Cyber Security News

Walter Wutzl – Head of Technical Sales Secondary
Franziska Diestel – Head of Software & Digitalization

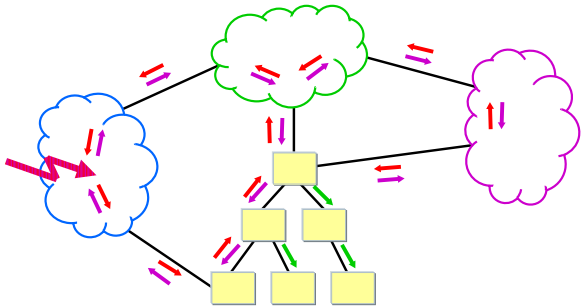
VAR Partner Day 2022 | September 12 -14 | Zagreb, Croatia

SIEMENS

System and Product Solutions for Cyber Security

Intensive collaboration with Austrian utilities since 2013

- Due to a communication problem that affected almost all utilities in May 2013



Siemens Digital Grid Austria certified for ISO/IEC 27001 since 2015

NIS Directive entered into force in August 2016

- 27 months for member states to transpose the NIS Directive into national laws

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

SIEMENS

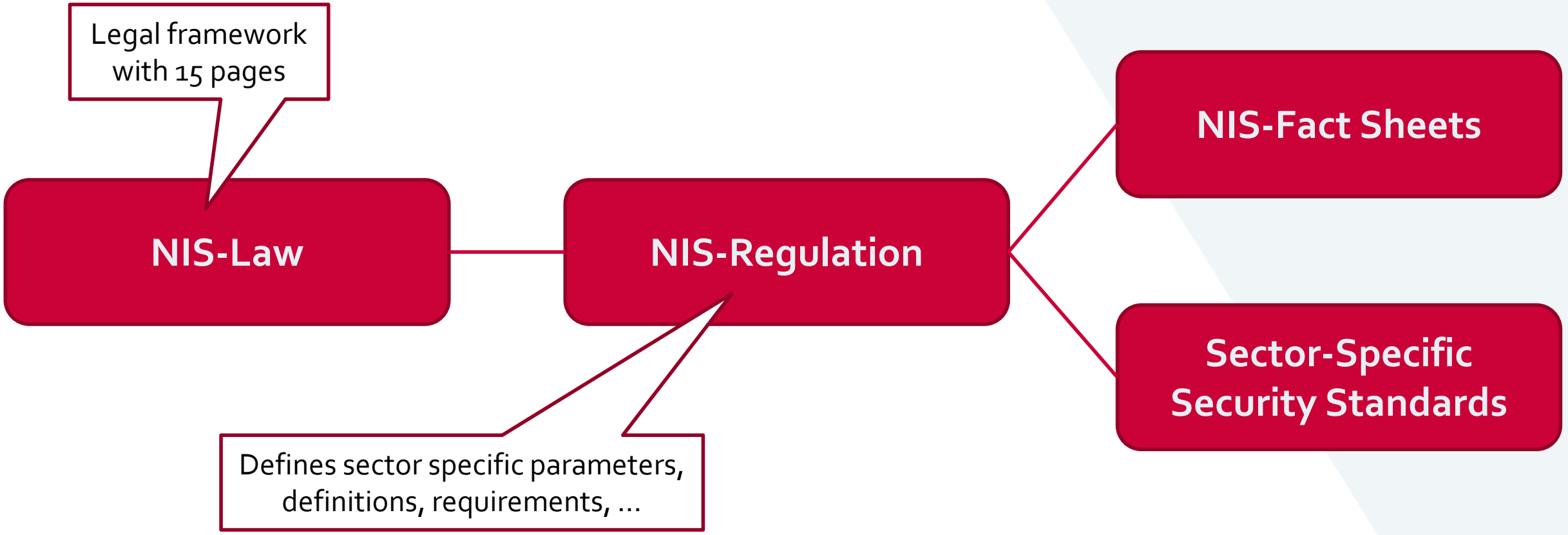
Implementation of the NIS Directive in Austria…

…from the point of view of the Operational NIS Authority in the Ministry of Internal Affairs

Customers started late, are struggling now …

Gernot Goluch, II/.BVT/5-NIS
Wien, 27. Juni 2019

Security Measures – Framework



Sector-Specific Security Standards

Bundesministerium
Inneres

bmi.gv.at

Security Measures – Framework

Legal framework with 15 pages

NIS-Law

NIS-Regulation

NIS-Fact Sheets

Sector-Specific Security Standards

Defines sector specific parameters, definitions, requirements, ...

Siemens – 27. Juni 2019

4

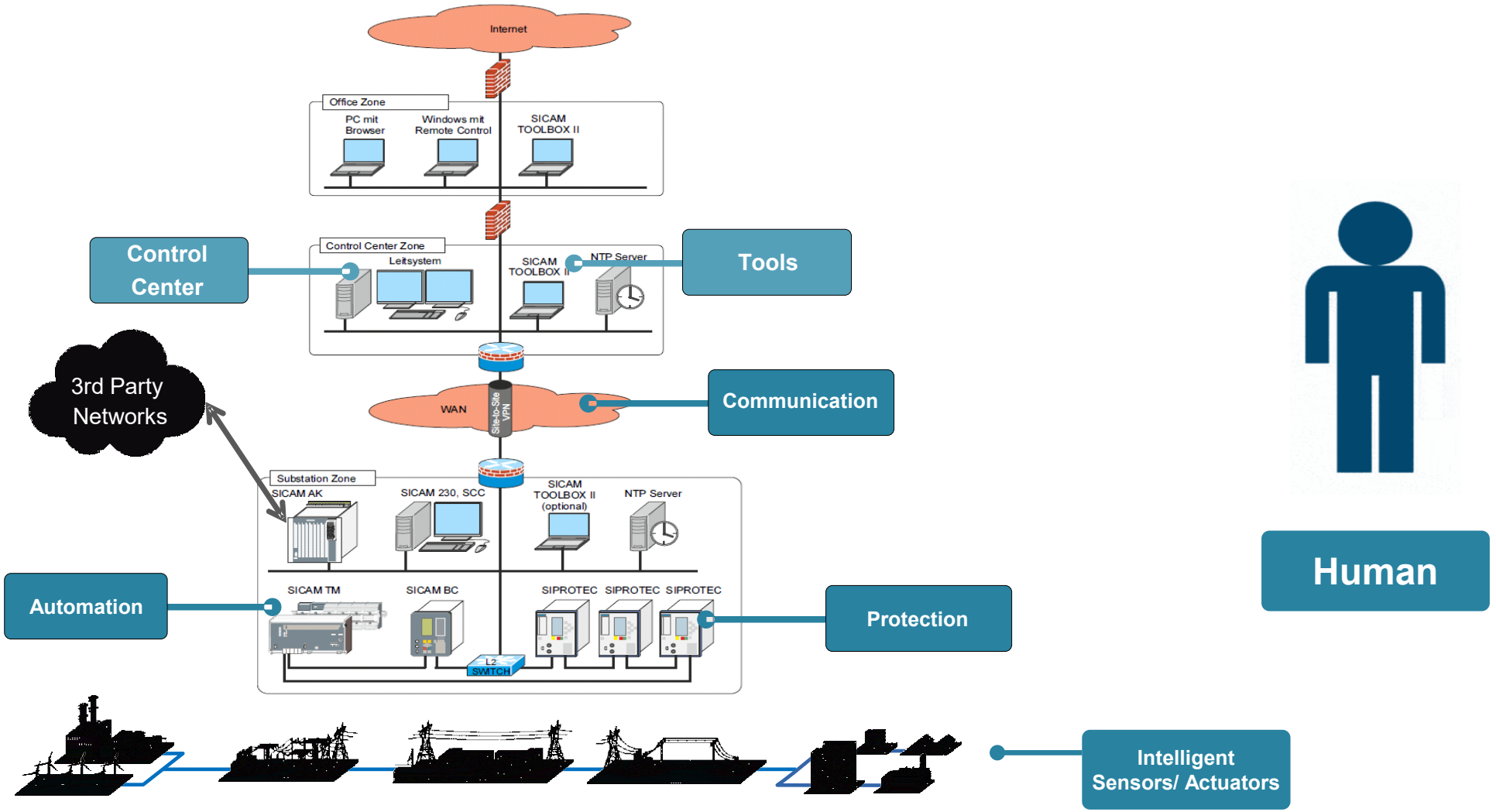
AT-3SV-Elektrizität

Sektorenspezifische Sicherheitsvorkehrungen für den Sektor Energie (AT-3SV-Elektrizität) im Sinne des § 17 Abs. 2 NISG mit Einschränkung auf den Teilsektor Elektrizität im Sinne des § 4 Abs. 1 Z 1 NISV

Versionsnummer: 1.4
Ausstellungsdatum: 24. Juni 2021
Österreichs E-Wirtschaft

SIEMENS

Security – A Holistic View



SIEMENS

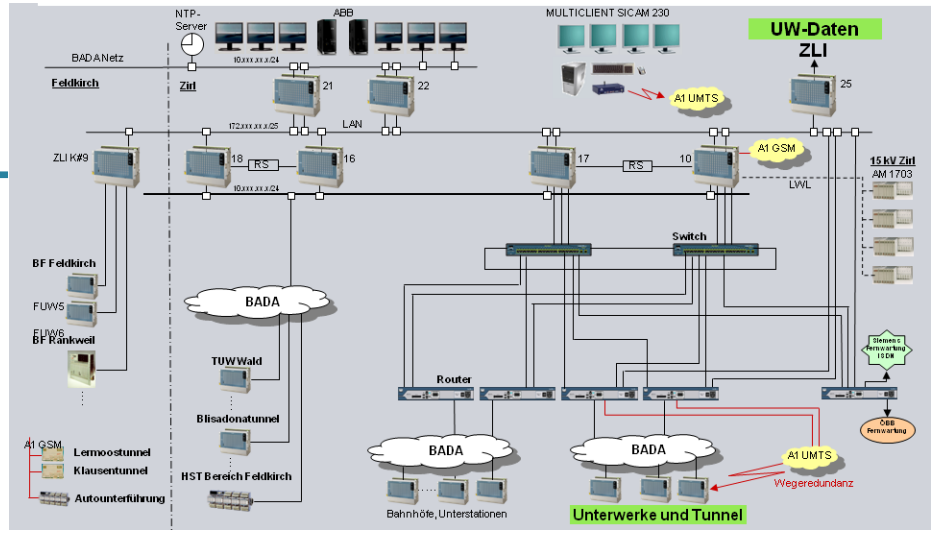
Security - Topics

Products

- Security for control centers
- Security for embedded systems
- Security for engineering tools

System - Security4projects

- Network segmentation
- Data transmission via unsecured networks
- Back up / Restore
- Patch management
- Integration / upgrade of existing systems



Human

- Security Know How
- Security Maintenance

SIEMENS

Security - Topics
SICAM A8000 – Security Features (Excerpt)

Firewall

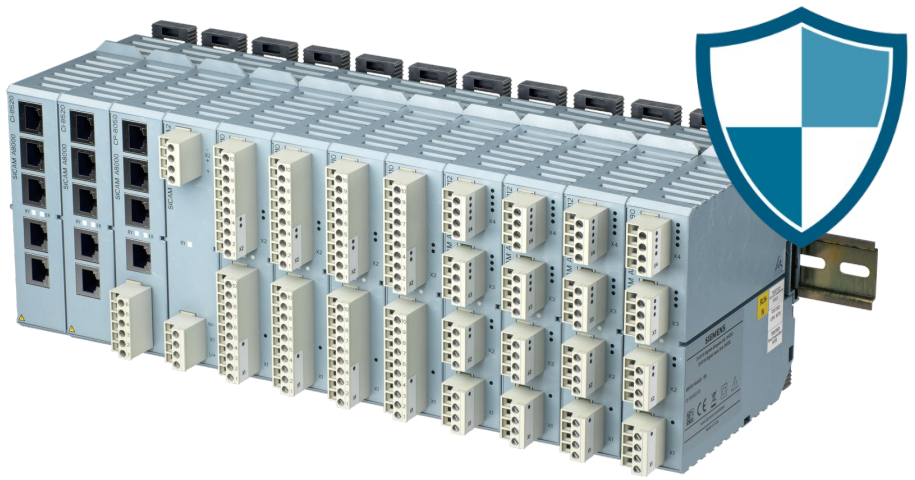
For the separation of TCP/IP networks via integrated software firewall or additional hardware-based application firewall

Firmware Signature

Protection against firmware manipulation

Security Logbook

Non-volatile storage of SYSLOG events



TLS encryption

Certificate based encryption in accordance IEC 62351-3

IPSec encryption

Communication encryption via pre-shared keys

Role Based Access Control

in accordance with IEC 62351-8

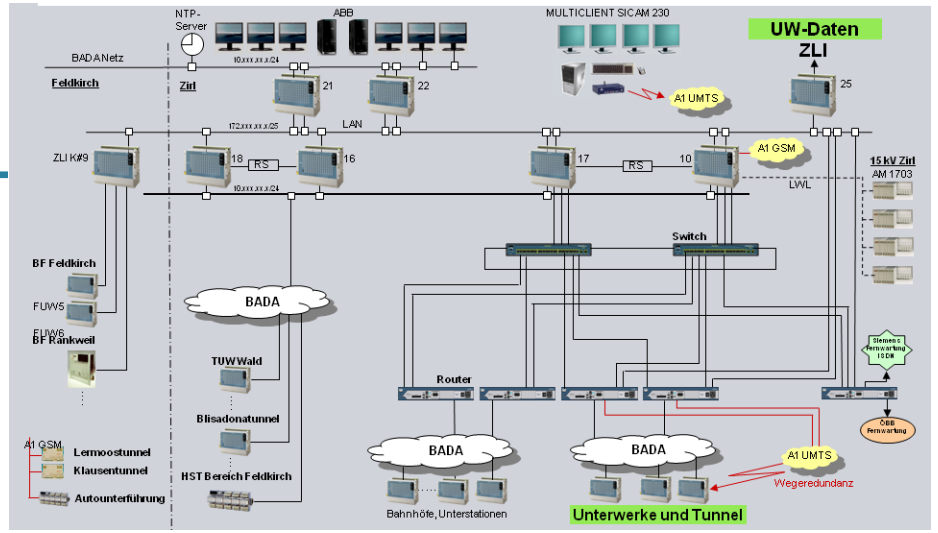
VLAN support

in accordance with IEEE 802.1Q

Security – Topics
Data transmission via unsecured networks

Products
- Security for control centers
- Security for embedded systems
- Security for engineering tools

System - Security4projects
- Network segmentation
- Data transmission via unsecured networks
- Back up / Restore
- Patch management
- Integration / upgrade of existing systems



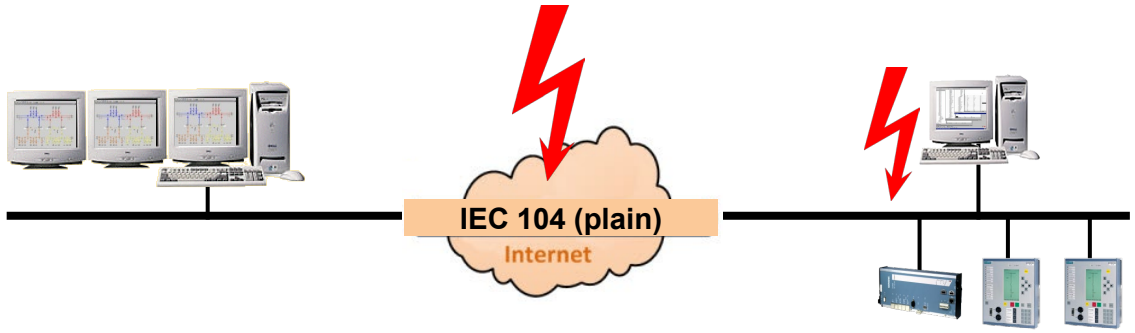
Human
- Security Know How
- Security Maintenance

SIEMENS

Data transmission via unsecured networks
System - Security4Projects

No secured communication between control center zone ⇔ substation zone

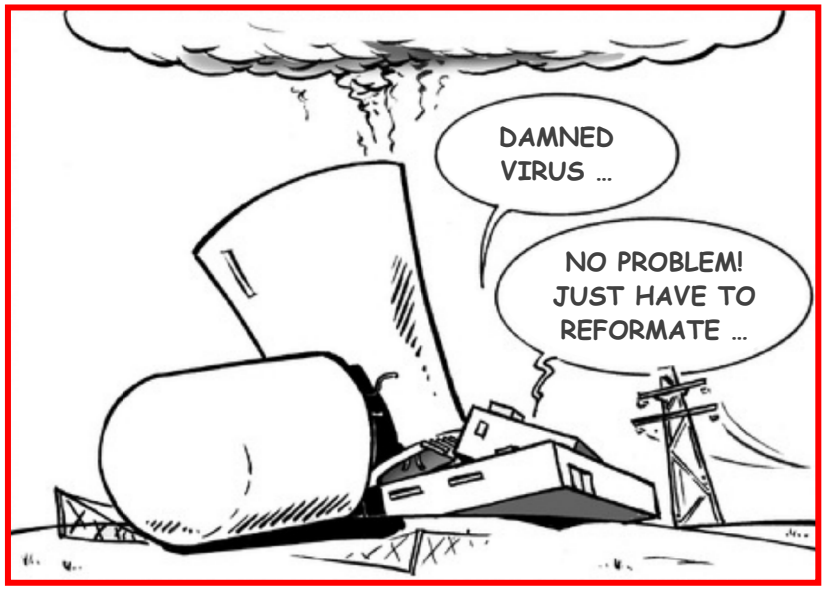
- No problem if secure wide area network …



Control Center Zone **Substation Zone**

Potential threat of

- Man-in-the-middle attack
  - Replay attack for commands …
- IP-based unauthorized access
  - e.g. substation ⇒ control center

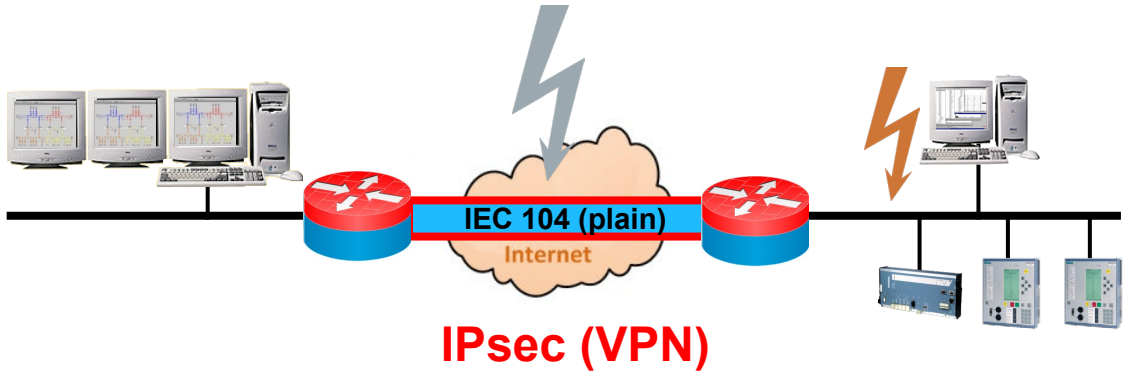


SIEMENS

Data transmission via unsecured networks
System - Security4Projects

Site-to-Site Security between
control center zone ⇔ substation zone

- No impact on existing system/devices
- Actual standard for encryption
- Based on network components
  - Need for network know how …



Potential threat of

- Man-in-the-middle attack
  - Replay attack for commands …
- IP-based unauthorized access
  - e.g. substation ⇒ control center

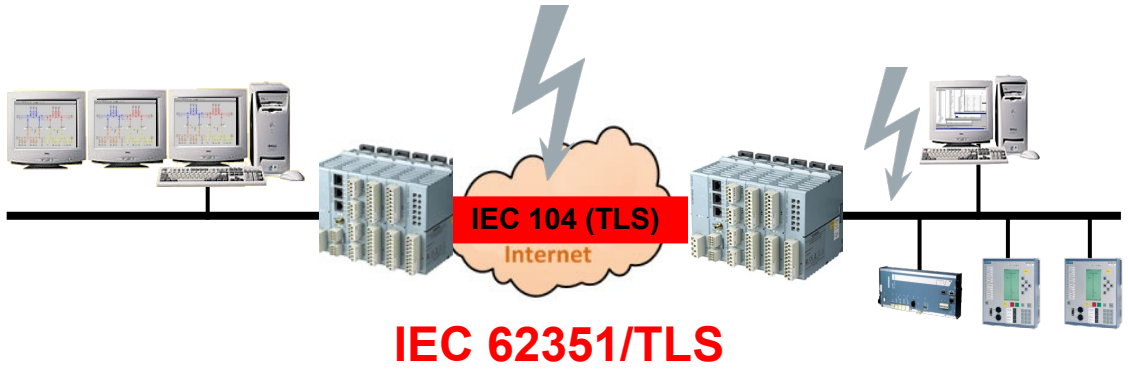
Data transmission via unsecured networks
System - Security4Projects

End-to-End Security between
control center zone ⇔ substation zone

- By Hardware Application Layer Firewall
  - Encryption, authentication
- No impact on existing system/devices
  - Easy to configure
  - Independent from communication network

Potential threat of

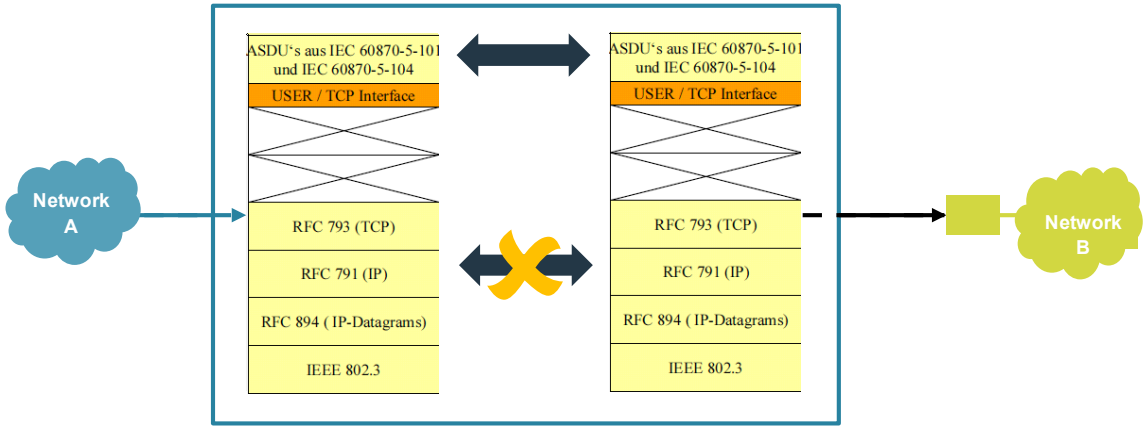
- Man-in-the-middle attack
  - Replay attack for commands …
- IP-based unauthorized access
  - e.g. substation ⇒ control center



IEC 62351/TLS

Control Center Zone **Substation Zone**

Hardware Application Layer Firewall



No Bridging, switching or routing of IP-frames through IED

SIEMENS

Data transmission via unsecured networks
System - Security4Projects

End-to-End Security between
control center zone ⇔ substation zone

- By Hardware Application Layer Firewall
  - Encryption, authentication
- No impact on existing system/devices
  - Easy to configure
  - Independent from communication network

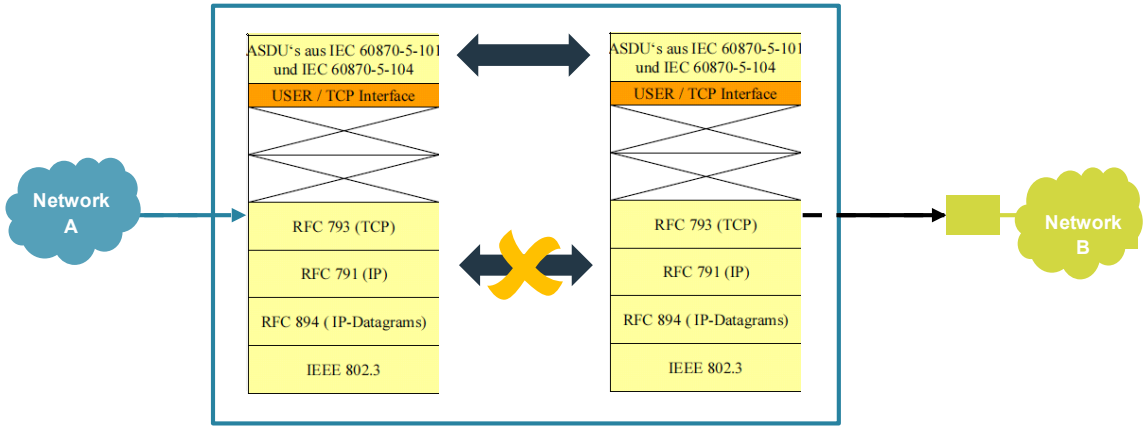
Potential threat of

- Man-in-the-middle attack
  - Replay attack for commands …
- IP-based unauthorized access
  - e.g. substation ⇒ control center

IEC 62351/TLS

Control Center Zone **Ring Main Unit**

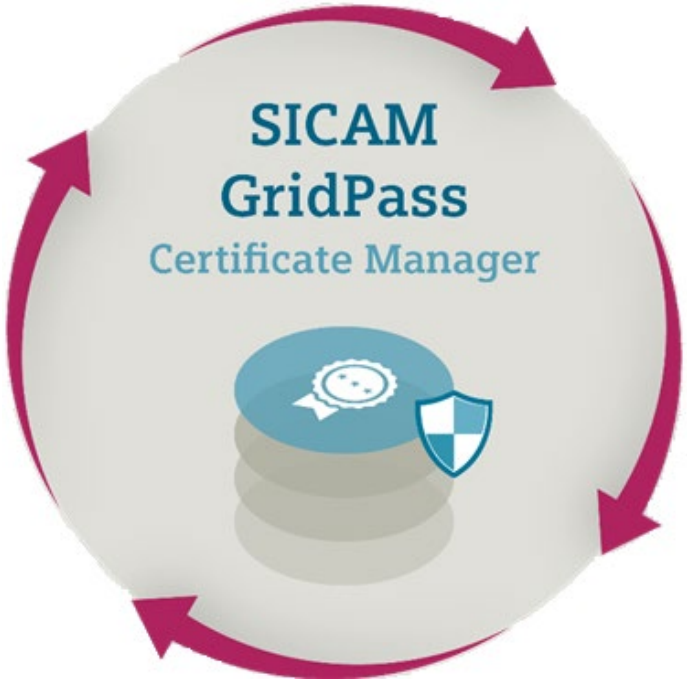
Hardware Application Layer Firewall

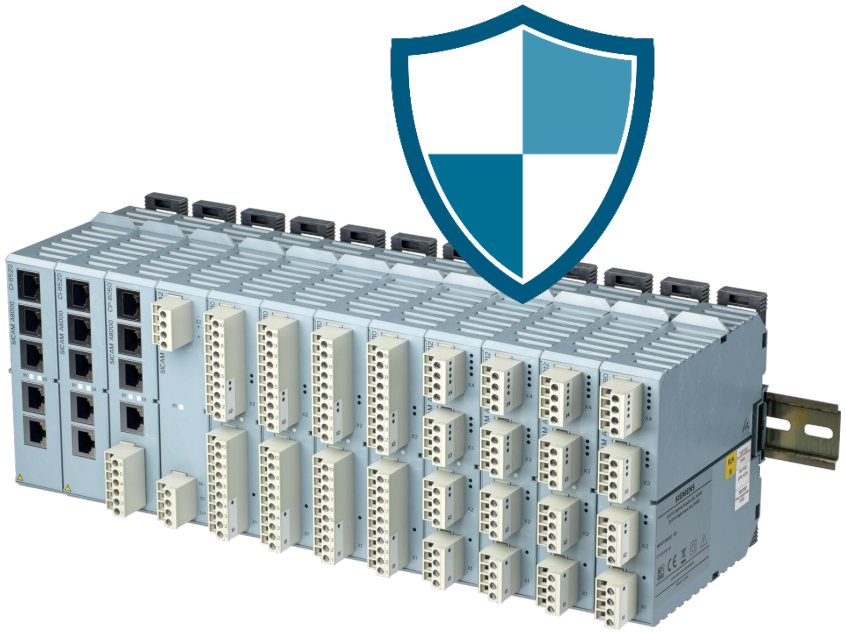


No Bridging, switching or routing of IP-frames through IED

SIEMENS

Data transmission via unsecured networks
Certificate Management (SICAM Gridpass)



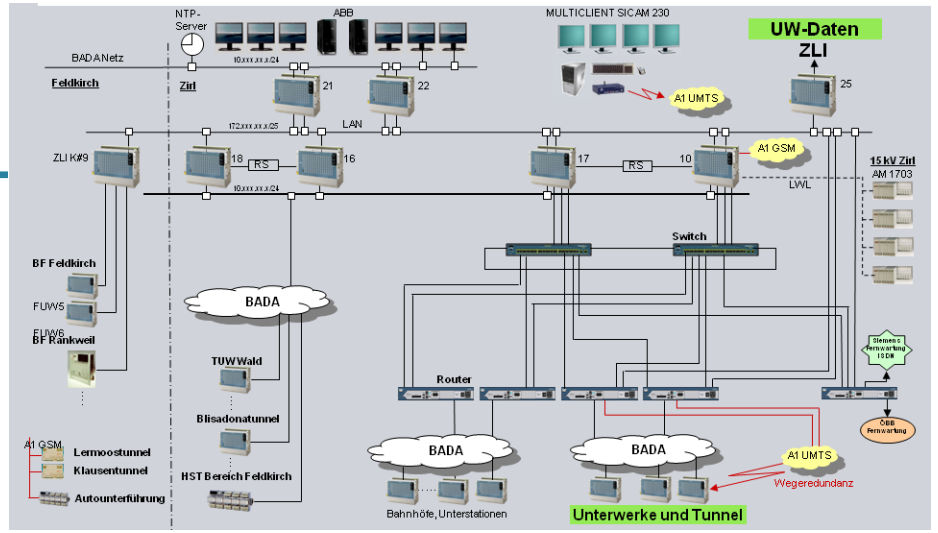


For automatic exchange of certificates in IED

Security – Topics
Patch management

Products
- Security for control centers
- Security for embedded systems
- Security for engineering tools

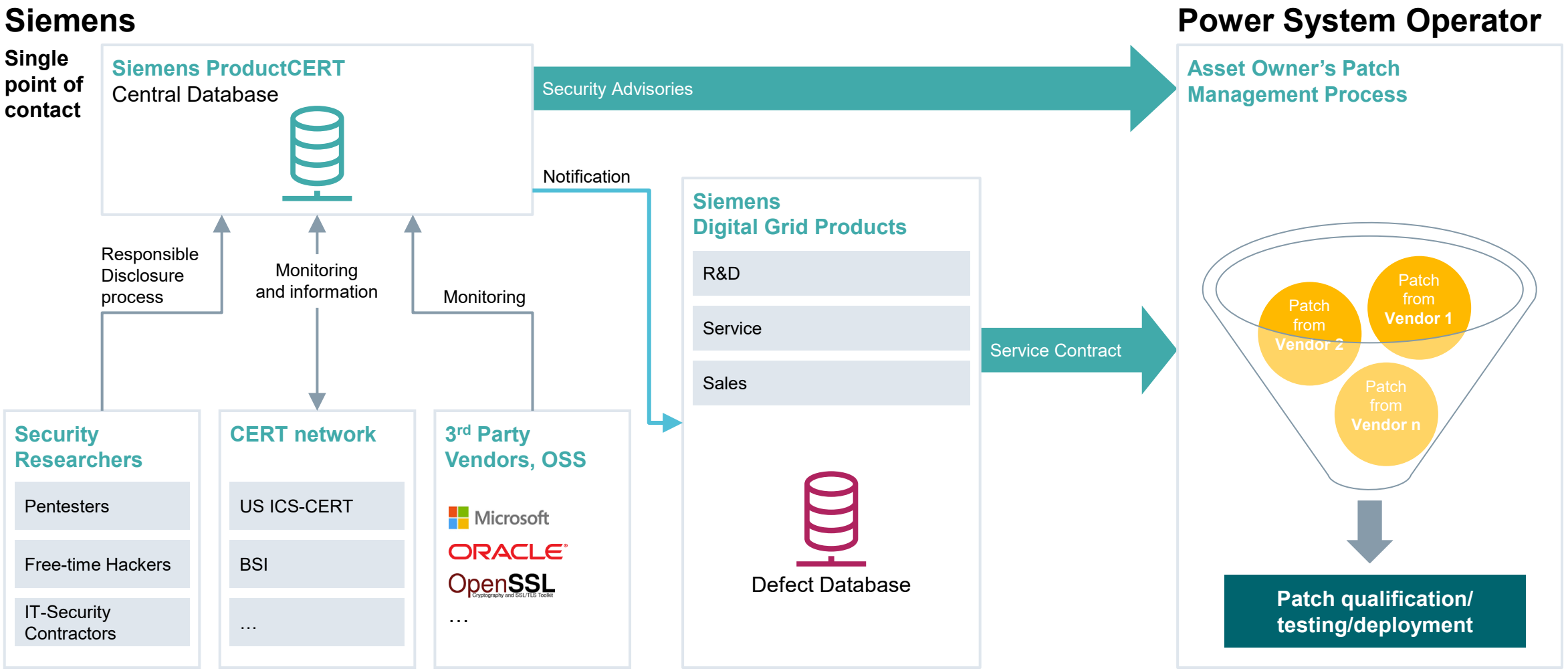
System - Security4projects
- Network segmentation
- Data transmission via unsecured networks
- Back up / Restore
- Patch management
- Integration / upgrade of existing systems



Human
- Security Know How
- Security Maintenance

SIEMENS

Patch management
Precondition: Monitoring for Vulnerabilities



1st Patch Management Contract @ Austrian Utility since 2017

One of the biggest Austrian Utilities

- Huge installed base
- Over years …

Motivation

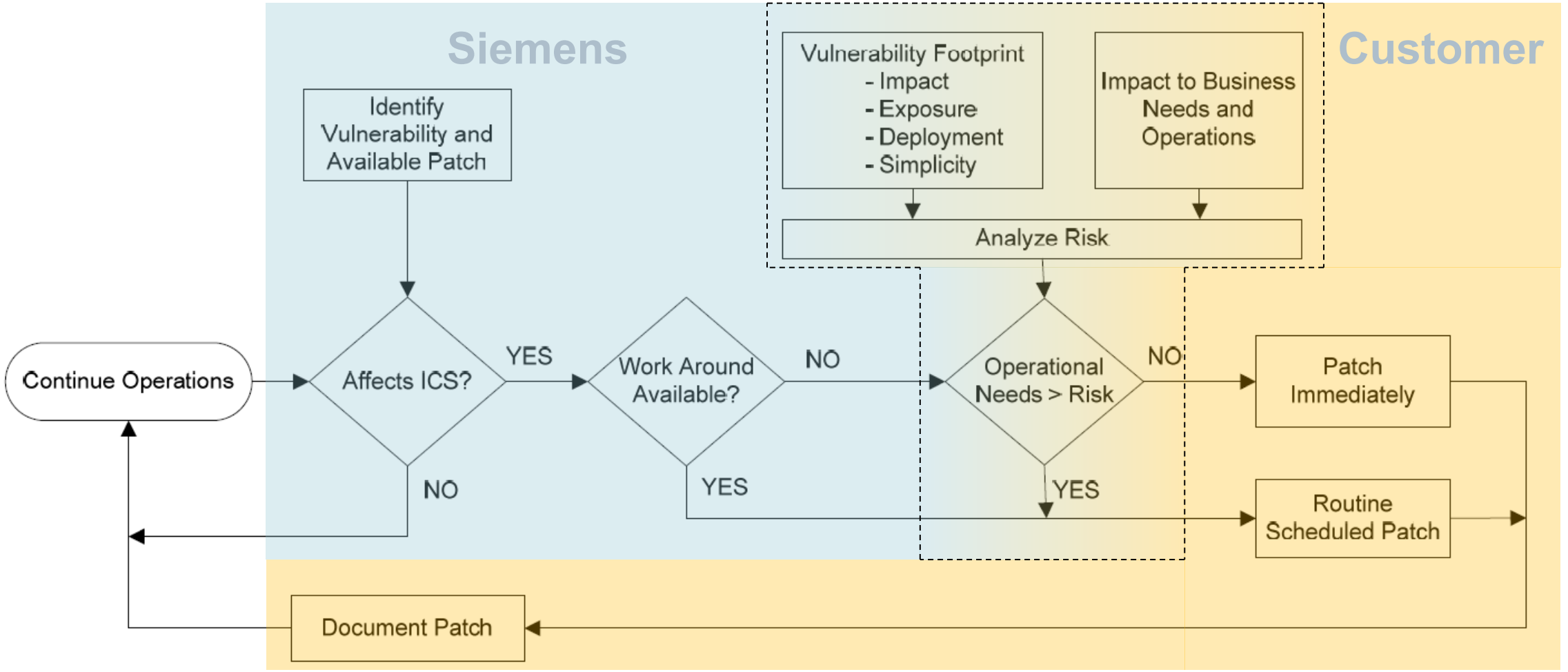
- ISO 27001 certified
- NIS Directive

Common development of process/ setup with customer

- Over months …

SIEMENS

1st Patch Management Contract @ Austrian Utility since 2017
Patch Urgency Decision Tree



Intrusion Detection
How it works in office IT

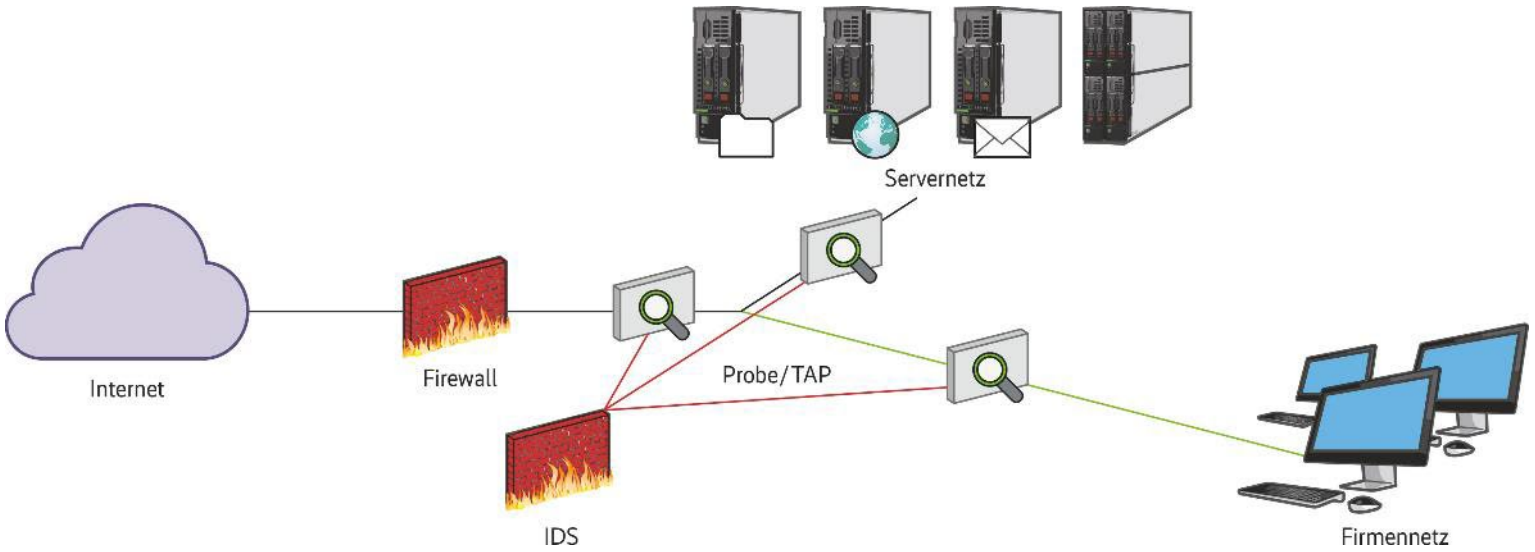
SIEMENS
Ingenuity for life

IDS (Intrusion Detection System) analyzes the data stream in network and reports suspicious behavior by

- comparison with known attack signatures (“blacklisting”) and
- statistical analyses

IDS is „listening“ the data stream via

- mirror ports and/ or
- sensors



Intrusion Detection
How it works in office IT

SIEMENS
Ingenuity for life

IDS (Intrusion Detection System) analyzes the data stream in network and reports suspicious behavior by

- comparison with known attack signatures (“blacklisting”) and
- statistical analyses

Not working for process networks (OT) so far …

- Experience of joint research project together with university and utility
- Feedback from users from other pilot installations

Intrusion Detection
Approach for Process Networks

SIEMENS
Ingenuity for life

IED = sensor and reports

everything it doesn't know („Whitelisting“)

- unknown messages, IP-address, etc. defined in parameters

As well as other „anomalies“

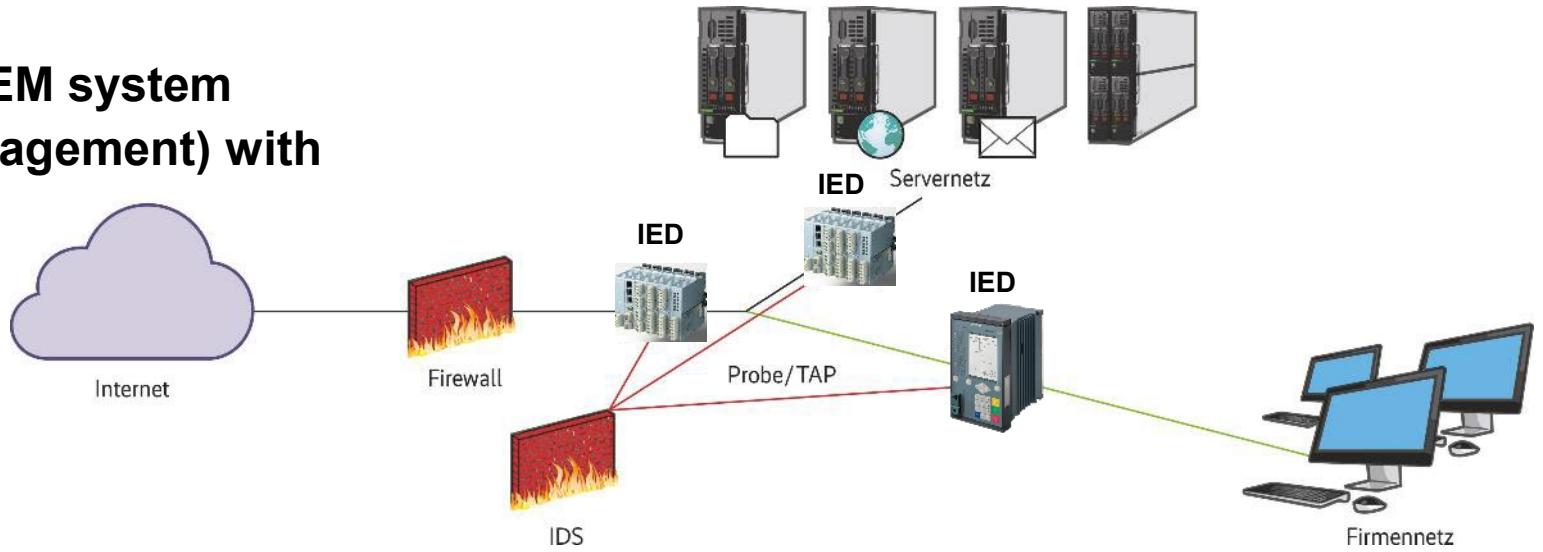
- Remote Access, Ping, new MAC-address, high data load, …

Many sensor functions implemented already

- Integrated syslog with A8000, SIPROTEC 5

Already practical experience with SIEM system (Security Information and Event Management) with

- projects
- internal technical OT network

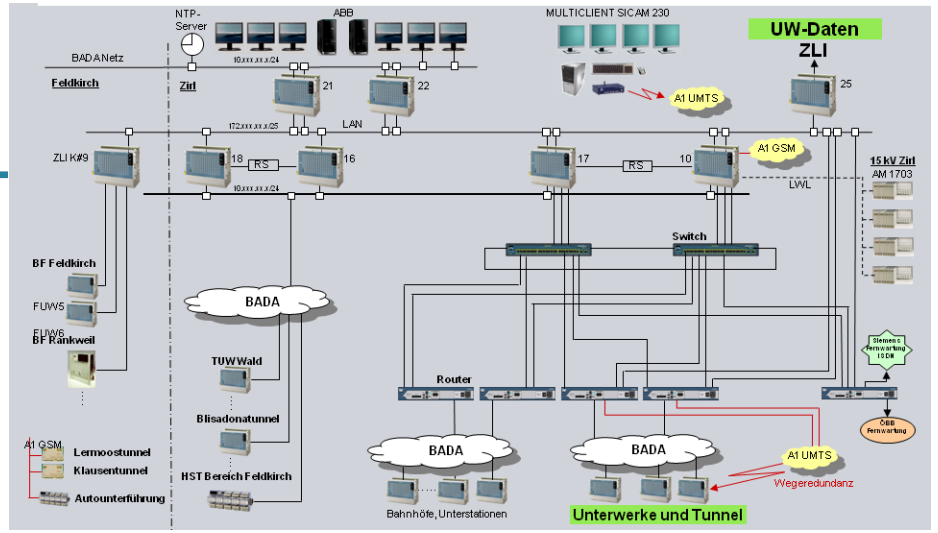


Security – Topics
Patch management

Products
- Security for control centers
- Security for embedded systems
- Security for engineering tools

System - Security4projects
- Network segmentation
- Data transmission via unsecured networks
- Back up / Restore
- Patch management
- Integration / upgrade of existing systems

Human
- Security Know How
- Security Maintenance



SIEMENS

Implementation of Security Requirements by Defined Process

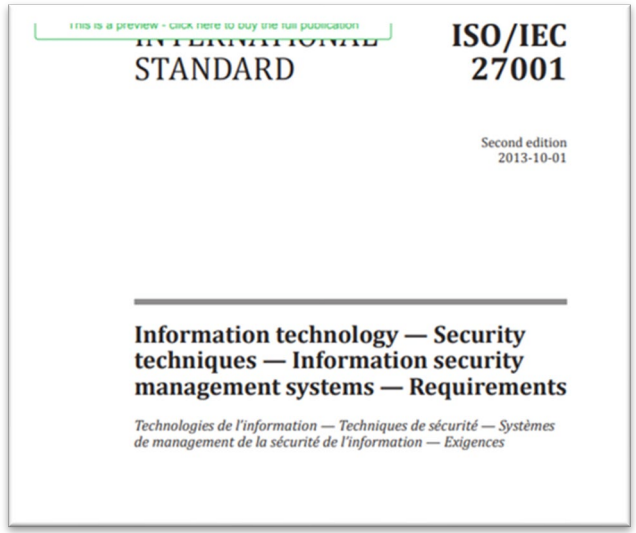
1. Technical assessment of existing system

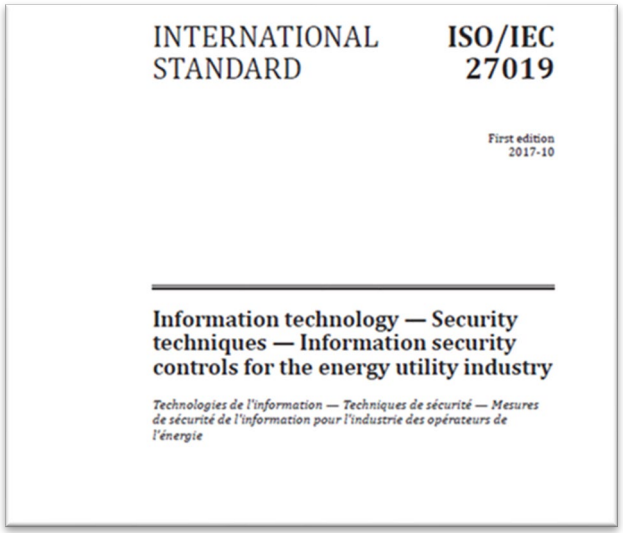
2. Assessment of technical risks in existing system

- Based on ISO 27001

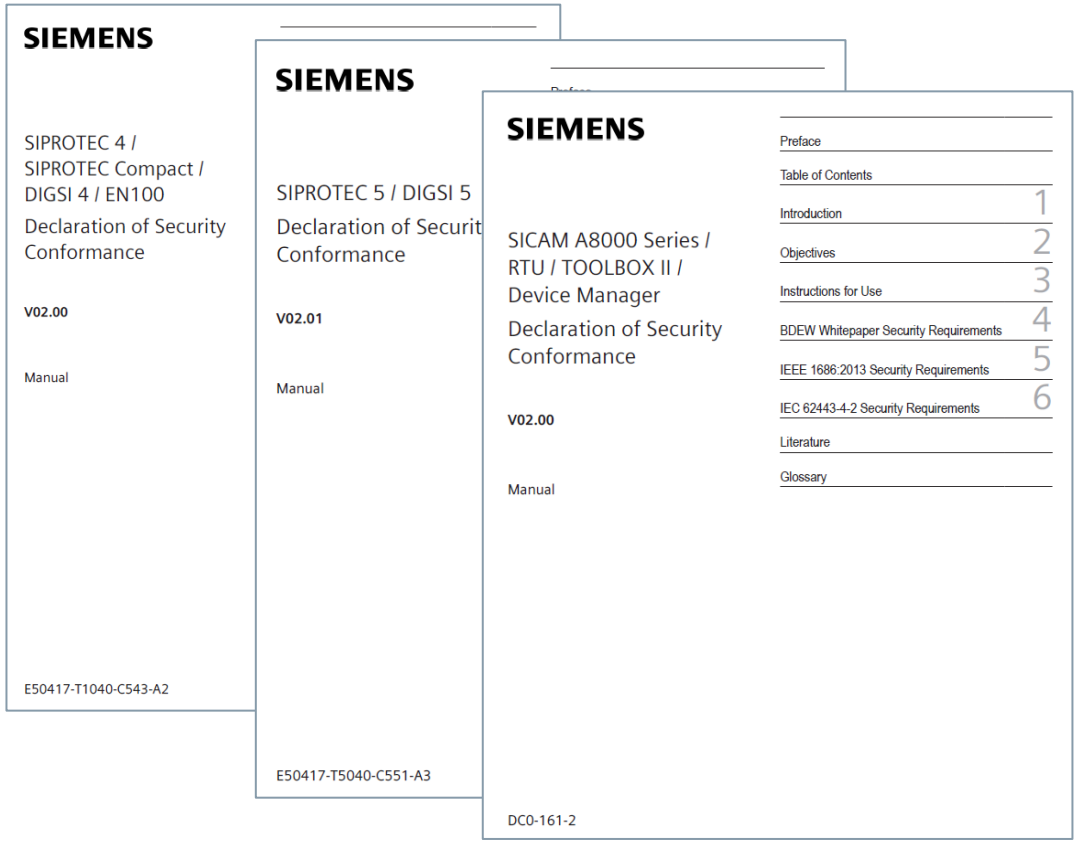
3. Definition of measures for the security enhancement

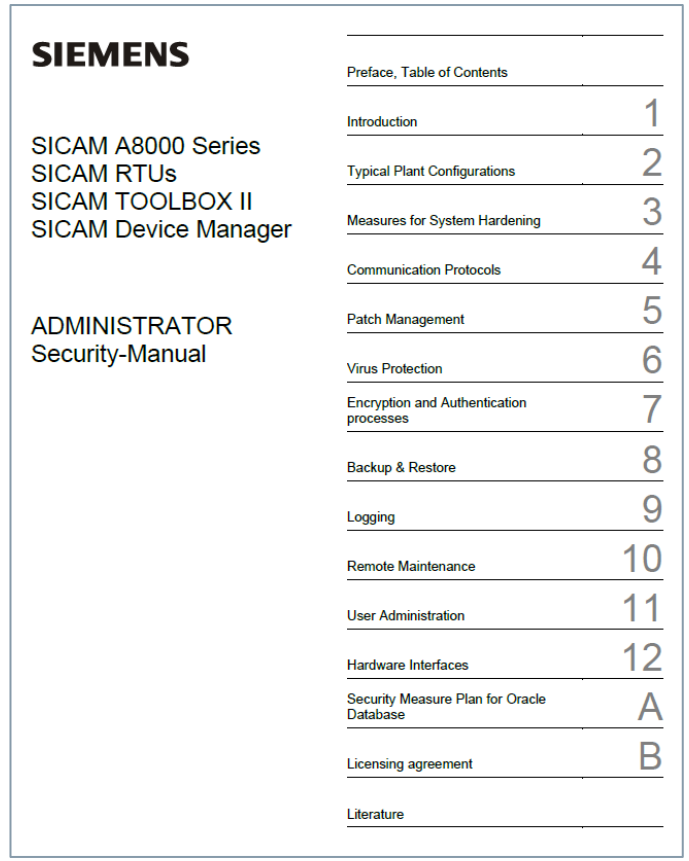
- Based on BDEW Whitepaper and ISO 27001/ ISO 27019





Implementation of Security Requirements by Defined Process





Product security conformance/ functions according to bdew/OE Whitepaper requirements

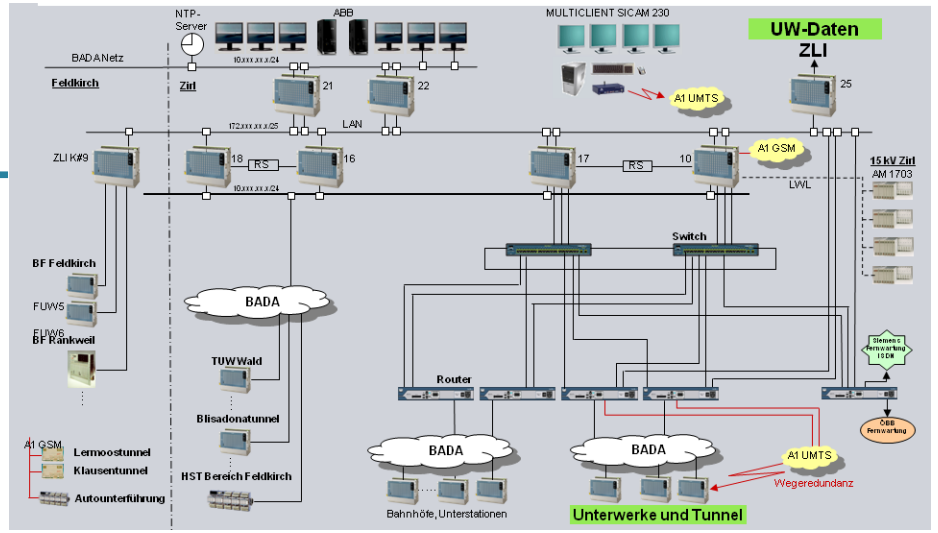
Guidelines, blueprints, examples

SIEMENS

Security – Topics
Data transmission via unsecured networks

Products
- Security for control centers
- Security for embedded systems
- Security for engineering tools

System - Security4projects
- Network segmentation
- Data transmission via unsecured networks
- Back up / Restore
- Patch management
- Integration / upgrade of existing systems



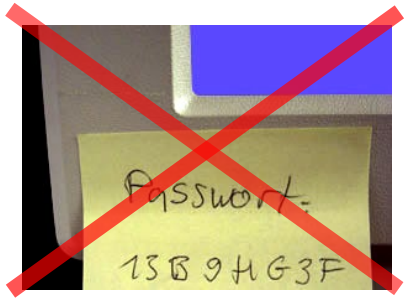
Human
- Security Know How
- Security Maintenance

SIEMENS

Human – Security Know How

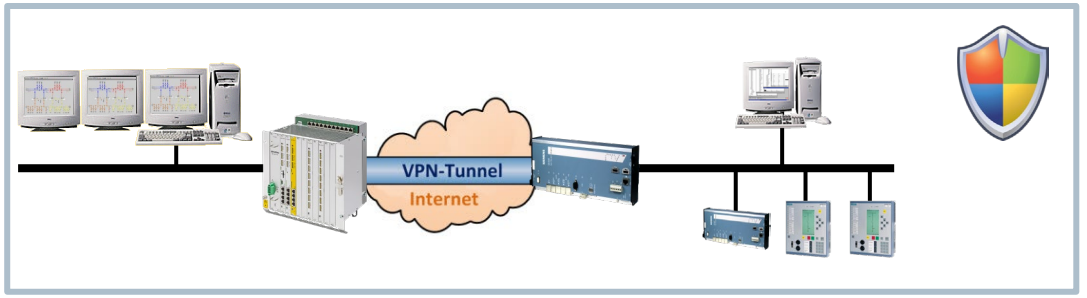
OT Security Basics

- Organizational and technical measures have to be defined and implemented
- Transfer/ training of security know how
- Available applications, technologies, …
- Awareness of staff …



OT Security in projects

- Has to be considered from the beginning
- Has to be tested
- Has to be maintained



Trainings offered by

Contact

Published by Siemens AG

Walter Wutzl
Head of Technical Sales Secondary

Franziska Diestel
Head of Software & Digitalization

Siemensstrasse 90
1210 Wien
Austria

E-mail walter.wutzl@siemens.com

SIEMENS