Harmonisierte Normen zur Umsetzung des Cyber Resilience Act

Thomas Bleier

t@b-sec.net

☎ +43 664 3400559

Classification:	PUBLIC
Version:	01
Date:	20.11.2023
Status:	Final

B-SEC better secure

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 - Spiegelkommittee 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.

Cyber Resilience Act

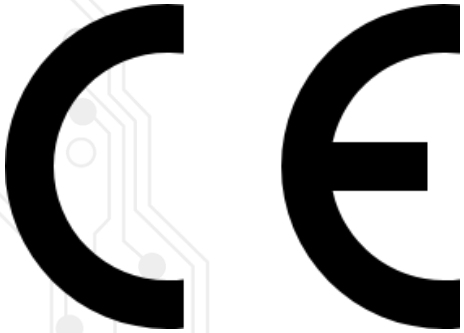
Definiert IT-Sicherheitsanforderungen für Produkte / Services, spezifiziert aber keine Details zur Umsetzung…

Wie kann ich als Unternehmen also feststellen, ob mein Produkt die Anforderungen erfüllt?

- Eigener Nachweis der Interpretation der Anforderungen?
- Prüfung/Begutachtung durch unabhängige Stellen?
- Warten ob sich jemand beschwert dass die Anforderungen nicht erfüllt sind? ☺
- … ???

Exkurs: Maschinensicherheit (Safety)

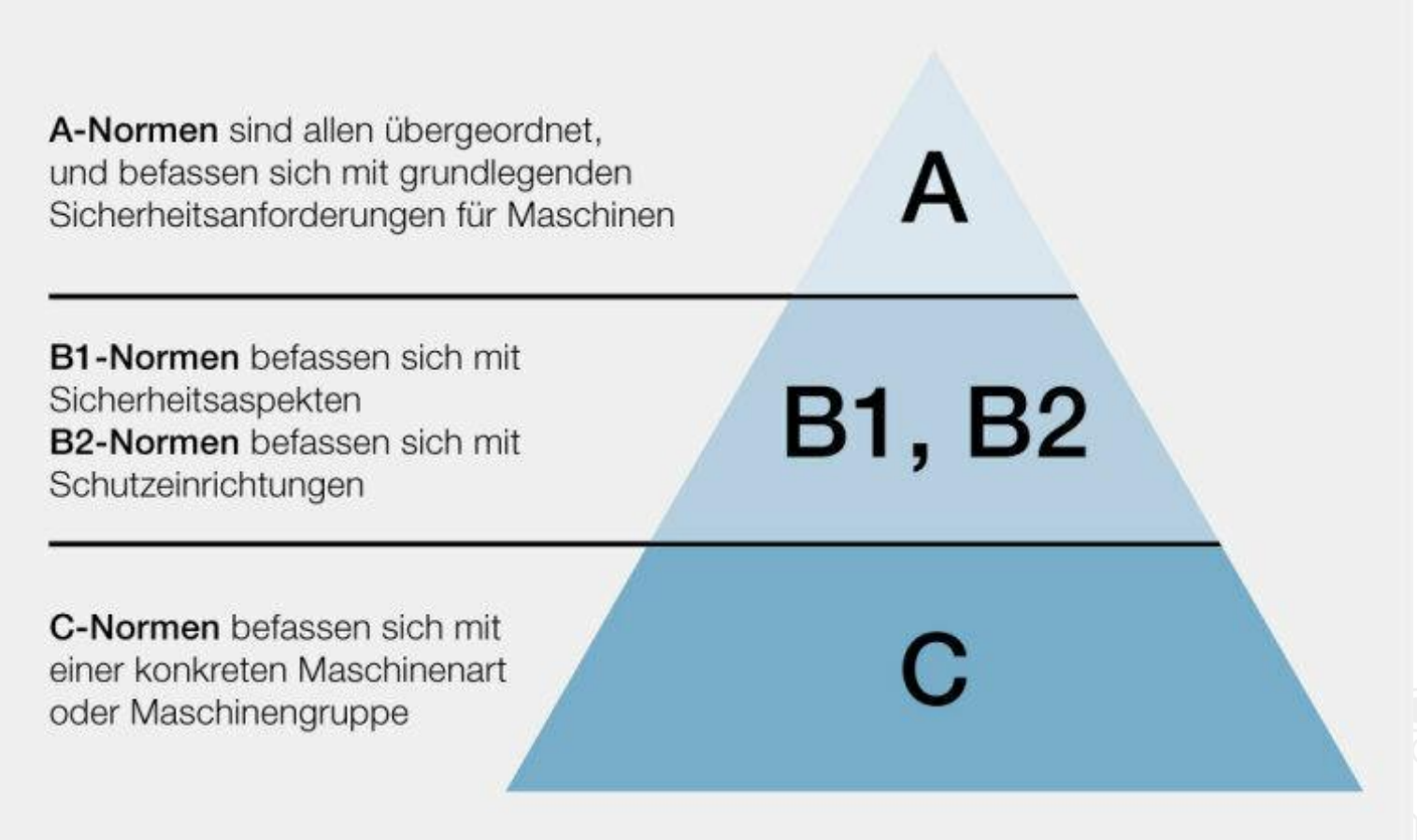
- Maschinenrichtlinie (EU RL 2006/42/EG) definiert Anforderungen an die Sicherheit (Safety) von Maschinen
- Inverkehrbringen in der EU nur erlaubt, wenn **alle** geltenden Richtlinien erfüllt werden
- → CE Kennzeichen
- CE Kennzeichen dokumentiert Erfüllung **aller** geltenden Richtlinien denen ein Produkt unterliegt



„… dass das Produkt den geltenden Anforderungen genügt, die in den Harmonisierungsrechtsvorschriften der Gemeinschaft […] festgelegt sind."

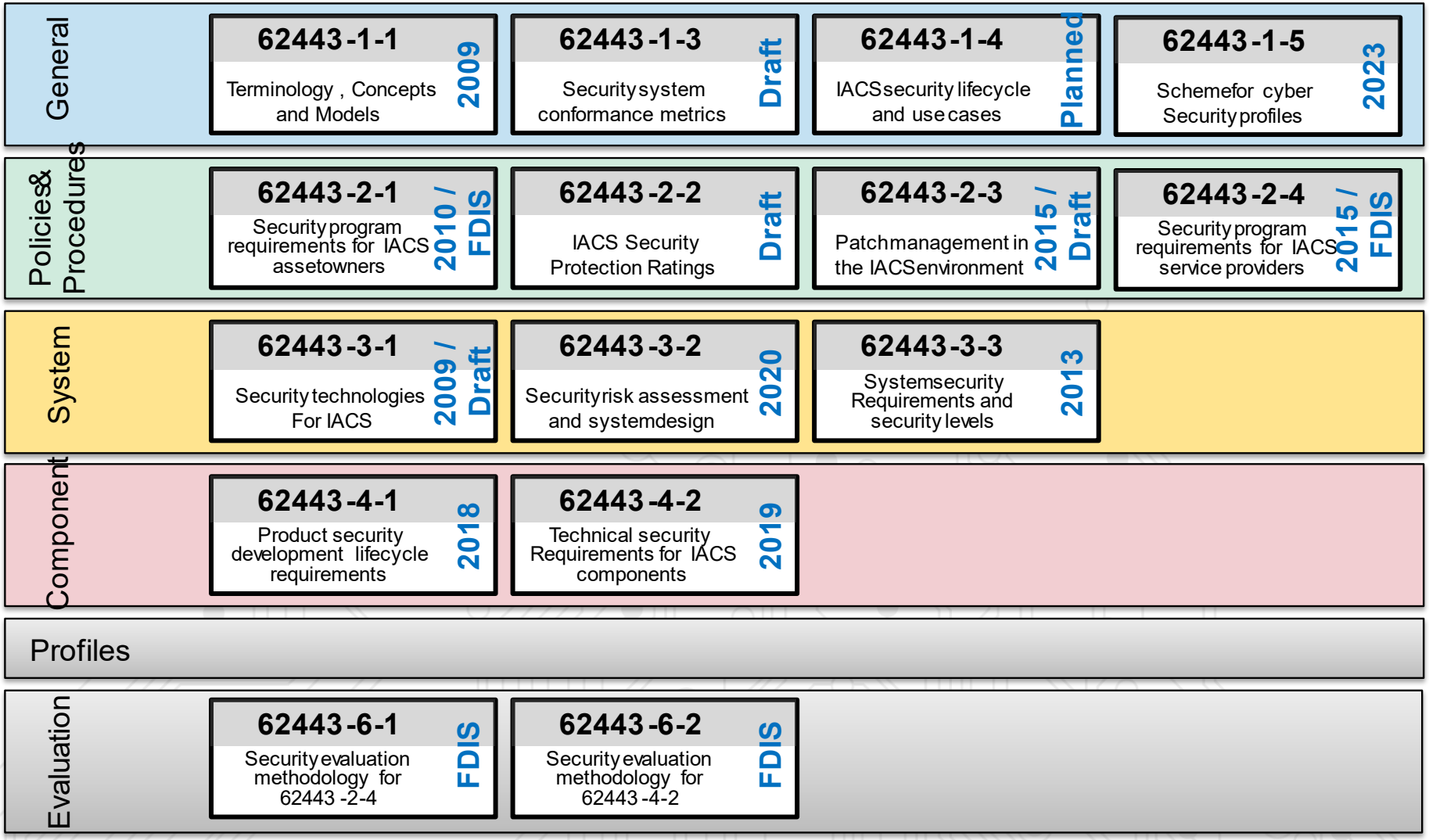
Exkurs: Maschinensicherheit (Safety)

→ Nachweis der Anforderungen: harmonisierte Normen

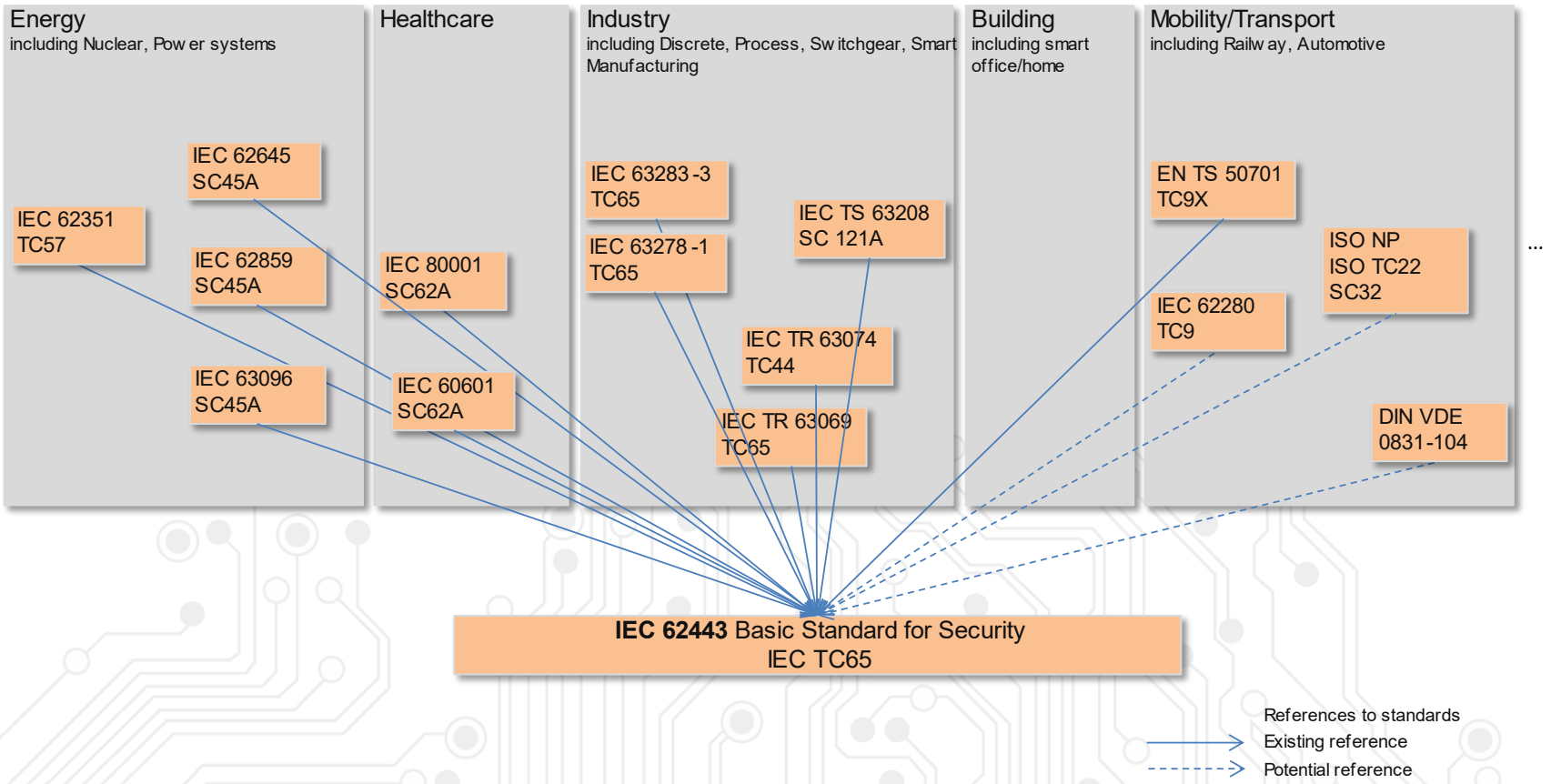


Quelle: https://www.pilz.com/de-AT/support/law-standards-norms/iso-standards

Die IEC 62443

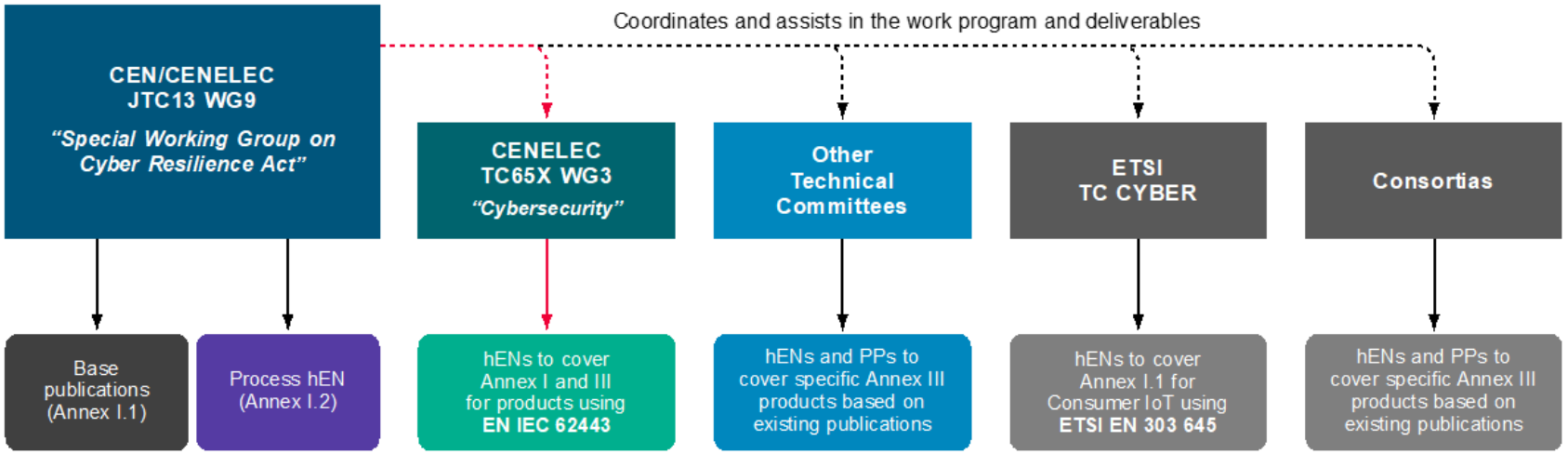


IEC 62443 als Basis f. branchenspezifische Standards



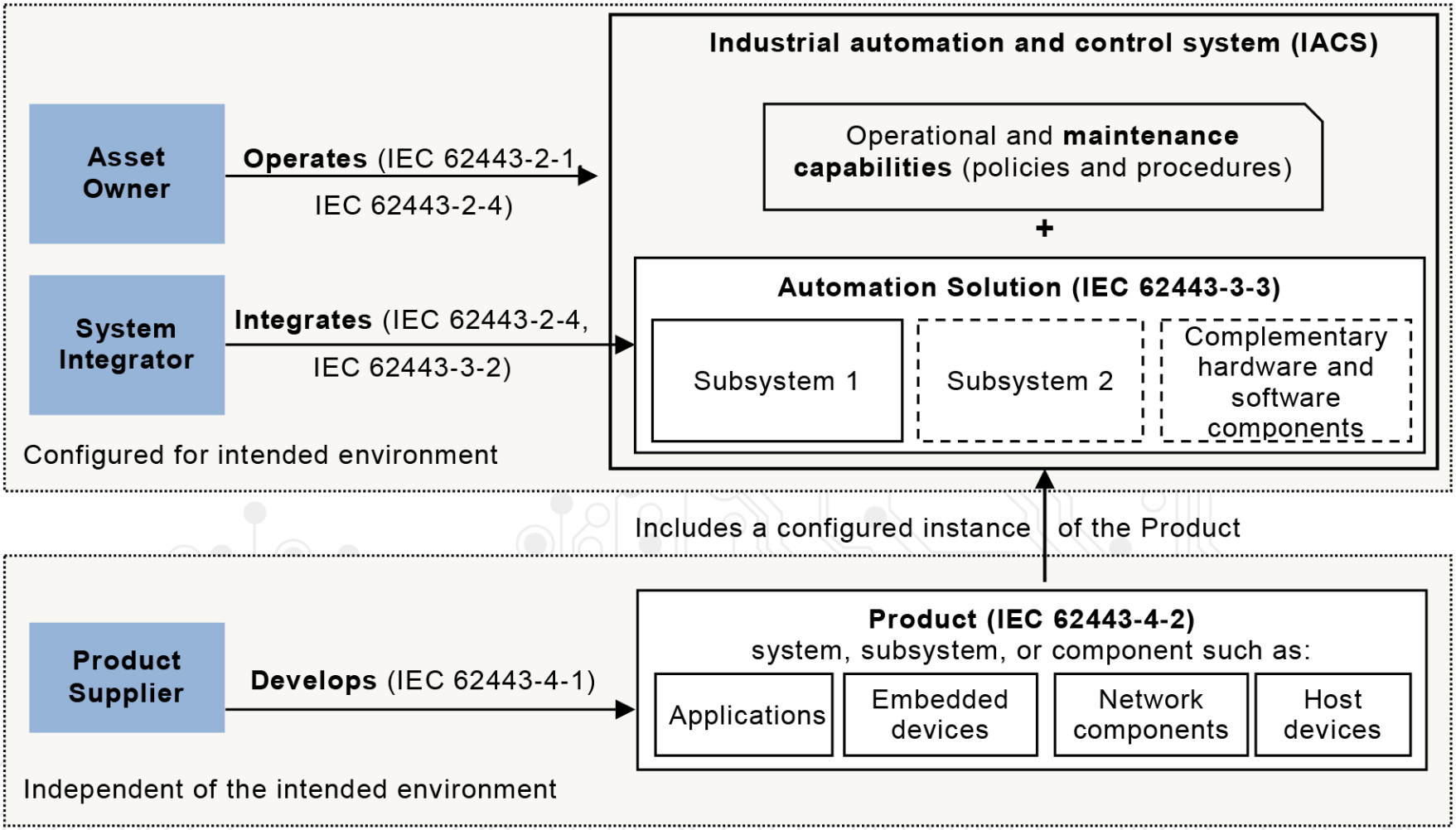
Standardisierungs-Arbeitsgruppen zum CRA

Overview/Structure CEN/CLC JTC13 WG9
(in discussion)

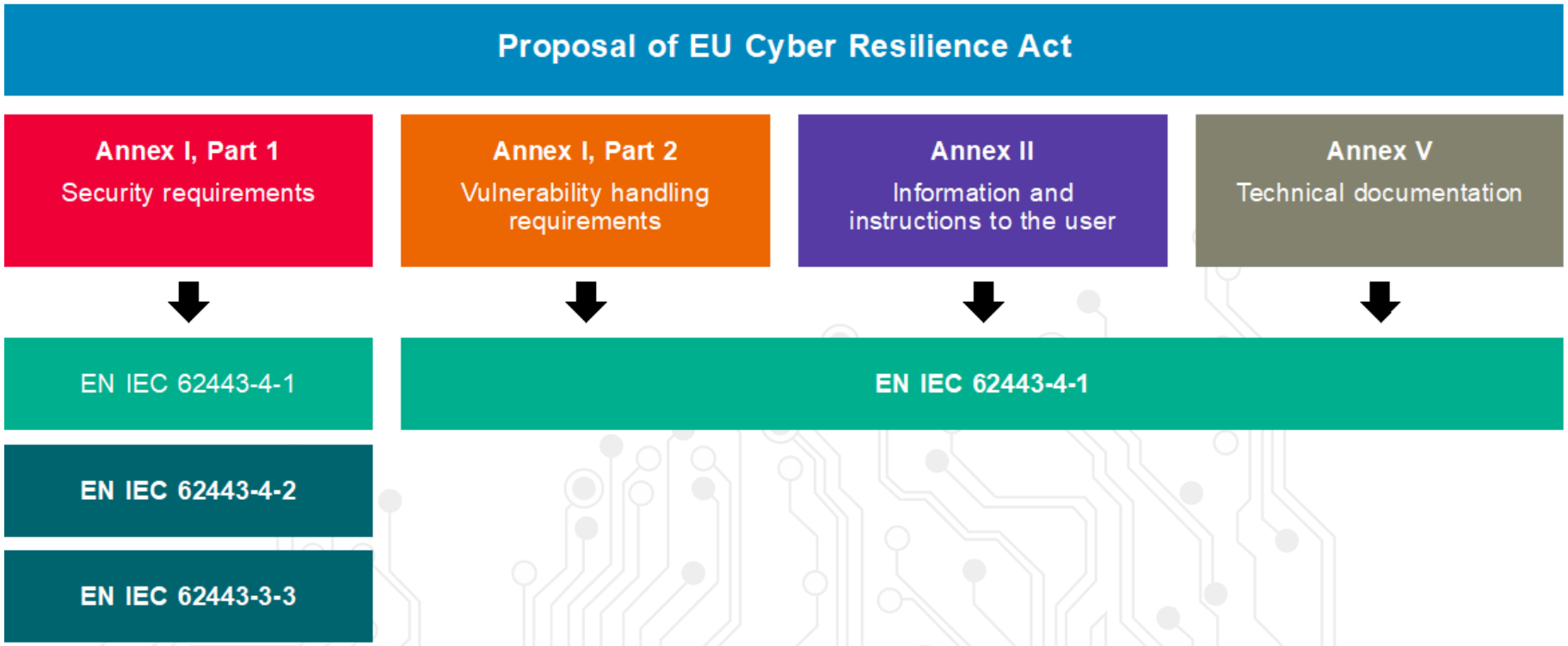


31.10.2023

Rollen & Verantwortlichkeiten für OT Security

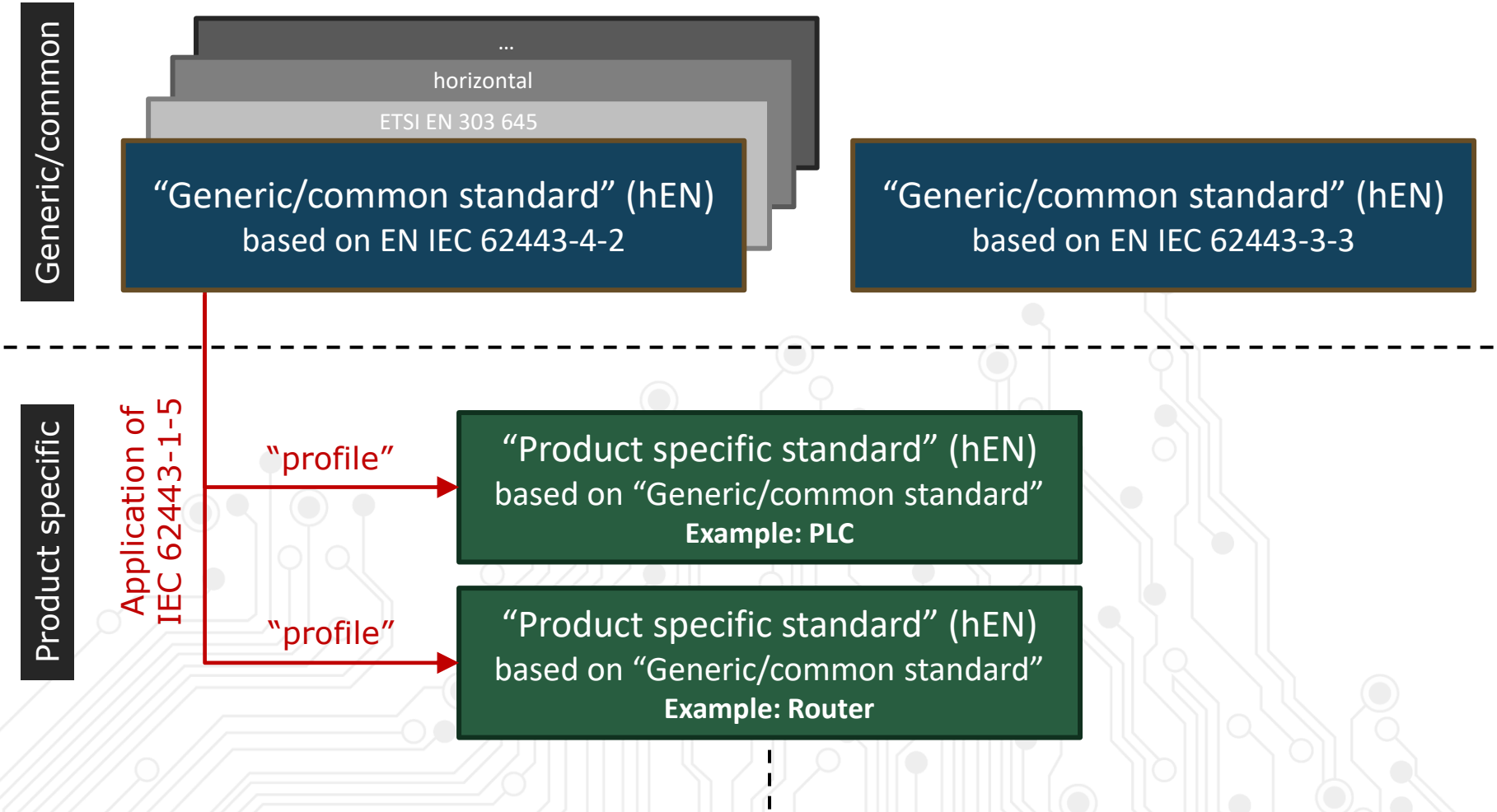


TC65X WG3 Vorschlag



Aktueller Diskussionsstand aus CENELEC TC65X WG3 – nicht final!

Umsetzung von hEN auf Basis IEC 62443



Was bedeutet das für Unternehmen?

- Anwendung harmonisierter Normen → „Konformitätsvermutung“
- Prüfung: entsprechend der Anforderungen des CRA entweder intern, durch externe Dritte oder durch „benannte Stellen“ (Produktzertifizierung)
- IEC 62443 voraus. wesentliche Grundlage für hEN‘s → kleine Änderungen möglich, aber Basis vorhanden
- Dokumentation: Nachweis der Erfüllung der Anforderungen im Entwicklungsprozess

Remember

Effizientester Weg der Umsetzung der CRA Anforderungen ist vermutlich die Anwendung harmonisierter Normen

Die IEC 62443 ist eine wesentliche Grundlage für hEN‘s

Diese Anforderungen können jetzt schon in die Produktentwicklungsprozesse einfließen um Produkte fit für die kommenden Anforderungen des CRA zu machen

Nebenbei werden die Produkte damit auch sicherer ☺

Kontakt

Thomas Bleier

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

t@b-sec.net ☎ +43 664 3400559

B-SEC better secure

https://www.b-sec.net