
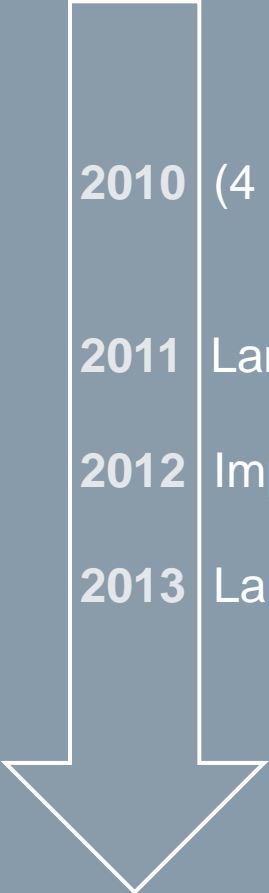


Un sujet nouveau

La cybersécurité

Que fait Siemens en la matière ?

- 
- 1998** Création du CERT Siemens pour la protection des infrastructures IT internes du groupe.
 - 2004** Création du laboratoire de sécurité pour WinCC et PCS7.
 - 2005** Naissance de la gamme Scalance S (firewall et modules VPN)
Publication du premier guide de mise en sécurité des systèmes PCS7 et WinCC.
 - 2006** Sécurisation des installations de production.
 - 2008** Intégration dans les roadmap produits de fonctions de sécurité.
 - 2010** Apparition du malware Stuxnet.

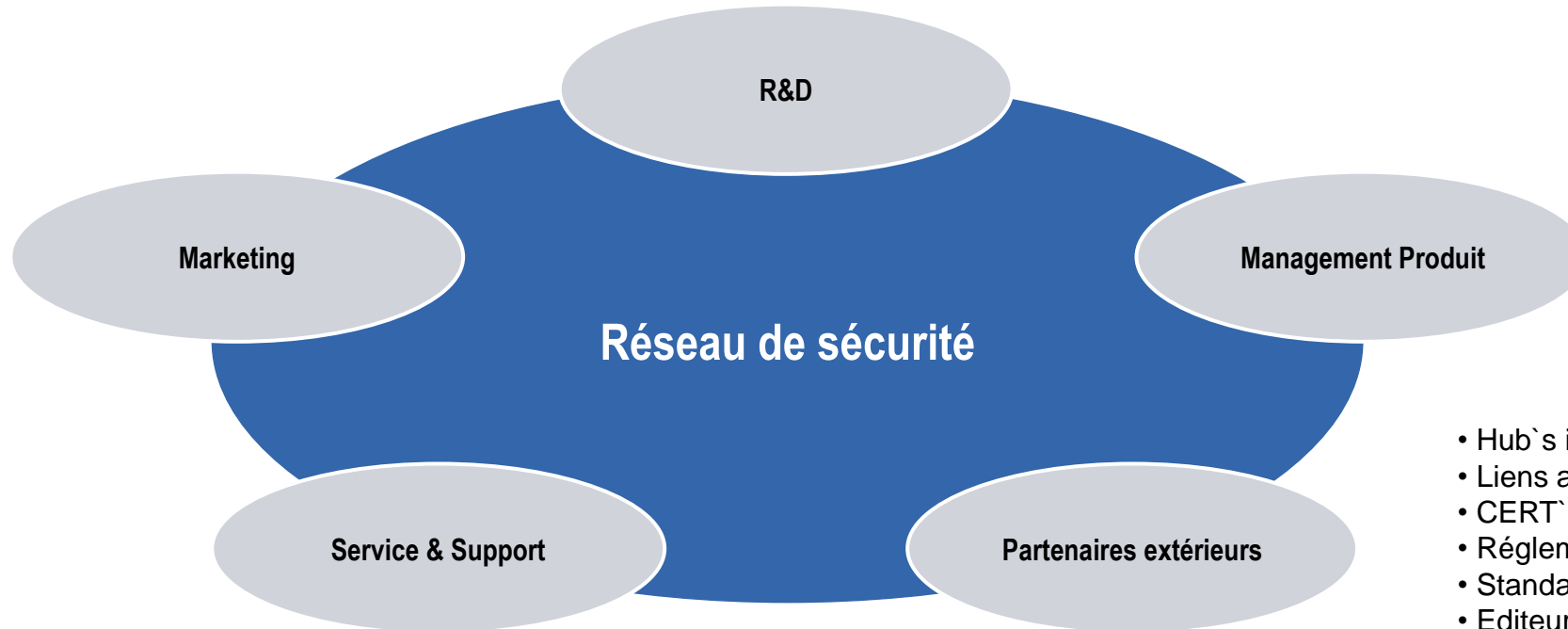


2010 (4 semaines) Mise à disposition par Microsoft, Siemens et différents éditeurs de logiciels d'antivirus, d'une première solution de détection et d'élimination de ce malware.

2011 Lancement du projet "Industrial Security".

2012 Implémentation de fonctions de sécurité dans une large gamme de produits.

2013 Lancement du S7-1500 avec fonctions de sécurités intégrées.



- Hub`s internationaux
- Liens avec organismes étatiques
- CERT`s
- Réglementation Import / Export
- Standardisation & Normalisation
- Editeurs de logiciels de sécurité
- Réseau de sécurité des éditeurs logiciels OEM`s

Mise en place d'un réseau de sécurité pour ...
...réagir rapidement en cas de situation de crise
...piloter et coordonner tous les sujets relevant de la sécurité

+ System Test

- IP Hardening
- Durcissements des tests de robustesse

+ Process d'escalade et de réaction en cas d'incident

- Process d'escalade et de réaction définis et fonctionnels

+ Nouveaux postes

- Product Security Officer et Security Expert

+ Modifications des Process

- Guide de codage, analyse statique de code, etc. pour la R&D
- Mise en place d'une politique de gestion du risque dans le cycle de vie produit.

+ Standards & Regulations

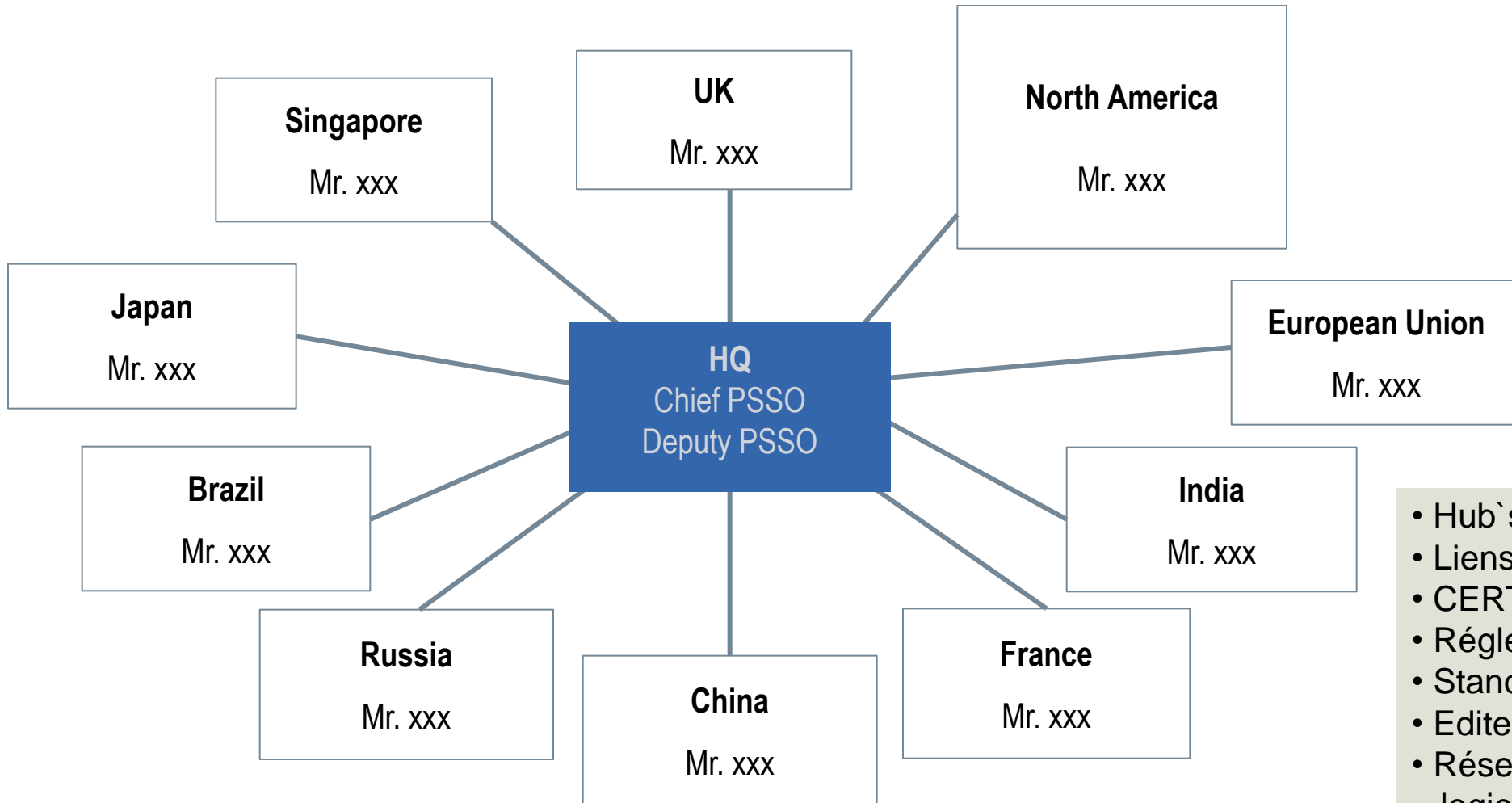
- Forte coopération avec les organismes de standardisation
- Certifications Achilles Niveau 2 ...

+ Sensibilisation et renforcements des connaissances

- Workshops, formation en ligne obligatoires, conférences, présentations
- Formations spécifiques pour les développeurs

Sécurité industrielle

Un réseau international



- Hub`s internationaux
- Liens avec organismes étatiques
- CERT`s
- Réglementation Import / Export
- Standardisation & Normalisation
- Editeurs de logiciels de sécurité
- Réseau de sécurité des éditeurs logiciels OEM`s

Création d'un site Internet sur la cybersécurité industrielle ouvert à tous

The screenshot shows the Siemens Industrial Security website. At the top left is the Siemens logo. Below it is a navigation bar with links for 'Siemens Industry Sector', 'Deutsch', and 'Contact'. To the right is a 'Site Explorer' search bar. Below the navigation bar is a breadcrumb trail: 'Industrial Security > News/Alerts > News'. The main content area is divided into two columns. The left column is titled 'Industrial Security News' and contains a paragraph about the news ticker, followed by an 'Overview' section with a list of news items, each with a downward arrow icon and a date. The right column contains a 'Text Size' control, a 'SHARE' button, and a 'Find out more about' section with three items: a PDF brochure, a link to 'Industrial Security in the United States', and a contact instruction.

SIEMENS

Industrial Security

Siemens Industry Sector ▶ Deutsch ▶ Contact ▶ Site Explorer Search

> Industrial Security > News/Alerts > News

Industrial Security News

Take advantage of our news ticker to obtain an overview of current developments in the area of industrial security.

Overview

- ▼ New Vulnerability 06/18/2013
- ▼ New Vulnerability 06/14/2013
- ▼ New Vulnerability 05/24/2013
- ▼ New Vulnerability 03/15/2013
- ▼ New Vulnerability 03/15/2013
- ▼ New Vulnerability 02/13/2013
- ▼ New Vulnerability 01/23/2013
- ▼ New Vulnerability - 01/11/2013
- ▼ New Vulnerability - 12/20/2012
- ▼ New Vulnerability - 12/12/2012
- ▼ New Vulnerability - 12/12/2012
- ▼ Achilles Level 2 Certification
- ▼ New Vulnerability - 10/08/2012
- ▼ New Vulnerability - 09/13/2012
- ▼ New Vulnerability - 09/10/2012
- ▼ New vulnerability - 08/31/2012
- ▼ New Vulnerability - 08/21/2012
- ▼ New Vulnerability - 08/10/2012
- ▼ New Vulnerability - 07/31/2012
- ▼ Siemens summary relating to ICS Alert 11-223-01
- ▼ New Vulnerability - 06/05/2012
- ▼ New Article
- ▼ Hanover Fair 2012

Text Size SHARE

Find out more about

- ▼ PDF Brochure "Security all around - Industrial security for your plant-at all levels."
- > Industrial Security in the United States
- > For all other questions regarding industrial security, please contact the experts on our consulting team.

The screenshot shows the Siemens Industrial Security website. At the top left is the Siemens logo. The main header area contains the text "Industrial Security". Below this is a navigation bar with links for "Siemens Industry Sector", "Deutsch", and "Contact". A "Site Explorer" search bar is also present. The main content area is titled "White Papers and Further Information" and includes a paragraph: "On this page, we have compiled current documents and white papers on the topics of industrial security and Security Integrated." Below this is a featured white paper titled "Security concept for the protection of industrial plants" with a small thumbnail image and a "Download PDF" link. A list of other white papers is provided below, including "Operational Guidelines", "ARC white paper cyber security", "Security for S7-controller", "Security white paper PC-based", "ARC whitepaper on Industrial Security in PCS 7", "SIMATIC PCS 7 / WinCC Security concept - White paper", and "Security concept COMOS (German only)". There is also a section for "Technical articles" and "Security concept PCS 7 & WinCC". A callout box on the right side of the page highlights the featured white paper, providing a larger description and a "Download PDF" link.

Security concept for the protection of industrial plants

This whitepaper gives an overview of Industrial Security. It describes the threats and risks to which industrial automation networks are exposed and presents concepts for minimizing these risks and achieving adequate protection from an economic standpoint. In addition, it also gives an insight into what direction the situation will take as it develops based on current trends and what security mechanisms will also be able to be used in industrial environments in the future.

[Download PDF](#)

White papers

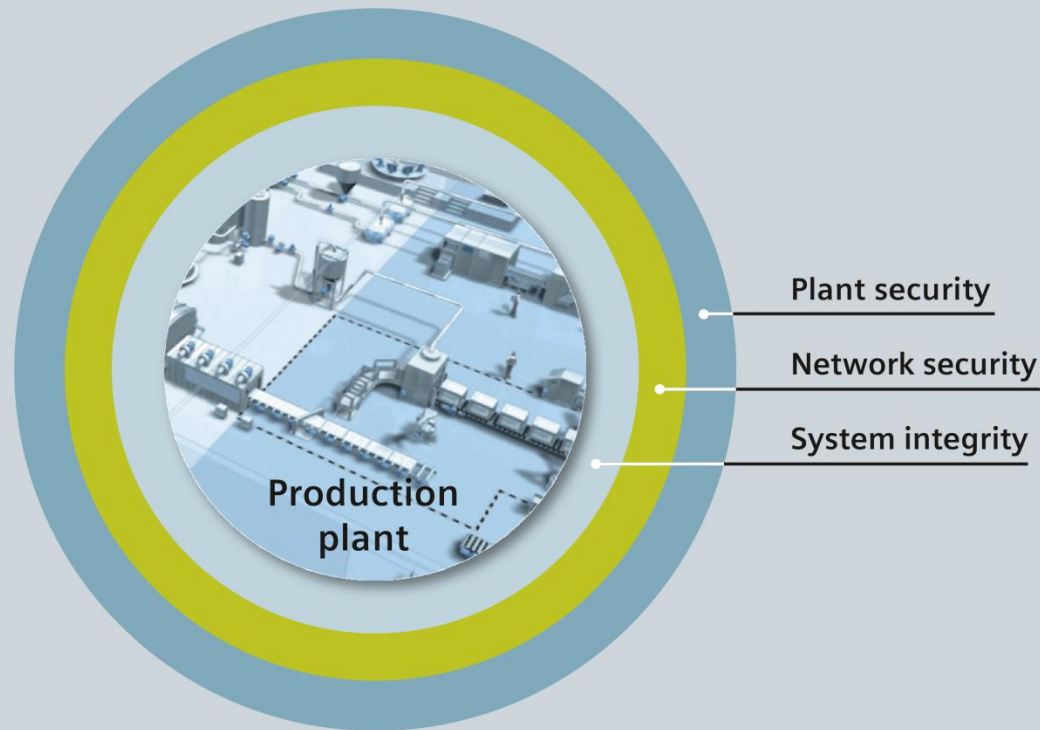
- [Operational Guidelines](#)
- [ARC white paper cyber security](#)
- [Security for S7-controller](#)
- [Security white paper PC-based](#)
- [ARC whitepaper on Industrial Security in PCS 7](#)
- [SIMATIC PCS 7 / WinCC Security concept - White paper](#)
- [Security concept COMOS \(German only\)](#)

Technical articles

- [Interview with Thomas Brandstetter, Siemens CERT](#)
- [Interview with CEO Eckard Eberle \(german\)](#)
- [Why does automation need IT - Read this series of articles](#)
- [Stepped system for security \(german\)](#)
- [How secure are industrial plants? \(german\)](#)
- [Security concept for industrial plants \(german\)](#)
- [Security in data traffic \(Advance 01/2012\)](#)
- [Securing systems, raising awareness \(Process News 01/2012\)](#)

Security concept PCS 7 & WinCC

- [Basic Function Manual](#)



Sécurité Site

- Contrôle d'accès pour éviter les intrusions
- Protection physique des zones sensibles

Sécurité réseau

- Séparation des réseaux bureautique et des réseaux de production
- Segmentation des réseaux de production

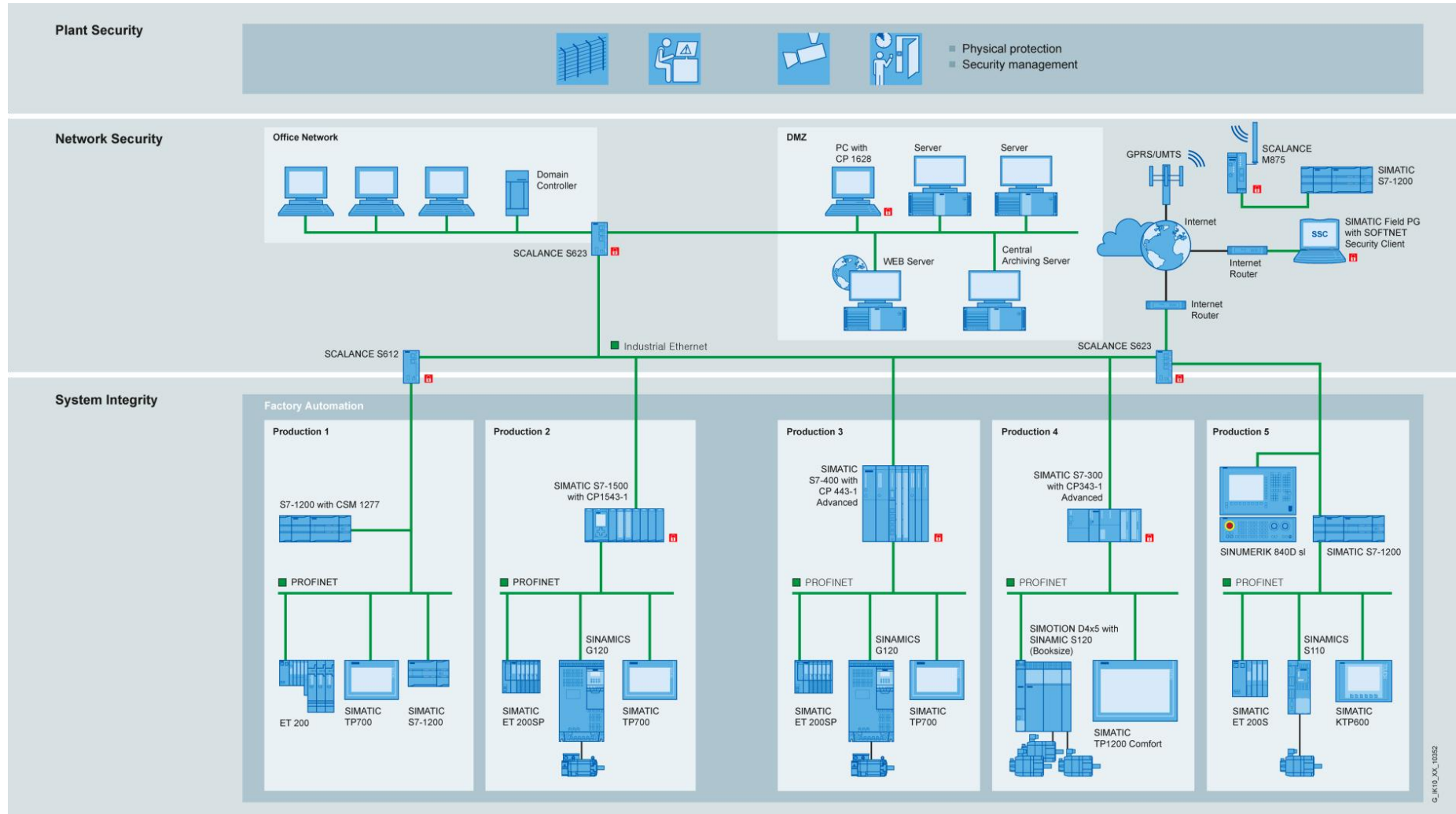
Intégrité du système

- Antivirus et logiciel de whitelisting
- Maintenance et mise à jour logiciel
- Authentification des utilisateurs
- Mécanismes de protection d'accès intégrés aux équipements lorsque que cela est possible

Dans un contexte industriel les solutions de sécurité doivent prendre en compte tous les niveaux de protection.

Cybersécurité des systèmes Industriels

Architecture type



Besoin Client

Protection réseau et segmentation

Protection contre:

- Espionnage
- Manipulation Données
- Accès indésirable
- Mise en place **d'accès distant sûr**:
- Télémaintenance

Notre solution

SCALANCE S Modules de sécurité:

- Stateful Inspection Firewall
- VPN (chiffrement des données)
- NAT/NAPT (translation d'adresse)
- Fonction router (PPPoE, DDNS)
- S623 port additionnel (DMZ)
- Redondance de firewall



SCALANCE S
602/612/623

Besoin Client

Protection réseau et segmentation

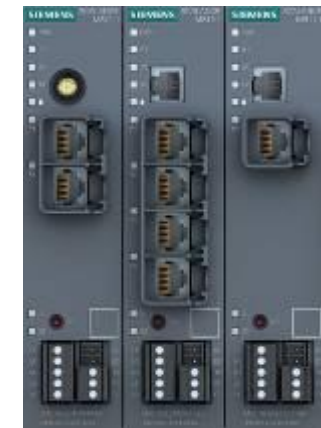
Protection contre:

- Espionnage
- Manipulation Données
- Accès indésirable
- Mise en place **d'accès distant sûr**:
- Télémaintenance

Notre solution

SCALANCE M:

- Stateful Inspection Firewall
- VPN (chiffrement des données)
- NAT/NAPT (translation d'adresse)
- Router pour accès mobile (GPRS, UMTS et même LTE)
- Routeur d'accès ADSL
- Routeur d'accès SHDSL



SCALANCE M

Besoin Client

Protection et segmentation réseau sans ajout de composant supplémentaire

Protection contre:

- Espionnage
- Manipulation Données
- Accès indésirable

Notre solution

CP 343-1/ CP 443-1 Advanced

- Stateful Inspection Firewall
- VPN (chiffrement des données)
- NAT/NAPT (translation d'adresse)
- HTTPs (pages HTML chiffrées SSL)
- FTPs (Transfert de fichiers sécurisé)
- NTP(secure) (Transfert sécurisé de la date et l'heure avec authentification)
- SNMP V3



CP 343-1 Advanced
CP 443-1 Advanced

Besoin Client

Protection et segmentation réseau sans ajout de composant supplémentaire

Protection contre:

- Espionnage
- Manipulation Données
- Accès indésirable

Notre solution

CP 1543-1

- Stateful Inspection Firewall
- VPN (chiffrement des données)
- NAT/NAPT (translation d'adresse)
- HTTPs (pages HTML chiffrées SSL)
- FTPs (Transfert de fichiers sécurisé)
- NTP(secure) (Transfert sécurisé de la date et l'heure avec authentification)
- SNMP V3



CP 1543-1

* as of V12 SP1

Besoin Client

Protection des stations de développement et des postes opérateurs

Protection contre:

- Espionnage
- Manipulation Données
- Accès indésirable

Notre solution

CP 1628

- Stateful Inspection Firewall
- VPN (chiffrement des données)
- NTP(secure) (Transfert sécurisé de la date et l'heure avec authentification)
- SNMP V3



CP 1628

Besoin Client

Accès sécurisé pour stations de développement et les PC de télémaintenance

Protection contre:

- Espionnage
- Manipulation Données
- Accès indésirable

Notre solution

SOFTNET Security Client

- VPN (chiffrement des données)



SOFTNET
Security Client



STOP

incoming 6:40:35 PM
1/6/2012

Temporary CPU error: Copy protection for FC 1 violated (MemoryCard binding)

Compilation error detected; correct and reload program block: ..

HW_ID= 00052

ESC



Security Integrated



- + Protection de la propriété intellectuelle et des investissements
- + Protection contre la copie des programmes applicatifs
- + Protection avancée contre les modifications de projet non autorisées
- + Protection contre les manipulations non autorisées

Besoin Client

Détection et prévention des Virus, Worms et chevaux de Troyes

Protection contre:

- Code malicieux
- Manipulation de code

Notre solution

Antivirus et whitelisting

- Nos solutions sont testées avec de grands éditeurs de logiciel d'Antivirus



Nouveaux produits

Fonctions de sécurité intégrées



	SCALANCE S family	SCALANCE M875	CP 343-1 Adv/ CP 443-1 Adv	S7-1200 CPU ²⁾ S7-1500 CPU	CP1543-1	CP 1628	SOFTNET Security Client
Configurable copy protection							
Access protection (authentication)				•			
Extended access protection (Firewall)	•	•	•		•	•	
Virtual Private Network with IPsec	•	•	•		• ¹⁾	•	•
Manipulation protection (communication, configuration)	•	•	•	•	•	•	•

• applies

1) VPN (V12 SP1 or higher)

2) Firmware V4.0 (V12 SP1 or higher)

G_IK10_XX_10347

Cybersécurité des systèmes Industriels

Premier équipementier avec la certification Achilles Niveau 2 depuis 2012

SIEMENS



API certifiés Achilles Niveau 2

S7-1500 PN/DP
S7- 300 PN/DP
S7- 400 PN/DP
ET 200S CPU

CP certifiés Achilles Niveau 2

CP 343-1 Advanced
CP 443-1 Advanced
CP 1628
CP 1543-1

- + Protection contre DoS
- + Comportement prédéfini en cas d'attaque
- **Disponibilité accrue**
- **Protection IP**
- **Standard International**

Merci de votre attention!

SIEMENS

Jean-Christophe MATHIEU

Product and Solution Security Officer

Secteur Industry



© Siemens SAS 2013. All Rights Reserved.