RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SPO2-T11

What Is the Right Approach for Critical Infrastructure Protection?

MODERATOR: **Prof. Dr. Norbert Pohlmann**

Director of the Institute for Internet Security – if(is) at the Westphalian University of Applied Sciences Gelsenkirchen, Germany *and* Chairman of the board of the IT Security Association TeleTrusT

PANELISTS:

Ammar Alkassar
CEO, Rohde & Schwarz Cybersecurity

Markus Bartsch
Business Development, TÜViT

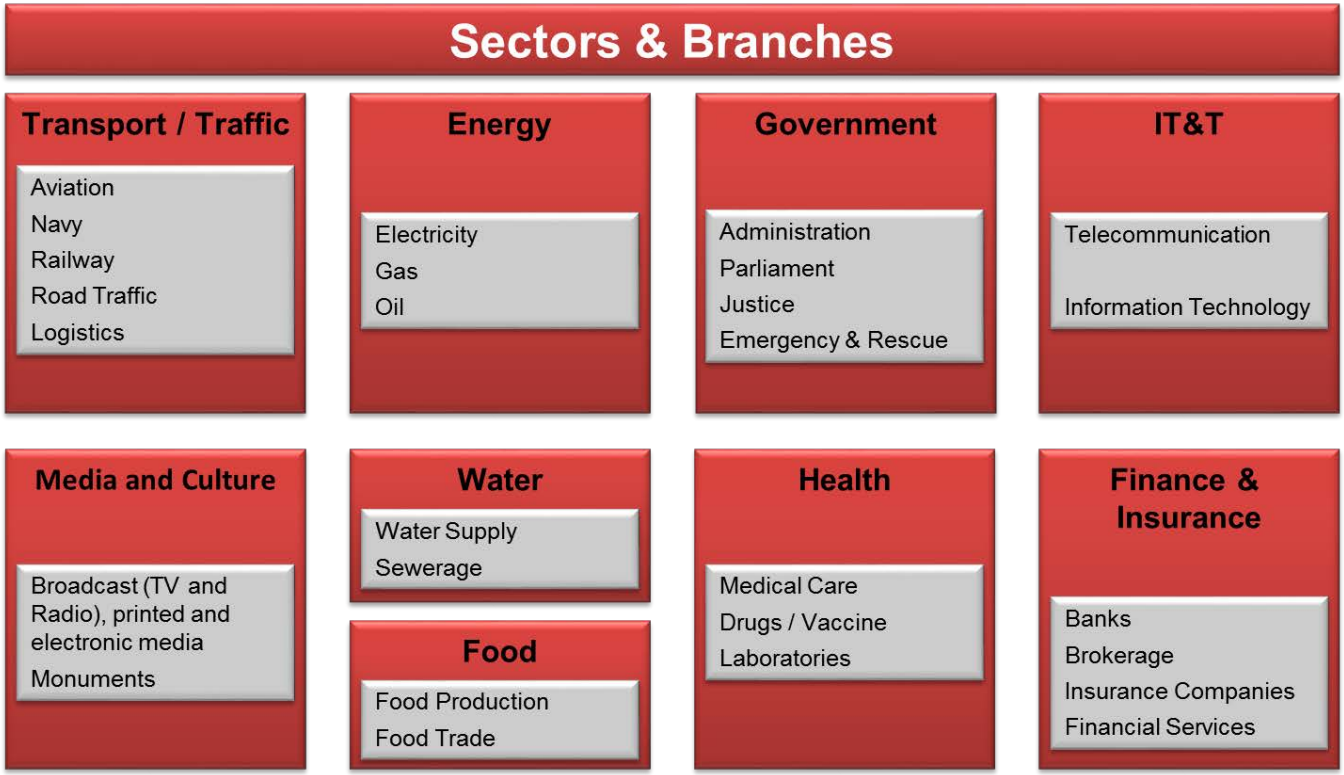
Dr. Thomas Störtkuhl
Team leader Industrial IT Security, TÜV SÜD Rail GmbH

#RSAC

Topics of The Panel Discussion

- Critical Infrastructures: Definition, Safety and Security Standards,
  Goals of Protection
- The Right IT Security Level for Critical Infrastructures
  Concepts and methods with respect to appropriate
  IT security functions
- The effectiveness, quality, manageability of IT security solutions
  A generally Road-Map

Critical Infrastructures



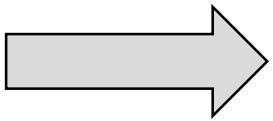
The General Security Problems of CI

- Recent development of ICS from island networks to highly networked infrastructures with high integration of suppliers
- More and more standardized products are used
- High sophisticated attacks: organized crime and political activism; rapid changes in technologies and strong increase in know-how
- lack of experiences with security
- IT security solution from office/business IT often cannot directly be transferred to ICS

Many possible attack vectors, large attack surface!

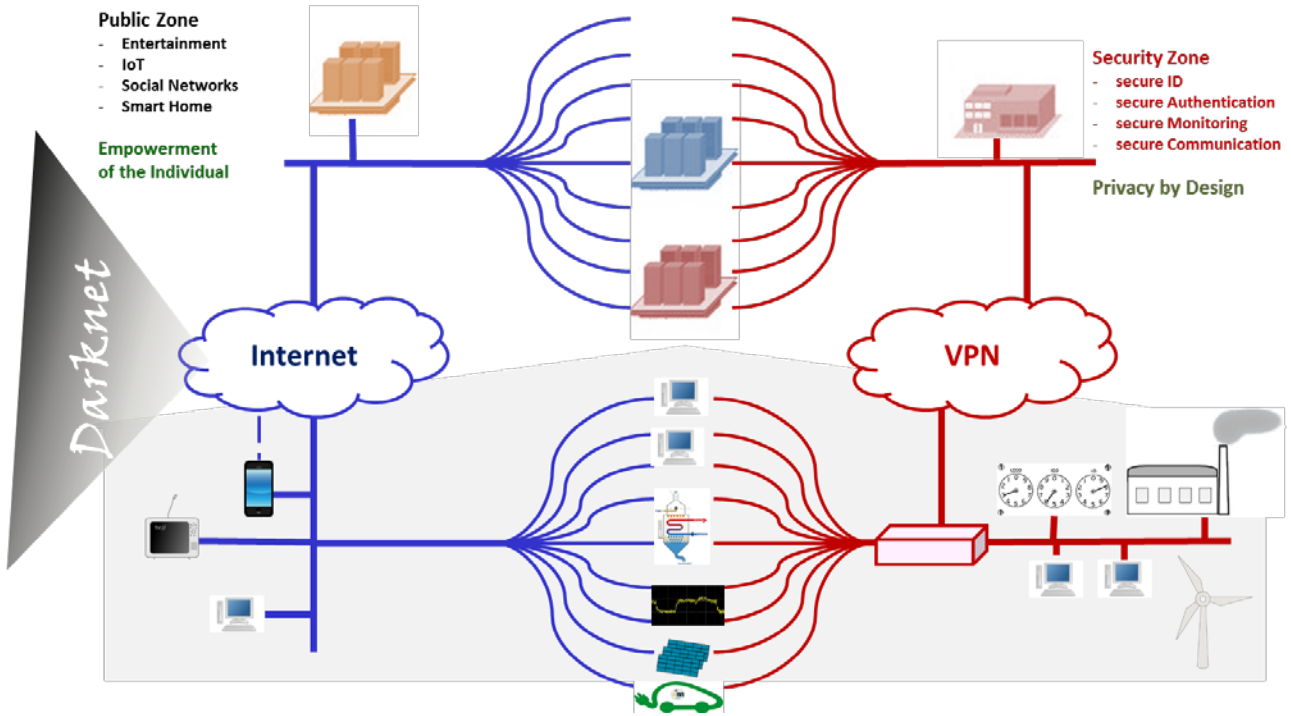
Security issues special to CI

- Legacy paradigm in CI networking infrastructure: for decades existence of disconnection
- Outdated components (e.g., OS, stacks etc.), outdated architectures
- Different life-time cycles (e.g. patch-management)
- ….



Heaven for (even old-fashion) attackers!

The Model: A Generic Security Zone



How important is Security Management in the field of Critical Infrastructure?

Sustainable, effective and efficient security is only possible with

- Holistic view
- Considering the triangle People, Process and Technology
- Control over processes and procedures
- Document management
- Risk analysis and management
- Continuous improvement

Establish an Information Security Management System!

TeleTrusT
Pioneers in IT security.

Classification in Protection Classes

Class 0 — Consumer

Share (# of devices out of all)

- Threat: privacy of personal data, Cybercrime
  Expected costs: adds 5% to personal IT costs | products and vendors: achieve market trust

100%

Class 1 — Companies, authorities

- Threat: Cybercrime (higher degree of risk), compliance, **legal privacy protection**
- Expected costs: adds 10% to IT | products and vendors: certified for effectiveness

70%

Class 2 — Companies, authorities, infrastructure

- Threat: Cybercrime, targeted attacks on corporate values, **corporate espionage**
- Breach of security leads only to individual damage
- Expected costs: adds 20% to IT | products and vendors: certified by internationally approved bodies

27%

Class 3 — Companies, authorities, infrastructure

- Threat: Economic espionage (intelligence services) and cyber attacks, **cyberwar (sabotage)**
- Breach of security leads to collective damage
- Expected costs: adds 50% to IT | products and vendors: certified by nationally approved bodies

3%
+ cost of infrastructure

Class 4 — Classified (beyond Restricted)

- National Security, Protection requirements: according to classification regimes
- Expected costs: adds 400% to IT | products and vendors: approved and certified by national authorities

0,01%

Core Classes for Enterprises

Appropriate Mechanisms

MDM, VPN, Secure Messaging, Voice and Cloud, Container solution

\+ Secure Operating System, Mutli-factor authentication, Approved PKI, End2End Encrypted Voice, Messaging and Cloud, E-Mail encryption

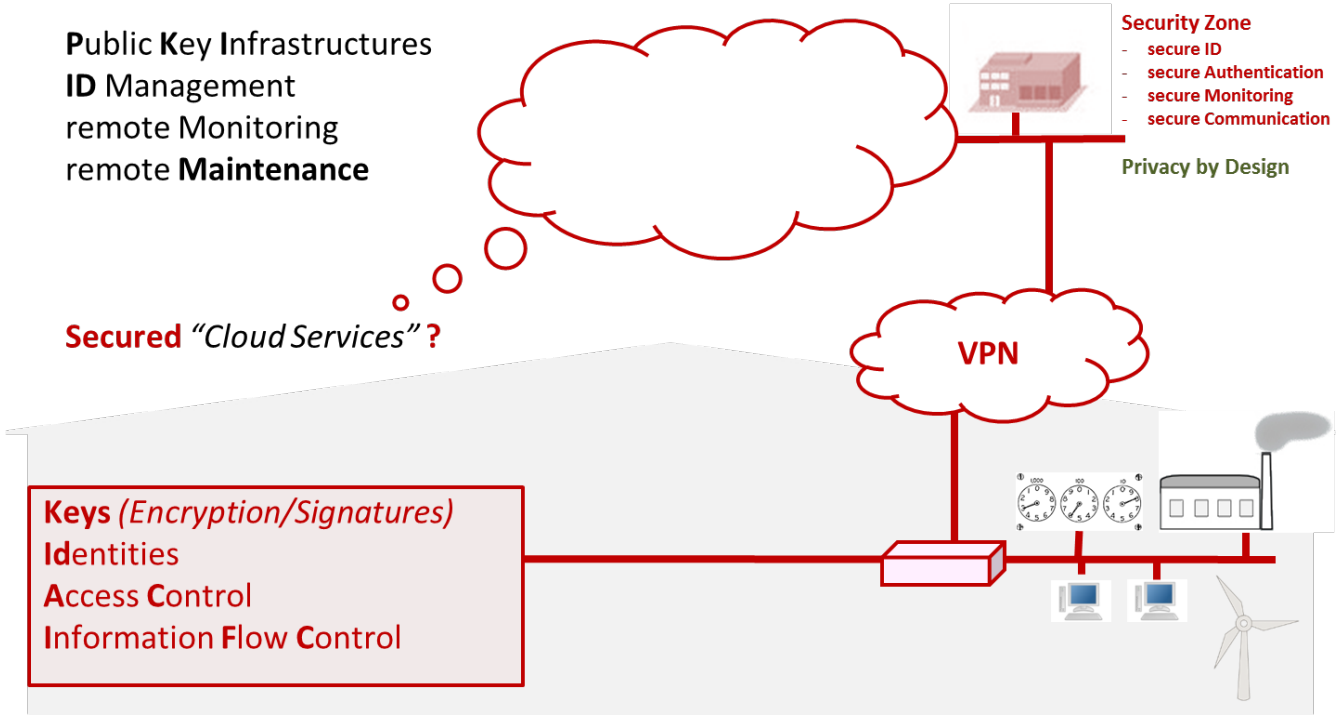
\+ Hardware-based 2-factor authentication (Smartcard, Token)

TeleTrusT
Pioneers in IT security.

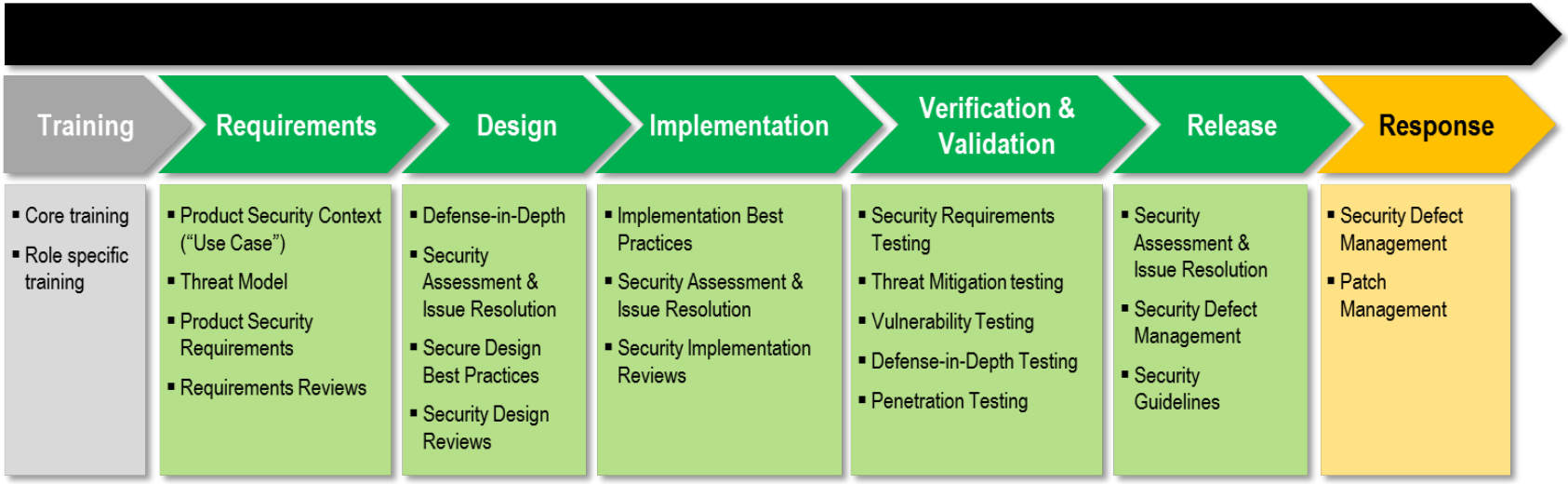
Use Centralized Management of decentralized IT Security Functionalities

Public **K**ey **I**nfrastructures
ID Management
remote Monitoring
remote **Maintenance**

Secured *"Cloud Services"* **?**



How can IT Security as a quality be integrated into solutions?



Security must be integrated in the processes!

or

Security is a process!

Case Study

Informatikzentrum Landesverwaltung Baden-Württemberg (IZLBW)

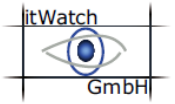
- State Police of Baden-Württemberg
- No. of locations/clients: 1,850/27,000
  narrow band local data access
- Critical Infrastructure: Secure client access to web
- Challenge: manage 24/7 - 99,999% availability

What You Have Learned Today

- At First: Analyze the security needs for the specific CI.
  Pay attention to the relationship between safety and security during the risk assessment!
- For the ICT solution of CI take standardized products and infrastructure components in account.
- For trustworthiness, consider evaluation results and relevant certificates for products and services.
- Organize a Security Management System and consider the triangle People, Process and Technology.

Visit the German Pavilion at North Expo Hall, Booth 4020

The partners of the German Pavilion at RSA® Conference 2016

TeleTrusT
Pioneers in IT security.