

Status und aktuelle Entwicklungen bei der ISA/IEC 62443

Thomas Bleier

 t@b-sec.net

 +43 664 3400559

Classification: PUBLIC

Version: 01

Date: 10.10.2023

Status: Final



<https://www.b-sec.net>

About me...

DI Thomas Bleier, MSc | t@b-sec.net | +43 664 3400559



B-SEC better secure KG

- IT-Sicherheit in industriellen Umgebungen (OT / IACS / SCADA / I4.0, etc.)
- **Assessment** – Prüfung technischer und organisator. Sicherheitsmaßnahmen
- **Training** – Security Engineering, Security-Architektur, Zertifizierungen, etc.
- **Beratung** – Design/Implementierung von sicheren Systeminfrastrukturen

Allgemein beeideter, gerichtlich zertifizierter Sachverständiger

- für IT-Sicherheit, Verschlüsselung, Datenschutz, Gebäudeautomation

Geschäftsführer / CTO Bioenergie Bleier GmbH & Co KG

Auditor für ISMS nach ISO 27001/27018/27701, NIS-V Auditor

FH Lektor für angewandte IT-Sicherheit & Security Engineering

Normung & Standardisierung:

- Vorsitzender OVE TSK MR65 - Spiegelkomitee des IEC TC65 – IEC 62443, IEC 61508, etc.
- Vorsitzender OVE AG MR65 Industrial Automation & Control Systems Security (IEC 62443)
- Mitarbeit bei ISA WG 99 (IACS Security); ASI (Austrian Standards) Komitee 001 (IT), AG 001.18 (Datenschutz), AG 001.27 (Information security, Cybersecurity and privacy protection)

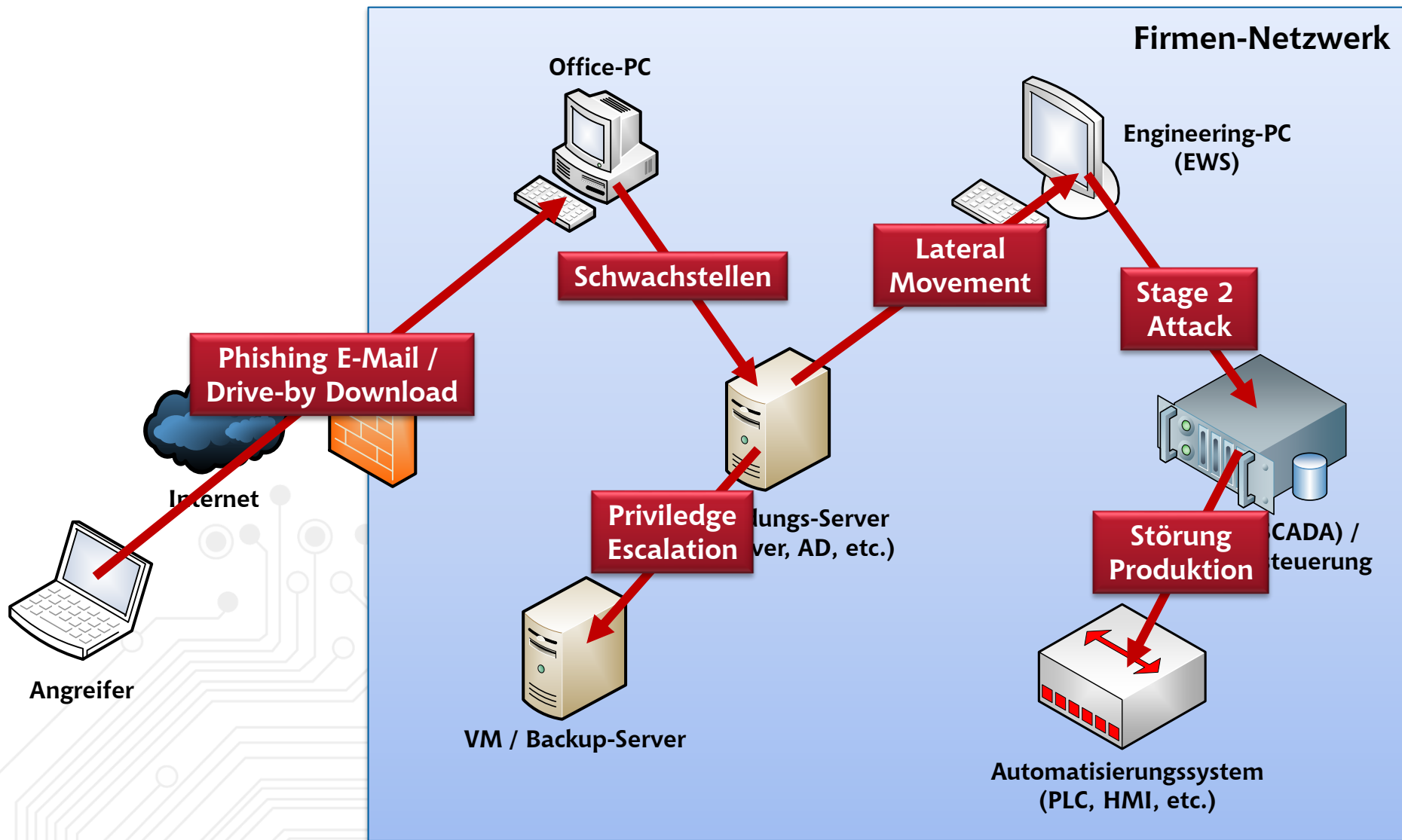
Zertifizierungen:

- CISSP-ISSAP/ISSMP/ISSEP, CSSLP, CISM, CISA, ISO 27001 Manager/Auditor, TÜV Trusted Sec. Auditor
- SANS/GIAC GICSP/GRID/GPEN/GXPN/GWAPT/GAWN/GMOB/GCPN, IEC 62443, CMSE, CEH, etc.



Wozu überhaupt IEC 62443?

Ein „typischer“ Tag in einem Industrieunternehmen...



Also was tun?



62443



IEC 62443 to the rescue

Secure System Design

Risk Assessment, Zones and Conduits,
Security Levels, etc.

62443-3-2



Cyber Security Management

Configuration Mgmt, Network Security,
User access control, etc.

62443-2-1

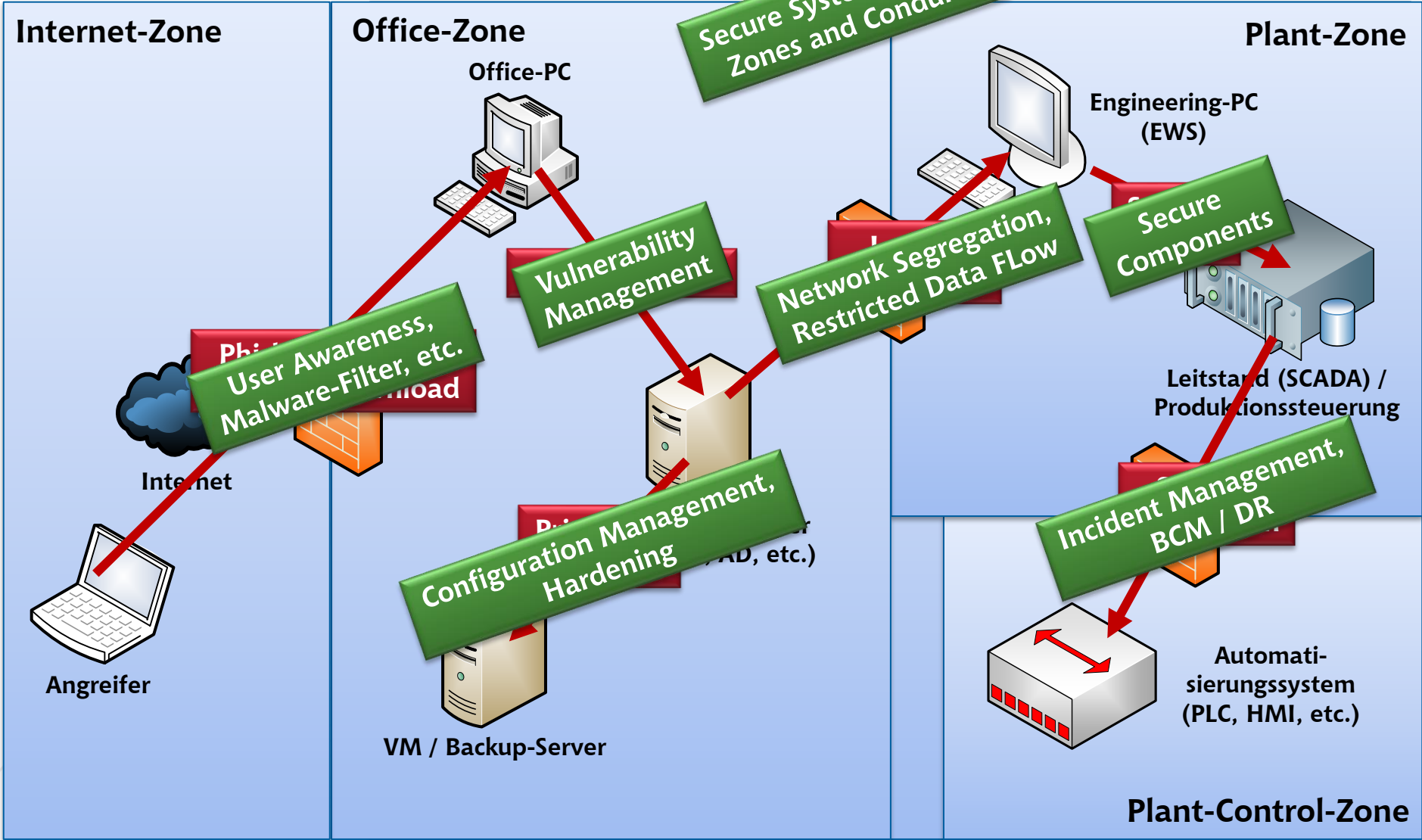


Secure components & lifecycle

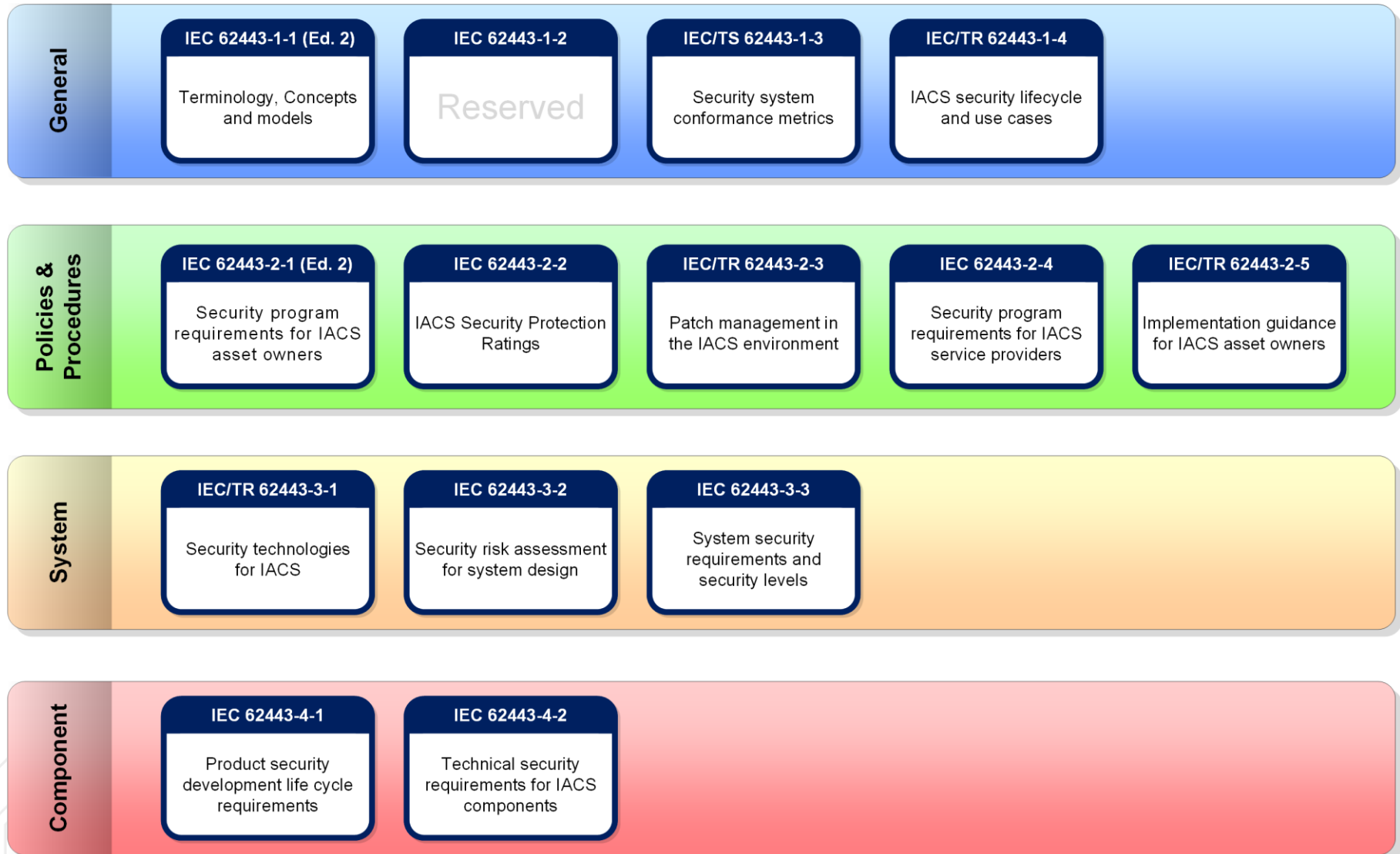
Security features, tested and verified
Vulnerability mgmt.

62443-4-2

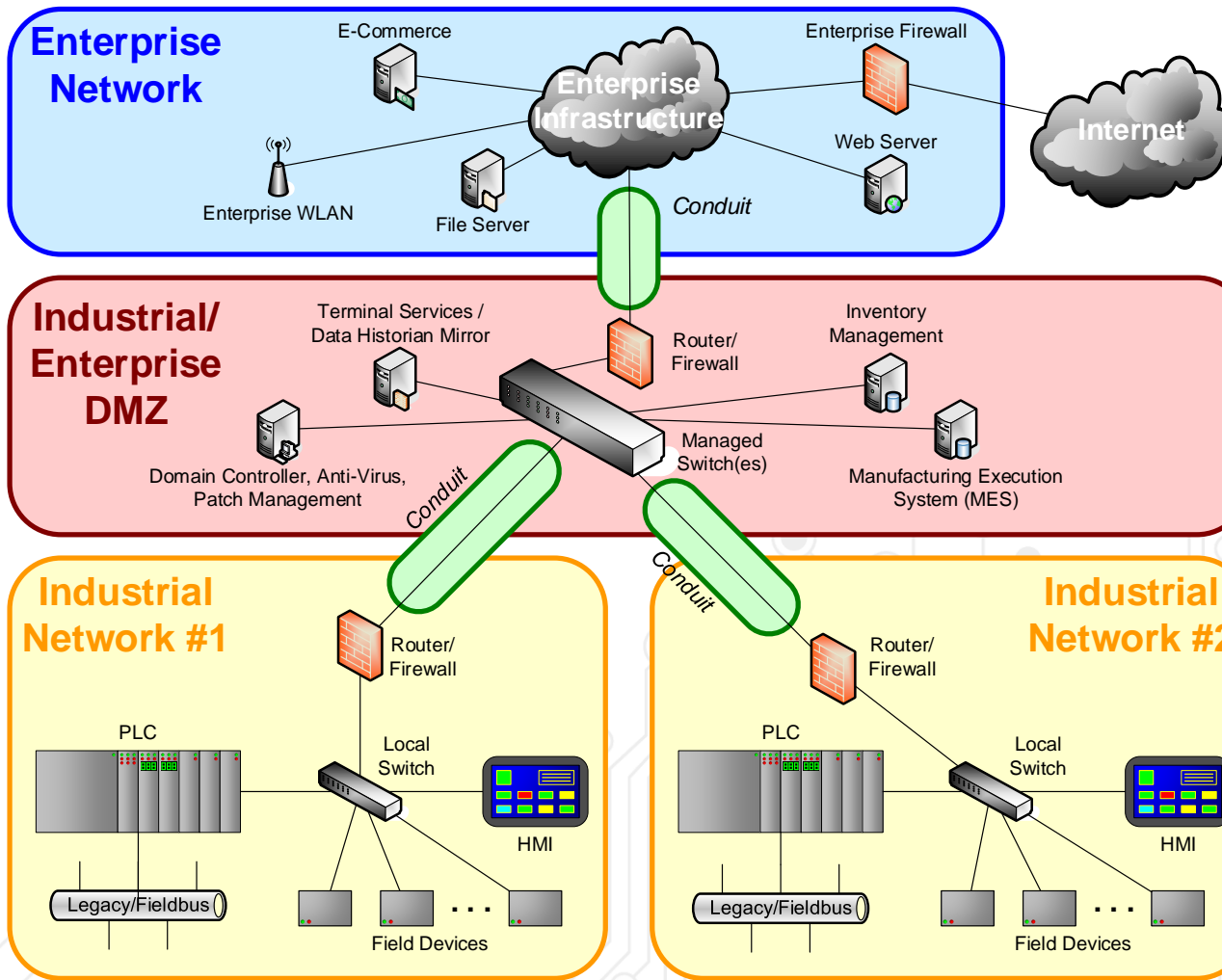
Problem gelöst 😊



Die IEC 62443 – Security for „IACS“



Scope der IEC 62443 Standards



IT Security Policies & Pract.
(e.g. ISO 2700x, etc.)

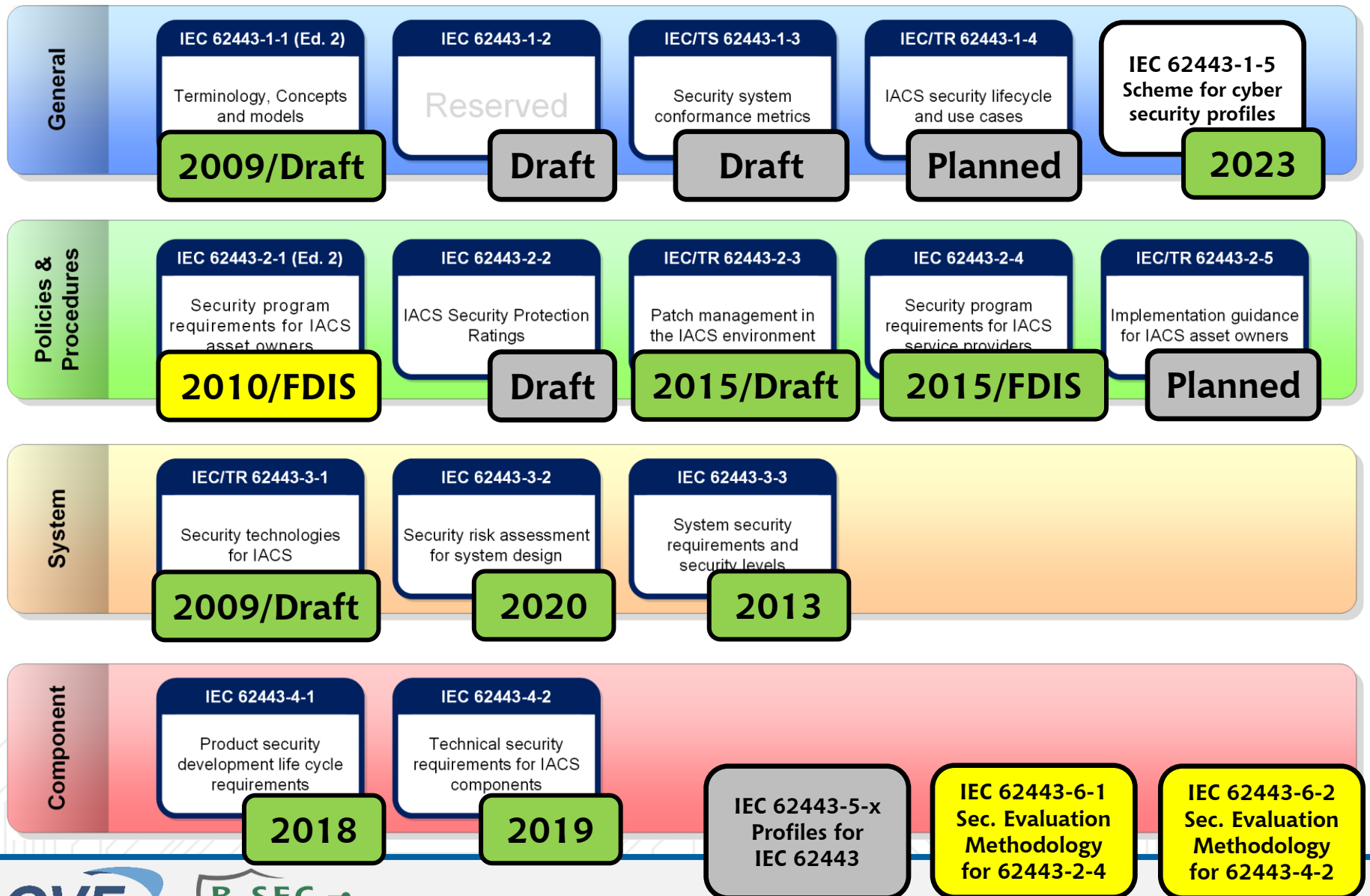


Process Safety
(e.g. IEC 61508)



ISA/IEC 62443
OT Security Policies & Practices

Status der IEC 62443 Normenreihe



Aktuelle Entwicklungen in der IEC 62443

Security evaluation methodology (für 2-4 & 4-2)

- Einheitliche Zertifizierung nach IEC 62443 – CSA / CRA
- 62443-6-1 und 62443-6-2 kurz vor Veröffentlichung

„Horizontal framework“ – Harmonisierung

- Standardization Request der EU - SRAHG

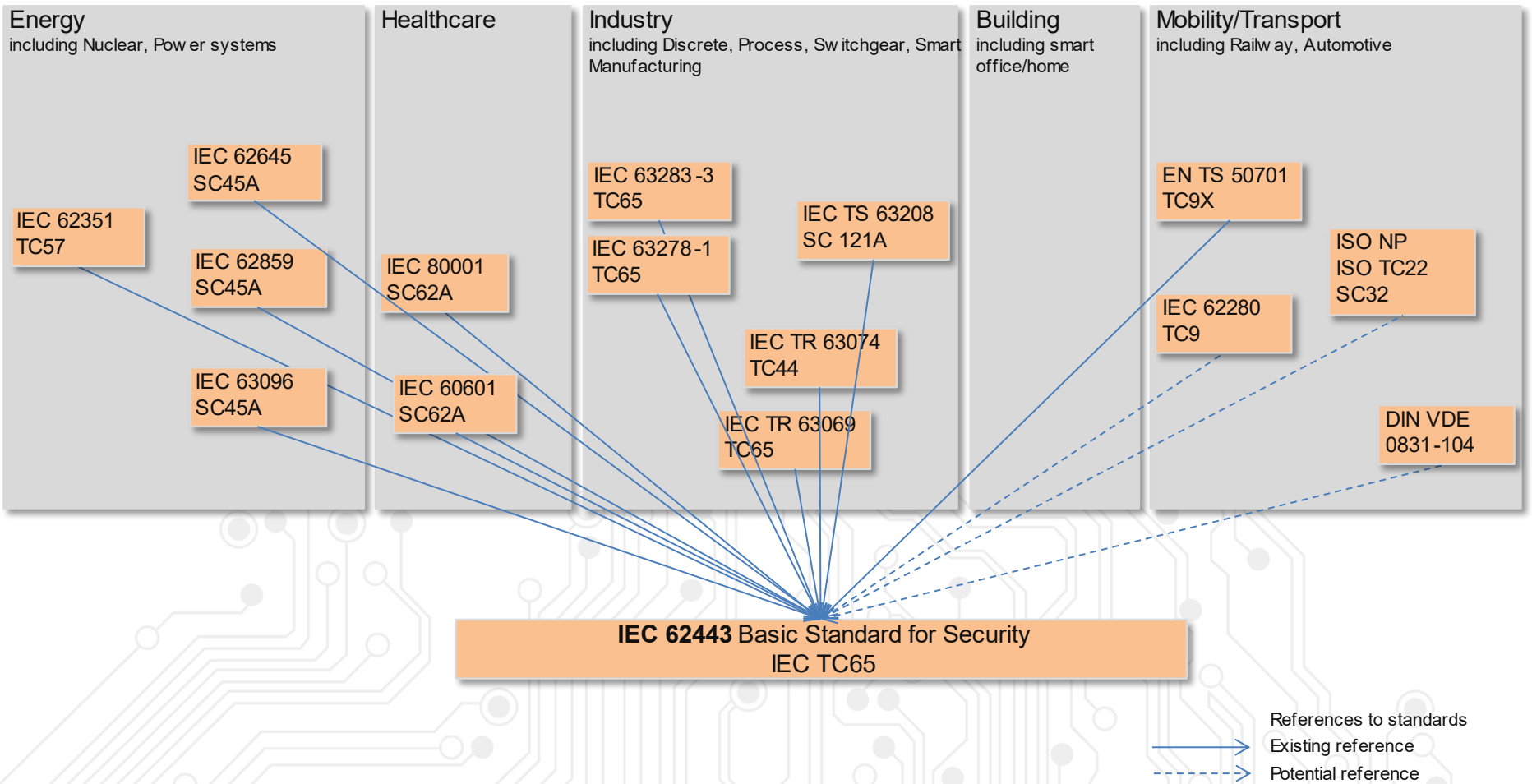
IEC 62443 Profiles (1-5) – Profile für Use-Cases/Branchen

- Standard fertig entwickelt, positive Abstimmung,

Weitere Teile die derzeit entwickelt/überarbeitet werden:

- **2-1 Ed. 2 - Security Program Requirements for Asset Owners**
- 2-2 – IACS Security Program Ratings
- 2-3 Ed. 2 – Patch Management in the IACS Environment
- 2-4 Ed. 2 – Security Program Requirements for Service Providers
- 3-1 Ed. 2 – Security technologies for IACS
- 3-3 Ed. 2 – System security requirements and security levels

IEC 62443 als Basis f. branchenspezifische Standards



from IEC TC65 WG10 TF Horizontality

OVE Akademie - Seminar zur IEC 62443

Systematische Absicherung industrieller Automatisierungssysteme mit der IEC 62443

Inhalt

Automatisierungssysteme sind immer häufiger Teil von modernen Industrieanlagen – und die Gefahr IT-basierter Angriffe auf diese Anlagen wird zu einem immer wichtigeren Aspekt bei der Planung und beim Betrieb solcher Systeme.

Im Seminar wird daher auf Basis der Norm IEC 62443 die systematische Absicherung von Automatisierungssystemen gegenüber Cyberangriffen anhand theoretischer Grundlagen und praktischer Beispiele vermittelt.

Die Teilnehmer können nach dem Seminar Gefahren für ihre Anlagen realistisch beurteilen und objektiv analysieren und dokumentieren, sowie systematisch Maßnahmen ergreifen um die Risiken zu senken.

- Gefahren und Herausforderungen im Bereich der Sicherheit industrieller Automatisierungssysteme
- Gesetzliche Anforderungen und Standards in diesem Bereich
- Aufbau eines IACS Information Security Programms
- Systematische Bedrohungs- und Risikoanalyse
- Design sicherer Anlagenkonzepte
- Anforderungen an Betreiber, Integratoren und Hersteller
- Sicherheitstechnologien für IACS
- Praktische Beispiele und Tipps für die Umsetzung

<https://www.ove.at/oveacademy>

Remember

Die IEC 62443 liefert **Best Practices für die Planung und Umsetzung von Cybersicherheitsmaßnahmen** für Betreiber, Systemintegratoren und Hersteller von industriellen Automatisierungs- und Steuerungssystemen (IACS)



Die Normenreihe wird ständig weiterentwickelt und von immer mehr **branchenspezifischen Normen** als Basis genutzt



Kontakt

Thomas Bleier

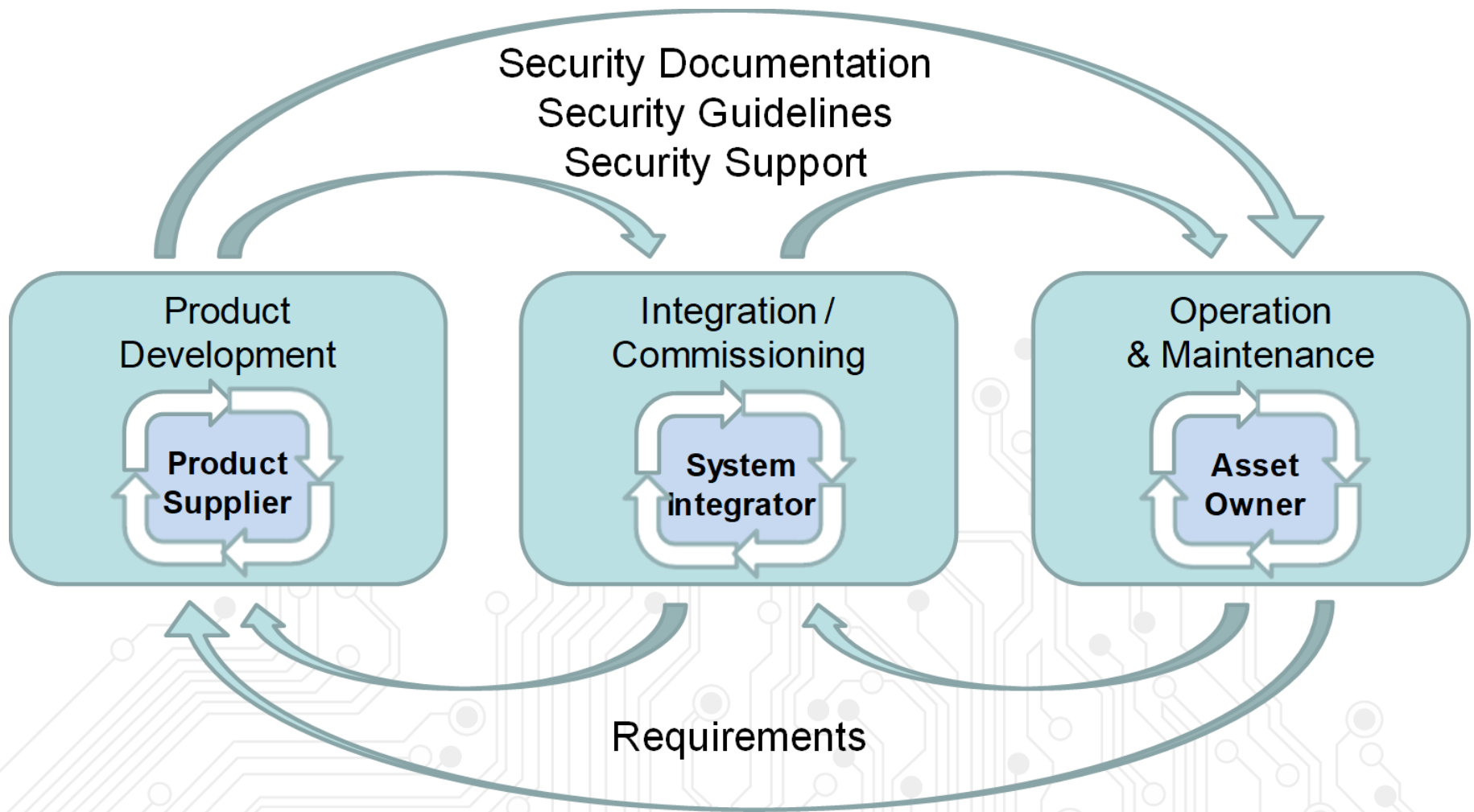
Dipl.-Ing. MSc CISSP-ISSAP, ISSMP, ISSEP CISA CISM CSSLP GICSP GPEN

 t@b-sec.net  **+43 664 3400559**

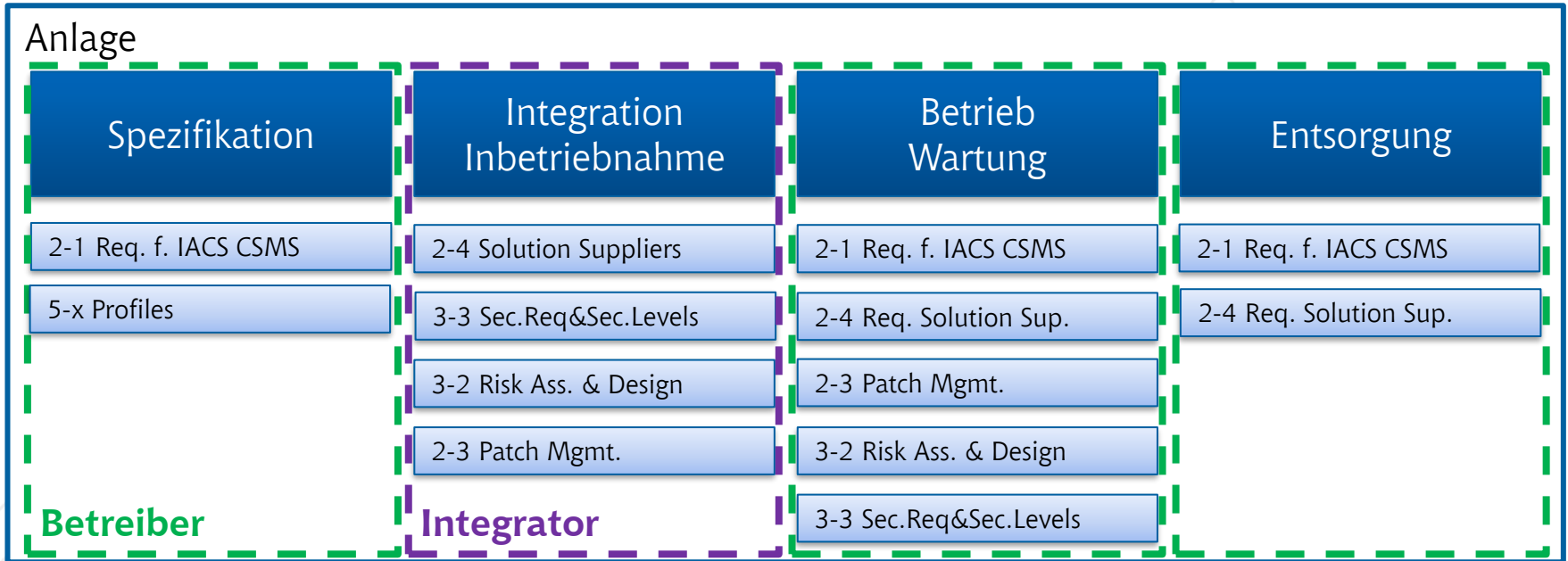
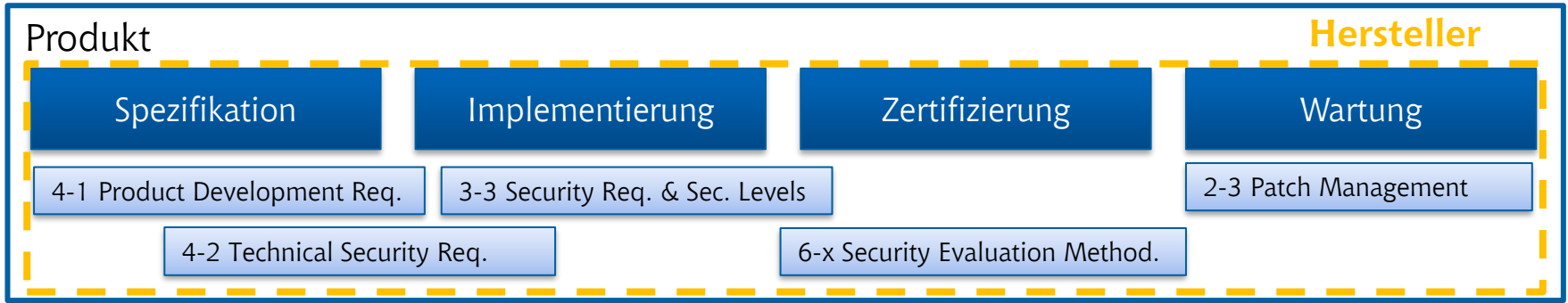


Backup

Rollen in der IEC 62443



Rollenspezifische Anwendung der IEC 62443

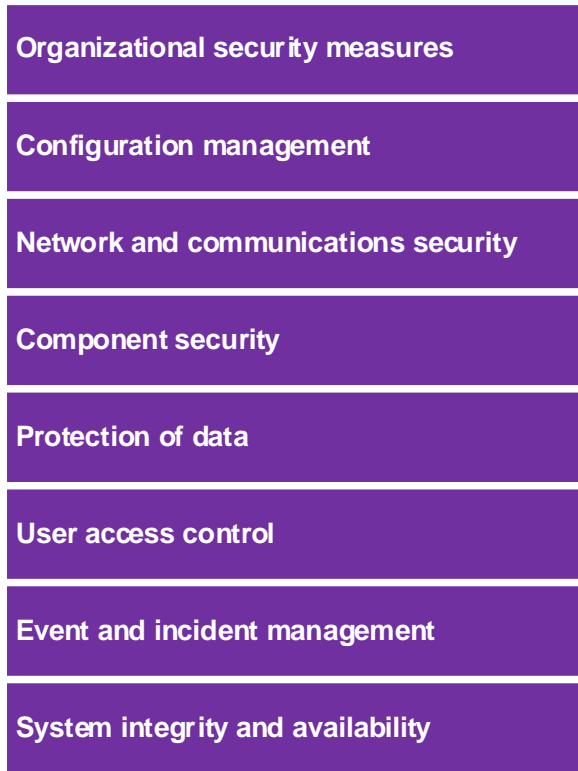


Security Level aus der IEC 62443

SL0	Keine Anforderungen bzw. kein Schutz notwendig				
SL1	Schutz gegen ungewollten, zufälligen Missbrauch				
SL2	Schutz gegen gewollten Missbrauch	Einfache Mittel	Niedriger Aufwand	Allgemeine Skills	Niedrige Motivation
SL3		Technisch ausgefeilte Mittel	Moderater Aufwand	IACS spezifische Skills	Moderate Motivation
SL4			Erheblicher Aufwand		Hohe Motivation

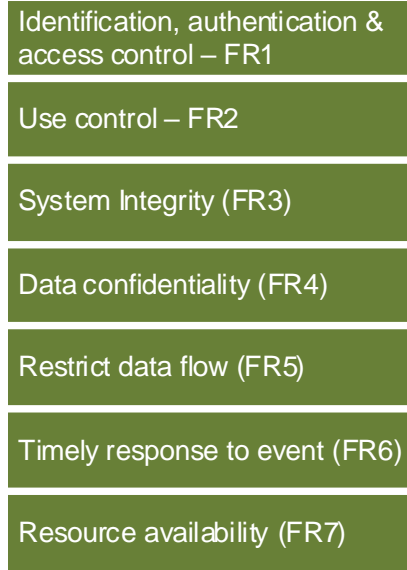
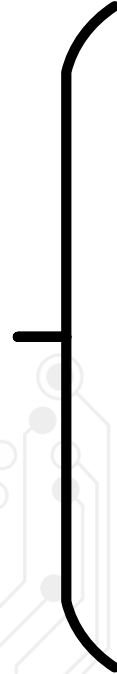
Angreifer

Security Element Groups



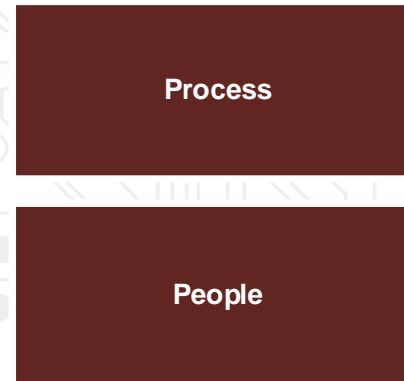
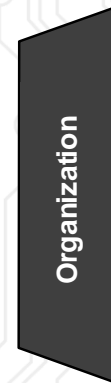
Security program requirements

ISA/IEC 62443-2-1
ISA/IEC 62443-2-2



ISA/IEC 62443-3-3
ISA/IEC 62443-4-2

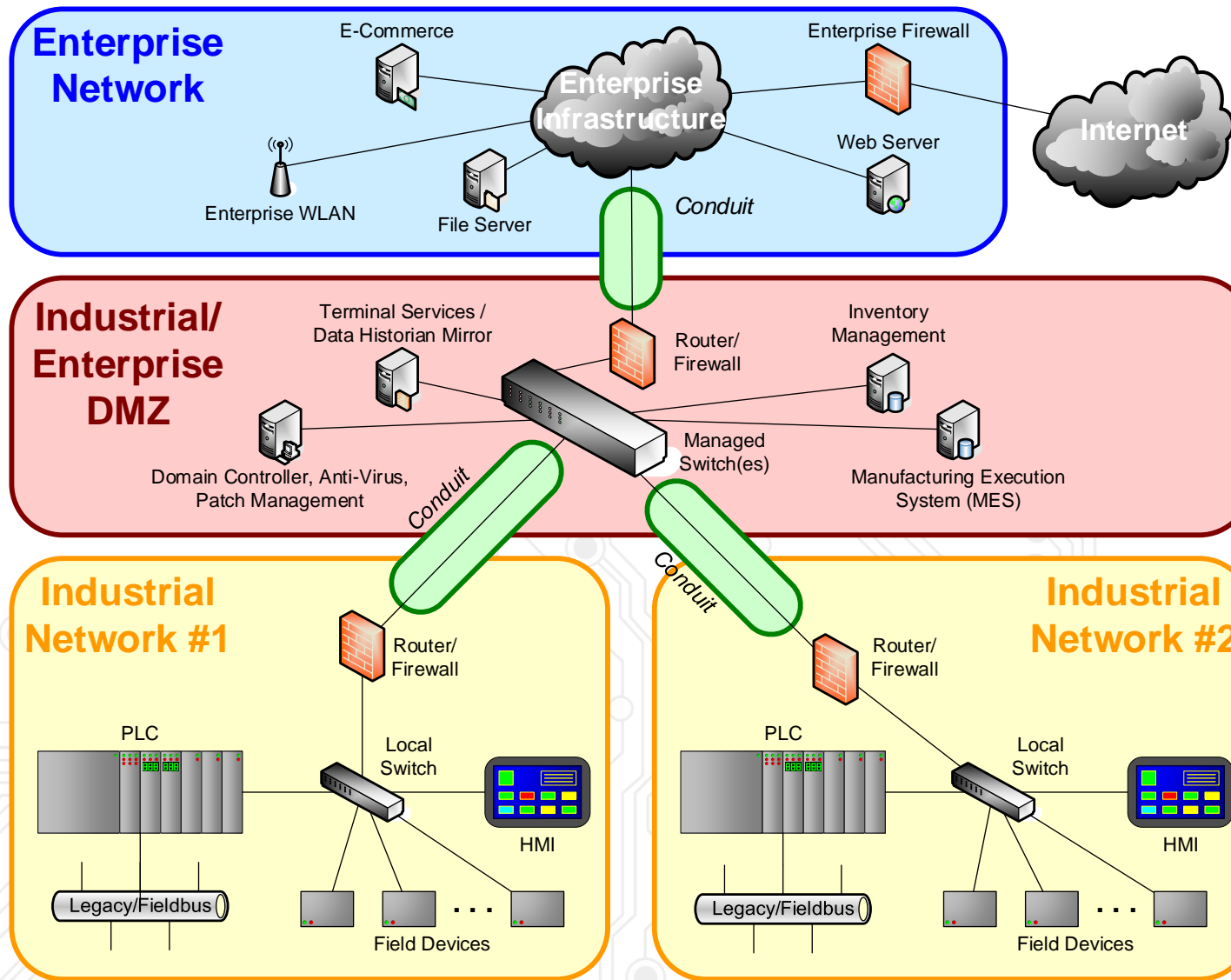
Technical Requirements



ISA/IEC 62443-2-1
ISA/IEC 62443-2-2
ISA/IEC 62443-2-4
ISA/IEC 62443-4-1
ISO 27001 & other ISMS

Organizational requirements

Zones and Conduits



ISA – International Society of Automation

- Non-profit technical society for engineers
- Previously „Instrument Society of America“, now international focus
- Many workings groups on automation technology and different application areas
- Publications, training courses, certification programs, etc.
- Cybersecurity Standard started as ISA99, later joined efforts with IEC to develop IEC 62443



IEC – International Electrotechnical Commission

- International Standards for electrical, electronic and related technologies
- See also ISO / ITU / IETF and ETSI / CEN / CENELEC / etc.
- ISO/IEC JTC 1 (Joint Technical Committee)
 - Information technology related standards
 - ISO/IEC 2700x, ISO/IEC 15408, etc.
- IACS Security standards 62443 developed as part of TC 65 (Industrial-process measurement, control and automation)
- > 80 countries, > 100 technical committees, > 500 working groups, > 6700 standards



OVE – Österreichischer Verband für Elektrotechnik

- Nationaler Verband für elektrotechnische Normung
- Nationalkomitee des IEC
- Jedes Mitgliedsland (>80) hat im IEC eine Stimme
- IEC TC65 → OVE TSK MR65 „Industrielle Prozess-, Mess-, Regelungs- und Steuerungstechnik“
- AG MR65 IACS Security → IEC 62443 + related Standards
- GIT – Gesellschaft für Informationstechnologie im OVE



IEC standard development process (overview)

Proposal of a new / revised standard

Preliminary work item (PWI)

New Work Item Proposal (NP)

Review Report (RR)



Preparation of the content

Working Draft (WD)

Committee draft (CD)

Document for Comments (DC)



Commenting/Review

Committee draft for vote (CDV) (only for IS)

Compilation of comments (CC)



Voting

Final draft international standard (FDIS)

Draft Technical Standard (DTS)

Draft Technical Report (DTR)



Publication

International Standard (IS)

Technical Specification (TS)

Technical Report (TR)