SIEMENS
Ingenuity for life

Tutorial: Industrial Security

IARIA CYBER, 22 Sep. 2019

Dr. Rainer Falk

Our industrial society confesses a growing demand for IT-Security

IT Security trends are determined by drivers such as

- Industry infrastructures changes (Digitalization)
- More networked embedded systems
- Increasing device-to-device communication
- Need to manage intellectual property

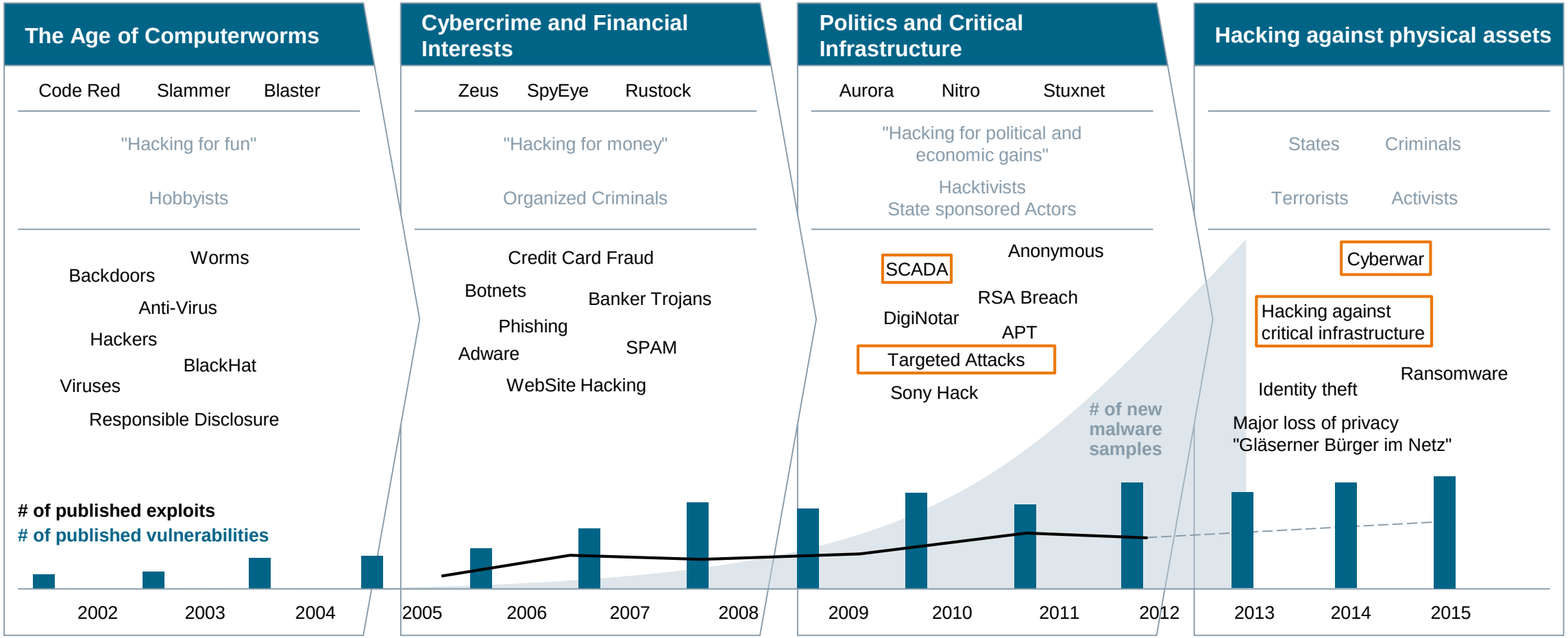
And

- Increasing international organized crime
- Privacy
- Compliance enforcement
- Cyber war fare
- Cloud/Virtualization
- PDAs, Smart Mobiles
- Social Networks / data mining concepts
- ….

The threat level is rising – Attackers are targeting critical infrastructures

SIEMENS
Ingenuity for life

Evolution of attacker motives, vulnerabilities and exploits



Cyber Security is the most important enabler for Digitalization

SIEMENS
Ingenuity for life

Design & Engineering | Automation & Operation | Maintenance & Utilization

Siemens Software

Siemens Digital Services

MindSphere

The cloud-based, open IoT operating system

Platform as a Service

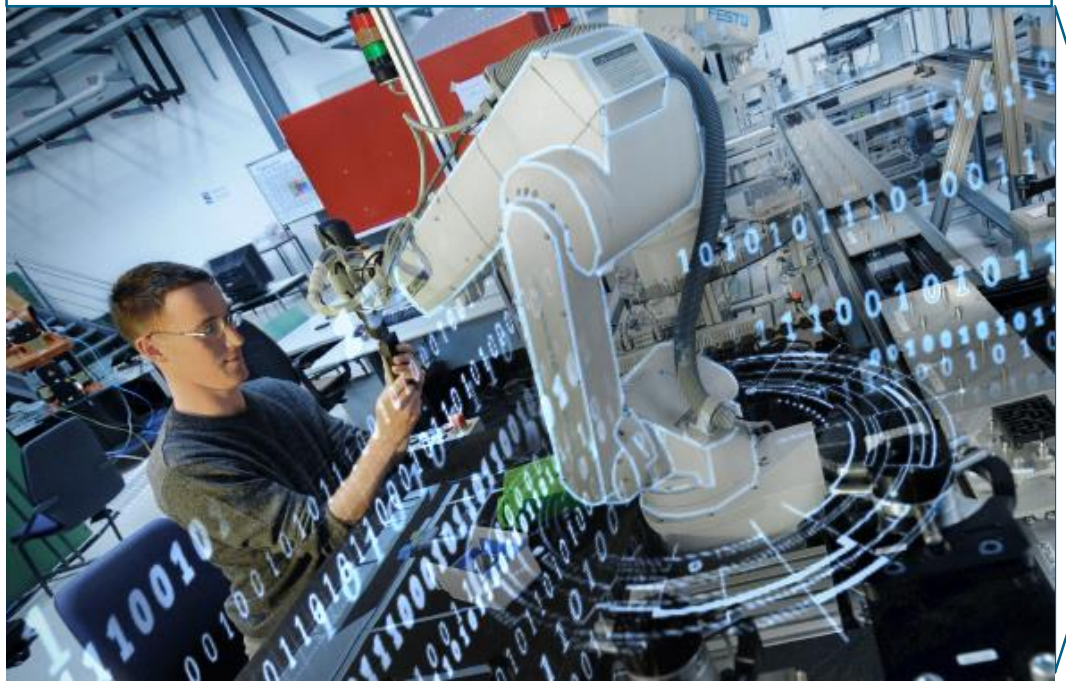
Enabler: Infrastructure as a Service (storage, processing power, provider agnostic)

Digitally enhanced Electrification and Automation

Holistic IT security concept

Office world versus industrial systems - Protection targets for security

Industrial Systems :
Protection of Production Resources



Lifetime up to 20 years and more

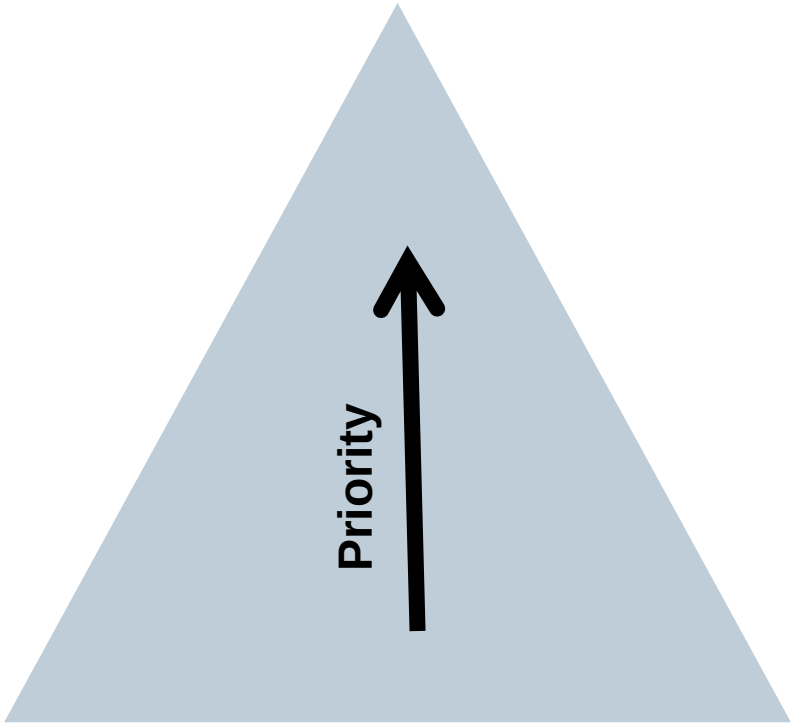
Office IT :
Protection of IT-Infrastructure

Lifetime 3-5 years

The CIA pyramid is turned upside down in industrial automation and control systems: “Protect Productivity”

SIEMENS
Ingenuity for life

Industrial Automation and Control Systems	Office IT Systems
Availability	**C**onfidentiality
Integrity	**I**ntegrity
Confidentiality	**A**vailability



Caught between regulation, requirements, and standards

Solution design and deployment plays an essential role in designing compliant solutions

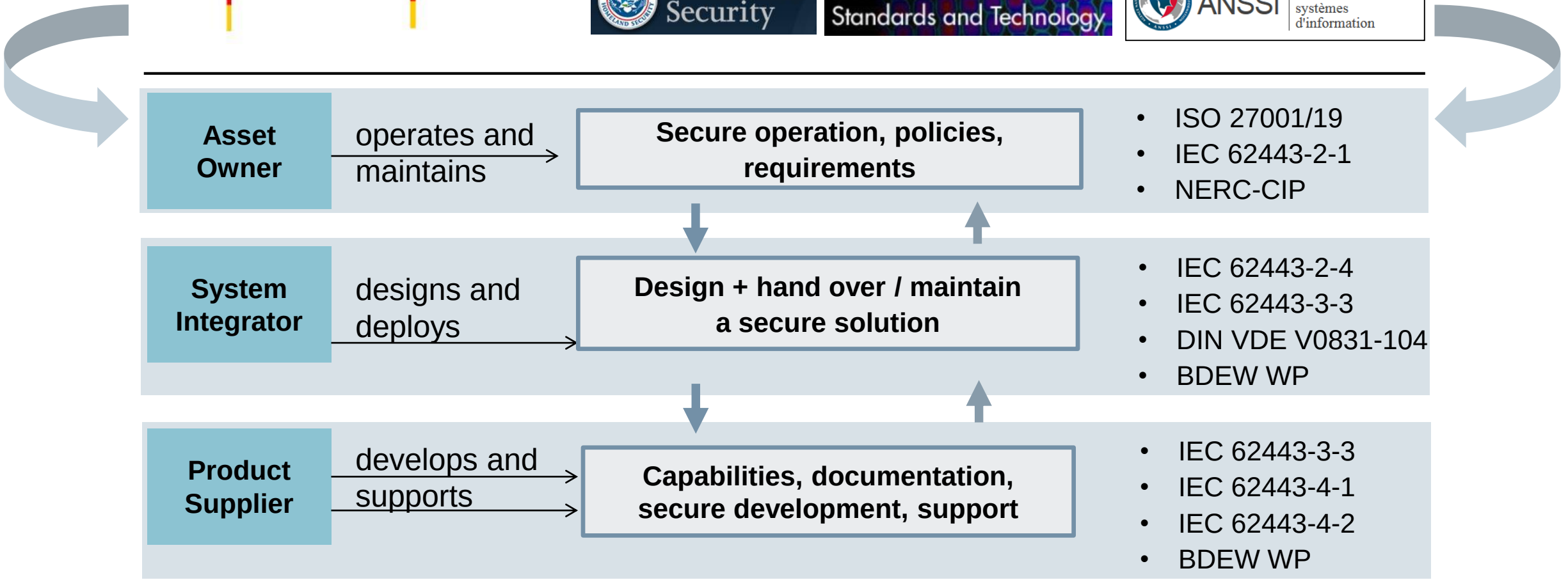
Bundesamt für Sicherheit in der Informationstechnik

Bundesnetzagentur

Homeland Security

National Institute of Standards and Technology

ANSSI Agence nationale de la sécurité des systèmes d'information



IEC 62443 Covers Security Management, System, and Component Level for Industrial Automation Control Systems (IACS)

SIEMENS
Ingenuity for life

IEC 62443 (ISA-99)

General

- 1-1 Terminology, concepts and models
- 1-2 Master glossary of terms and abbreviations
- 1-3 System security compliance metrics
- 1-5 IACS Protection Levels

Definitions

Metrics

Policies and procedures

- 2-1 Establishing an IACS security program
- 2-2 Operating an IACS security program
- 2-3 Patch management in the IACS environment
- 2-4 Certification of IACS supplier security policies

Requirements to the security organization and processes of the plant owner and suppliers

System

- 3-1 Security technologies for IACS
- 3-2 Security assurance levels for zones and conduits
- 3-3 System security requirements and security assurance levels

Requirements to a secure system

Component

- 4-1 Product development requirements
- 4-2 Technical security requirements for IACS products

Requirements to secure system components

IEC 62443 addresses all stakeholders for a holistic protection concept

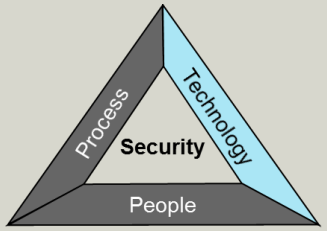
SIEMENS
Ingenuity for life

On site / site specific

Asset Owner

Service Provider

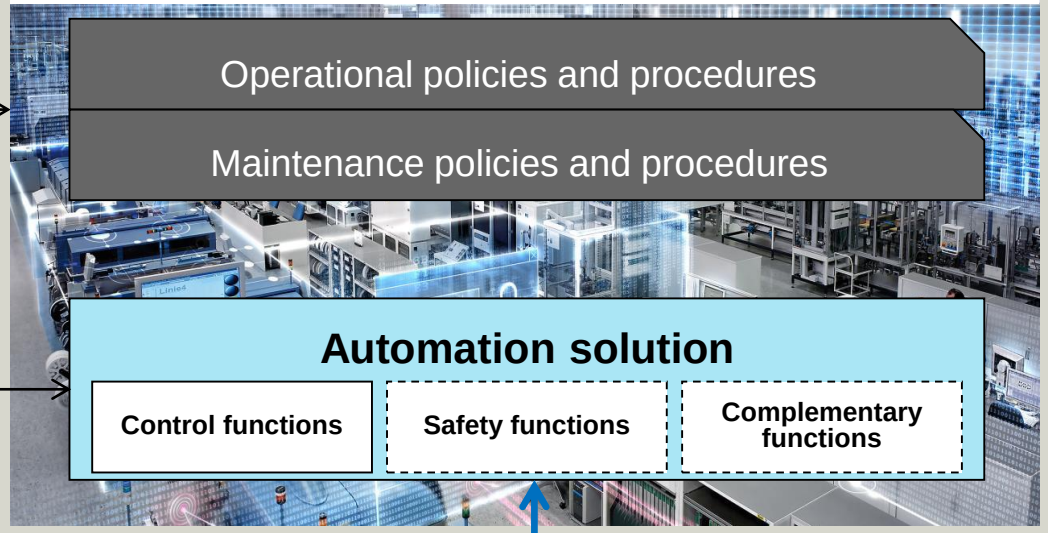
operates and maintains



System Integrator

designs and deploys

Industrial Automation and Control System (IACS)



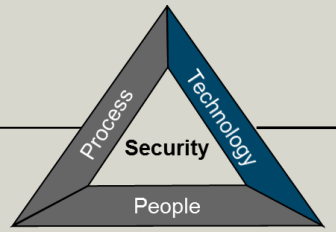
Parts of IEC 62443

2-1, 2-3, 2-4

2-4, 3-2, 3-3

Off site

Product Supplier

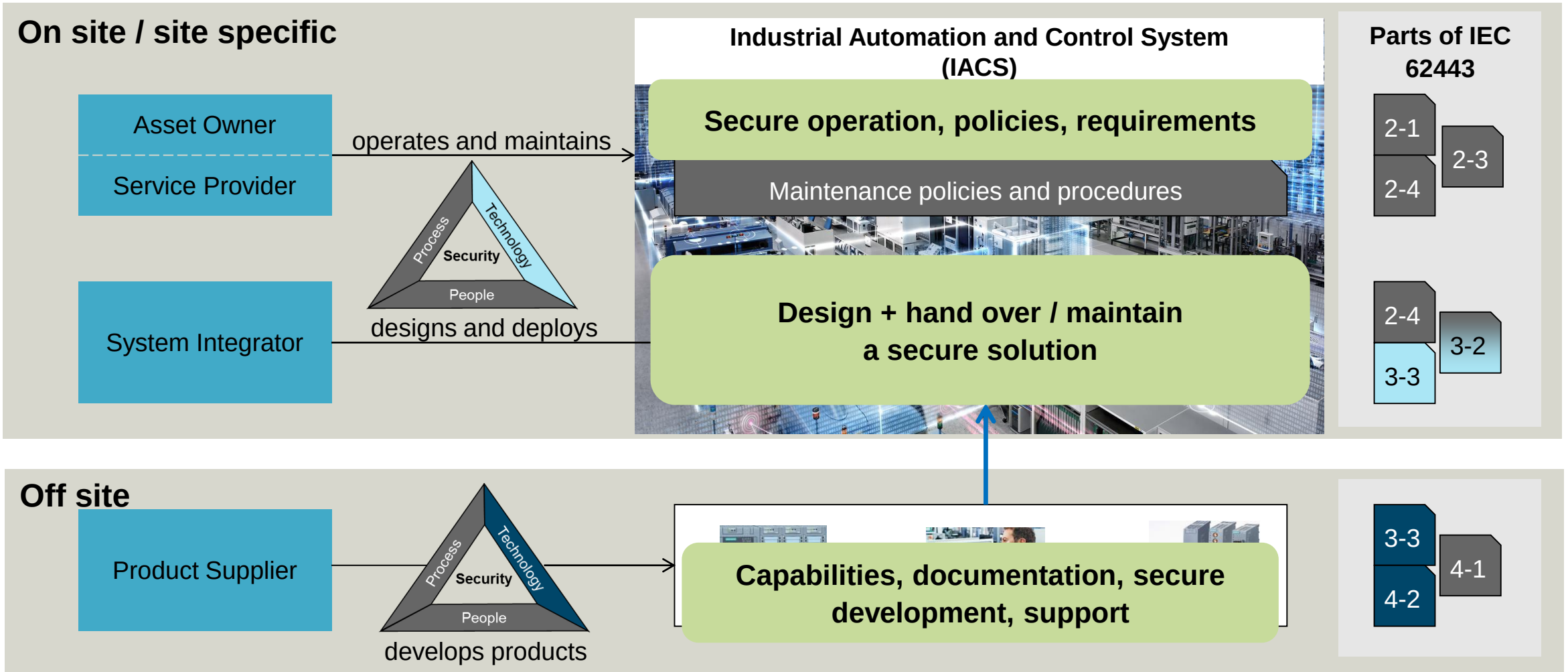


develops products

3-3, 4-1, 4-2

IEC 62443 addresses all stakeholders for a holistic protection concept

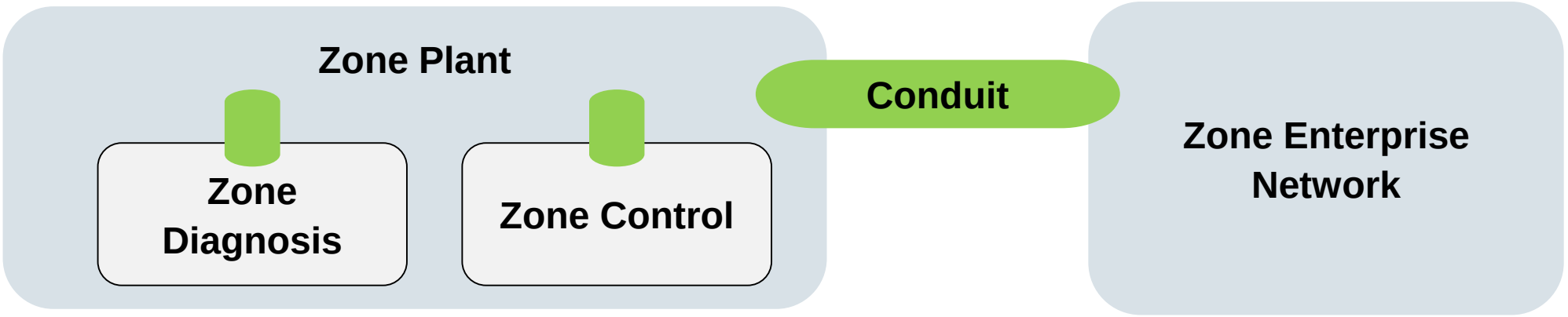
SIEMENS
Ingenuity for life



Security levels provide for protection against different attack levels

SIEMENS
Ingenuity for life

Zones and Conduits



The targeted security level is determined by a threat and risk analysis

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

Security Standard IEC 62443-3.3 defines security requirements for industrial control systems

SIEMENS
Ingenuity for life

7 Foundational Requirements	Example Security Vector: SL-x=(3,3,3,1,2,1,3)
FR 1 – Identification and authentication control	3
FR 2 – Use control	3
FR 3 – System integrity	3
FR 4 – Data confidentiality	1
FR 5 – Restricted data flow	2
FR 6 – Timely response to events	1
FR 7 – Resource availability	3

Example: Requirements for the foundational requirement FR1 “Identification and authentication control”

SRs und REs	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control				
SR 1.1 – Human user identification and authentication	✓	✓	✓	✓
SR 1.1 RE 1 – Unique identification and authentication		✓	✓	✓
SR 1.1 RE 2 – Multifactor authentication for untrusted networks			✓	✓
SR 1.1 RE 3 – Multifactor authentication for all networks				✓
SR 1.2 – Software process and device identification and authentication		✓	✓	✓
SR 1.2 RE 1 – Unique identification and authentication			✓	✓
SR 1.3 – Account management	✓	✓	✓	✓
SR 1.3 RE 1 – Unified account management			✓	✓
SR 1.4 – Identifier management	✓	✓	✓	✓
SR 1.5 – Authenticator management	✓	✓	✓	✓
SR 1.5 RE 1 – Hardware security for software process identity credentials			✓	✓
SR 1.6 – Wireless access management	✓	✓	✓	✓
SR 1.6 RE 1 – Unique identification and authentication		✓	✓	✓
SR 1.7 – Strength of password-based authentication	✓	✓	✓	✓
SR 1.7 RE 1 – Password generation and lifetime restrictions for human users			✓	✓
SR 1.7 RE 2 – Password lifetime restrictions for all users				✓
SR 1.8 – Public key infrastructure certificates		✓	✓	✓
SR 1.9 – Strength of public key authentication		✓	✓	✓
SR 1.9 RE 1 – Hardware security for public key authentication			✓	✓
SR 1.10 – Authenticator feedback	✓	✓	✓	✓
SR 1.11 – Unsuccessful login attempts	✓	✓	✓	✓
SR 1.12 – System use notification	✓	✓	✓	✓
SR 1.13 – Access via untrusted networks	✓	✓	✓	✓
SR 1.13 RE 1 – Explicit access request approval		✓	✓	✓

Detailed example: SR 1.1
Human user identification and authentication

SIEMENS
Ingenuity for life

Requirement

The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.

Rationale and supplemental guidance

All human users need to be identified and authenticated for all access to the control system. Authentication of the identity of these users should be accomplished by using methods such […]

Requirement enhancements

SR 1.1 RE 1 – Unique identification and authentication

SR 1.1 RE 2 – Multifactor authentication for untrusted networks

SR 1.1 RE 3 – Multifactor authentication for all networks

Security levels

- SL-C(IAC, control system) 1: SR 1.1
- SL-C(IAC, control system) 2: SR 1.1 (1)
- SL-C(IAC, control system) 3: SR 1.1 (1) (2)
- SL-C(IAC, control system) 4: SR 1.1 (1) (2) (3)

Basic concepts used in IEC 62443-3-3
Compensating Countermeasures

SIEMENS
Ingenuity for life

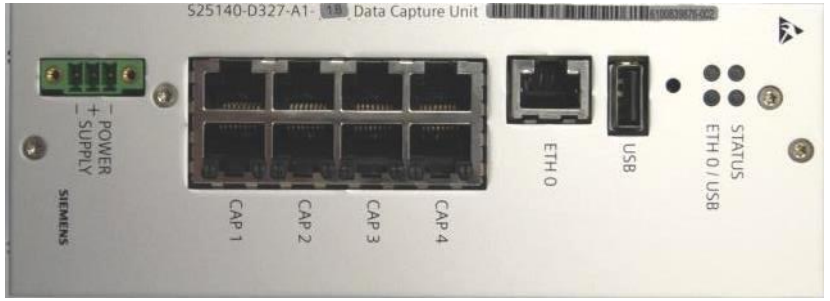
According to IEC 62443-3-3, a **compensating countermeasure** is a “countermeasure employed in lieu of [= instead of] or in addition to inherent security capabilities to satisfy one or more security requirements”

When designing a control system to meet a specific SL-Ts, it is not necessary that every component of the proposed control system support every system requirement to the level mandated in IEC 62443-3-3. **Compensating countermeasures** can be employed to provide the needed functionality to other subsystems, such that the overall SL-T requirements are met at the control system level.

Examples (mentioned in IEC 62443-3-3):

- Locked cabinet around a controller that doesn’t have sufficient cyber access control countermeasures
- A vendor’s programmable logic controller (PLC) can’t meet the access control capabilities from an end-user, so the vendor puts a firewall in front of the PLC and sells it as a system.

Secure Data Connector DCU – Protecting our installed base and enabling cloud connectivity



Challenge

- Legacy systems were designed and built as isolated from other networks (for security reasons)
- Digitalization will get everything connected, incl. legacy systems

Availability

- Released in 2018
- OPC-UA support, IEC 62443-4-2 SL3

Business Benefit/USPs

- Cost-effective (compared to competitor diode solutions)
- Safety certification: No inferences of critical safety networks
- Safe, secure and easy enabling cloud connect (MindSphere)

Technical Solution

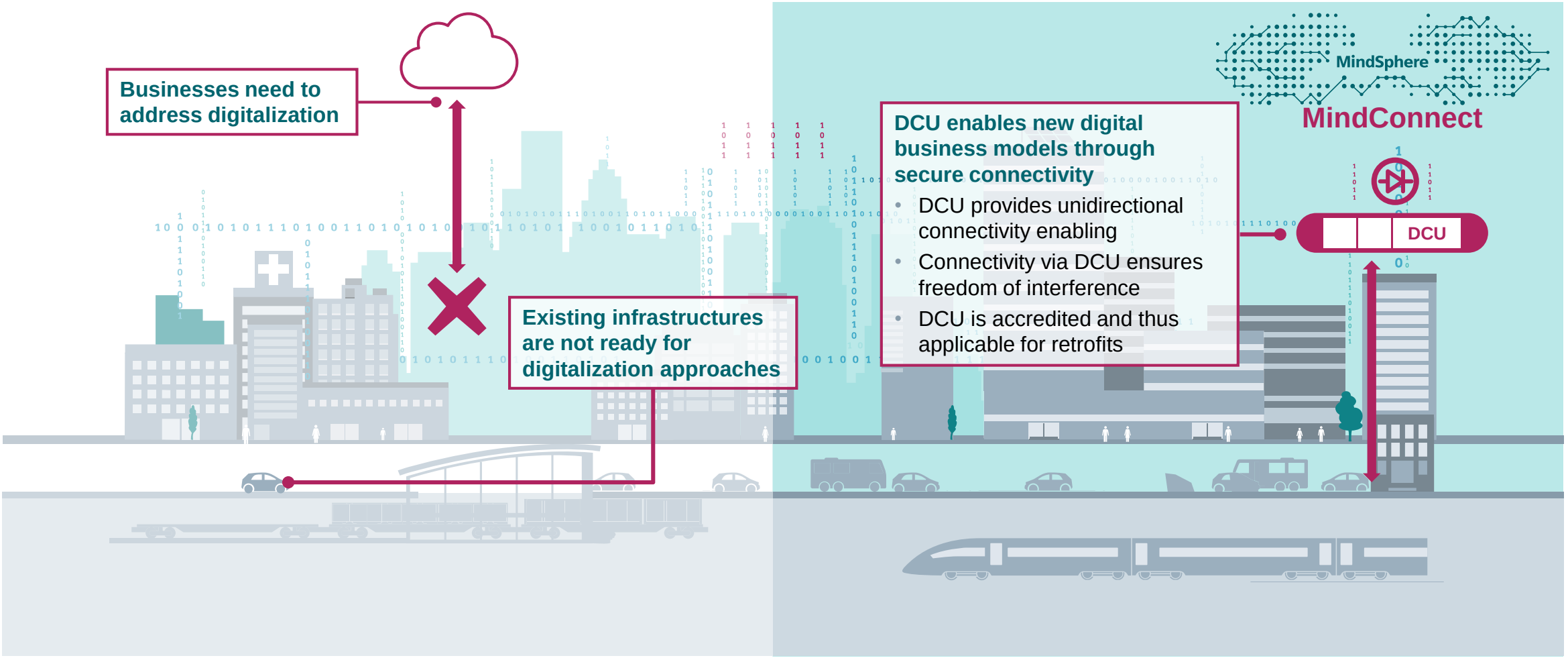
- HW design to guarantee one-way data connection only
  → 100% resistant against a break into a protected network
- Maintains safety and integrity for all connectivity scenarios
- Edge computing enabled for 3rd party applications
- Joint development by Mobility and Corporate Technology

https://www.siemens.com/dcu

DCU: Data Capture Unit | **OPC-UA**: Open Platform Communications – Unified Architecture **| IEC:** International Electrotechnical Commission

DCU enables business to address opportunities of digitalization with their existing infrastructures

SIEMENS
Ingenuity for life



Digitalization meets industry:
Securely connecting and improving all steps along the lifecycle

SIEMENS
Ingenuity for life

“Industrie 4.0”

Merging the real factory with its digital twin:
consistent data and security on all levels and throughout all lifecycle phases by integrating engineering software and plant automation

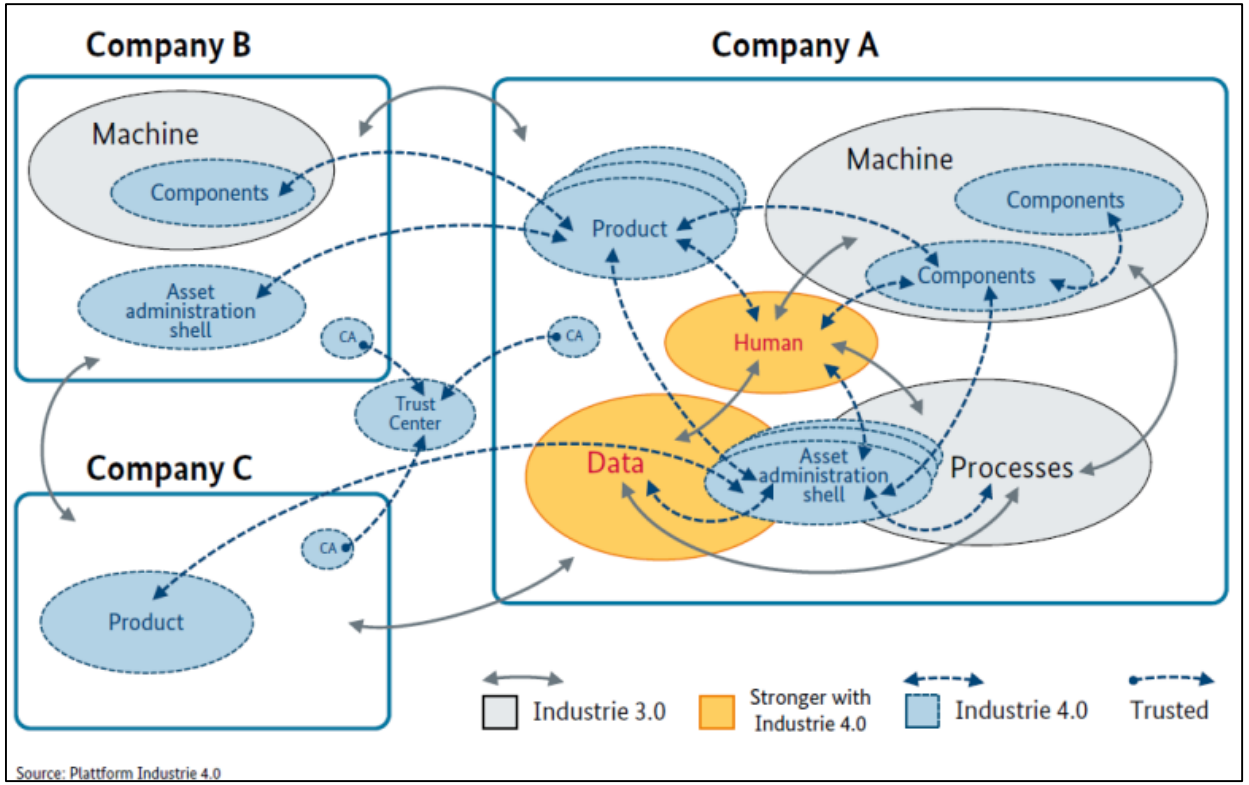
Security needs to protect throughout the complete life cycle

Cooperation across security domains characterises I4.0 use cases

SIEMENS
Ingenuity for life

- Increasing flexibility and customer-specific production by
  - ad-hoc interconnections realize value creation networks across company boundaries
  - direct data exchange of all entities (people, machines, processes etc.)

⇒ Increased attack surface



Boundary Conditions of Industrie 4.0

- Data exchange between the entities is based on trust of the partners
- Legally relevant communication between machines entities will be necessary to realize ad-hoc interconnections

Security within Industrie 4.0 = Security-by-Design

SIEMENS
Ingenuity for life

Security-by-Design as a superior principle

- Subsequent enrichment of systems is not sufficient.
- Security measures have to be integrated (up to application level).

Security for the digital model + physical representation

- Security for the physical instance, its digital twin and their interactions must take place in a concerted way.

Authentication and Secure Identities for Devices

- Unforgeable identities and trust anchors are needed.
- Keys, security credentials must be bound to the device.

Security for Inter Domain Communication

- Interconnect existing I3.x-Security architectures to enable secure inter domain cooperation;
- Global, robust, and trustworthy key management infrastructure needed

Industrial Security will enable Industrie 4.0

SIEMENS
Ingenuity for life

Trustworthiness is needed for cooperation

- Authenticity and Integrity of data and systems along the value chain support confidence about security levels of involved parties

Adaptive security architectures

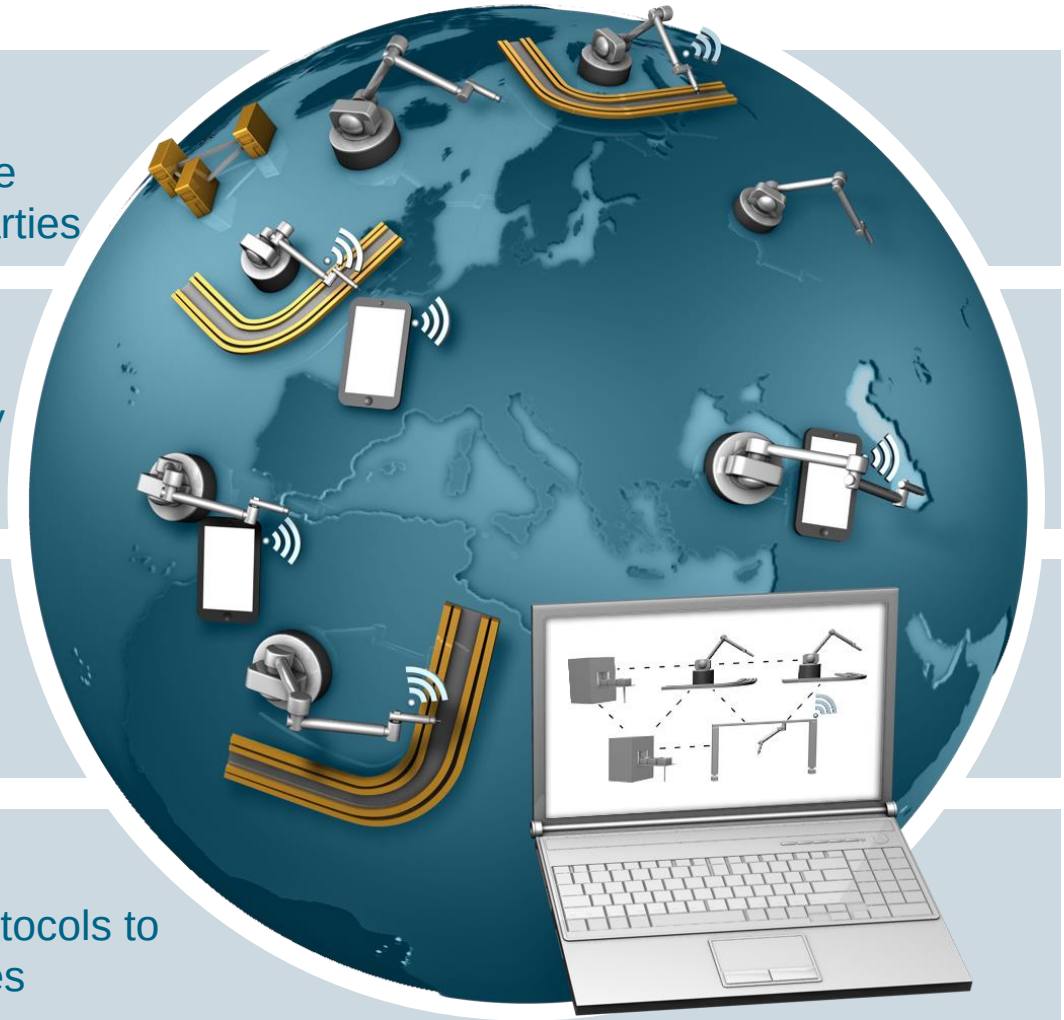
- Agile security profiles have to be adaptable in a dynamic way
- Fast configuration must include security.

Prevention and reaction are still needed

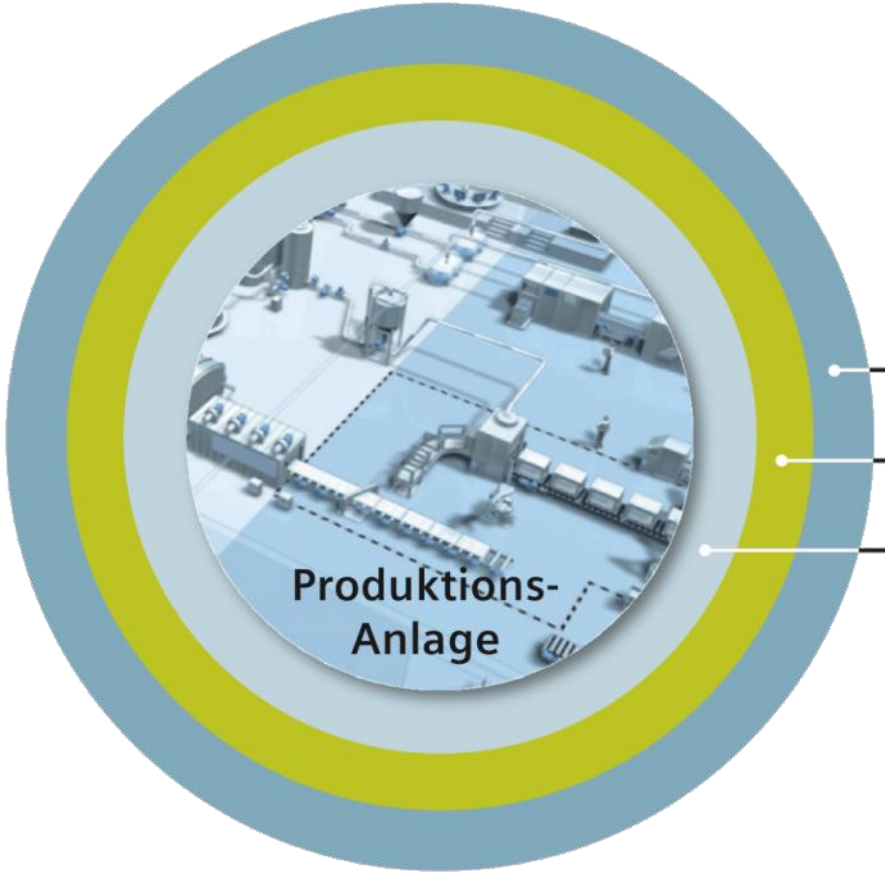
Security will remain a moving target. There will be no final I4.0 security solution without a need for further measures.

Standardization enables secure infrastructures

Security requires standardized specifications of interfaces and protocols to support requirements and to negotiate and operate security profiles (security semantics) between different domains.



Developing Industrial Security based on IEC 62443



Plant security

Network security

System integrity

Control of the physical access to plants or critical infrastructures +

Security management processes and technical measures +

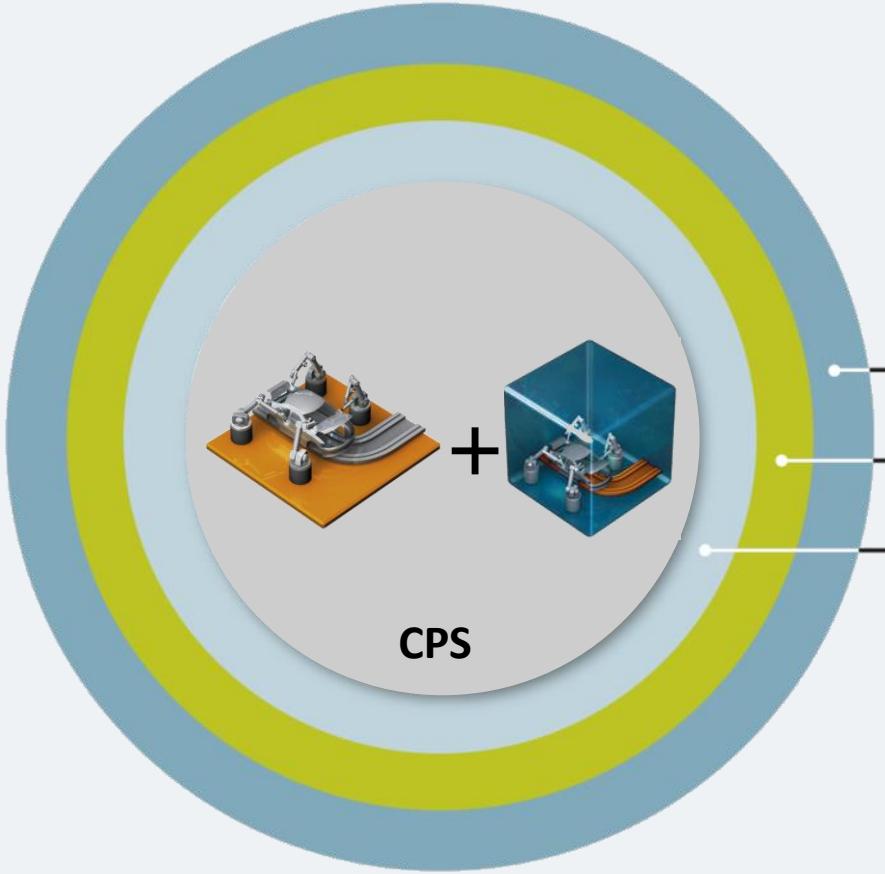
Network segmentation with zones and conduits +

Security Services for the protection of the plant during the whole lifecycle +

System integrity with integrated security functions +

Developing Industrial Security based on IEC 62443

SIEMENS
Ingenuity for life



Plant security

- Intelligent physical access to buildings and plants
- Self synchronizing access control

+

- Self learning security management processes
- Dynamic threat analysis and adaption

+

Network security

- Dynamic, flexible network architectures
- Permanent monitoring of networks and communications

+

System integrity

Protection and proof of the integrity of the overall system during the whole lifecycle

+

Unambiguous and secure integrity of products, processes and machines

+

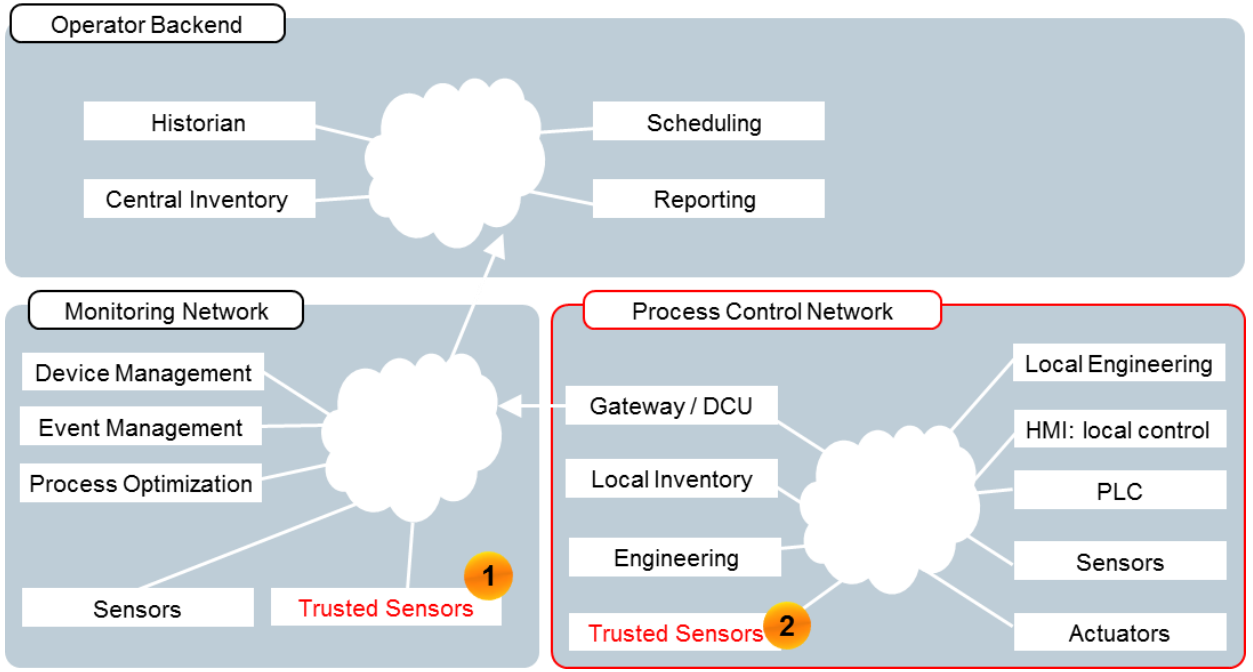
Increase reliability of sensing data by adding trusted sensors

Trusted sensor node

- Platform with a trust anchor, supporting security functionality like trusted boot and secured communication of sensor values
- Support for device integrity monitoring (and reporting), locally as well as remotely
- Additional measures to support physical integrity (e.g., tamper detection)

Validation of Sensing Data

- Sensor network is enhanced with trusted sensors
- Trusted sensors support sensor fusion by providing additional information for plausibility checks of provided data of untrusted sensors
- Data fusion performed onsite, in edge cloud, or in the backend, trusted sensors feature a higher trust value for the data fusion.



Deployment options

1. As part of monitoring network and independent from process core network
2. As part of the core network, either as additional sensor without interfering the core network or as replacement of selected existing sensors

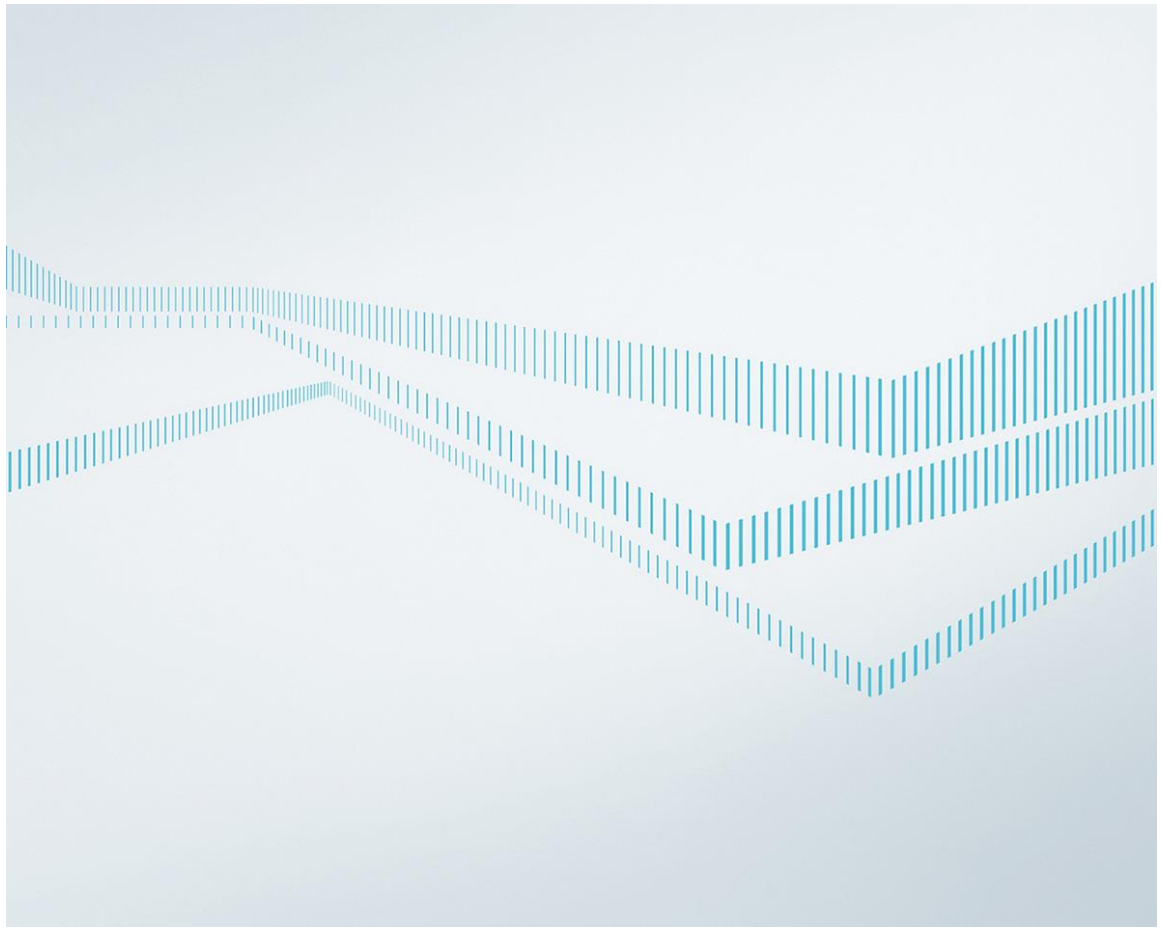
Security has to be suitable for the addressed environment

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



Dr. Rainer Falk
Principal Key Expert

Siemens AG
Corporate Technology
CT RDA CST
Otto-Hahn-Ring 6
D-81739 Munich
Germany

E-mail
rainer.falk@siemens.com

Internet
siemens.com/corporate-technology