secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

IEC 62443: Prüfschema und typische Erkenntnisse bei Zertifizierungen

„Industrial Security“, Bubenreuth

Sebastian Fritsch, secuvera

- Sitz der Gesellschaft: Gäufelden „bei Stuttgart“
- Gründung: 1. Juli 1982
- aktuell 20 Mitarbeiter
- Inhabergeführt
- Herstellerunabhängig
- Berater, keine Consultants
- IT-Sicherheit seit 1988
- reiner IT-Sicherheitsdienstleister

- Drei Beratungsfelder
  - BSI-Prüfstelle für Common Criteria (Produktzertifizierungen)
  - Penetrationstests/Webanwendungsprüfungen
  - BSI-Grundschutz/ISO 27001
- BSI-zertifizierter IT-Sicherheitsdienstleister
  - Kompetenzfeststellung durch das Bundesamt für Firma und Berater

- BSI-Prüfstelle

  auch anerkannt bei TÜV NORD CERT
  für Prüfungen nach IEC 62443

  Zertifizierung von

  - Komponenten (62443-4-1 und 62443-4-2)
  - Systemen (62443-3-3)
  - Anlagen (62443-2-1 und 62443-2-4)

In cooperation with TÜV NORD

IEC 62443

- OT Security Incidents

Stromausfall in der Ukraine augenscheinlich durch Hacker ausgelöst

06.01.2016 11:32 Uhr – Stefan Krempl vorlesen

- # BSI Report Industrial Control System Security: Top 10 Threats and Countermeasures 2019

Source: BSI

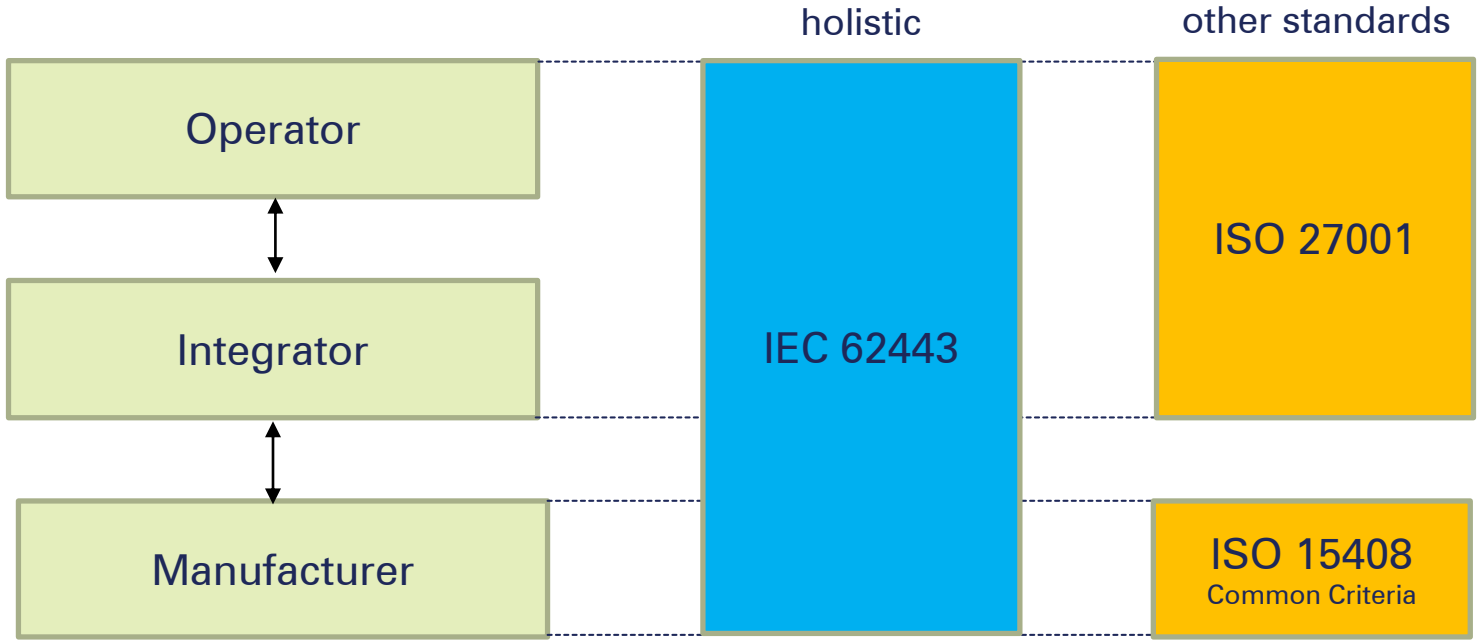
Top 10 Bedrohungen	Trend seit 2016
Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	↗
Infektion mit Schadsoftware über Internet und Intranet	↗
Menschliches Fehlverhalten und Sabotage	↑
Kompromittierung von Extranet und Cloud-Komponenten	↑
Social Engineering und Phishing	↘
(D)DoS Angriffe	↑
Internet-verbundene Steuerungskomponenten	→
Einbruch über Fernwartungszugänge	→
Technisches Fehlverhalten und höhere Gewalt	↘
Kompromittierung von Smartphones im Produktionsumfeld	→

- Extract ICS-Security Standards

  Alphabetical order
  - BDEW-Whitepaper & Praxisleitfaden
  - BSI Industrial Control System Security Compendium
  - CPNI: Process Control and SCADA Security

    CPNI = (UK) Centre for the Protection of National Infrastructure
  - **ISA/IEC 62443: Security for industrial automation and control systems**
  - ISO 27001 bzw. ISO 27019: Leitfaden für das Informations-sicherheits-Management von Steuerungssystemen der Energieversorgung auf Grundlage der ISO 27002
  - NIST SP 800-82: Guide to Industrial Control Systems Security
  - VDI/VDE Richtlinie 2182: Informationssicherheit in der industriellen Automatisierung

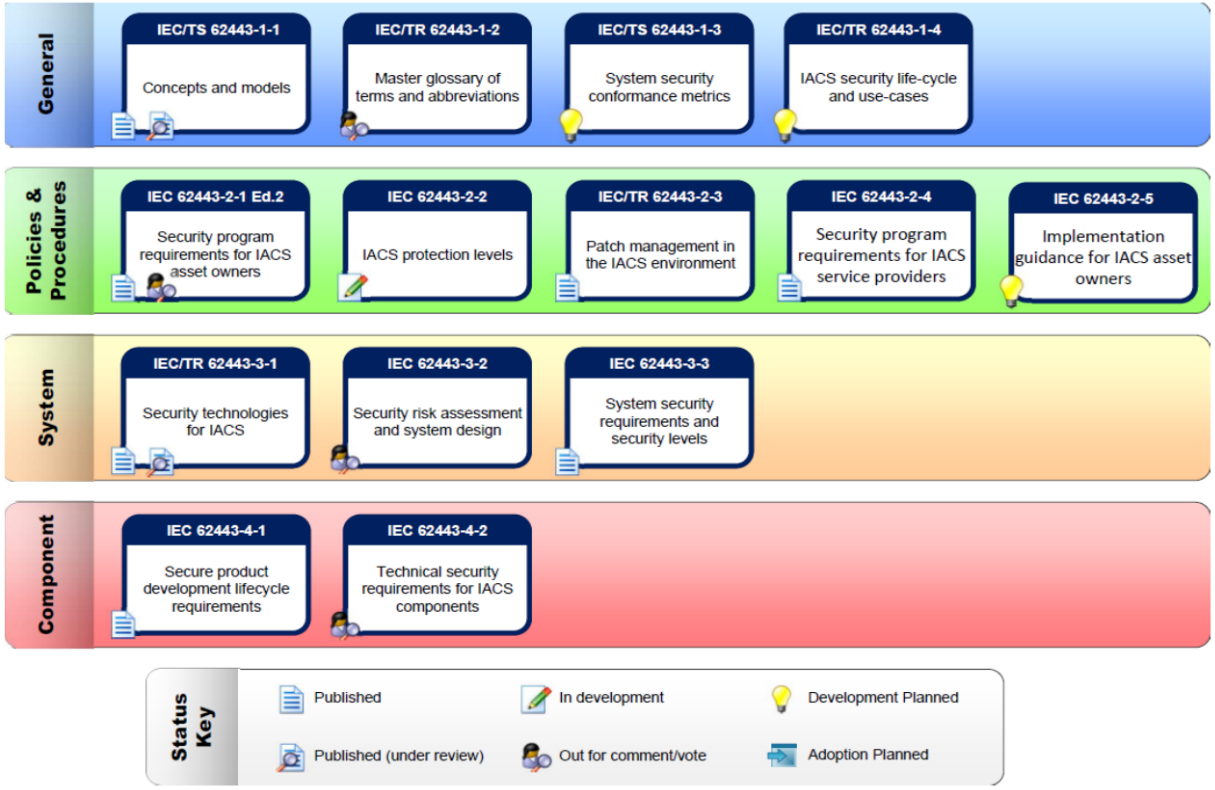
- Focus of IEC 62443



- Global Principles in IEC 62443
  - Developer, Integrator und Operator
  - Defense-in Depth
  - Zones and Conduits
  - Technical measures and processes
  - Applicable for brownfield and greenfield
  - Security Levels: Requirements and attacker type

https://www.sichere-industrie.de/iec-62443-teil-1-iec-62443-einfuehrung-ueberblick/

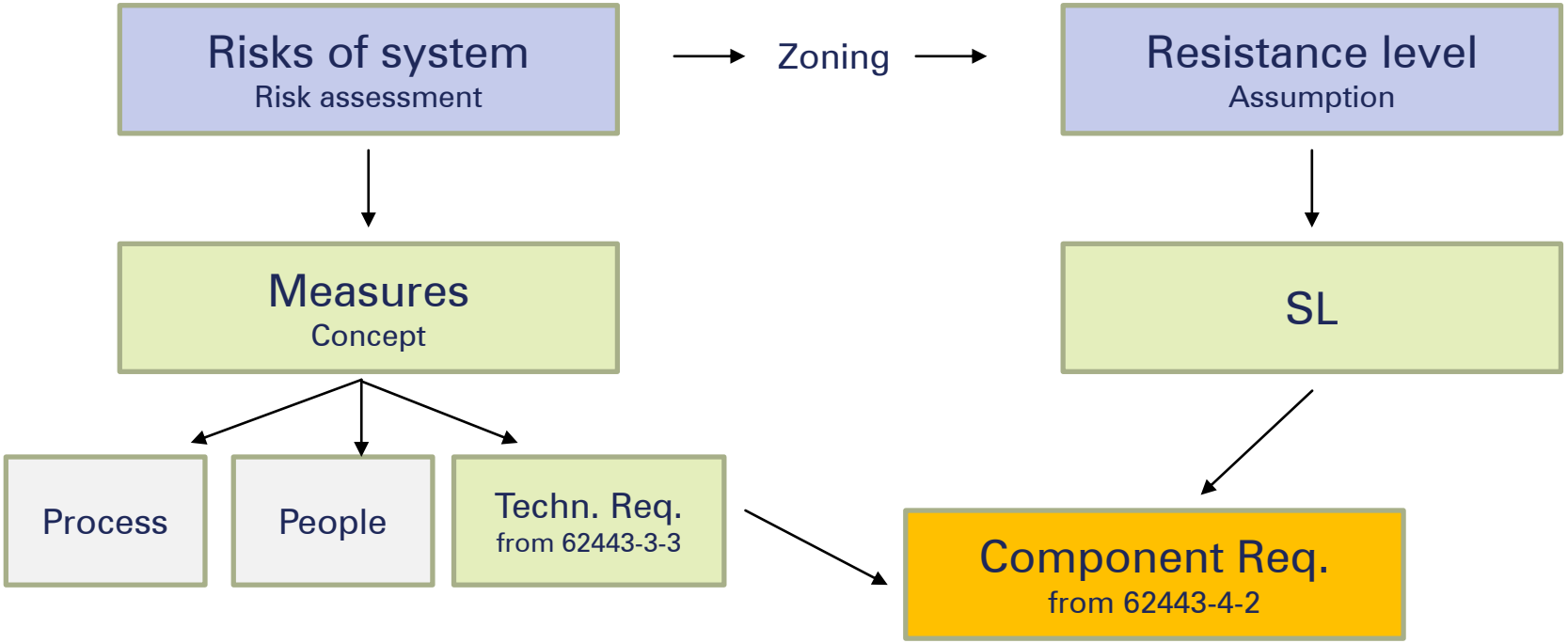
Structure of ISA/IEC 62443



Prüfschema für IEC 62443-4-2

Evaluation Methodology for IEC 62443-4-2

- IEC 62443 selection of technical requirements



- IEC 62443-4-2 key facts for component assessment
  - Component Types
    - Embedded Devices (e.g. PLC, Sensors)
    - Host Devices (e. g. notebooks or PC workstations)
    - Network Devices (e. g. Industrial Router)
    - Applications (e. g. Configuration software)
  - Security Level
    - Technical capability (selection of CR)
    - Resistance Level
  - Development/support following processes from 62443-4-1

- No evaluation methodology

Auditprozess:	NIST SP800-115 (adaptiert) & OSSTMM.
Konzeptaudit:	BSI Grundschutz-Katalog, IEC 62443-3-3, IEC62443-4-2 Draft.
Komponentenaudits:	Vulnerability-Analyse, Angriffe mit Standardwerkzeugen, Fuzzing über Ethernetport, Prüfung des Signierungsverfahrens für Firmware, Analyse der Kommunikationsverfahren.
Systemaudit:	Securityprüfung anhand eines Referenz-Aufbaus (Ende zu Ende), Schwachstellenanalyse der Komponenten von Drittherstellern mittels CVEs, OWASP Top 10 Bedrohungsanalyse.

  - No comparable results
  - No comparable IEC 62443 certificates
  - Wild west… (yee-haw)

- Why do we need an evaluation methodology (Prüfschema)?
  - IEC 62443-4-2 defines functional (+ process) requirements
    - process = IEC 62443-4-1 practices
  - Evaluation methodology defines assessment requirements
  - → Eval. Meth. not part of the standard
    - Missing content
    - Clarification for users of the standard

- IECEE (private certification scheme)
  - Program OD-2061 already defines:

	IEC 62443-2-4	IEC 62443-3-3	IEC 62443-4-1	IEC 62443-4-2 (Future Consideration)
Process	✓ Scenario 1		✓ Scenario 1	
Product	✓ Scenario 1*	✓ Scenario 1* Optionally in conjunction with an IEC 62443-4-1 Scenario 2 certificate***	✓ Scenario 2 possibly in conjunction with an IEC 62443-3-3 or IEC 62443-4-2 Scenario 1 certificate**	✓ Scenario 1* in conjunction with an IEC 62443-4-1 Scenario 2 certificate****
Solution	✓ Scenario 2			

  - But also no evaluation method

- Not only focused on certification
  - Scope is first-, second- or third-party assessment
  - Self-Assessment (first-party) was important design goal
  - More use cases:
    - Verification of suppliers technical capability linked to procurement process

- Overview Evaluation Method
  - Evaluation steps
    1. Intended Use Verification
    2. Documentation (Design)
    3. Documentation (User)
    4. Conformity Assessment
    5. Vulnerability Analysis
  - plus
    - Acceptance criteria
      - Clarification but still technology agnostic
    - Component specification
      - Additional guidance for component developers
  - Limited to: SL-1 - SL-3
    - less experience with SL-4

- Discussions/Standardization
  - TeleTrusT content contributed to German standardization working groups
    - Initiative from TeleTrusT helped to gain response from vendors, certifiers and national security agencies
    - But long-term approach needs standardization
  - Two tracks
    - IECEE: Submitted for adoption as guideline document for certification
    - IEC / ISA99: Proposal to add evaluation method into the standard

Erkenntnisse bei Zertifizierungen / Prüfungen

- IEC 62443 Zertifizierungen
  - werden bisher wenig bis nicht durchgeführt
  - Mehrwert für Markt noch nicht klar
  - Einkäufer fragen nach “Security”, aber (noch) nicht nach “Norm xxx umgesetzt”
  - Verdacht: erste Welle durch Marketing-Budgets bezahlt

- erste IEC 62443 Zertifizierungen
  - Fokus hier: IECEE Schema
    - 2x IEC 62443-2-4 Integrator Lösungen / Dienstleitungen
    - 1x IEC 62443-4-1 Entwicklungsprozess
    - 0x IEC 62443-4-2 Komponenten*
  - zusätzlich
    - Zertifizierungen außerhalb IECEE, z. B. in DE nach DAkkS
    - ISAsecure Schema
    - UL (kein IEC 62443!) *führt zu weiterer Unsicherheit*
    - …
  - aber keine/wenig Prüfmethodiken veröffentlicht

* aktuell nur TÜV NORD anerkannt fürIEC 62443-4-2 Komponenten
https://www.iecee.org/dyn/www/f?p=106:58:0::::FSP_STD_ID:34421

- Trend bei Regulierung
  - EU hat 2019 Cybersecurity Act in Kraft gesetzt
  - Fokus auf Produkte
    - nicht auf Anlagen/Systeme
  - 2020 wird eine Initiative bzgl. KRITIS-Komponenten erwartet
    - ggf. ab 2021 ein EU-weit einheitliches Zertifizierungsschema
    - IEC 62443 ist ein Kandidat

- IEC 62443-4-2 Prüfprojekte bei secuvera bisher i.d.R. nach “time-box”-Modell
  - Fokus: Feststellung Reifegrad, risiko-orientiertes Vorgehen
  - Typisches Projekt: 20 PT, davon 12 PT technische Prüfung
- Erkenntnisse
  - Getestete Produkte wurden nicht bzgl. Security entwickelt
    → man merkt es, d.h. viele Empfehlungen
    → Verwendungszweck und Security Context nicht festgelegt
      z. B. Welche Netzwerke werden angebunden? Sind weitere physisch Schutzmaßnahmen notwendig, oder ist das Gerät bereits selbst sicher?

- Typische Prüfergebnisse
  - Authentisierung: Standard-Kennworte, feste Berechtigungsstufen mit Rollen-Benutzern
  - Kommunikationssicherheit: bei Echtzeitnetzwerken in den Protokollen nicht vorgesehen
  - Firmware: keine Schutzmaßnahmen gegen Reverse-Engineering und Manipulationen

- Fazit
  - Pragmatisch vorgehen: beginnen!
    - Standard ist für Hersteller stabil und fertig
    - IEC 62443 Vorgehensweisen nutzen

      https://www.sichere-industrie.de/iec-62443-teil-2-vorgehensweisen/
  - Verbesserung des Entwicklungsprozesses durchführen: IEC 62443-4-1 anwenden
    - führt zu Ergebnissen, die später in einer Komponentenzertifizierung nach TeleTrusT-Modell nutzbar sind
    - Modell lässt flexibel die Integration von externen Prüfern zu
  - Zwischenzeitlich Sortierung der IEC 62443-Zertifizierungen

secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

Vielen Dank!
Thank you!

Sebastian Fritsch
sfritsch@secuvera.de
+49-7032/9758-24

secuvera GmbH
Siedlerstraße 22-24
71126 Gäufelden/Stuttgart
Germany