



TeleTrust Information Security Professional



TeleTrust
Pioneers in IT security.

T.I.S.P. Community Meeting 2019

Bundesverband IT-Sicherheit e.V. (TeleTrust)

Berlin, 05. - 06.11.2019

Prüfschema für Industrie 4.0 nach IEC 62433

Tobias Glemser, secuvera GmbH

- **Drei Beratungsfelder**
 - Sicherheitsberatung
(BSI-Grundschatz/ISO 27001)
 - Penetrationstests
 - BSI-Prüfstelle (Produktzertifizierungen)
62443 für Industrial Security (TÜV Nord)



- whoami
 - Tobias Glemser
 - 20 Jahre in der Branche
 - BSI-zertifizierter Penetrationstester
 - Autor
 - iX, c't, ...
 - Whitepaper „Projektierung der Sicherheitsüberprüfung von Webanwendungen“
 - OWASP Top10 Übersetzung
 - Hobbies..





(c) irinastrel123, fotolia

- Eine Zustandsbeschreibung IoT
 - Time to Market
 - Nicht funktionale Anforderung: Sicherheit
 - Ergebnisse

- Eine Zustandsbeschreibung IoT

INTELLIGENTE STROMZÄHLER

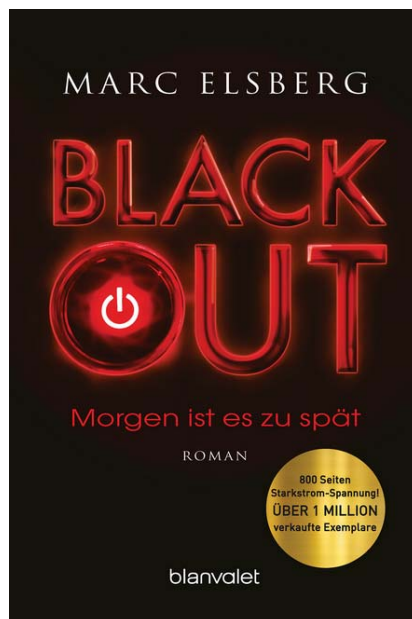
Gehackte Smart Meter machen Lichter aus

Black Hat Europe

Sicherheitsexperten ist es gelungen, in Spanien eingesetzte intelligente Stromzähler zu hacken. Damit könnten sie den Strom abschalten, den Zähler manipulieren oder dort Malware installieren.

Quelle: golem.de

- Eine Zustandsbeschreibung IoT
 - 8 Millionen Haushalte potentiell betroffen
 - Zentrales Abschalten nicht durch Stromnetz ausgleichbar



- Eine Zustandsbeschreibung IoT: Risiko
 - Für Infrastrukturen: Viele Geräte, wenige Hersteller → Abschalten großer Infrastrukturen mit einer Schwachstelle möglich
 - Für Consumerprodukte (Kameras, Uhren, Kühlschränke, Fernseher): Bedrohung des Einzelnen

- Eine Zustandsbeschreibung IoT: Gegenmaßnahmen?
 - Consumerprodukte: EU Cyber Security Act
 - Drei Ebenen der "Assurance"
 - Basic
 - Substantial
 - High
 - Selbst-Aussage (self declaration)?
 - Updatepflicht?
 - Mindestanforderungen (minimum requirements) verpflichtend?
 - Zertifizierung (3rd-party-certification) verpflichtend?

- Eine Zustandsbeschreibung IoT: Gegenmaßnahmen?

Digitalisierung stockt – Intelligente Stromzähler kommen später

05.04.2018 16:16 Uhr – Claus Haffert, dpa

 [vorlesen](#)



Stromzähler im Haushalt. (Bild: dpa, Jens Büttner/Archiv)

Der Stromzähler soll intelligent werden und die Energiekosten für Verbraucher senken. Doch der Weg dahin ist lang, denn smarte Messgeräte müssen hohe Sicherheitsstandards erfüllen.

Quelle: heise.de

- Eine Zustandsbeschreibung IoT: Gegenmaßnahmen?
Erstes Smart Meter Gateway zertifiziert

Meilenstein der Energiewende erreicht

Ort	Bonn
Datum	20.12.2018

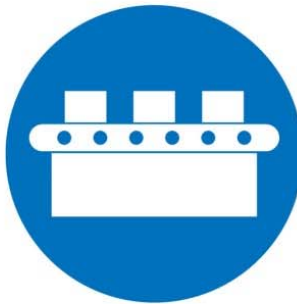
Quelle: [bsi.bund.de](https://www.bsi.bund.de)

1st revolution



Mechanization, steam
and water power

2nd revolution



Mass production and
electricity

3rd revolution



Electronic and IT
systems, automation

4th revolution



Cyber physical
systems

(c) Vectimus, fotolia

- Eine Zustandsbeschreibung IIoT/Industrie 4.0
 - Time to Market
 - Nicht funktionale Anforderung: Sicherheit
 - Ergebnisse

- Eine Zustandsbeschreibung IIoT/Industrie 4.0
Industrial Secure Routers



Keep Your Automation Network Safe

- Supports transparent firewall
- Deep packet inspection
- Real-time event alarms

[Learn More ►](#)

Moxa's EDR series industrial Gigabit-performance secure routers are designed to protect the control networks of critical facilities while maintaining fast data transmissions. The EDR series security routers provides integrated cyber security solutions that combine industrial firewall, VPN, router, and L2 switching* functions into one product specifically designed for automation networks, which protects the integrity of remote access and critical devices.

- Eine Zustandsbeschreibung IIoT/Industrie 4.0



Industrial Secure Routers EDR-810 / EDR-G902 / EDR-G903 -
Insecure Configuration Management

- when you navigate the server automatically you redirect to the login page (<http://site/login.asp>).
- so just add in the end of URL (admin.htm) then you get the Form to change the Admin configurations.

- Eine Zustandsbeschreibung IIoT/Industrie 4.0



- Eine Zustandsbeschreibung IIoT/Industrie 4.0

PATSCHERKOFEL

Gondelbahn mit Sicherheitslücken

Die Steuerungsanlage der neuen Gondelbahn am Innsbrucker Patscherkofel ist ohne Sicherheitsmaßnahmen im Netz zu finden gewesen. Ein Angreifer hätte die Bahn aus der Ferne übernehmen können - trotzdem beschwichtigt der Hersteller.

Quelle: [golem.de](https://www.golem.de)



- Eine Zustandsbeschreibung IIoT/Industrie 4.0: Risiko
 - Gefahr für Leib und Leben, z. B. durch ferngesteuerte Roboter/Überwindung von Sicherheitsdefinitionen
 - Fehlerhafte Produktion
 - Defekte Anlagen
 - Erpressung
 - Reputation
 - Massenhafter/Gleichzeitiger Ausfall (z. B. Fahrstühle)

Top 10 Bedrohungen	Trend seit 2016
-----------------------	--------------------

Quelle: BSI ICS Security Top 10

- Eine Zustandsbeschreibung IIoT/Industrie 4.0:
Gegenmaßnahmen?
 - EU Cyber-Security Act?
 - IEC/ISO 62443

Wie wird aktuell (zu oft) geprüft?



Security Zertifikat

Security-Audit Januar 2018

Die IoT-Lösung der Zukunft gibt es bereits!

Ist Ihr Lieferant sicherheitszertifiziert?

← Wirklich?

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.

Wir brauchen Prüfvorgaben!

Beispiel IEC 62443 – „Industrie 4.0 Sicherheit“

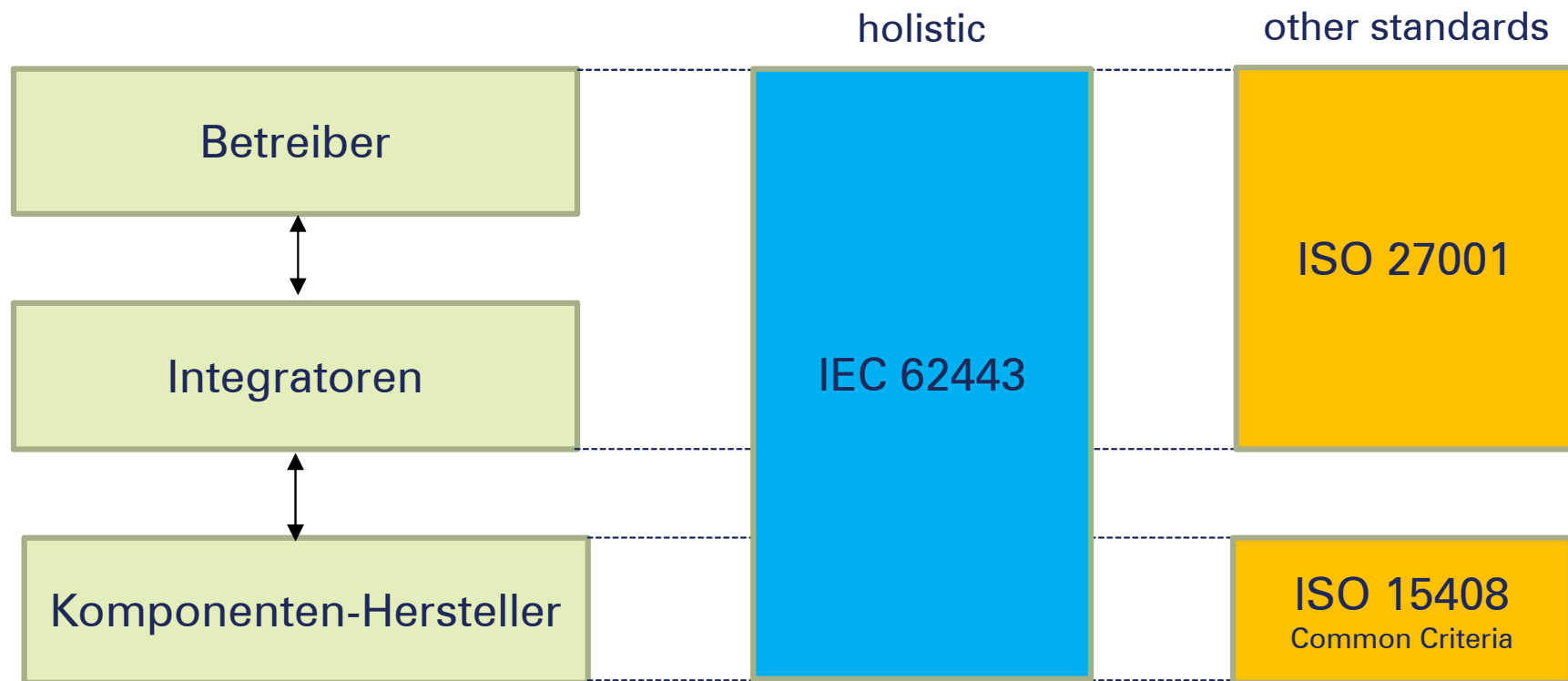


- ICS-Security Standards

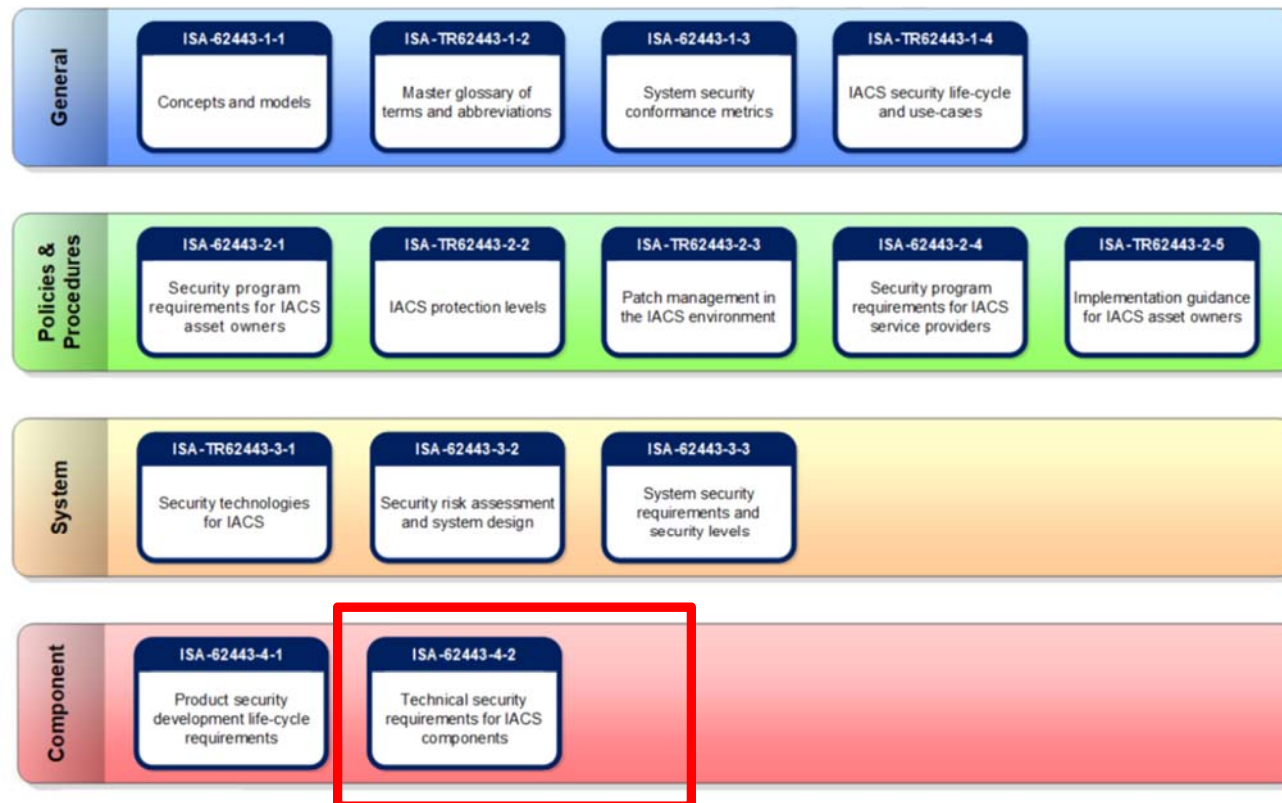
Alphabetisch sortiert

- 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 Informationssicherheits-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 der IEC 62443



- Aufbau der ISA/IEC 62443



Quelle: ISA99 Committee

- IEC 62443-4-2 Komponentenprüfung - Basis
 - Komponententypen
 - Embedded Geräte (z. B. PLC, Sensoren)
 - Host Geräte (z. B. Notebooks, PCs)
 - Netzwerkgeräte (z. B. Industrial Router)
 - Anwendungen (z. B. Konfigurationswerkzeuge)
 - Security Level
 - Technische Fähigkeiten Technical (Auswahl von CRs)
 - Widerstandsfähigkeiten/Resilienz
 - Entwicklungs-/Unterstützungsprozesse gem. 62443-4-1

- 62443-4-2 definiert Anforderungen an das Produkt
 - aber aus Standard lassen sich
 - Detailgrad der Component Requirements (CR) häufig nicht ausreichend
 - keine konkreten Tests ableiten
 - ergeben sich keine Vorgaben für Bewertung
 - CRs decken Bedrohungsaspekt nicht ab
 - im Ergebnis: Prüfstellen/Zertifizierungsstellen gehen mit Standard sehr unterschiedlich um
- Prüfschema definierte Anforderungen an die Prüfung
 - Sowohl Eigen-, als auch Drittparteienprüfung

- TeleTrust Prüfschema
 - Prüfschritte
 1. Prüfung des Verwendungszwecks
 2. Dokumentation (Design/Prüfung)
 3. Dokumentation (Anwender)
 4. Konformitätsprüfung
 5. Schwachstellenanalyse

- Diskussionen/Standardisierung
 - Übergabe TeleTrust Inhalte an deutsche Standardisierungsgremien
 - Rückmeldung durch Hersteller, Zertifizierer und BSI
 - Es dauert..
 - Zwei Wege
 - IECEE: Als Zertifizierungsleitfaden eingereicht
 - IEC / ISA99: Vorschlag, das Prüfschema in den Standard aufzunehmen

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 für IEC 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

- Anfangen!

- Standard ist für Hersteller stabil und fertig
 - 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

secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

Sprechen Sie mich gerne an. Ich freue mich auf Ihre
Fragen/Anregungen/Diskussionspunkte

Tobias Glemser
tglemser@secuvera.de
07032/9758-15



secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

Vielen Dank

