Rechtliche und technische Anforderungen an die IT-Sicherheit im Energiesektor
Berlin, 10.11.2017

Dr. Dennis-Kenji Kipker
Dipl.-Ing. Sven Müller

Gefördert vom
FKZ: 16KIS0213
bis 16KIS0216
Bundesministerium für Bildung und Forschung

Universität der Bundeswehr München
FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG
DKE VDE DIN
Universität Bremen

IT-Sicherheit als Compliance-Herausforderung

- **Erkenntnisquellen** der IT-Security Compliance:
  - Allgemeine gesetzliche Vorschriften/Rahmenvorschriften (z.B. BSIG, BDSG, GmbHG)
  - Branchenspezifische gesetzliche Vorschriften (z.B. für Banken, Versicherungen, Industrie, IuK, Logistik, öffentliche Verwaltung und Energie)
  - Technische Normen und Standards
  - Unternehmensinterne Vorgaben, vertragliche Bestimmungen und Selbstverpflichtungen
  - “Soft Law” (z.B. Deutscher Corporate Governance-Kodex – DCGK, § 161 AktG)
- **Keine kodifizierte Regelung** der IT-Sicherheit
- **Herausforderung** für IT-Security Compliance

- Juristische Erkenntnisquellen für die IT-Security Compliance im Energiesektor – Beispiele:
  - EURATOM-V: Art. 78
  - VO (EU) Nr. 347/2013 (Leitlinien der transeuropäischen Energieinfrastruktur)
  - RL (EU) 2009/72 (Elektrizitätsbinnenmarkt)
  - RL (EU) 2012/27 (Energieeffizienz-RL)
  - RL (EU) 2013/40 (Angriffe auf Informationssysteme)
  - **RL (EU) 2016/1148 (NIS-RL)**
  - **AtG:** §§ 6; 7 II; 7c; 7d; 9; 12 I Nr. 7; 12b; 19a; 44b
  - **EnWG:** §§ 1 IV Nr.3; 11 Ia; 11 Ib; 11 Ic; 12; 12g; 13h I Nr. 20, 22, 23; 14 I 1; 49; 52; 59
  - **BSIG:** §§ 3; 7; 7a; 8a - 8d; 9; 10; 14
  - **MsbG:** §§ 19-28; 52; 53; 61; 73; Anlage zu § 22 II 1

Rechtsvorschriften der IT-Sicherheit im Energiesektor II

- Juristische Erkenntnisquellen für die IT-Security Compliance im Energiesektor – Beispiele:
  - EEG: §§ 10 II; 14; 93 Nr. 13
  - KWKG: §§ 15 II; 24 I, II; 27; 28 VI
  - EnEG: §§ 3a, 7b
  - StromNZV: §§ 4 IV; 14 I
  - StromGVV: §§ 8; 9; 11
  - ARegV: §§ 23 I Nr. 7; 27; 28; 29; 31
  - AtSMV: §§ 3; 4; 6; 7; 7a; 8 II; 9
  - NAV: §§ 13-15; 19-22
  - **BSI-KritisV:** § 2; Anhang 1
  - ÜnSchutzV
- **→ Vielzahl verschiedener Rechtsquellen sowohl im gesetzlichen als auch im untergesetzlichen Recht**
- **→ Sowohl transnational als auch national**
- **→ Nicht nur Betroffenheit von KRITIS**

- **Gemeinsamkeit aber:** Nahezu alle benannten Rechtsvorschriften verwenden in unterschiedlicher Ausprägung sog. "**unbestimmte Rechtsbegriffe**", um die rechtlichen Anforderungen in technischer Hinsicht zu **konkretisieren**

- **Problem:** Wie (technisch) konkret sind die gesetzlichen IT-Security Compliance-Anforderungen im Einzelfall?

IT-Security Compliance und unbestimmte Rechtsbegriffe I

- IT-Security Compliance als interdisziplinäres Themenfeld:
  - **IT-Security-Bezug** bei gesetzlichen Vorschriften **nicht immer klar erkennbar** bzw. Erwartungshorizont **nicht hinreichend konkretisiert**
  - Allgemeine gesellschaftsrechtliche Beobachtungs- und Sorgfaltspflichten beziehen sich aber auch auf die Gewährleistung der IT-Security
    - Beispiel: Sorgfalt eines "**ordentlichen Geschäftsmannes**" im GmbHG
  - Zugang oft über sog. "**unbestimmte Rechtsbegriffe**" oder "**Generalklauseln**"
    - **Vielzitierte Trias:**
      - Allgemein anerkannte Regeln der Technik
      - Stand der Technik
      - Stand von Wissenschaft und Technik
    - Aber auch zahlreiche **weitere konkretisierungsbedürftige Begriffe**, z.B. "Zuverlässigkeit" i.S.d. § 21 I Nr. 1 MsbG

- Zwecksetzung unbestimmter Rechtsbegriffe:
  - Implementierung außerhalb des Rechts stehender Sachverhalte in Gesetze
  - Recht als “Einfallstor” für technische Vorgaben
  - **Flexibilität, Anpassungsfähigkeit und Technikoffenheit**
  - **Jedoch:** Teils erhebliche Schwierigkeiten in der Anwendungspraxis, vor allem für KMUs
    - Bei Bezugnahme auf außerhalb des Rechts liegende Sachverhalte
    - Bei noch nicht vollständig abgeschlossener Konkretisierung unbestimmter Rechtsbegriffe, insb. im Falle neuer Regelungsmaterien
  - **Hilfestellung in der Konkretisierung unbestimmter Rechtsbegriffe durch technische Normen & Standards**

„Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen“

DKE VDE DIN DIN Universität Bremen IT-Security NAVIGATOR ITS KRITIS

Start | IT-Security Standards | IT-Security Laws | Research | Notification

Letzte Änderungen: 2017-08-16 — Alle durchsuchen

Bezeichnung	Abk./Link	Einzelne rechtliche Vorschriften	Unbestimmte Rechtsbegriffe/ Generalklauseln	Technische Normen & Standards	Relevanz	Gesetzesmaterialien	Rechtspr./Literatur	Sektor	Branche	Ebene	Rechtsakt	Bundesland
Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz)	MsbG	Alle, insbes. §§ 19-28; 52; 53; 61; 73; Anlage zu § 22 II 1	Aufrufen	BASI/TR 03109-2 V1.1 TR-03109-2; BASI/TR 03109-6 V1.0; DVGW G 694; PTB-A 50.8; DIN IEC/TS 62056-6-9 (DIN SPEC 42056-6-9); IEC 61968-9; DIN EN 62056-1-0 (VDE 0418-6-1-0); DIN EN 62056-3-1 (VDE 0418-6-3-1); DIN EN 13757-1; DIN EN 13757-2; DIN EN 13757-3;	1		Aufrufen	Energie	Elektrizität	Bundesrecht	Gesetzlich	

Unbestimmte Rechtsbegriffe / Generalklauseln:

§19(4) … Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, … Vertraulichkeit und Integrität der Daten sowie die Feststellbarkeit der Identität der übermittelnden und verarbeitenden Stellen gewährleisten. Im Falle der Nutzung allgemein zugänglicher Kommunikationsnetze sind Verschlüsselungsverfahren anzuwenden, die dem jeweiligen Stand der Technik entsprechen.

Auszug aus der DIN EN 13757-1

Kommunikationssysteme für Zähler – Teil 1: Datenaustausch

Allgemeines zur Sicherheit:

Für den Einsatz intelligenter Zähler bzw. Smart Metering sind vier Hauptsicherheitsaspekte erforderlich:

a) die Sicherstellung, dass nur entsprechende befugt Personen Zugriff auf die Informationen erhalten;
b) die Sicherstellung, dass die Informationen nicht unabsichtlich oder absichtlich geändert werden;
c) die Sicherstellung, dass die Informationsquelle nicht gefälscht werden kann;
d) die Sicherstellung, dass die Informationsquelle nicht verleugnet werden kann.

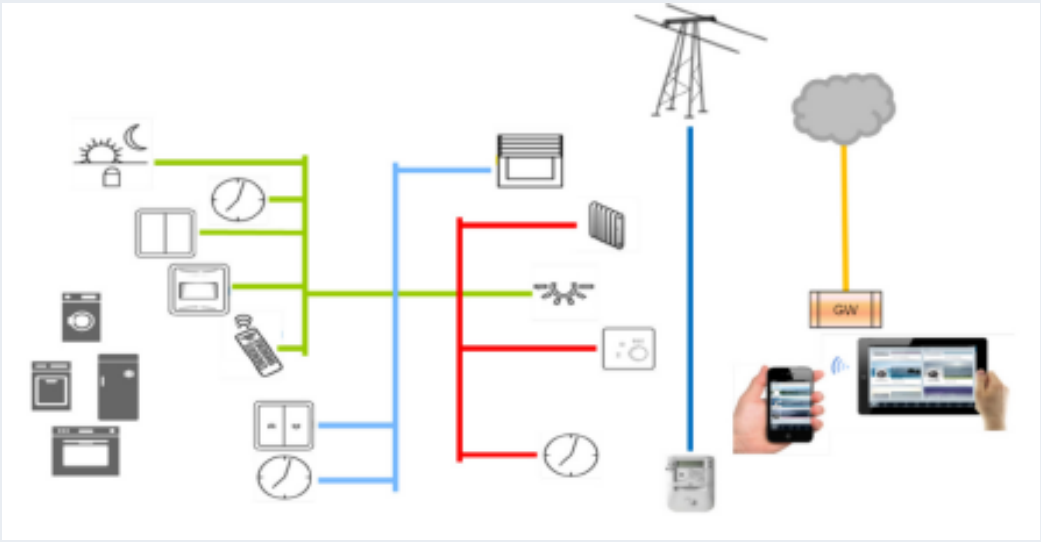
Allgemeines zur Schlüsselverwaltung:

Für einen Zähler wird von einer Lebensdauer von etwa 10 Jahren ausgegangen. Es ist daher zu erwarten, Dass die Schlüssel innerhalb dieser Zeitspanne mehrfach geändert werden müssen.
Als allgemeines Konzept gilt, dass es mindestens drei Stufen von Schlüsseln geben sollte.
a) Es gibt einen für die Verteilung des Schlüssel-Kodierschlüssel (key encryption key, KEK) zu verwendenden Hauptschlüssel (master key).
b) Es gibt einen Schlüssel-Kodierschlüssel, der zur Verteilung oder Erzeugung des normalen Schlüssels verwendet wird.
c) Es gibt „normale“ Schlüssel für die Verschlüsselung und Signierung der Daten.

Auszug aus der DIN EN 50631-1 (VDE 0705-631-1)

Netzwerk- und Stromnetz-Konnektivität von Haushaltsgeräten –
Teil 1: Allgemeine Anforderungen, allgemeine Datenmodellierung und neutrale Meldungen

Heutige Netzwerkstruktur:

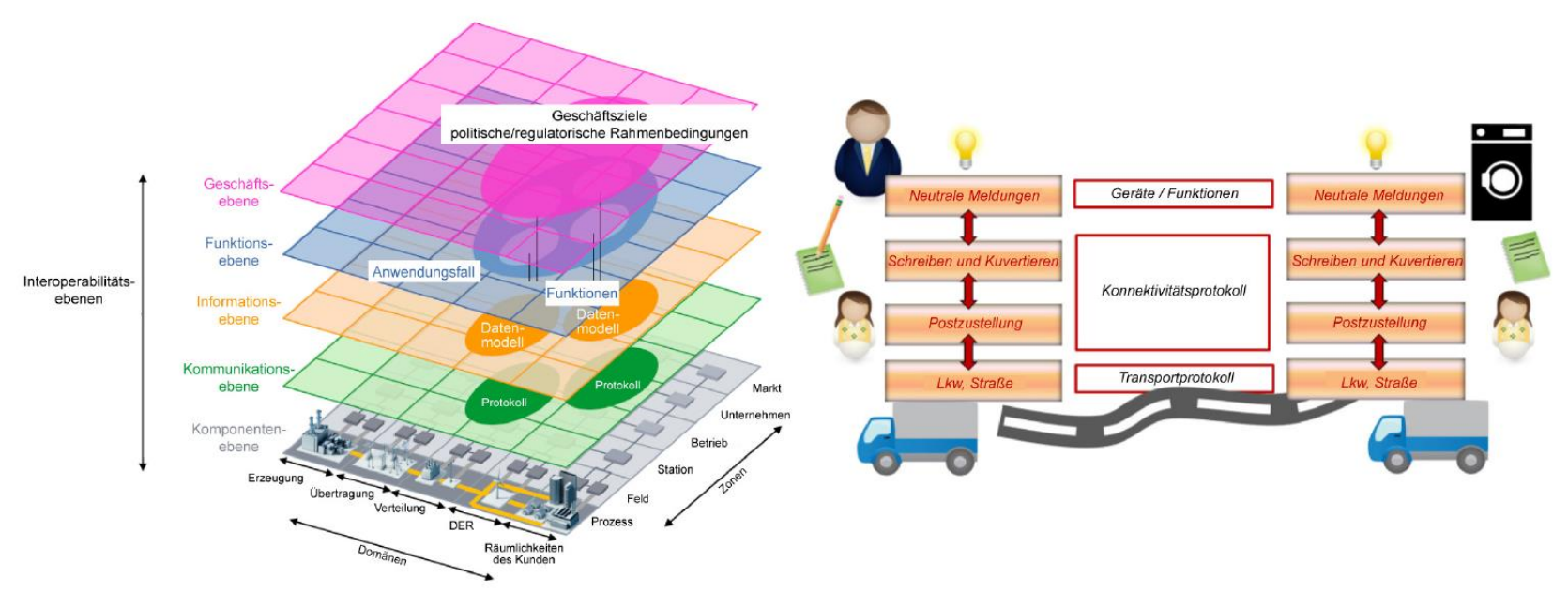


Es ist die Absicht in der DIN EN 50631-1, die Hauptpfeiler der Interoperabilität zu beschreiben, eines Satzes von neutralen Meldungen für den Informationsaustausch, der auf allgemeinen, für intelligente Haushaltsgeräte maßgeblichen Benutzergeschichten und Anwendungsfällen beruht. Sowie einer Zuordnung zu existierenden und aufkommenden Kommunikationstechnologien, um Interoperabilität innerhalb eines Intelligenten Stromnetz-, intelligenten Gebäude- und intelligenten Heim-Bereichs zu ermöglichen.

Auszug aus der DIN EN 50631-1 (VDE 0705-631-1)

Netzwerk- und Stromnetz-Konnektivität von Haushaltsgeräten – Teil 1: Allgemeine Anforderungen, allgemeine Datenmodellierung und neutrale Meldungen

Die Norm verwendet das Konzept des M490 Smart Grid Architecture Model (SGAM) als Vorlage.



Sowohl Funktions- als auch Informationsschicht liegen auf der Ebene von Anwendungen/Funktionen und Oberhalb jeder Art von Kommunikationsschicht wie dem ISO/OSI-Schichtmodell.

Auszug aus der DIN IEC 62746-3:2014-11

System-Schnittstelle zwischen Kunden-Energiemanagementsystemen und Energieversorgungsmanagementsystemen - Teil 3: Architektur

Prinzipien:

- Schnittstellen müssen auf Technologien und Normen beruhen;
- Schnittstellen müssen auf üblichen Softwaretechnologien beruhen oder deren Verwendung zulassen;
- Schnittstellen müssen grundsätzlich erweiterbar sein, zulassen, das neue Anwendungsnachrichten mit der Zeit festgelegt werden sowie zulassen, das neue Elemente in bestehende Nachrichten eingeführt werden;
- Schnittstellenentwicklung muss bezüglich der Programmiersprachen und Betriebssysteme agnostisch sein, darf aber zur selben Zeit die Verwendung von Java, C++, C#, Python, Linux, Windows, Android, usw. nicht ausschließen;
- Schnittstellenspezifikationen müssen bezüglich der Kommunikationstechnologie agnostisch sein, um mehrere Protokollzuordnungen zuzulassen;
- Schnittstellenspezifikationen müssen bezüglich der Kommunikationstechnologie agnostisch sein, um mehrere Protokollzuordnungen zuzulassen;
- Muss eine niedrige Technologieschwelle für Endprodukte und zugehörige Softwarekomponenten einrichten, um die Begrenzung der Fähigkeiten und der technischen Reichweite der Architektur zu vermeiden, um „beschränkte“ Geräte zu unterstützen, die nicht ohne Weiteres Internet-basierte Kommunikation unterstützen können.

Auszug aus der DIN IEC 62746-3:2014-11

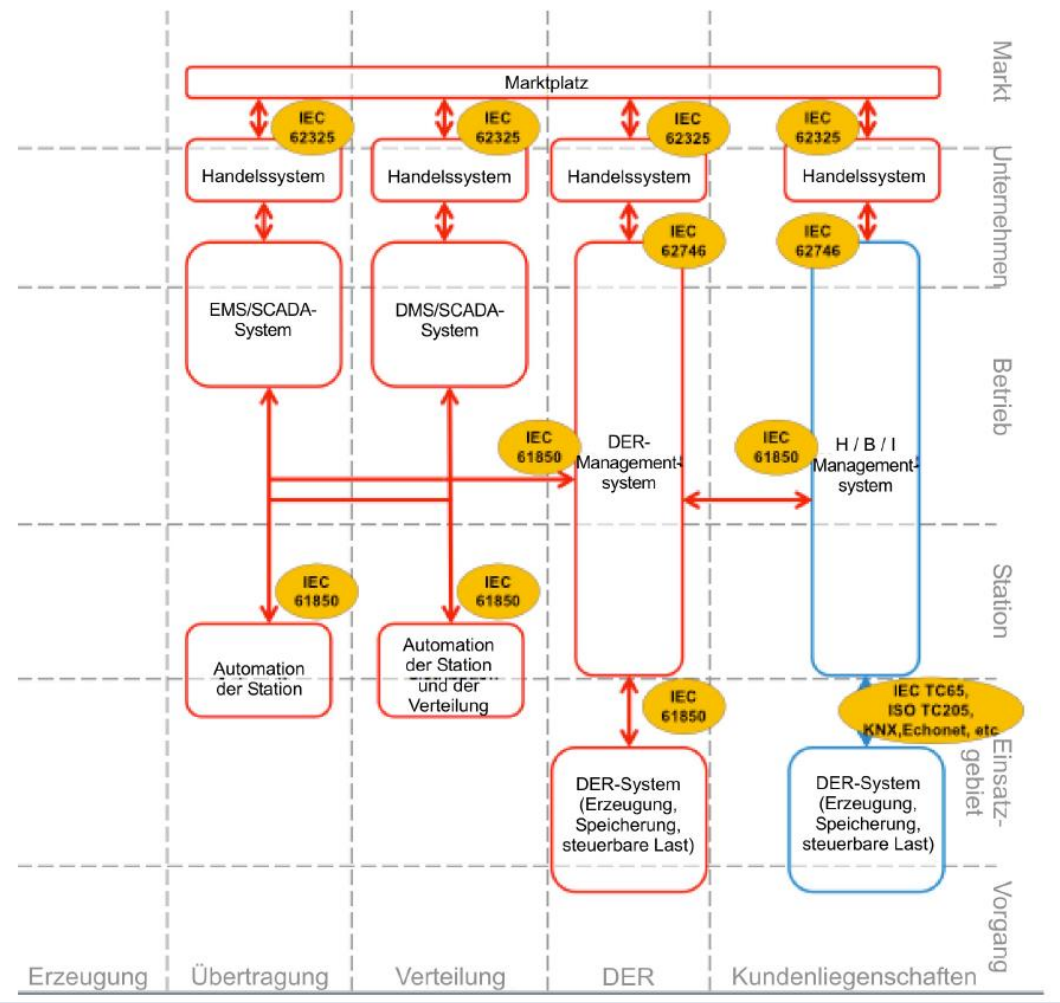
System-Schnittstelle zwischen Kunden-Energiemanagementsystemen und Energieversorgungsmanagementsystemen - Teil 3: Architektur

Zusätzliche kommunikationsspezifische funktionale Anforderungen:

- Virtuelle Ressourcen müssen eine eindeutige Identität aufweisen. Diese Identität darf als logische Adresse für die Kommunikation verwendet werden.
- Virtuelle Ressourcen müssen mit Berechtigungen konfiguriert werden, die es ihnen ermöglicht, authentifizierte Verbindungen mit einer vertrauenswürdigen Kommunikationsinfrastruktur aufzubauen.
- Kommunikation über das Internet muss verschlüsselt sein.
- Es darf nicht erforderlich sein, dass virtuelle Ressourcen eingehende Verbindungen akzeptieren, wo es keine Notwendigkeit geben darf, Ports in der Firewall zu öffnen, um ihnen die Kommunikation über das Internet zu gestatten. Virtuelle Ressourcen werden nur ausgehende Verbindungen zur Kommunikations-infrastruktur unter Verwendung ihrer Berechtigungen aufbauen.
- Es muss Mechanismen zur zeitlichen Synchronisation und Zeitstempel an den Nachrichten geben.
- Als Grundlage der Kommunikationsinfrastruktur müssen bestehende, bewährte Protokolle verwendet werden.
- Virtuelle Ressourcen oder Controller müssen einen rollenbasiertes Sicherheitsmodell unterstützen, das den Zugriff bis auf Parameter- oder Nachrichtentypebene festlegt.
- Geräte oder Controller müssen dazu fähig sein, gleichzeitig mehrere Verbindungen mit verschiedenen Kommunikationspartnern mit unterschiedlichen Vertrauensstufen aufrecht zu erhalten.

Auszug aus der DIN IEC 62746-3:2014-11

Beziehung von IEC 62746 zu anderen Normen



DKE VDE DIN DIN Universität Bremen **IT-Security NAVIGATOR** ITS|KRITIS

Ihre Mitarbeit und Unterstützung ist gefragt...

Der IT-Security-Navigator wird kein statisches Werkzeug bleiben, sondern sich mit den wachsenden rechtlichen und technischen Innovationen weiterentwickeln. Daher möchten wir **alle Nutzer** bitten, ihre Anmerkungen zum Navigator hinsichtlich

- Erweiterungen, Aktualisierungen
- Fehler
- neuer Gesetze und Standards

zu melden.

Bei Fragen und Anmerkungen für

IT-Normen und Standards
DKE
Sven Müller
Tel.: 069 63 08-395
it-securitystandards@vde.com

IT-Recht
Universität Bremen
Dr. Dennis-Kenji Kipker
Tel.: 0421 218 66049
kipker@uni-bremen.de

Wir danken Ihnen für Ihre Mithilfe!

Koordination VDE|DKE:
Andreas Harner
it-securitystandards@vde.com

Koordination DIN|KITS:
Volker Jacumeit