SIEMENS

Industrial Security

Helping to increase your resistance to attack

Industrial Security

SIEMENS

- **Introduction**
- The Siemens Solution
- Application Examples
- Benefits of Working with Siemens

Security Trends

Globally we are seeing more network connections than ever before

Trends Impacting Security

- Cloud Computing approaches
- Increased use of Mobile Devices
- Wireless Technology
- Reduced Personnel Requirements
- Smart Grid
- The worldwide and remote access to remote plants, remote machines and mobile applications
- The “Internet of Things”

The physical world is becoming an information system.

Industrial Security

Vulnerability disclosures are headline news

SIEMENS

Pressure SCADA Developers on Security

U.S. at Risk of Hack Attack

Dangerous Security Holes in U.S.
Power Plant & Factory Software

Hacking the Grid

Aging industrial control systems increasingly
vulnerable to cyberattack

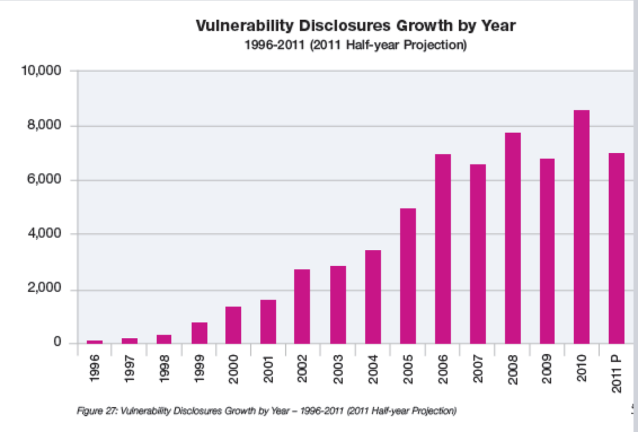
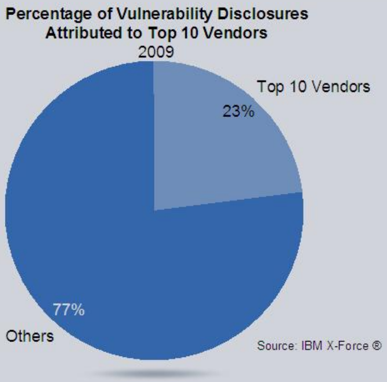


Figure 27: Vulnerability Disclosures Growth by Year – 1996-2011 (2011 Half-year Projection)



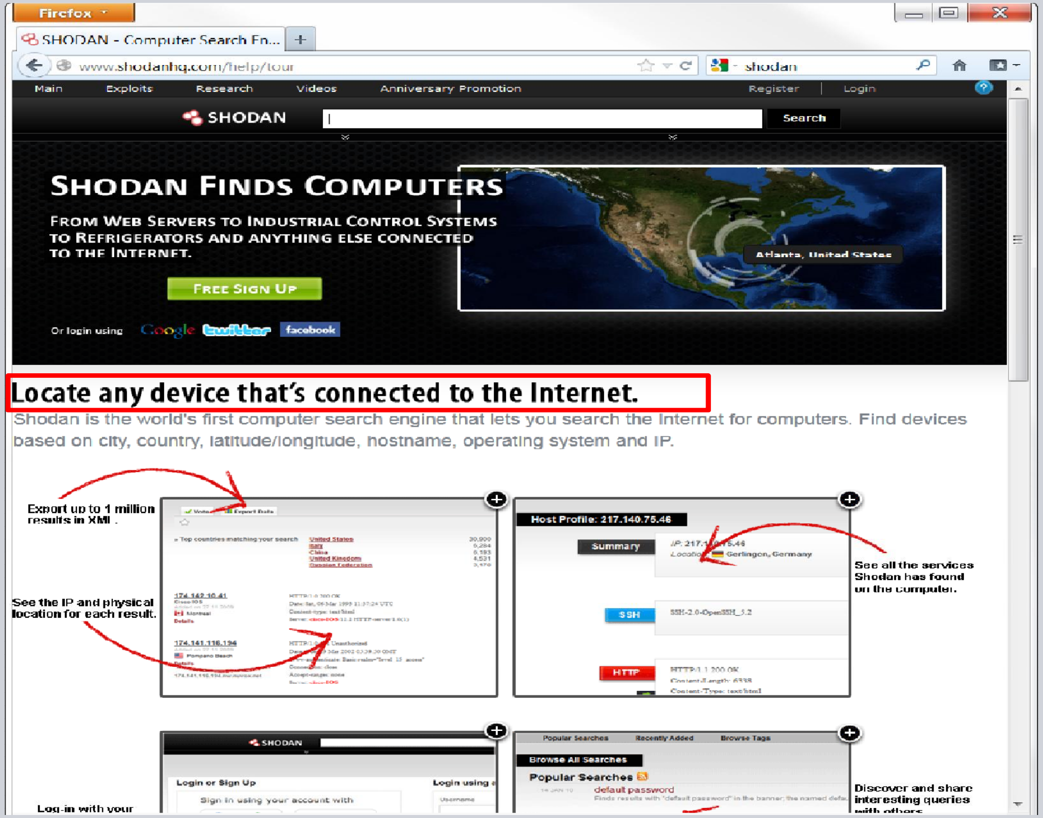
Source: IBM X-Force ®

March 7, 2012: "These are older systems so they are harder to control. And for convenience and cost savings, people have connected them to the internet in order to control them from remote locations. So this is almost a perfect storm in terms of vulnerability because the nation is so dependent on these systems."

- Donald Purdy, chief cybersecurity strategist at CSC
and former cyber official at the Department of Homeland Security.

Search engines are being used to identify and access control systems over the Internet

SIEMENS



SHODAN FINDS COMPUTERS

FROM WEB SERVERS TO INDUSTRIAL CONTROL SYSTEMS TO REFRIGERATORS AND ANYTHING ELSE CONNECTED TO THE INTERNET.

Locate any device that's connected to the Internet.

Shodan is the world's first computer search engine that lets you search the Internet for computers. Find devices based on city, country, latitude/longitude, hostname, operating system and IP.

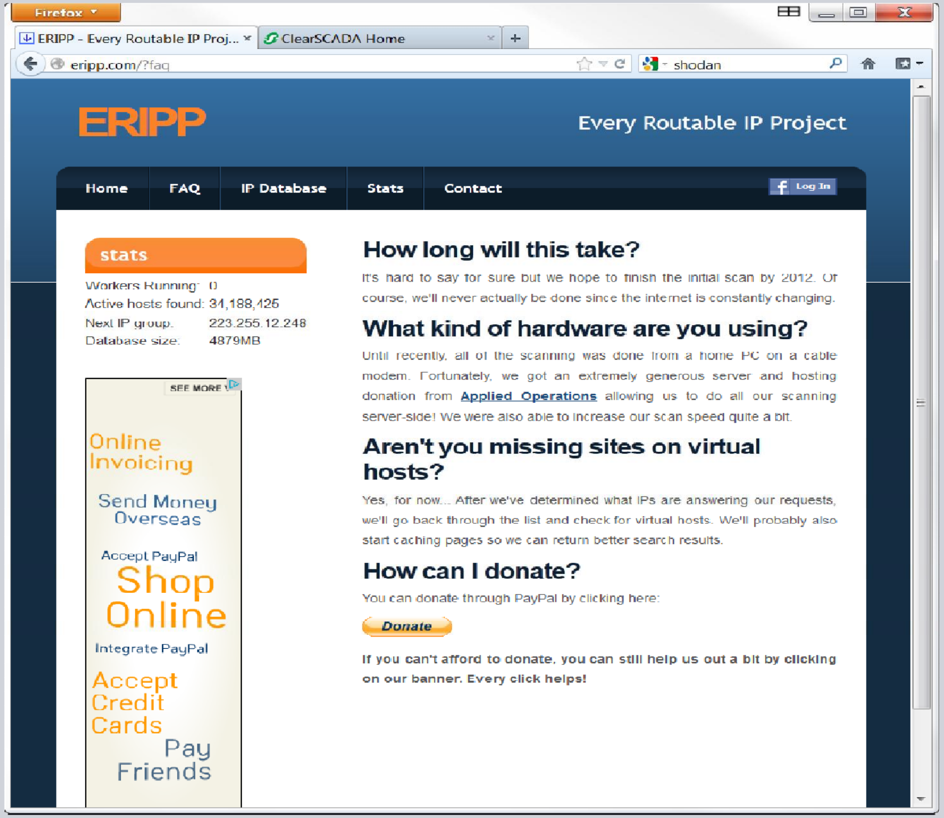
Export up to 1 million results in XML.

See the IP and physical location for each result.

See all the services Shodan has found on the computer.

Log-in with your

Discover and share interesting queries with others



Workers Running:	0
Active hosts found:	34,188,425
Next IP group:	223.255.12.248
Database size:	4879MB

How long will this take?

It's hard to say for sure but we hope to finish the initial scan by 2012. Of course, we'll never actually be done since the internet is constantly changing.

What kind of hardware are you using?

Until recently, all of the scanning was done from a home PC on a cable modem. Fortunately, we got an extremely generous server and hosting donation from Applied Operations allowing us to do all our scanning server-side! We were also able to increase our scan speed quite a bit.

Aren't you missing sites on virtual hosts?

Yes, for now... After we've determined what IPs are answering our requests, we'll go back through the list and check for virtual hosts. We'll probably also start caching pages so we can return better search results.

How can I donate?

You can donate through PayPal by clicking here:

If you can't afford to donate, you can still help us out a bit by clicking on our banner. Every click helps!

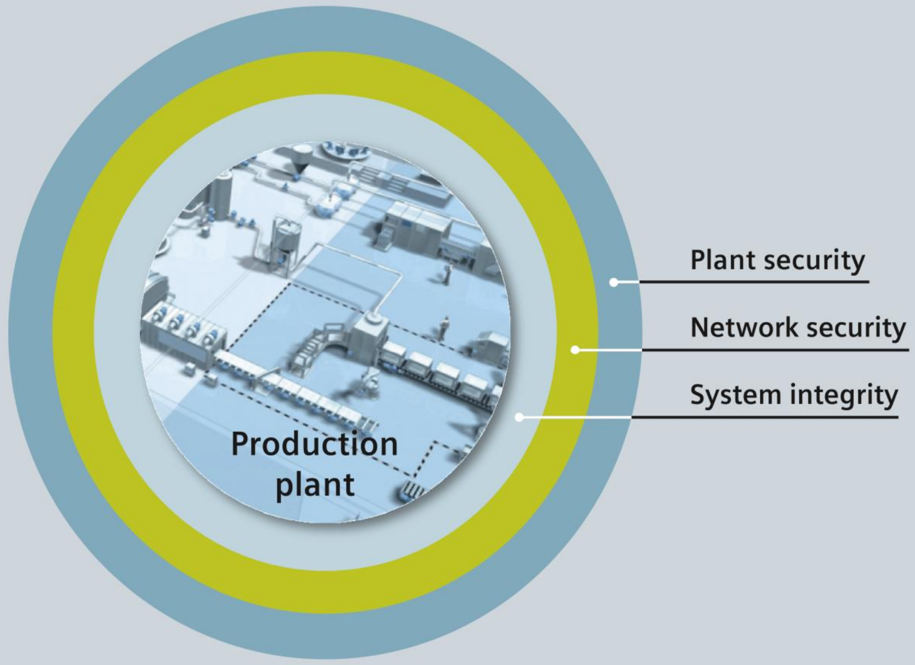
Industrial Security

SIEMENS

- Introduction
- **The Siemens Solution**
- Application Examples
- Benefits of Working with Siemens

Industrial Security

The Defense in Depth Concept



Plant security

- Access blocked for unauthorized persons
- Physical prevention of access to critical components

Network security

- Controlled interfaces between office and plant network e.g. via firewalls
- Further segmentation of plant network

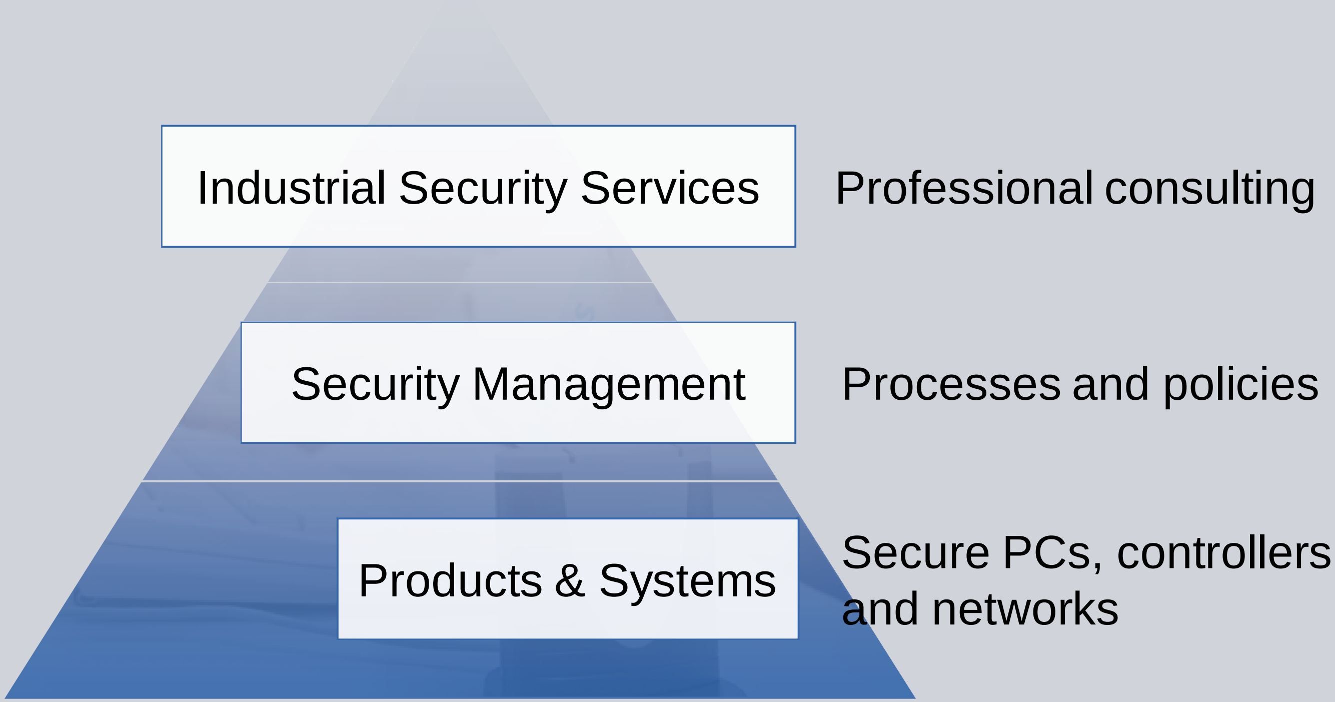
System integrity

- Antivirus and whitelisting software
- Maintenance and update processes
- User authentication for plant or machine operators
- Integrated access protection mechanisms in automation components

Security solutions in an industrial context must take account of all protection levels

Industrial Security

The Siemens Solution


Industrial Security Services

Professional consulting

Security Management

Processes and policies

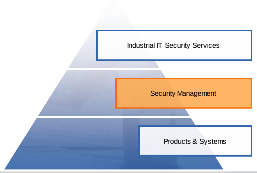
Products & Systems

Secure PCs, controllers and networks

The Siemens solution reduces your risk with a well thought-out security concept.

Industrial Security

The Siemens solution for plant security



SIEMENS

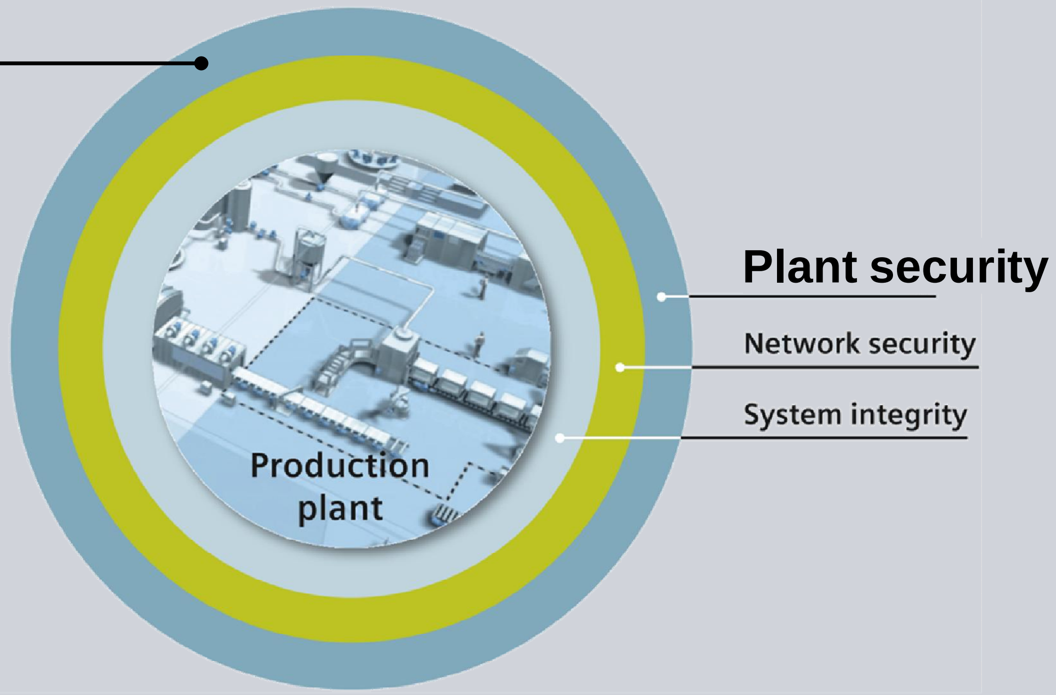
Implementation of **Security Management**

The **interfaces** are subject to regulations - and are monitored accordingly.

PC-based systems must be protected.

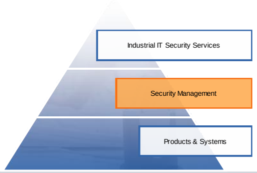
The **control level** must be protected.

Communication must be monitored and can be segmented.



Industrial Security

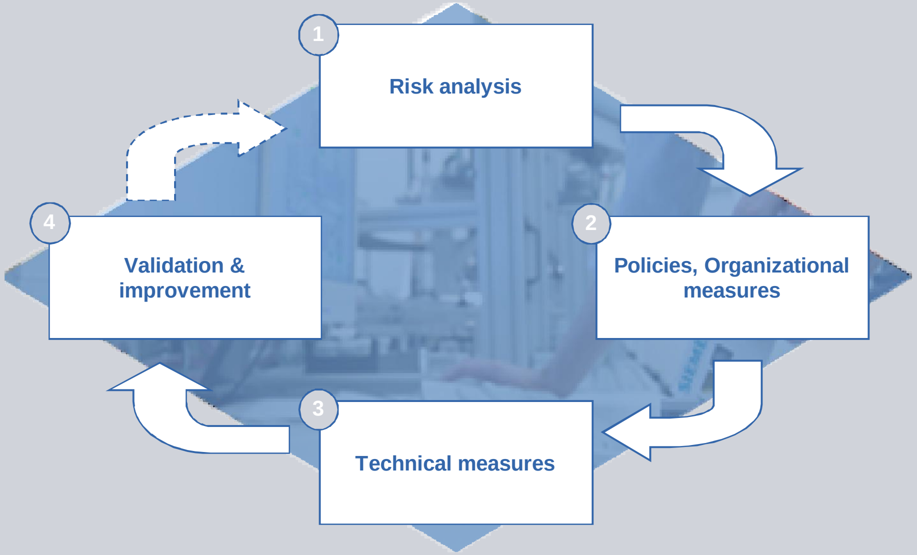
Security Management



SIEMENS

Security Management Process

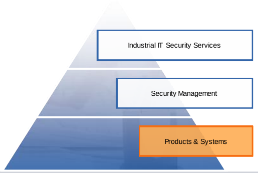
- Risk analysis with definition of mitigation measures
- Setting up of policies and coordination of organizational measures
- Coordination of technical measures
- Regular / event-based repetition of the risk analysis



Security Management is essential for a well thought-out security concept.

Industrial Security

The Siemens Solution for Network Security



SIEMENS

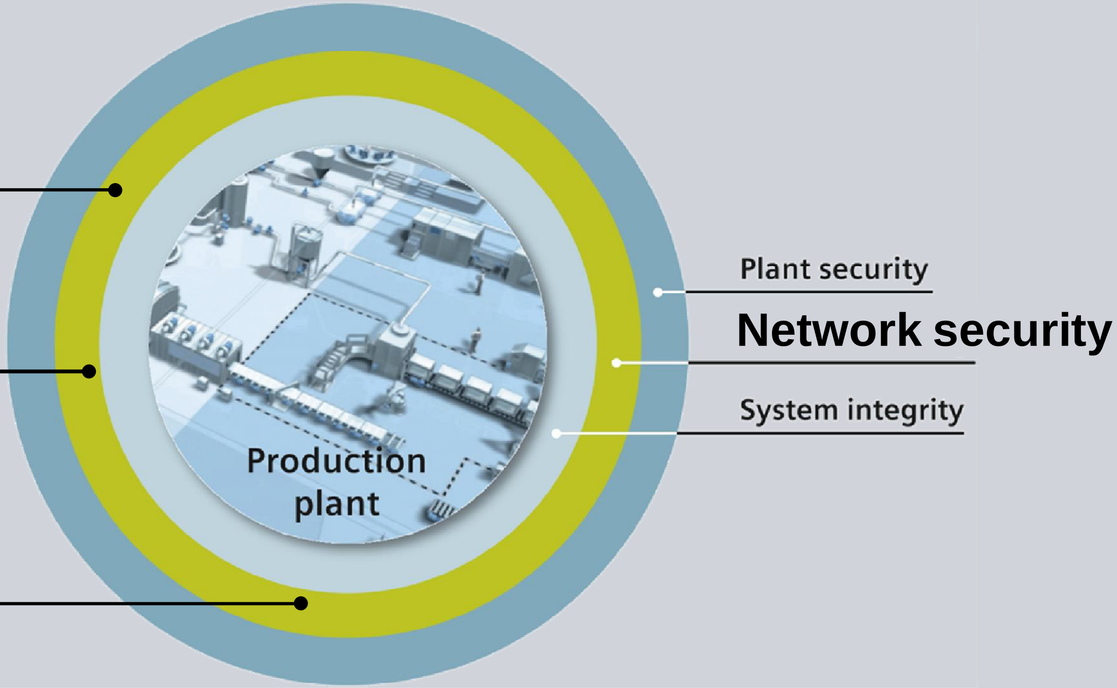
Implementation of **Security Management**

The **interfaces** are subject to regulations - and are monitored accordingly.

PC-based systems must be protected.

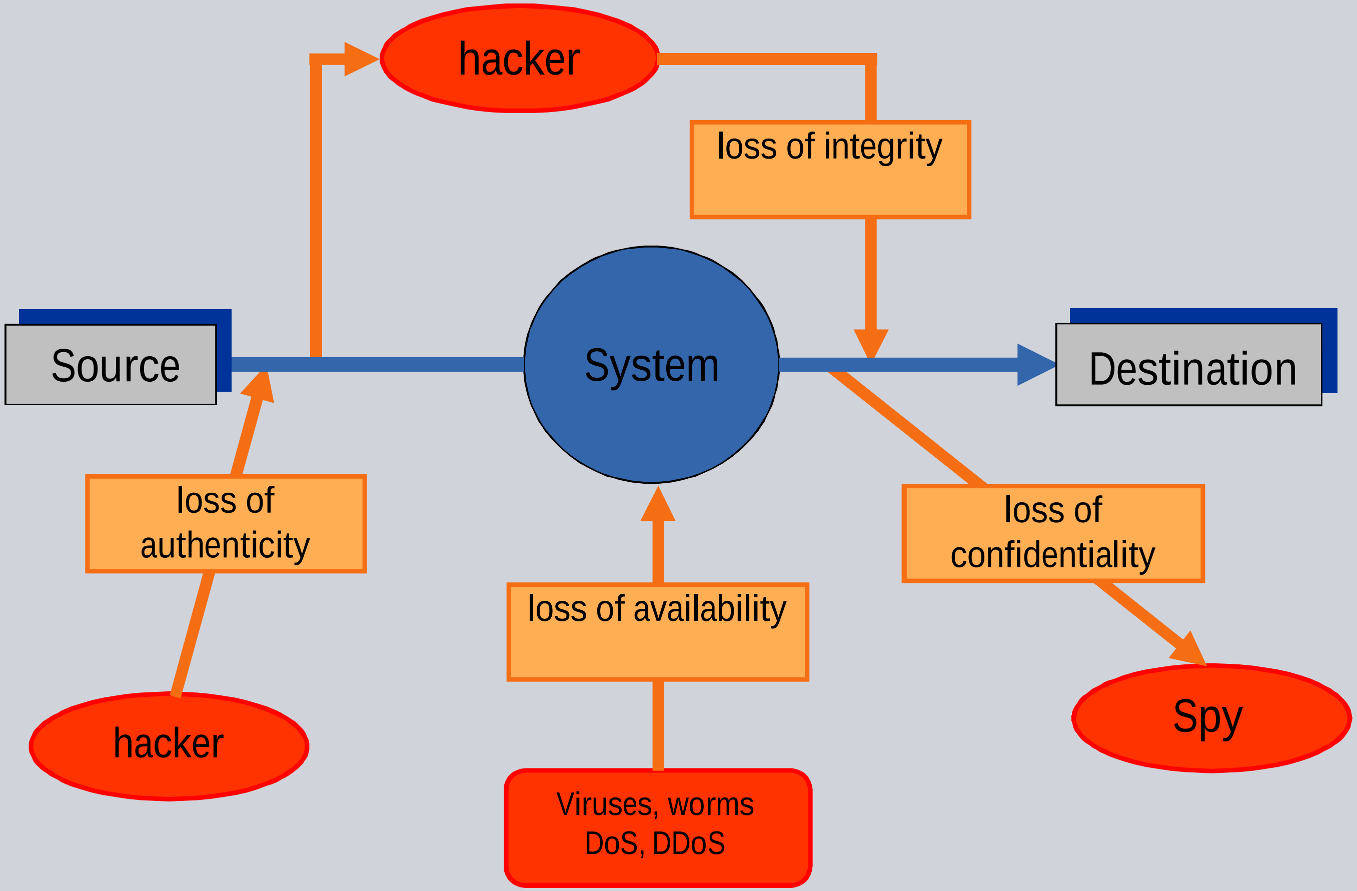
The **control level** must be protected.

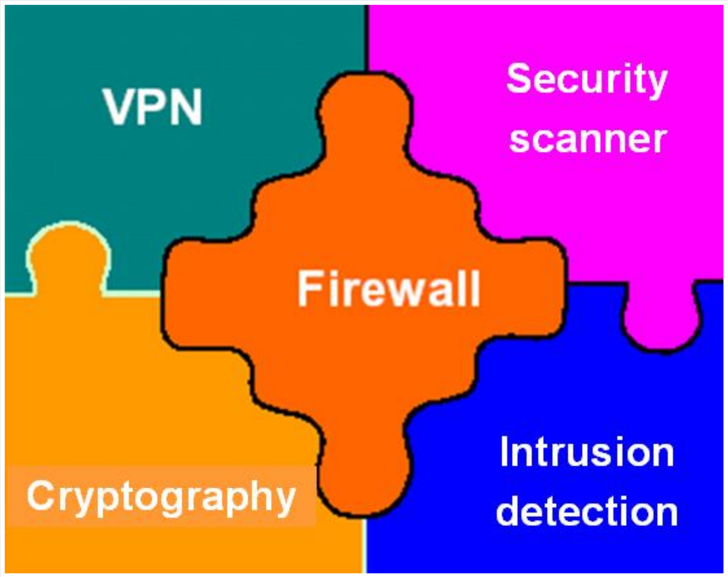
Communication must be monitored and can be segmented.



Industrial Security

Security Integrated – Basic Concepts



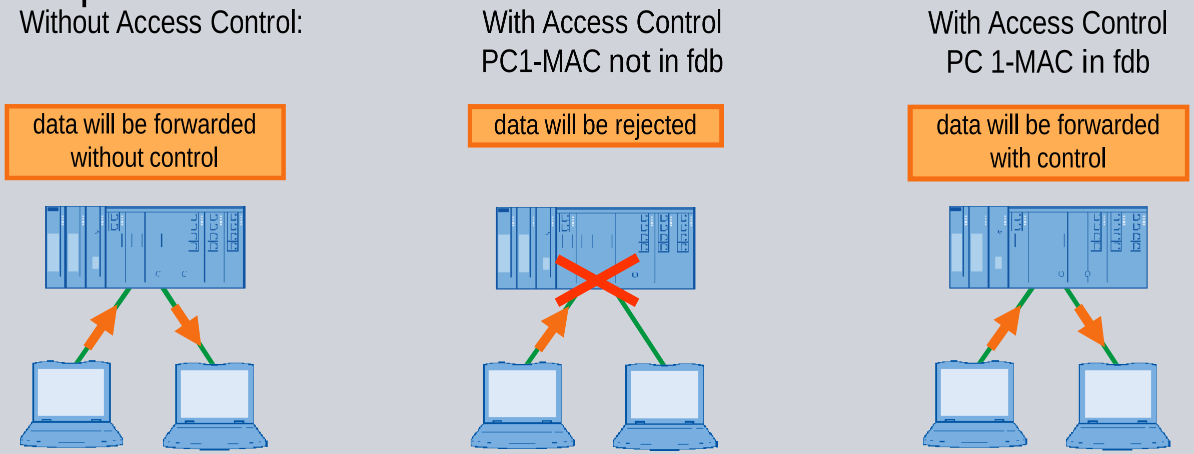


Industrial Security

Security Integrated – Basic Concepts – Access Control List (ACL)

If Access-Control is enabled, a switch will only forward frames whose Source-MAC-Address is registered as **static entry** in the Unicast-MAC Address-Table (fdb).

Examples:



Without Access Control:

data will be forwarded without control

With Access Control PC1-MAC not in fdb

data will be rejected

With Access Control PC 1-MAC in fdb

data will be forwarded with control

Advantages of Access Control Lists:

- Good for small or mid-sized networks
- Good for networks that are never or rarely changed
- Good for networks where end-devices are always connected to the same switch ports

Disadvantage of Access Control Lists:

- Time-consuming configuration
- Source of Error
- Can be fooled by MAC-Spoofing (manipulation)

Solution:

- 802.1X RADIUS

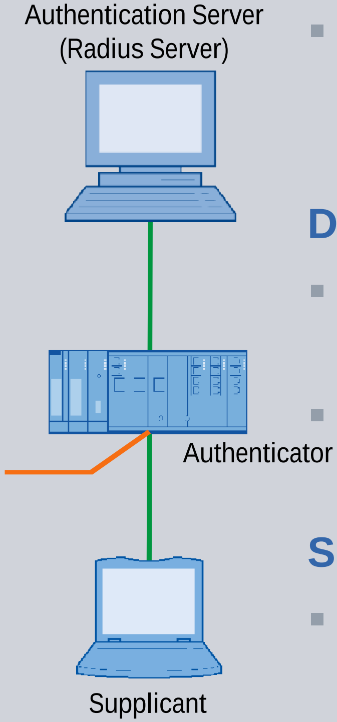
Industrial Security

Security Integrated – Basic Concepts – 802.1X RADIUS

SIEMENS

If the supplicant has been accepted from the Radios Server, it unblocks the port, otherwise the port will remain blocked

→Switch plays the role of a doorman



Port in forwarding, if identification was successfully, only !!!

Advantages of Radius Authentication:

- Good for big enterprise networks
- Good for automation networks that are connected to enterprise networks

Disadvantage of Radius Authentication :

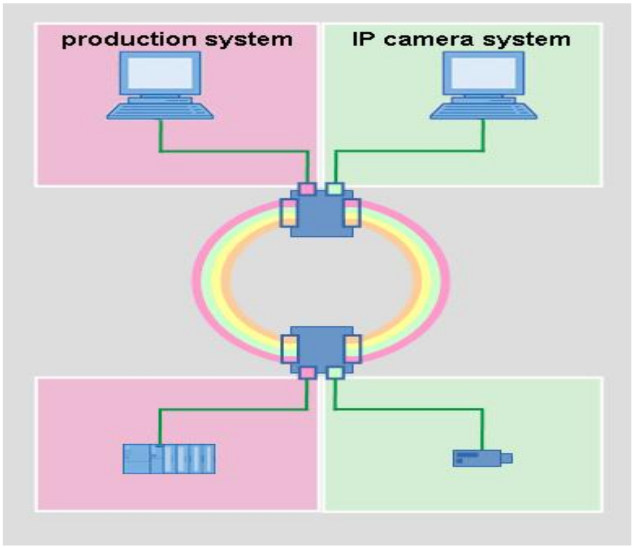
- Every authenticated supplicant has full access to the entire network
- End devices must support EAP protocol

Solution:

- VLANs

Industrial Security

Security Integrated – Basic Concepts – 802.1Q VLAN



802.3 Ethernet Frame (max. 1526 Bytes)							
Pre-ambel 7 Byte	Sync 1 Byte	Source address 6 Byte	Dest. address 6 Byte	VLAN & Prio. 4 Byte	Ether-type 2 Byte	Process data up to 1440 Bytes	FCS 4 Byte
Ethernet-Header						Data	

Advantages of VLANs:

- Multiples splitted LANs over the same cable
- Flexible network structures
- Limited broadcast domain
- Limited network access

Disadvantage of VLANs:

- No definition of specific communication filters

Solution:

- Firewalls

Industrial Security

Security Integrated – Basic Concepts – Firewall

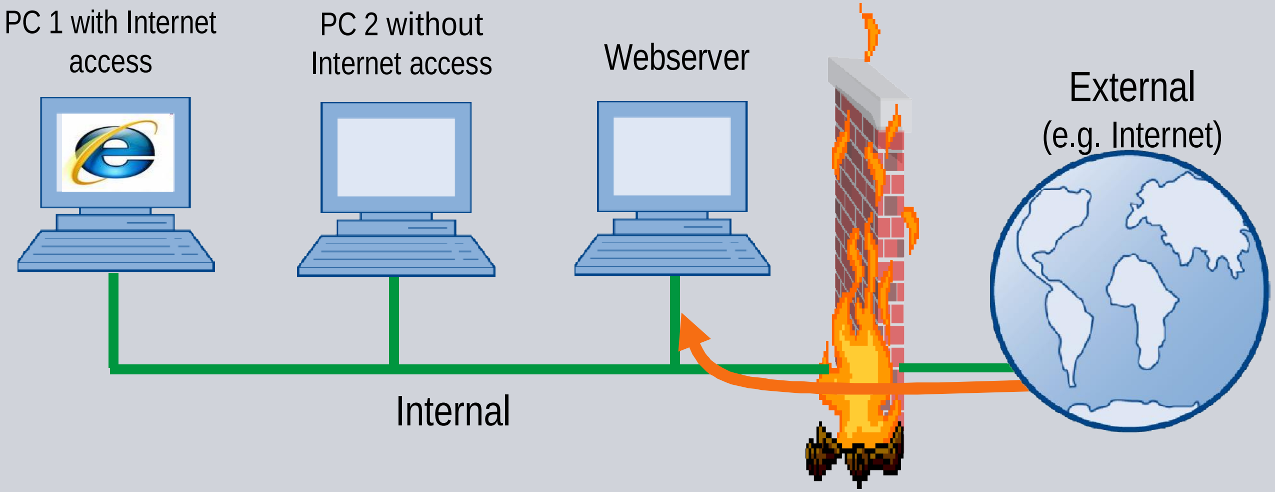
SIEMENS

Firewall between the Internet and an office network:

PC1: **Internal->External:** Allow TCP/IP communication on Port 80 and 443

PC2: **Internal->External:** Drop all communication

Webserver: **External->Internal:** Allow TCP/IP Port 80



Advantages of Firewalls:

- Make possible specific communication filters
- Provide intrusion detect mechanism
- Can work on all OSI/ISO layers

Disadvantage of Firewalls :

- Need to be statefull
- Don’t provide any mechanism against lost of authenticity, integrity or confidentially

Solution:

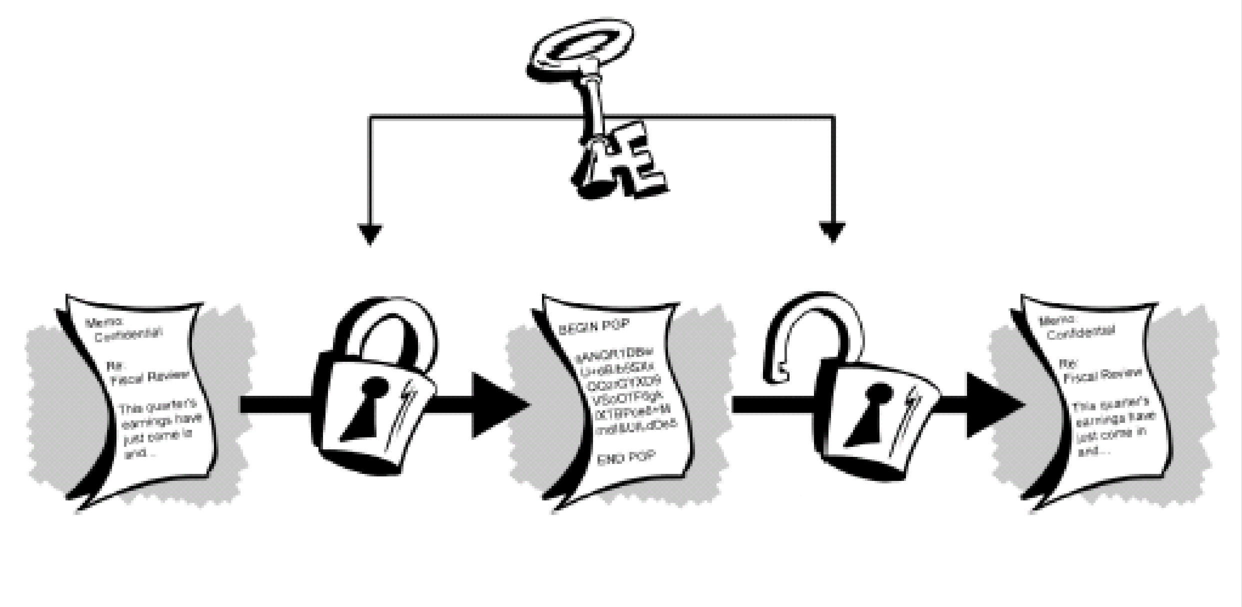
- Cryptography

Industrial Security

Security Integrated – Basic Concepts – Cryptography

Symmetrical encryption

..**one key** for encryption and decryption



Plain text — Encryption (key) — Cipher text — Decryption (key) — Plain text

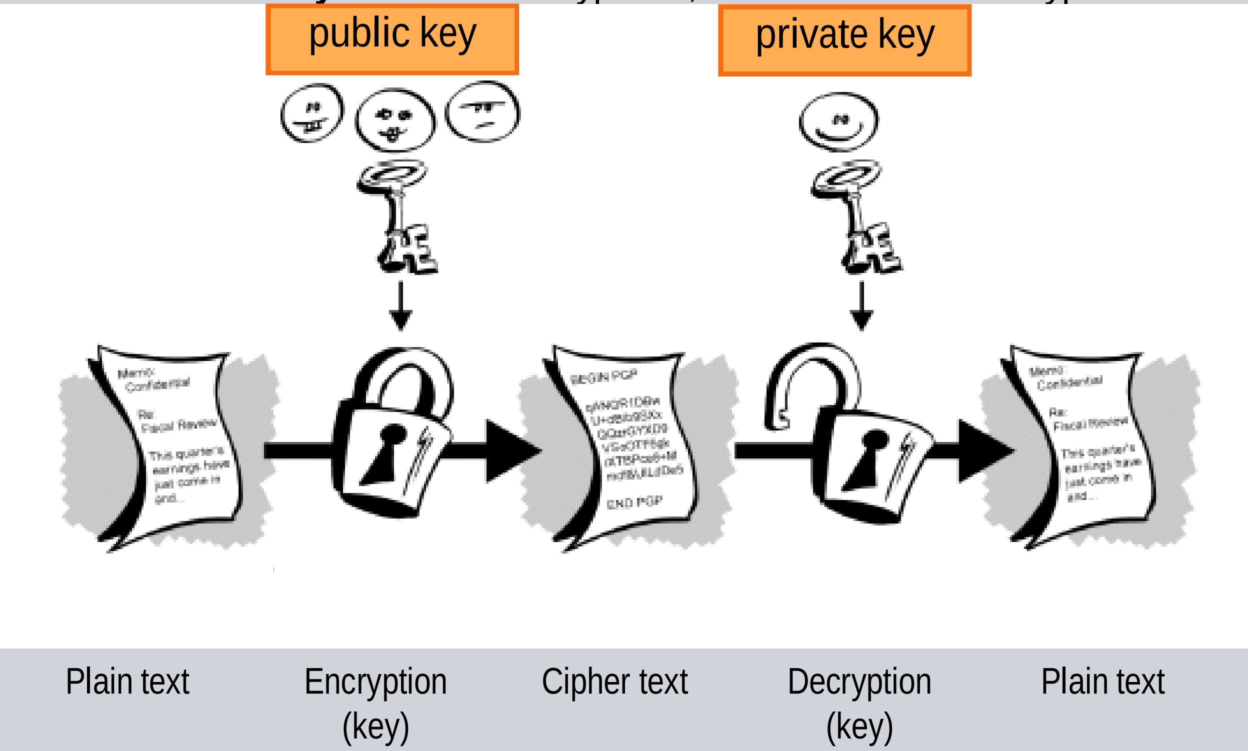
Name	Key length [bit]	Security	Protected by patent
DES	56	Broken	No
Triple-DES	112 or 168	Secure	No
IDEA	128	Secure	Ascom Systec
RC4	Variable (56-2048)	Secure with large keys	RSA Data Security Inc.
Blowfish	Variable (32-448)	Secure with large keys	No
AES	128/192/256	Secure	No
CAST-5	Variable (80-128)	Secure with large keys	Yes

Industrial Security
Security Integrated – Basic Concepts – Cryptography

SIEMENS

Asymmetrical encryption

..**two different keys**: one for encryption ; another one for decryption



Plain text

Encryption (key)

Cipher text

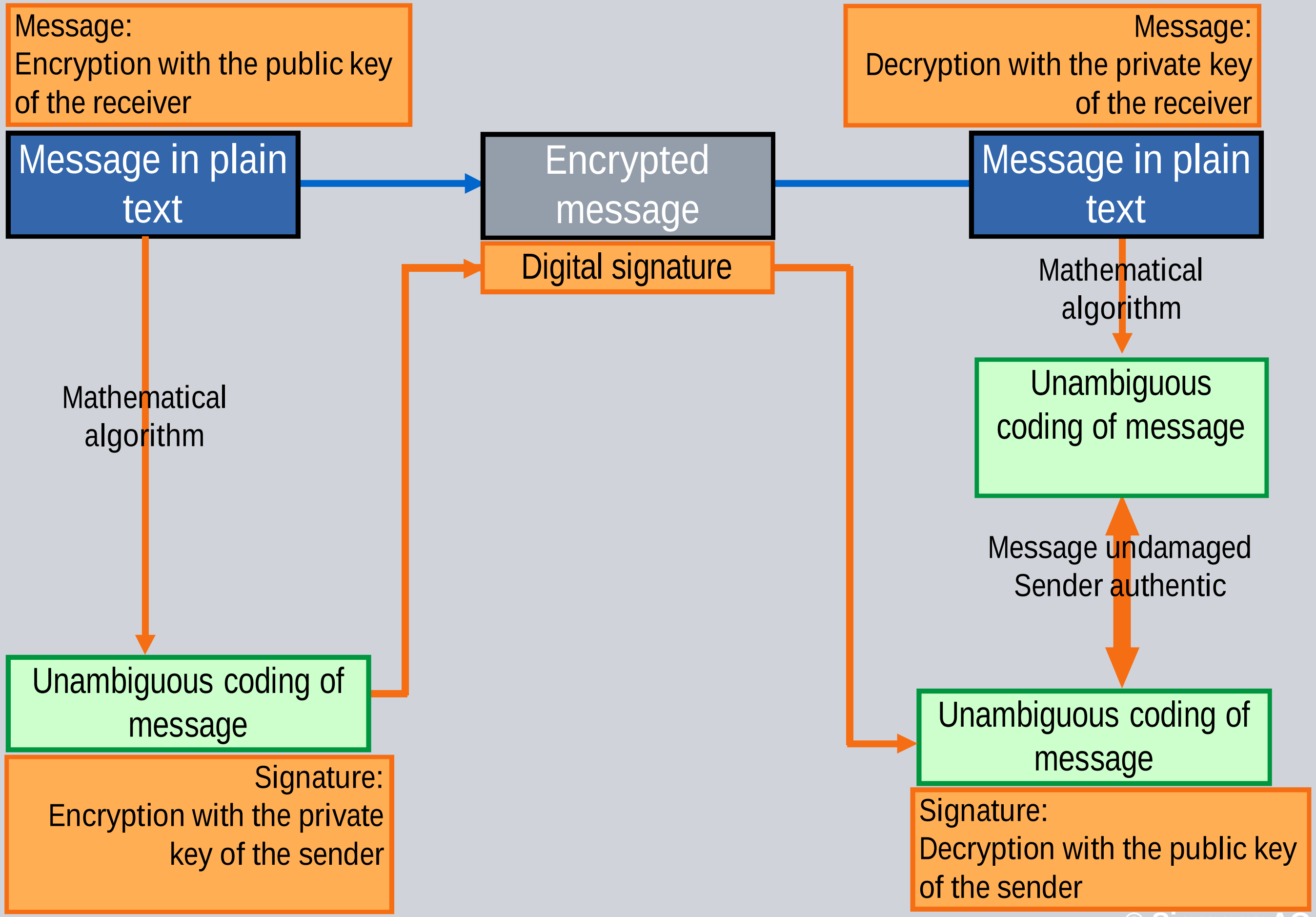
Decryption (key)

Plain text

Name	Key length [bit]	Security	Protected by patent
RSA	Variable (512-2048)	Secure with large keys	In USA: RSA DSI
ElGamal/DSA	1024	Secure	No
DH (Diffie-Hellmann)/ DSS	Key replacement	Secure	No

Industrial Security

Security Integrated – Basic Concepts – Cryptography



Message:
Encryption with the public key of the receiver

Message in plain text

Encrypted message

Digital signature

Message:
Decryption with the private key of the receiver

Message in plain text

Mathematical algorithm

Unambiguous coding of message

Mathematical algorithm

Unambiguous coding of message

Message undamaged
Sender authentic

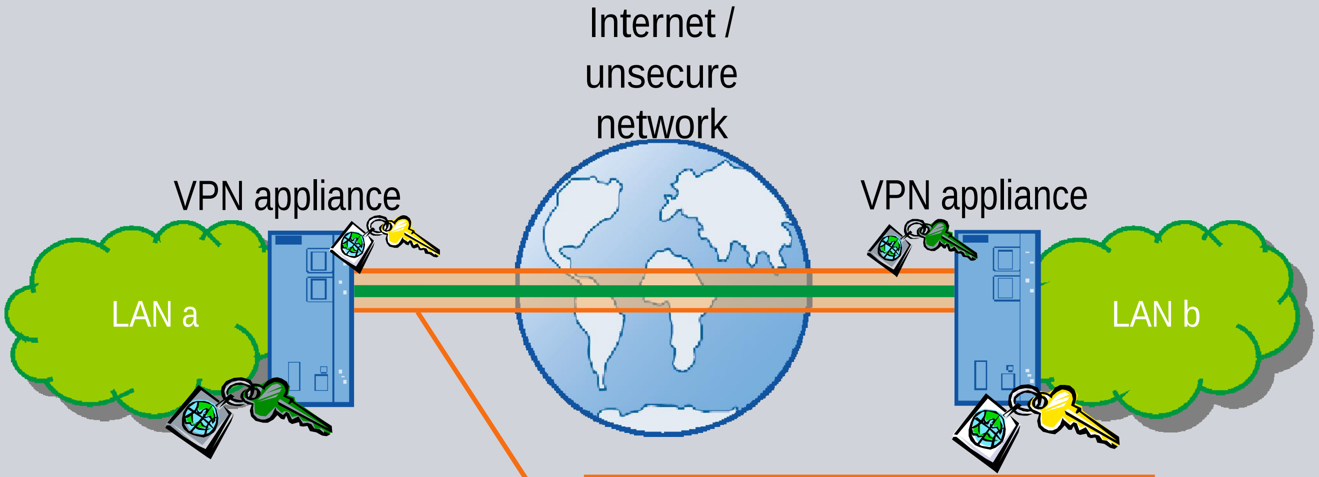
Unambiguous coding of message

Signature:
Encryption with the private key of the sender

Signature:
Decryption with the public key of the sender

Industrial Security

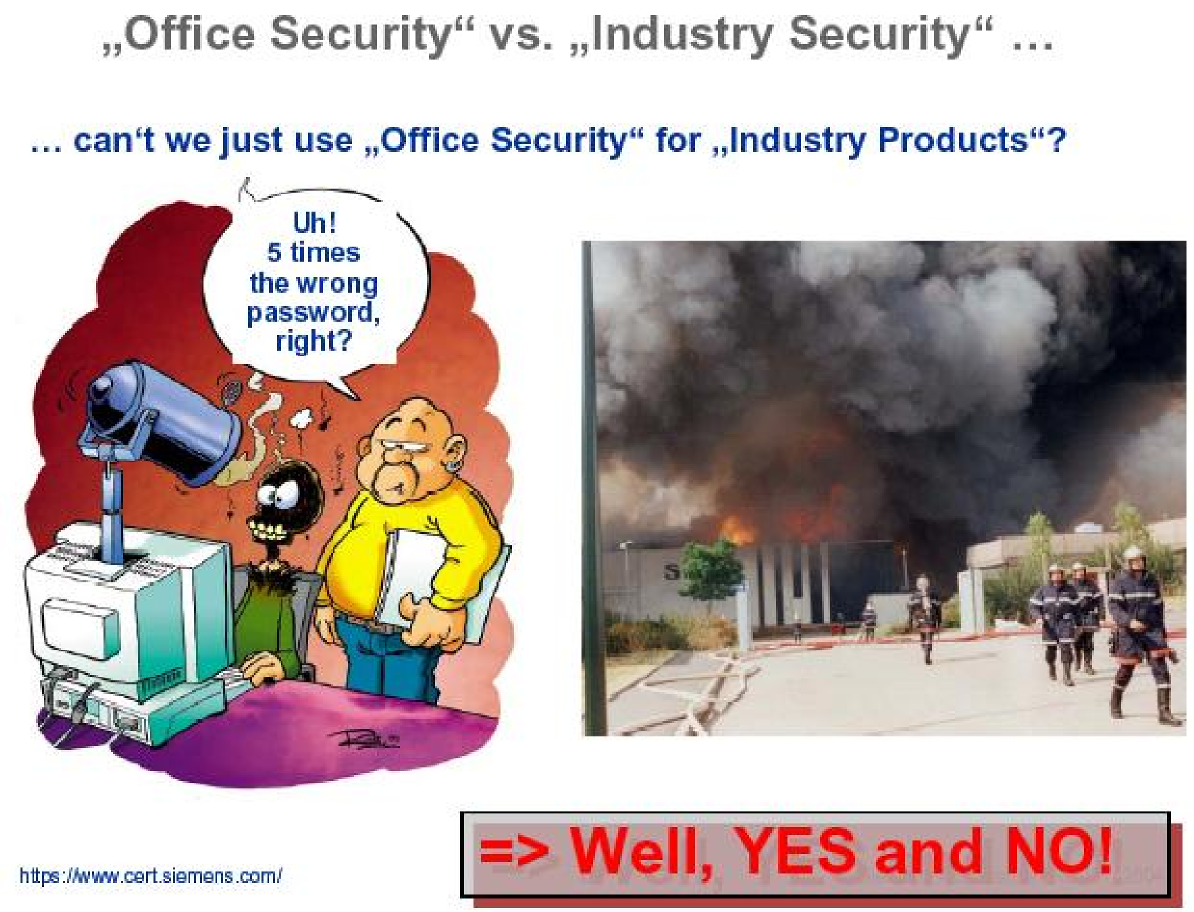
Security Integrated – Basic Concepts – VPN



VPN-tunnel
..provides secure connection between two LAN networks.

Industrial Security

IT Security versus Industrial Security



„Office Security“ vs. „Industry Security“ …

… can‘t we just use „Office Security“ for „Industry Products“?

Uh!
5 times
the wrong
password,
right?

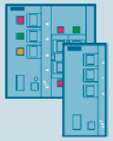
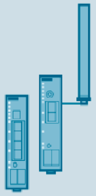
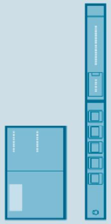
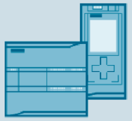
https://www.cert.siemens.com/

=> Well, YES and NO!

Industrial Security

Security Integrated – Overview

SIEMENS

	SCALANCE S family	SCALANCE M family	CP 343-1 Adv CP 443-1 Adv	S7-1200 CPU [1] S7-1500 CPU	CP 1243-1 [1] CP 1543-1	CP 1628	SOFTNET Security Client
							
Configurable copy protection				●			
Access protection (authentication)				●			
Extended access protection (Firewall)	●	●	●		●	●	
Virtual Private Network with IPSec	●	●	●		●	●	●
Manipulation protection (communication, configuration)	●	●	●	●	●	●	●

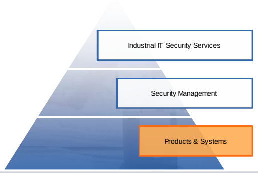
● applies

[1] from CPU firmware V4.0
from STEP 7 Professional V13 (TIA Portal)

G_IK10_XX_10347

Industrial Security

Security Integrated: SCALANCE S Security Modules



SIEMENS

Customer requirement

Network protection and segmentation

Protection against:

- Espionage
- Data manipulation
- Accidental access

Enabling of **secure remote access** for:

- Telecontrol
- Teleservice

Our solution

SCALANCE S Security Modules provide several security functions:

- Firewall
- VPN (data encryption)
- NAT (address translation)
- Router functionality (PPPoE, DynDNS) for broadband Internetaccess (DSL, cable)
- S623 with an additional VPN port (DMZ), allowing the possibility of securely connecting an additional network for service or remote maintenance purposes.

SCALANCE S 602/612/623

Industrial Security

Security Integrated: SCALANCE M875

Customer requirement

Network protection

Protection against:

- Espionage
- Data manipulation
- Accidental access

Enabling of **secure remote access** for:

- Telecontrol
- Teleservice

Our solution

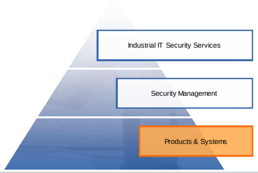
UMTS Router SCALANCE M875 with **Security Integrated** provides several security functions:

- Firewall
- VPN (data encryption)
- NAT (address translation)
- Router functionality for mobile broadband Internet access (GPRS, UMTS)

SCALANCE M875

Industrial Security

Security Integrated: CP1543-1



Customer requirement

Network protection and separation without separate security appliance

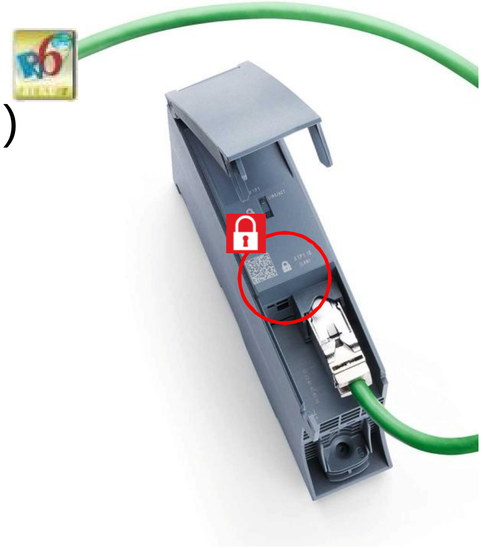
Protection against:

- Espionage
- Data manipulation
- Accidental access

Our solution

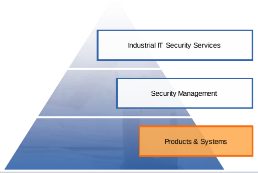
CP 1543-1 with **Security Integrated** provides several security functions:

- Firewall
- VPN (data encryption and authentication)
- IPv6 support
- Network separation
- Web server access via http / https
- FTP / FTPS (Client/Server), E-Mail
- S7-Communication and open TCP-Communication



Industrial Security

Security Integrated: CP 1628



SIEMENS

Customer requirement

Protection of engineering and operator station PCs

Protection against:

- Espionage
- Data manipulation
- Accidental access

Our solution

CP 1628 with **Security Integrated** provides several security functions:

Firewall (Stateful Inspection Firewall (Layer 3/4)

- Filter function for Layer 2 packages ; Global firewall rules (for several devices simultaneously)

VPN

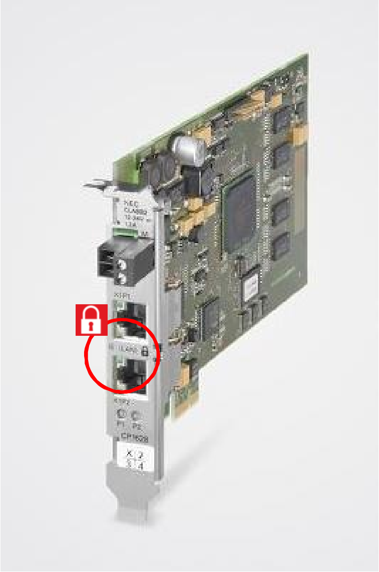
- Tap-proof access to control points ; VPN Server / VPN Client; Up to 64 VPN tunnels simultaneously

NTP V3

- Secure transfer with time of day and authentication

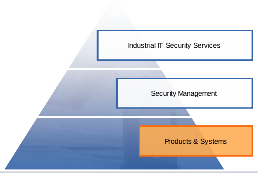
SNMP V3

- Tap-proof transfer of network analysis information



Industrial Security

The Siemens solution for access control



SIEMENS

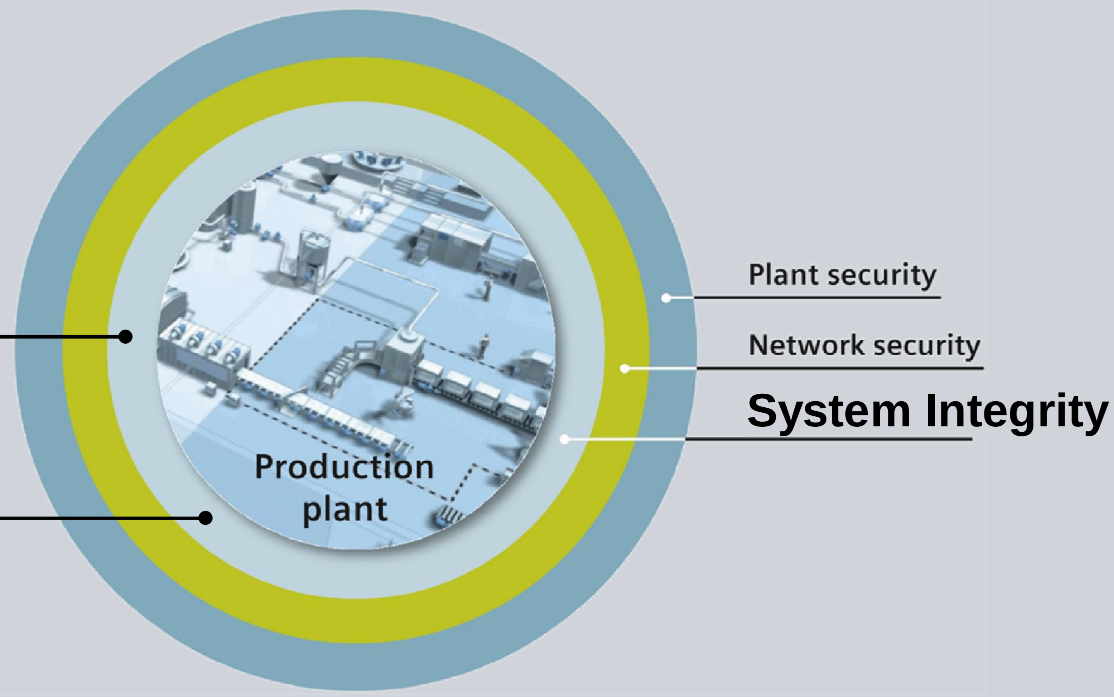
Implementation of **Security Management**

The **interfaces** are subject to regulations - and are monitored accordingly.

PC-based systems must be protected.

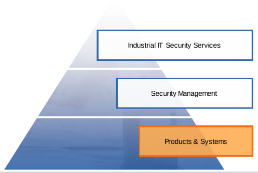
The **control level** must be protected.

Communication must be monitored and can be segmented.



Industrial Security

SIMATIC S7-1500, S7-1200, S7-300, S7-400 and the TIA Portal

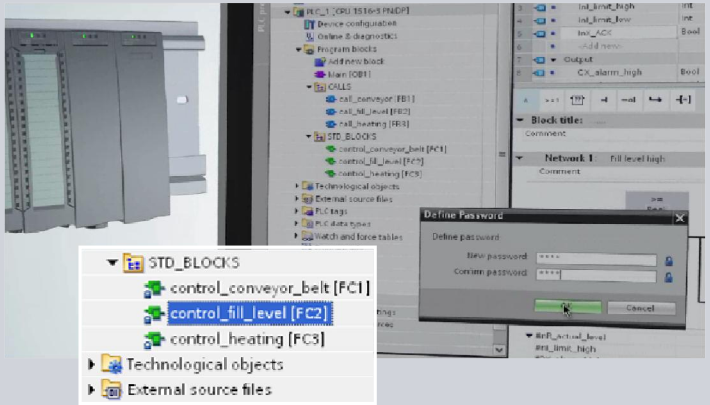


SIEMENS

Security Highlights

The **SIMATIC S7-1500 and the TIA Portal** provide several security features:

- **Increased Know-How Protection in STEP 7**
  Protection of intellectual property and effective investment:
  - Password protection against unauthorized opening of program blocks in STEP 7 and thus protection against unauthorized copying of e.g. developed algorithms
  - Password protection against unauthorized evaluation of the program blocks with external programs
- **Increased Copy Protection**
  Protection against unauthorized reproduction of executable programs:
  - Binding of single blocks to the serial number of the memory card or PLC
  - Protection against unauthorized copying of program blocks



Define password

New password ****

Confirm password ****

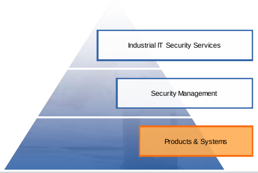
6:40:35 PM 1/6/2012

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

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

HW_ID= 00052

Industrial Security
SIMATIC S7-1500, S7-1200 and the TIA Portal



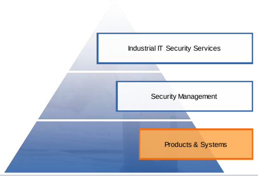
SIEMENS

Security Highlights

The **SIMATIC S7-1500 and the TIA Portal** provide several security features:

- **Increased Access Protection (Authentication)**
  Extensive protection against unauthorized project changes:
  - Configurable levels of authorization (1-3 with own password)
- **Expanded Access Protection**
  - Extensive protection against unauthorized project changes:
- **Increased Protection against Manipulation**
  Protection of communication against unauthorized manipulation for high plant availability:
  - Improved protection against manipulated communication by means of digital checksums when accessing controllers
  - Protection against network attacks such as intrude of faked / recorded network communication (replay attacks)

Industrial Security
WinCC V7


Industrial IT Security Services

Security Management

Products & Systems

SIEMENS

Customer requirement

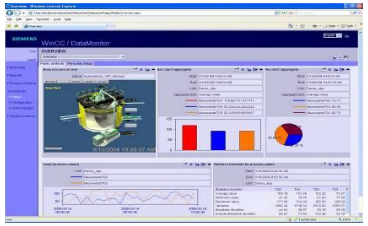
Secured SCADA environment

Protection against:

- Espionage
- Data manipulation
- System failure

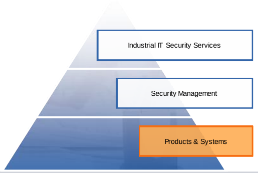
Our solution

WinCC V7 offers a wide range of security supporting features:



- **WinCC User Administrator**
  Only authenticated user get access to the system
  Supports Windows Domain Users
- **WinCC Change Control / Audit**
  Tracking of user actions e. g. for FDA environment solutions
- **WinCC Runtime Redundancy**
  Higher availability of servers / process connection in case of failures
- **Encrypted Messages Between Server and Clients**
  Only authenticated computers get access to the system

Industrial Security
SIMATIC Logon



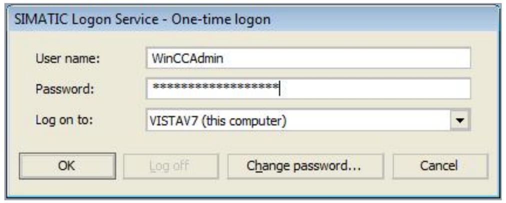
SIEMENS

Customer requirement

- Central, system-wide user management
- Conforms with the requirements of the Food and Drug Administration (FDA)
- Configuration at runtime (add / lock / remove user accounts)
- High Security through being based on MS Windows
- Supports domain concept and Windows workgroups

Our solution

Secure access control …with SIMATIC Logon


SIMATIC Logon Service - One-time logon

User name: WinCCAdmin

Password: ******************

Log on to: VISTAV7 (this computer)

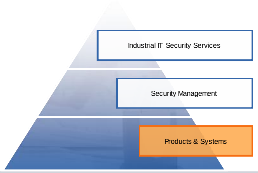
User Management of WinCC based on SIMATIC Logon with…

- Central administration (incl. password aging, auto logoff after inactivity time or multiple wrong password entries, lock screen)
- Configuration at runtime (add / lock / remove user accounts)
- All WinCC configurations are supported included web
- Supports domain concept and Windows work groups

User management and authentication for the security of your plant

Industrial Security

Secure data exchange from production level to ERP



SIEMENS

Customer requirement

Secure and reliable data exchange between different vendors

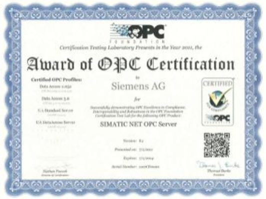
Protection against:

- Espionage
- Data manipulation
- Accidental access

Our solution

Data exchange based on **OPC UA Standard** even between different vendors

- Digitally signed messages
- Encrypted messages
  - 128 bits
  - 256 bits
- Unified Solution
  - Online data access
  - Historical data access
  - Alarms and events



OPC FOUNDATION

Certification Testing Laboratory Presents in the Year 2011, the

Award of OPC Certification

to

Siemens AG

for

Successfully demonstrating OPC Excellence in Compliance, Interoperability and Robustness in the OPC Foundation Certification Test Lab for the following OPC Product:

SIMATIC NET OPC Server

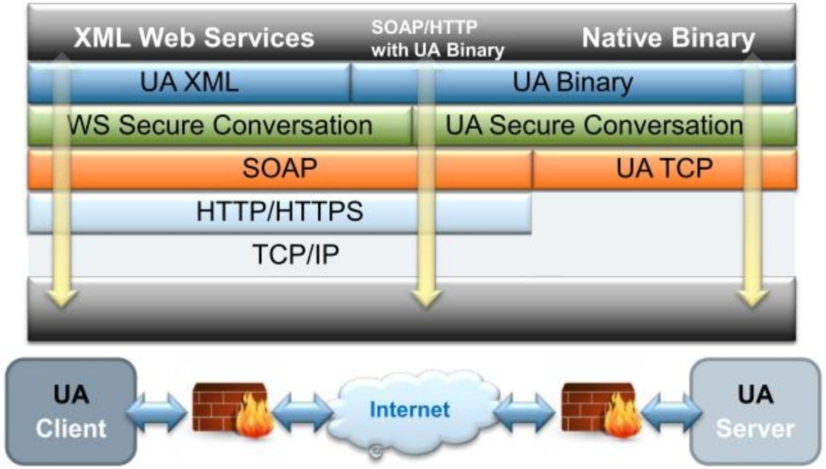
Certified OPC Profiles:
Data Access 2.05a
Data Access 3.0
UA Standard Server
UA DataAccess Server

Version: 8.1
Presented on: [illegible]
Expires: [illegible]
Serial Number: [illegible]

Nathan Pocock
Director of Certification

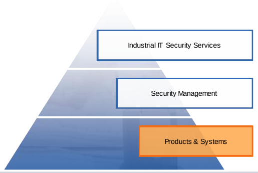
Thomas Burke
President

CERTIFIED FOR COMPLIANCE OPC FOUNDATION



© Siemens AG 2014. All Rights Reserved.

Industrial Security
Antivirus and whitelisting



SIEMENS

Customer requirement

Detection and prevention of Viruses, Worms and Trojans

Protection against:

- Malicious or unwanted Software
- Manipulation

Our solution

Antivirus and whitelisting solutions provide different security functions:

- Protection against Viruses, Worms and Trojans
- Stop unauthorized applications and malware

TREND MICRO™

Symantec.

intel Security

Industrial Security

SIEMENS

- Introduction
- The Siemens Solution
- **Application Examples**
- Benefits of Working with Siemens

Construction of a demilitarized zone (DMZ) e.g. for data server access with SCALANCE S623

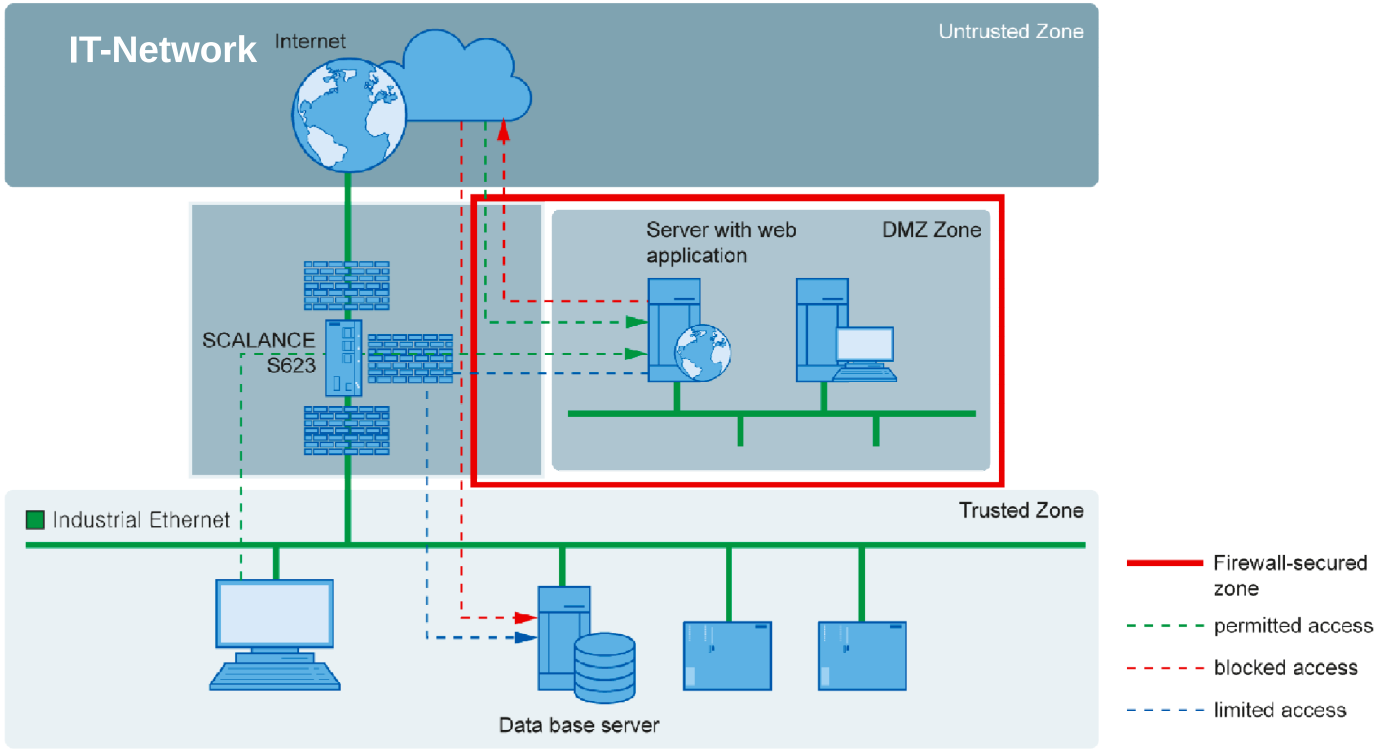
SIEMENS

Task

Network users (e.g. MES servers) should be reachable from the secure and non-secure network without creating a direct connection between the networks.

Solution

A DMZ can be established on the yellow port with the SCALANCE S623, in which the aforementioned server can be placed.



VPN for secure remote maintenance with SCALANCE M875

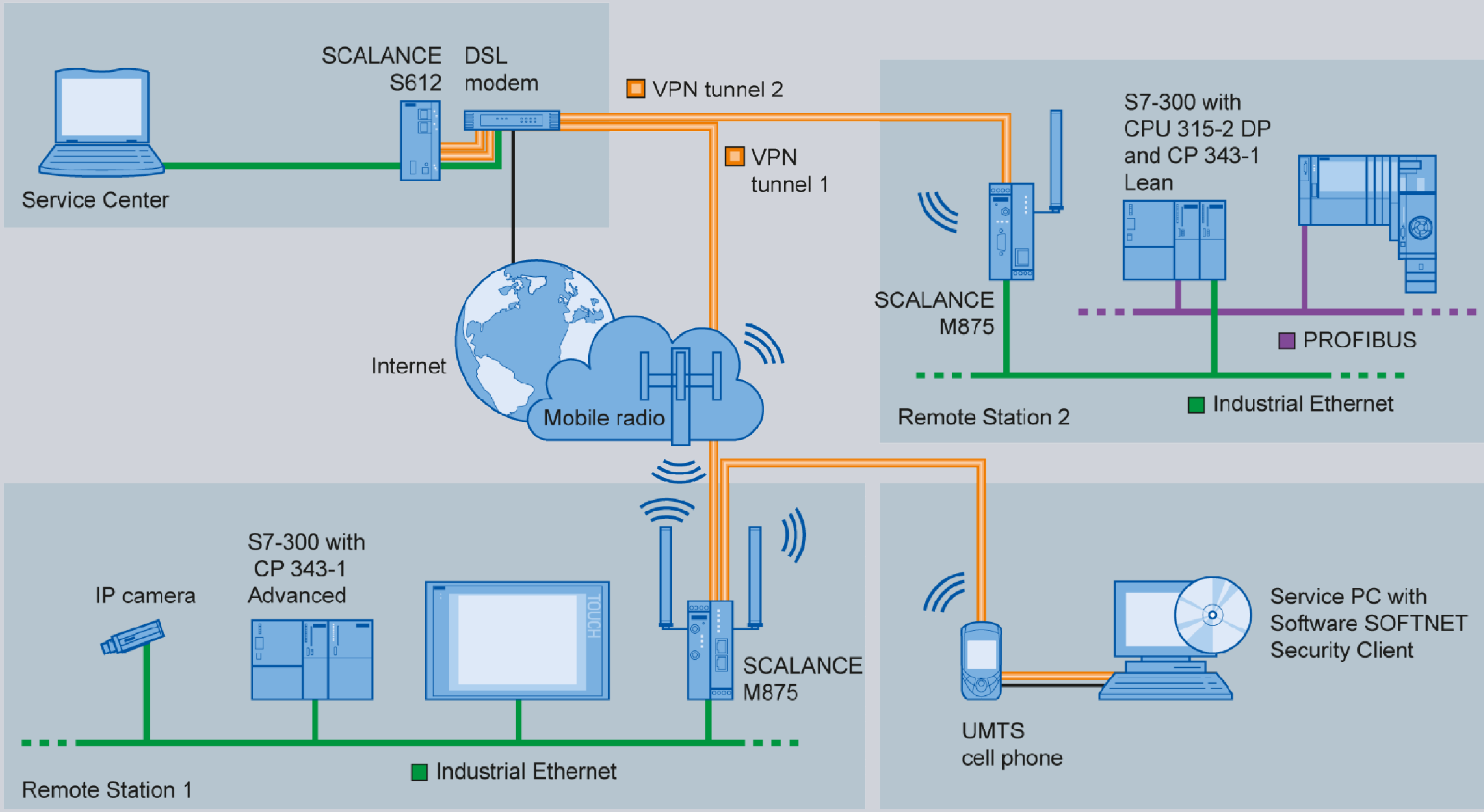
SIEMENS

Task

Classical applications such as remote programming, parameterization and diagnosis, but also monitoring of machines and plants installed worldwide can be performed from a service center that is connected over the Internet.

Solution

Any IP-based devices, particularly automation devices that are downstream
of the SCALANCE M875 in the local network, can be accessed. Multimedia applications like video streaming can be implemented thanks to the increased bandwidth in the uplink. The VPN functionality allows the secure transfer of data around the world.



Protection and segmenting through firewalls with SCALANCE S

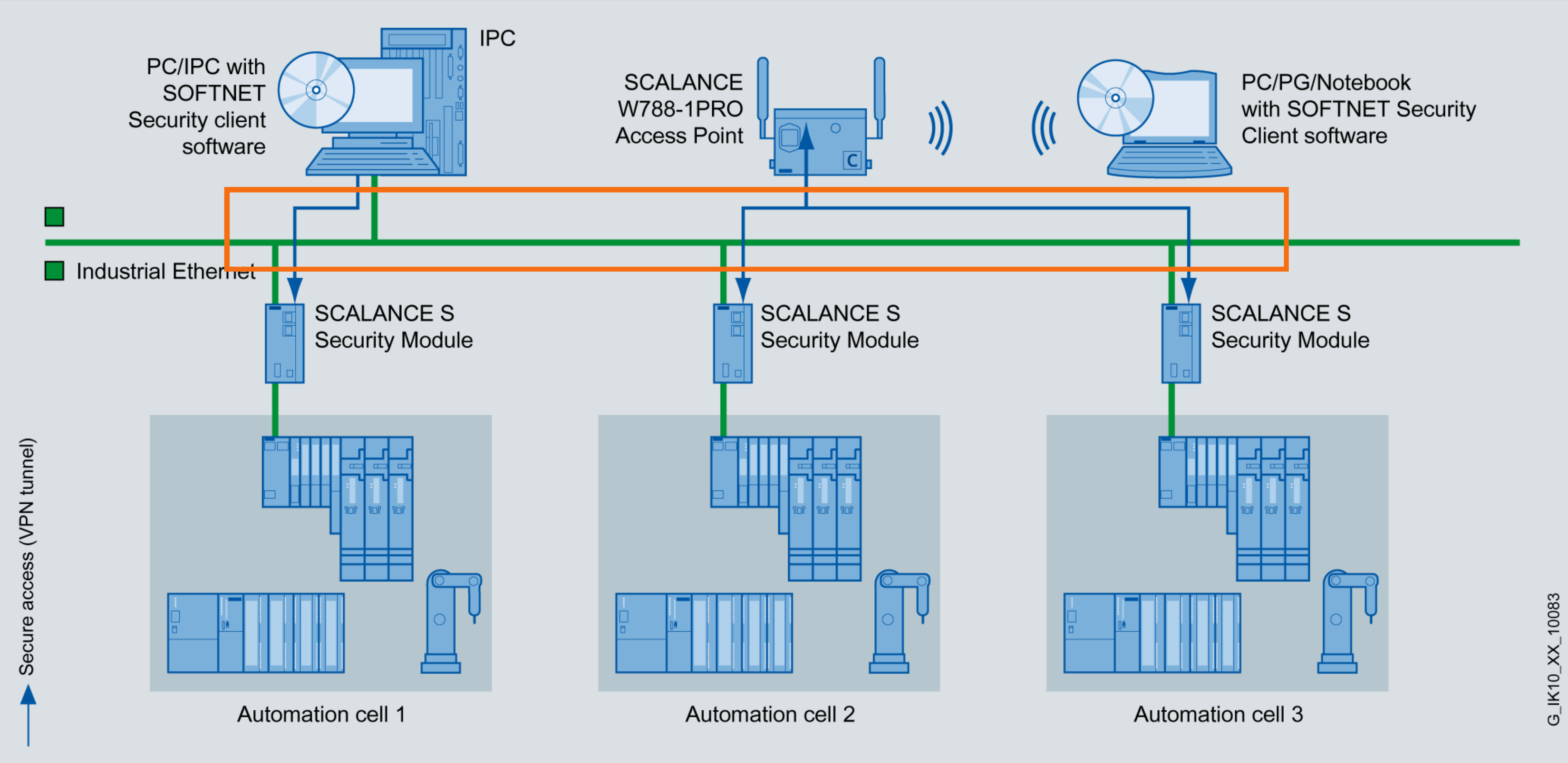
SIEMENS

Task

Parts of the system, which represent a logical unit and sometimes even come from different suppliers, should have only as many connections to one another as are absolutely necessary.

Solution

SCALANCE S is placed before an automation cell, thereby segmenting the network and reducing communication through firewall rules on the permitted connections.


PC/IPC with SOFTNET Security client software
IPC
SCALANCE W788-1PRO Access Point
PC/PG/Notebook with SOFTNET Security Client software
🟩 Industrial Ethernet
SCALANCE S Security Module
SCALANCE S Security Module
SCALANCE S Security Module
Secure access (VPN tunnel)
Automation cell 1
Automation cell 2
Automation cell 3
G_IK10_XX_10083

Access control and network separation through Firewalls with CP1543-1

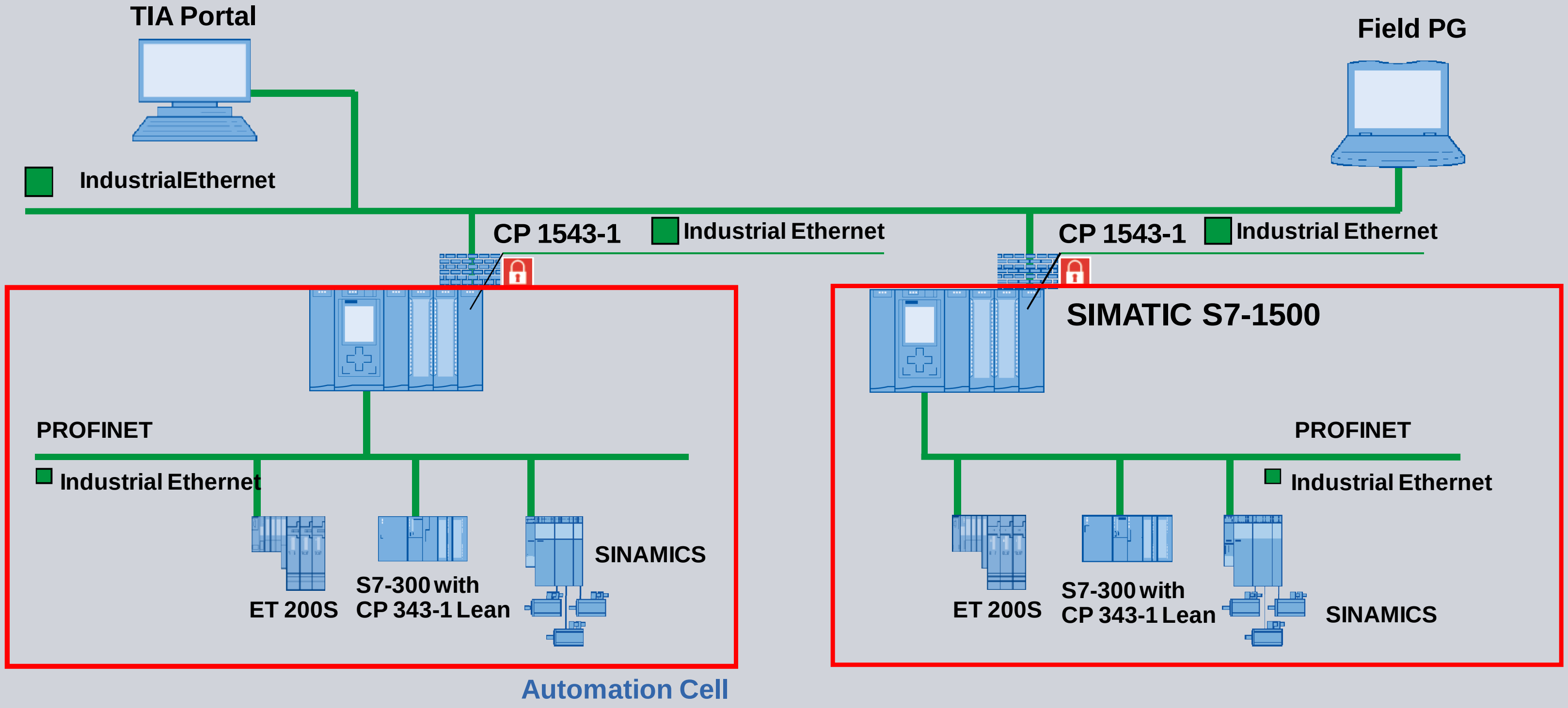
SIEMENS

Task

The communication between automation network and separated automation cells should be controlled and secured agains unauthorized access.

Solution

CP1543-1 will be placed in front of the automation cells, which should be protected. So, the communication from and to the automation cells can be controlled and only allowed connections are possible.



Industrial Security

SIEMENS

- Introduction
- The Siemens Solution
- Application Examples
- **Benefits of Working with Siemens**

Industrial Security

First vendor with certification on Achilles Level 2

SIEMENS

Certified CPUs

S7- 300 PN/DP

S7- 400 PN/DP

S7- 1500 PN/DP

S7- 400 HF CPU V6.0

S7- 410-5H

Certified CPs

CP343-1 Advanced

CP443-1 Advanced

CP1543-1

CP1628

Certified DP

ET200 PN/DP CPUs

Certified Firewalls

SCALANCE S602, S612, S623, S627-2M

+ Protection against DoS attacks

+ Defined behavior in case of attack

- **Improved Availability**
- **IP Protection**
- **International Standard**

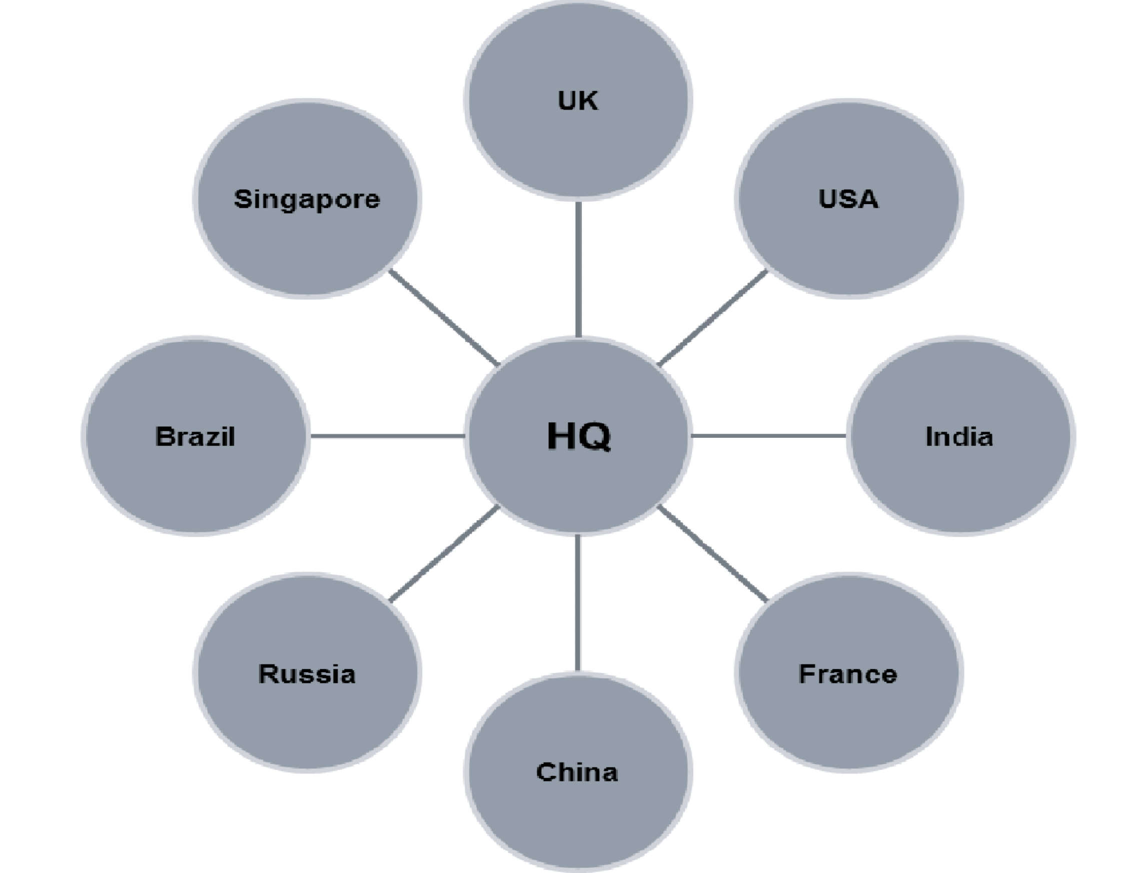
Industrial Security
Siemens Initiatives

System Test	- IP Hardening - Robustness and Test enhancements
Escalation process in case of incident	- Process and Escalation levels defined
New roles	- Product Security Office and Security Expert
Invest	- High investment in R&D - App. 100 persons involved in the security network
Central process enhancements	- Security aspects in project and product life cycle - Standardization & Regulations
Awareness and competence enhancements	- Workshops, web based trainings, announcements - Security training

Industrial Security

Siemens Security Network

SIEMENS

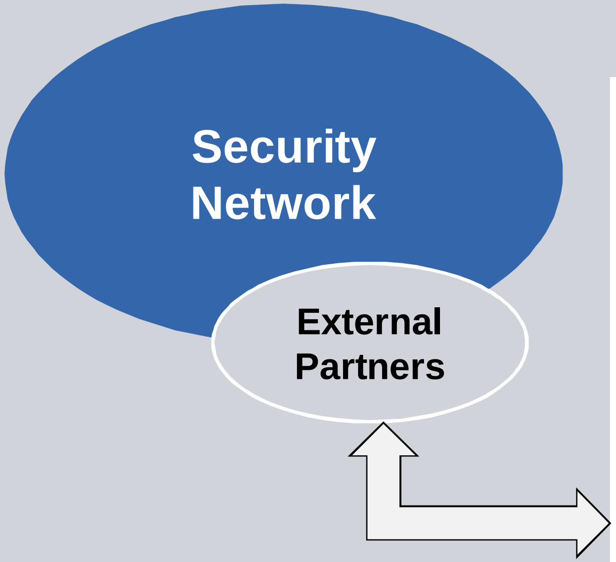


Tasks of the Security Hubs

- Setup of Security Network
- Worldwide Incident handling
- Setup of Alerts and remedies
- Cooperation with …
  - local CERT
  - Governmental Departments
  - Standardization & Regulations
  - Handling of Import/Export Issues

Industrial Security

Cooperation with standards bodies



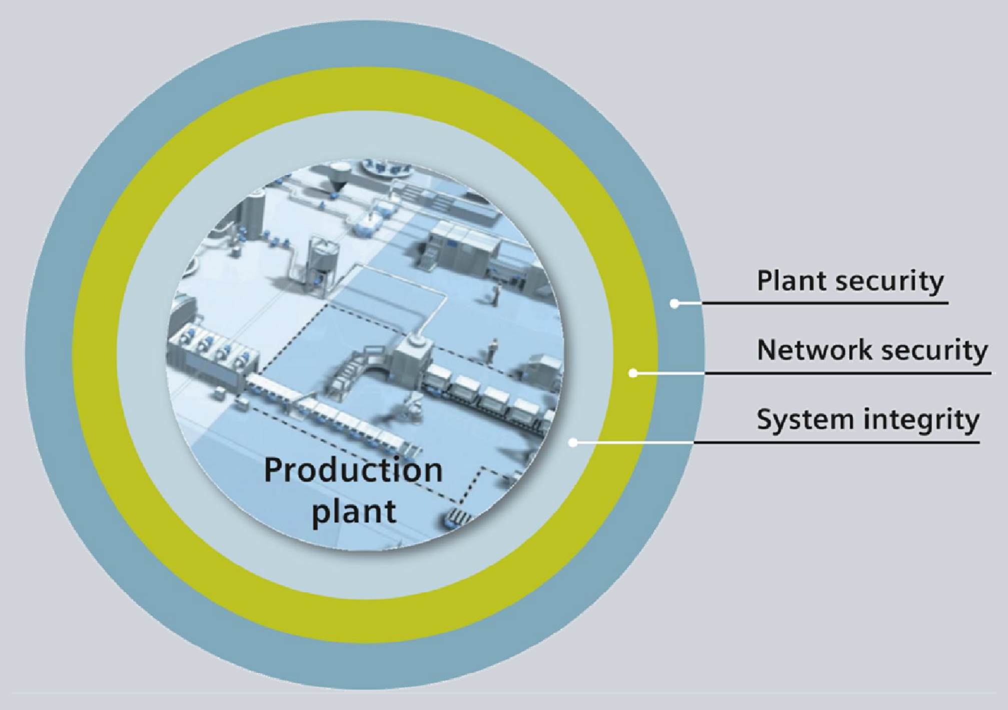
IEC TC 65	International Electrotechnical Commission
ISA SP99	International Standard for Automation
ISCI	ISA Security Compliance Institute
DKE	DKE German Commission for Electrical, Electronic & Information Technologies of DIN and VDE (Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE)
ZVEI	ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e.V.

Industrial Security

SIEMENS

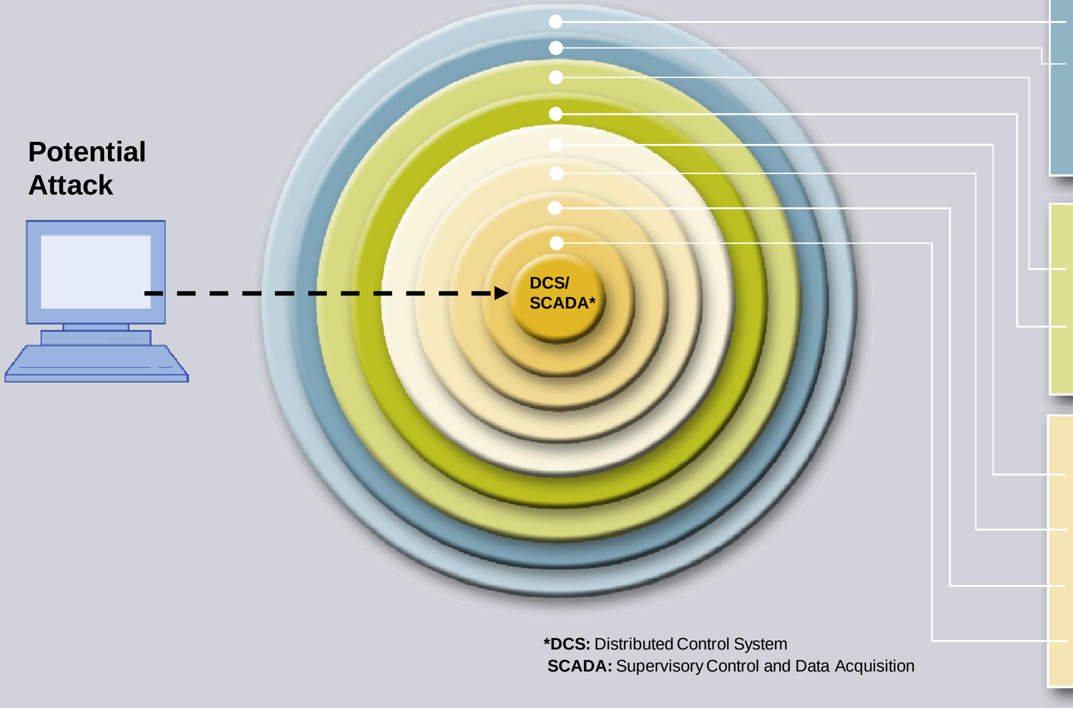
Customer benefits...

- Security is at the Core of TIA
- Increased Protection
- Increased Plant Availability
- Reduced Risk
- Intellectual Property Protection
- Complete Security Life-Cycle Support



Backup: Industrial Security

The Defense in Depth Concept in Detail



Plant Security

Physical Security
- Physical access to facilities and equipment

Policies & procedures
- Security management processes
- Operational Guidelines
- Business Continuity Management & Disaster Recovery

Network Security

Security cells & DMZ
- Secure architecture based on network segmentation

Firewalls and VPN
- Implementation of Firewalls as the only access point to a security cell

System Integrity

System hardening
- Adapting system to be secure by default

User Account Management
- Access control based on user rights and privileges

Patch Management
- Regular implementation of patches and updates

Malware detection and prevention
- Anti Virus and Whitelisting

***DCS:** Distributed Control System
SCADA: Supervisory Control and Data Acquisition