PCIC EUROPE
PETROLEUM & CHEMICAL INDUSTRY COMMITTEE

PCIC Europe 2017
CYBER SECURITY TUTORIAL
ENERGY AUTOMATION AND IEC 62443

Dirk Kroeselberg, Siemens AG, Corporate Technology
Frederic Buchi, Siemens AG, Energy Management
Hans Meulenbroek, Siemens Nederland N.V.

Tutorial Agenda

Agenda

Motivation and Threat Landscape

Cyber Security Standards

Risk Driven Approach

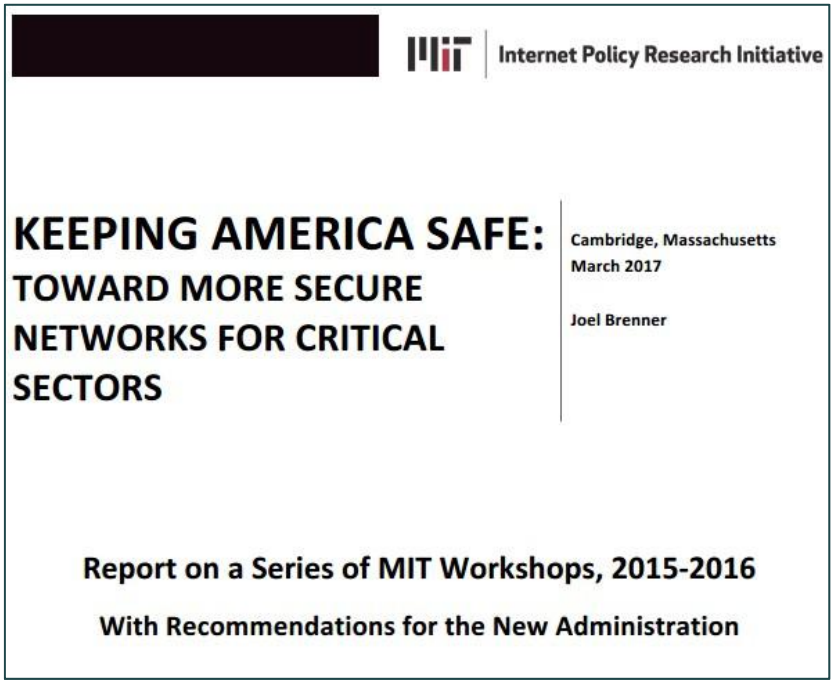
Realization Approaches

Summary and Outlook

Why Cyber Security?

Statements from the MIT report on the right (issued in March 2017)

- "[..] The Internet is a legacy system designed for non-commercial uses with little or no need for security. Security has chiefly been an option for end points,[..]"
- "[..] The digital systems that control critical infrastructure in the United States and most other countries are easily penetrated and architecturally weak [..]"

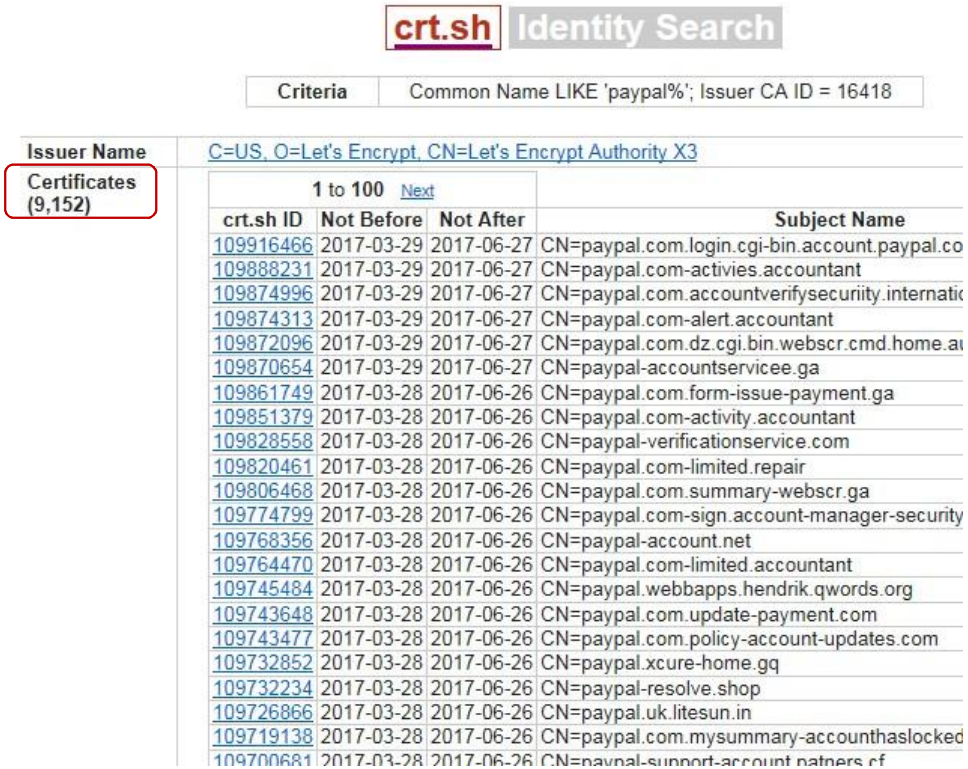


Source: https://internetpolicy.mit.edu/reports/Report-IPRI-CIS-CriticalInfrastructure-2017-Brenner.pdf

Why Cyber Security?

There is no “air gap”

- OT is interconnected with IT
  - Interfaces with Enterprise/Office network
  - Remote access
  - USB sticks, maintenance computers
- One of the main attack vectors today is “phishing”, also for attacks on OT environments
- General Internet security does not prevent phishing on its own:
  - Example on the right: Number of certificates issued for Web servers by “Let’s Encrypt” with “paypal” in the name



crt.sh Identity Search

Criteria	Common Name LIKE 'paypal%'; Issuer CA ID = 16418
Issuer Name	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Certificates (9,152)	

1 to 100 Next

crt.sh ID	Not Before	Not After	Subject Name
109916466	2017-03-29	2017-06-27	CN=paypal.com.login.cgi-bin.account.paypal.co
109888231	2017-03-29	2017-06-27	CN=paypal.com-activies.accountant
109874996	2017-03-29	2017-06-27	CN=paypal.com.accountverifysecuriity.internatic
109874313	2017-03-29	2017-06-27	CN=paypal.com-alert.accountant
109872096	2017-03-29	2017-06-27	CN=paypal.com.dz.cgi.bin.webscr.cmd.home.a
109870654	2017-03-29	2017-06-27	CN=paypal-accountservicee.ga
109861749	2017-03-28	2017-06-26	CN=paypal.com.form-issue-payment.ga
109851379	2017-03-28	2017-06-26	CN=paypal.com-activity.accountant
109828558	2017-03-28	2017-06-26	CN=paypal-verificationservice.com
109820461	2017-03-28	2017-06-26	CN=paypal.com-limited.repair
109806468	2017-03-28	2017-06-26	CN=paypal.com.summary-webscr.ga
109774799	2017-03-28	2017-06-26	CN=paypal.com-sign.account-manager-security
109768356	2017-03-28	2017-06-26	CN=paypal-account.net
109764470	2017-03-28	2017-06-26	CN=paypal.com-limited.accountant
109745484	2017-03-28	2017-06-26	CN=paypal.webbapps.hendrik.qwords.org
109743648	2017-03-28	2017-06-26	CN=paypal.com.update-payment.com
109743477	2017-03-28	2017-06-26	CN=paypal.com.policy-account-updates.com
109732852	2017-03-28	2017-06-26	CN=paypal.xcure-home.gq
109732234	2017-03-28	2017-06-26	CN=paypal-resolve.shop
109726866	2017-03-28	2017-06-26	CN=paypal.uk.litesun.in
109719138	2017-03-28	2017-06-26	CN=paypal.com.mysummary-accounthaslocked
109700681	2017-03-28	2017-06-26	CN=paypal-support-account.patners.cf

Source: https://crt.sh
(March 2017)

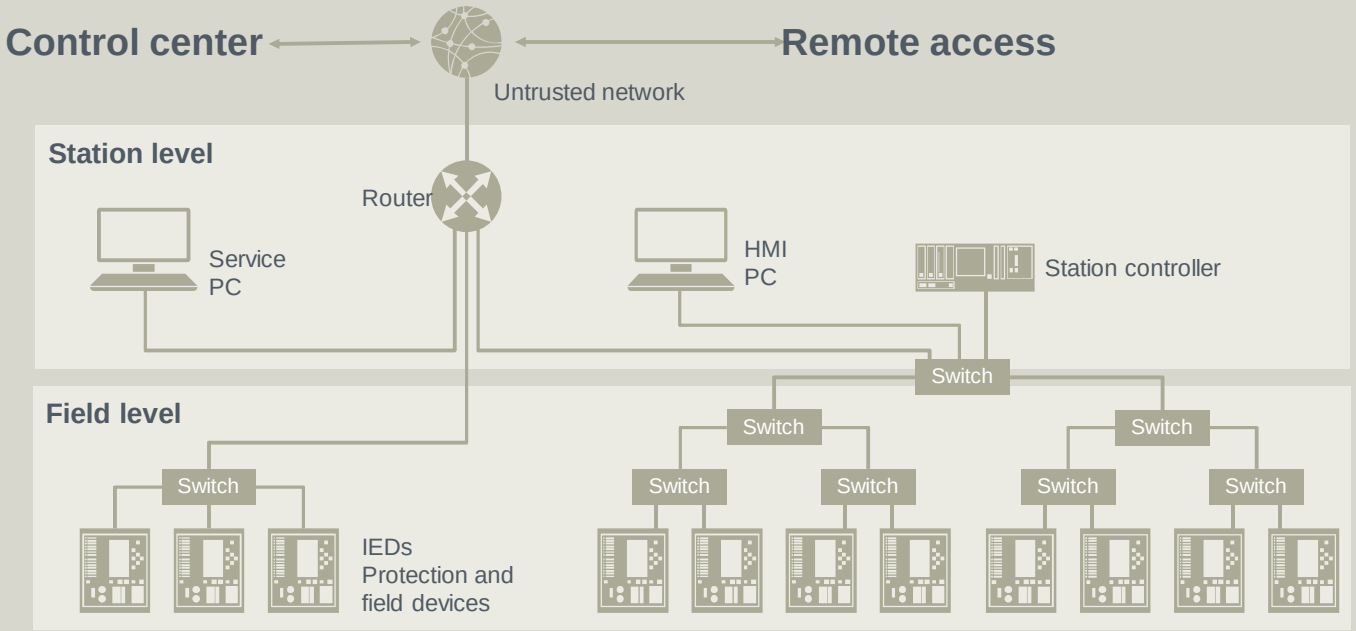
Cyber Security: Factors for Threat Consideration

General Factors

- Critical Infrastructure, 24 h Operation, geographically distributed

Functional Factors

- Proprietary technology
- Windows/Linux standard components
- Mix of components from different vendors with different technologies
- Interfaces to office networks
- Interfaces across unsecure networks
- Legacy components



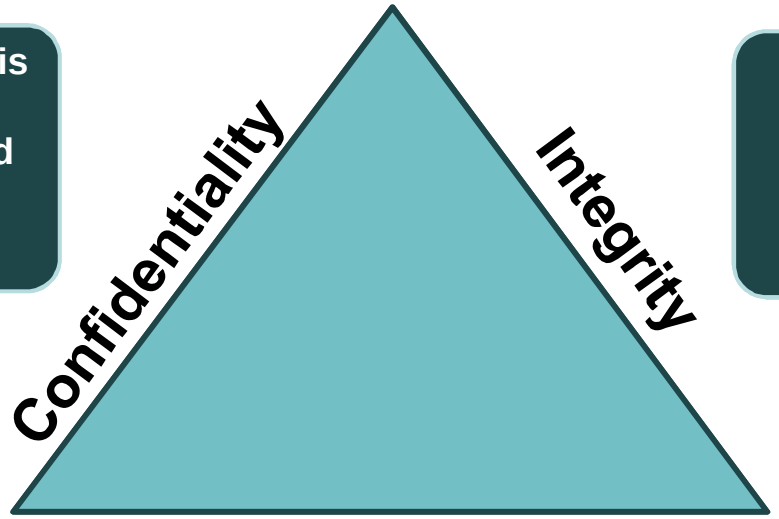
Example:
Substation Automation

- IEDs
- Embedded Controllers
- Standard-OS PCs (HMI, Engineering)
- Network equipment
- External interfaces

Protection Goals

- High-level protection goals: prevent loss of C, I, A

Property that information is not made available or disclosed to unauthorized individuals, entities, or processes

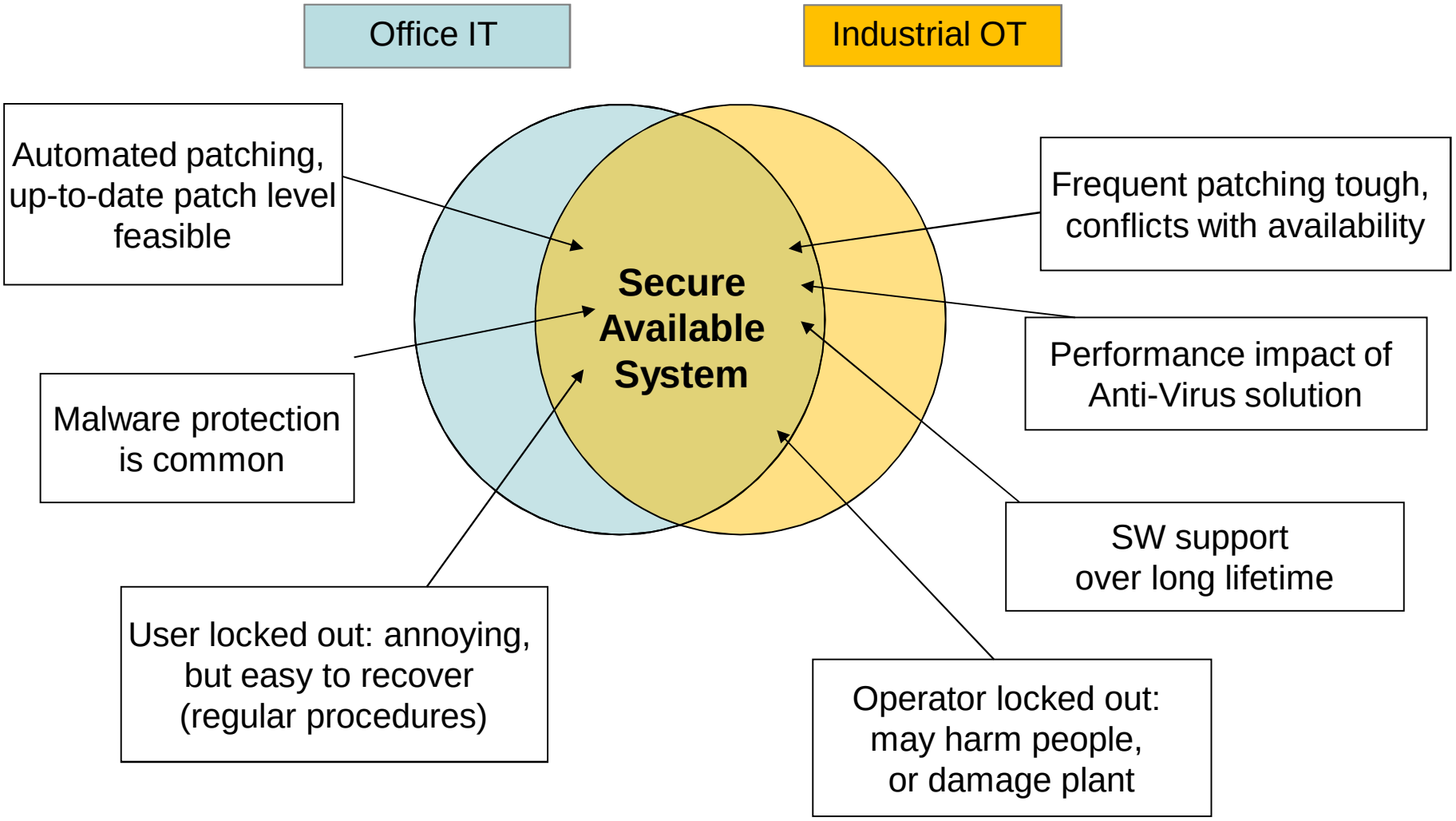


Property of protecting the accuracy and completeness of assets

Property of being accessible and usable upon demand by an authorized entity

Definitions from ISO/IEC27000:2012

Areas of Conflict



How realistic are cyber security threats today?

- Wide availability of tools for automation
  - Example: Shodan will tell you all publicly available IP addresses of a specific controller, or IoT device
  - Bulk searching support via API and dictionary file
  - Do you know how exactly your devices are connected?

- Attack on Ukraine Power Grid
  - Affecting Power Grid operators, substations, approx. 220.000 people without power (end of 2015, follow-up attacks during 2016)

- “SAP Cybersecurity for Oil and Gas”, ERPScan Whitepaper presented at Blackhat Europe, Nov. 2015
  - IT/OT integration extends IT domain threats into the OT domain

Basic steps of the Ukraine power grid attack

- Spearphishing, infection of an office laptop with the “BlackEnergy” malware.
- Network scans in the IT network
  - Found a connection to an OT supervision platform
- Network scans in the OT network
  - Collect information about installed OT components
- Install further malware components in the IT and OT parts of the network
- Ready to trigger the actual attack later

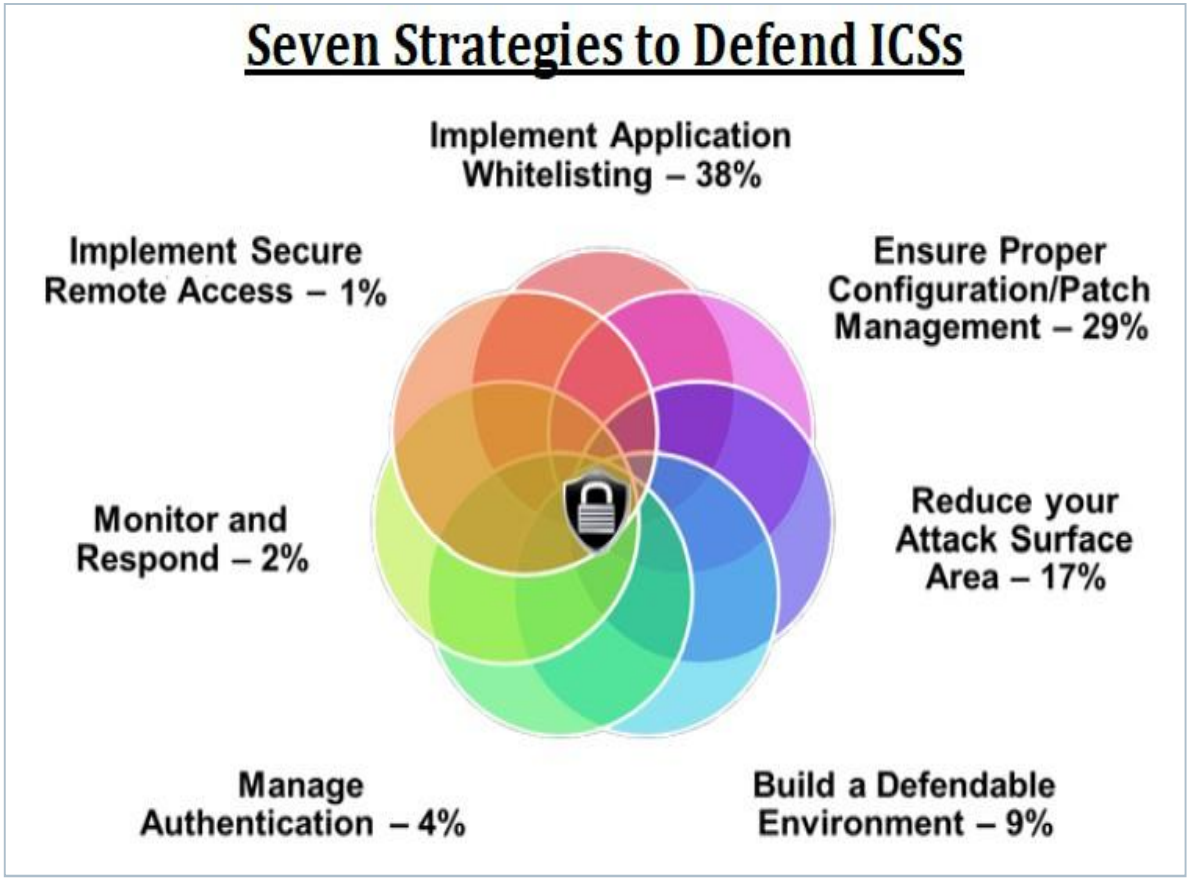
„Two days before Xmas, in the afternoon as stated by an operator, the mouse moved on the HMI and started switching off breakers remotely.

As the local operator attempted to regain control of the supervision interface, he was logged off and couldn’t login again because the password had been changed (figure3). “

Souce: ISA France,
ISA FLASH N ° 62 – Décembre 2016

But where to find good approaches to secure deployments?

- Source: US NCCIC (ICS-CERT), FBI, NSA
- Percentage of ICS-CERT FY 2014 and FY 2015 incidents potentially mitigated by each strategy
- But this does not really help us
  - Application whitelisting is just a tool
  - Configuration, Patch management, attack surface reduction, are huge areas



See: https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

Tutorial Agenda

Agenda

- Motivation and Threat Landscape
- **Cyber Security Standards**
- Risk Driven Approach
- Realization Approaches
- Summary and Outlook

Capabilities based on risks within the organization

Organizational Security & Processes

People, Policies, Processes, Governance

Organizational Preparedness	Secure Development	Secure Integration and Service	Secure Operation	Vulnerability and Incident Handling
Secure System Architecture	System Hardening	Access Control and Account Management	Security Logging & Monitoring	Data Protection and Integrity
Secure Patching	Malware Protection	Backup and Restore	Secure Remote Access	Privacy

Products, Systems, Solutions

- Common security activities need to be performed
- Common security technologies need to be implemented

Cyber security standards target different areas and roles

Domain specific scope

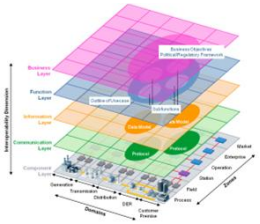
- **Focus on process industries, system suppliers:**
  - WIB
- **Focus on general IACS (industrial automation control system):**
  - IEC 62443
- **Focus on energy:**
  - BDEW Whitepaper
  - NERC-CIP
  - ISO/IEC 27019
- **Focus on health care:**
  - HIPAA
  - DIARMF

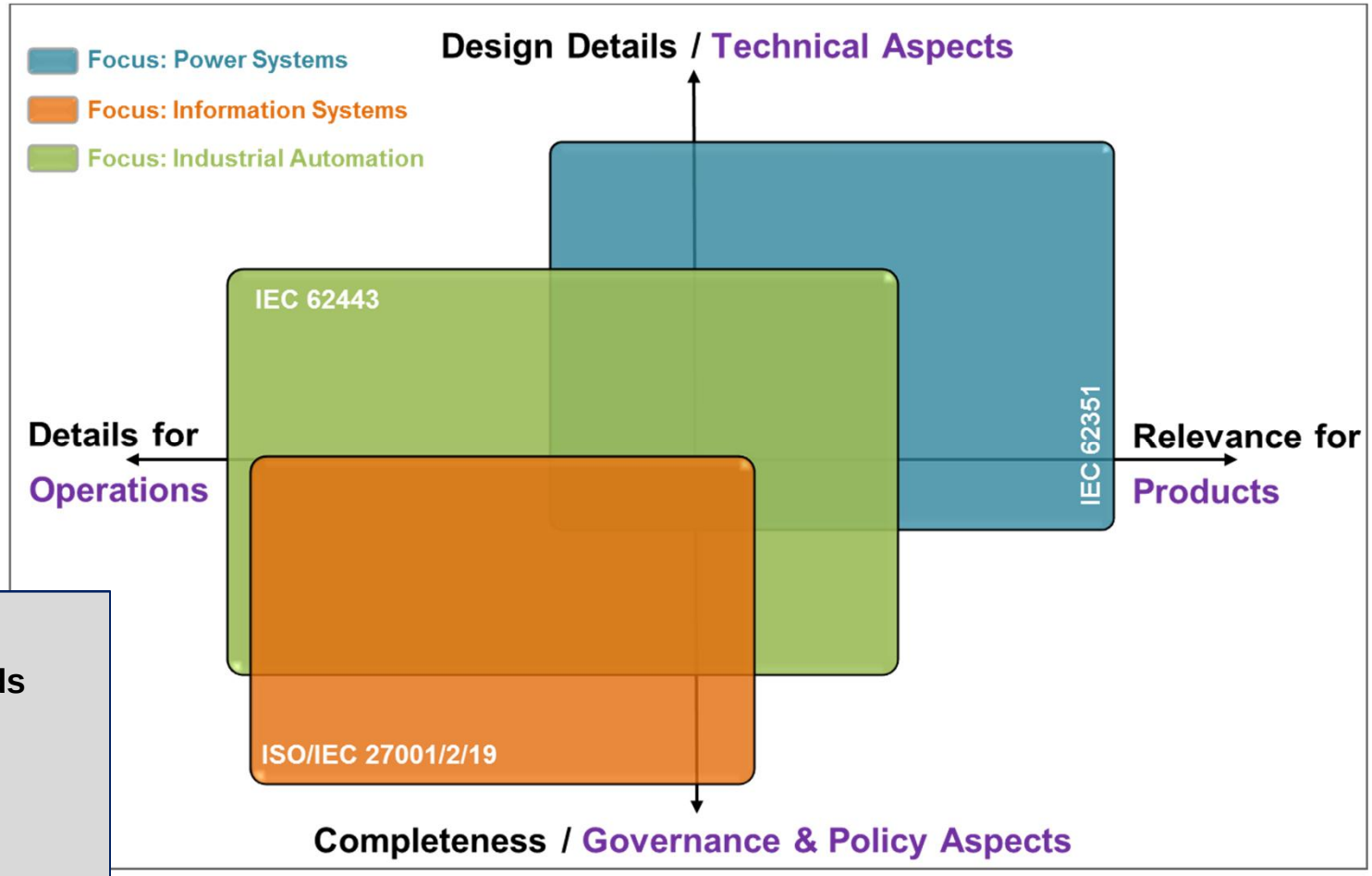
Role specific scope

- **Focus on product security features:**
  - IEC 62443-4-2
- **Focus on system security capabilities:**
  - IEC 62443-3-3
- **Focus on integration and maintenance:**
  - IEC 62443-2-4
- **Focus on secure operation:**
  - NERC-CIP
  - IEC 62443-2-2
- **Focus on secure development lifecycle:**
  - IEC 62443-4-1
  - Security by Design with CMMI for Dev.
  - ISO 27034

Selected Key Security Standards for Energy Automation

Smart Grid Coordination Group / Smart Grid Information Security Mandate M/490





Key Standards

- **IEC 62443** (System Security)
- **IEC 62351** (Communication Security)
- **ISO/IEC 27001/27019** (Security Management)

ISO 27000 Definitions

„Information Security Management System“ - ISMS

> “part of the overall **management system,** based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security [ISO27000]

„Management System“

> “framework of policies, procedures, guidelines and associated resources to achieve the objective s of the organization

Information Security Management System (ISMS)

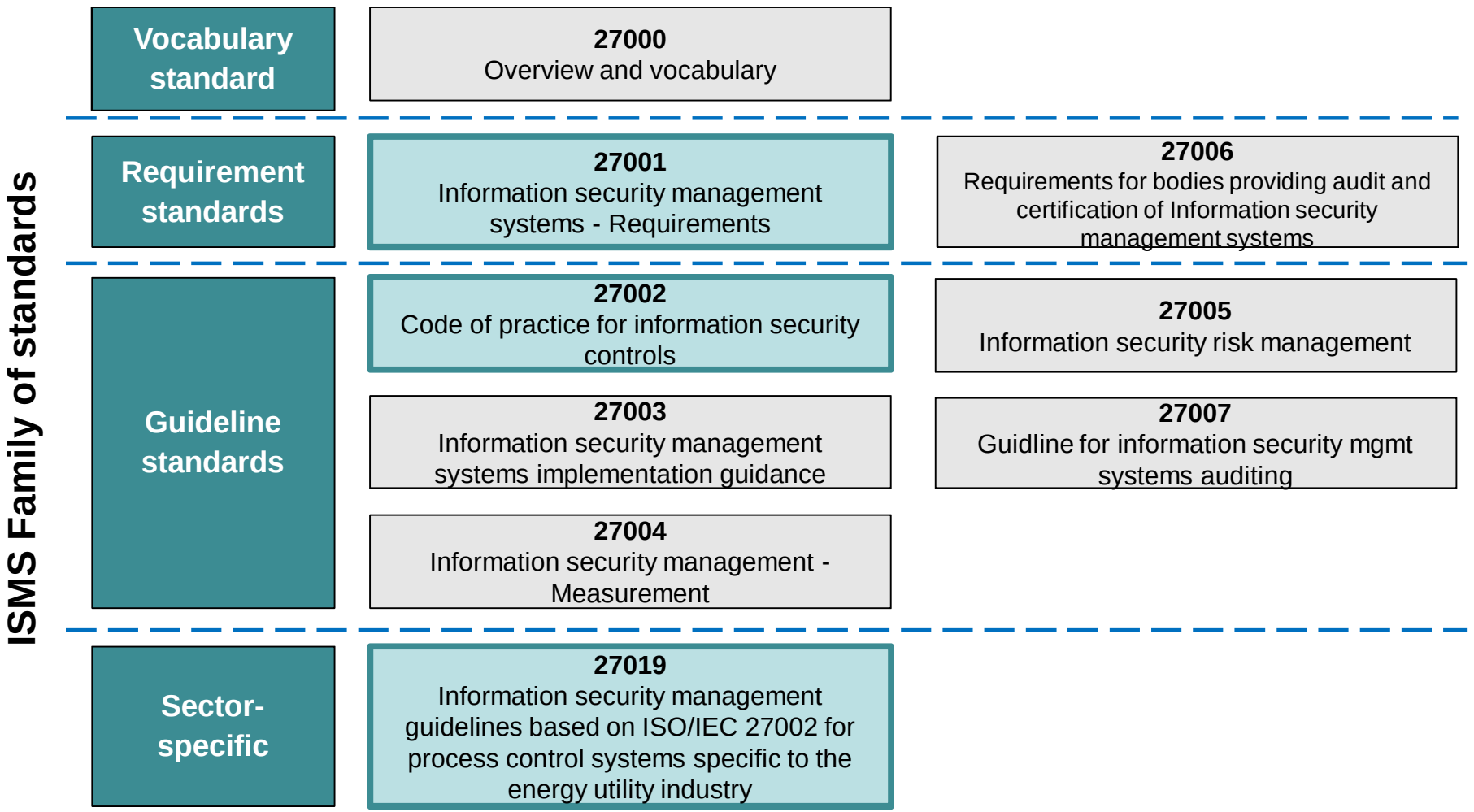
ISO/IEC 27001:
Information Security Management System

Maintaining the **confidentiality**, **integrity** and **availability**, whatever the form of information, values. This includes all written, pictorial and spoken information.

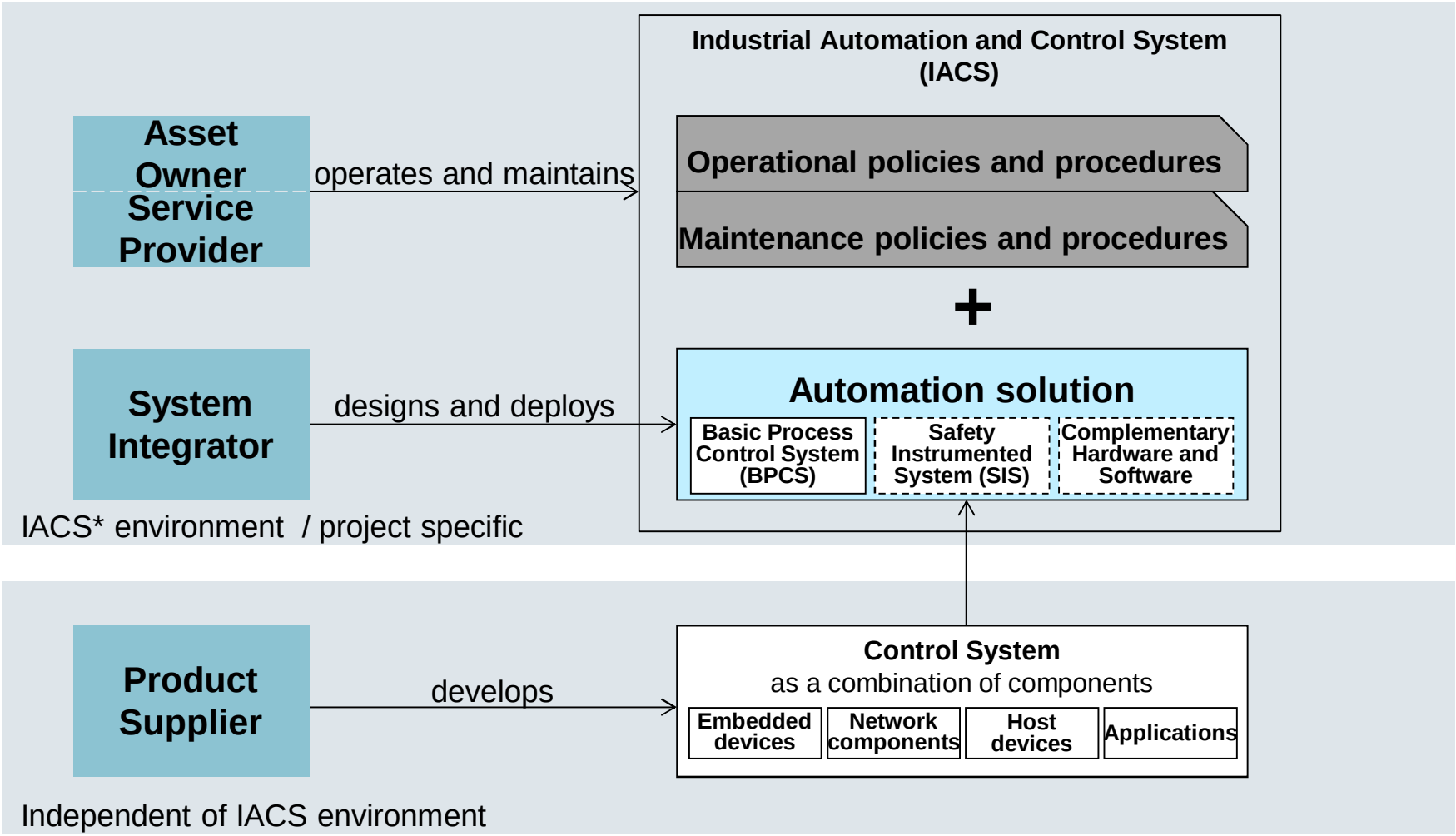
ISO / IEC 27001 was developed as a model for the development, implementation, monitoring, review, maintenance and improvement of an **information security management system - ISMS**.

ISO/IEC 27001 is process- and organization-oriented
ISO/IEC 27001 bases on continuous improvement
(Plan-Do-Check-Act)
ISO/IEC 27001 overlaps with ISO 9001.

ISO/IEC 27000 Framework overview (selected parts)

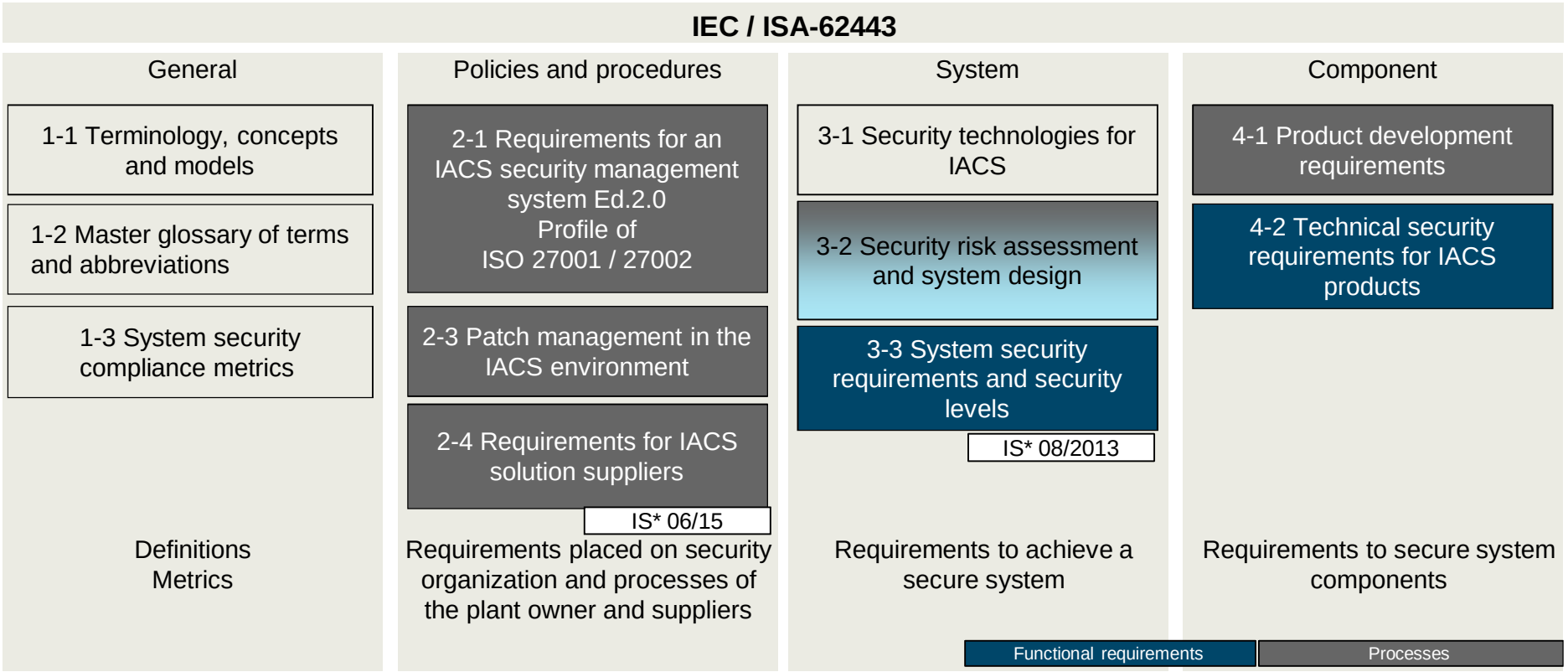


Security Standards – Structuring based on the Role



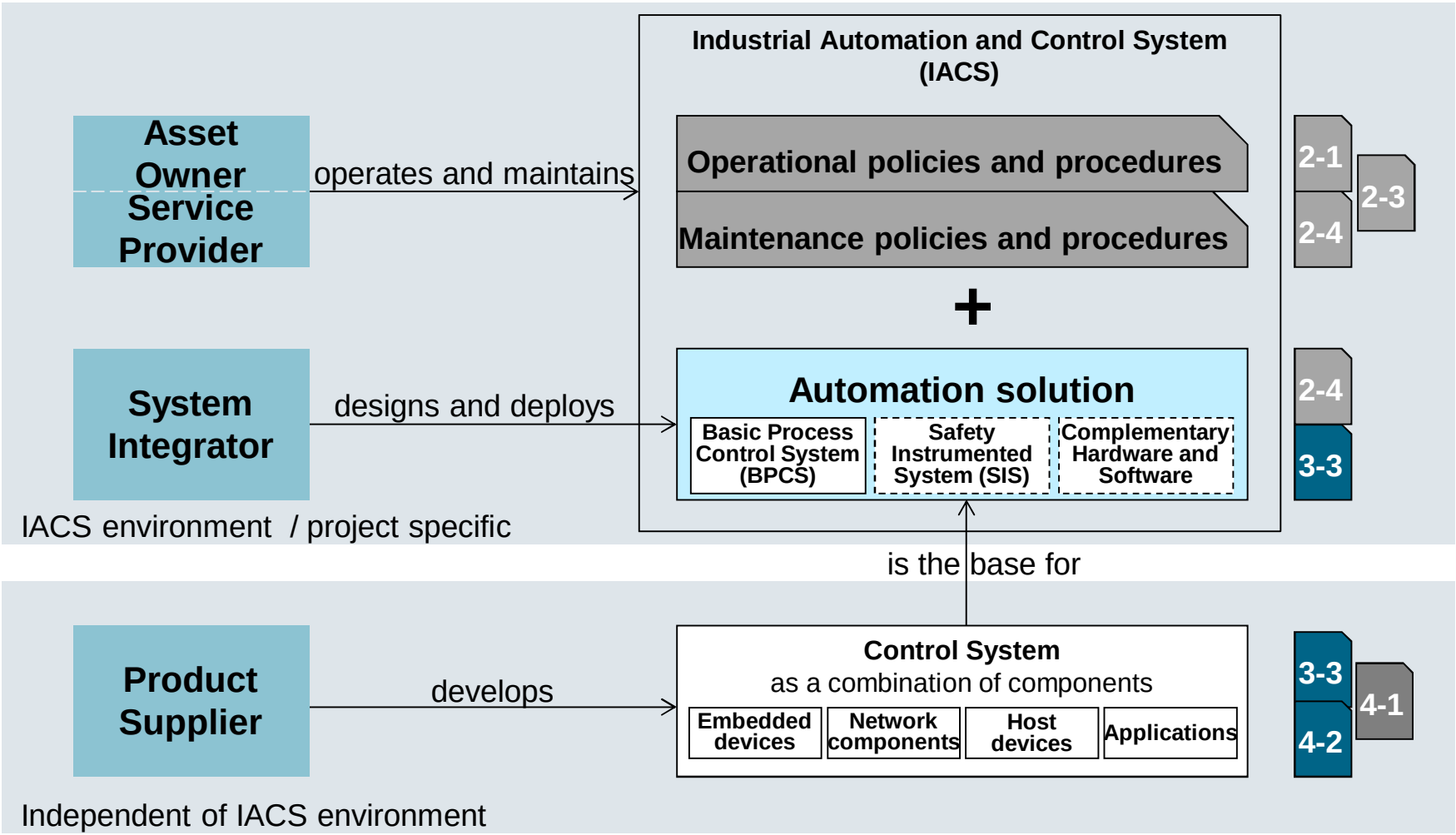
*IACS = Industrial Automation Control System

The IEC-62443 Framework of Security Standards: Covering all areas

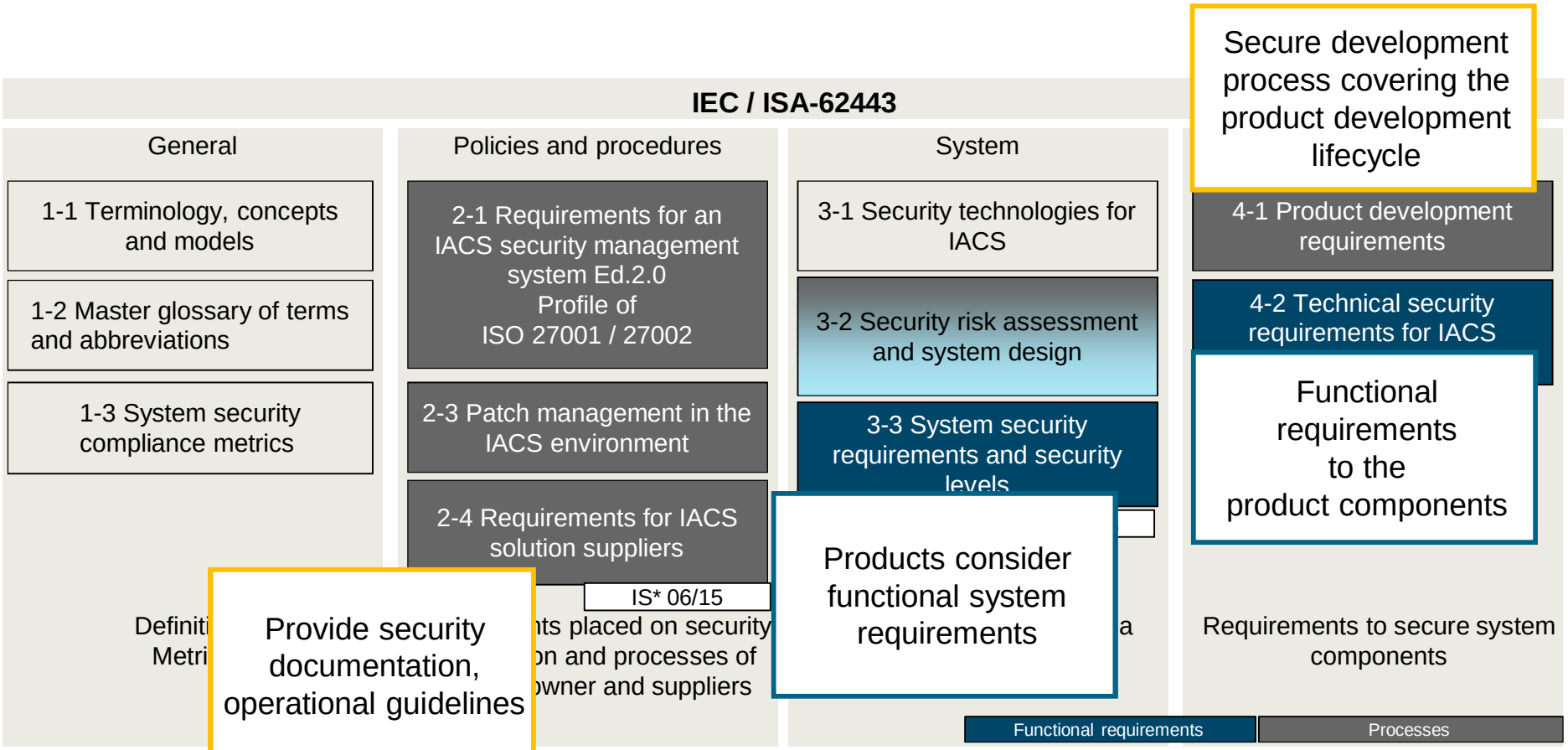


*IS = International Standard

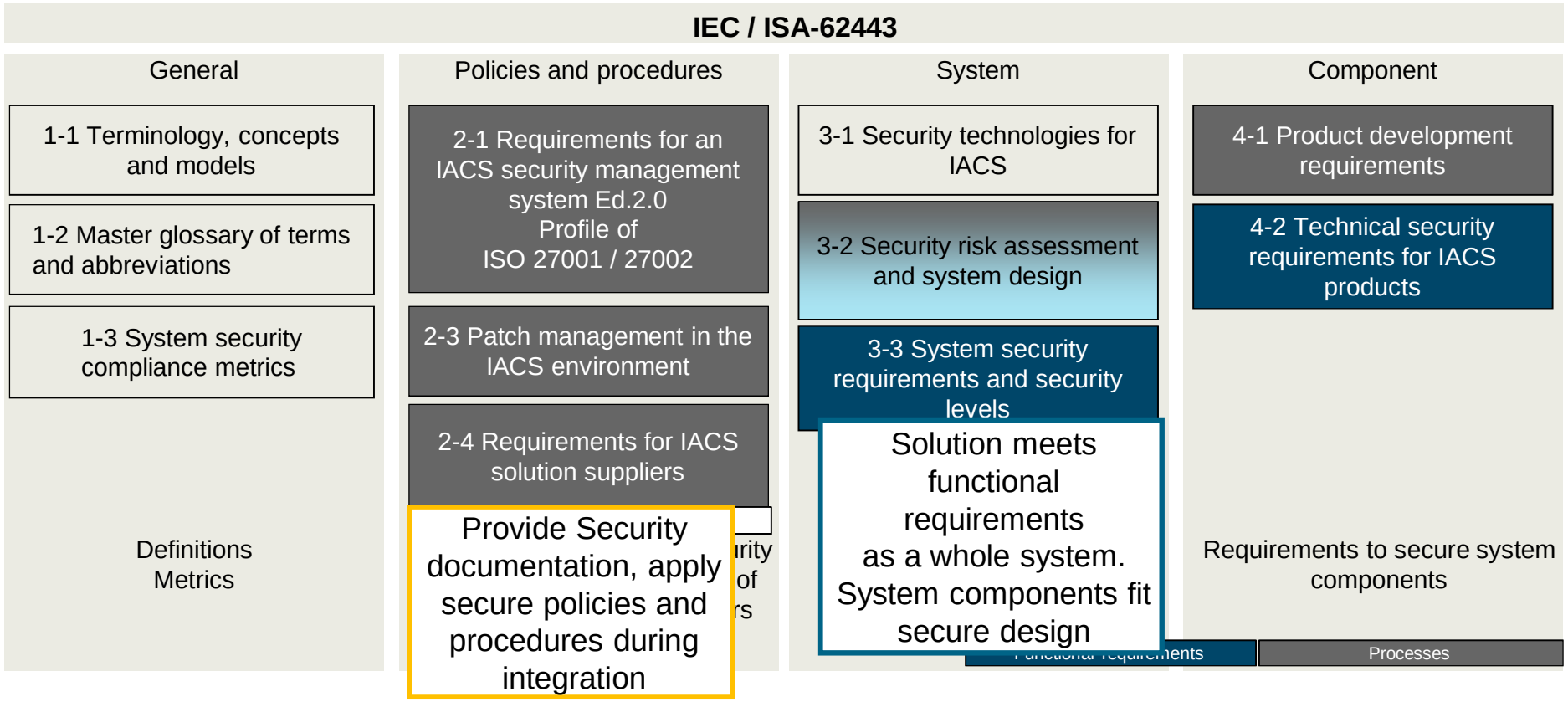
IACS, automation solution, control system



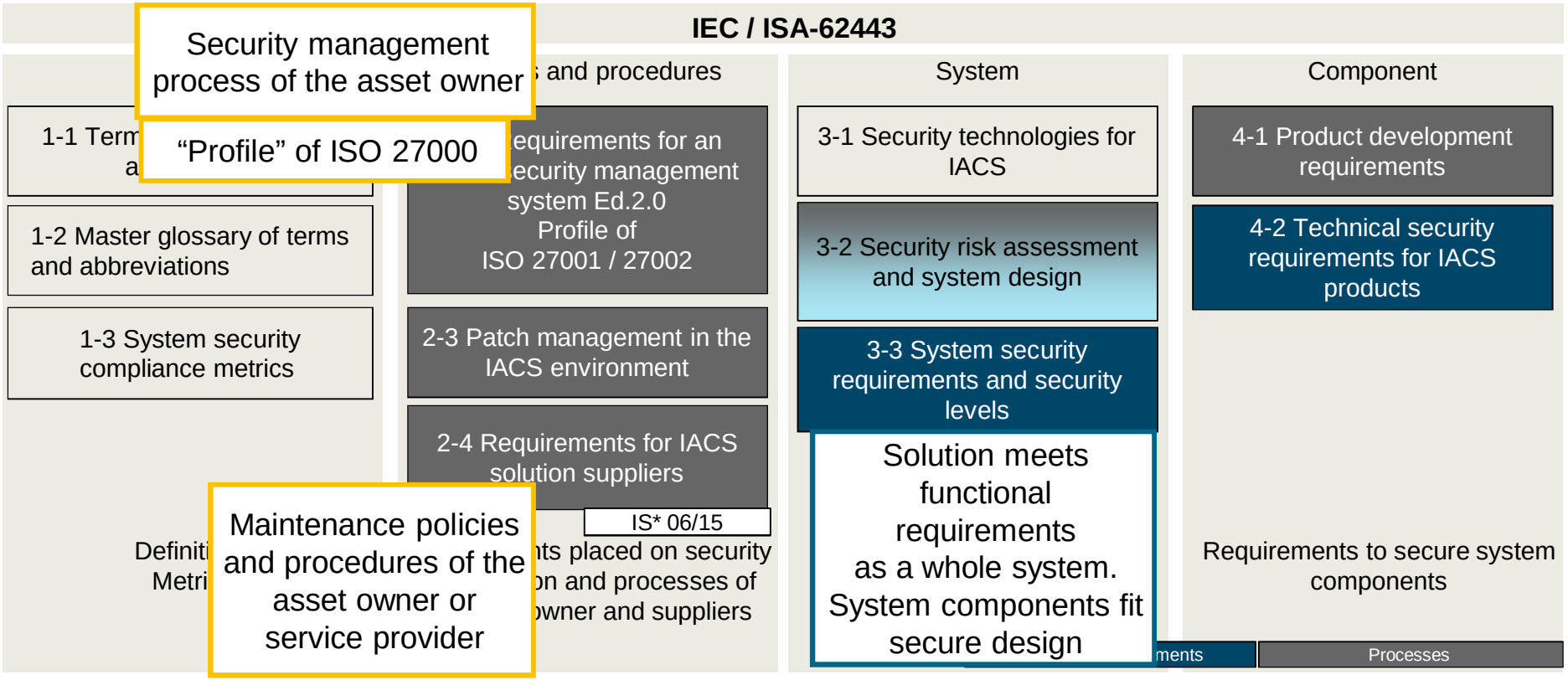
IEC 62443: Product Supplier View



IEC 62443: System Integrator View



IEC 62443: Asset Owner View



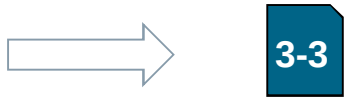
Why such standards at all?

Cybersecurity Myths

- "My industrial networks are isolated, so I'm protected".
- "I use proprietary protocols and databases, so I'm protected.“
- "Cybersecurity will stop me from working the way I want to".
- "Cybersecurity is expensive".

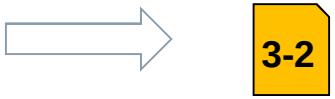
… and how to address them.

No remote access, enterprise network, USB?



Own crypto strong? Really hard to analyze?

Tested desaster recovery procedures?



Better do cyber security risk analysis?

Source: ANSSI, „Managing Cyber Security for Industrial Control Systems“, v1.0, June 2012.

IEC 62443-3-3 Foundational Requirements (FRs)

Foundational Requirements (FRs)
FR 1 – Identification and authentication control
FR 2 – Use control
FR 3 – System integrity
FR 4 – Data confidentiality
FR 5 – Restricted data flow
FR 6 – Timely response to events
FR 7 – Resource availability

Detailed example: IEC 62443-3-3 SR 1.1

- **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 […]

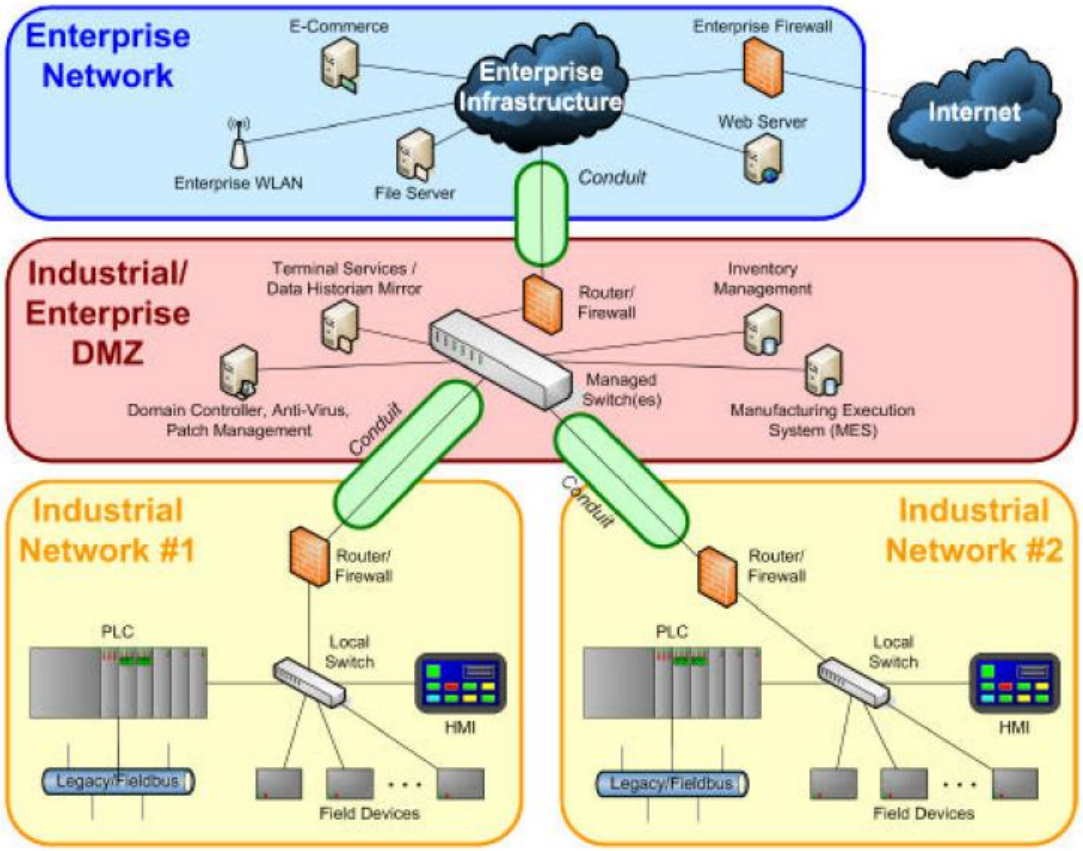
- **Requirement enhancements**
- SR 1.1 RE 1 – Unique identification and authentication
- SR 1.1 RE 2 – Multifactor authentication for untrusted networks
- SR 1.1 RE 3 – Multifactor authentication for all networks

- **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)

Zones and Conduits (IEC 62443-3-2)

- **Zone** – Group of logical or physical assets sharing common security requirements
- **Conduit** – Logical grouping of communication channels, connecting two or more zones, that share common security requirements

- Zones and conduits are e.g. established by grouping assets based on
  - functionality,
  - location,
  - responsible organization,
  - the result of a risk assessment.



IEC62443-2-4: Functional Areas, Topics

Functional Area	Topic
SP01 Solution Staffing (e.g. trained Staff, Security Contacts)	Training
	Background checks
	Personnel assignments
SP02 Assurance (e.g. security testing, hardening guides)	Solution components
	Security tools and software
	Hardening guidelines
SP03 Architecture (e.g. secure NW design deployed, hardening, Vulnerability handling)	Risk assessment
	Network design
	Solution components
	Devices - all
	Devices - workstations
	Devices - network
	Data protection

Functional Area	Topic
SP04 Wireless	Network design
SP05 SIS (specific requirements for safety-instrumented systems and wireless)	Risk assessment
	Network design
	Devices - workstations
	Devices - wireless
	User interface
SP06 Configuration Management (config documentation, inventory)	Network design
	Devices – all
	Devices - control and instrumentation
SP07 Remote Access (secure, approved, documented remote access solution)	Security tools and software
	Data protection

IEC62443-2-4: Functional Areas, Topics (continued)

Functional Area	Topic
SP08 Event Management (e.g. logging configuration, Incident handling)	Events - Security compromises
	Events – Security related
	Alarms & Events
SP09 Account Management (e.g. administration, centralized, policy config, documentation)	Accounts - User and service accounts
	Accounts – Administrator
	Accounts – Default
	Accounts – User
	Passwords

Functional Area	Topic
SP10 Malware Protection (e.g. installation, signature updates, portable media)	Manual process
	Security tools and software
	Devices – All
	Portable media
SP11 Patch Management (e.g. process, ensure up-to-date system, follow operator policies)	Manual process
	Patch list
	Security patch
SP12 Backup / Restore (e.g. backup procedures, capabilities, disaster recovery plan)	Manual process
	Restore
	Portable media
	Backup

IEC 62443-2-1

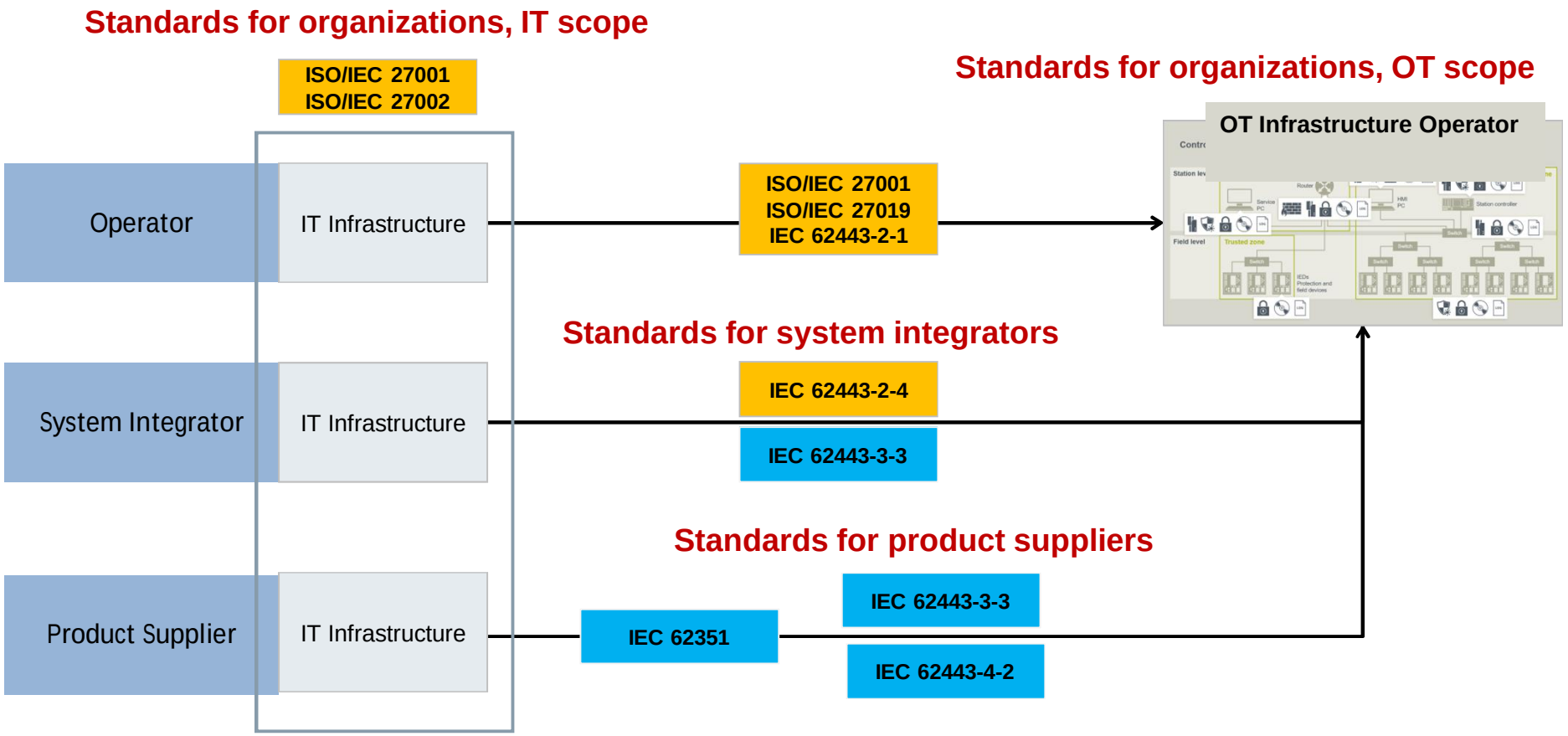
The IEC 62443-2-1 specification:

- Is based on ISO/IEC 27001:2013 and 27002:2013
- IACS – SMS: Describes implementation, management, operation of an IACS (industrial automation control system) security management system
- Requirements largely address policies, procedures, practices, personnel

Main content:

- **Additions to ISO/IEC 27001**
  - e.g. related to information security risk management
- **Guidance for ISO/IEC 27002 controls**
  - Example: Clarify “teleworking” in the context of remote access to industrial deployments
- **Extended set of specific controls for industrial automation**
  - Example: centralized vulnerability monitoring

Relation between IEC 62443 and ISO/IEC 27000

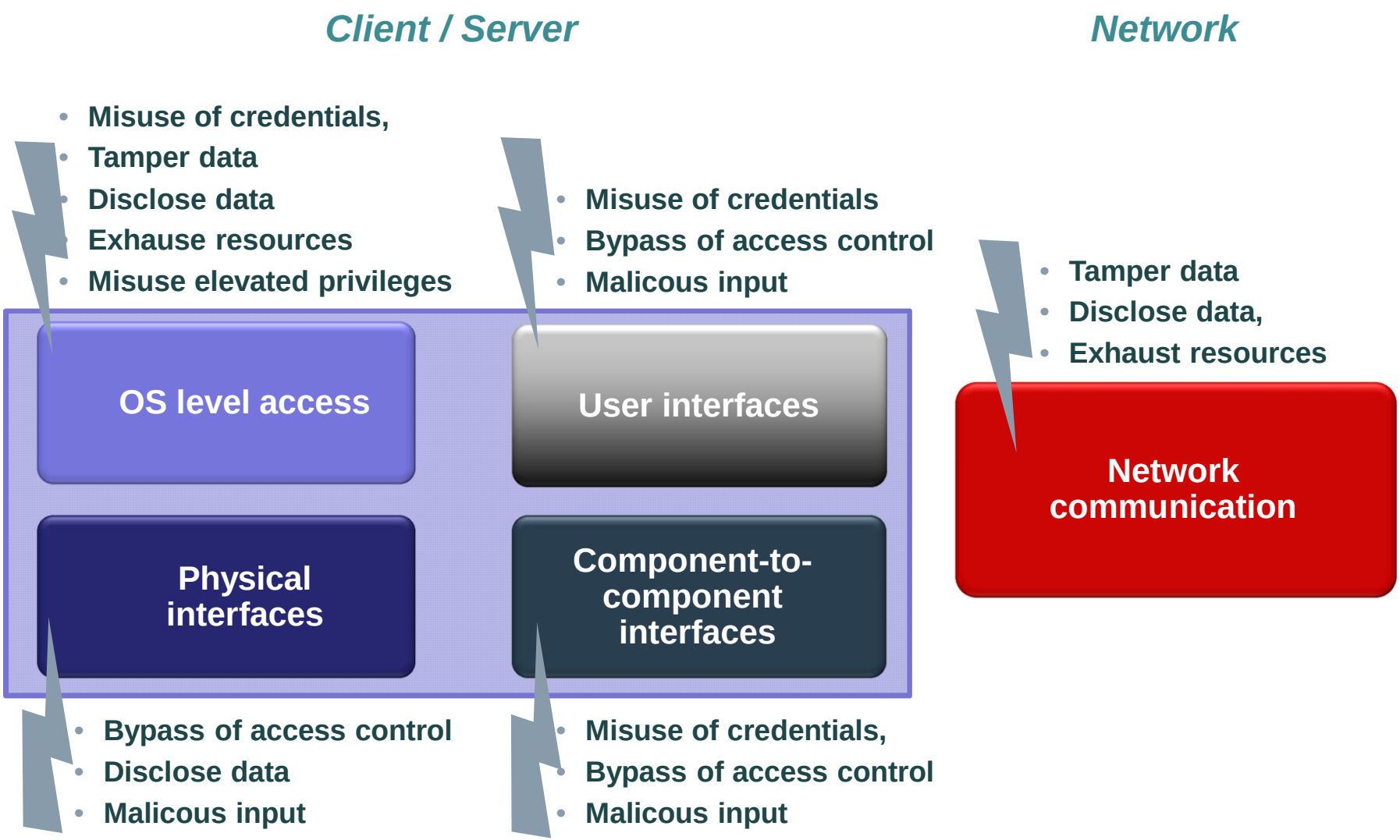


Tutorial Agenda

Agenda

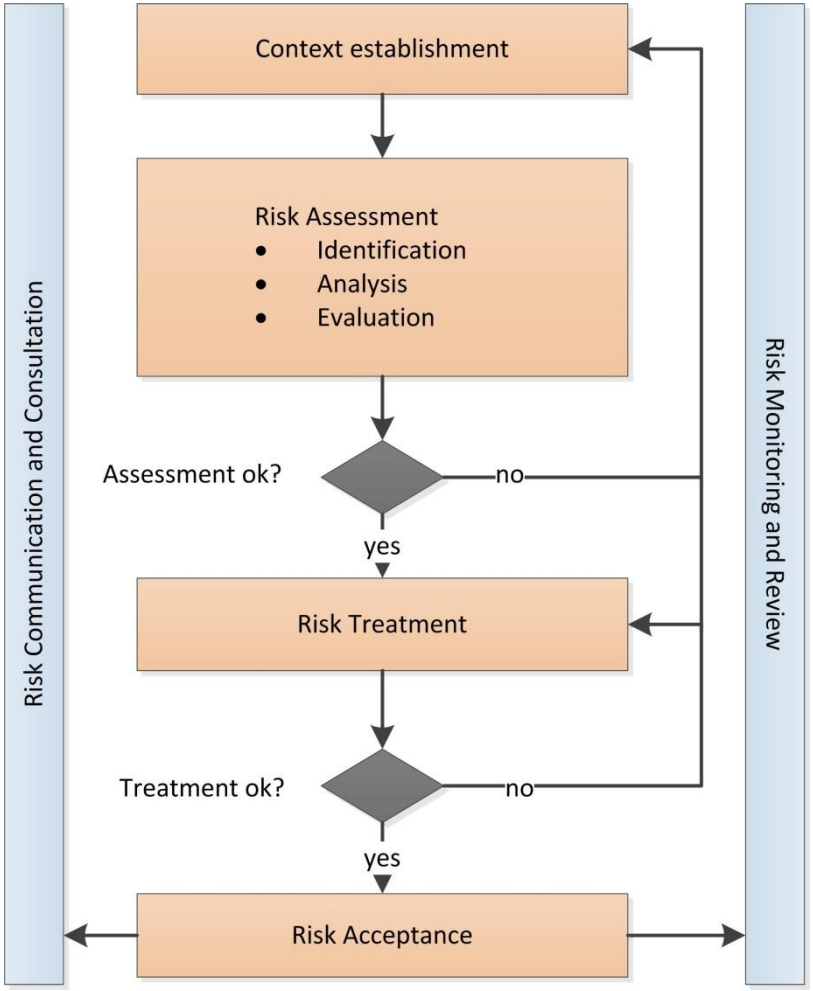
- Motivation and Threat Landscape
- Cyber Security Standards
- **Risk Driven Approach**
- Realization Approaches
- Summary and Outlook

Goal: analyze possible attack actions, understand risks



Security Risk Management

- Security Standards like ISO/IEC 27k and IEC 62443 require
  - establishment of a systematic security risk management approach
  - performing it as a continuous process
- Risk analysis is a key step: Implementations of security controls need to be risk based
- Risk management procedure details are not mandated, but best-practices are available
- Risk analysis methods for IT/OT security can be adapted to many different types of organizations
- Risk analysis is required for all stakeholders
  - Product Supplier
  - System Integrator
  - Asset Owner

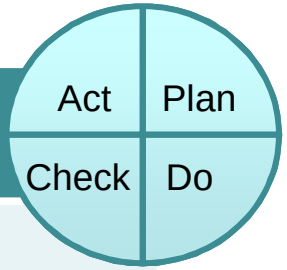


Risk management process based on ISO27005:2011

Risk Management along the PDCA Cycle

Continuous Improvement

ISMS Steps	Risk Management Steps
Plan	• Context establishment • Risk assessment • Develop risk treatment / risk acceptance
Do	• Risk treatment implementation
Check	• Continual monitoring of effectiveness • Review of risk
Act	• Maintain and improve security risk management process



Definition: Threat

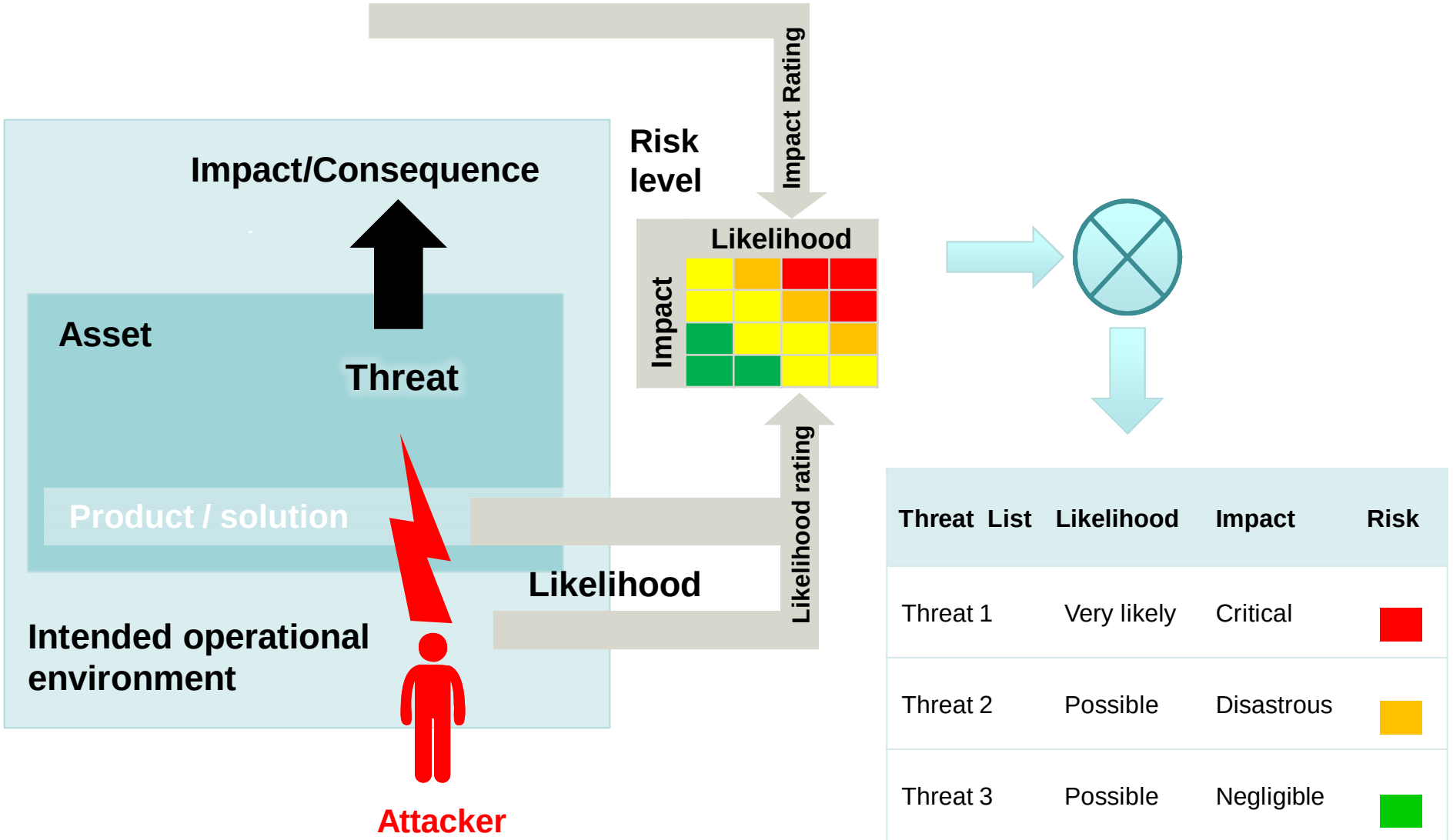
Threat	
A **potential cause** of an unwanted incident, which may result in **harm** to a system or organization.	ISO 27000
Potential for **violation of security**, which exists when there is a circumstance, capability, action or event that could breach security and cause **harm**.	IEC 62443
A threat is any circumstance or event with the **potential** to **adversely impact** organizational operations and assets, individuals […] through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.	NIST 800-30

Definition: Risk Evaluation

Level of Risk	
Magnitude of a risk , expressed in terms of the combination of **consequences** and their **likelihood**	ISO 27000

Risk Analysis / Risk Assessment	
Input: A list of identified relevant incident scenarios, including identification of threats, vulnerabilities, affected assets, consequences to assets and business processes. *Output*: List of risks with value levels assigned to all relevant incident scenarios	ISO 27005:2011
Process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources, quantfies loss exposures and consequences based on probability of occurrence […].	IEC 62443

Risk Assessment Methodology



Threat List	Likelihood	Impact	Risk
Threat 1	Very likely	Critical	
Threat 2	Possible	Disastrous	
Threat 3	Possible	Negligible	

Risk Treatment Options

Threat List	Likelihood	Impact	Risk
Threat 1	Very likely	Critical	
Threat 2	Possible	Disastrous	

Options to follow-up on risk assessment results

Risk modification	Risk retention	Risk avoidance	Risk sharing
• Introduce or modify security controls (techn. or procedure) • Example: Add firewall rule to block access to a vulnerable component	• Accept risk. Risk meets acceptance criteria • Example: Identified risk below threshold	• Avoid condition creating the risk • Example: Remove vulnerable component	• Share with another party • Example: Subcontractor, Insurance

Resulting Risk and Security Levels

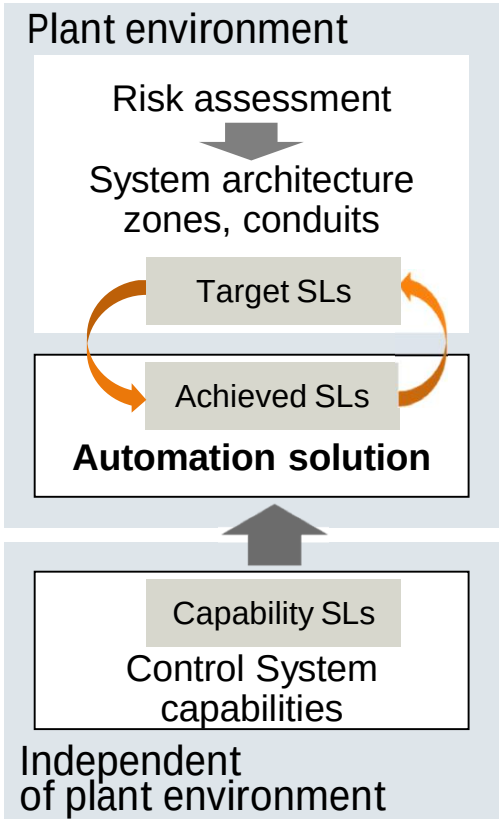
- To define appropriate security controls aligned with identified risks, „levels“ can be used

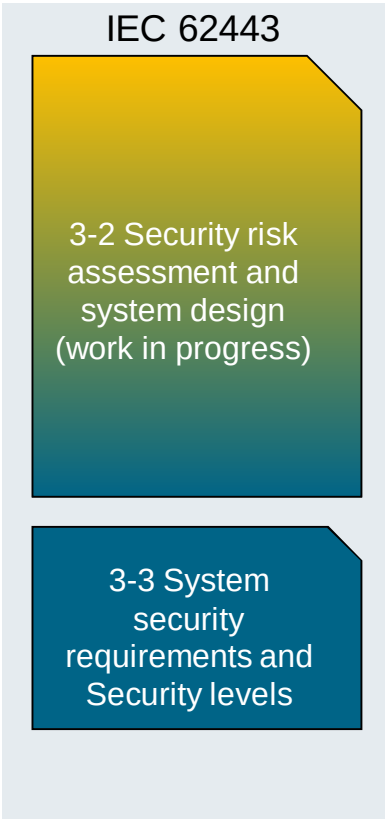
Name	Source	Function
Security Level	IEC62443-3-3	Organizes security requirements in security levels 1 up to 4 that build upon each other.
Maturity Level	IEC62443-2-4	Assign a maturity level to an organization (per requirement or requirements group?)
Maturity Level	CMMI (different definition)	Assign a maturity level to an organization. Select blocks of requirements in scope, depending on the targeted level
Bronze/Silver/Gold	WIB M 2784 X-10 (predecessor of IEC62443-2-4)	Bronze/Silver/Gold, organizes security requirements in three levels that build upon each other
...		

- Such „levels“, however, can mean quite different things

IEC 62443-3-3 Security Levels: Interrelation

SL 1	Protection against **casual or coincidental** violation
SL 2	Protection against **intentional violation** using **simple means** with low resources, generic skills and low motivation
SL 3	Protection against intentional violation using **sophisticated means** with **moderate resources**, IACS specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with **extended resources**, IACS specific skills and high motivation

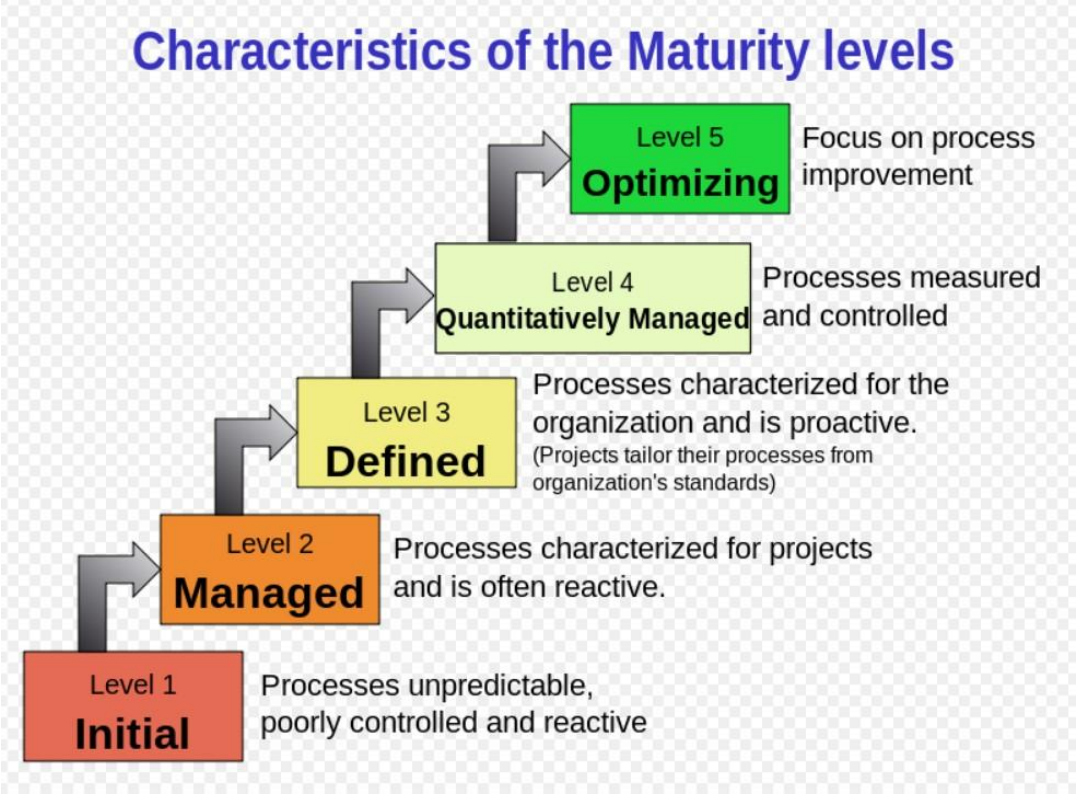




Measures to address gaps between target and achieved
SL can be of technical or organizational nature

How to measure process compliance

- Security Levels of IEC 62443-3-3 relate to technical capabilities
- Established approach for process / organizational evaluation: Maturity Levels



IEC 62443-2-4
Improving
Defined (Practiced)
Managed
Initial

Source: http://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration

Tutorial Agenda

Agenda

- Motivation and Threat Landscape
- Cyber Security Standards
- Risk Driven Approach
- **Realization Approaches**
- Summary and Outlook

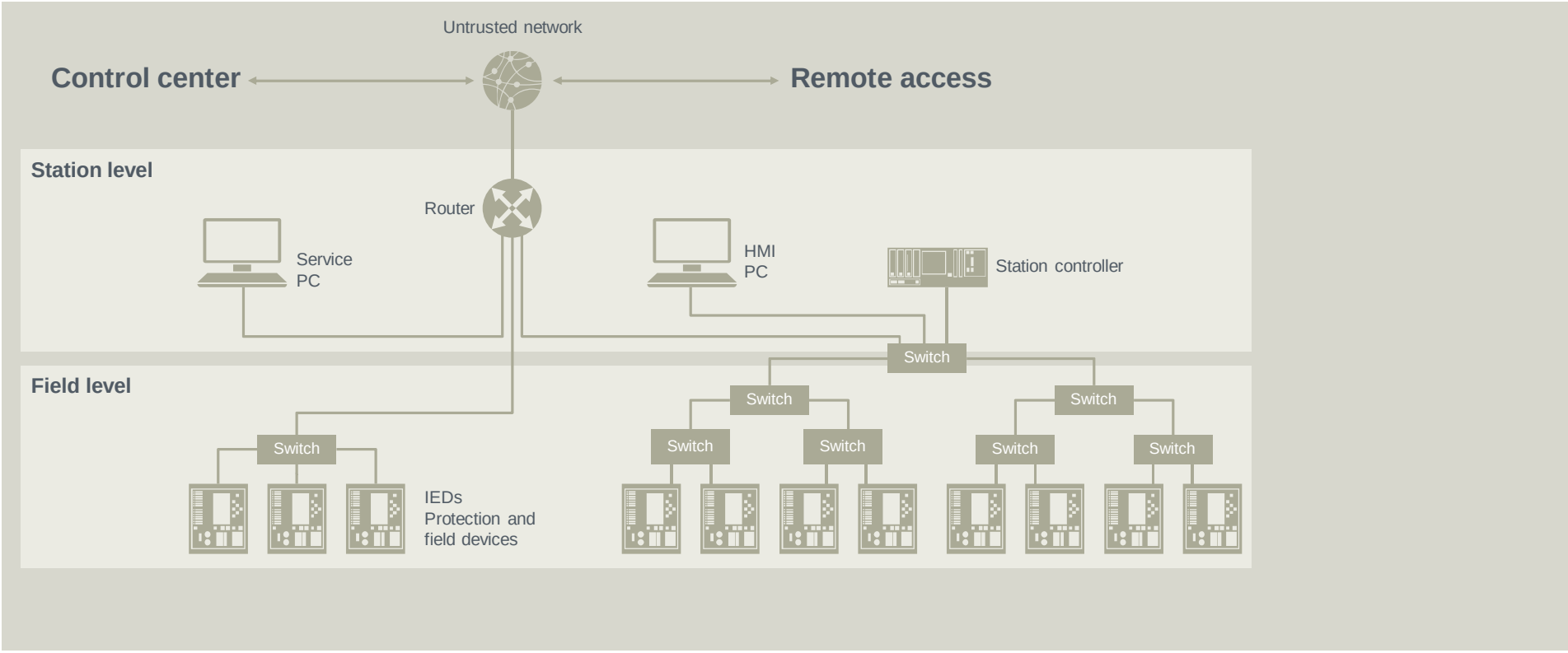
How to address IEC 62443-3-3

- **The specification requirements need to be met by the control system**
  - **"[..]** it is **not necessary that every component** of the proposed control system support every system requirement to the level mandated in this standard. **[..]"**
  - 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."**

- **The specification does not limit realization options. It describes what is required, but does not describe (or limit) how this can be achieved.**

- **Adapted requirements at component level can be found in IEC 62443-4-1 for:**
  - **Embedded devices (e.g., PLC, IED)**
  - **Host devices (e.g., operator workstation, engineering workstation)**
  - **Network devices (e.g., switch, router, firewall, access point)**

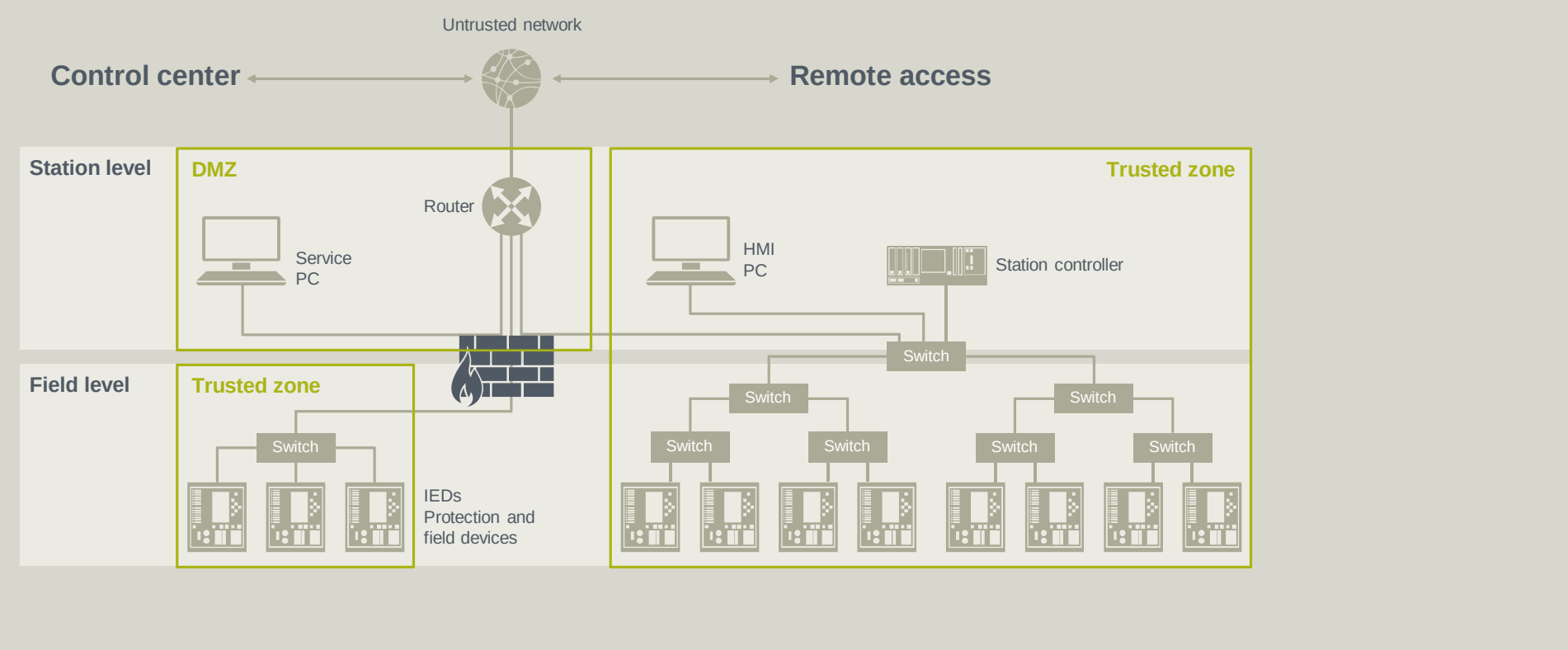
Example: Substation Automation



Network Segmentation in IEC 62443-3-3

FR 5.1 – Restricted Data Flow	SL 1	SL 2	SL 3	SL 4
FR 5.1 – Network segmentation	✔	✔	✔	✔
SR 5.1 RE 1 – Physical network segmentation		✔	✔	✔
SR 5.1 RE 2 – Independence from non-control system networks			✔	✔
SR 5.1 RE 3 – Logical and physical isolation of critical networks				✔
SR 5.2 – Zone boundary protection	✔	✔	✔	✔
SR 5.2 RE 1 – Deny by default, allow by exception		✔	✔	✔
SR 5.2 RE 2 – Island mode			✔	✔
SR 5.2 RE 3 – Fail close			✔	✔
SR 5.3 – General purpose person-to-person communication restrictions	✔	✔	✔	✔
SR 5.3 RE 1 – Prohibit all general purpose person-to-person communications			✔	✔
SR 5.4 – Application partitioning	✔	✔	✔	✔

Security Zones with Protection at Zone Borders



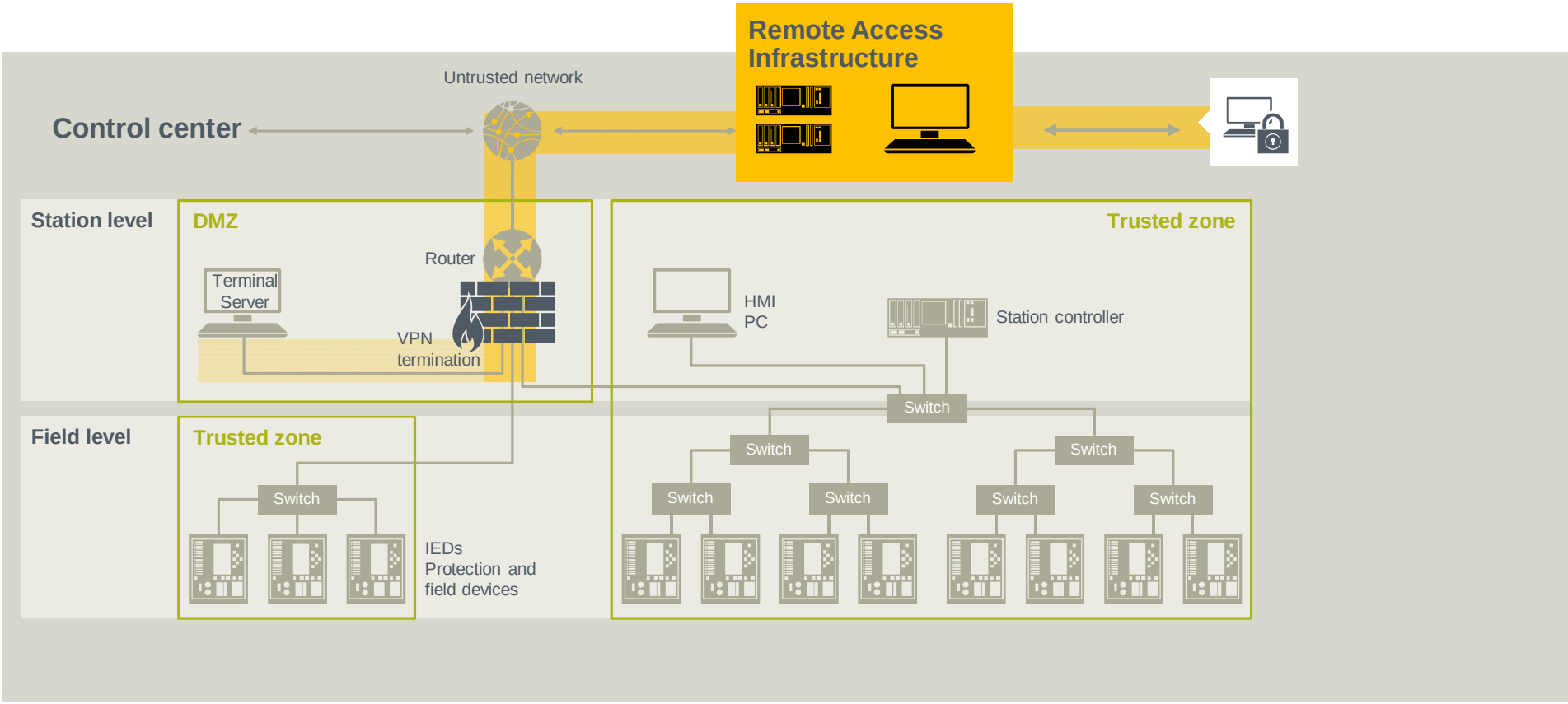
Introducing secure zones (SR5.1, SR5.2):

- All traffic in and out must pass through the de-militarized zone (DMZ)
- Within the substation network, one or more trusted zones (IP subnetworks) are configured
- Separation via switches (VLAN) at layer 2, and via Firewall at layer 3
- If communication through DMZ fails, substation automation will continue on its own

Authentication in IEC 62443-3-3

FR 1 - Identification and Authentication Control	SL 1	SL 2	SL 3	SL 4
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			✔	✔

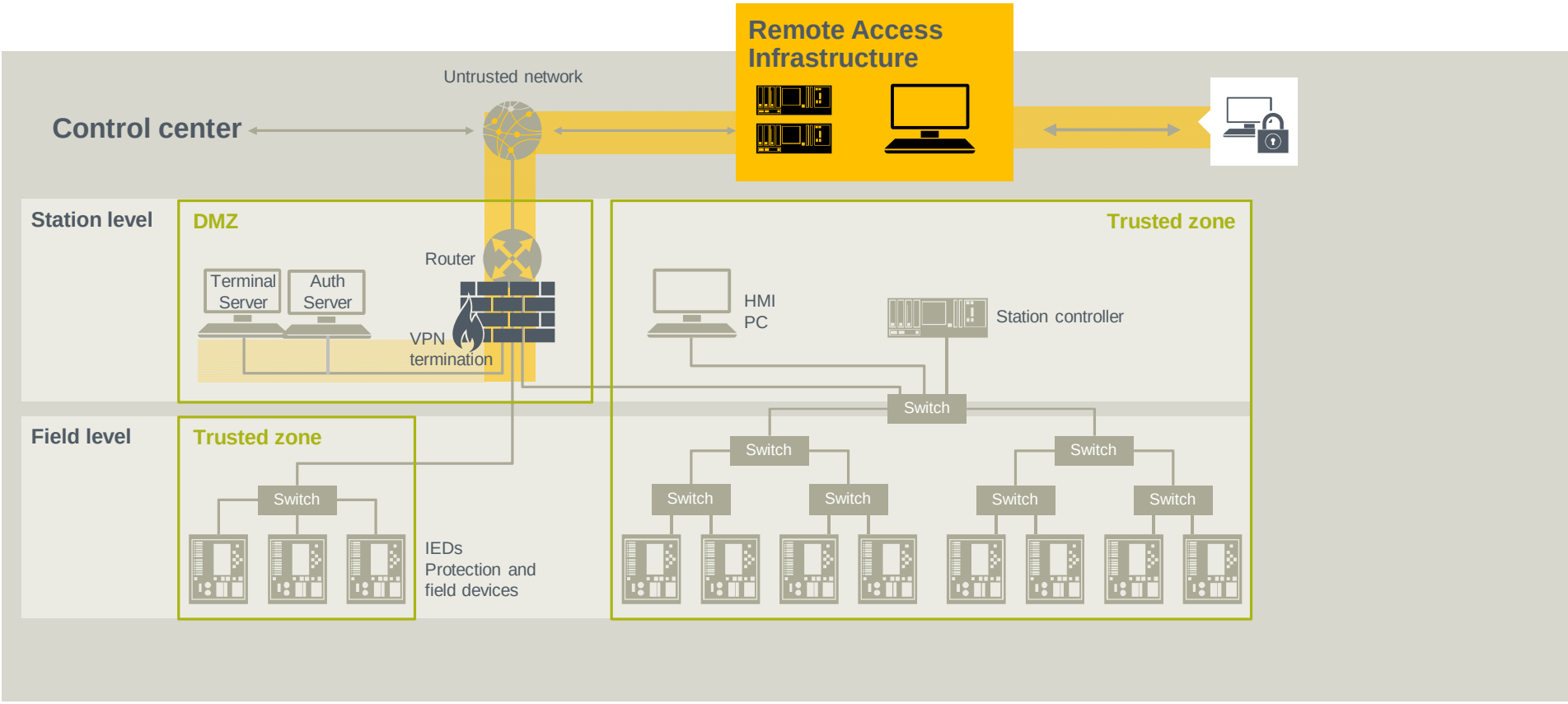
Places for User Authentication



Remote access introduces additional users:

- Authentication can theoretically be realized in different places: externally, in the DMZ, or directly at the substation devices (e.g. HMI)
- Unique user authentication can be enforced locally by a terminal server in the DMZ

Centralized User Authentication



Centralized user management:

- For unified and centralized management of accounts and account-related security policies, an authentication server (e.g. Active Directory Domain Controller for Windows) can be used.
- Accounts for network devices can be managed through RADIUS.
- Not mandatory, but improved security and reduced management effort as soon as more than a few machines need to be covered

Tutorial Agenda

Agenda

- Motivation and Threat Landscape
- Cyber Security Standards
- Risk Driven Approach
- Realization Approaches
- **Summary and Outlook**

Summary and Outlook

- Cyber security threats are real. Threats need to be addressed by implementing both organizational and technical capabilities that are appropriate and effective.
- It is important for all stakeholders to establish security risk management procedures that ensure appropriate realizations that implement security controls.
- Appropriate realizations vary based on the actual system and its operational environment. However, they need to consider the state-of-the-art. Hence, appropriate realizations will evolve over time.
- The IEC 62443 security standards framework provides security requirements that address all involved stakeholders along the lifecycle. Integration with ISO/IEC 27000 is possible.

Sources for further information

- ISA-99 62443 document overview with draft versions: http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx
- CEN-CENELEC-ETSI, Smart Grid Coordination Group, “SG-CG/M490/H_Smart Grid Information Security”, December 2014.
- SG-CG/M490/D_ Smart Grid Information Security ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Security.pdf
- ISO/IEC 27001: Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27002: Information technology — Security techniques — Code of practice for information security management
- ISO/IEC 27005: Information technology — Security techniques — Information security risk management
- ISO/IEC TR 27019: Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
- IEC 62443-2-4: Security for industrial automation and control systems - Network and system security - Part 2-4: Requirements for Industrial Automation Control Systems (IACS) solution suppliers
- IEC 62443-3-3: Security for industrial automation and control systems, Part 3-3: System security requirements and security levels
- IEC 62443-4-2: Security for industrial automation and control systems, Part 4-2: Technical Security Requirements for IACS Components
- IEC TC 57 WG 15, IEC TS 62351 suite, see http://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID:1273
- IEC TC 57 WG 15, TS 62351-12, “Resilience and Security Recommendations for Power Systems with DER”, under development.

Sources for further information

- Bulletin d'Information d'ISA France, ISA FLASU no. 62, Patrice Bock et al, "A forensic analysis of the cyber-attack on the Ukrainian power", December 2016.
- German IT security law, BSI Information (German language only):
- https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/it_sig_node.html
- A. Polyakov, M. Geli, "SAP Cybersecurity for Oil and Gas", ERPScan Whitepaper presented at Blackhat Europe, Nov. 2015

Authors

- **Dirk Kroeselberg** received a diploma degree in Mathematics and Computer Science from the University of Giessen, Germany, in 1997. He worked for Siemens and Nokia Siemens Networks on a broad range of security topics and technologies, including smartcards, and mobile telecommunication networks. Joining Siemens Corporate Technology in 2011, he currently works as principal key expert in the field of security in industrial environments, critical infrastructures, and energy automation.
  dirk.kroeselberg@siemens.com

- **Frederic Buchi** received an engineer degree in Communication Engineering from ESSTIN (Ecole Supérieure des Sciences et Technologies de l'Ingénieur de Nancy/France) in 2000. Following a first position at Alcatel, his involvement with power utilities started in 2003 as a Technical Project Manager for turn-key communication networks at Alstom. Since 2008 he works at Siemens' HQ in Germany in the areas of product lifecycle management, business development and is currently responsible for Siemens Cyber Security solutions for protection and control system in Digital Grids Systems, where he passionately addresses this dynamic topic, both within Siemens and customers, especially focusing on defining and implementing challenging cyber security measures on the OT side to comply with international and industry standards..
  frederic.buchi@siemens.com

- **Hans Meulenbroek** graduated in 1985 from the HTS Hilversum, the Netherlands with a bachelor degree (Ing.) in Electrical Engineering. From 1987 he worked for Rossmark Water Treatment as process automation engineer and manager process automation department. In 1997, he joined Eaton Electric in the role of application engineer/SCADA specialist, followed by Product Manager responsible for LV Switchgear & MCC, Motor Management Systems and Smart Grid Automation solutions. In 2014 he joined Siemens as Proposal Expert Energy Automation.
  hans.meulenbroek@siemens.com