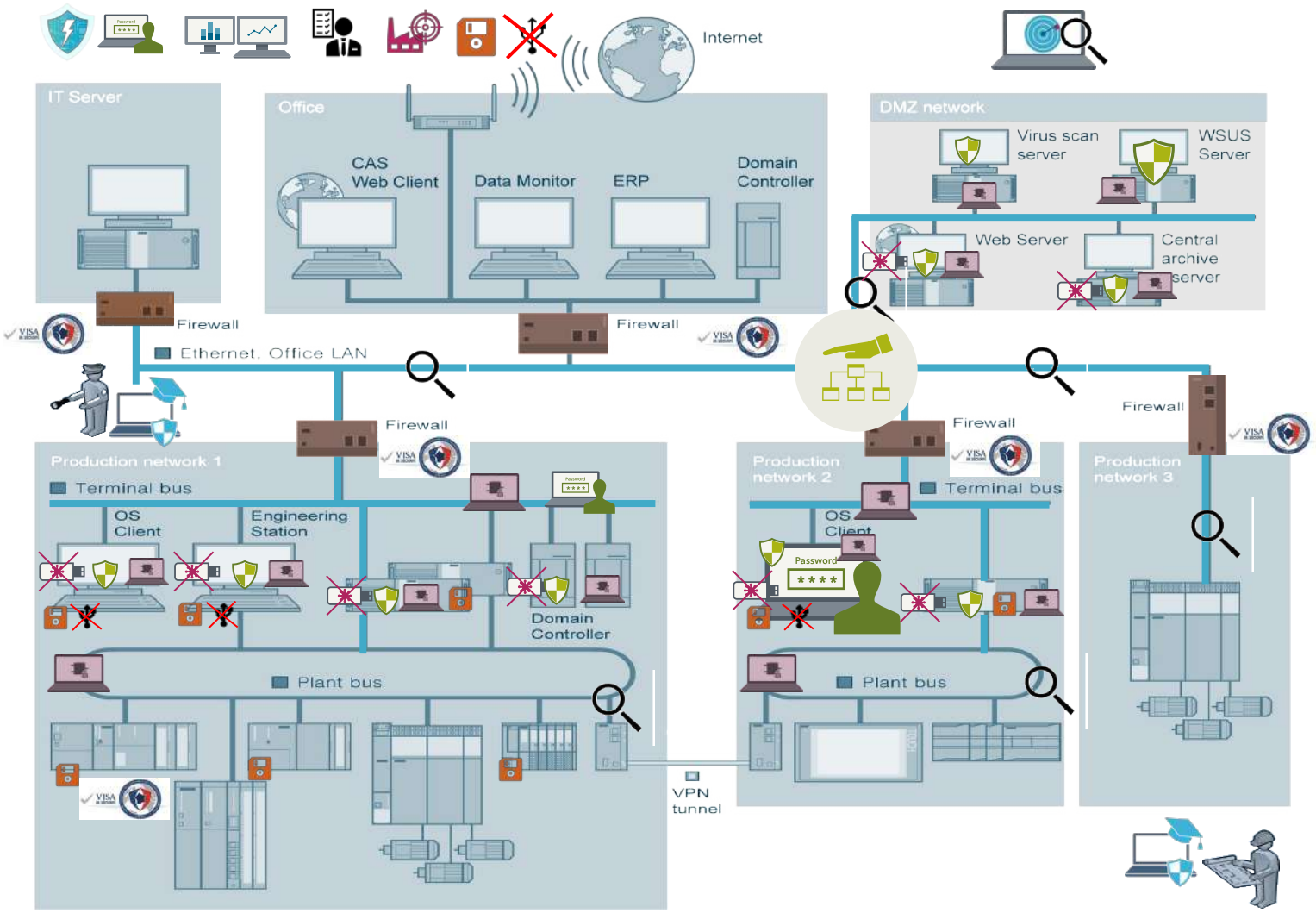
Une sécurité complète à travers des services de gestion

- Détection des anomalies
- Supervision de la Sécurité Industrielle
- Gestion des Incidents à distance
- Gestion des Vulnérabilités Industrielles
- Gestion des Patchs
- Package de services pour la sécurité des SIMATIC

SIEMENS

Sécurité des systèmes industriels
Exemple d‘implémentation

SIEMENS
Ingenuity for life



Industrial Security Services

- Evaluation de sécurité - Consulting
- Cartographie de l‘architecture industrielle
- Formation et sensibilisation à la Cybersécurité des Systèmes Industriels
- Antivirus et Liste Blanche
- Durcissement du système
- Gestion des Identités et des Accès
- Pare feux industriels, Ségmentation des réseaux et VPN
- Zone Démilitarisée
- Patchs Windows
- Gestion de la Sécurité des Vulnérabilités
- Détection des Anomalies de l‘architecture industrielle
- Supervision de la sécurité
- Sauvegarde et Restauration
- USB Station

SIEMENS
Ingenuity for life

Sécurité des Systèmes Industriels

Aspect réseau – Présentation Scalance

www.siemens.com/industrial-security-services

SIEMENS
Ingenuity for life

Gamme Scalance S

Appareils de Sécurité Industrielle – SCALANCE S
Différentes tailles pour un ajustement prix / performance optimal

SIEMENS
Ingenuity for life

Industrial security appliance SCALANCE S

SC632-2C **SC636-2C** **S615** **SC642-2C** **SC646-2C**

SCALANCE SC-600
Appareil de sécurité industrielle haute-performance

SIEMENS
Ingenuity for life

http://www.siemens.com/scalance-s

- Fair highlight
- SPS highlight
- INC wall, Security wall
- Product News SPS18

Delivery start: 12/2018

Caractéristiques / Fonctions	Bénéfices
Passerelle pare feux NEW	Vérification et filtrage des données de couche 2, par ex. pour une utilisation dans les passerelles sécurisées
Supporte les protocoles redondants: • **MRP et HRP Client** [1)] • **VRRP-coupling, STP/RSTP** NEW	Intégration dans des structures réseau redondantes. Des switchs / routeurs de sécurité aditionnels ne sont plus nécessaires.
Pare-feu ou performances de chiffrement envir. 600 Mbps ou 120 Mbps respectivement	Débit de données élevé et la meilleure sécurité des données possible sur le réseau.
Virtual Private Network: VPN (IPsec) [1)]	Écoute et protection de l'intégrité
• **Jusqu'à 6 ports** • **2 d'entre eux sont des ports combo**	• Ports configurables – en fonction de la structure des besoins et des quantités • Peut être équipé avec SFPs pour les topologies FO
• **Pare feu d'inspection dynamique/ pare feux user-specific** • **NAT/NAPT** NEW	• Protection contre les accès réseau non-autorisés • Intégration des réseaux avec des @IP identiques (ex. serial machines)
Permet des concepts flexibles de zones de sécurité.	Séparation réseaux, DMZ (ex: pour accès distants)
• **Intégration avec TIA Portal** • **Intégration avec SINEC NMS** NEW	• Ingénierie de bout en bout dans TIA Portal • Diagnostiques et gestion centrale des firmwares
Intégration avec SINEMA Remote Connect	Accès à distance sécurisé aux machines / usines

[1)] Only SCALANCE SC642-2C, SC646-2C

Appareils de Sécurité Industrielle – SCALANCE S
Protection des réseaux industriels avec SCALANCE S615

SIEMENS
Ingenuity for life

Caractéristiques / Fonctions	Bénéfices
Firewall et VPN (IPsec et OpenVPN avec SINEMA RC)	Protection contre les accès non autorisés venant de l'extérieur et la transmission de données associée
Différentes zones de sécurité via VLAN	Haut niveau de flexibilité pour la configuration du pare feu
Entrée numérique pour la création de tunnel contrôlé	Communication via des réseaux non protégés uniquement si nécessaire
Interface d'auto-configuration pour SINEMA Remote Connect	Gain de temps et de cout Pas besoin d'avoir des connaissances élevées.
Intégration avec TIA Portal[1)] et SINEC NMS[2)]	Gestion du réseau et ingénierie de bout en bout via TIA Portal.

[1)] TIA Portal V15 or higher
[2)] Planned start of delivery in 9/2018

SIEMENS
Ingenuity for life

Gamme Scalance X

Commutateurs Ethernet industriel manageables SCALANCE X

Les commutateurs industriels manageables de la famille de produits SCALANCE X sont adaptés pour la configuration de **topologies réseaux en ligne, en étoile et en anneau.**

Les commutateurs SCALANCE X-200, X-300, X-400 et X-500 peuvent **contrôler l'accès au réseau** et possèdent les **fonctions de sécurité** suivantes:

- Gestion ACL (Access Control List)
- IEEE 802.1X (RADIUS)
- 802.1Q-VLAN – permet une séparation logique du trafic de données entre les ports prédéfinis sur les commutateurs.
- Broadcast/Multicast/Unicast Limiter
- Broadcast blocking

De plus, les **protocoles sécurisés** suivants sont pris en charge:

- SSH
- HTTPS
- SNMP v3

Ligne de produit X-200

SCALANCE XM
Structure de base de l'appareil

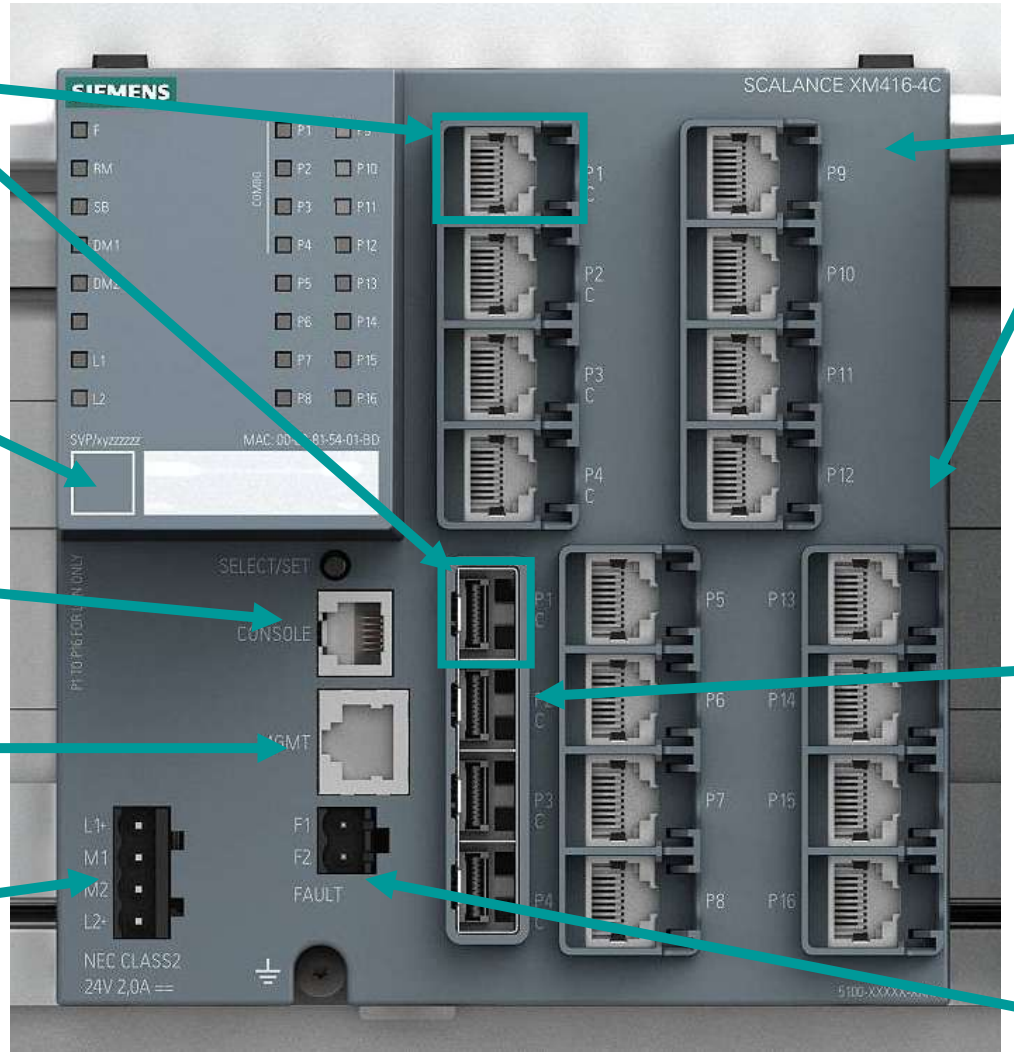
Combo ports
Technologie de connecteur alternative:
RJ45 ou SFP comme demandé

NFC
Option de diagnostic mobile grâce à NFC et WLAN
- Site mobile du SCALANCE XM-400
- Surveillance et diagnostic simples des appareils et du réseau

Console port
- Interface Série RJ11
- Gestion et diagnostics via CLI

Management Ethernet port
- Interface RJ45 10/100/1000 Mbps
- Gestion out-of-band pour la configuration et les diagnostics

Input voltage
Borne à 4 broches pour le raccordement d'une alimentation redondante (2 x 24 VDC)



16 x RJ45 ports

4 x SFP slots
pour 100/1000 Mbps SFP transceivers

Contact de signalisation

Commutateur Ethernet industriel manageable SCALANCE XC-200:

«Basculez vers le futur» avec les meilleurs composants IEC 62443-4 de leur catégorie

SIEMENS
Ingenuity for life

Exigences IEC 62443	Caractéristiques produit
• Comptes utilisateur / Identification utilisateur	• Local ou • Central via RADIUS et UMAC *
• Segmentation réseau/ Restriction des flux de données	• Sur couche 2 avec VLAN • Utilisation non prévue comme par ex. un Pare-feu
• Supervision Réseau / Sécurité	• Syslog client • SNMPv3
• Sauvegarde / Restauration	• Localement via C-Plug • (à distance) admin via SSH (+?) • En central via SINEC NMS
• Sécuriser le plan de gestion	• WBM via HTTPS par défaut • SSH par défaut

SIEMENS
Ingenuity for life

Gamme Scalance M

SCALANCE M876-3/ M876-4
Connection aux réseaux sans fil mobile 2G, 3G et 4G

SIEMENS
Ingenuity for life

Caractéristiques / Fonctions	Bénéfices
Débit de données élevé (100 Mbps descendant, 50 Mbps montant) et diversité d'antenne.	Transmission de débits de données élevés via une connexion sans fil robuste
Plage de température étendue (-20°C à +60°C)	Utilisation dans des environnements avec des fluctuations climatiques accrues
Mécanismes de sécurité supportés: IPsec, OpenVPN, firewall	Sécurité accrue du réseau grâce à l'utilisation de normes communes
4-ports switch manageables intégrés	Jusqu'à 4 adresses IP peuvent être configurées pour différents sous-réseaux
Alimentation redondante	Fonctionnement fiable, même en cas de panne d'une alimentation
Prise en charge des normes spécifiques	Utilisation mondiale généralisée
Compatible avec SINEMA Remote Connect	Maintenance pratique et sécurisée des machines et des installations via un accès à distance
Entrée/Sortie numériques	Connection simple des modules I/O

SCALANCE M812/816
Accès au réseau public via ADSL

SIEMENS
Ingenuity for life

Caractéristiques / Fonctions	Bénéfices
Connection aux réseaux téléphonique ou DSL	Taux de transmission jusqu'à 25 Mbps
Chiffrement de bout en bout	Protection contre les accès non autorisés
Fonctionnalité de routage intégrée (M816)	Enregistre le deuxième commutateur
Entrée/Sortie numériques	Connexion simple des modules I/O
Alimentation redondante 24V	À l'abri des pannes et haute disponibilité

SCALANCE M826-2
Utilisation des câbles existants et privés

SIEMENS
Ingenuity for life

Caractéristiques / Fonctions	Bénéfices
Utilisation d'un modem SHDSL	Connexion pas chère et sécurisée
Ethernet industriel sur de longues distances	Protège les réseaux segmentés contre les accès non autorisés
Câbles bifilaires et multifilaires existants	Taux de transmission symétrique élevés
RSTP (Rapid Spanning Tree) sur les ports Ethernet	Haute disponibilité grâce à la redondance en anneau à la fois via la connexion SHDSL et via les connexions Ethernet
Chiffrement de bout en bout au travers d'un tunnel IPsec	Protection contre les accès non autorisés

SCALANCE M804PB
Connection aux systèmes existants avec PROFIBUS/ MPI

SIEMENS
Ingenuity for life

Caractéristiques / Fonctions	Bénéfices
Interface PROFIBUS/MPI pour la connexion de PROFIBUS à des réseaux Ethernet en combinaison avec SINEMA Remote Connect (plate-forme de gestion pour réseaux distants)	Connexion directe, pratique et économique d'installations existantes avec PROFIBUS / MPI à SINEMA RC (sans appareils supplémentaires) pour un accès à distance sécurisé aux machines et aux installations distantes.
Interface utilisateur et fonctions du firmware analogues à SCALANCE M-800/S615 (par ex. prise en charge VLAN ; un sous-réseau interne peut être configuré ; entrée/sortie numérique ; WBM / CLI / SNMP)	Utilisation et fonctionnalité familières de la famille SCALANCE M800/S615 grâce à une base de firmware uniforme
Connexion TIA Portal Cloud Connector	Gestion centralisée simple du logiciel d'ingénierie (TIA Portal) sur un seul serveur
Interface utilisateur et concept de commande analogues à la gamme existante SCALANCE M-800/S615 basée sur MSPS	Manipulation aisée et compatibilité avec les systèmes existants (portefeuille SIMATIC, logiciel de gestion de réseau, etc.)
Entrée/Sortie numériques	Permet le contrôle d'accès sur site via keyswitch
Prend en charge l'accès à distance des anciennes installations avec Step 7 V5.5 et versions ultérieures	Concept de télémaintenance uniforme pour les installations nouvelles et existantes

Contact

Publié par Siemens SAS

Thomas JAUNIAUX

Responsable des services de cybersécurité
DI / FR / CS - ISS
40 Avenue des Fruitiers
93200 Saint-Denis
France
Mobile +33 6 09 78 02 23
E-mail thomas.jauniaux@siemens.com

Vincent Bouvet

Ingénieur des ventes

Dept 45 18 36

40 avenue des Fruitiers
93527 Saint-Denis Cedex, Frankreich
Tel.: +33 627992161
Fax: +33 149223202
Mobil: +33 627992161
mail : vincent.bouvet@siemens.com
www.siemens.com

Eric Gilmant
Directeur de Région
Nord-Paris-Centre

SIEMENS
Digital Industries
40 avenue des Fruitiers
93527 Saint-Denis Cedex
Mob : 00 33 6 80 34 87 09
E-mail : eric.gilmant@siemens.com

SIEMENS