(Neue) Sicherheitsanforderungen durch die IEC 62443

Sicherheitsrisikobeurteilung und Systemgestaltung bei Betriebsführern der Windenergie

(Neue) Sicherheitsanforderungen durch die IEC 62443

Übersicht

(Neue) Sicherheitsanforderungen durch die IEC 62443

Was ist das Simulatorzentrum?

Seit nunmehr 40 Jahren führt das Simulatorzentrum der KSG|GfS in Essen das Simulatortraining für das lizenzierte Personal der deutschen und eines holländisches Kernkraftwerkes durch.

Unsere Tätigkeitsbereiche umfassen technische Ausbildung und Verhaltenstraining sowie Engineering und Consulting z.B. in den Bereichen Informationssicherheit und Datenschutz.

Gesellschafter: PreussenElektra GmbH (41,66%)
RWE Nuclear GmbH (30,73%)
EnBW Energie Baden-Württemberg AG (19,02%)
Vattenfall Europe Nuclear Energy GmbH (6,54%)
N.V. EPZ Kraftwerk Borssele NL(2,05%)

Sitz des Simulatorzentrums: Deilbachtal 173, 45257 Essen

Das Simulatorzentrum besteht aus den folgenden beiden Unternehmungen:
1. KSG Kraftwerks-Simulator-Gesellschaft mbH
2. GfS Gesellschaft für Simulatorschulung mbH

Weitere Informationen finden Sie zum Simulatorzentrum unter:
www.ksg-gfs.de sowie unter www.simulatorzentum.de

IT-Bereich zertifiziert nach
DIN EN ISO/IEC 27001:2017

Zertifiziert nach
DIN EN ISO 9001

(Neue) Sicherheitsanforderungen durch die IEC 62443

Zur Person des Stefan Loubichi

Stefan Loubichi

Abteilungsleiter Consulting, KSG mbH (Simulatorzentrum)

- Studium der Betriebswirtschaftslehre, Volkswirtschaftslehre [Schwerpunkt Wirtschaftsinformatik], Promotion im Bereich Managementsysteme
- IT-Ausbildungen
  Datenverarbeitungskaufmann, Organisationsprogrammierer (IBM)
- IT-Personalzertifizierungen
  MCSE, MCSA, MCAP, MCDBA, CCNA, CompTIA A+
- Leitender Senior-Auditor für die Managementsysteme
  ISO 27001, § 8a BSI-Gesetz, IT-Sicherheitskatalog § 11 EnWG, u.a.
- Relevante Zusatzqualifikation
  Datenschutzbeauftragter, BNetzA Qualifikation § 11 EnWG, Prüfer nach § 8a BSI-G

Referenzen in dem Sektor der Energieerzeugung

RWE, E.ON., EnBW, Uniper, Vattenfall, Siemens, Kisters, wpd, RheinEnergie, Schluchseewerk, Stadtwerke Düsseldorf, Stadtwerke Bremen, Steag, Großkraftwerk Mannheim, innogy u.v.a.

(Neue) Sicherheitsanforderungen durch die IEC 62443

Zur Person des Stefan Loubichi

Relevante Publikationen der letzten 24 Monate
VGB PowerTech Journal, atw

10/2017	Zertifizierungsstellen für Managementsysteme in der Energiewirtschaft
01/2018	Der IT-Sicherheitskatalog – Was jetzt getan werden muss
05/2018	Rechtliche Aspekte in Bezug auf die IT-Sicherheit für Energieerzeuger nach § 11 Abs. 1b EnWG
05/2018	Datenschutzgrundverordnung – Was Unternehmen der Energiewirtschaft ab 25.5.2018 umgesetzt haben mussten
12/2018	Development on NIS Directive in different EU countries in the energy sector
01-02/2019	Der finale Countdown des IT-Sicherheitskataloges nach § 11 Abs. 1b EnWG
03/2019	Prüfung nach § 8a BSI-Gesetz: Pflicht für Betriebsführer der Windindustrie
05/2019	IEC 62443: IT-Sicherheit für industrielle Automatisierung – eine Einführung in die Systematik
07/2019	Cybersecurity Act, IT-Sicherheitsgesetz 2.0 und die aktuellen Cybergefahren in der Energiewirtschaft

Hinweis:	Mehrere Werke sind mittlerweile in die Bibliothek des Deutschen Bundestages aufgenommen

(Neue) Sicherheitsanforderungen durch die IEC 62443

Die aktuelle de facto Cyber-Security-Lage

Weltweite Cyberangriffe auf die Honeypotinfrastruktur der Deutschen Telekom AG und ihrer Partner am 18.08.19 15:20 Uhr

Statistik der Attacken

20.737	**Attacken in der letzten Minute**
1.320.189	Attacken in der letzten Stunde
30.892.855	Attacken in den letzten 24 Stunden

Top 3 der Attackierer August 2019

Russland:	94.823.902
Frankreich:	**91.142.158**
USA:	**74.381.880**

Quelle: sicherheitstacho.eu/start/main

Global Cybersecurity Index 2018 der ITU

1. Großbritannien	9. Kanada	17. Südkorea	25. Ägypten
2. USA	10. Norwegen	18. Oman	26. Kroatien
3. Frankreich	11. Australien	19. Qatar	27. Italien
4. Litauen	12. Luxemburg	20. Georgien	28. Russland
5. Estland	13. Niederlande	21. Finnland	29. China
6. Singapur	14. Saudi-Arabien	22. Türkei	30. Österreich
7. Spanien	15. Japan	23. Dänemark	31. Polen
8. Malaysia	16. Mauritius	**24. Deutschland**	32. Belgien

Quelle: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

(Neue) Sicherheitsanforderungen durch die IEC 62443

Die aktuelle de facto Cyber-Security-Lage

Zugangsdaten zu Ihrem SCADA-System vergessen: Kein Problem

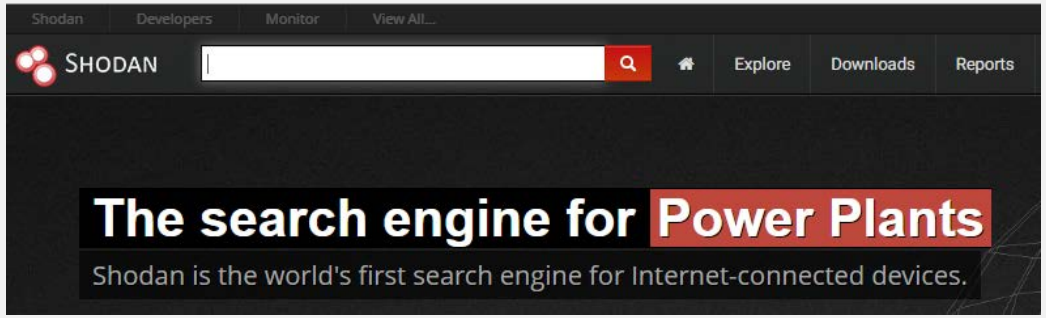
Im Internet findet sich die **SCADA Manufacturers Shame List***, Stand:* **14.11.16**
mit **215 Einträgen** *zu* **Vendor, Device, Default password, Port, Device typ, Protocol, Source** *und es finden sich hier auch die Produkte von bekannten Herstellern.*

Auf E-Mail-Anfrage senden wir Ihnen die so genannte „Shame-List“ zu.

Quelle: scada.sl (Vorsicht: unsichere Seite)

Standortbild, Adressen, freie Ports und Art Ihrer Systeme

Nach einem längeren Urlaub haben Sie Ort und Art Ihrer Systeme der industriellen Automatisierung vergessen und wissen nicht mehr welche freien Ports Sie haben, die gefährlich sein könnten. Auch hier kann das Internet weiterhelfen:



Quelle: shodan.io

(Neue) Sicherheitsanforderungen durch die IEC 62443

Die aktuelle de facto Cyber-Security-Lage

Heartbleed Report, Stand: 11.07.2019

Sichtbare, relevante Hosts

1.	USA	21.258
2.	China	8.655
3.	Deutschland	5.647
4.	Russland	3.869
5.	Frankreich	3.660
6.	Südkorea	3.407
7.	Italien	2.858
8.	Taiwan	2.639
9.	Japan	2.368
10.	Großbritannien	2.176

TLS-Verbindungen

TLS 1.0	**89.257**
TLS 1.1	88.364
TLS 1.2	88.823

TLS 1.0 seit 30.06.2018 unstrittig nicht mehr sicher

SSL Zertifikate

Nicht abgelaufen	54.665
Abgelaufen	**36.393**

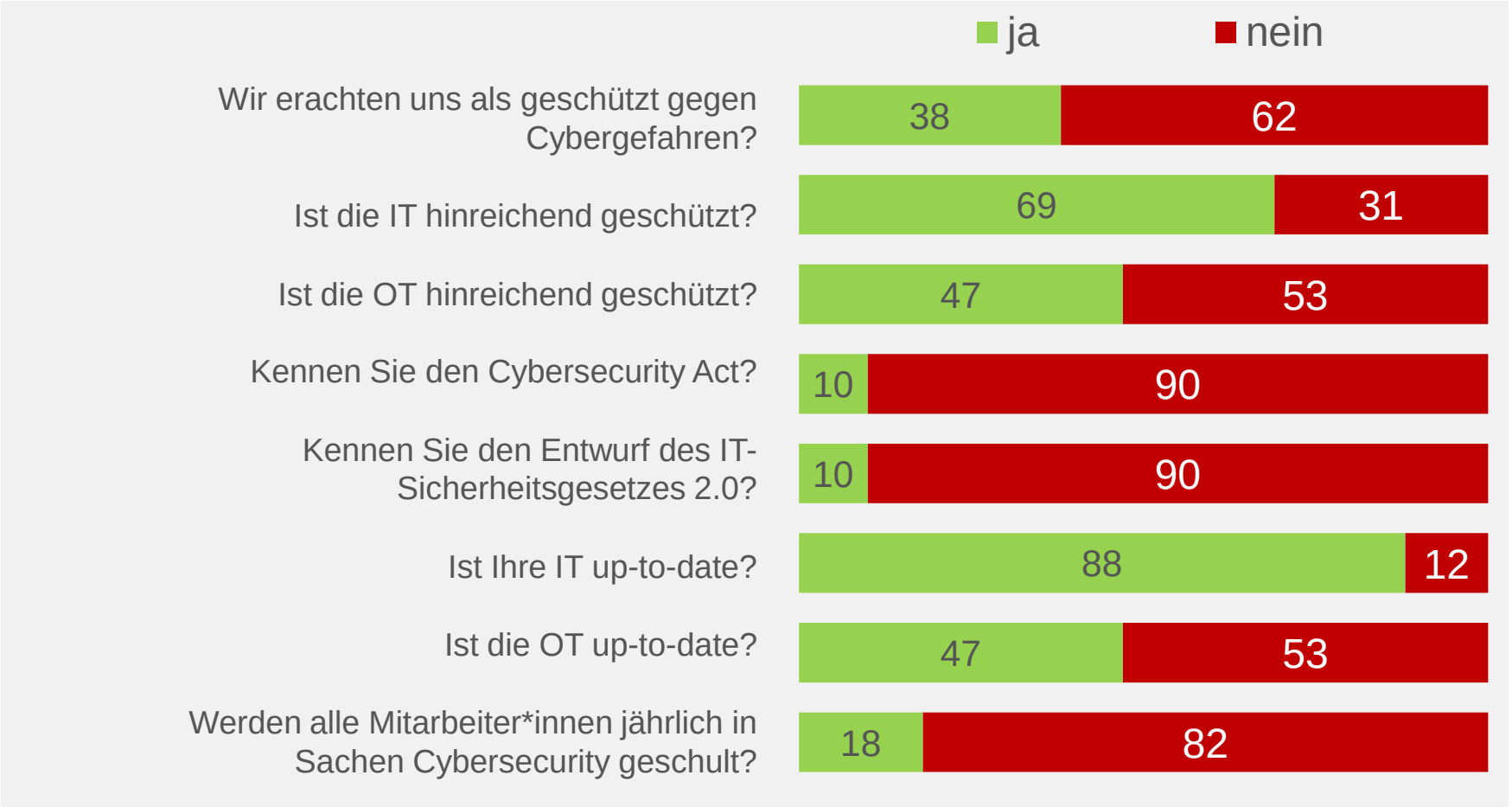
Grobe Fahrlässigkeit im Sinne des § 276 Abs. 2 BGB

Liegt immer dann vor, wenn die verkehrserforderliche Sorgfalt in besonders schwerem Maße verletzt wird, indem schon einfachste, naheliegende Überlegungen nicht angestellt werden.

(Neue) Sicherheitsanforderungen durch die IEC 62443

Die aktuelle de facto Cyber-Security-Lage

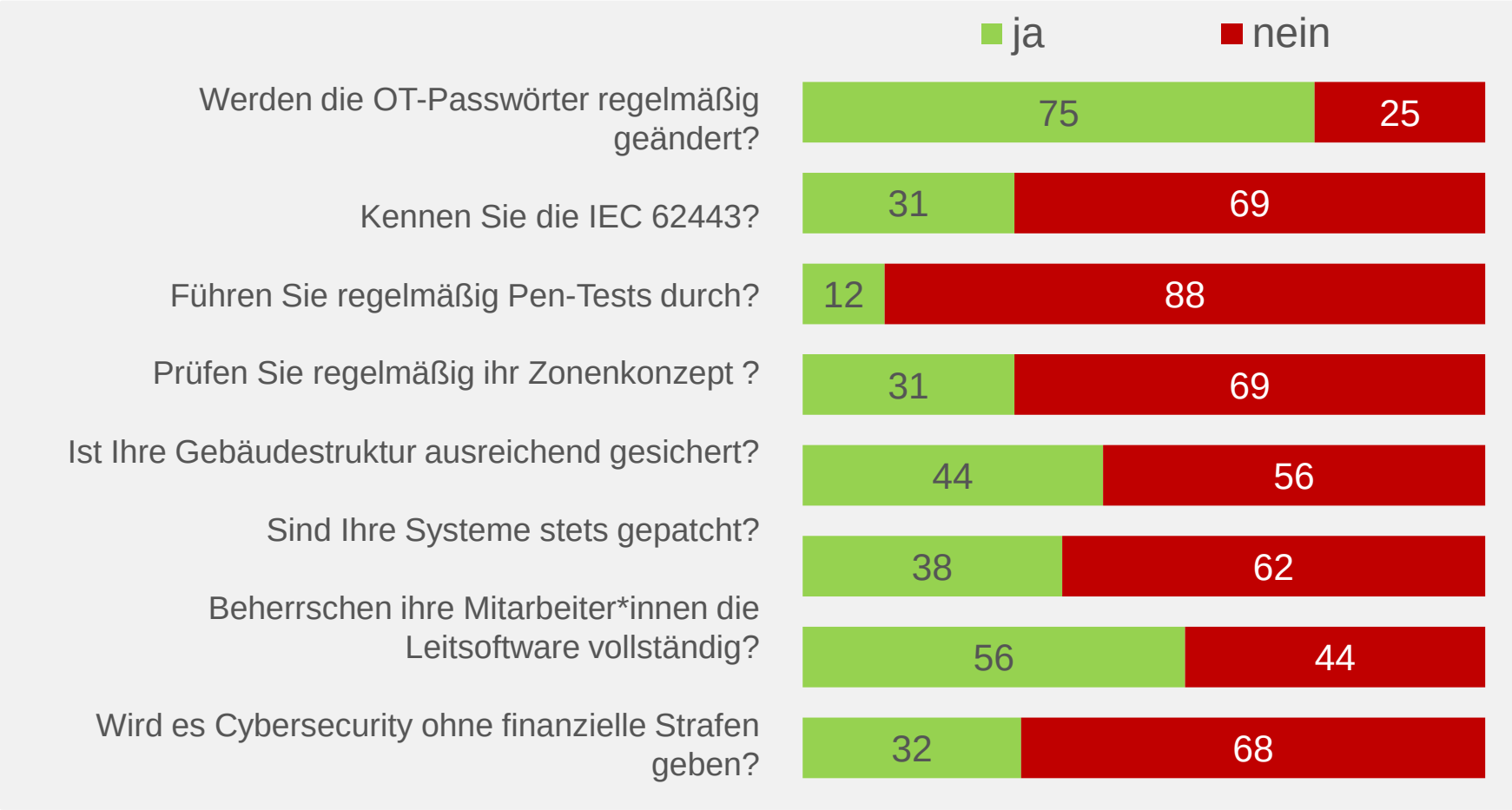
Ergebnis aktuelle Cybersecurity-Umfrage bei Energieunternehmen



(Neue) Sicherheitsanforderungen durch die IEC 62443

Die aktuelle de facto Cyber-Security-Lage

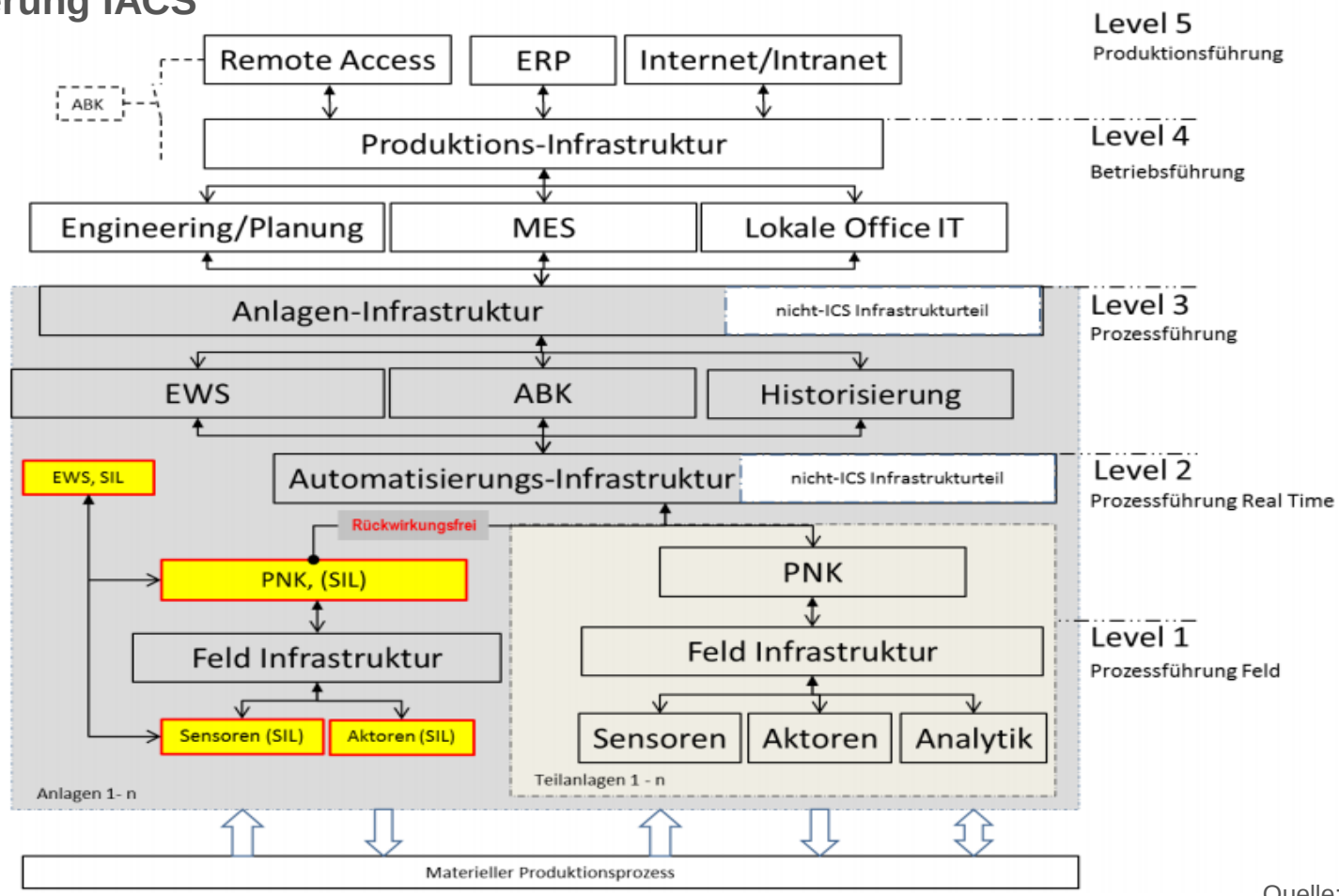
Ergebnis aktuelle Cybersecurity-Umfrage bei Energieunternehmen



(Neue) Sicherheitsanforderungen durch die IEC 62443

IACS und 62443

Hierarchische Gliederung IACS



Quelle: BSI,ICS-Securitykompendium, S. 18

(Neue) Sicherheitsanforderungen durch die IEC 62443

IT-Sicherheitsgesetz 2.0 – Was erwartet die Energiewirtschaft?

Die wichtigsten Erweiterungen des seit 04/19 im Referentenstatus befindlichen IT-Sicherheitsgesetzes 2.0 (baldige Inkraftsetzung)

- **Schaffung eines unbestimmten Sektors „Infrastruktur von besonderem öffentlichen Interesse“**
  heute wird z.B. Entsorgung darunter subsumiert und morgen?
- **Einführung/Anwendung einer Vertrauenswürdigkeitserklärung**
  KRITIS-Kernkomponenten dürfen nur von solchen Herstellern bezogen werden, die vor dem erstmaligen Einsatz der Komponenten eine Erklärung über ihre Vertrauenswürdigkeit gegenüber dem Betreiber der Krit. Infr. abgeben haben. Diese Verpflichtung erstreckt sich auf die gesamte Lieferkette des Herstellers.
  Dies sind stets IT-Produkte für die Leittechnik oder die Steuerungstechnik von Anlagen [→ Sichere EU-Produkte/Systeme mit IEC 62443 ?!]
- **Meldung der Hersteller von KRITIS-Kernkomponenten an das BSI**
  Hersteller von KRITIS-Kernkomponenten müssen alle Störungen bzgl. Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer Software unverzüglich dem BSI melden.
- **Neue Sanktionierungshöhen (Angleichung an die DSGVO)**
  Bußgeldrahmen von bis zu EUR 20.000.000,00 oder 4 % des jährlichen Unternehmensumsatzes

(Neue) Sicherheitsanforderungen durch die IEC 62443

IT-Sicherheitsgesetz 2.0 – Womit muss noch gerechnet werden?

Es wird eine Regelung der Nachfolgeverordnungen (Kritis-VO etc.) bzw. eine Klarstellung von Schwachstellen erwartet/erhofft

- *Welche* **Komponenten der OT** *müssen wirklich erfasst werden? (-> siehe auch IT-Grundschutz, IND.2.3 Sensoren und Aktoren)*
- *In wie weit kann man sich durch* **Auslagerung von Leitständen** *in rechtlich selbständige juristische Personen aus der Haftung „retten“?*
- *In wie weit ist die* **420 MW Grenze im Sinne der Kritis-VO** *im Rahmen der Energiewende und der Umstrukturierung der Energieerzeugung überhaupt noch geeignet, IT-/OT-Sicherheit zu gewährleisten?*
- *Wann wird die* **ISO/IEC 27019** *(=ISMS Norm für die Energiewirtschaft) in den Zertifizierungsverfahren nach dem IT-Sicherheitskatalog endlich stärker berücksichtigt?*
- *Ist die* **Reduktion auf Prüfverfahren nach § 8a BSI-Gesetz** *nicht eine einseitige Begünstigung bzgl. bestimmter Entitätsgruppen der Energiewirtschaft?*
- *Derzeit existiert* **kein offizieller Stand der Technik** *IT-Sicherheit/Cyber-Security. Wann wird endlich ein derartiger Stand der Technik für die Energiewirtschaft verbindlich festgelegt?*

(Neue) Sicherheitsanforderungen durch die IEC 62443

Cyber-Security Act der EU – Was erwartet uns?

Hauptziele des Juni 2019 in Kraft getretenen EU-Cyber-Security Act

dauerhaftes Mandat *für die EU-Cyber-sicherheitsagentur (ENISA), wäre 2020 ausgelaufen*	*Stärkung der ENISA im neuen* **Rahmen für die Zertifizierung der Cybersecurity**
Sicherheitsmerkmale für Produkte *müssen zukünftig* **bereits in der Konzeptionierung** *berücksichtigt werden:* *Bedeutet dies auch den* **Durchbruch der IEC 62443** *in Europa?*	*Schaffung eines EU-weit geltenden Zertifizierungsrahmens für die* **Zertifizierung von:** ▪ **Produkten** ▪ **Verfahren** ▪ **Diensten**
Durchführung von **EU-weiten regelmäßigen Cybersicherheitsübungen**	**Orientierung an internationalen Standards** *statt an nationalen Best-Practice-Beispielen*

Angedachte Strukturdaten:
125 Mitarbeiter, Jahresbudget: 23 Mio. EUR

(Neue) Sicherheitsanforderungen durch die IEC 62443

Cyber-Security Act der EU – Was wird noch getan werden müssen?

- Orientierung an europäisch-einheitlichen statt national-uneinheitlichen Zertifizierungs-schemata (besonders wichtig für multinational aufgestellte Energieerzeuger)
- Klassifizierung aller Projekte in die drei Vertrauenswürdigkeitsstufen niedrig, mittel und hoch
- Änderung des Beschaffungswesen dahingehend, dass zumindest KRITIS-Kernkomponenten nach „eingebauter Sicherheit“ ausgesucht werden sollten, wobei eine freiwillige Zertifizierung Sinn macht
- Zumindest mittel- bis langfristige Orientierung an der Normenfamilie IEC 62443, IT-Sicherheit für Netze und Systeme
- Länderübergreifende Integration von Managementsystemen, wobei die deutsche Schwellenwertphilosophie 420 MW nicht das Maß der Dinge sein wird
- Integration der IEC 62443 in die ISO/IEC 27001

Dies wird bedeuten:

- **mehr Schulungen für Mitarbeitende**
- **zusätzliche Ressourcen, v.a. im OT-Bereich**
- **nicht unerhebliche zusätzliche Kosten**

(Neue) Sicherheitsanforderungen durch die IEC 62443

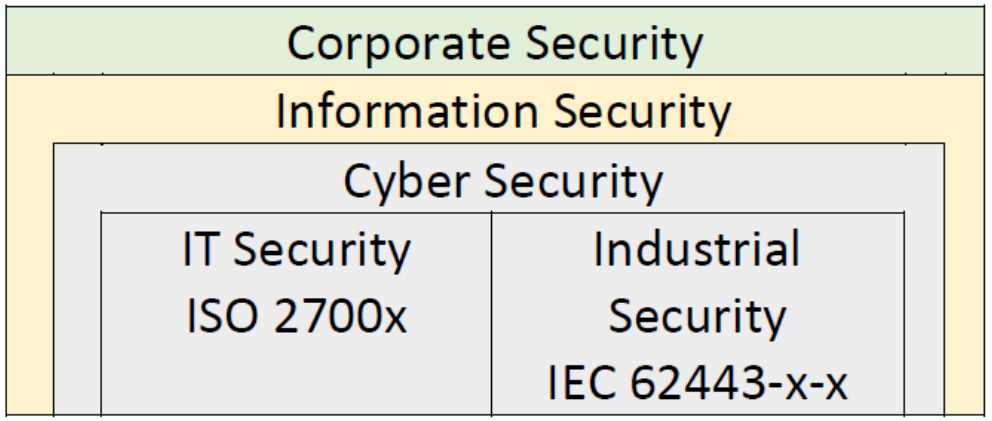
Ein ganzheitlicher Ansatz

HEUTE

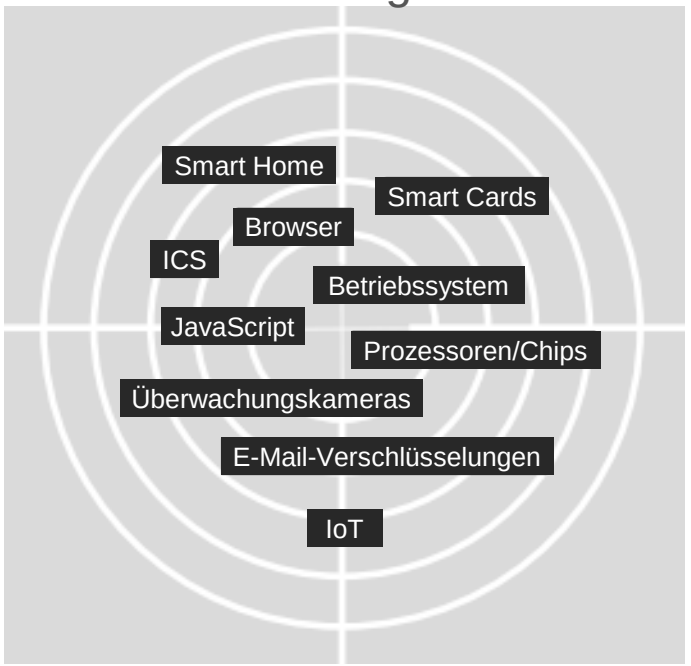
NIS Directive
IT-SiG, BSI-G, Kritis-VO
ISO 2700x, IT-Sich.katalog

MORGEN

Cyber Security Act
Internetgesetz 2.0
ISO 62443-x-x



Fokus der Angreifer 2019



Quelle: BSI – Lagericht 2018

Was wir benötigen ist nicht ein Neben-einander des Schutzes von IT und OT, sondern ein ganzheitlicher Ansatz des Schutzes industrieller Automatisierung!

(Neue) Sicherheitsanforderungen durch die IEC 62443

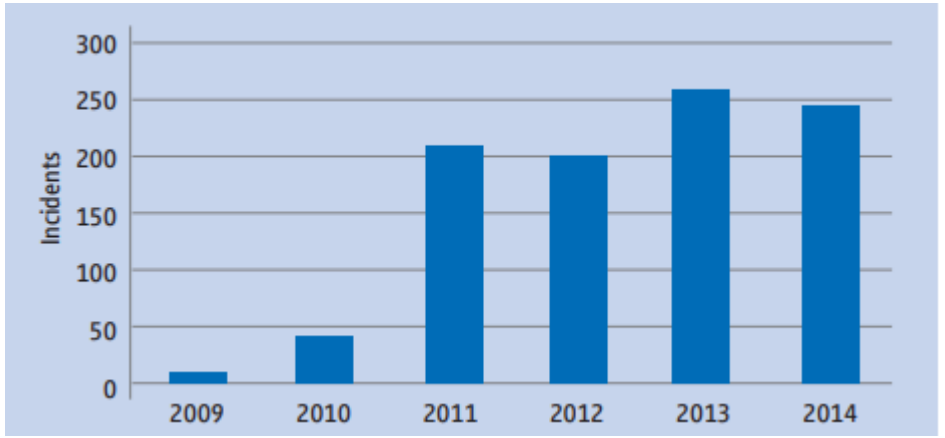
Ein ganzheitlicher Ansatz

Wir haben IT-Sicherheit, deshalb brauchen wir keine OT-Sicherheit…

	IT	OT
Lebens-dauer	3-5 Jahre	5-20 Jahre
Patch-mana-gement	oft, täglich	Selten, Freiga-be durch Anla-genhersteller
Zeitab-hängig-keit	Verzöge-rungen akzeptiert	Kritisch
Verfüg-barkeit	Kurze Ausfälle tolerabel	24/7

IT-Welt und OT-Welt sind anders, deshalb brauchen Sie OT-Sicherheit

Es gibt Angriffe auf die IT-Welt, aber doch nicht auf die OT-Welt…



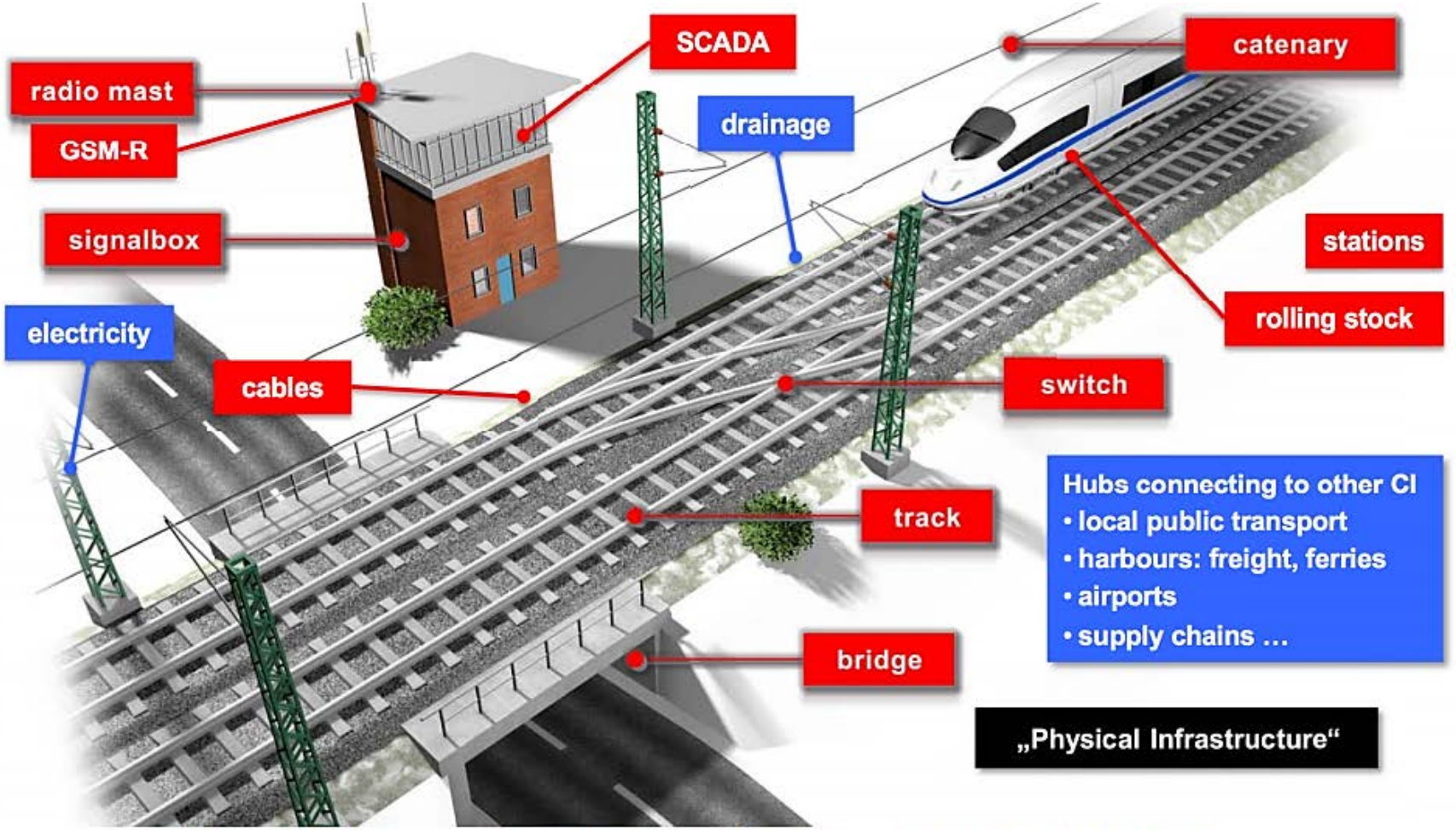
Quelle: ZVEI

Und die Zahl der Angriffe ist noch gestiegen, auch wenn aus Sicherheitsgründen nicht mehr so viel veröffentlicht wird.

Das große Gefährdungspotential für morgen ist die OT-Welt…

(Neue) Sicherheitsanforderungen durch die IEC 62443

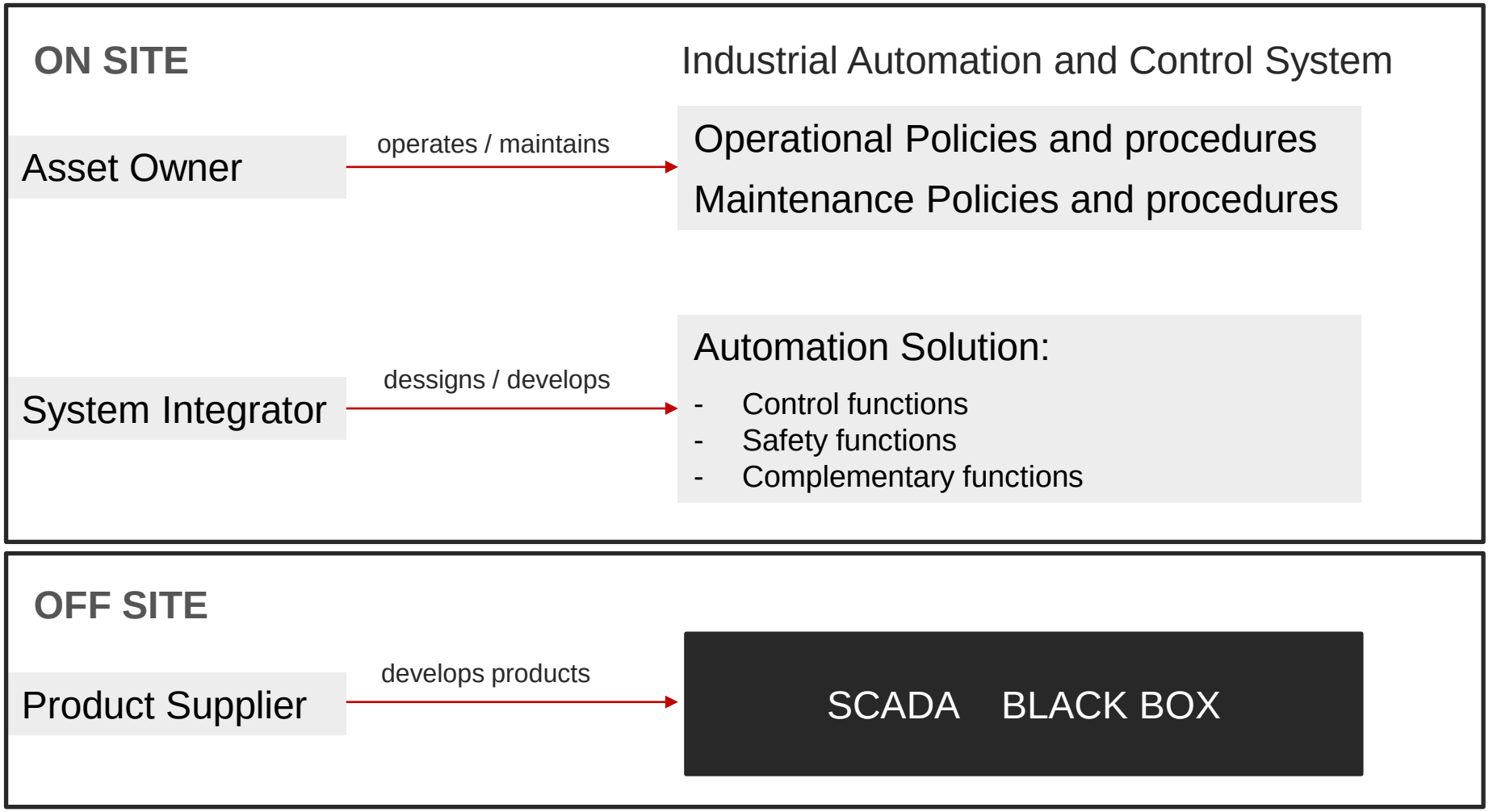
Ein einfaches fachfremdes Beispiel dafür, was mit wem zusammenhängt



© DB. Source: https://docplayer.org/storage/22/1656988/1537105373/VEOjfqYiU4umT70Ex5FBsQ/1656988.pdf

(Neue) Sicherheitsanforderungen durch die IEC 62443

Ein ganzheitlicher Ansatz in Sachen Schutz

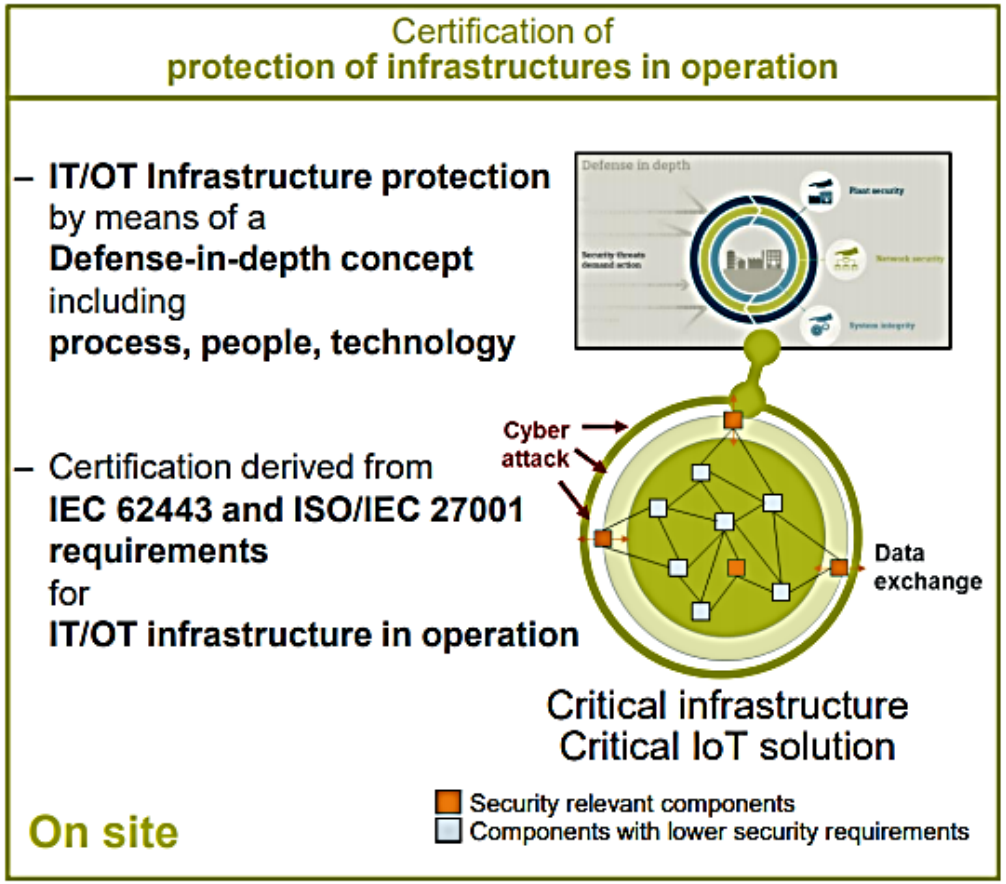


62443 Philosophie - Ansatz

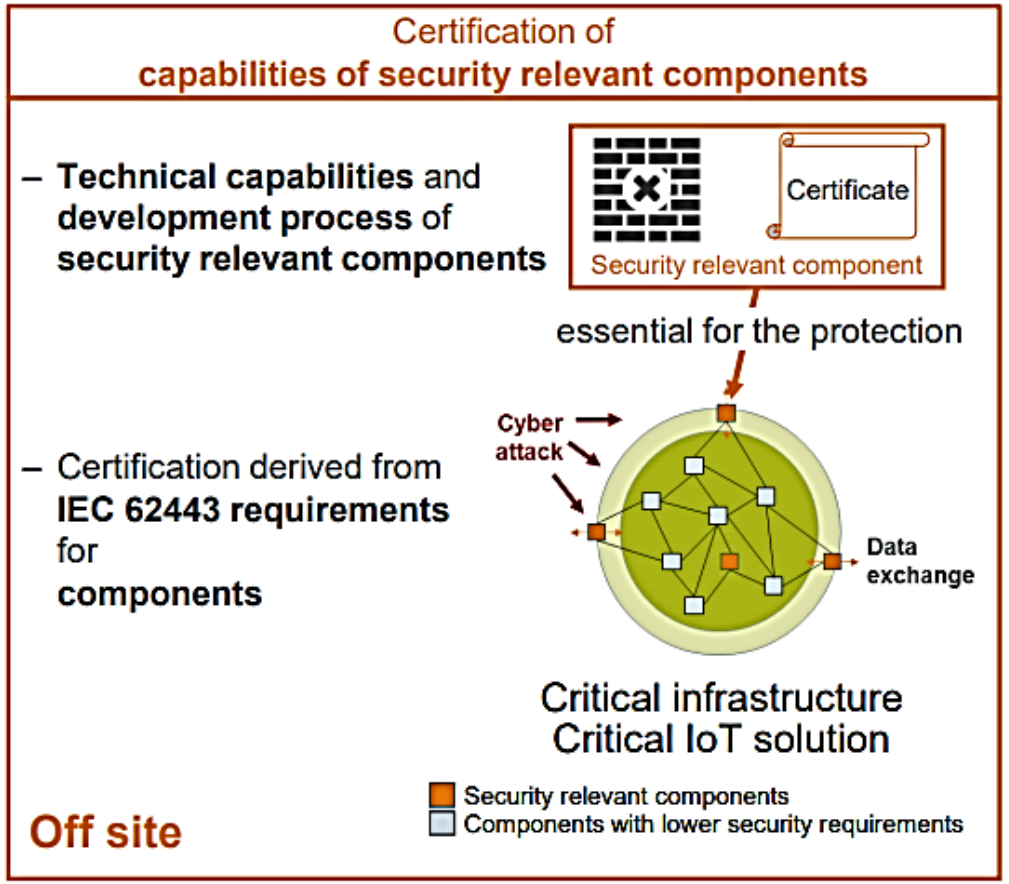
(Neue) Sicherheitsanforderungen durch die IEC 62443

Ein ganzheitlicher Ansatz in Sachen Schutz

Der 2 Komponentenansatz zum Schutz industrieller Automatisierung:



AND



Quelle: http://www.oecd.org/gov/risk/Pierre%20Kobes%20Cyber%20risks.pdf

(Neue) Sicherheitsanforderungen durch die IEC 62443

Die 62443-3-2 und ihre Einbettung

Übersicht über die IEC 62443-Familie

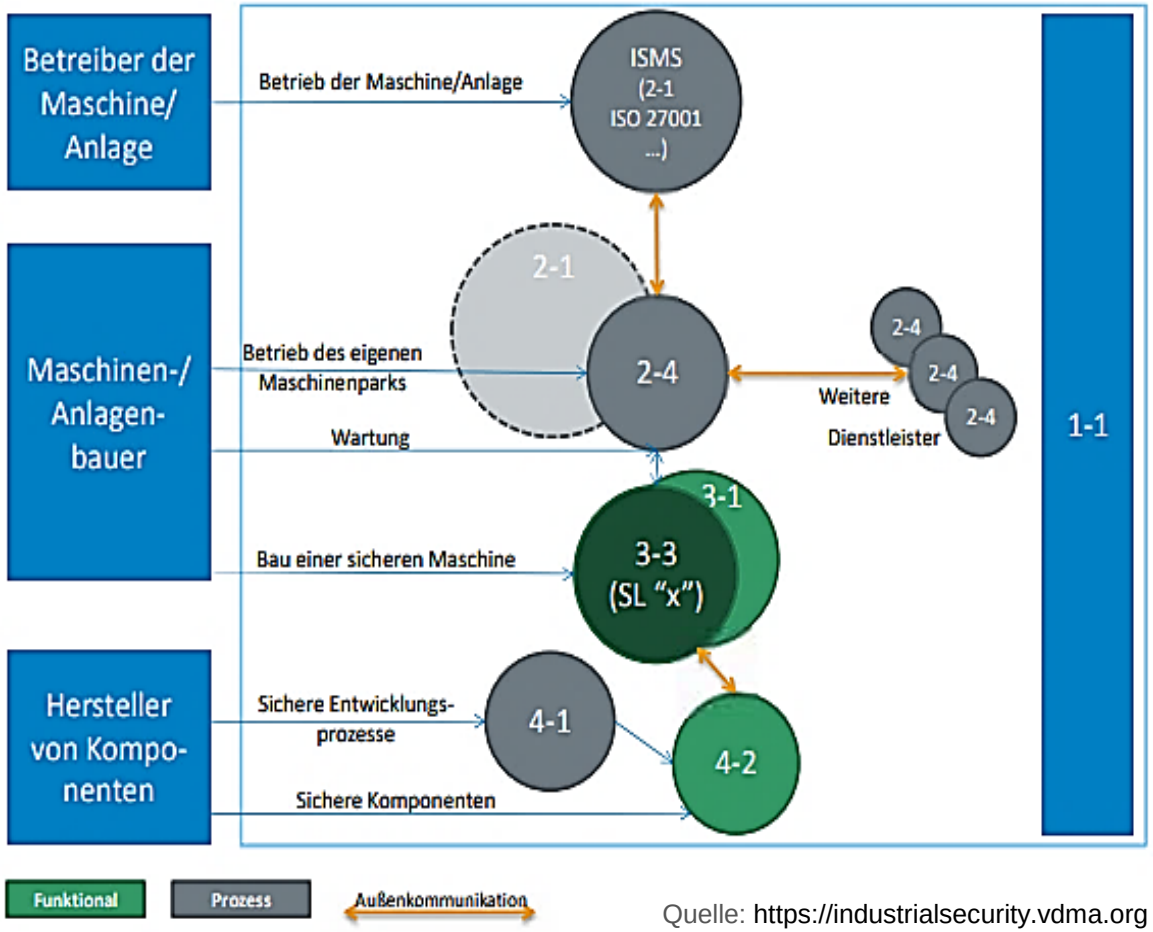
General	**ISA-62443-1-1**	**ISA-62443-1-2**	**ISA-62443-1-3**	
	Terminology, concepts and models	Master glossary of terms and abbreviations	System security compliance metrics	
Policies and Procedures	**ISA-62443-2-1**	**ISA-62443-2-2**	**ISA-62443-2-3**	**ISA-62443-2-4**
	Requirements for IACS security management system	Implementation guidance for an IACS security management system	Patch management in the IACS environment	Requirements for IACS solution suppliers
System	**ISA-62443-3-1**	**ISA-62443-3-2**	**ISA-62443-3-3**	
	Security technologies for IACS	Security risk assessment and system design	System security requirements and security levels	
Component	**ISA-62443-4-1**	**ISA-62443-4-2**		
	Product development requirements	Technical security requirements for IACS products		

Wollte man die 62443 – Familie mit der 270xx – Familie quantitativ vergleichen wollen, so würde man eine Brockhaus-Enzyklopädie mit einem Taschenlexikon vergleichen. Dieser plakative Vergleich mag die Mächtigkeit der 62443 Familie verdeutlichen.

(Neue) Sicherheitsanforderungen durch die IEC 62443

Die 62443-3-2 und ihre Einbettung

Verschiedene Rollen und die 62443 Familie



Quelle: https://industrialsecurity.vdma.org

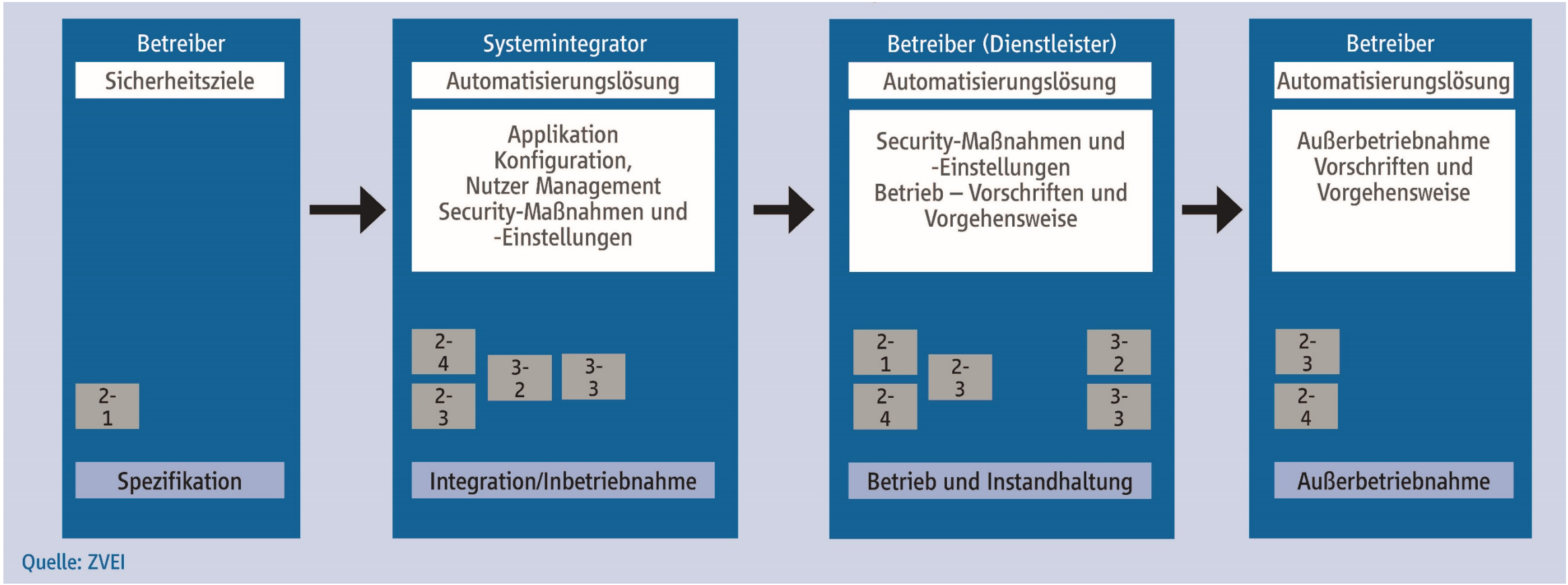
Basisanforderungen an die 62443

1. Identifizierung und Authentifizierung
2. Nutzungskontrolle
3. Systemintegrität
4. Vertraulichkeit der Daten
5. Eingeschränkter Datenfluss
6. Rechtzeitig Reaktion auf Ereignisse
7. Verfügbarkeit der Ressourcen

(Neue) Sicherheitsanforderungen durch die IEC 62443

Die 62443-3-2 und ihre Einbettung

Lebenszyklus und Korrelation zur 62443-Familie



Quelle: ZVEI

(Neue) Sicherheitsanforderungen durch die IEC 62443

Die 62443-3-2 und ihre Einbettung

Security Level gemäß IEC 62443

Level:	Schutz gegen:
1	zufällige Fehlanwendung
2	absichtliche Versuche mit einfachen Mitteln
3	SL2, aber mit erweiterten Kenntnissen und Mitteln
4	SL3, aber mit spezifischen Kenntnissen und erheblichen Mitteln

Securitylevel (SL) im Lebenszyklus IEC 62443

Level:	Bedeutung:
SL-C	SL, den ein Gerät oder System erreichen kann, wenn es richtig eingesetzt und konfiguriert wird
SL-T	SL, welches das Ergebnis der Bedrohungs-/Risikoanalyse darstellt
SL-A	Das im Gesamtsystem erreichbare messbare Security Level

(Neue) Sicherheitsanforderungen durch die IEC 62443

Anwendungsbereich IEC 62442-3-2

Die 62443-3-2 und ihre Einbettung

1. Festlegung eines zu betrachtenden Systems (SuC) für ein industrielles Automatisierungssystems (IACS)
2. Aufteilung der SUC in Zonen und Conduits
3. Beurteilung des Risikos für jede Zone und jeden Conduit
4. Festlegung des zu erreichenden Security-Level für jede Zone und jedes Conduit
5. Dokumentation der Sicherheitsanforderungen

Conduit:
Eine logische Gruppierung von Kommunikationskanälen, die gemeinsamen Sicherheitsanforderungen unterliegen und zwei oder mehr Zonen miteinander verbinden

Zone:
Gruppierung logischer oder physischer Anlagen auf der Grundlage des Risikos oder anderer Kriterien wie der Kritikalität der Anlagen der Betriebsfunktion, des physischen oder logischen Standortes, des erforderlichen Zugangs oder der verantwortlichen Organisation

(Neue) Sicherheitsanforderungen durch die IEC 62443

Vorgehensweise:

Die 62443-3-2 und ihre Einbettung

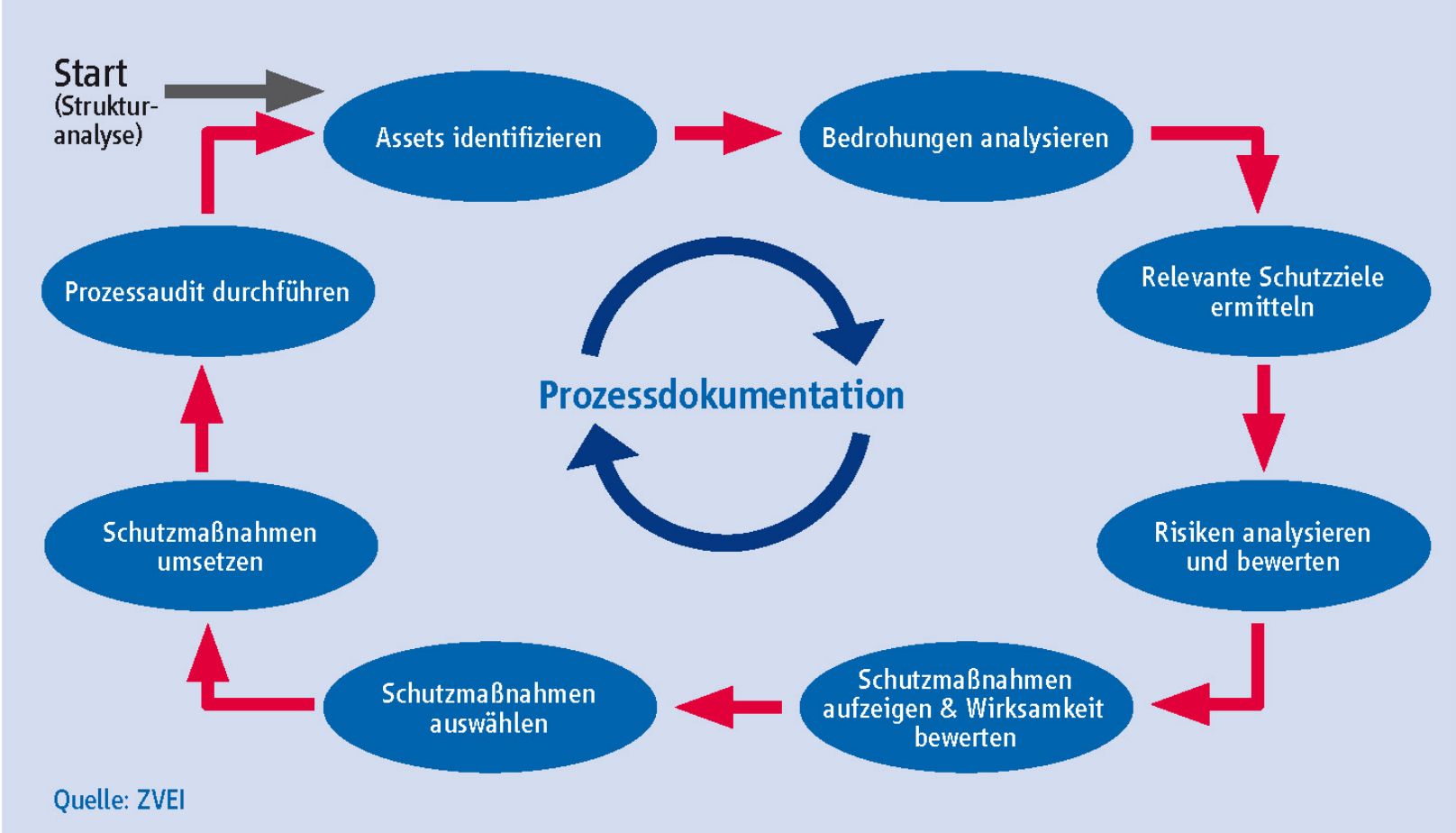
Die 7 Schritte:

1. Identifizieren des zu berücksichtigenden Systems
2. Erste Cybersicherheitsrisikobeurteilung
3. Aufteilung des SUC in Zonen und Kanäle
4. Risikovergleich
5. Durchführung der ausführlichen Cybersicherheitsrisikobeurteilung
6. Dokumentation der Anforderungen
7. Einholen der Genehmigung des Anlagenbetreibers

(Neue) Sicherheitsanforderungen durch die IEC 62443

Analoge Vorgehensweise nach VDI/VDE Richtlinie 2182 Blatt 1 – eine Option:

Die 62443-3-2 und ihre Einbettung



(Neue) Sicherheitsanforderungen durch die IEC 62443

Nächste Möglichkeiten

Cyber-Security-Fachtagung

Wann:	21.11.2019
Wo:	Energie-Campus Deilbachtal Deilbachtal 173, 45257 Essen
Wer:	Simulatorzentrum, VGB und die Kraftwerksschule zusammen mit Partnern
Was:	Kurzvorträge (30-45 min) rund um das Thema Cyber-Security, aus der Sicht: ▪ Zertifizierer ▪ Kraftwerke ▪ Kritis-Komponentenhersteller ▪ Lieferanten ▪ IT-/OT-Umfeld

Unser Cyber-Security-Zentrum

- Normen, Standards und Gesetze:
  ISO 27001, IEC 62443, DSGVO, IT-Sicherheitskatalog, IT-Grundschutz
- Klassische OT-Sicherheit:
  Siemens-Welt (SPPA-T3000 u.a.), ABB (800xA)
- Klassische IT-Sicherheit:
  Microsoft, Cisco, CompTIA
- Social Competence:
  Konflikttraining, Kommunikationstraining, HPO Human Performance
- Grundlagen Cyber-Security:
  Angriffsmethoden, Abwehrmethoden

(Neue) Sicherheitsanforderungen durch die IEC 62443

Ihre Ansprechpartner

Fachliche Fragen / Projektfragen:

Prof. h.c. PhDr. Stefan Loubichi

Tel.: +49 201 4862-201
Fax: +49 201 4862-404
Mobil: +49 173 6925188
E-Mail: s.loubichi@ksg-gfs.de

Administrative Fragen

Peter Lasch

Tel.: +49 201 4862-169
Fax: +49 201 4862-156
Mobil: +49 176 42250302
E-Mail: p.lasch@ksg-gfs.de