Panel Discussion

Security Gaps and Cyber Systems

Moderator
Rainer Falk, Steffen Fries, Siemens AG, Germany

Panelists
Maxime Puys, CEA-LETI, France
Stefan Schauer, Austrian Institute of Technology, Center of Digital Safety and Security, Vienna, Austria
Rainer Falk, Steffen Fries, Siemens AG, Germany

Security must be (continuously) adopted to the changing threat and vulnerability landscape

Changing threat landscape*

Burglary over the Internet

Human misconduct and sabotage

Unauthorized access

D-DOS Attacks

Attacks on standard components

Ransomware

Increased connectivity

Cloud Applications

Changing infrastructure and processes

IT standard components

Collaboration in the digital world

Big Data and Internet of Things

 *e.g. based on the German BSI Top10 Threats and Risk 2018

Starting points for discussion

Starting points for the panelists, examples for challenges:

- Security in cyber-physical systems. How good is existing best practice from different domains applicable?
- Secure system interaction – New approaches like zero trust lead to a new structure of system components and their communication and requires more security functionality at the resource side like fine grained access control and security monitoring
- Ensuring system resilience, independent of the reason of potential system failures (through intentional and unintentional changes)
- Simulation can contribute to system security and resilience also during operation to detect deviations from expected behavior specifically. How to connect simulation securely to the real world?
- How to establish trust in a more open environment, between the components and also along the component value chain?
- Which further challenges exist?

Panelists & Topics

Maxime Puys, CEA-LETI, France
- *Securing your Industrial Facility 101 – Challenges and Solutions*

Stefan Schauer, Austrian Institute of Technology, Center of Digital Safety and Security, Vienna, Austria
- *Tackling Large-Scale Effects of Cyber incidents*

Rainer Falk, Steffen Fries, Siemens, Germany
- *Cyber Security in Industrial Systems*

Panellist Summary

Securing your Industrial Facility 101 – Challenges and Solutions

Maxime Puys, CEA-LETI, FR/EU maxime.puys@cea.fr

- Differences between industrial systems and classical IT systems
- Industrial protocols
- Safety/Security convergence
- Hard real-time security
- Security solutions

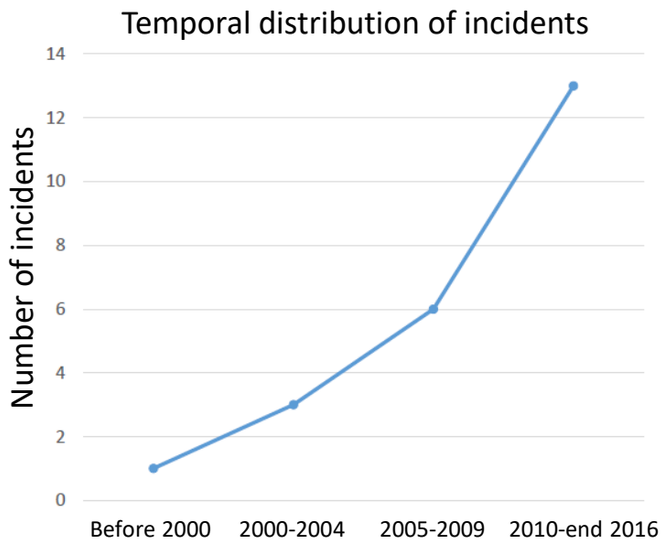
→ Industrial IoT are less protected that IT systems, yet can cause disasters

→ Securing industrial IoT result in various scientific and technical challenges (safety/security, real time, etc)

→ Existing and in-development security solutions for industrial IoT

Context

- Increasing number of cyberattacks against ICS
- Sabotage (Stuxnet, BlackEnergy, Industroyer, etc)
  - Political motivations, terrorism
- Information gathering (Duqu)
  - Industrial spy, later attacks
- Ransomware:
  - WanaCry, NotPetya, etc (not ICS specific)



[Figure 1] Fiches Incidents Cyber SI Industriels, CLUSIF –Groupe de Travail SCADA, 2017
[Figure 2] Common Cybersecurity Vulnerabilities in Industrial Control Systems; Homeland Security, 2011

Differences with IT Systems

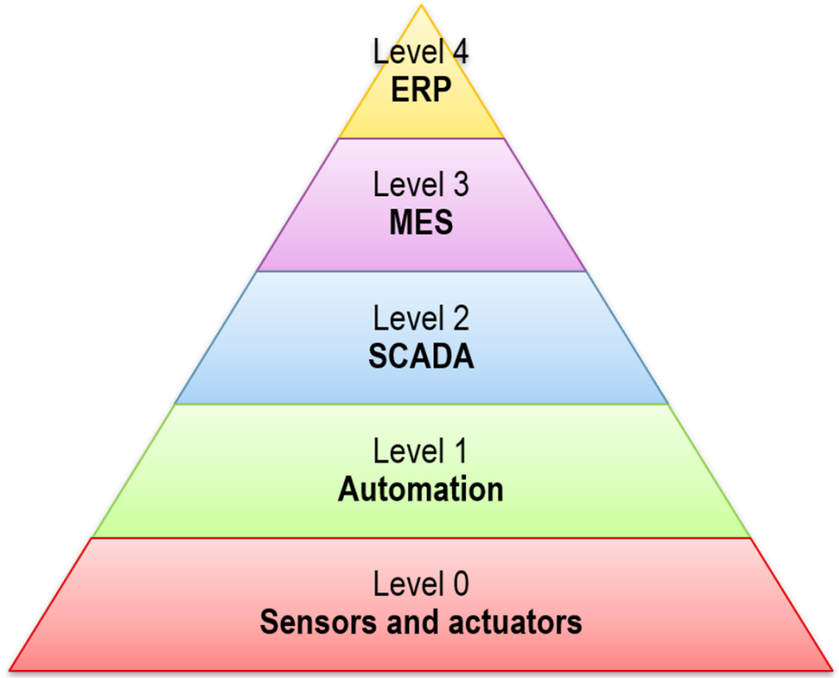
- Historically isolated from networks:
  ➔Secure by design.

- Properties to be ensured:
  - Mainly availability (time is money!), very low importance of confidentiality
  - Safety vs. Security

- Real time:
  - Include non TCP/IP networks
  - Hard time constraints for low level protocols (< 10ms)

Topology and Protocols

- Mostly proprietary to vendors
- Mostly unsecure
  - Cryptography only begins to appear

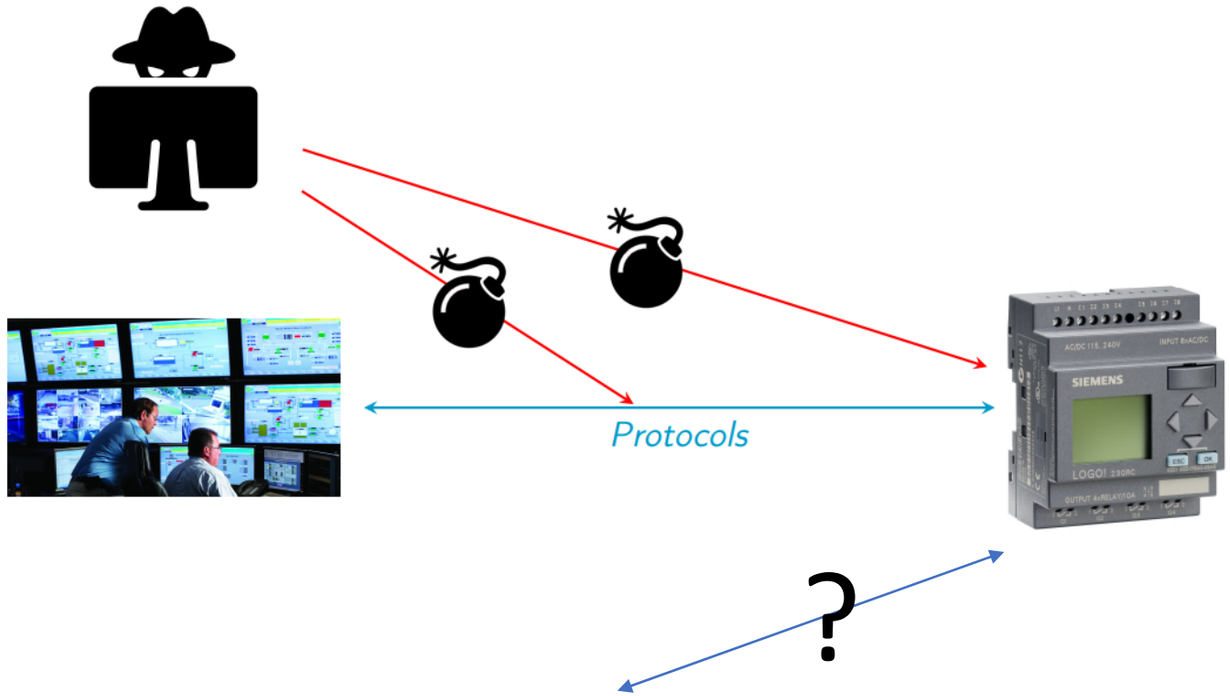


		Protocol Data Unit (PDU)			
Start	Slave ID	Function code	Data	CRC error check	Stop
3.5 Bytes	1 Byte	1 Byte	n Bytes	2 Bytes	3.5 Bytes
	Application Data Unit (ADU)				

Modbus RTU Frame

Safety vs. Security

- Safety ➔ Functionnal protection against disasters, mistakes
  - No attacker
- Security ➔ Protection of IT against attackers
  - No functionnal properties
- Combining both is a real challenge:
  - Interdependancies, combinatorial explosion, etc



Solutions

- Diodes, gateways, industrial VPN, etc
  - Ensure network protection against threats (some handle realtime)
- Testbeds, numerical twins, honeypots
  - Allow to test attacks, find vulnerabilities, discover attacker behaviors
- Formal methods dealing with safety and security
  - Cybersecurity of industrial protocols (should be systematic!)
  - Full safety analysis in presence of attacker (still need improvements)

Panellist Position

“Small cause, large effect – cyber incidents can shut down entire industries”

Tackling large-scale effects of cyber incidents

Stefan Schauer, AIT Austrian Institute of Technology, Austria Stefan.Schauer@ait.ac.at

- Big organizations have developed into complex cyber-physical ecosystems
- Integration of SCADA and ICS systems is required to be efficient
- New threats arise from interconnecting systems
- Cyber threats have affected large industries in the past (WannaCry, NotPetya, etc.)
- If cyber-physical systems are shut down, the company remains inoperable

→ Comprehensive overview on complex cyber-physical systems is required

→ Physical and cyber domain need to be correlated

→ Hybrid Situational Awareness can support security operators

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

TACKLING LARGE-SCALE EFFECTS OF CYBER INCIDENTS

Panel on Security Gaps and Cyber Systems

NetWare Conference, 20. – 26.11.2020

Stefan Schauer

Stefan.Schauer@ait.ac.at

CYBER-PHYSICAL SYSTEMS

- Industry companies and critical infrastructures have evolved into complex ecosystems operating numerous cyber-physical systems
  - Application of Supervisory Control and Data Acquisition (SCADA)
  - Industrial Control Systems (ICS)
  - Distributed Control Systems (DCS)

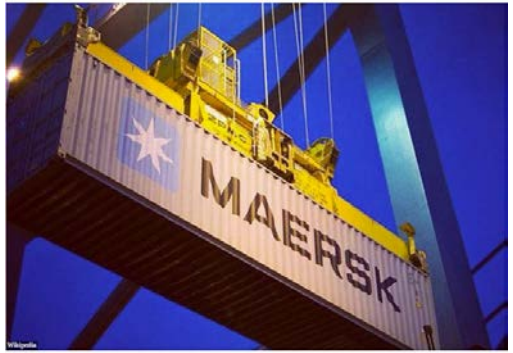
- With the increasing digitalization new threats have arisen with potentially high impact on the entire infrastructure
  - Malware and ransomware attacks
  - Advanced Persistent Threats (APTs)
  - Distributed Denial of Service (DDoS) attacks

LARGE-SCALE INCIDENTS

NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million

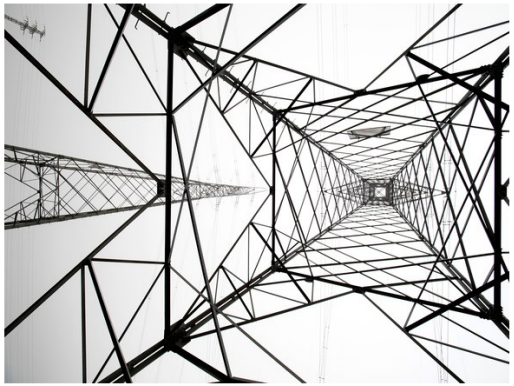
Lee Mathews Contributor
Aug 16, 2017, 11:47am • 7,624 views • #CyberSecurity

In June, the NotPetya ransomware hit companies in the U.S. and throughout Europe. One of those hardest hit was Copenhagen-based shipping giant A.P. Moller-Maersk, which moves about one-fifth of the world's freight. Operations at Maersk terminals in four different countries were impacted, causing delays and disruption that lasted weeks.



KIM ZETTER SECURITY 03.03.16 07:00 AM

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid



Home › Cyberwarfare

DDoS Attacks More Likely to Hit Critical Infrastructure Than APTs: Europol

By Eduard Kovacs on September 27, 2017

Share Tweet Empfehlen 24 RSS

While critical infrastructure has been targeted by sophisticated threat actors, attacks that rely on commonly available and easy-to-use tools are more likely to occur, said Europol in its 2017 Internet Organised Crime Threat Assessment (IOCTA).

The report covers a wide range of topics, including cyber-dependent crime, online child exploitation, payment fraud, criminal markets, the convergence of cyber and terrorism, cross-cutting crime factors, and the geographical distribution of cybercrime. According to the police agency, we're seeing a **"global epidemic" in ransomware attacks.**

When it comes to **critical infrastructure attacks**, Europol pointed out that the focus is often on the worst case scenario - sophisticated state-sponsored actors targeting supervisory control and data acquisition (SCADA) and other industrial control systems (ICS) in power plants and heavy industry organizations.

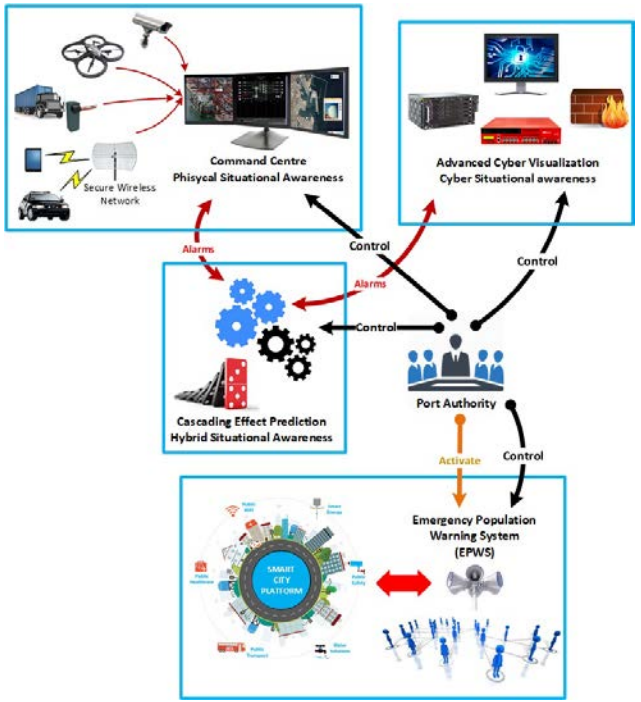
However, these are not the most likely and most common types of attacks - at least not from a law enforcement perspective as they are more likely to be considered threats to national security. More likely attacks, based on reports received by law enforcement agencies in Europe, are ones that don't require attackers to breach isolated networks, such as distributed denial-of-service (DDoS) attacks, which often rely on easy-to-use and widely available tools known as booters or stressers.

While these types of attacks may not lead to a shutdown of the power grid, they can still cause serious disruptions to important utilities and services.

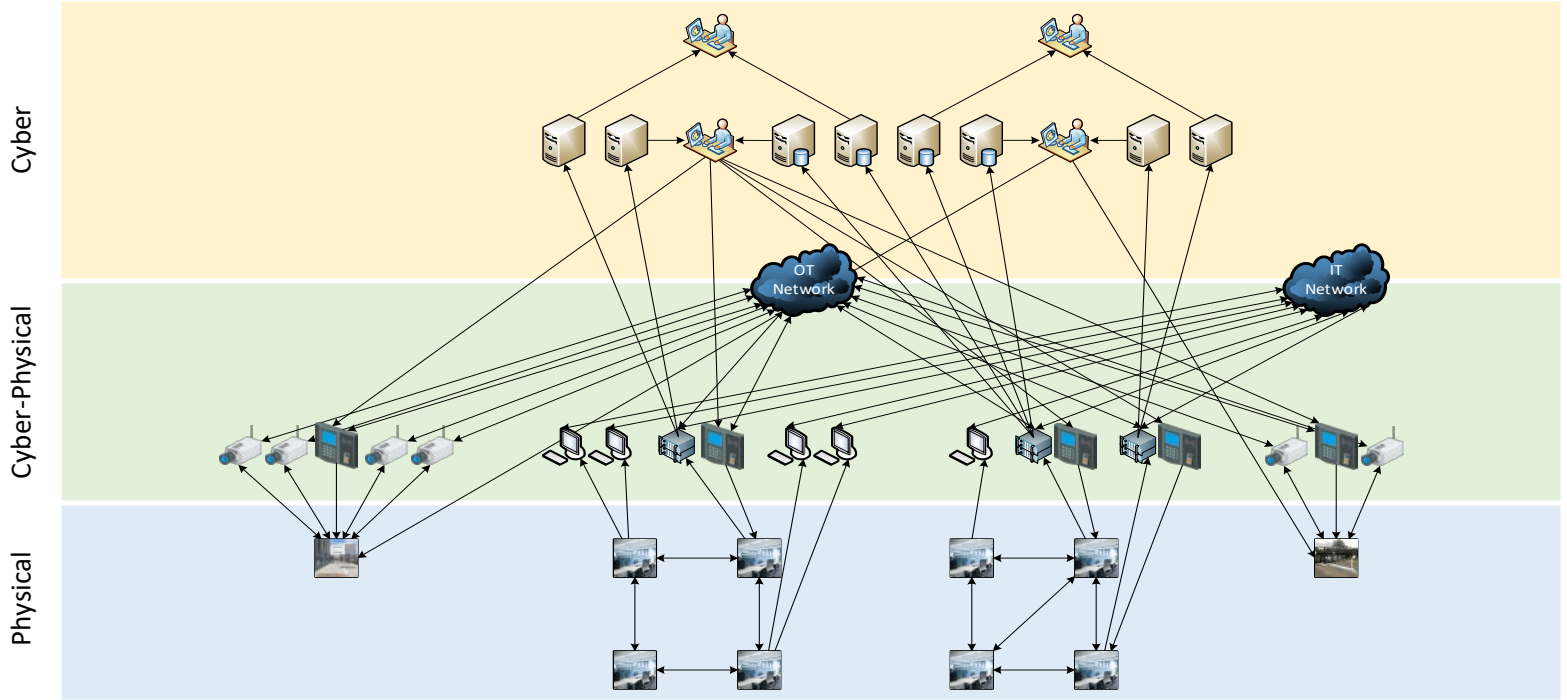
HYBRID SITUATIONAL AWARENESS

- Obtaining a comprehensive situational awareness on the physical and cyber parts of an infrastructure has become crucial for security operators

- Hybrid Situational Awareness provides such a holistic view
  - Takes interdependencies between physical and cyber assets into account
  - Identifies potentially malicious events by combining information from both domains
  - Allows to extrapolate potential cascading effects

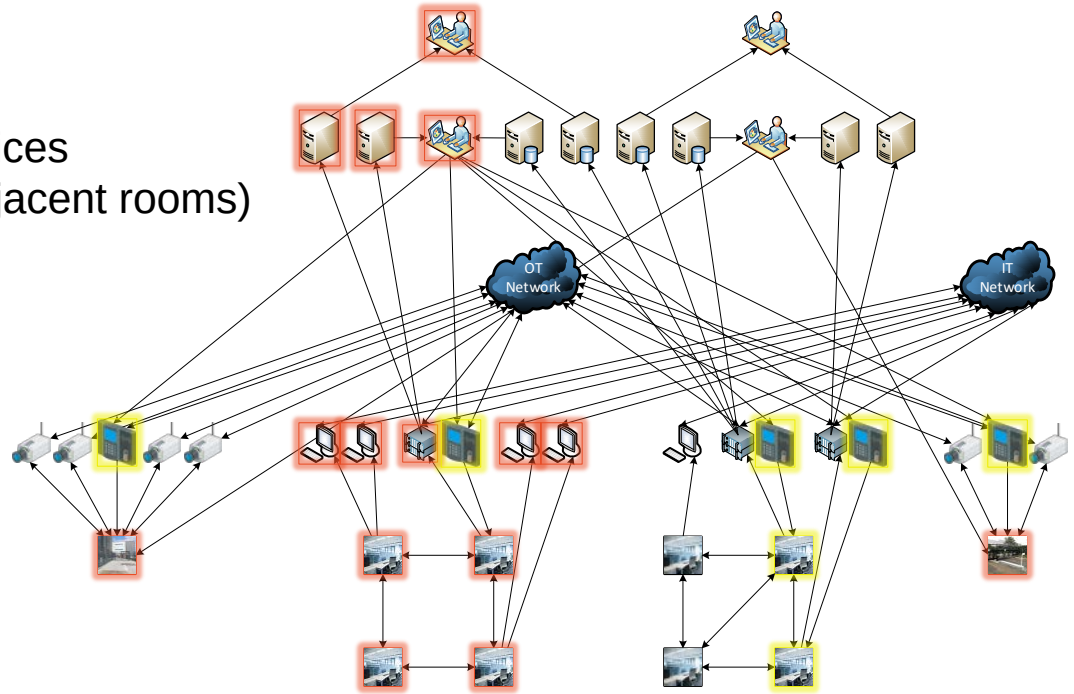


CYBER-PHYSICAL SYSTEM



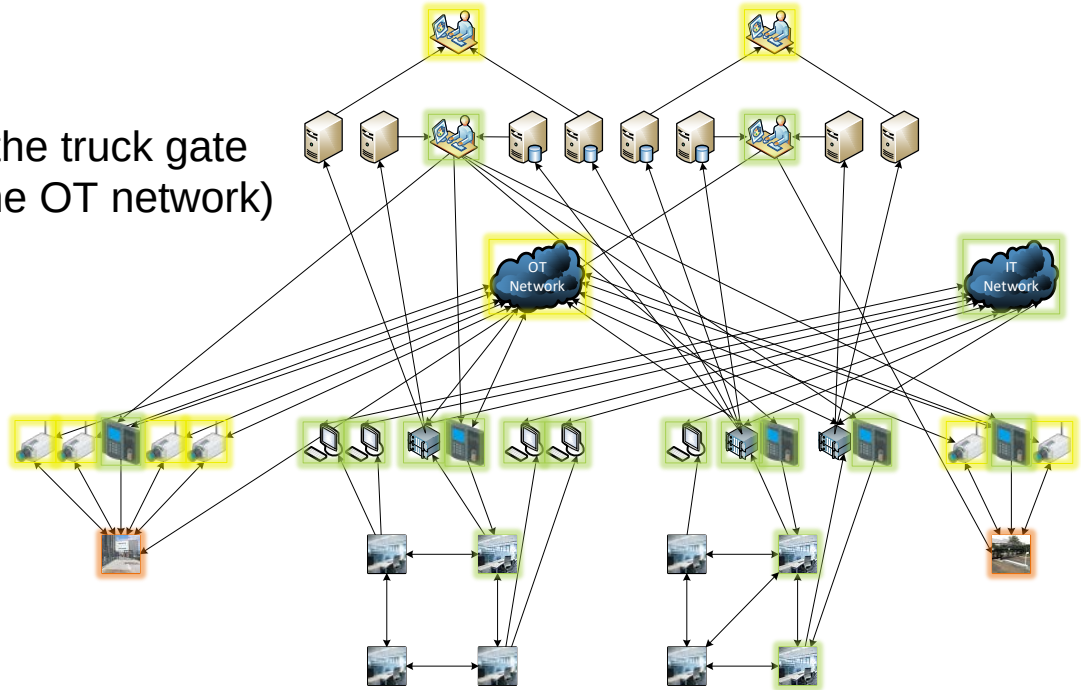
INCIDENT SCENARIO

- **Physical Incident**
  - Fire in room B1-1
    Building 1 hosts several offices
    (no special protection in adjacent rooms)



INCIDENT SCENARIO

- **Cyber Incident**
  - Camera “Cam F” is hacked
    observes the entrance via the truck gate
    (no special protection for the OT network)



CONCLUSIONS

- Hybrid Situational Awareness provides a concise view on complex organizations
  - Assets in both the physical and cyber domain are modeled
  - Available information is correlated
  - Cascading effects are simulated across different domains

- Specification of cyber-physical interdependencies can be a laborious task
  - Dependencies among assets might not always be directly visible
  - Probabilities need to be specified for each interdependency
  - Formal approach to make the description more efficient

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THANK YOU!

Dr. Stefan Schauer

Stefan.Schauer@ait.ac.at

Austrian Institute of Technology
Lakeside B10a
9020 Klagenfurt, Austria

Panelist Summary

Cyber Security for Industrial Systems

- Industrial systems need a security design that address the relevant security objectives and respect side conditions for the specific environment (e.g., lifetime, real-time, safety, usability).
- The industrial security standard IEC62443 is applied in different verticals. The responsibilities of the different roles (system operator, integrator, component manufacturer) are distinguished.
- System integrity monitoring of control systems and technical processes can provide an additional layer of defense.

Dr. Rainer Falk
Principal Key Expert
Siemens Technology

Steffen Fries
Principal Key Expert
Siemens Technology

SIEMENS

Cyber Security for Industrial Systems

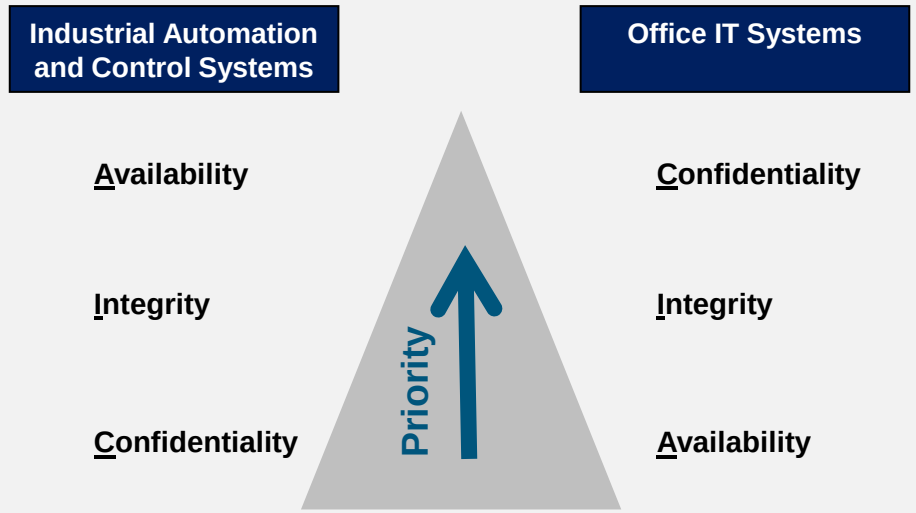
Dr. Rainer Falk, Steffen Fries

SIEMENS

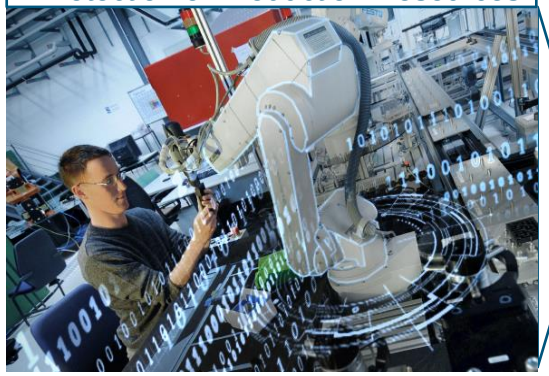
Industrial systems require a specific approach to cybersecurity.

Applying security guidelines (and defined requirements, specific measures) suitable for enterprise IT directly to industrial systems does not work. A security design has to address the relevant security objectives and respect side conditions for the specific environment.

CIA Pyramid Turned Upside Down



Industrial Systems :
Protection of Production Resources



Lifetime up to 20 years and more

Office IT :
Protection of IT-Infrastructure

Lifetime 3-5 years

SIEMENS

Critical infrastructures are addressed through standards and regulative requirements (examples, global view)

SIEMENS
Ingenuity for life

- IEC 62351 – Power systems management and associated information exchange – Data and communications security
- IEC 62443 – Security for industrial automation and control systems
- ISO/IEC 15118 – Road vehicles -- Vehicle to grid communication interface

- ISO/IEC 27001 – Information technology - Security techniques - Requirements
- ISO/IEC 27002 – Code of Practice for information security management
- ISO/IEC 27019 –Information security controls for the energy utility industry

- IEEE 1588 – Precision Clock Synchronization
- IEEE 1686 – Intelligent Electronic Devices Cyber Security Capabilities

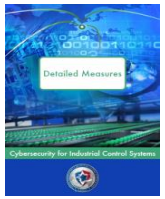
- RFC 4301 – Security Architecture for the Internet Protocol
- RFC 5246 – Transport Layer Security TLS v1.2
- RFC 8446 – Transport Layer Security TLS v1.3

- Critical Infrastructure Protection CIP 001-014
- Executive Order EO 13636 improving Critical Infrastructure Cyber Security
- IoT Cybersecurity Improvement Act 2017

- IT Security Act
- B3S Standards
- BNetzA Security Catalogue
- German Energy Act

- Network Information Security Directive

- Critical Infrastructure Protection
- Certification and Key Measures



- Cyber Essential Scheme
- Direct adaptation of European NIS Directive and GDPR (General Data Protection Regulation

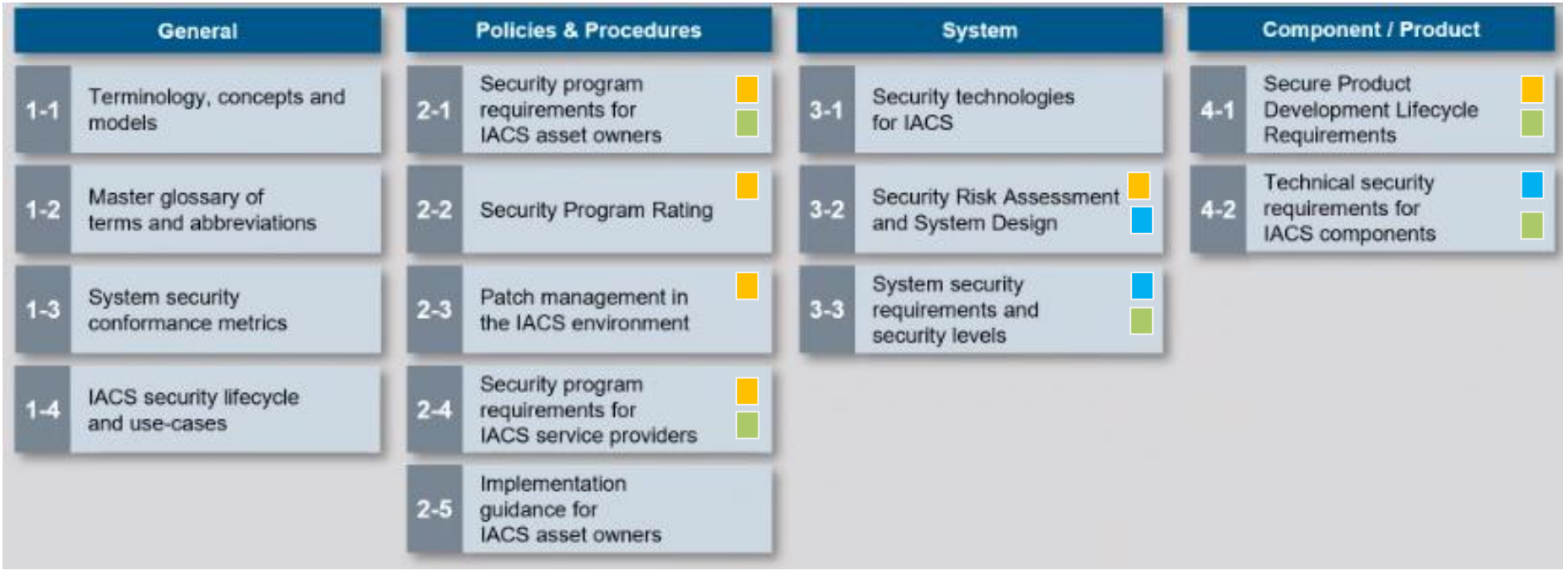
Note: the stated organizations and standards are just examples and are not complete

SIEMENS

IEC 62443 Security for Industrial Automation and Control Systems addresses the complete value chain from product to service

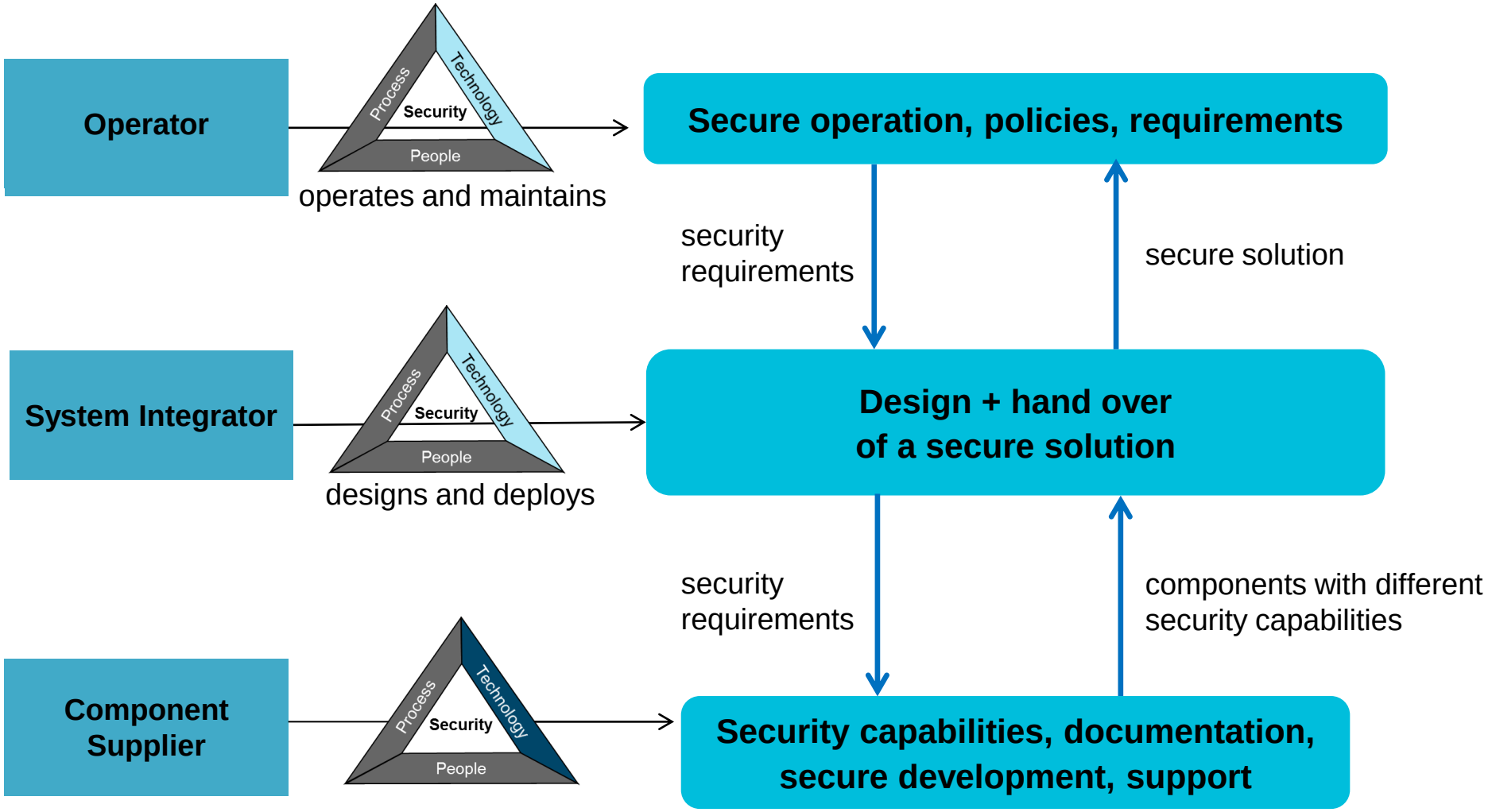
SIEMENS
Ingenuity for life

- Addresses
  - Operator
  - Integrator
  - Product Supplier
- in terms of
  - processes and
  - security capabilities
- and allows for
  - certification



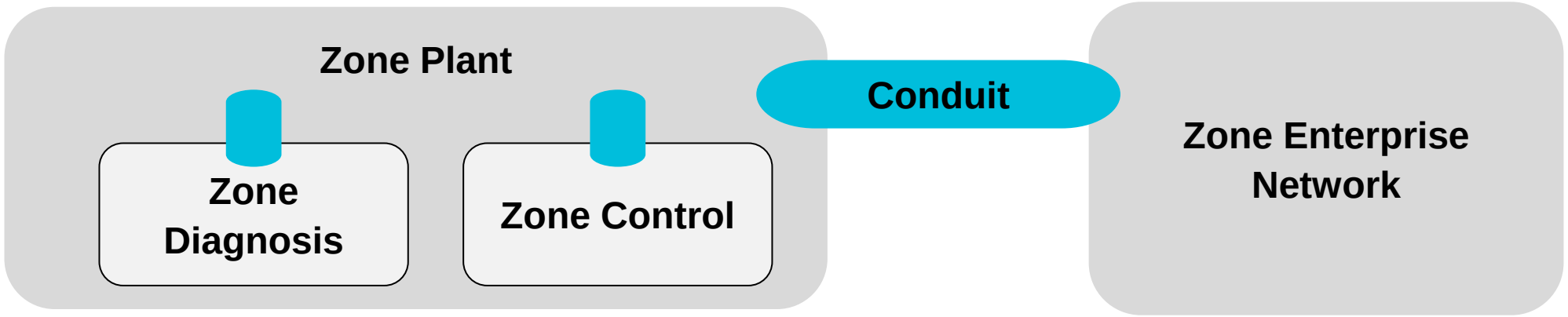
SIEMENS

The security standard IEC 62443 addresses security in a holistic way, suitable for an industrial environment including the responsible roles and products lifecycle



SIEMENS

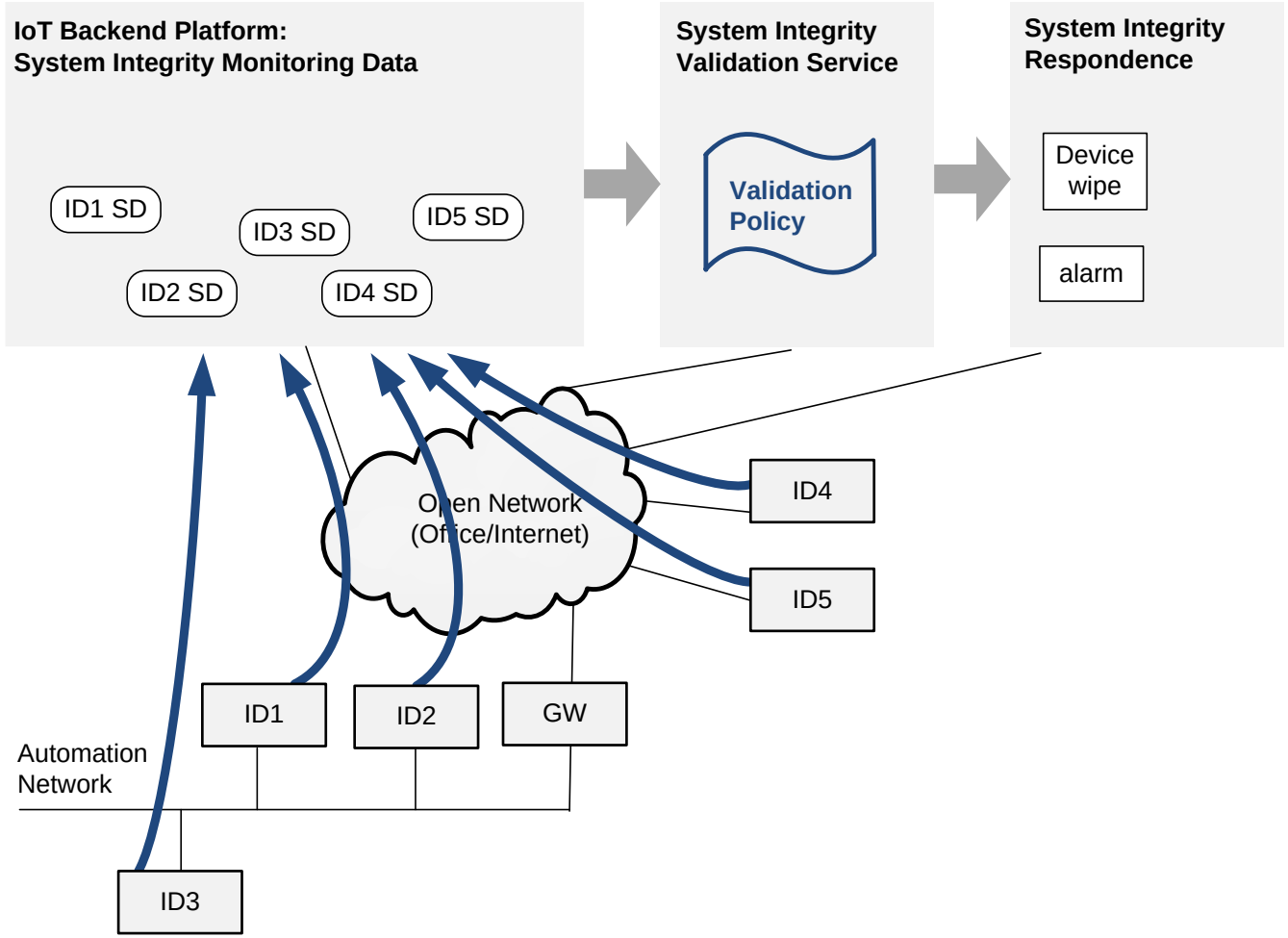
The security levels defined by IEC62443 provide for protection against different attack levels



SL1	Protection against casual or coincidental violation
SL2	Protection against intentional violation using simple means, low resources, generic skills, low motivation
SL3	Protection against intentional violation using sophisticated means, moderate resources, IACS specific skills, moderate motivation
SL4	Protection against intentional violation using sophisticated means, extended resources, IACS specific skills, high motivation

SIEMENS

Besides secure system design and development, system integrity monitoring realizes an additional layer of defense during operation



Integrated integrity monitoring of control systems and technical process:

- Device inventory
- Runtime device integrity measurements
- Network monitoring
- Physical automation process monitoring
- Power monitoring, …
- Physical world integrity (trusted sensors)

SIEMENS

Security has to be suitable for the addressed environment.

Awareness and Acceptance

Since security is not just a technical solution, which can be incorporated transparently, we need to consider how humans can get along with this issue.

This needs, especially for automation environments, actions for:

- awareness trainings
- help people to understand security measures and processes
- provide user-friendly interfaces and processes

SIEMENS