Functional Safety and Cybersecurity:

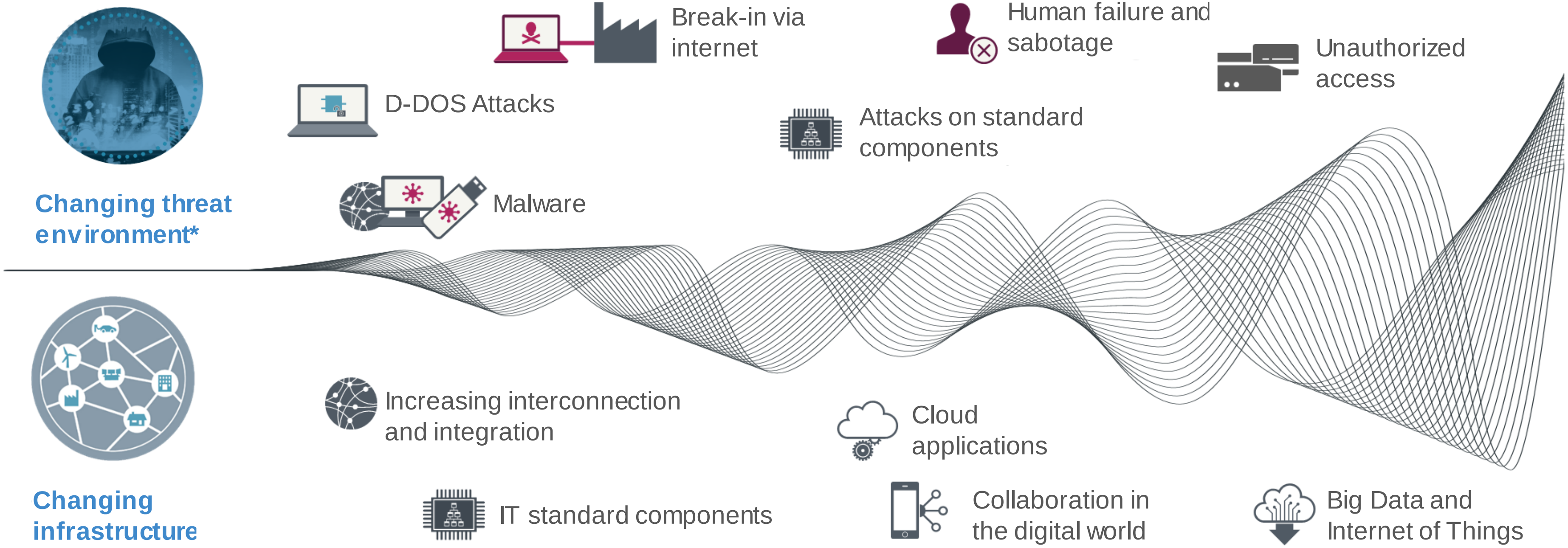
Dependencies
Standards
Pragmatic approaches

Florian Spiteller

May 27th 2022, Toronto

DKE

Cybersecurity needs continuous processes due to the changing threat environment



Changing threat environment*

D-DOS Attacks

Malware

Break-in via internet

Human failure and sabotage

Attacks on standard components

Unauthorized access

Changing infrastructure

Increasing interconnection and integration

IT standard components

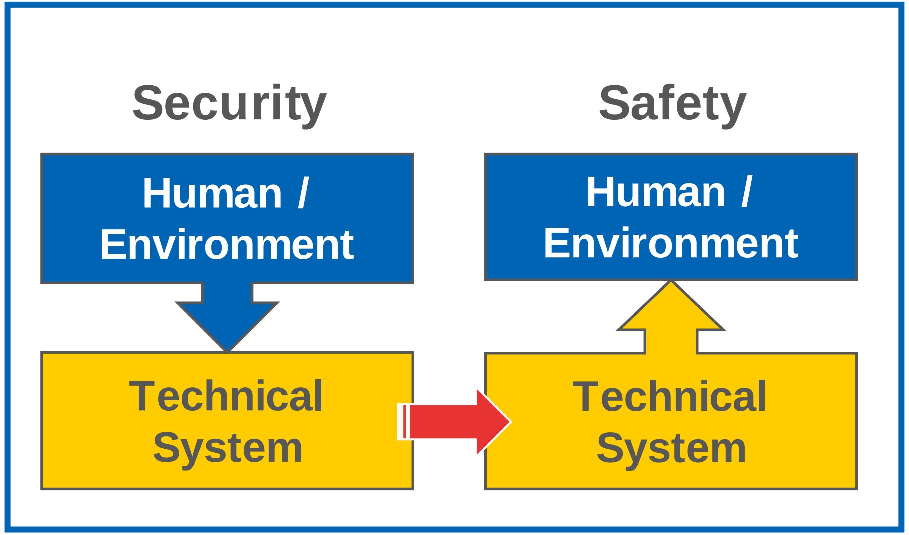
Cloud applications

Collaboration in the digital world

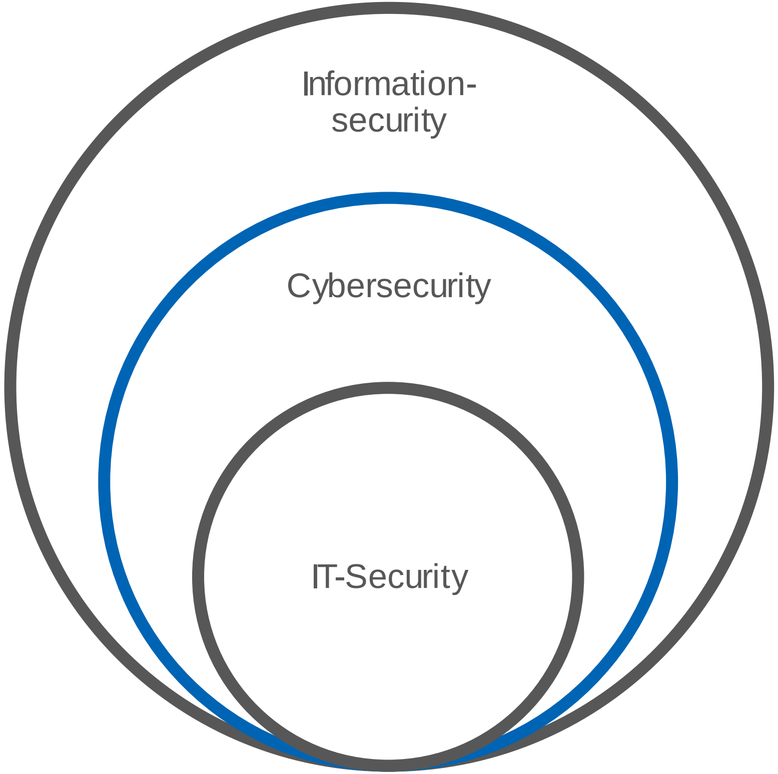
Big Data and Internet of Things

* Based on BSI Top10 threats in 2018

What is Security and what is Safety?



What is Informationsecurity?



Informationsecurity

- Protection of informationen in all possible forms: analog (e.g. paper) or digital (e.g. files). Basics are the classical security objectives confidentiality, integrity and availability

Cybersecurity

- Refers to all connected networks, applications, processes, and devices across borders. Includes critical infrastructures such as energy supply, transportation
- Management of physical processes

IT-Security

- Refers to the security of classical IT, the "office environment". Includes web/mail servers, management systems
- Management of information

Information Technology (IT) & Operational Technology (OT)

IT – Management of information

- web/app/data/email server, management systems
- Primary security objective: **confidentiality**
- e.g. ISO/IEC 27000 series

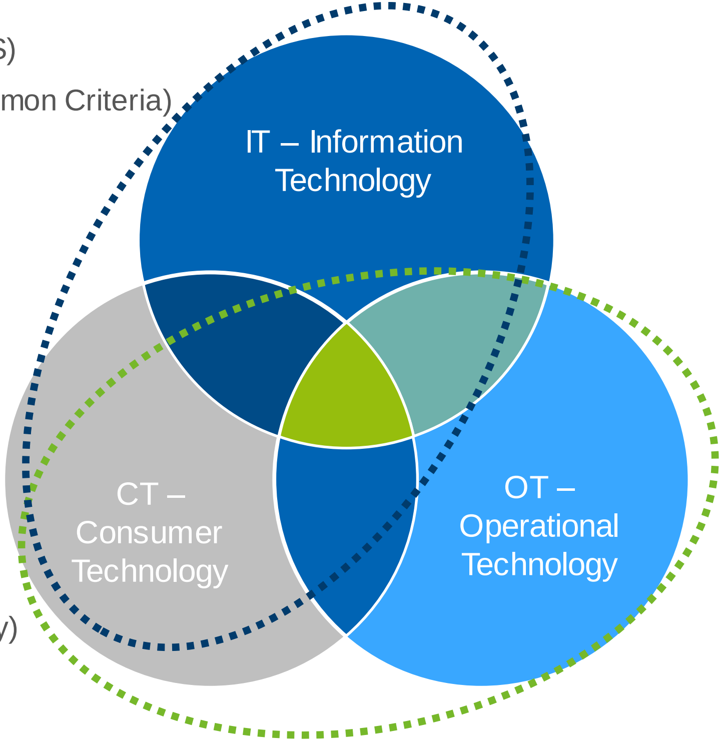
OT – Management of physical processes

- Industrial Controls (PLC, DCS, SCADA & I/O), sensors, embedded systems, …
- Primary security objectives: **availability & integrity**
- e.g. IEC 62443 series

Information Technology (IT) & Operational Technology (OT)

Embedding in the IT/OT/CT standardization landscape

- ISO/IEC 27000 series (ISMS)
- ISO/IEC 15408 series (Common Criteria)



- IEC 62443 series (Industrial Automation
- IEC 62351 series (Smart Grid Communication)
- IEC 63096 (Nuclear Power Plants)
- IEC 80001 series (Medical Devices)
- IEC 63110 series (Charging Infrastructure)
- …

- ETSI EN 303 645 (IoT-Security)

Sectors for Operational Technology

Energy Supply

Process Industry

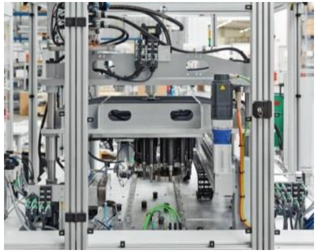
Automotive Industry

Renewable Energy

Shipbuilding

Railway Industry

Water Industry



Machine Building Industry

Industrial Electronics

Building Automation

Implement Cybersecurity

source: Adobe Stock_40-140531253

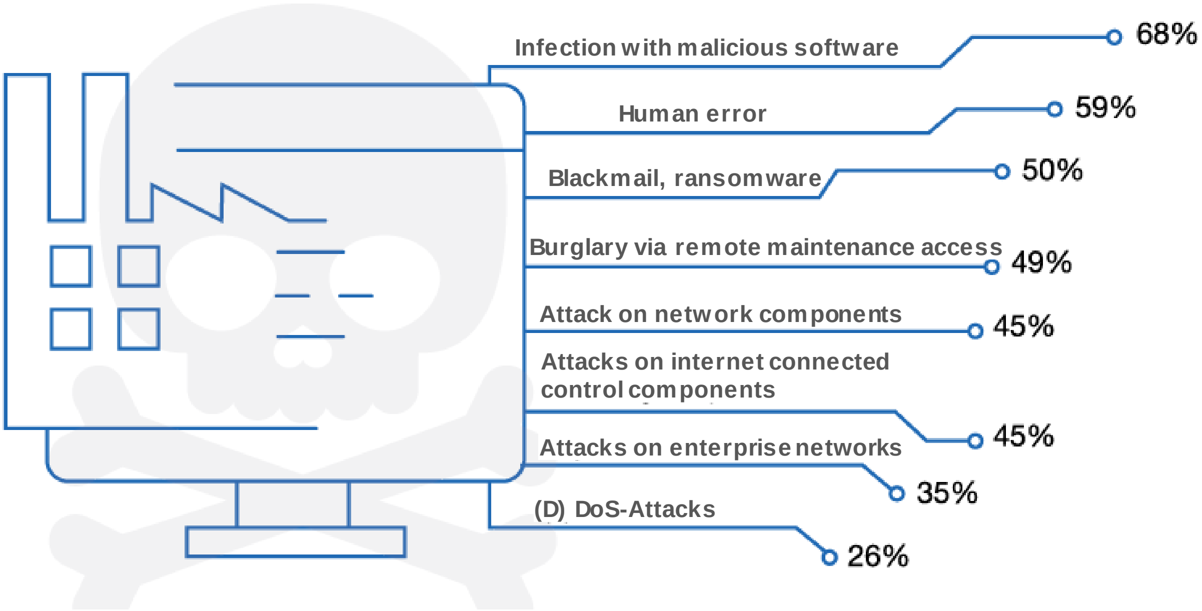
- Industrial systems rely more and more on the use of IT and OT
  - Increasing implementation of IT in OT
  - Increased need for information
  - Increasing degree of automation
  - Increasing internal and external networking
  - Prerequisite for Industry 4.0
- A mixture of IT and OT results in a completely new starting point
  for the assessment of security risks

Differences in requirements for IT and OT

	IT	OT
Service life	3-5 years	5-20 years Note: IEC 62443 uses the term service life in Part 1-1 with regard to key management but does not specify a time frame
Patch management	Often, daily	Seldom, requires release from system manufacturer Note: IEC 62443 explicitly regulates the topic in Part 2-3
Time dependency	Delays accepted	Critical Note: IEC 62443 defines security objectives in Part 1-1; the real-time capability is indicated in the millisecond range
Availability	Short down-times tolerated	24/7 Note: IEC 62443 defines security objectives in Part 1-1, where availability is defined as the highest security goal

source:https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2017/April/Orientierungsleitfaden_fuer_Hersteller_IEC_62443/Orientierungsleitfaden_fuer_Hersteller_IEC_62443.pdf

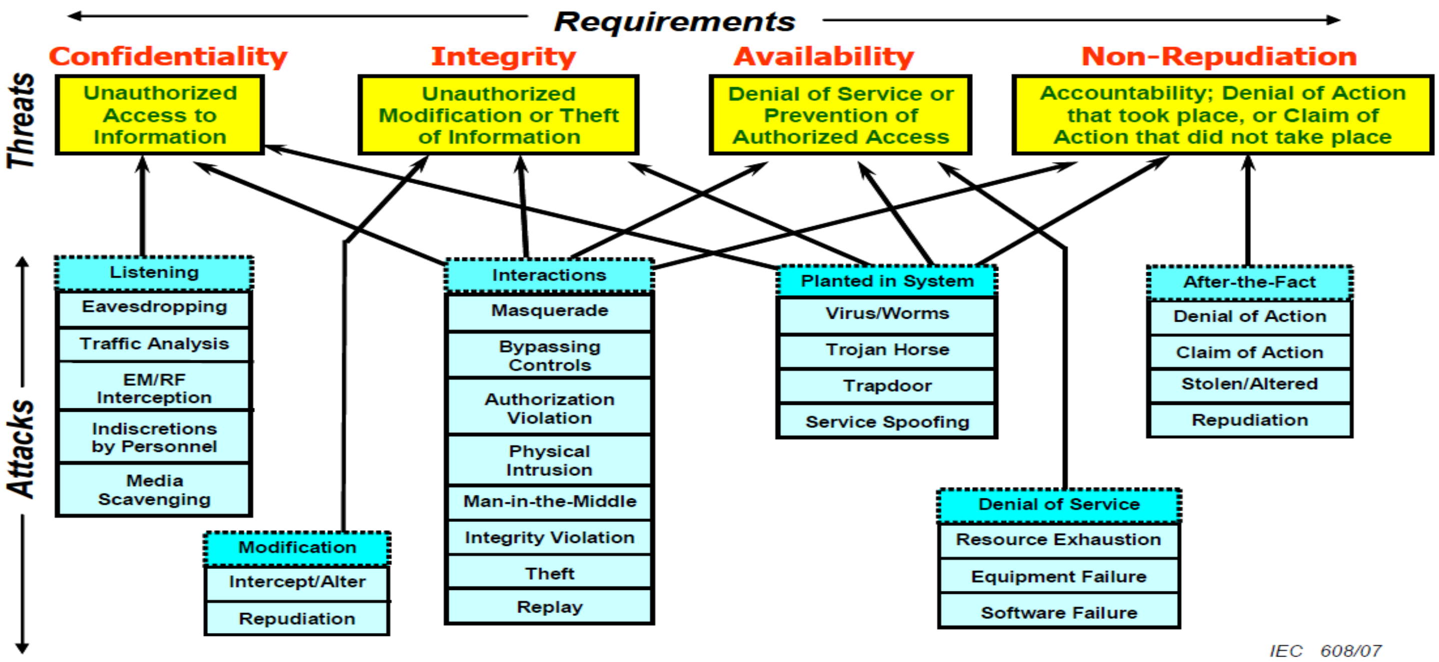
Industry 4.0 – Networking poses hidden risks



Infection with malicious software	68%
Human error	59%
Blackmail, ransomware	50%
Burglary via remote maintenance access	49%
Attack on network components	45%
Attacks on internet connected control components	45%
Attacks on enterprise networks	35%
(D) DoS-Attacks	26%

source: VDE Member Survey 2018

IT security is complex



source: IEC Draft Guide 120

To reduce complexity: use standardisation!

„The product/system is secure!“

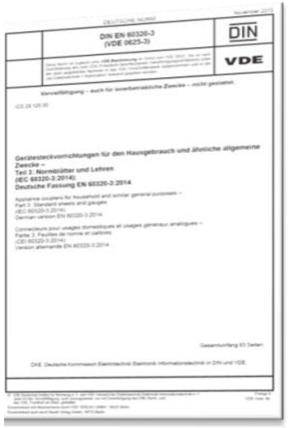
- ...can never be shown due to unpredictability (environment changes almost daily)
- ...is not a useful goal (deterrent)

→ **complex!!**

„We have done everything reasonable to make the product/system secure."

- …can be shown
- …can be documented and certified!

Improvement due to use of norms and standards!!!



DEUTSCHE NORM

November 2015

DIN EN 60320-3
(VDE 0625-3)

DIN

VDE

[illegible]

Vervielfältigung – auch für innerbetriebliche Zwecke – nicht gestattet.

ICS 29.120.30

Gerätesteckvorrichtungen für den Hausgebrauch und ähnliche allgemeine Zwecke –
Teil 3: Normblätter und Lehren
(IEC 60320-3:2014);
Deutsche Fassung EN 60320-3:2014

Appliance couplers for household and similar general purposes –
Part 3: Standard sheets and gauges
(IEC 60320-3:2014);
German version EN 60320-3:2014

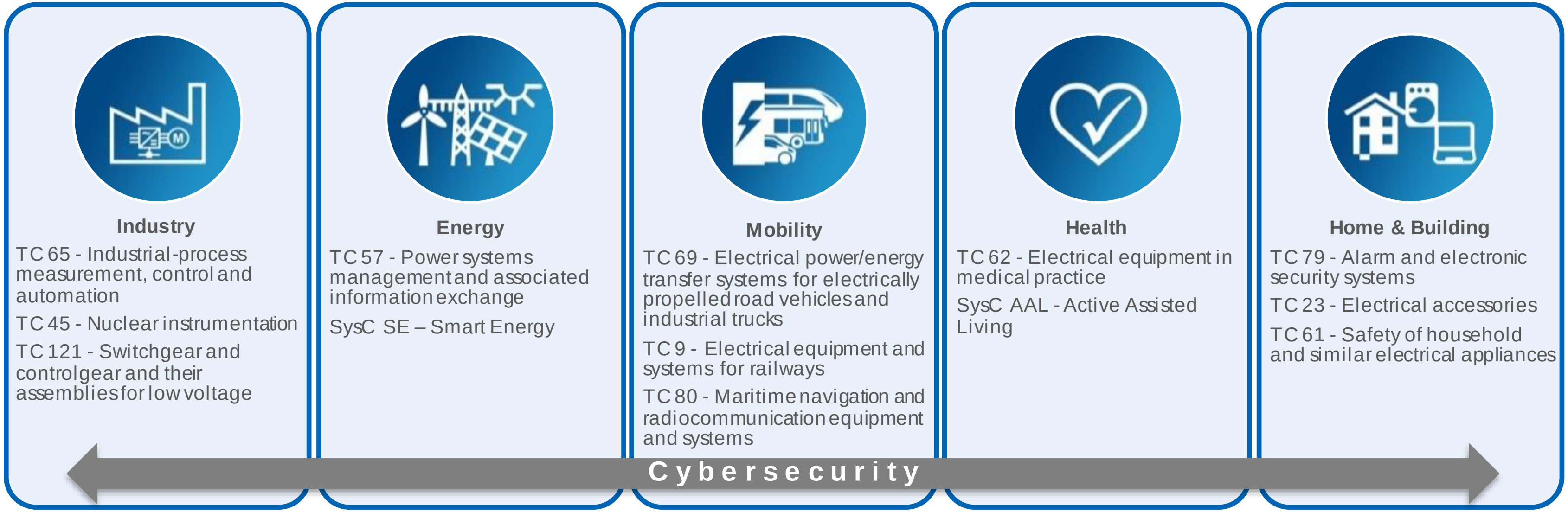
Connecteurs pour usages domestiques et usages généraux analogues –
Partie 3: Feuilles de norme et calibres
(CEI 60320-3:2014);
Version allemande EN 60320-3:2014

Gesamtumfang 63 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

[illegible]

Cybersecurity in DKE mirrors Cybersecurity in IEC



Industry

TC 65 - Industrial-process measurement, control and automation

TC 45 - Nuclear instrumentation

TC 121 - Switchgear and controlgear and their assemblies for low voltage

Energy

TC 57 - Power systems management and associated information exchange

SysC SE – Smart Energy

Mobility

TC 69 - Electrical power/energy transfer systems for electrically propelled road vehicles and industrial trucks

TC 9 - Electrical equipment and systems for railways

TC 80 - Maritime navigation and radiocommunication equipment and systems

Health

TC 62 - Electrical equipment in medical practice

SysC AAL - Active Assisted Living

Home & Building

TC 79 - Alarm and electronic security systems

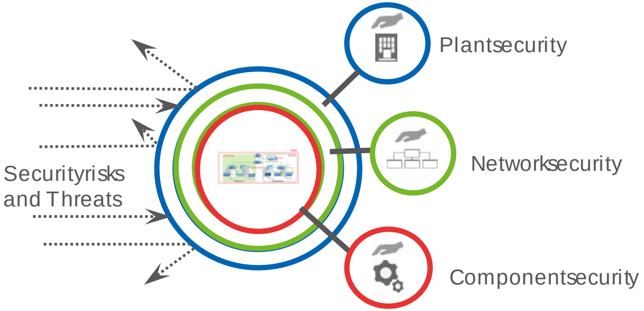
TC 23 - Electrical accessories

TC 61 - Safety of household and similar electrical appliances

- DKE mirrors all IEC projects and adopts the IEC-Standards into German body of standards
- DKE supports IEC/ACSECs goal: coherent and holistic approach for all sectors
- DKE avoids the development of national standards to prevent a proliferation of requirements

Basic Cybersecurity concepts for Operational Technology

Defense-in-Depth

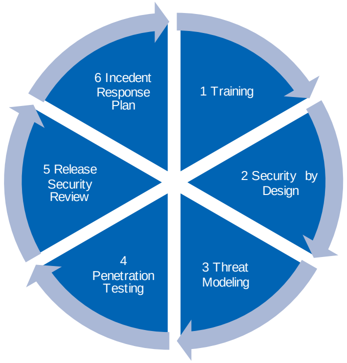


Only one Security measure is not sufficient!

PlanDoCheckAct-Cycle

Security is a process!

Secure Development Lifecycle



„Security-by-Design“

IEC 62443 series - Security for industrial automation and control systems

General	Guidelines and procedures	System	Component / Product	Profiles	Evaluation
1-1 Terminology, concepts and models 🟨	2-1 Security program requirements for IACS asset owners 🟨	3-1 Security technologies for IACS 🟩	4-1 Secure Product Lifecycle Requirements 🟩	5-X Profile X 🟥	6-1 Security Evaluation Methodology for IEC 62443-2-4 🟥
1-2 Master glossary of terms and abbreviations 🟥	2-2 Security Program Rating 🟥	3-2 Security Risk Assessment and System Design 🟩	4-2 Technical security requirements for IACS components 🟩		6-2 Security Evaluation Methodology for IEC 62443-4-2 🟥
1-3 System security conformance metrics 🟥	2-3 Patch management in the IACS environment 🟨	3-3 System security requirements and security levels 🟨			
1-4 IACS security lifecycle and use-cases 🟥	2-4 Security requirements for IACS service providers 🟨				
1-5 Scheme for IEC 62443 Cybersecurity Profiles 🟥	2-5 Implementation guidance for IACS asset owners 🟥				

▭ Process requirements

■ Functional requirements

🟩 Published

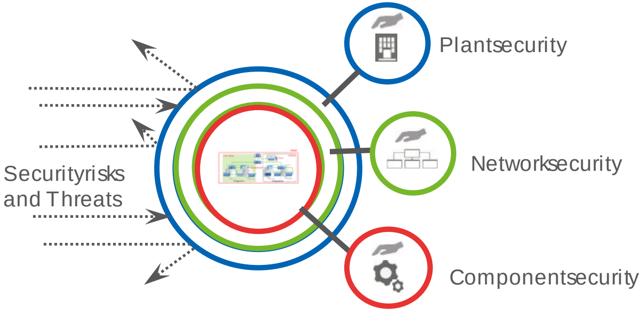
🟨 Under revision

🟥 In development

Basic Cybersecurity concepts for Operational Technology

Applicationin IEC 62443series

Defense-in-Depth

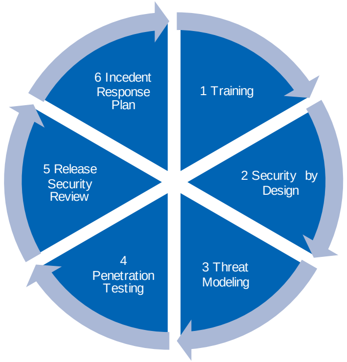


IEC 62443-1-1 Terminology, concepts and models
IEC 62443-4-1 Secure Product Lifecycle Requirements

PlanDoCheckAct-Cycle

IEC 62443-1-1 Terminology, concepts and models
IEC 62443-4-1 Secure Product Lifecycle Requirements

Secure Development Lifecycle



IEC 62443-4-1 Secure Product Lifecycle Requirements

IT security via norms and standards
Certification in accordance with ISO/IEC 27001

Staff security

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the intended roles.

Instructions for implementation:

a) submission of satisfactory character references, e.g. a professional and personal testimony

b) an applicant CV that has been checked for completeness and accuracy

c) confirmation of specified academic and professional qualifications

d) independent identity verification (passport or similar document)

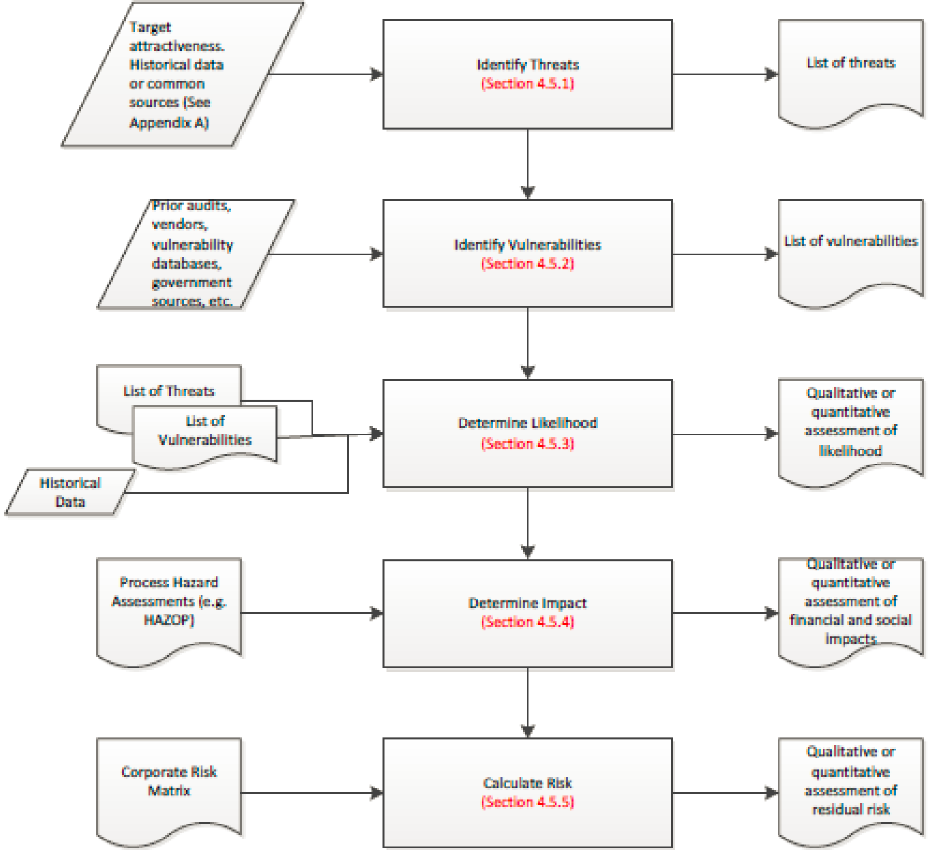
e) detailed supporting documents such as a credit check or criminal record review.

If a person is hired for a specific role in information security, organisations should ensure that the applicant:

a) possess the necessary skills for the security task

b) possesses the required level of trustworthiness, especially if the role is crucial for the organisation.

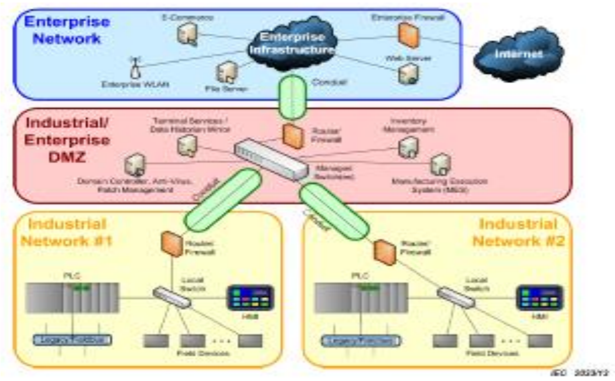
Risk-Assessment according to IEC 62443


Target attractiveness. Historical data or common sources (See Appendix A)
Identify Threats
(Section 4.5.1)
List of threats
Prior audits, vendors, vulnerability databases, government sources, etc.
Identify Vulnerabilities
(Section 4.5.2)
List of vulnerabilities
List of Threats
List of Vulnerabilities
Historical Data
Determine Likelihood
(Section 4.5.3)
Qualitative or quantitative assessment of likelihood
Process Hazard Assessments (e.g. HAZOP)
Determine Impact
(Section 4.5.4)
Qualitative or quantitative assessment of financial and social impacts
Corporate Risk Matrix
Calculate Risk
(Section 4.5.5)
Qualitative or quantitative assessment of residual risk

- IEC 62443-3-2:
  „Security Risk Assessment and System Design"

- Identify assets
- Identify threats
- Identify vulnerabilities
- Calculate occurrence probability
- Identify possible impact
- Calculate risk

IEC 62443 - Protection against violations



Level	Protection against…
1	incidental incorrect use
2	intentional attempts using simple means
3	SL2, but with extended knowledge and expanded means
4	SL3, but with specific knowledge and considerable means

Short form	Long form	Meaning
SL-C	Security-Level – Capability	Security level the device or system can reach if it is correctly used and configured
SL-T	Security-Level – Target	This target security level is a result of the threat/risk analysis
SL-A	Security-Level – Achieved	The achieved and measurable security level achieved in the overall system

source: IEC 2033/13
source: Security Level during the life cycle IEC 62443

source: Security Level (SL) in accordance with IEC 62443

Thank you for your attention!

We are building the e-dialistic future.
Please join us.

Your contact:

Florian Spiteller
Head of External Relations & Support
Member of the DKE Executive Board
Phone +49 69 6308-380
florian.spiteller@vde.com

DKE