Industrial Security
Protecting Productivity

Unrestricted © Siemens AG 2017
Siemens.com/industrialsecurity
Industrial Security

- Introduction
- The Siemens Solution
- Holistic Security Concept
- 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”

Source: World Economic Forum, 50 Global Risks
Industrial Security
The corporate security chain is only as strong as its weakest link

Security Can Fail at Any of these Points

- Employees
- Smartphones
- Laptops
- PC workstations
- Network infrastructure
- Mobile storage devices
- Tablet PC
- Computer center
- Policies and guidelines
- Printer
- Production systems/plants
Industrial Security
Vulnerability disclosures are headline news

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 cyber attack

Feb. 12, 2013: „Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy. That’s why, earlier today, I signed a new executive order that will strengthen our cyber defenses... Now, Congress must act as well, by passing legislation to give our government a greater capacity to secure our networks and deter attacks.“

- U.S. President Barack Obama


In the ICS-CERT fiscal year (October 2013 until September 2014) ICS-CERT analyzed 245 attacks to control systems in the USA.
Industrial Security
Essential for secure industrial automation

Information technologies are used in industrial automation

- Horizontal and Vertical integration
- Open standards
- PC-based systems

Increased security threats demand action

- Loss of intellectual property, recipes …
- Plant standstill, e.g. due to viruses or malware
- Sabotage in the production plant
- Manipulation of data or application software
- Unauthorized use of system functions
- Compliance to standards and regulations is required

The Siemens solution provides a higher level of security
Digitalization is next level to yield productivity within automation industries

Discrete and Process Industries → Electrification, Automation and Digitalization as levers to increase productivity

**Technological driver**
- Computing power
- Communication
- New sensors
- Virtualization
- Cloud computing
- Simulation
- …

**Digitalization**
- TIA
  - Efficient interoperability of all automation components along the life cycle
- Digital Enterprise
  - Integrated Engineering and Integrated Operations

**Electrification**
- Electrical power wherever and whenever

**Automation**
- TIP

**Time**

Next level of productivity

Experienced partner for automation and electrification

Pioneer for digitalization in industry
Driving the Digital Enterprise – with security in automation

Industrial Security – prerequisite for Digitalization

Digitalization means:

- **Total Connectivity**: every real component has a digital twin in the IIoT → every component, every production- and network-level is connected and needs to communicate.

- **Big data**: transfer and storage of all machine and plant data – real-time, process data, diagnostics, quality data, IT data.

- **Use of open Standards**: required for a barrier-free data exchange

But these Trends increase also the vulnerability of production plants against cyber attacks and require effective and suitable security concepts and measures.
Industrial Security
Foundation and measures for secured operation in a Digital Enterprise

Secured Communication
- Encryption and monitoring for communication

Secured Access
- Access control for industrial components and networks

Secured Integrity
- Protection of the data transmission and storage

Secured Identification
- Authentication of devices and user

Foundation for continuous reliable operations in a Digital Enterprise
- Robust products with security characteristics & security services
- Security concepts like Defense in Depth and Holistic Security Concept
- Security philosophy like “need to connect”

*Holistic Security Concept
Industrial Security

- Introduction
- The Siemens Solution
- Holistic Security Concept
- Benefits of Working with Siemens
Industrial Security Concept from Siemens
Defense in Depth based on IEC 62443 / ISA 99

- **System integrity**
  - System hardening
  - Patch management
  - Detection of attacks
  - Authentication and access protection

- **Network security**
  - Cell protection and perimeter network
  - Firewalls and VPN

- **Plant security**
  - Physical access protection
  - Processes and guidelines
  - Holistic security monitoring

- **System hardening**
- **Patch management**
- **Detection of attacks**
- **Authentication and access protection**

**Defense in depth**

**Security threats demand action**

**Always Active**

**Plant Security Services**

**Perimeter network**
Industrial Security
Complete offering from Siemens: Concepts, products and services

The Siemens security concept – “Defense in Depth”

Siemens products and systems offer integrated security

- Know how and copy protection
- Authentication and user management
- Firewall and VPN
- System hardening

Siemens Plant Security Services

Assess Security  Implement Security  Manage Security

Unrestricted © Siemens AG 2017
Page 12
Industrial Security
The Siemens solution for plant security
Security Management Process

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

Security Management is essential for a well thought-out security concept
Industrial Security
The Siemens solution for network security
**Industrial Security**  
*Overview: Network Security*

**Adapted measures for production**

### Network Access Control
- Interface to IT networks:
  - Secure architecture with DMZ
  - Secure Remote Access via Internet
  - Local network access (port security) via device and user authentication

### Redundancy
- Protection of redundant network topologies

### Cell Protection
- Risk mitigation through network segmentation
- Extension of the cell protection concept with
  - Security PC- and S7-CPs
  - Flexible VLAN configuration

![Diagram showing network security measures](image-url)
Industrial Security –
Essential Network Security use cases

**DMZ**

Increased protection through data exchange via DMZ by avoiding direct access to the automation network

- A Firewall controls all data traffic between the different networks and DMZ.

**Remote access**

Secured remote access via the Internet or mobile networks avoiding espionage and sabotage.

- Encryption of data transmission and access control via Security modules or Internet- and mobile wireless routers

**Secure redundancy**

Higher reliability and availability and securing of redundant network structures

- Security modules in synchronized standby mode and integrated in redundant rings.

**Cell protection**

Devices without own network security functionality can be protected within the automation cells

- Access to cell is secured by firewall mechanisms
Industrial security appliances – SCALANCE S

Industrial Security Appliance SCALANCE S

Industrial Security
The Siemens solution for system integrity
Industrial Security
SIMATIC S7-1200, S7-1500 and the TIA Portal

Security Highlights

The SIMATIC S7-1200 V4, S7-1500 incl. S7-1500 Software Controller and the TIA Portal provide integrated 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
    - from the STEP 7 project
    - from the data of the memory card
    - from program libraries

- **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 with STEP 7
  - Protection against duplicating the project saved on the memory card
Industrial Security
SIMATIC S7-1200, S7-1500 and the TIA Portal

Security Highlights

The SIMATIC S7-1200 V4, S7-1500 incl. S7-1500 Software Controller and the TIA Portal provide integrated security features:

- **Increased Access Protection (Authentication)**
  Extensive protection against unauthorized project changes:
  - New degree of Protection Level 4 for PLC, complete lockdown (also HMI connections need password) *
  - Configurable levels of authorization (1-3 with own password)
  - General blocking of project parameter changes via the built-in display

- **Expanded Access Protection**
  Extensive protection against unauthorized project changes:
  - Via Security CP1543-1 by means of integrated firewall and VPN communication

- **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)
  - Detection of manipulated firmware updates by means of digital checksums

* Optimally supported by SIMATIC HMI products and SIMATIC NET OPC Server
OPC UA Security

- Selectable security policies in Controller and Clients
- Device/application authentication based on certificates
- Integrity protection and encrypted communication
- User authentication and restricted access to PLC tags

Integrated security mechanisms

- User authentication and restricted access to PLC tags
- Device/application authentication based on certificates
- Integrity protection and encrypted communication
- Selectable security policies in Controller and Clients

OPC UA

S7-1500, 1500S, 1500T
ET 200SP CPU, PLCSIM Adv.
**Industrial Security**
Security for HMI Systems

<table>
<thead>
<tr>
<th>Security Highlights</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Panel access protection</strong></td>
</tr>
<tr>
<td>Protect device settings of the panels by assigning a password.</td>
</tr>
<tr>
<td><strong>User management</strong></td>
</tr>
<tr>
<td>Protect again unauthorized access with permission-based user management</td>
</tr>
<tr>
<td><strong>System hardening functions</strong></td>
</tr>
<tr>
<td>Increased security with configurable system hardening measures such as locking task switching, Web server authentication</td>
</tr>
</tbody>
</table>
Industrial Security
WinCC SCADA

Customer Requirement
Secured SCADA environment

Protection against:
• Espionage
• Data manipulation
• System failure

Our Solution
WinCC offers a broad spectrum of security-promoting features:
• **More secure communication** of the terminal bus via **SSL encryption** and use of **static ports** in communication (Firewalls)
• System tests and result documentation with current **virus scanners** and patterns
• **WinCC User Administration / SIMATIC Logon**
  Only authenticated users obtain access to the system
• **WinCC Runtime**
  No access or limited access to the operating system (desktop)
• **WinCC Web Viewer**
  Access only to operator screens/no access to Internet pages in order to prevent unintentional download of malware etc.
• **WinCC/WebUX**
  Web-based access using an protected connection (HTTPS)
• **WinCC/Audit, WinCC/Change Control**
  Logging of operator actions, e.g. with solutions in the FDA environment
• **WinCC/Redundancy**
  Higher availability of servers/process connections in the case of an error
Industrial Security
SIMATIC Logon

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

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 workgroups

User management and authentication for the security of your plant
## Industrial Security

### Antivirus and whitelisting

<table>
<thead>
<tr>
<th>Customer Requirement</th>
<th>Our Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection and prevention of Viruses, Worms and Trojans</td>
<td><strong>Antivirus and whitelisting</strong> solutions provide different security functions:</td>
</tr>
<tr>
<td><strong>Protection</strong> against:</td>
<td>• Protection against Viruses, Worms and Trojans</td>
</tr>
<tr>
<td>• Malicious or unwanted Software</td>
<td>• Stop unauthorized applications and malware</td>
</tr>
<tr>
<td>• Manipulation</td>
<td></td>
</tr>
</tbody>
</table>
Industrial Security

- Introduction
- The Siemens Solution
- Holistic Security Concept
- Benefits of Working with Siemens
Holistic Security Concept takes security on the next level - A holistic approach for IT and OT

HSC answers key questions for security in business

“What in my business do I need to protect?”
Identification of the critical business assets is a core component of the concept

“What level of security do I need?”
Security level drives requirements, in alignment with IEC 62443, to protect against attacks

“How do I protect the specific assets?”
Standards based security solutions are applied to protect and monitor the critical assets

HSC addresses 5 levers including the IT

- IT - Infrastructure
- Handle incidents
- Improve process
- Security features
- Enhance Awareness
General Workflow for the Protection of Product-specific Assets

IEC62443/ISO27001 Based Method

**Definition of Scope**
The scope comprises the product and business activities to be considered by HSC.

**Identification and Business Impact Assessment of Product-specific Assets**
Product-specific assets (e.g. specifications, source code) are generated during the product lifecycle.

**Definition of Target Level**
The protection concept is assessed by measuring the achieved protection level and by conducting a risk analysis to identify the residual risks.

**Risk Assessment**

**Development and Implementation of Protection Concept**
The protection concept includes adequate technical and procedural measures to address the requirements.
Protection Levels are the key criteria and cover security functionalities and processes

<table>
<thead>
<tr>
<th>Security process</th>
<th>Maturity Level 1 - 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Based on IEC 62443-2-4 and ISO27001</td>
<td></td>
</tr>
<tr>
<td>- Maturity Level 1 - 4</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security functions</th>
<th>Security Level 1 - 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Based on IEC 62443-3-3</td>
<td></td>
</tr>
<tr>
<td>- Security Level 1 - 4</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protection Level (PL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maturity Level</td>
</tr>
<tr>
<td>Security Level</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>PL 1</td>
</tr>
</tbody>
</table>
## Selected HSC security measures from PL 1 to PL 4

<table>
<thead>
<tr>
<th>Secure Physical Access</th>
<th>Organize Security</th>
<th>Secure Solution Design</th>
<th>Secure Operations</th>
<th>Secure Lifecycle management</th>
</tr>
</thead>
<tbody>
<tr>
<td>PL 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revolving doors with card reader</td>
<td>Dual approval for critical actions</td>
<td>Firewalls with Fail Close (e.g. Next Generation Firewall)</td>
<td>Monitoring of all device activities</td>
<td>Online security functionality verification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PL 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revolving doors with card reader</td>
<td>No Email, No WWW, etc. in Secure Cell</td>
<td>2 PCs (Secure Cell/outside)</td>
<td>Monitoring of all human interactions</td>
<td>Automated backup / recovery</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PL 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Doors with card reader</td>
<td>Persons responsible for security within own organization</td>
<td>Physical network segmentation or equivalent (e.g. SCALANCE)</td>
<td>Continuous monitoring (e.g. SIEM)</td>
<td>Remote access restriction (e.g. need to connect principle)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PL 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Locked building/doors with keys</td>
<td>Awareness training (e.g. Operator Awareness Training)</td>
<td>Network segmentation Firewall protection (e.g. SCALANCE S)</td>
<td>Security logging on all systems</td>
<td>Backup / recovery system</td>
</tr>
<tr>
<td></td>
<td>Mandatory rules on USB sticks (e.g. Whitelisting)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Unrestricted © Siemens AG 2017**

Page 47
Industrial Security

- Introduction
- The Siemens Solution
- Holistic Security Concept
- Benefits of Working with Siemens
Industrial Security
Granted Certificates

- TIA Ethernet based devices
  - E.g. S7-1500, 1505S, S7-300, CP343-1 SCALANCE S, …
- Protection against DoS attacks
- Defined behavior in case of attack
- Improved Availability

- Development process
  - Certification of “Secure Product Development Lifecycle” for Division DF and PD based on IEC 62443-4-1

- S7- 1500 Controllers
  - SCALANCE XM408-8C
  - First security level certification (CSPN – Certification de Sécurité de Premier Niveau)

Find more information:
http://www.wurldtech.com/product_services/certifications/certified_products/
http://ssi.gouv.fr/certification_cspn/simatic-s7-1518-4-version-du-micrologiciel-
1-83/ http://www.ssi.gouv.fr/entreprise/certification_cspn/scalance-xm408-8c/
Stakeholders according to IEC 62443

- Integrator
- Vendor
- Asset Owner

SIEMENS

<table>
<thead>
<tr>
<th>Security by design</th>
<th>✓</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security verification and validation testing</td>
<td>✓</td>
</tr>
<tr>
<td>Security update management</td>
<td>✓</td>
</tr>
</tbody>
</table>

Relationships and responsibilities
Industrial Security
Siemens is the leading vendor of Achilles level 2 certified products

Certified CPUs
- LOGO!
- S7- 300 PN/DP
- S7- 400 PN/DP
- S7- 1500 and 1505S
- S7- 1200
- S7- 400 HF CPU V6.0
- S7- 410-5H

Certified CPs
- CP343-1 Advanced
- CP443-1 & Advanced
- CP1243-1
- CP1543-1
- CP1628

Certified DP
- ET 200 PN/DP CPUs
- ET 200SP PN CPUs

Certified Firewalls
- SCALANCE S602, S612, S623, S627-2M

+ Protection against DoS attacks
+ Defined behavior in case of attack
  - Improved Availability
  - International Standard
Industrial Security
Security-related expertise

- We collaborate intensively with CERT organizations (e.g. FIRST, ANSSI, and ICS-CERT)
- We are member of the Software Assurance Forum for Excellence in Code (SAFECode)
- We maintain partnership with Security researchers around the world
Industrial Security
Security concepts for industry

- Siemens brings its experience into the relevant committees
- Siemens internal security measures are based upon the requirements set by IEC 62443
- We offer specific security solutions for the manufacturing and process industry
Industrial Security
Security Vulnerability Handling

- We created a sophisticated team of security experts and Product Computer Emergency Response Team (ProductCERT)
- We maintain open communication with customers
- We make advisories and updates available on a public website
Industrial Security
Security of Siemens Products

- We do product design for fundamental system hardening
- We adapted PLM, SCM, and CRM processes to fulfil IEC 62443 requirements
- We do 3rd party product certifications
### Industrial Security

#### Siemens Initiatives

<table>
<thead>
<tr>
<th>Topic</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Test</td>
<td></td>
</tr>
<tr>
<td>Escalation process in case of incidents</td>
<td>• Process and Escalation levels defined</td>
</tr>
<tr>
<td>New roles</td>
<td>• Product Security Office and Security Expert</td>
</tr>
<tr>
<td>Invest</td>
<td>• High investment in R&amp;D</td>
</tr>
<tr>
<td></td>
<td>• App. 100 persons involved in the security network</td>
</tr>
<tr>
<td>Central process enhancements</td>
<td>• Security aspects in project and product life cycle</td>
</tr>
<tr>
<td></td>
<td>• Standardization &amp; Regulations</td>
</tr>
<tr>
<td>Awareness and competence enhancements</td>
<td>• Workshops, web based trainings, announcements</td>
</tr>
<tr>
<td></td>
<td>• Security training</td>
</tr>
</tbody>
</table>
Industrial Security
Siemens Security Network

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
Siemens has a comprehensive organization to handle all aspects of Industrial Security

Establish a Security Network to …
… react quickly in case of emergency
… drive and coordinate all security relevant topics

- Standardization & Regulations
- International Hubs
- Governmental Departments
- CERTs
- Anti-malware companies
- Security Network of Software OEMs
# Industrial Security

Cooperation with standards bodies

<table>
<thead>
<tr>
<th>Organization</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC TC 65</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>ISA SP99</td>
<td>International Standard for Automation</td>
</tr>
<tr>
<td>IECCE</td>
<td>IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components</td>
</tr>
<tr>
<td>DKE</td>
<td>DKE German Commission for Electrical, Electronic &amp; Information Technologies of DIN and VDE (Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE)</td>
</tr>
<tr>
<td>ZVEI</td>
<td>ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V.</td>
</tr>
<tr>
<td>VDE</td>
<td>Verband der Elektrotechnik Elektronik Informationstechnik e.V.</td>
</tr>
</tbody>
</table>
Industrial Security
Siemens Vertical Expertise: Chemical

Chemical Environment
- Chemical Environment
- Production Flexibility
- Operational Efficiency
- Product Quality

Industrial Security provides
- Increased Plant Availability
- Secure User Access

Industrial Security to keep your plant running securely
Industrial Security

Customer benefits...

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

Protecting productivity with Industrial Security from Siemens
Conclusion: For our customers is Siemens the partner to drive the Digitalization

We understand Digitalization
We have vertical Know-how
We understand Industrial Communication
We offer Industrial Security products and services
Our processes and products are proved and certified

Reliable Base for a secure Automation!
Industrial Security
Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens’ products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens’ guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens’ products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer’s exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under http://www.siemens.com/industrialsecurity.
Thank You

Alan Cone
Siemens Industry Inc.
5300 Triangle Parkway
Norcross, GA 30092
alan.cone@siemens.com

www.siemens.com/industrialsecurity

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations, product names, etc. may contain trademarks or other rights of Siemens AG, its affiliated companies or third parties. Their unauthorized use may infringe the rights of the respective owner.

siemens.com