Network Security

Industrial Security

Prof. Dr. Henning Trsek, Institute Industrial IT

Agenda of todays lecture

- **Why Security in isolated systems?**
- **Typical vulnerabilities and threats in industrial systems**
- **Commonalities and differences**
- **Best practices and Standards**
  - IEC 62443
  - VDI 2182 – procedure model
  - Case Study of applying VDI 2182

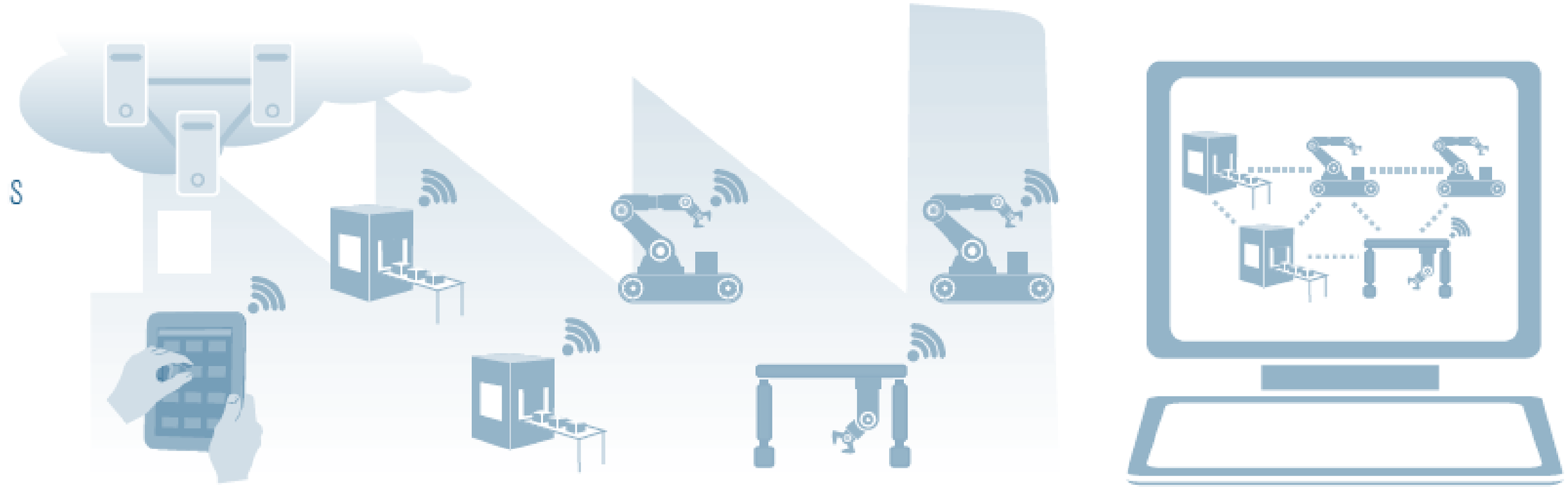
Any idea why Security is also important in industrial systems?

Go to **www.menti.com** and use the code **2577 3508**

Why is Security also important for industrial systems?

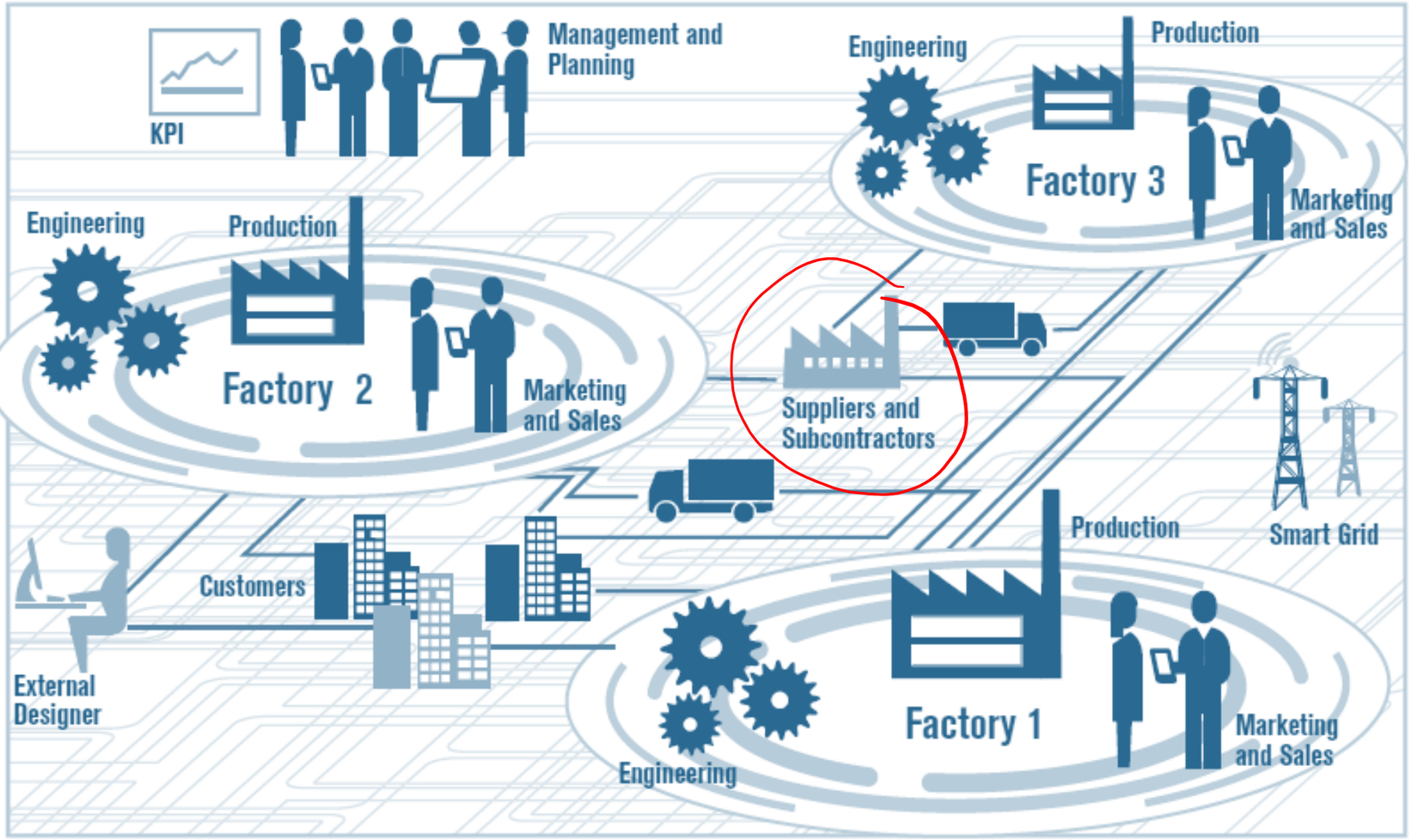
Mentimeter

- **Intelligent autonomous production units**
- **Standardized IT components**
- **Connected to each other and the Internet**



Source: Siemens 2013

Industry 4.0 means ubiquitous networking



Source: Hewlett Packard 2013

- Everything is connected
- Vertical and horizontal integration
- Smart and connected products
- Availabel data is used to monitor all plants

Attacks on Industrial Control System are on the rise

Cyber-Angriff auf Stahlwerk: Hochofen in undefiniertem Zustand

Auch die industrielle Produktion wird durch eine stärkere Vernetzung sensibler für Cyber-Attacken, mit teilweise dramatischen Folgen: Hacker haben den Hochofen eines Stahlwerks unter ihre Kontrolle gebracht und dabei massive Schäden verursacht. Die Kenntnisse der Angreifer gingen hierbei weit über die Kenntnisse der klassischen IT-Sicherheit hinaus und umfassten detailliertes Fachwissen über die eingesetzten Industriesteuerungen und Produktionsprozesse.

BSI, Cyber-Security Report 2014

Stuxnet-Worm controls industrial plants

Stuxnets final goal is to reprogram industrial control systems (ICS) by modifying PLC code without informing the operator of the ICS. It specifically manipulates Siemens WinCC Software for SCADA systems.

Heise

Havex

Dieser Angriff verlief über manipulierte Webseiten der Hersteller von industriellen Steuerungssystemen, sodass eine mit Havex infizierte Firmware für die Geräte von den Angreifern zur Verfügung gestellt werden konnte. Sobald ein Betreiber seine Geräte aktualisierte, wurde die Schadsoftware ebenfalls installiert. Sie sammelt gezielt Informationen über das Produktionsnetz und leitet diese an die Angreifer weiter.

Belden

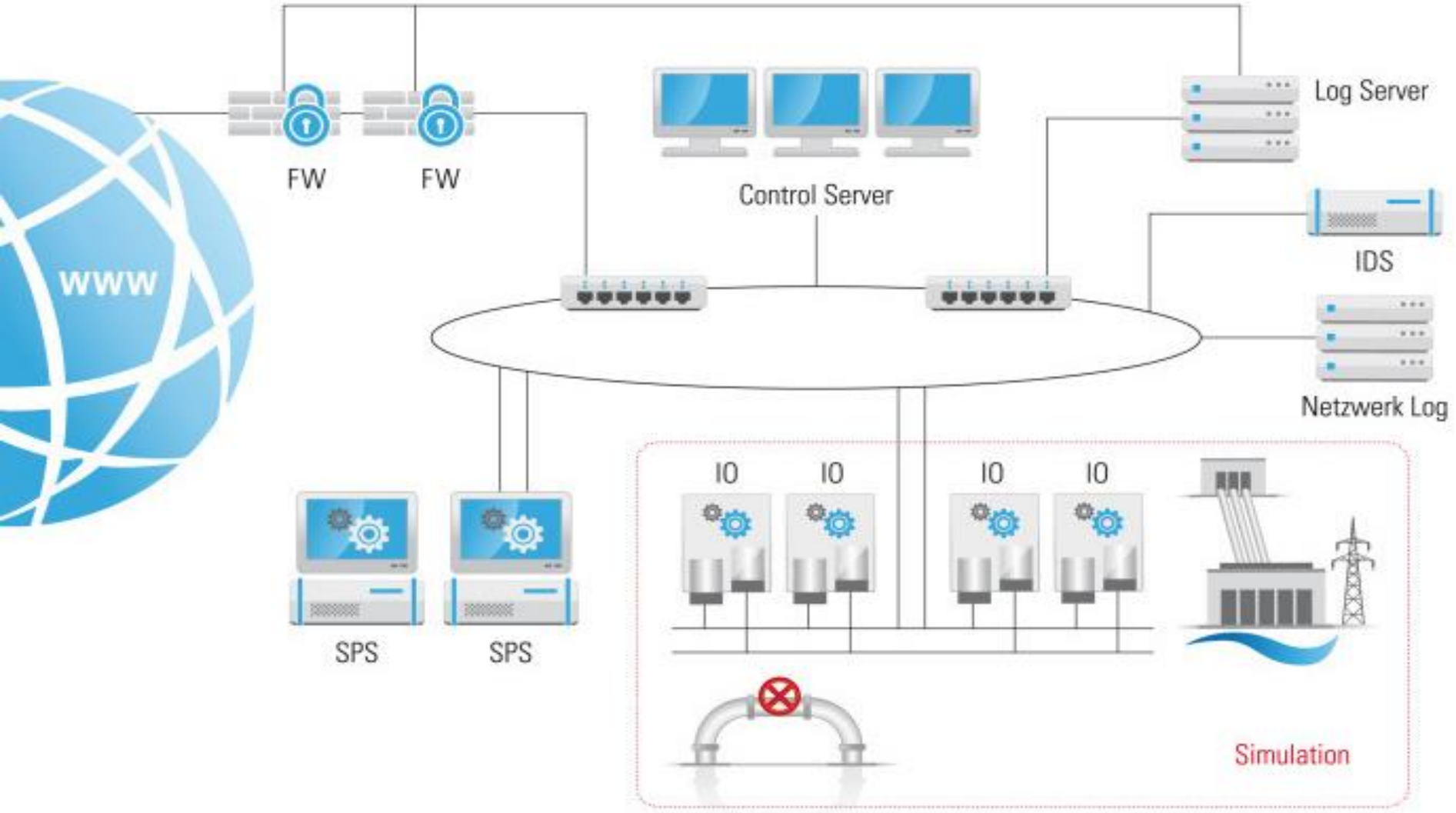
Maroochy Waste Water

More than 800.000 litres of untreated sewage intentionally released into parks, rivers, and hotel grounds. As a result a loss of marine life could be observed and the public health was jeopardized. Overall the incident caused costs of $ 200.000. The incident happened in Maroochy Shire Council in Queensland, Australia.

NIST

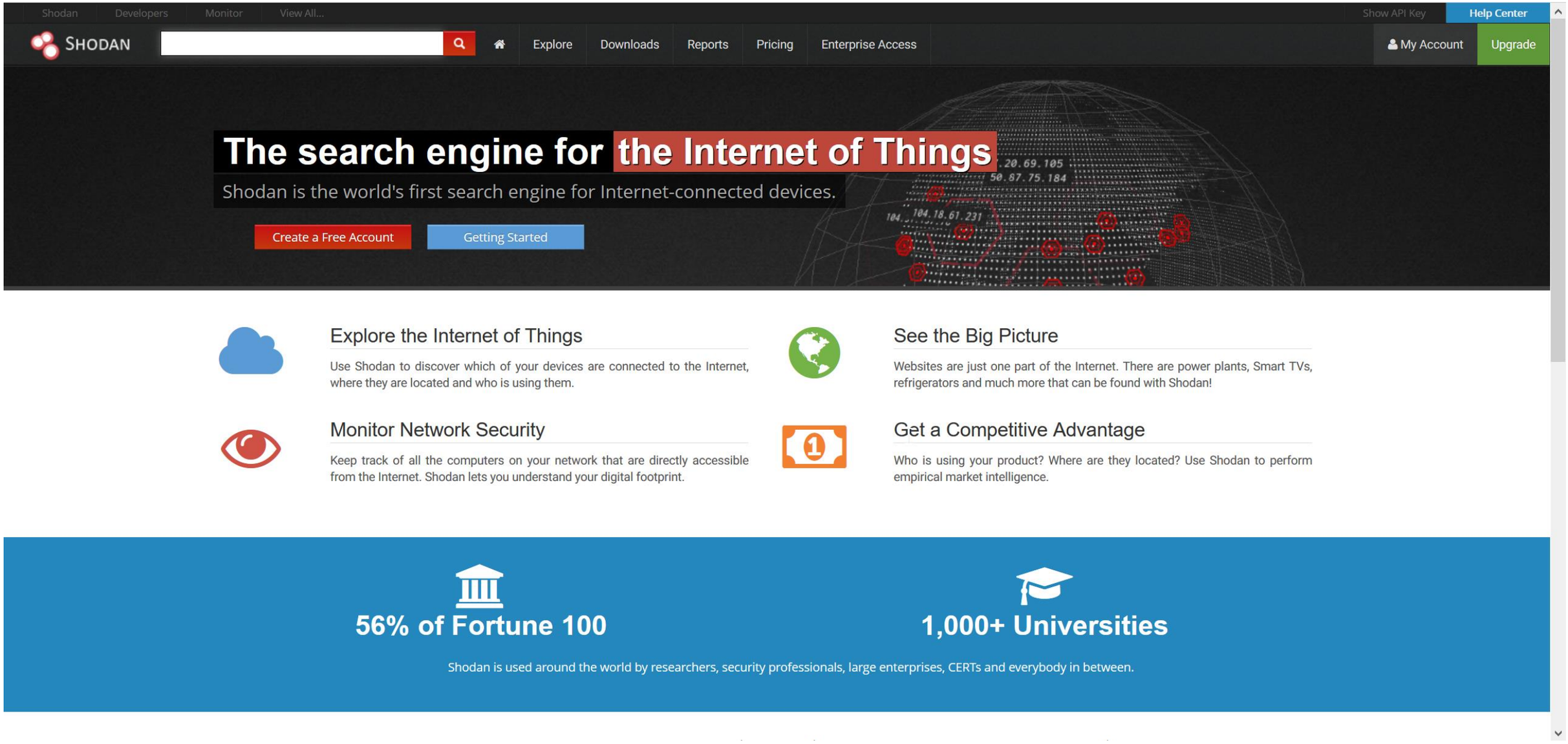
„The chain is no weaker than its strongest link"
Photo by ToHell, 2003-09-23 in Slagsta, SE

Honeynet: Logical structure



Source: TÜV SÜD

Have you ever heard about Shodan?



To sum it up

- **Worldwide attacks of ICS systems are reality**
- **If there is a connection to the Internet, it will be found**
- **Small companies are also in focus**
- **Standard protocols as well as very specific protocols are used**
- **Companies might become victims if not selected a priori**
- **Companies that are under observation could be attacked at a later stage**

Agenda of todays lecture

- Why Security in isolated systems?
- **Typical vulnerabilities and threats in industrial systems**
- Commonalities and differences
- Best practices and Standards
  - IEC 62443
  - VDI 2182 – procedure model
  - Case Study of applying VDI 2182

BSI Top Ten Threats on ICS

Critical threats	Scenarios
Malware Infection via Internet and Intranet	Exploitation of known weaknesses, manipulation of external web pages, untargeted malware
Introduction of Malware on Removable Media and External Hardware	Infected USBs, maintenance computers are infected
Social Engineering	Phishing, spear-phishing, unauthorised access
Human error and sabotage	Incorrect configuration, uncoordinated patching
Intrusion via remote access	Direct attack, indirect attack
Control components connected to the Internet	Retrieval of control components, exploitation of known weaknesses
Technical malfunctions	Defects of components, software errors
Compromised Smartphones	Theft or loss, attack on the Smartphone
Compromised Extranet or Cloud	Disruption of communication, insufficient external security mechanisms
DDoS attacks	Individual components of the systems

Common Security Gaps in Industrial Control Systems

- **Networks lack**
  - overall segmentation
  - antivirus protection
- **Open to well known vulnerabilities**
  - Standard OSs
  - No patch management
- **Most IP-based communications are not encrypted**
- **Limited or no logging within ICS systems**
- **No host based security controls are configured on these devices**
- **Many organizations still rely heavily on physical security measures**

- **No risk management**
  - No interface to the company risk management
- **No guidelines and standards**
  - Responsibilities are not clearly defined
- **Lack of financial planning**
  - Ongoing process, not once in the whole life cycle
- **Missing commitment of the management**
  - No policies available

Vulnerabilities – Operational level

- **No separation of ICS and Office**
- **Shared usage of admin accounts**
- **Remote access for third parties**
- **No IAM solutions in place**
- **Internet access points are not secured**
- **Security incidents are not addressed as required**
- **No change management**
- **Missing testing procedures and environments**

- **Encompass errors in Hardware, Software and network infrastructures**

- **Most challenging vulnerability level**
  - Huge amount of industrial devices
  - Lack of asset management

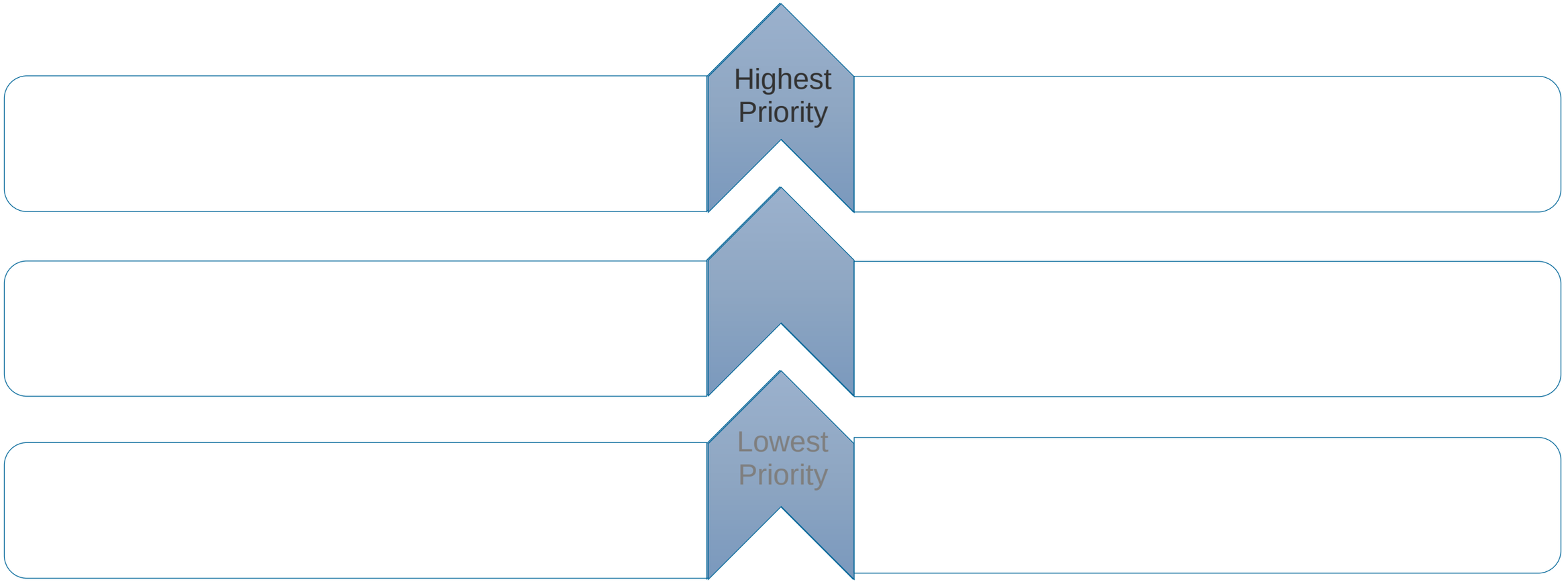
- **Research in common vulnerability databases reveals a very low number of ICS specific vulnerabilities**
  - Limited interest of Security researchers (up to now)

Agenda of todays lecture

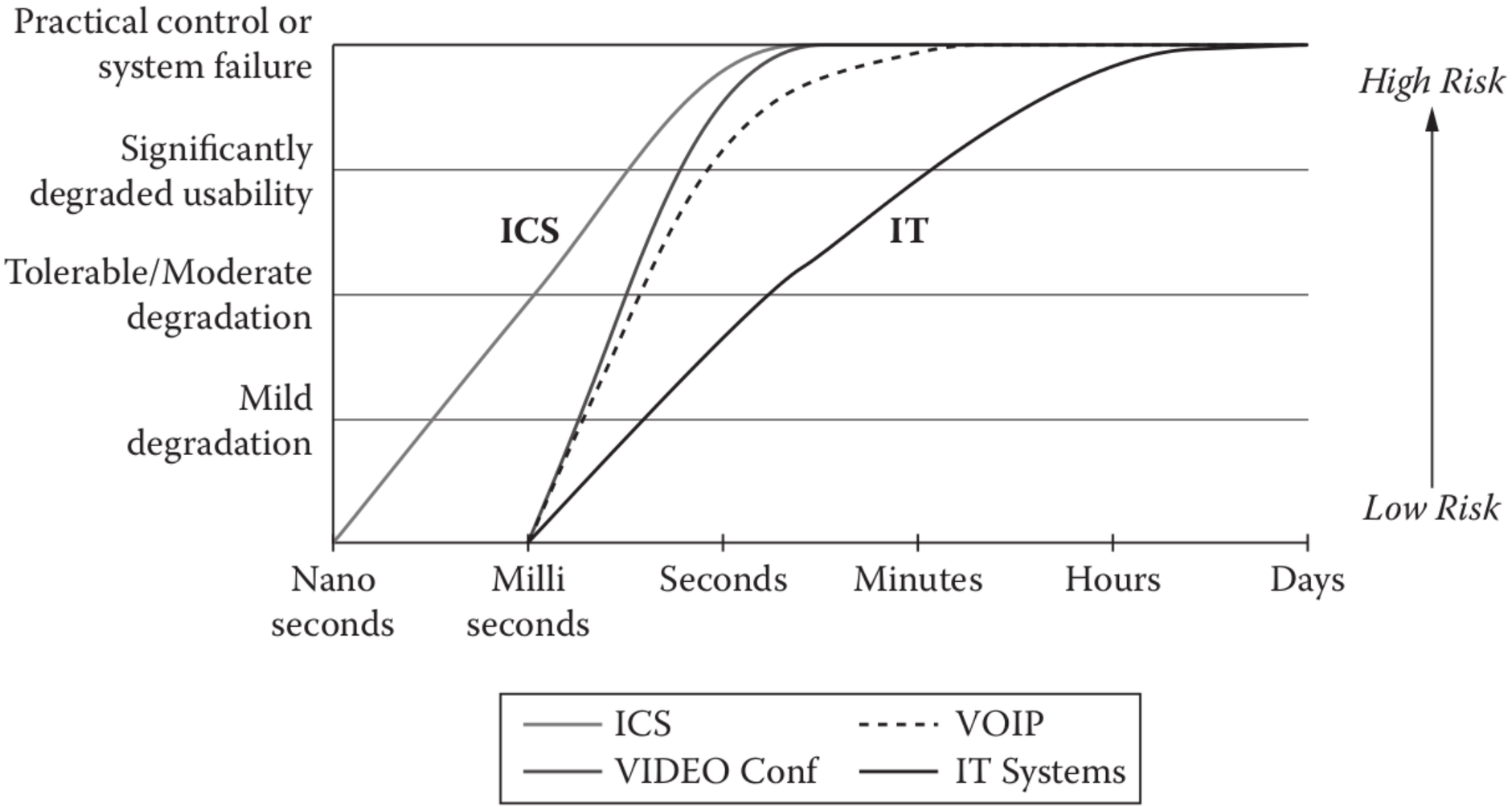
- Why Security in isolated systems?
- Typical vulnerabilities and threats in industrial systems
- **Commonalities and differences**
- Best practices and Standards
  - IEC 62443
  - VDI 2182 – procedure model
  - Case Study of applying VDI 2182

Industrial automation and control systems

General Purpose IT systems

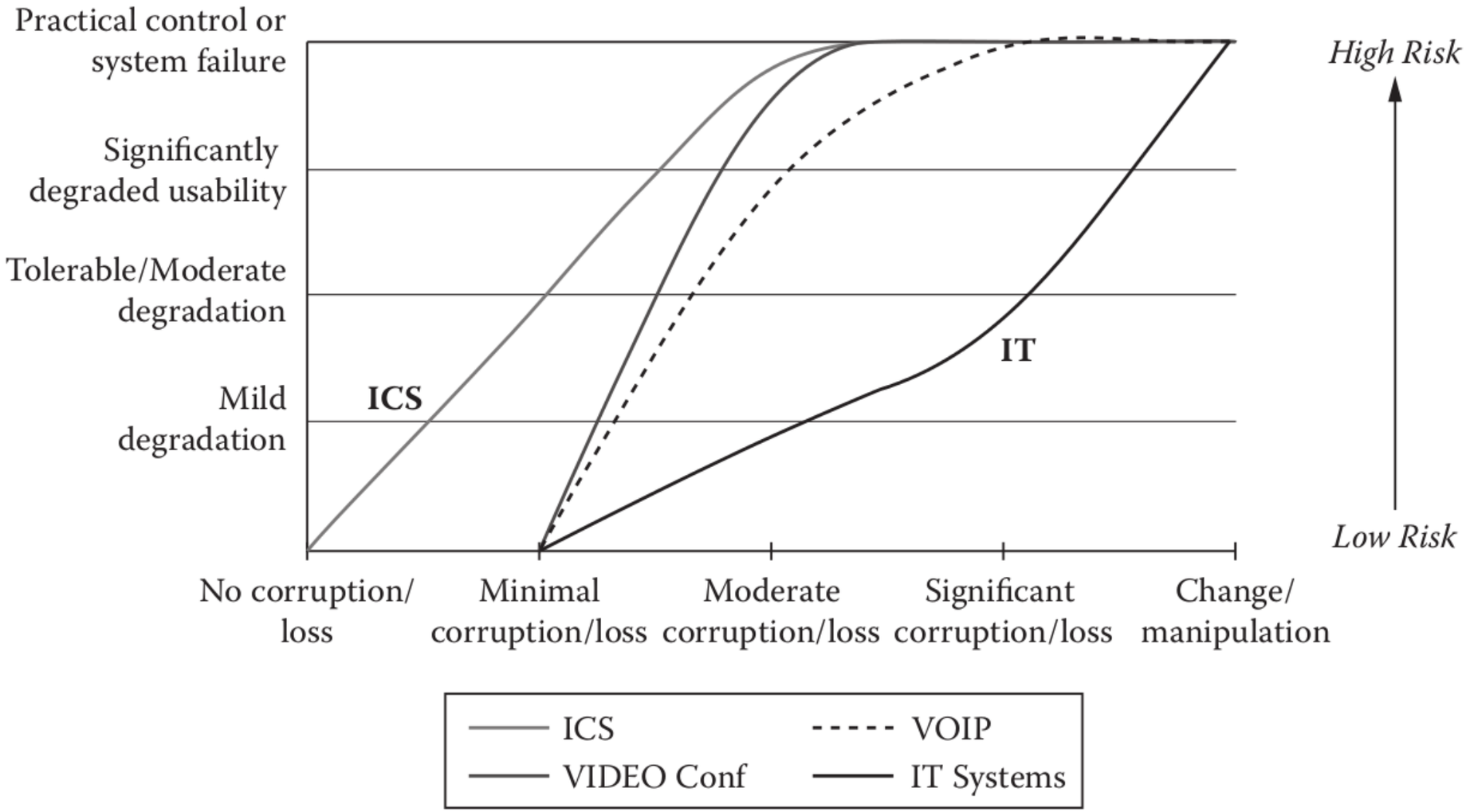


Security objectives comparison - Availability



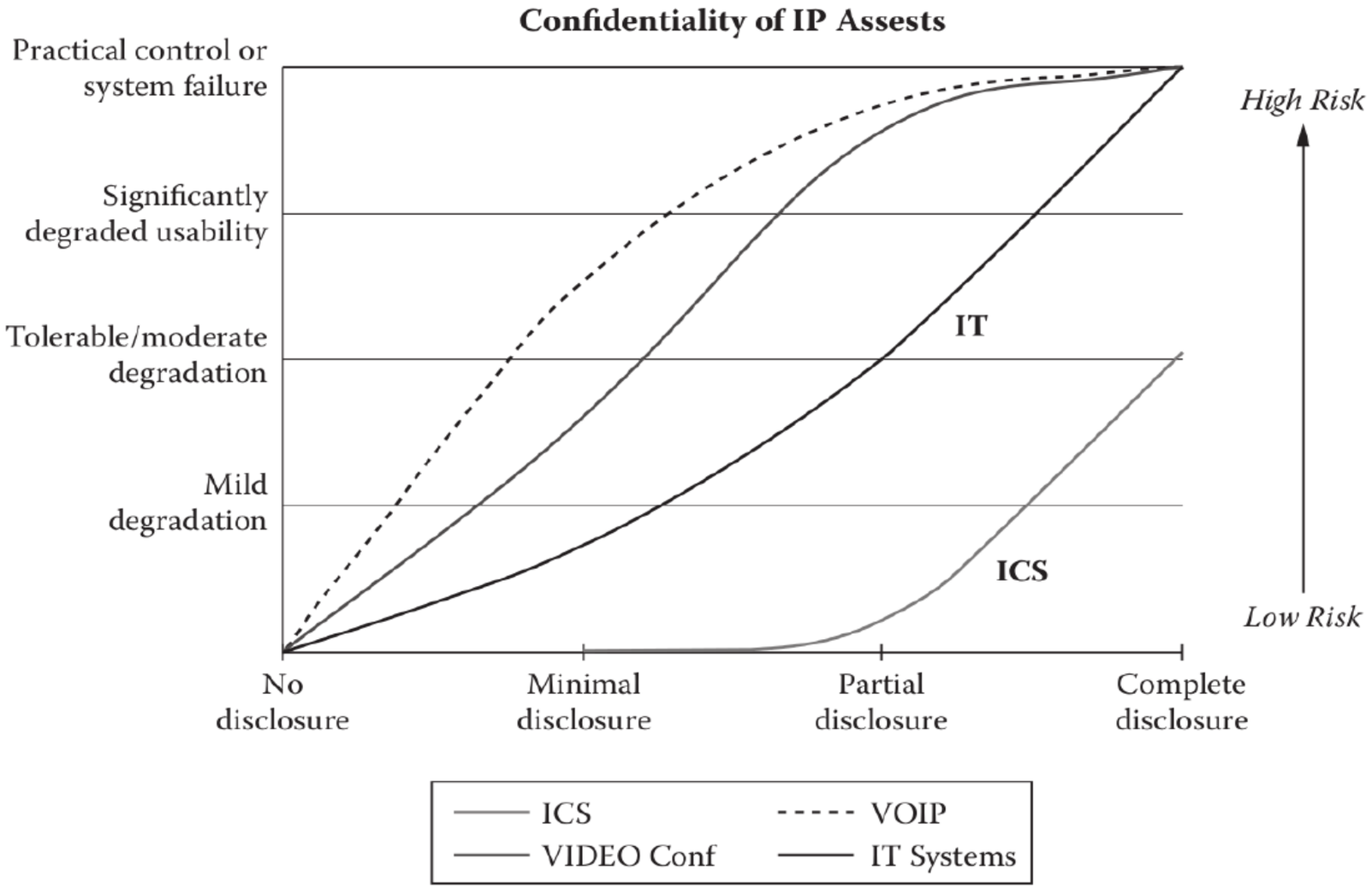
Source: Tyson Macaulay und Bryan Singer. *Cybersecurity for Industrial Control Systems - SCADA, DCS, PLC, HMI, and SIS*. CRC Press, 2012.

Security objectives comparison - Integrity



Source: Tyson Macaulay und Bryan Singer. *Cybersecurity for Industrial Control Systems - SCADA, DCS, PLC, HMI, and SIS*. CRC Press, 2012.

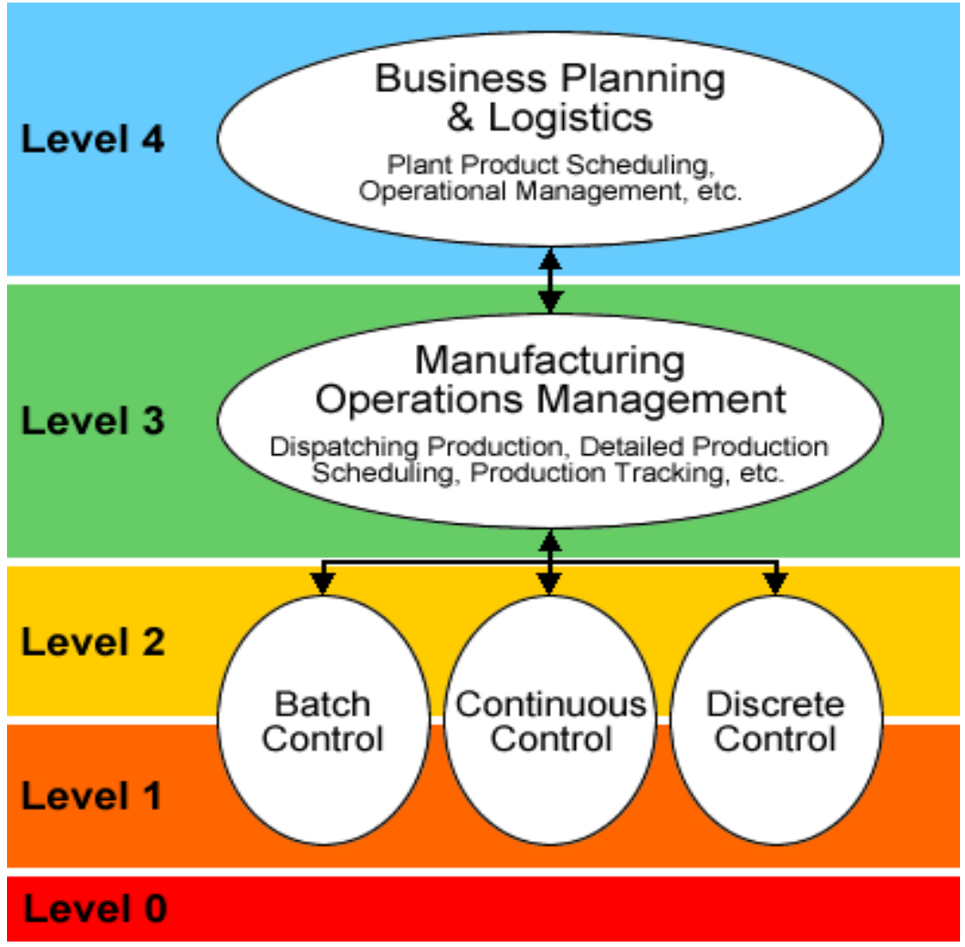
Security objectives comparison - Confidentiality



Source: Tyson Macaulay und Bryan Singer. *Cybersecurity for Industrial Control Systems - SCADA, DCS, PLC, HMI, and SIS*. CRC Press, 2012.

Enterprise Integration

ISA 95 / IEC 62264

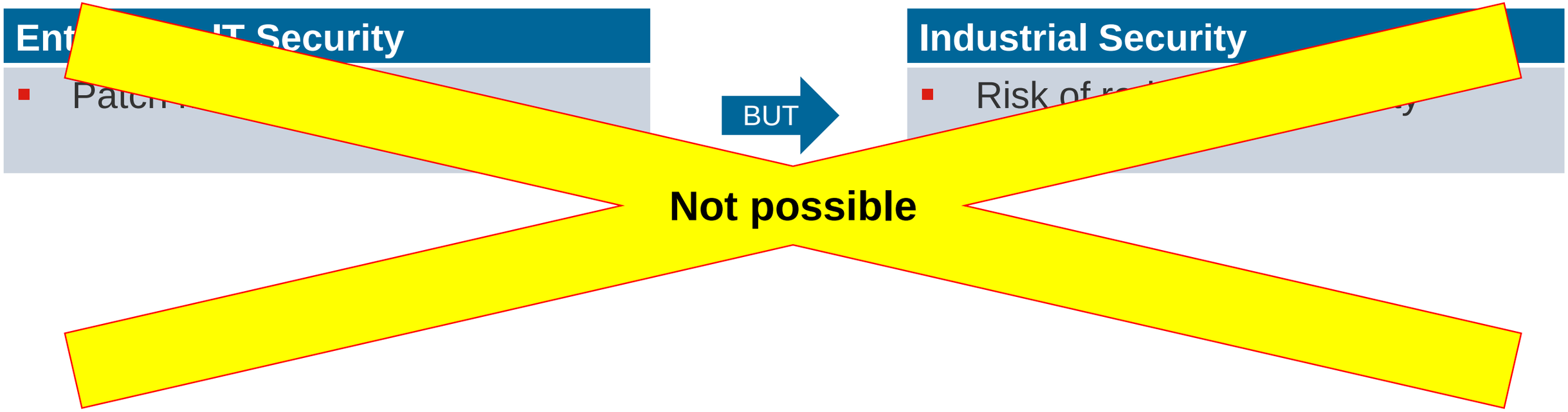


Typical responsibilities:

- **Enterprise IT**
  - IT security for all IT systems within the company
- **Production**
  - Plant operation incl.
    - DCS/MES Operation
    - “Automation Security”
    - Availability
    - Safety

Standard controls of IT security applied to manufacturing

Example: *Protection against Malicious Code*



IT Security and Industrial Security
… similar but not the same

Office IT Systems

Industrial Control Systems

Short-term

- Endangerment of public or employee safety
- Financial loss or impact incl. penalties (violation of regulatory requirements)

Mid-term

- Damage to the environment
- Impact on infrastructure

Long-term

- Damage to company image
- Loss of customer base or public confidence
- Loss of proprietary or confidential information

Agenda of todays lecture

- Why Security in isolated systems?
- Typical vulnerabilities and threats in industrial systems
- Commonalities and differences
- **Best practices and Standards**
  - IEC 62443
  - VDI 2182 – procedure model
  - Case Study of applying VDI 2182

7 easy steps to ICS security

Step 1
- Assess existing system

Step 2
- Document policies and procedures

Step 3
- Train personnel and contractors

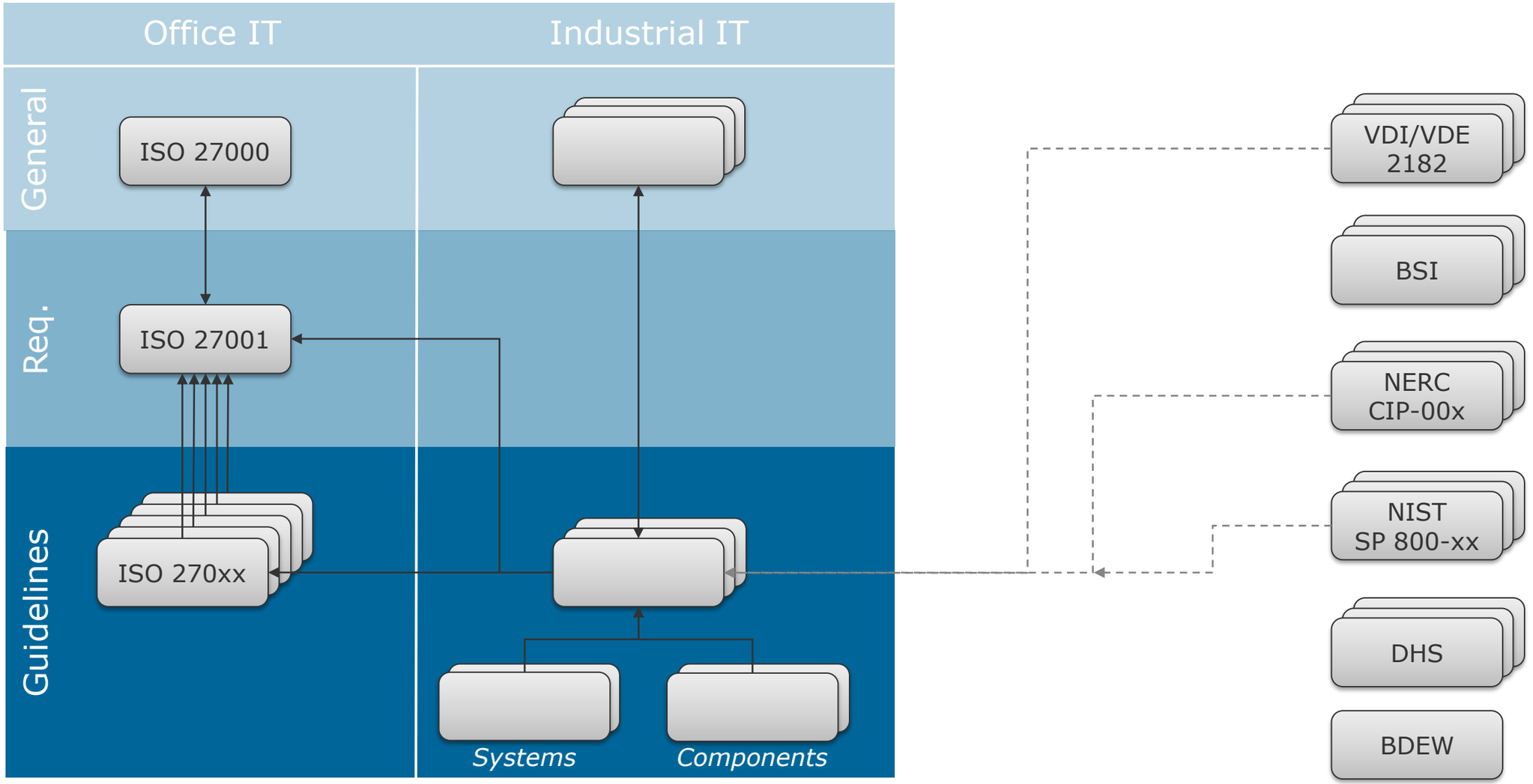
Step 4
- Segment the control network

Step 5
- Control access to the system

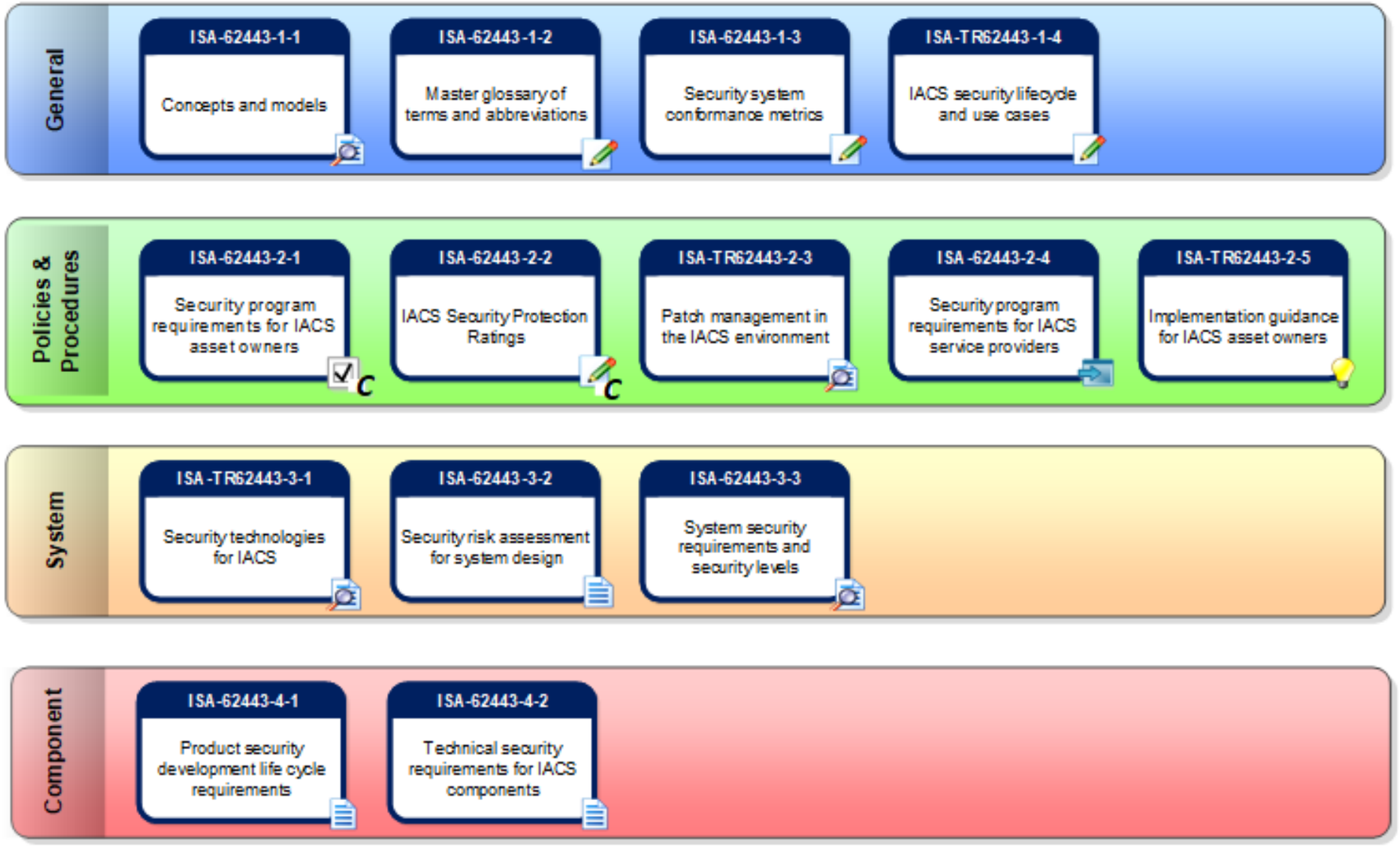
Step 6
- Harden the components

Step 7
- Monitor and maintain security

Activities in Standardization

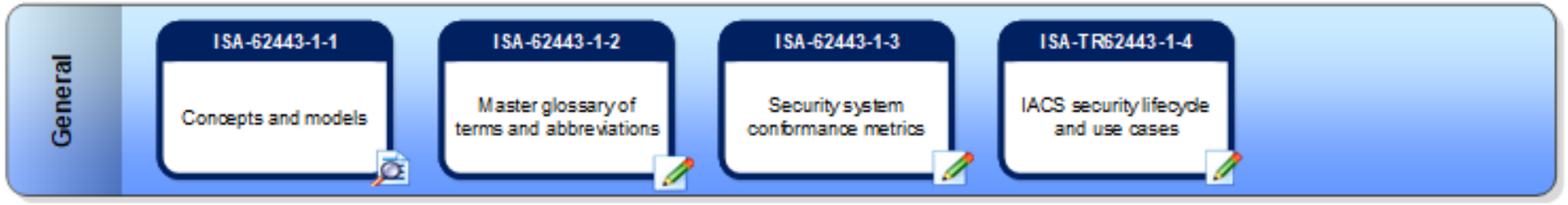


Standardization IEC 62443



Source: ISA 99, IEC 62443.

IEC 62443 - General

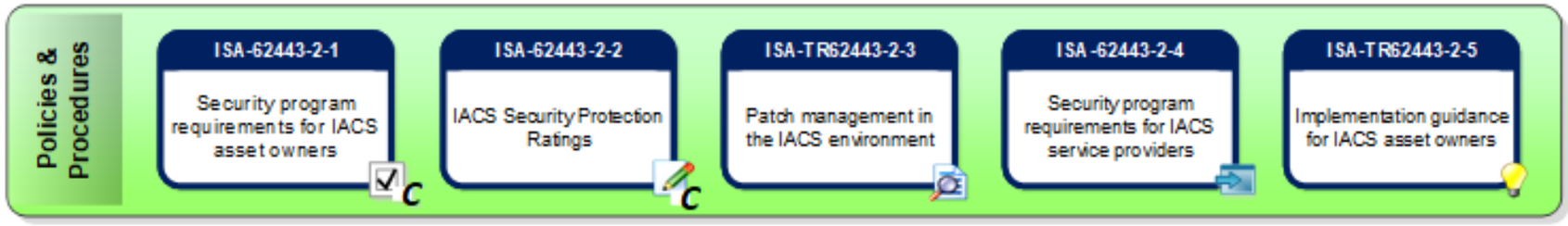


- **Terminology**
- **Concepts**
- **Models**
- **Compliance metrics**
- **Security levels (SL)**

Source: ISA 99, IEC 62443.

IEC 62443 – Policies and procedures

- Organization
- Training / awareness
- Continuity plan
- Policies, procedures
- Risk management and implementation



- Personnel security, Physical security, Network segmentation
- Account administration, Authentication, Authorization
- System development and maintenance
- Information, documentation management
- Incident planning and response

Source: ISA 99, IEC 62443.

IEC 62443 – System

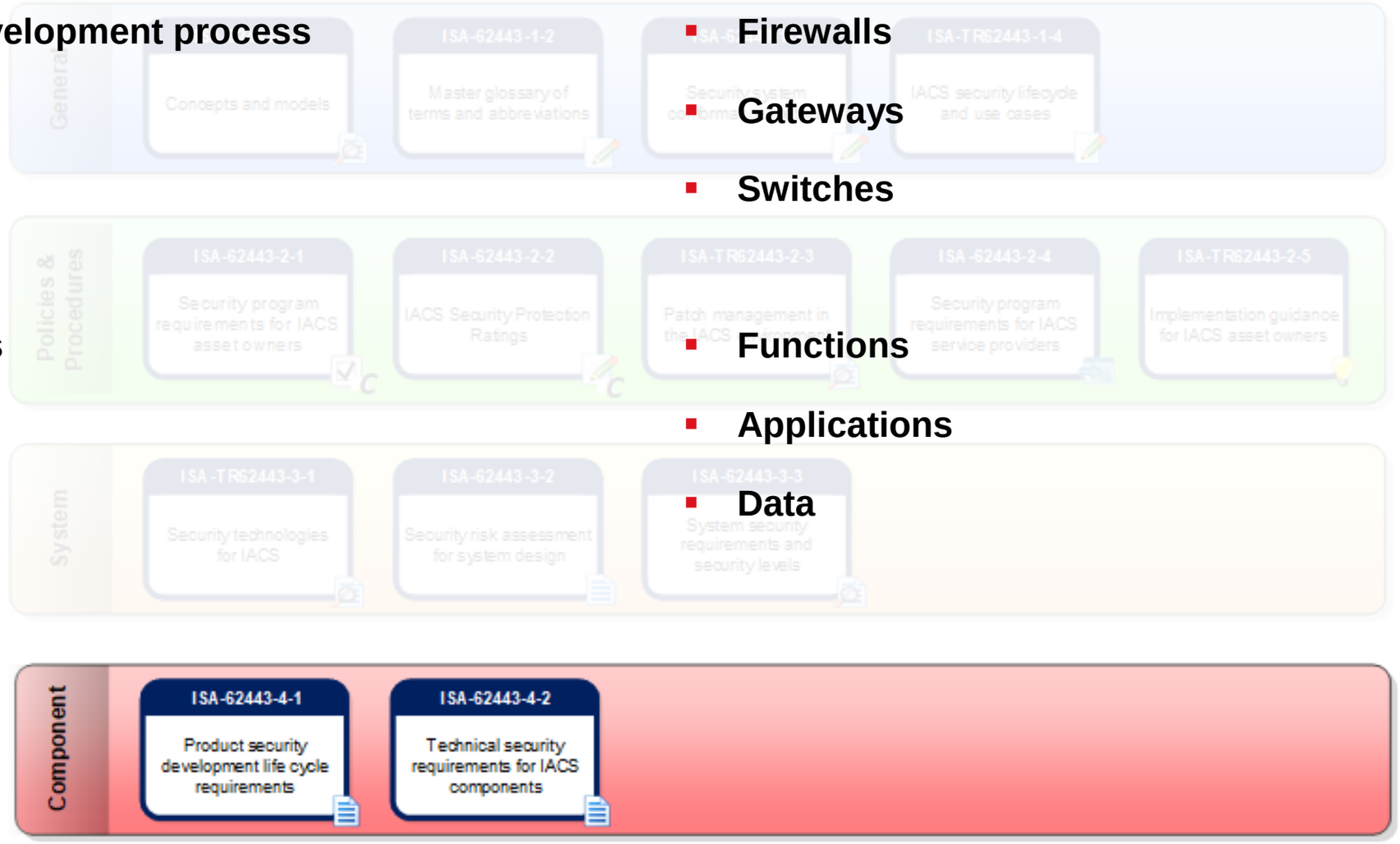
- System architecture, network segmentation
- Zones and conduits
- SL for systems

- Identification and authentication control
- Use control
- System integrity
- Data confidentiality
- Restricted data flow
- Timely response to events
- Resource availability

Source: ISA 99, IEC 62443.

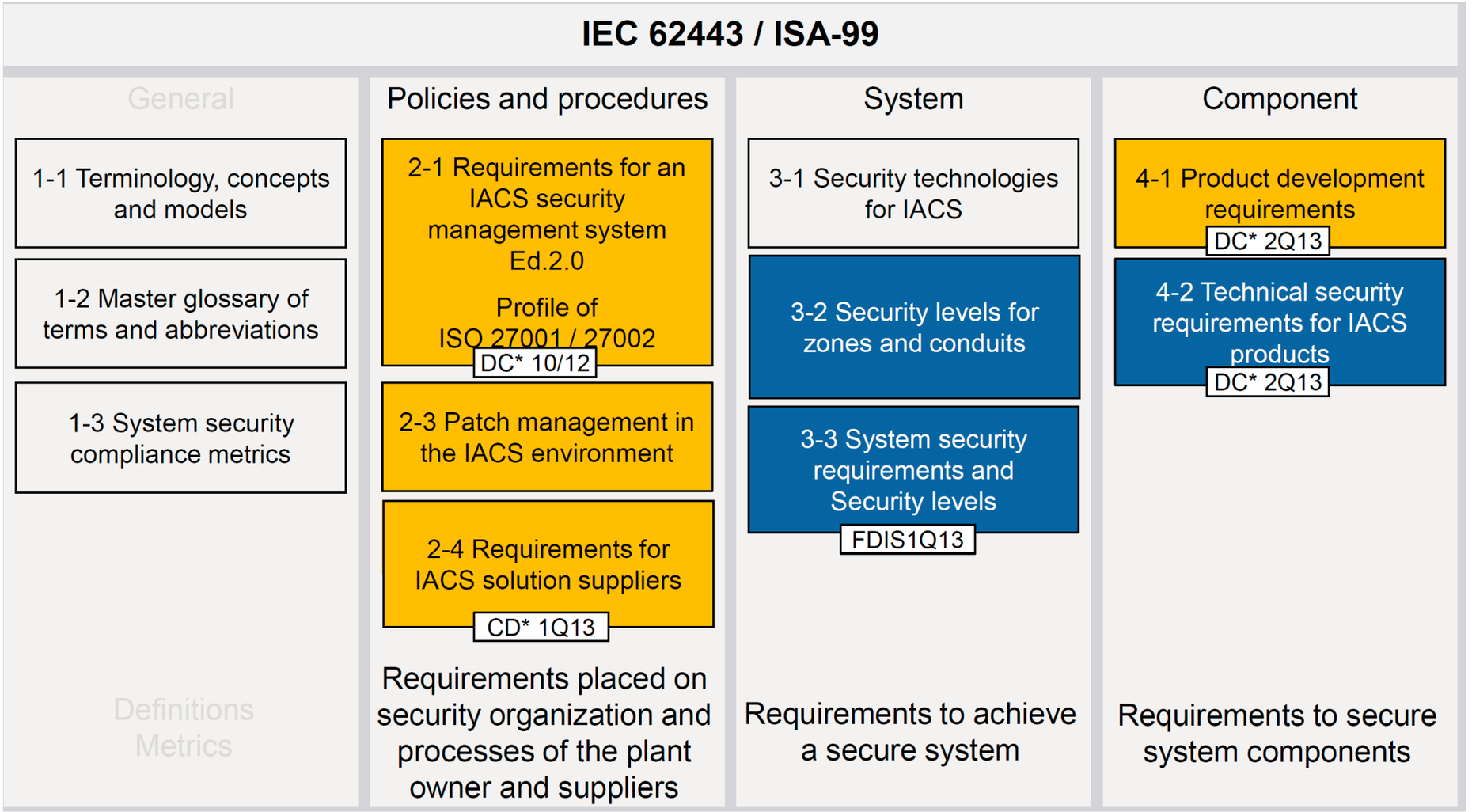
IEC 62443 – Components

- **Product development process**
- **PLCs**
- **HMI devices**
- **PC stations**
- **Firewalls**
- **Gateways**
- **Switches**
- **Functions**
- **Applications**
- **Data**



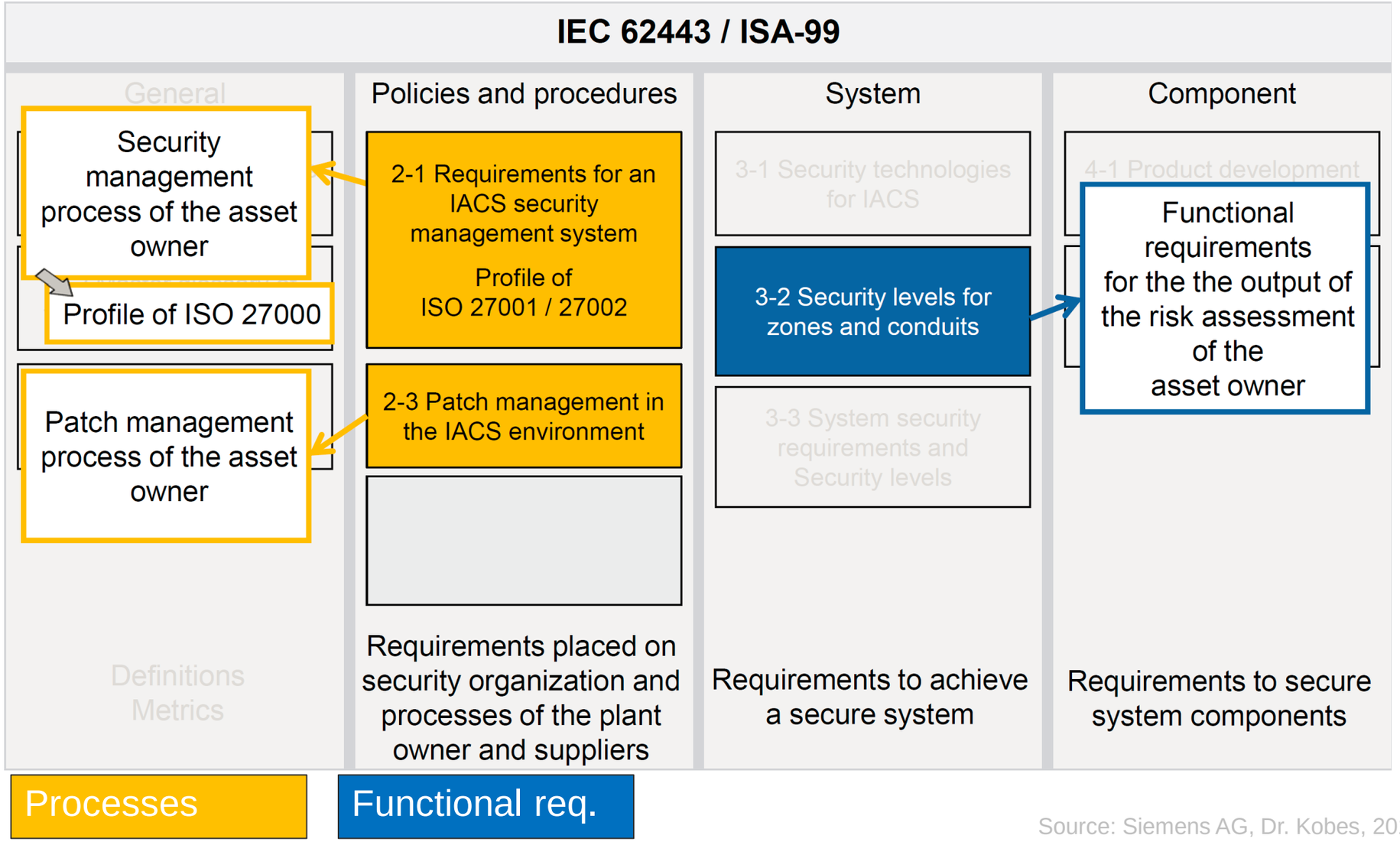
Source: ISA 99, IEC 62443.

Structure of IEC 62443



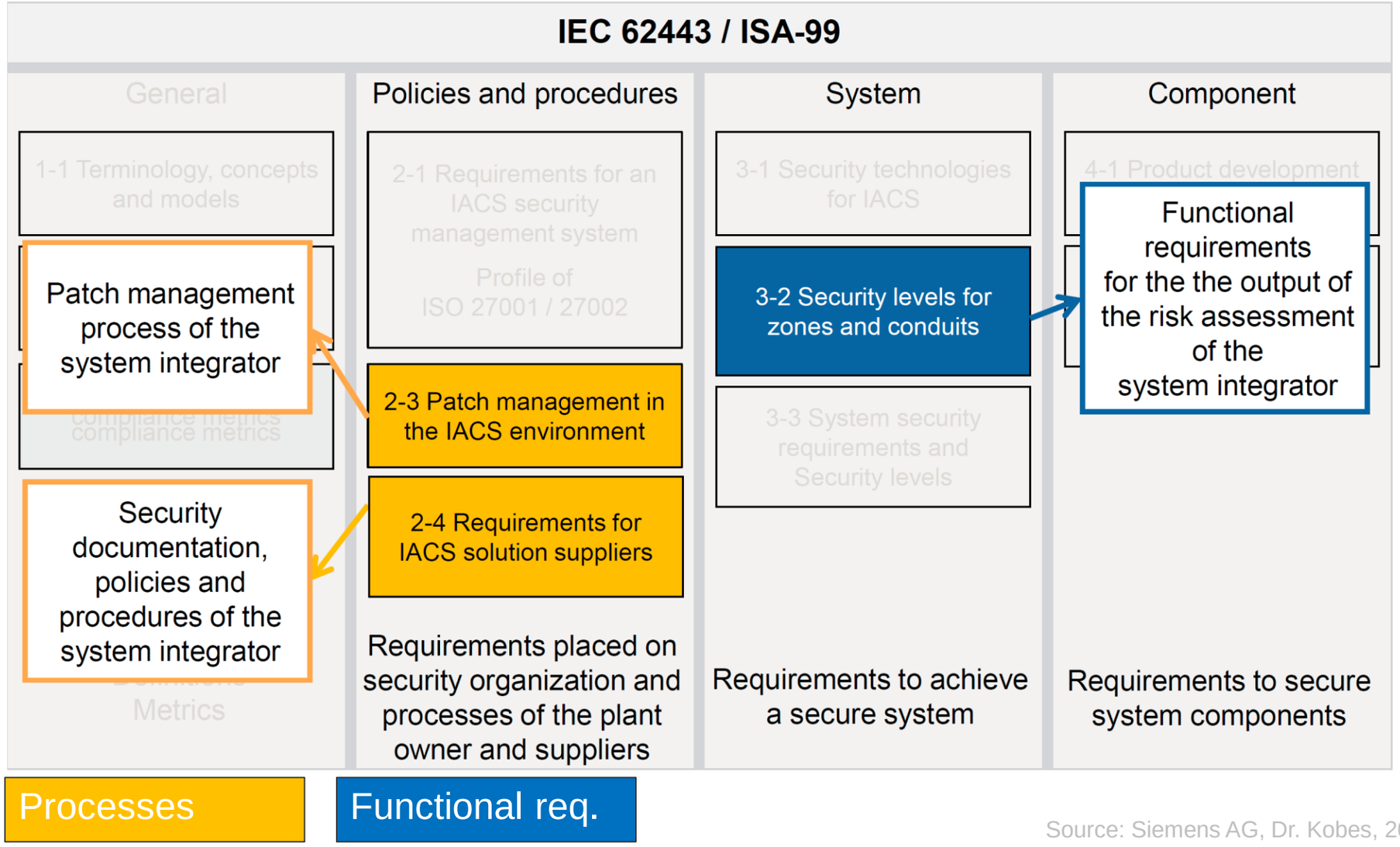
Source: Siemens AG, Dr. Kobes, 2015

Structure of IEC 62443 – Asset owner



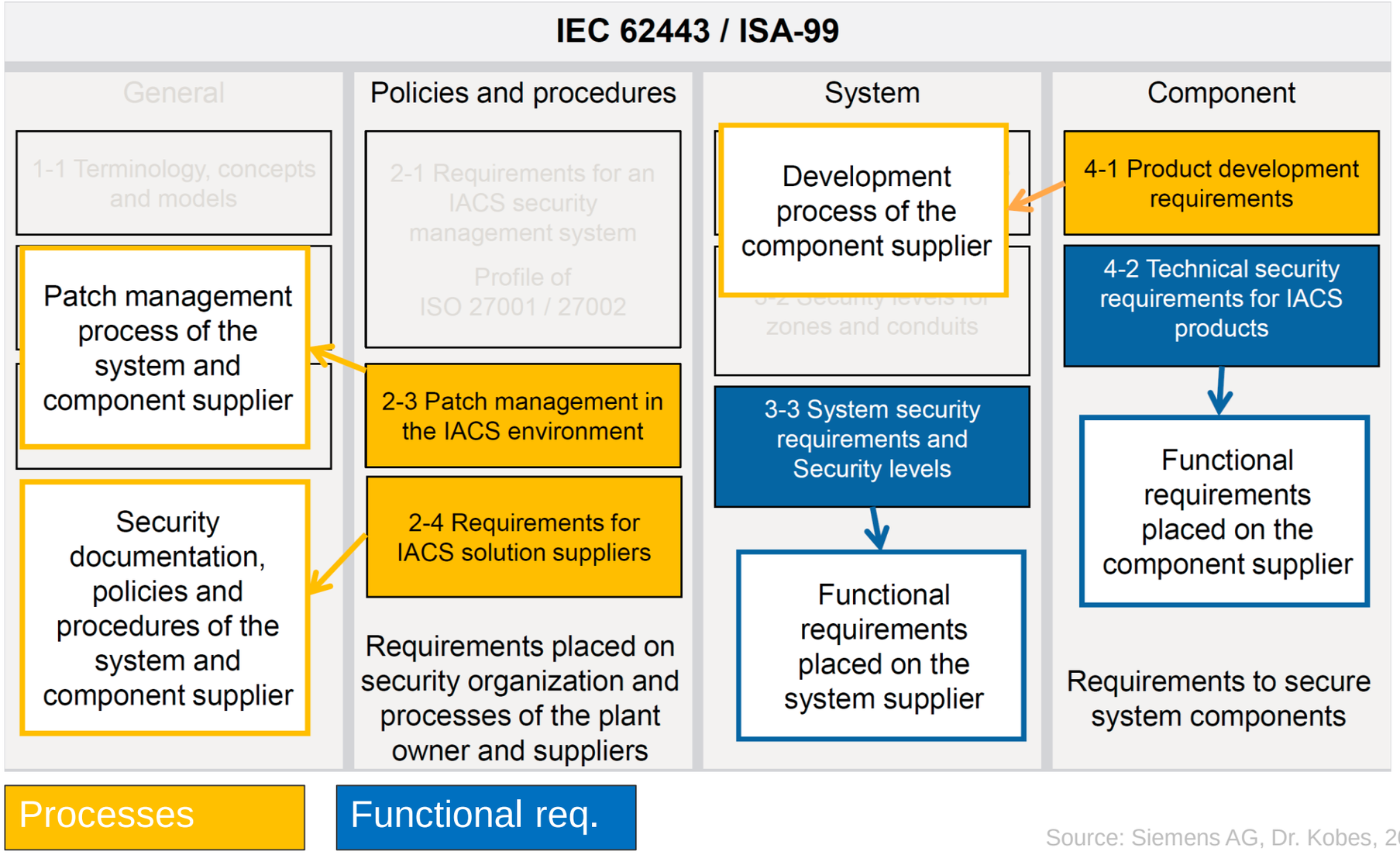
Source: Siemens AG, Dr. Kobes, 2015

Structure of IEC 62443 – System integrator



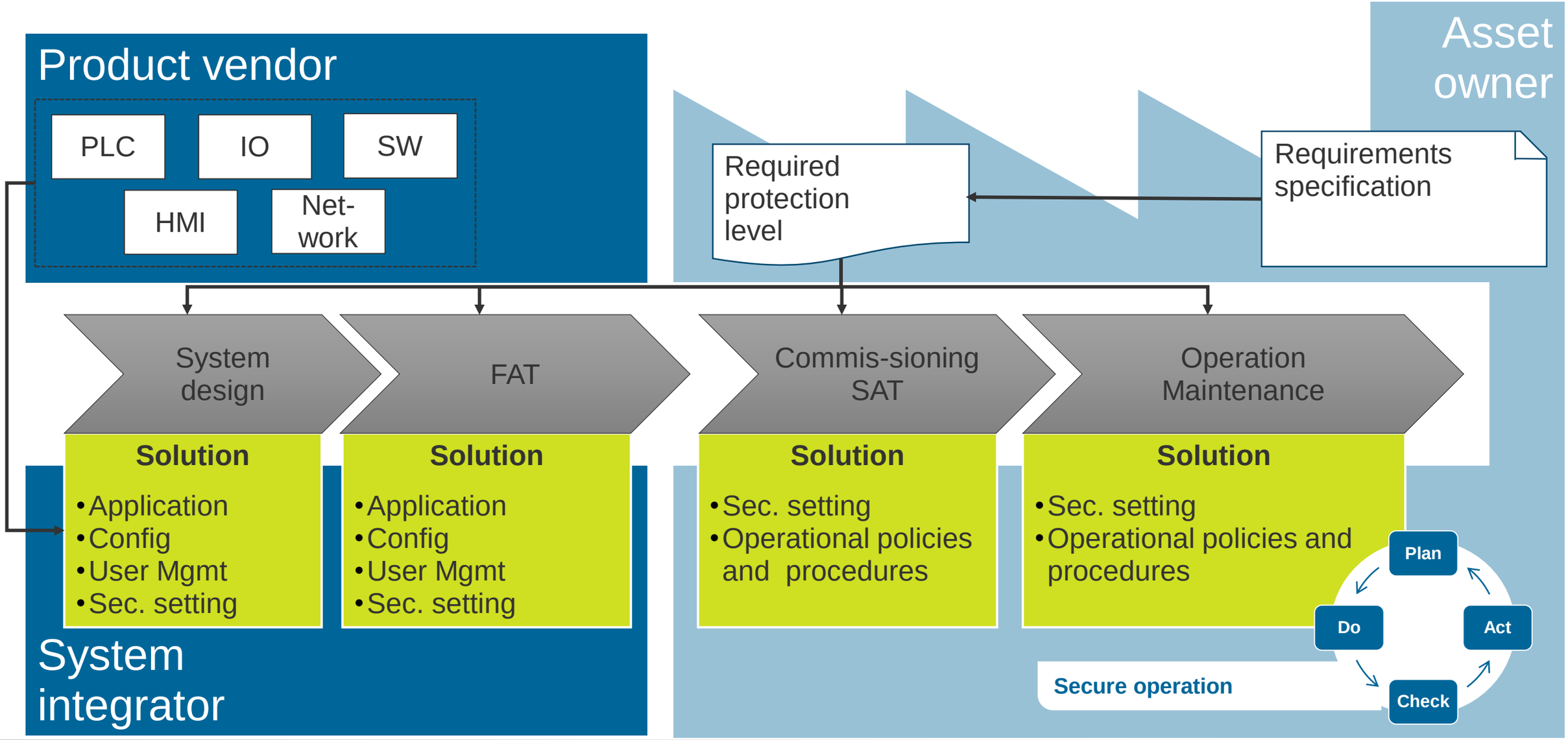
Source: Siemens AG, Dr. Kobes, 2015

Structure of IEC 62443 – Product supplier

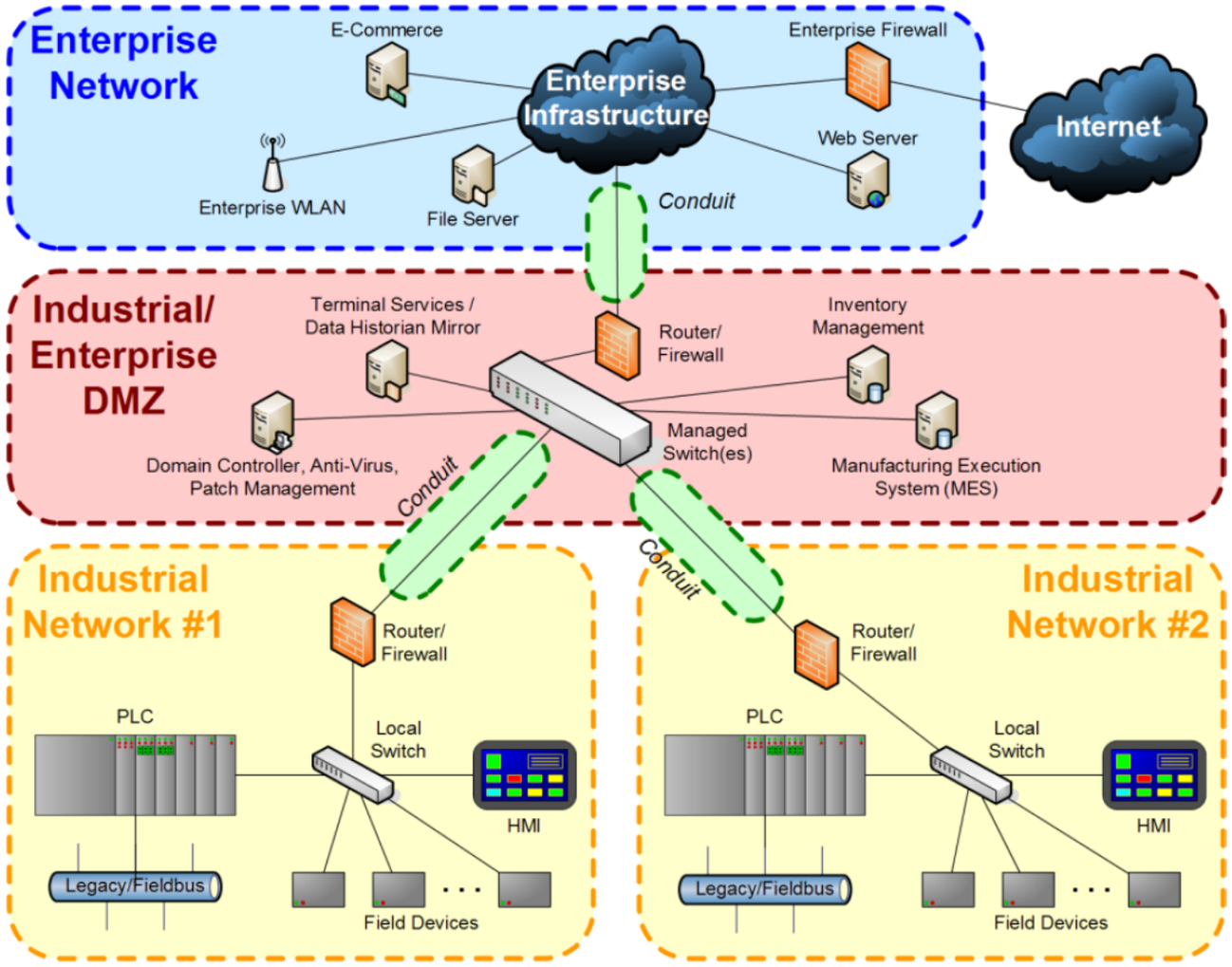


Source: Siemens AG, Dr. Kobes, 2015

Protection during the plant life cycle



Example Implementation – Zones and Conduits



Source: IEC 62443-1-1

Objective

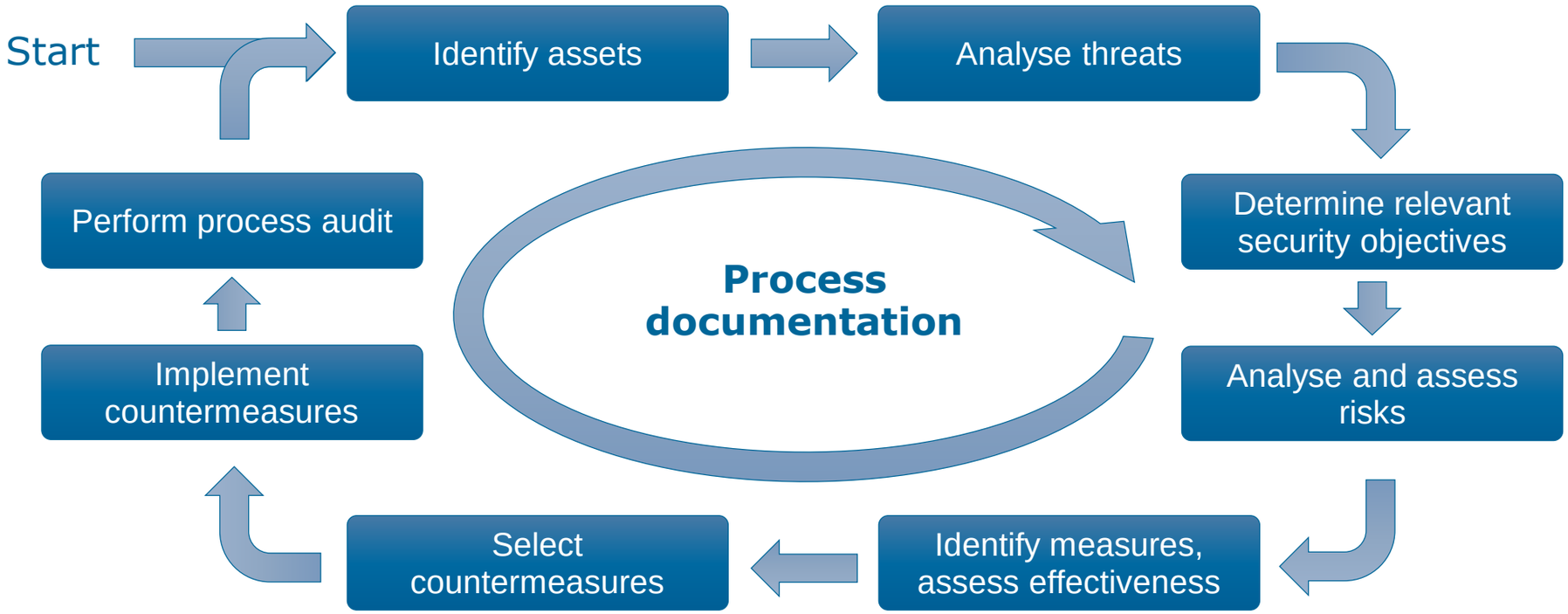
- **Specification and assessment of the protection level**

Security Levels	Protection level	FRs*/ Dimensions of the SL vector
SL 1	Protection against casual or coincidental violation	FR 1: Identification and Authentication Control (IAC) FR 2: Use Control (UC) FR 3: Data Integrity (DI) FR 4: Data Confidentiality (DC) FR 5: Restrict Data Flow (RDF) FR 6: Timely Response to an Event (TRE) FR 7: Ressource Availability (RA)
SL 2	Protection against intentional violation using simple means (low)	
SL 3	Protection against intentional violation using sophisticated means (moderate)	
SL 4	Protection against intentional violation using sophisticated means (high)	

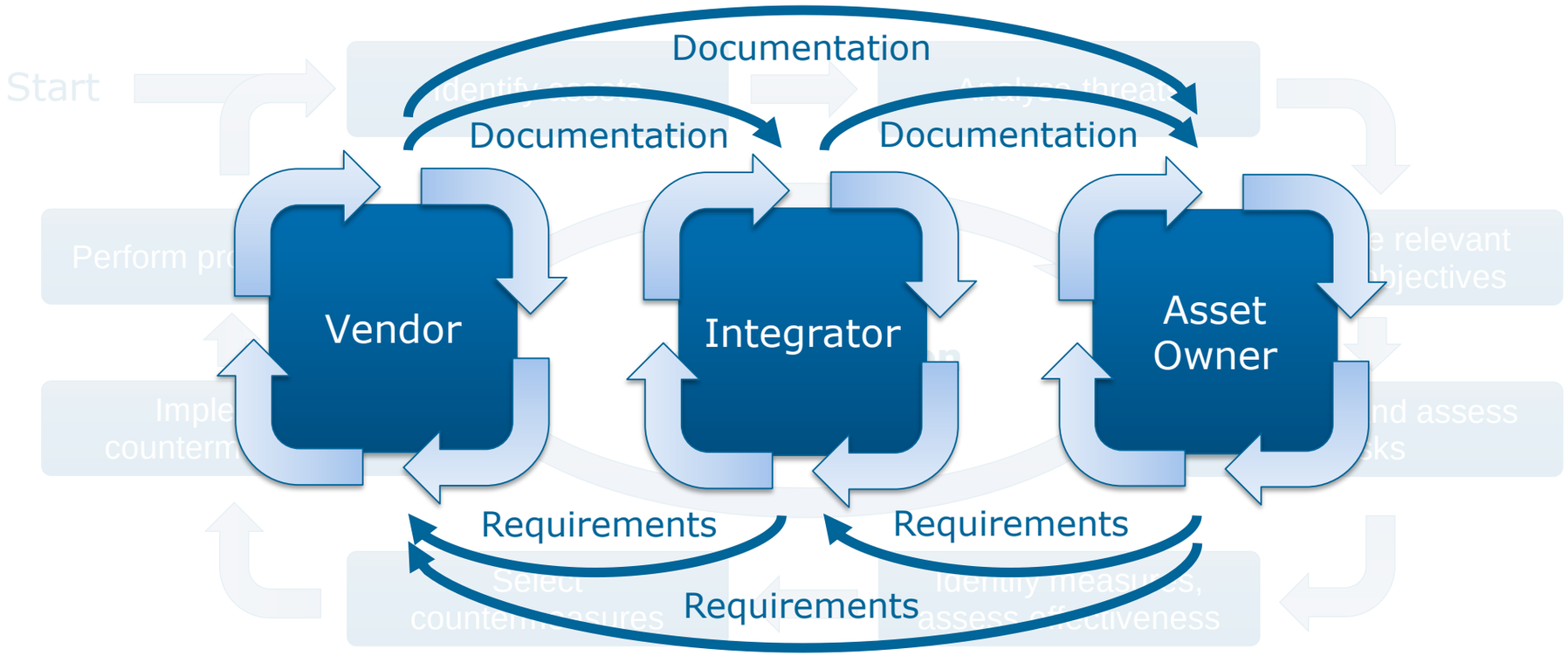
FRs*: Foundational Requirements (Source: IEC 62443-1-1-WD)

Applying the security level concept

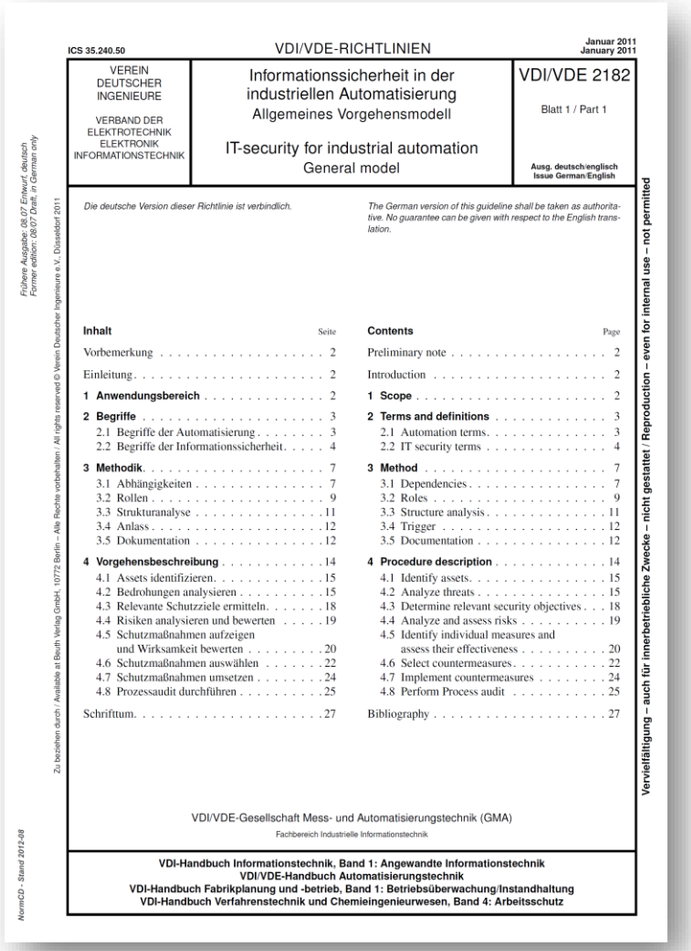
VDI 2182 – a generic procedure model



Always consider the whole value-added chain



Different parts of the guideline



ICS 35.240.50 VDI/VDE-RICHTLINIEN Januar 2011 / January 2011

VEREIN DEUTSCHER INGENIEURE
VERBAND DER ELEKTROTECHNIK ELEKTRONIK INFORMATIONSTECHNIK

Informationssicherheit in der industriellen Automatisierung
Allgemeines Vorgehensmodell

IT-security for industrial automation
General model

VDI/VDE 2182
Blatt 1 / Part 1

Ausg. deutsch/englisch
Issue German/English

Die deutsche Version dieser Richtlinie ist verbindlich.

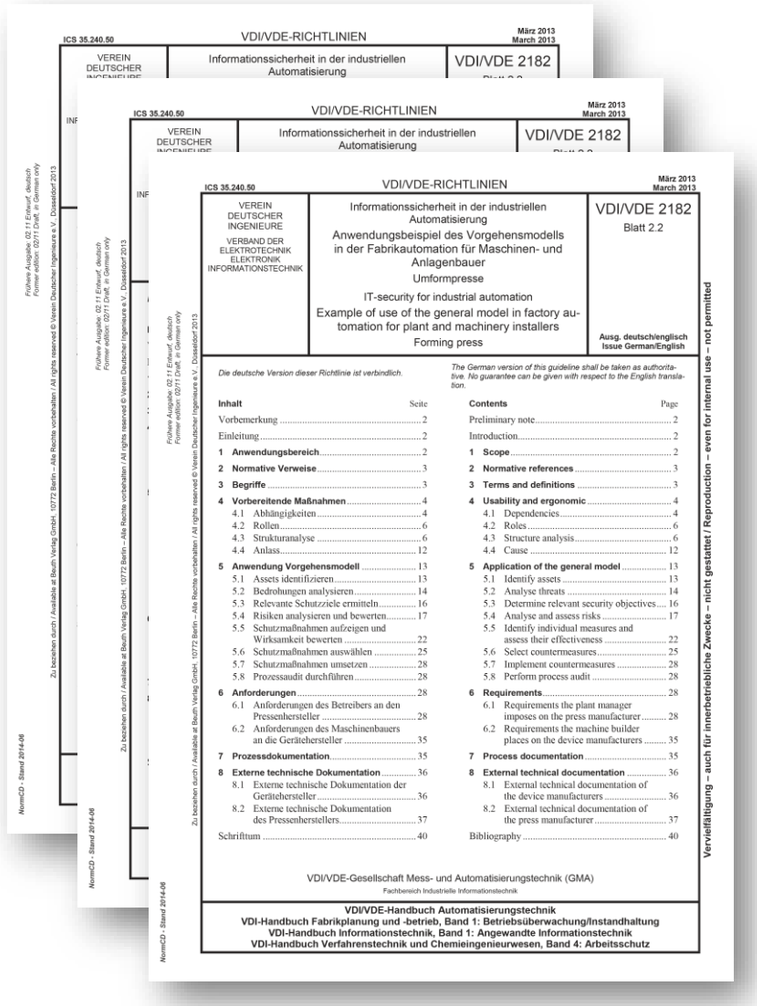
The German version of this guideline shall be taken as authoritative. No guarantee can be given with respect to the English translation.

Inhalt Seite

Contents Page

VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA)
Fachbereich Industrielle Informationstechnik

VDI-Handbuch Informationstechnik, Band 1: Angewandte Informationstechnik
VDI/VDE-Handbuch Automatisierungstechnik
VDI-Handbuch Fabrikplanung und -betrieb, Band 1: Betriebsüberwachung/Instandhaltung
VDI-Handbuch Verfahrenstechnik und Chemieingenieurwesen, Band 4: Arbeitsschutz



ICS 35.240.50 VDI/VDE-RICHTLINIEN März 2013 / March 2013

VEREIN DEUTSCHER INGENIEURE
VERBAND DER ELEKTROTECHNIK ELEKTRONIK INFORMATIONSTECHNIK

Informationssicherheit in der industriellen Automatisierung
Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Maschinen- und Anlagenbauer
Umformpresse

IT-security for industrial automation
Example of use of the general model in factory automation for plant and machinery installers
Forming press

VDI/VDE 2182
Blatt 2.2

Ausg. deutsch/englisch
Issue German/English

Die deutsche Version dieser Richtlinie ist verbindlich.

The German version of this guideline shall be taken as authoritative. No guarantee can be given with respect to the English translation.

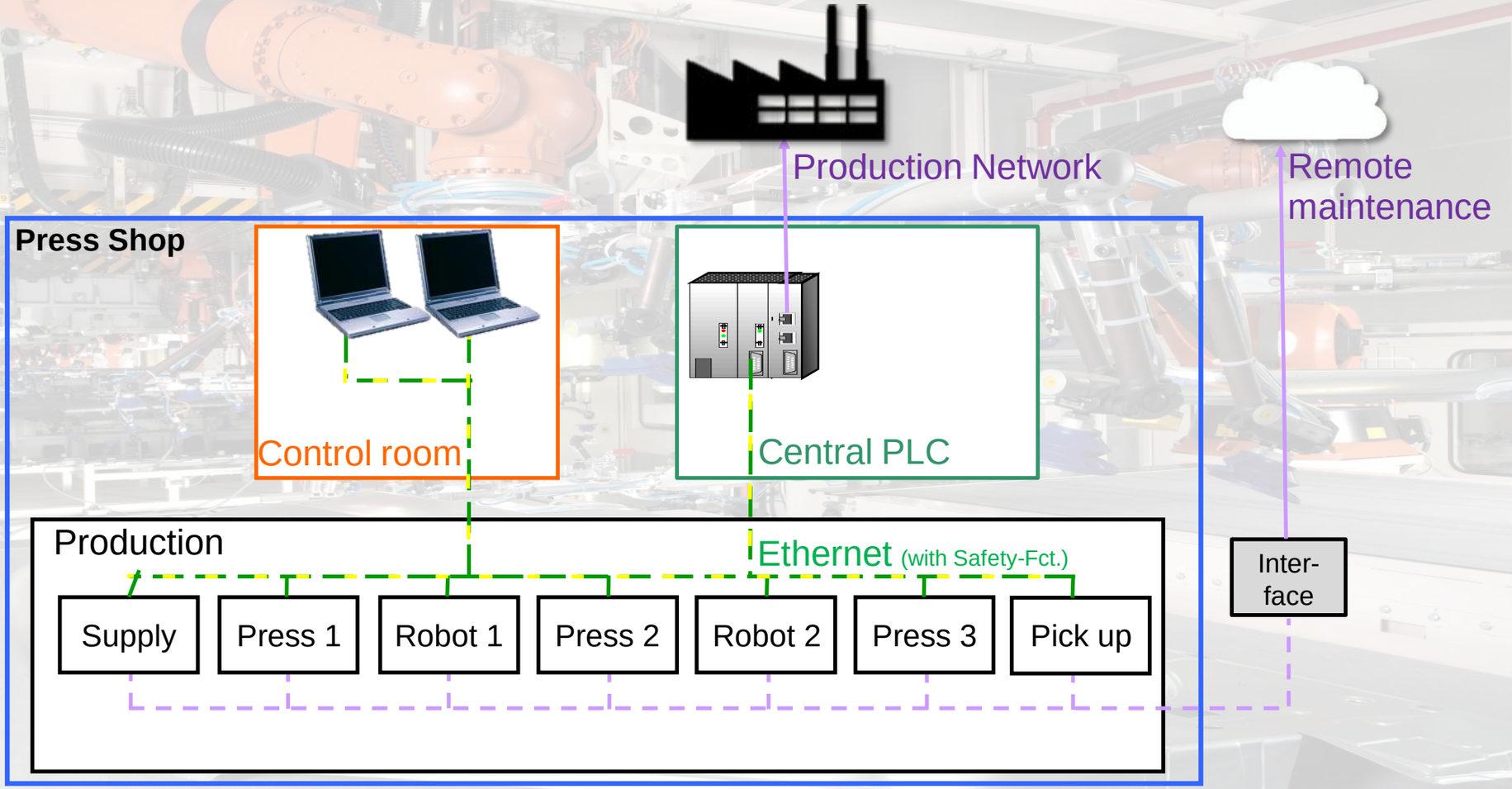
Inhalt Seite

Contents Page

VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA)
Fachbereich Industrielle Informationstechnik

VDI/VDE-Handbuch Automatisierungstechnik
VDI-Handbuch Fabrikplanung und -betrieb, Band 1: Betriebsüberwachung/Instandhaltung
VDI-Handbuch Informationstechnik, Band 1: Angewandte Informationstechnik
VDI-Handbuch Verfahrenstechnik und Chemieingenieurwesen, Band 4: Arbeitsschutz

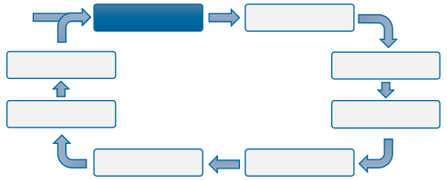
Case study as example:
Press shop in the automobile industry



Quelle: Schuler AG

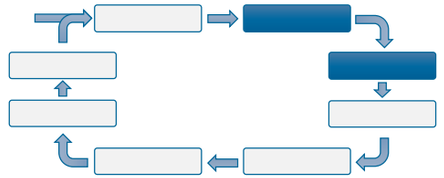
Identify assets

- **Parts of the machine and plant**
  - Press1, Press2, Press3
  - Robot1, Robot2
  - Supply
  - Pick-up
  - Central PLC and control room
- **Internal and external communication**
  - Internal traffic
  - External traffic from/to production network
  - External traffic for remote maintenance
- **Legal position**
  - Ensure a production without errors and outages
  - Ensure Safety

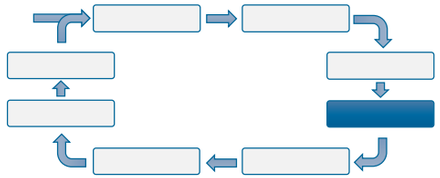


Analyse threats and determine objectives

Betrachtungsgegenstand: Presswerk												
Komponente	*Assets (Funktion/Dienst)*	*Bedrohung*	*unmittelbare Folge*		*Schutzziele*							
	Assets können z.B. sein: + Verarbeitungsgeräte oder -komponenten mit ihren materiellen oder immateriellen Werten + Komminikationskanäle mit ihren materiellen oder immateriellen Werten + Management Aspekte				*Verfügbarkeit*	*Integrität*	*Vertraulichkeit*	*Benutzer-Authentizität*	*Daten-Authentizität*	*Nichtabstreitbarkeit*	*Überprüfbarkeit*	
Maschinen-/Anlagenteile												
Presse1	Maschinen-Funktionalität	Datenverlust durch Geräteausfall	Maschine nicht mehr betriebsfähig		X							
		Manipulation von Informationen	Maschine nicht mehr betriebsfähig, Produktionsdaten und Know-how gehen verloren		X		X					
		Schadsoftware bedroht Presswerk	Performance der Maschine (Taktzeiten, Qualität) sinkt		X	X						
		Fehlfunktion durch fehlerhafte Software	Fehlproduktion durch falsche Parameter, Fehler sofort erkennbar		X			X				
	Bedienbarkeit der Presse	Fehlbedienung durch Maschinenführer	Fehlproduktion durch falsches Programm,		X					X		

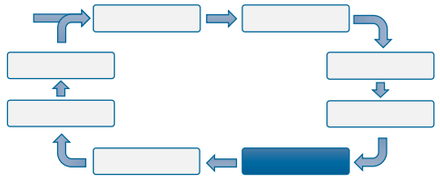


Analyse and evaluate risk



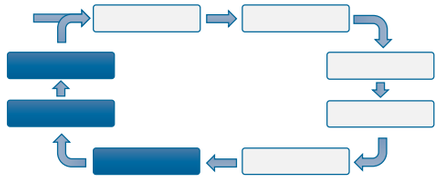
Betrachtungsgegenstand: Presswerk										
Komponente	*Assets (Funktion/Dienst)*	*Bedrohung*	*unmittelbare Folge*	*Akzeptables Risiko*			*Identifiziertes Risiko*			*Risikoreduzierung erforderlich?*
				Wahrscheinlichkeit	*Ausmaß*	*Risiko*	*Wahrscheinlichkeit*	*Ausmaß*	*Risiko*	
	Assets können z.B. sein: + Verarbeitungsgeräte oder -komponenten mit ihren materiellen oder immateriellen Werten + Komminikationskanäle mit ihren materiellen oder immateriellen Werten + Management Aspekte			*Legende: Wahrscheinlichkeit 0 = ausgeschlossen 1 = gering 2 = mittel 3 = hoch 4 = sehr hoch 5 = garantiert*	*Legende: Ausmaß 0 = kein 5 = gering 10 = mittel 15 = hoch 20 = sehr hoch 25 = extrem*	*(Wahrscheinlichkeit * Ausmaß)*	*Legende: Wahrscheinlichkeit 0 = ausgeschlossen 1 = gering 2 = mittel 3 = hoch 4 = sehr hoch 5 = garantiert*	*Legende: Ausmaß 0 = kein 5 = gering 10 = mittel 15 = hoch 20 = sehr hoch 25 = extrem*	*(Wahrscheinlichkeit * Ausmaß)*	*Wert=identifiziertes Risiko-tolerierbares Risiko Handlungsbedarf, wenn Wert >0 je größer der Wert, desto zwingender die Maßnahme*
Maschinen-/Anlagenteile										
Presse1	Maschinen-Funktionalität	Datenverlust durch Geräteausfall	Maschine nicht mehr betriebsfähig	0	15	0	2	15	30	30
		Manipulation von Informationen	Maschine nicht mehr betriebsfähig, Produktionsdaten und Know-how gehen verloren	0	20	0	1	20	20	20
		Schadsoftware bedroht Presswerk	Performance der Maschine (Taktzeiten, Qualität) sinkt	0	15	0	3	15	45	45
		Fehlfunktion durch fehlerhafte Software	Fehlproduktion durch falsche Parameter, Fehler sofort erkennbar	0	10	0	4	10	40	40

Assess countermeasures and determine effectiveness



Betrachtungsgegenstand: Presswerk							
Komponente	*Assets (Funktion/Dienst)*	*Bedrohung*	*unmittelbare Folge*	*Risikoreduzierung erforderlich?*	*Maßnahme*	*Kosten*	*Wirksamkeit*
interne/externe Kommunikationsbeziehungen							
Externer Datenfluss für Fernwartung	Fernwartungs-Funktionalität	Die PCs der Dienstleister werden nicht nach Schadsoftware untersucht	Virus Befall auf Maschine, im Netzwerk und bei weiteren Produktionseinrichtungen	60	Fernwartungskonzept erarbeiten und mit Lieferanten vereinbaren	30.000 Euro	ausreichend
		Hackerangriff (DOS-Attacke), da keine gesicherte Übertragung	Produktionsstillstand, Produktionsschaden durch unkontrollierten Produktionsvorgang, Verlust der funktionalen Maschinensicherheit	60	VPN-Übertragung installieren	15.000 Euro	ausreichend
		Maschinenbauer führt nicht erlaubte Fernwartungsfunktionen aus	Produktionsstillstand, Produktionsschaden durch unkontrollierten Produktionsvorgang, Verlust der funktionalen Maschinensicherheit	80	Fernwartungskonzept erarbeiten und mit Lieferanten vereinbaren	s.o.	ausreichend
	Produktionsparameter	Maschinenbauer überträgt geheime Produktionsparameter	Spionage, Know-how-Verlust an externe Dienstleister	75	Fernwartungsfunktionalität begrenzen (s. fernwartungskonzept)	s.o.	ausreichend

Select and implement countermeasures, perform audits



- **Further criteria during selection**
  - Required investment
  - Operational cost per annum
  - Feasibility of the control within the organization
- **Aggregation of single controls**
  - Maßnahmen zum Desaster Recovery
  - Maßnahmen zur Konfiguration von Geräten
  - Investitionen in Security Einrichtungen
  - Maßnahmen, die den Zulieferern zugeordnet werden
  - Organisatorische Maßnahmen

Industrial Security - Summary

Security is one of the essential ingredients for Industry 4.0

- A new range of security issues need to be solved

Industry 4.0 means highly networked and open systems

- Security by design as key design principle
- More standard IT products and increased connectivity

Industrial security is never static

- Ongoing process along the whole life cycle

Cyber security management system (CSMS)

- Technical and organizational measures to meet the desired level of protection

Security awareness

- Be proactive instead of suffering a great loss of …