

Industrial Security

An Ongoing Task



Industrial Security



- **Industrial Security History**
- The Building Blocks of Industrial Security

The Changing Security Situation – from Fieldbuses to Industrial Ethernet



Benefits of Industrial Ethernet

- Openness (e.g. for integration of wireless communication systems)
- Internet connectivity (e.g. for remote access)
- Higher number of nodes (theoretically billions within an IP subnet)
- Higher data rates (100/ 1,000/ 10,000 Mbit/s)

Issues to consider

- Vulnerability through openness
- Threats from the Internet
- Address conflicts if not carefully administrated
- Necessity to plan and structure networks

Industrial Ethernet means great benefit to the industry,
but also requires new security standards

Office versus Industrial Security

Office IT

Objectives and requirements

- Security of data
- Control administrative processes
- Prevent espionage



Features

- A lot of connections via the internet
- Regular patches possible
- Use of standard SW and HW
- Examples: PC, Microsoft, applications, internet

Production IT

Objectives and requirements

- Prevent loss of production (availability!)
- Product quality
- Safety: prevent hazards
- Security: prevent sabotage



Features

- Data connections to office IT / internet must be subject to clear security management
- SW update strictly limited
- Specific SW for automation and control of production processes
- Examples: SCADA systems, S7 control

Siemens Industrial Security History

- **1995:** Introduction of
 - **Knowhow Protect feature:** encryption of S7 program blocks
 - **Copy Protection:** program blocks bound to HW serial number
- **2004:** Start of cooperation with the Swiss CERN institute to identify any vulnerability and to improve the robustness of components against hacking etc.
- **2005:** Introduction of the **Cell Protection Concept** with the SCALANCE S security modules
- **2007:** **IP Hardening** of Ethernet-based SIMATIC components to improve the communication robustness of Ethernet
- **2010:** Improvement of the Knowhow Protect feature and the Copy Protection mechanism with STEP 7 V5.5

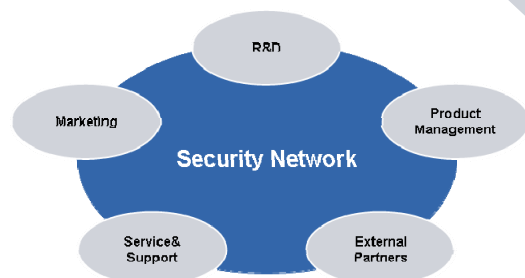
Industrial Security



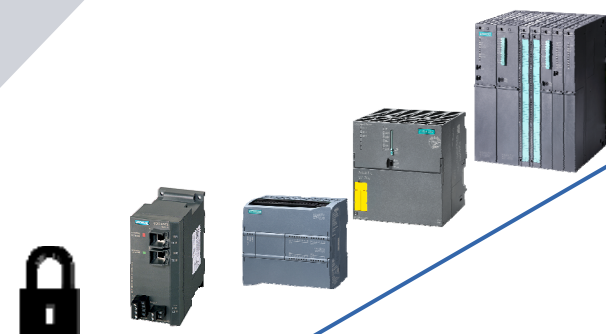
- Industrial Security History
- **The Building Blocks of Industrial Security**

Security is an Ongoing Task

Organization



Technical Security



Processes



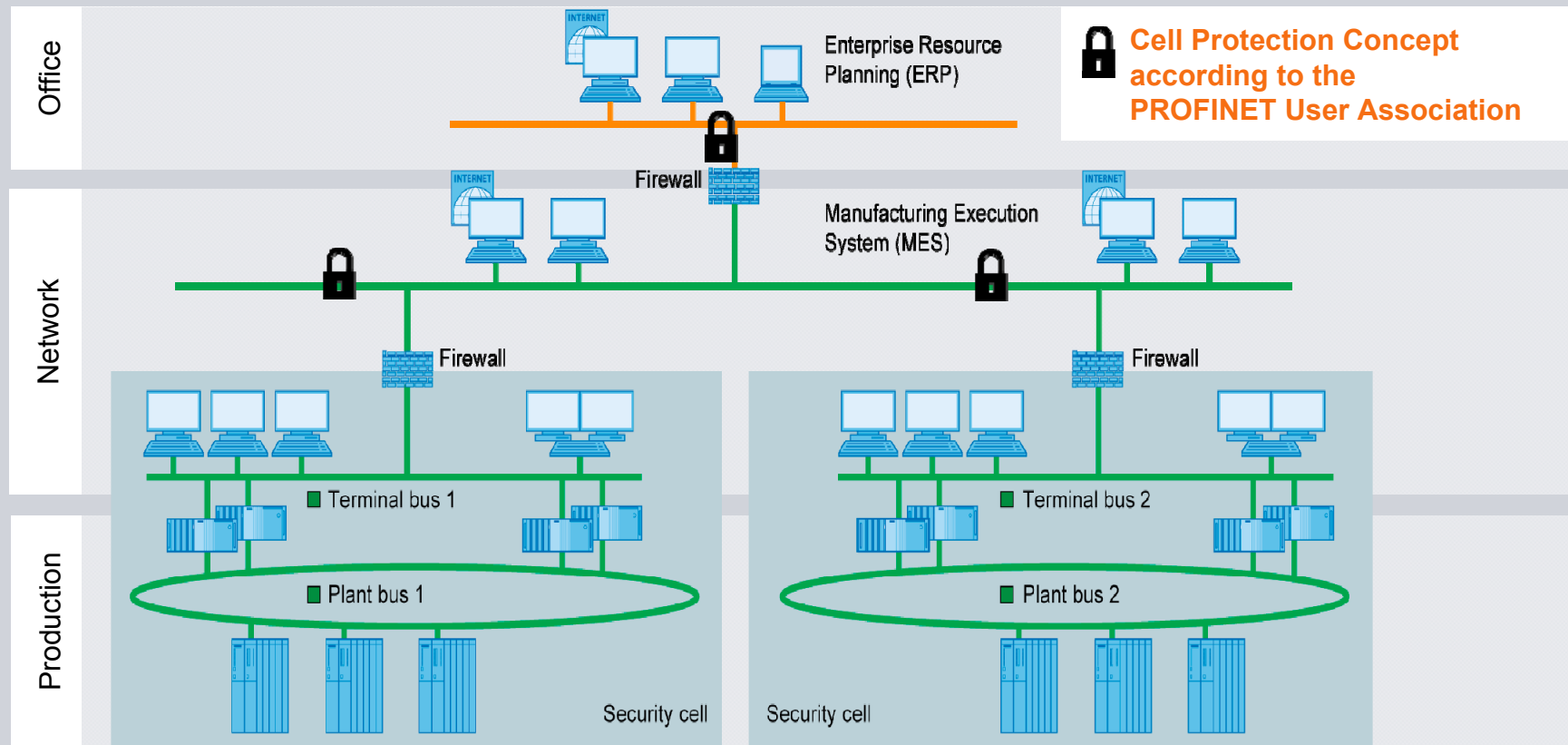
Standardization/ Regulations

e.g. IEC standards

Industrial Security must be addressed at various different levels

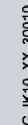
Technical Industrial Security Features in Production Systems

SIEMENS



Industrial security consists of processes, products and measures to prevent data abuse and intrusion by third parties into office environment & production processes

© Siemens AG 2011. All Rights Reserved.



Siemens Industrial Security Services Covering All Phases of the Plant Lifecycle

SIEMENS



Security services from Siemens Industry

- Security awareness training and workshops
- Vulnerability assessments
- Consulting on secure architectures and concepts
- Implementation services
- PCS 7 Firewall
- Application whitelisting

© Siemens AG 2011. All Rights Reserved.

Thank you for your attention!



Jochen Koch

Marketing Manager Industrial Communication
I IA SC IC PRM 4

Gleiwitzer Straße 555
90475 Nuremberg

Phone: +49 911 895-5305
Fax: +49 911 895-155305
Cellular: +49 172 8337452

E-Mail: jochen.koch@siemens.com