DIN/DKE - Roadmap

DEUTSCHE NORMUNGS-ROADMAP

IT-SICHERHEIT

Version 3

DIN

DKE

VDE DIN

Inhalt

0 Vorwort zur 3. Ausgabe 2

1 Einleitung 2

1.1 Allgemeines 2

1.2 Die Koordinierungsstelle IT-Sicherheit (KITS) 3

2 Ziel und Herangehensweise der Normungsroadmap 5

3 Normung und Standardisierung 5

3.1 Einführung in die Standardisierung und Normung 5

3.2 Einsatzgebiete der Normung im Bereich der Informationssicherheit 6

4 Grundlegende Rahmenbedingungen 7

4.1 Gesetzliche/regulatorische Entwicklungen auf europäischer Ebene 7

4.2 neue Paradigmen in Geschäftssystemen für Datensicherheit und Datenschutz 7

4.3 Security by Design 9

4.4 Usability von IT Sicherheit 11

5 Schwerpunktgebiete 13

5.1 Datenschutz 13

5.1.1 Themenbeschreibung 13
5.1.2 aktive Standardisierungsgremien 13
5.1.3 Derzeitige Landschaft (Status quo in Bezug auf IT-Sicherheit) 14
5.1.4 Handlungsbedarfe (Normungsbedarfe) 14

5.2 Energieversorgung und -erzeugung 15

5.2.1 Themenbeschreibung 15
5.2.2 Energieversorgung (Smart Grid) 16
5.2.3 Energieerzeugung (Kerntechnik) 12

5.3 Industrielle Produktion (Industrie 4.0) 14

5.3.1 Themenbeschreibung 14
5.3.2 aktive Standardisierungsgremien 15
5.3.3 Derzeitige Landschaft (Status quo in Bezug auf IT-Sicherheit) 15
5.3.4 Handlungsbedarfe (Normungsbedarfe) 21

5.4 Gesundheitsinformationssysteme und Medizintechnik 23

5.4.1 Themenbeschreibung 23
5.4.2 aktive Standardisierungsgremien 24
5.4.3 Derzeitige Landschaft (Status quo in Bezug auf IT-Sicherheit) 25
5.4.4 Handlungsbedarfe (Normungsbedarfe) 26

5.5 Elektromobilität 27

5.5.1 Themenbeschreibung 27
5.5.2 aktive Standardisierungsgremien 30
5.5.3 Standardisierungsaktivitäten Datensicherheit und Datenschutz 30

5.5.4 Handlungsbedarfe (Normungsbedarfe) 32
5.6 Smart Home 33
5.6.1 aktive Standardisierungsgremien 35
5.6.2 Anwendungsregel elektrische Systemtechnik in Heim und Gebäude – IT-Sicherheit und Datenschutz – Anforderungen 35
5.6.3 Kommunikationssicherheit 35
5.6.4 Kommunikation über Technologie-Grenzen 36
5.6.5 Schutzprofil für ein Smart Meter Gateway 36
5.6.6 Smart Home und Smart Building 38
6 aufkommende Normungsfelder 40
6.1 Ambient Assisted Living - AAL 40
6.1.1 Datenschutz bei AAL 41
6.1.2 Entwicklung der AAL-Normungslandschaft im Bereich Informationssicherheit 42
6.2 Smart Cities 43
7 Europäische Aktivitäten im Bereich Cybersecurity-Normung 44
7.1 Cyber Security Focus Group (CSCG) 44
7.2 ETSI TC Cyber 46
8 Kritische Infrastrukturen 46
9 Fazit 49

0 Vorwort zur 3. Ausgabe

Mit der dritten aktualisierten Ausgabe der Roadmap IT-Sicherheit stellt die Koordinierungsstelle IT-Sicherheit bei DIN die aktuelle Situation und zukünftige Entwicklungen in verschiedenen Schwerpunktgebieten rund um das Thema IT-Sicherheit bereit. Neu in der dritten Ausgabe sind den Schwerpunktgebieten vorangestellte allgemeine Entwicklungen, die übergreifend von Bedeutung sind. Statt der Auflistung relevanter Sicherheitsstandards im Anhang wird nun auf die im Internet verfügbare Auflistung verwiesen, die von DIN und DKE gepflegt wird. https://www.security-standards.de/

1 Einleitung

1.1 Allgemeines

Die Zeiten, in denen man unter Informationstechnik nur vernetzte Mikro-Computer verstand, die die Bürokommunikation und die betriebswirtschaftlichen Funktionen erleichtern, sind längst vorbei. Die zentrale Herausforderung der letzten Jahre war die umfassende Durchdringung der unterschiedlichsten Bereiche mit Informationstechnik. Dieser Prozess ist in vielen Bereichen immer noch in vollem Gange, dennoch ist aus Sicht der IT-Sicherheit bereits die nächste Herausforderung zu bewältigen, die zunehmende Vernetzung der IKT durchdrungenen Bereiche untereinander.

So verbirgt sich hinter dem Schlagwort Industrie 4.0 nicht nur die informationstechnische Durchdringung der Fertigungsprozesse, sondern eben auch die Vernetzung mit der „klassischen“ Büro-IT. Das „Internet der Dinge“ hält Einzug in die Fertigungshallen. Die Ausrüstung diverser

physischer Objekte (Cyber-physical Systems) mit informationstechnischer Intelligenz – meist mittels RFID-Transpondern - ermöglicht neue Verfahren: Fertigungsvorgänge, in denen die Rohlinge selbst Informationen per Funk an das Fertigungssystem senden („Smart Factory“); Materialflüsse, die vom Fördergut beeinflusst werden. All dies direkt verbunden mit den Entwicklungs-, Marketing- und Controlling-Abteilungen der Unternehmen.

Der Trend zum Einsatz von internetähnlichen Netzen, die „gewöhnliche Objekte“ einbeziehen, lässt sich auch im Heimbereich feststellen. Zum Thema „Intelligente Haussteuerung“ („Smart Home“) gibt es bereits etliche Angebote, zum Beispiel Heizkörperthermostate, Lichtschalter und Rolladensteuerungen, die hausintern (per Funk) ansteuerbar und per Steuergerät via Internet erreichbar sind; oder Waschmaschinen und Kühlschränke, deren Status sich per Smartphone und Hausbussystem abrufen lassen. Last but not least lassen sich diese Ideen und Technologien auch im Bereich des Ambient Assisted Living (AAL) anwenden. Assistenzsysteme für ein gesundes Leben (z.B. Servicesysteme für alte Menschen) können auf diese Weise realisiert werden.

Im „Smart Grid“ wird auf die Intelligenz des Energieversorgungssystems gesetzt. Heutzutage gibt es nicht nur Produzenten und Konsumenten, sondern auch „Prosumer“, also Verbraucher von Energie, die gleichzeitig auch Produzenten sind (Beispiel: Solaranlage). Weiterhin hat der massive Einsatz insbesondere von Solaranlagen und Windkraftanlagen zu einer nie dagewesenen dezentralen Verteilung der Energieeinspeisung geführt. Das Verteilen von elektrischer Energie und die Sicherstellung der Energieversorgung wird zu einem zunehmend komplexen Problem. Eine wichtige Systemkomponente im Smart Grid ist das Smart-Meter, der intelligente Energieverbrauchszähler. Das Gerät enthält eine Mikroprozessorsteuerung und ermöglicht die Fernauslesung (z.B. per GPRS).

Smart-Metering führt schnell zum Thema „Elektromobilität“, denn Aufladevorgänge beim Elektroauto müssen gemessen werden, um abrechenbar zu sein. Und bei der Mobilität von Fahrzeugen wird heutzutage immer mehr an Vernetzung gedacht (Car2X-Kommunikation): Autos kommunizieren mit anderen Autos (z.B. zur Unfallvermeidung) oder mit der Verkehrsinfrastruktur (z. B. Stauinformationen). Es gibt auch Ideen, einen intelligenten Fahrzeugschlüssel (biometrische Verifikation, Einsatz von PKI-Zertifikaten) einzuführen, der Benutzerprofile von Fahrern speichern kann.

Industrie, Energie, Verkehr, privates Umfeld: die Infrastrukturen wachsen zusammen. Und der Enabler für diese revolutionäre Entwicklung ist die Informationstechnik.

Viele Lösungen aus den genannten Themengebieten sind derzeit noch proprietär, es mangelt an Interoperabilität, der Bedarf an Normung ist leicht erkennbar.

Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität sind wohlbekannte Ziele der Informationssicherheit. Diese Ziele müssen auch in modernen Infrastrukturen erreichbar sein. Der Schutzbedarf von industriellen Anlagen, Smart-Metern und Fahrzeugsteuerungen ist hoch. Die Anwendung von Sicherheitsmaßnahmen darf nicht dem Zufall überlassen bleiben oder aufgrund von Wirtschaftlichkeitsbetrachtungen auf ein Minimum reduziert sein. Hier besteht ein dringender Bedarf an sicheren Produkten und Systemen, auch Managementsystemen. Und daher liegt die Notwendigkeit der Standardisierung von Anforderungen und Umsetzungsvarianten auf der Hand.

1.2 Die Koordinierungsstelle IT-Sicherheit (KITS)

Das reine Erarbeiten von Normen ist in einer Technikwelt, die Aspekte der IT-Sicherheit in einer Vielzahl von Verfahren und Produkten berücksichtigen muss, nicht mehr ausreichend. Die

branchenübergreifende Koordinierung und die Auswahl der am besten für den jeweiligen Anwendungszweck geeigneten Normen wird in Zeiten beschleunigter Technikkonvergenz immer wichtiger. Hier sehen sich die Experten, die bisher reine IT-Sicherheitsnormen entwickelt haben, vor die Notwendigkeit gestellt, in anwendungsbezogenen Technikbereichen über die vorhandenen IT-Sicherheitsnormen und deren Anwendungen vermehrt zu informieren. So wird z. B. das intelligente Stromnetz (Smart Grid) nur dann beim Kunden Akzeptanz finden, wenn neben der klassischen IT-Sicherheit auch Informationssicherheits- und Datenschutzaspekte von Anfang an in die Systemarchitektur einfließen. Dabei ist aber zu bedenken, dass solche Informationen über grundlegende IT- Sicherheitsnormen zwar Interessenten in verschiedenen Branchen erreichen, diese aber branchenspezifische IT-Sicherheitslösungen erarbeiten, deren Kompatibilität mit Lösungen anderer Branchen nicht von vorn herein gewährleistet ist. Angesichts gesellschaftlicher und politischer Forderungen nach übergreifender, vernetzter Sicherheit sind branchenspezifische Insellösungen im Bereich der IT-Sicherheit nicht mehr akzeptabel, da auch die IT-Sicherheit selbst interoperabel sein muss. Bei Querschnittsthemen, die mehrere Branchen betreffen, müssen also auch die branchenspezifischen Normungsaktivitäten untereinander koordiniert werden. Zu genau diesem Zweck betreibt das DIN die Koordinierungsstelle IT-Sicherheit (KITS). Die KITS hat im Auftrag des DIN-Präsidiums und dessen IKT-Koordinierungsausschusses FOCUS.ICT folgende Aufgaben:

- Koordinieren der Tätigkeiten unter schiedlicher Akteure (Normenausschüsse, Verbände, Behörden), die branchenspezifische IT-Sicherheitsstandards entwickeln
- Beraten von Normenausschüssen bei der Entwicklung von Normen mit IT-sicherheitsrelevantem Inhalt (z. B. Smart Grids, medizinische Informatik, industrielle Steuerung)
- Pflegen eines Verzeichnisses aller IT- und Informationssicherheitsrelevanten Normungsvorhaben, die von Bedeutung für die deutschen Interessenträger sind
- Pflegen einer Normungs-Roadmap IT-Sicherheit
- Gezielt und koordiniert Einfluss nehmen auf die europäische und internationale Normung im Interesse der deutschen Industrie, Behörden und Wissenschaft

Den strukturellen Rahmen, in den die KITS eingebettet ist stellt Abbildung 1 dar.

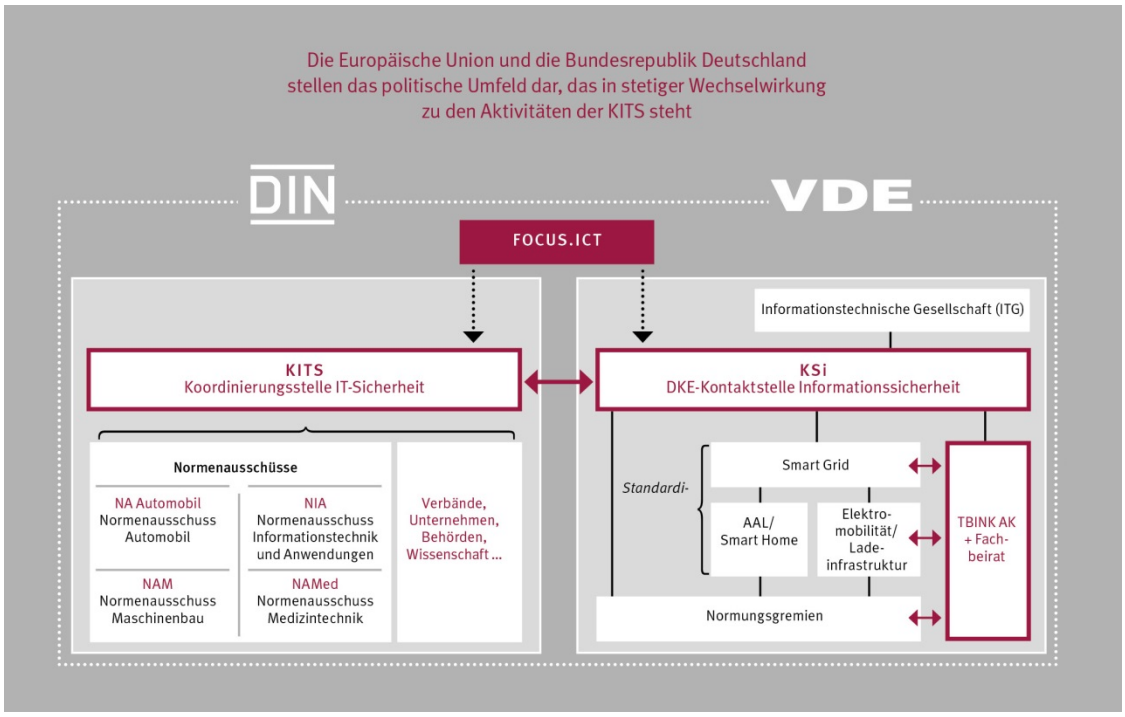


Abbildung 1: Struktur der Koordinierungsstelle IT-Sicherheit

Weitere Informationen zur KITS finden Sie unter www.din.de/go/kits

2 Ziel und Herangehensweise der Normungsroadmap

Ziel dieser Normungsroadmap ist es, Bereiche aufzuzeigen, in denen Bedarfe nach Sicherheitslösungen auf Einsatzmöglichkeiten der Standardisierung treffen. Die Roadmap soll dabei helfen, die Normungsaktivitäten zu koordinieren, indem aufgezeigt wird, in welchen Gremien bereits Arbeiten angestoßen oder sogar abgeschlossen worden sind. Die Diskussion in den Fachkreisen hat aufgezeigt, dass die Informationstechnik nicht mehr branchenspezifisch betrachtet werden kann sondern eine Querschnittstechnologie ist, die über Branchen hinweg zum Einsatz kommt. Daher ist das Bekanntmachen existierender Gremien und Standards der erste Schritt zur Koordinierung. Die Roadmap gibt Handlungsempfehlungen ab, welche Aktivitäten angestoßen werden sollten, um den Bedarfen in den identifizierten Bereichen gerecht zu werden. Durch den hohen Vernetzungsgrad, den aufkommende Trends in der Informationstechnik aufweisen ist eine Betrachtung branchenübergreifend notwendig um der Sachlage gerecht zu werden. In dieser Roadmap werden daher aktuelle branchen- und technikübergreifende Schwerpunktthemen aufgegriffen und näher beleuchtet.

3 Normung und Standardisierung

3.1 Einführung in die Standardisierung und Normung

Normung versteht sich als die planmäßige Gemeinschaftsarbeit der interessierten Kreise zur Vereinheitlichung von materiellen und immateriellen Gegenständen. Das wohl bekannteste Beispiel für erfolgreiche Normung ist das vereinheitlichte Papierformat DIN A4. Normen halten den Stand der Technik in öffentlich zugänglichen Dokumenten fest und sorgen somit durch diskriminierungsfreien Zugang zu Wissen und Information für:

- Marktbildung bei Innovativen Lösungen
- Marktöffnung
- Wissenstransfer
- Verbreitung von Best Practices
- Interoperabilität
- Reputationstransfer auf den Anwender
- Vertrauen in Dienste und Produkte die normgerecht erstellt wurden

Nach den Grundsätzen der Normungsarbeit darf sie nicht zu einem individuellen Sondervorteil führen, sondern hat dem gesamtgesellschaftlichen Nutzen zu dienen. Dies stellt den Hauptunterschied zur Konsortialstandardisierung dar. Die Normung findet in Deutschland in den Gremien des DIN Deutsches Institut für Normung statt, das durch einen Staatsvertrag mit der Bundesrepublik Deutschland autorisiert ist, die Erarbeitung nationaler Normen sowie die Vertretung Deutschlands in den europäischen und internationalen Normungsorganisationen zu übernehmen.

In einer vernetzten Welt nutzt die sichere Infrastruktur eines Teilnehmers auch den anderen Teilnehmern, da diese nicht für Angriffe missbraucht werden kann. Positive Netzwerkeffekte treten hier zutage. Die Normung als gemeinschaftliche Aufgabe bietet sich daher wie kaum ein anderes Instrument an, diese Netzwerkeffekte gezielt zu befördern und das allgemeine Sicherheitsniveau zum Nutzen aller zu erhöhen.

3.2 Einsatzgebiete der Normung im Bereich der Informationssicherheit

Ein Mittel zur Beförderung der IT-Sicherheit ist der Einsatz von Normen und Standards. Normen und Standards nehmen verschiedene Aufgaben war, die geeignet sind, das allgemeine Sicherheitsniveau in Systemen und Netzwerken der Informationstechnik, unternehmensübergreifend und auch unternehmensintern, zu erhöhen, wie auch die Entwicklung zukunftsweisender Technologien zu befördern. Normen und Standards adressieren mittels vereinheitlichter technischer und organisatorischer Maßnahmen die drei IT-Sicherheitsziele Verfügbarkeit, Vertraulichkeit und Integrität und können dabei folgendes leisten:

- Transparenz von Sicherheitslösungen (Vertrauen schaffen)
- Verbreitung von Best Practices
- Anwendungshilfe für kleinere Unternehmen
- Darstellung allgemein akzeptierter Sicherheitslösungen
- Interoperabilität durch definierte Schnittstellen
- Bereitstellung gemeinsamer Systemarchitekturen
- Bereitstellung einer gemeinsamen Terminologie
- Harmonisierung existierender Normen und Standards
- Nutzung existierender Lösungen anderer Branchen
- Internationalisierung nationaler Lösungen

4 Grundlegende Rahmenbedingungen

4.1 Gesetzliche/regulatorische Entwicklungen auf europäischer Ebene

Auf europäischer Ebene sind in den letzten Jahren einige Verordnungen und Richtlinien zum Thema Datenschutz und Datensicherheit entstanden und verabschiedet worden, welche die weitere Entwicklung im Bereich der Normung von IT-Sicherheit und Datenschutz zentral betreffen. Zu nennen sind hier insbesondere die EU Datenschutzgrundverordnung, die NIS Richtlinie und die e-IDAS Verordnung, die Geheimschutz Richtlinie sowie der Entwurf für eine e-Privacy Verordnung.

Die EU Datenschutzgrundverordnung strebt eine europaweite Harmonisierung des Datenschutzes an und enthält deutliche stärkere Nutzerrechte. Die am 14. April 2016 verabschiedete Verordnung tritt nach einer Übergangfrist von zwei Jahren im Mai 2018 in Kraft.

Die NIS-Richtlinie (Richtlinie (EU) 2016/1148) für Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union) ist Teil der Europäischen Cybersicherheitsstrategie mit dem Ziel, für Unternehmen, öffentliche Einrichtungen und Nutzern in der EU deutlich mehr Sicherheit für Netz- und Informationssysteme gegenüber dem deutlich gestiegenen Risiken aus dem Cyberraum zu schaffen. Insbesondere sog. Kritische Infrastrukturen oder auch Anbietern sog. “digitaler Dienste” werden neue Pflichten bezgl. Security auferlegt.

Die Mitgliedsstaaten müssen die am 8. August 2016 in Kraft getretene NIS-Richtlinie bis zum 10. Mai 2018 in nationales Recht umsetzen. In Deutschland wurde mit dem am 25. Juli 2015 in Kraft getretenen sog. IT-Sicherheitsgesetz für Kritische Infrastrukturen ein Teil bereits umgesetzt.

eIDAS (Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG) ersetzt die EU-Signaturrichtlinie von 1999 sowie das deutsche Signaturgesetz und regelt die Erstellung, Überprüfung und Aufbewahrung von qualifizierten elektronischen Signaturen, Zeitstempeln, Siegeln und Website-Authentifizierung sowie die Zustellung von elektronischen Einschreiben im öffentlichen Sektor.

Die im Entwurf vorliegende EU ePrivacy-Verordnung soll ergänzend zur Datenschutz-Grundverordnung die elektronische Kommunikation und den Umgang mit personenbezogenen Daten regeln.

4.2 neue Paradigmen in Geschäftssystemen für Datensicherheit und Datenschutz

Gegenwärtig werden wir mit massiven Paradigmenänderungen organisatorischer, methodologischer sowie technologischer Art in den Geschäftsprozessen konfrontiert, die massive Auswirkungen auf Anforderungen und Lösungen für IT-Security und den Datenschutz haben. Die technologischen Veränderungen umfassen neue Generationen von Rechnerarchitekturen und explodierende Speicherkapazitäten, aber auch die Hinwendung zu verteilten Systemen, mobilen Technologien, Nano- und Molekulartechnologien, Wissensrepräsentation und –management, KI, Big Data & Business Analytics, Cloud Computing, Social Business, etc.

Die Paradigmen moderner Informationsverarbeitung können wie in Bild 1 gezeigt generalisiert werden.

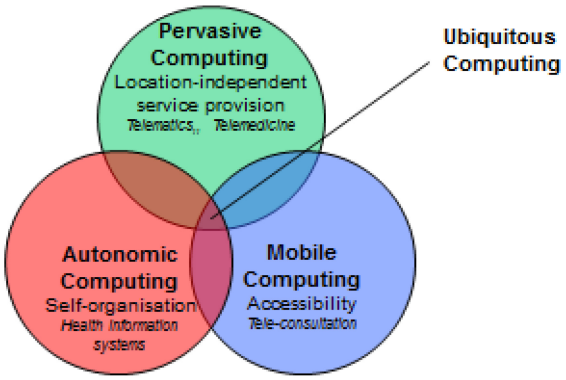


Abbildung 1: Neue Paradigmen der Informationsverarbeitung

Diese Paradigmenwechsel führen beispielsweise im Gesundheits- und Sozialwesen zu hochverteilten offenen Systemen, die multiple Zuständigkeits- und Policy-Domänen, Technologien, Wissens- und Konzeptrepräsentationsstile, Sprachen, Methodologien, Interessen und Verhalten, kultureller Hintergrund und Erwartungen, Bildung und Fertigkeiten, etc. integrieren. Diese Integration über mehrere Dimensionen hinweg erfordert fortgeschrittene Interoperabilitätslösungen. Die zu bewältigenden Interoperabilitätsherausforderungen beschränken sich dabei nicht allein auf die IKT-Umgebung, sondern schießen alle Akteure und ihren Kontext ein. So liefern geeignete transparente Datenschutz- und Datensicherheitslösungen Vertrauen und somit Akzeptanz von Lösungen und ihrer IT-Unterstützung. Die Bedeutung dieses Aspektes wird deutlich, wenn man beachtet, dass beispielsweise Länder, die die eHealth und Telemedizin-Szene dominieren 50% ihres Budgets für Datensicherheits- und insbesondere für Datenschutzlösungen verwenden. Die Ansicht, dass Datenschutz und Datensicherheit keine Verhinderungs- sondern Ermöglichungs-Technologien sind muss sich auf allen Ebenen durchsetzen. Technologien, die fortgeschrittene Geschäftsprozesse ermöglichen, müssen ebenso für Datenschutz- und Datensicherheitsdienste angewendet werden:

- Paradigma der verteilten Versorgung erfordert ein Verteiltes Datenschutz- & Datensicherheits-Management.
- Mobile Anwendungen erfordern mobile Sicherheitstechnologien
- Big Data & Analytics erfordern Big Data & Analytics für Datenschutz & Datensicherheit
- Adaptive Systeme erfordern adaptives Datenschutz- & Datensicherheits-Management
- Personenzentrierte Versorgung erfordert persönliche Policies
- Business Intelligence erfordert Security Intelligence

Diese neuen Paradigmen erfordern von den Komponenten “Build-in” Security und Datenschutz. Dies wiederum erfordert Konzepte für „Security and Privacy by Design“. Die Einbindung des Anwenders, vom Datentechnisch behandelten Objekt zum aktiven Element des Prozesses erfordert Konzepte für eine Bürger-Mündigkeit (Citizen Empowerment). Ein händisches Management der verschiedenen Komponenten wird nicht mehr möglich sein, die Definition, Harmonisierung und Durchsetzung von Policies muss automatisiert und durch spezielle SOA- bzw. Web-Services unterstützt werden (Policy Information Point, Policy Decision Point, Policy Enforcement Point). Hierzu müssen umfassende

Policies formal beschrieben werden. Dies wird zur Folge haben, dass Datenschutz- und Datensicherheitsmanagement zunehmend modellgetrieben, ontologiebasiert automatisiert werden wird. Dass der Erfolg bestimmter Mechanismen (z.B. die Anonymisierung) unter den Bedingungen moderner Versorgungsparadigmen wie pHealth und systemmedizin) nicht mehr garantiert werden kann (die umfassende informationelle Repräsentation des Individuums in wie pHealth- und Systemmedizinumgebungen macht jedes Individuum einzigartig), befreit uns nicht von der Anwendung datenschutzfreundlicher Technologien (De-Identifikation durch Anonymisierung bzw. Pseudonymisierung, Verschlüsselung, Hinterfragung von Datensammlungen anstatt prinzipieller Minimierung, etc.) Der Perimeter-Datenschutz- und –Datensicherheitsansatz muss durch einen datengetriebenen und datenzentrierten Ansatz ersetzt werden. „Data Segmentation for Privacy and Security“-Standards sind ein richtiger Ansatz dafür. Bespielstandards hierfür sind:

- National Institute of Standards and Technology. NIST FIPS 188 – Standard Security Label for Information Transfer. Gaithersburg, Maryland, USA; 1994.

- HL7 International Inc. HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1. Ann Arbor: HL7 International; September 2013, bzw.

Das Überprüfen von Compliance mit Regulierungen wird durch fallbezogenes und individualisiertes und damit kontinuierliches Controls- und Risikomanagement gemäß dem Datenschutz-Management abgelöst. Der vorgeschlagene und inzwischen standardisierte system-orientierte, architektur-zentrierte, ontologie-basierte und policy-getriebene Ansatz ermöglicht flexible und intelligente Interoperabilität von ubiquitären personalisierten Diensten durch die Harmonisierung der unterschiedlichen Perspektiven und Konzeptrepräsentationen vielfältiger Stakeholder-Gruppen. Im Gesundheitsbereich, der diesen Paradigmenwechsel frühzeitig aufgenommen hat, wurde die Lösung in ISO und CEN Gremien standardisiert (u.a. ISO 22600, ISO 21298, ISO EN 13606), implementiert und z.B. auf den HIMSS 2013-2016 demonstriert.

Letztendlich sei im Kontext zunehmender Cyber-Kriminalität auf die Bedeutung der funktionalen Sicherheit (safety) und ihre Verknüpfung mit der Informationssicherheit hingewiesen, die insbesondere im Bereich von eHealth und Telemedizin z.B. für Internet-verbundene Medizingeräte und Implantate ein wachsendes Problem zeitigt.

4.3 Security by Design

Die fortschreitende Digitalisierung bringt IKT und vertikale Technikbereiche wie z. B. Smart Cities, Mobilität, Gesundheitswesen oder tragbare Consumergeräte, die u.a. beim Sport Gesundheitsdaten aufzeichnen in Berührung und treibt sehr stark die Technikkonvergenz. Daraus resultieren gegenseitige Einflüsse auch in der Normung und Standardisierung. Je mehr Endgeräte auch im Consumerbereich im Internet angeschlossen sind, desto stärker muss IT-Sicherheit auf ergonomische Aspekte berücksichtigen und Anforderungen von den sogenannten Endnutzern im Design der Produkte und Lösungen integrieren. Im Bereich der B2B Themen kommt hinzu, dass die unterschiedlichen Standardisierungskulturen aus den klassischen Industrien, die eine sehr lange Normungs- und Standardisierungshistorie haben, mit der relativ neuen Internetwirtschaft aufeinander treffen. Im Bereich von Industrie 4.0 sind das der Shopfloor und der Officefloor.

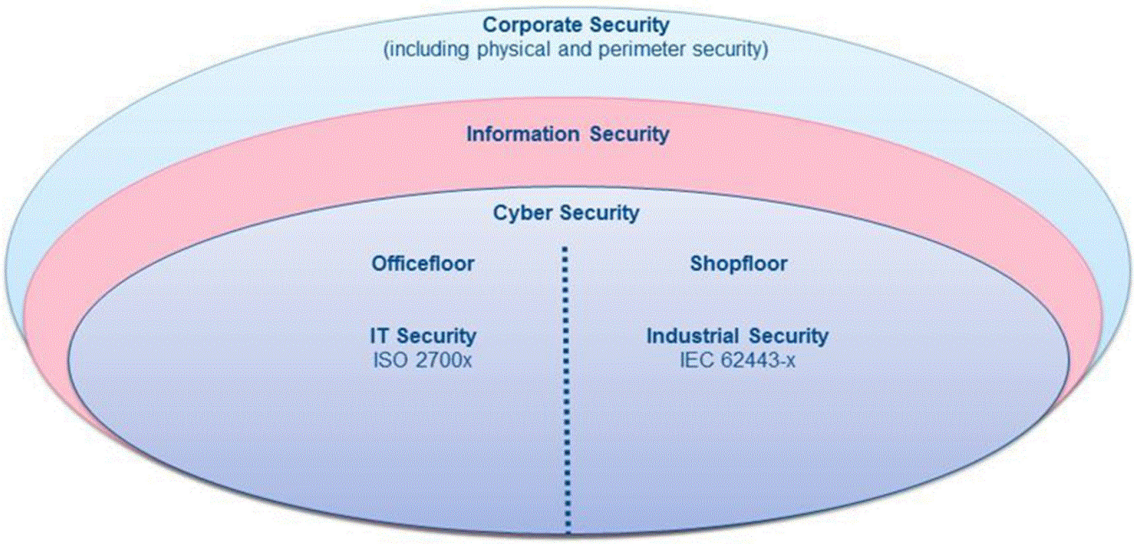


Abbildung 2: Einordnung Cyber Security

Hier müssen beide Bereiche sich zur Terminologie und Ontologie zusammen finden und die gegenseitigen Abhängigkeiten aber auch Vorgaben müssen erkannt und akzeptiert werden. In den Unternehmen bedeutet das ggf. eine Neuordnung von Verantwortlichkeiten und Prozessschnittstellen und in der Normung und Standardisierung ein stärkeres Kooperieren, wie es ISO und IEC bei der Erarbeitung einer gemeinsamen internationalen Norm zur Umsetzung der DIN SPEC 91345 – RAMI 4.0 durchführen.

Security by Design ist eine wesentliche Voraussetzung dafür, dass IT-Lösungen und Produkte interoperabel eingesetzt werden können, damit das Internet der Dinge auch Wirklichkeit werden kann. Dabei ist zu berücksichtigen, dass insgesamt eine Vertrauenskette hergestellt werden kann. Die Applikation, die Daten von anderen als Input bekommt, muss sich darauf verlassen können, dass die Daten von der richtigen Stelle und mit der vereinbarten Qualität angeliefert werden. Aber auch, dass die Daten auf dem Transportweg nicht manipuliert und gefälscht werden können oder gar mit „schädlichem“ Code angereichert werden. Hierzu bedarf es dann beim Empfänger entsprechender Automatismen, um die Integrität, Echtheit und „Schadstofffreiheit“ zu prüfen. Auf der anderen Seite müssen Produkte und System nicht nur vor Angriffen von außen gesichert werden. Security by Design muss auch berücksichtigen, dass die Ergebnisse, die eine Lösung oder Produkt anderen zuliefert für diese keine Gefahr darstellen.

Damit bettet sich das Thema Security by Design in eine ganze Reihe von Management-Normen ein und kann nicht nur einfach durch eine ISO/IEC JTC 1 SC 27001 Konformität erfolgen. Vielmehr sind die Bereiche

- Risikomanagement
- Evaluation von Prozessbewertungen
- Software Engineering
- Qualitätsmanagement

Insgesamt zu berücksichtigen.

Abbildung 3: Normungslandschaft für Security by Design

Abgeleitet aus den kritischen Erfolgsfaktoren des Unternehmen bzw. eines Bereichs fehlen heute jedoch noch Metriken für

- Qualitätsniveau
- Sicherheitsniveau

4.4 Usability von IT Sicherheit

Bei der Betrachtung von IT-Sicherheit von Technologien zeigt sich immer wieder das Konfliktfeld IT-Sicherheit versus Usability und Zugänglichkeit für den Nutzer. Wieviel IT-Sicherheit ist nötig, um eine Technologie und den Anwender vor Angriffen und Gefahren zu schützen und wann führen Maßnahmen zur IT-Sicherheit letztlich dazu, dass IT-Systeme nicht mehr nutzbar und akzeptabel für den Nutzer sind.

Für dieses horizontale Thema benötigt man Leitlinien und Gestaltungsprinzipien insbesondere in Bereichen, wo der Endnutzer direkt mit den Technologien interagiert oder der Endnutzer ggf. sogar einen erhöhten Schutzbedarf hinsichtlich von Ergonomie und Zugänglichkeit aufweist, z. B. im Bereich AAL bei der Nutzung durch ältere Personen.

Usability von Technologien wird schnell als „weiche“ Anforderung des Nutzers abgetan, wohingegen IT-Sicherheit als harte und damit dringend zu erfüllende Anforderung angesehen wird. Fehlende Usability von Technologien kann jedoch die Funktionsfähigkeit von Systemen so weit beeinträchtigen, dass im schlimmsten Fall der Wert des Systems als Ganzes in Frage gestellt ist. Beispiele für Beeinträchtigung der Systemfunktionsfähigkeit durch fehlende Usability können sein: 1. Wegen schlechter Benutzerführung stellt sich ein Passagier in der falschen Warteschlange an der (automatisierten) Grenzkontrolle an, alle hinter ihm stehenden Passagiere werden aufgehalten, weil die Problemlösung Zeit in Anspruch nimmt. Die Automatisierung der Grenzkontrolle wurde jedoch eingeführt, um Prozesse zu beschleunigen. 2. Das Display am Geldautomaten reagiert nicht auf Tastendrücke, die PIN wird falsch eingegeben.

Usability ist somit nicht allein eine Nutzeranforderung, sondern auch Systemanforderung. Fehlende Usability beeinflusst die Systemleistung im Hinblick auf Faktoren wie: Schnelligkeit und Durchsatz

(z.B. Zahl der Grenzübertritte in einer Zeiteinheit), Automatisierte Abwicklung von Abläufen, Fehlerraten von Systemen.

Ist Usability nicht gegeben, kann der Nutzer nicht „smart“ mit der Technologie umgehen und macht Fehler, weil er z.B. nicht weiß, was von ihm erwartet wird. Der Nutzer ist dann z.B. nicht in der Lage, Angriffe zu erkennen und sich vor diesen zu schützen.

Fehlende Usability kann zusätzlich die Akzeptanz der Nutzer negativ beeinflussen. Nicht-kooperative Nutzer können versuchen, ein System auszutricksen und zu korrumpieren.

Letztlich kann also fehlende Usability Fehler und Missbrauch provozieren und damit zu einer Schwächung der IT-Sicherheit führen.

Bei der Einführung von Maßnahmen zur IT-Sicherheit muss der Nutzer somit also eingebunden werden, indem ihm vermittelt wird, warum bestimmte Sicherheitsmaßnahmen notwendig sind und welchen Beitrag er dazu leisten kann. Auch muss der Nutzer in seiner Welt abgeholt werden: ein kooperativer Nutzer wird nicht versuchen, das System auszutricksen oder „umständliche“ Aktivitäten zu umgehen. Es sind solche Sicherheitsmaßnahmen zu wählen, die für den Nutzer transparent, akzeptabel und leicht umsetzbar (usable) sind.

Den Zielkonflikt zwischen IT-Sicherheit und Usability sollte man durch geeignete Maßnahmen versuchen aufzulösen. Hierfür muss man die konkreten und wesentlichen Anforderungen an die IT-Sicherheit und die Usability einzeln ermitteln und klare Grenzwerte, z.B. Fehlerraten, definieren, die nicht unterschritten werden dürfen. So hat man voraussichtlich einen Bereich definiert, innerhalb dessen man sich bewegen kann und die Usability einer Technologie und ihre IT-Sicherheit in Abwägung zueinander optimieren kann. Die Grenzwerte, also die wesentlichen Anforderungen an IT-Sicherheit und Usability dürfen dabei nicht über- oder unterschritten werden. Wenn es nicht möglich ist, eine Technologie ohne Verletzung dieser wesentlichen Anforderungen einzusetzen, so ist dies der klare Hinweis darauf, dass diese Technologie für die Aufgabe nicht geeignet ist und dass alternative Lösungen gefunden werden müssen.

Eine Methodik für die Auflösung des Zielkonflikts zwischen IT-Sicherheit und Usability wird hinsichtlich biometrischer Anwendungen in PDTR 29156 „Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics“ vorgestellt.

Diese Methodik sollte für den Einsatz anderer Technologien übernommen oder angepasst werden, so dass Entwicklern ein Leitfaden an die Hand gegeben wird, nutzbare Technologien zu entwickeln ohne die IT-Sicherheit zu gefährden und umgekehrt.

5 Schwerpunktgebiete

5.1 Datenschutz

5.1.1 Themenbeschreibung

Datenschutz, im Englischen oft mit „Privacy“ übersetzt dient dem Schutz von Bürgern und Verbrauchern sowie der Gesellschaft als Ganzes vor einer die Privatsphäre oder die gesellschaftliche Teilhabe bedrohenden Verarbeitung ihrer Daten. Welche Art von Datenverarbeitung bedrohlich ist, hängt insbesondere auch vom jeweiligen Kontext ab in dem die Datenverarbeitung vorgenommen wird. Dieser Komplexität Rechnung tragend sind einige Prinzipien, etwa „Privacy by Design“ oder Datensparsamkeit bereits in Normen verankert.

IT-Sicherheit und Datenschutz sind eng miteinander verwoben. So ist IT-Sicherheit einerseits, etwa in Form von Verschlüsselung oder Zugriffskontrolle, eine Voraussetzung für Datenschutz in IT-Systemen, andererseits werfen manche IT-Sicherheitsmaßnahmen, vor allem die Protokollierung, erhebliche Datenschutzprobleme auf. Die Normung im Bereich des Datenschutzes wird auch als Instrument zur Konkretisierung und technische Umsetzung von gesetzlichen Anforderungen herangezogen. So gibt es bspw. Normen zum Löschen von Daten oder Vernichten von Datenträgern, die Lösungen anbieten, wie gesetzliche Forderungen zur Datenlöschung nach Wegfall des Erhebungszweckes sicher und wirtschaftlich umgesetzt werden können.

Im Jahr 2013 wurde von der EU-Kommission das Normungsmandat M/530 „Privacy management in the design and development and in the production and service provision processes of security technologies” den Lenkungsgremien von CEN und CENELEC vorgelegt. Das Mandat wurde angenommen und daraufhin die Gründung einer Joint Working Group von CEN und CENELEC beschlossen. Diese JWG hat ihre Arbeit im Januar 2015 aufgenommen. Mittlerweile hat DIN das Sekretariat dieser JWG übernommen und die JWG wurde in ein CEN/CENELEC TC umgewandelt. Eine Mitarbeit in diesem TC 8 ist über das nationale Spiegelgremium, dem NA 043-01-27-05 AK im Normenausschuss Informationstechnik und Anwendungen möglich.

5.1.2 aktive Standardisierungsgremien

Im Bereich des Datenschutzes arbeiten verschiedene Gremien und Organisationen an Normen und Standards. Oftmals handelt es sich dabei nicht um generische, sondern um technik-, branchen- oder domänenspezifische Datenschutzstandardisierung. Die bedeutendsten Gremien sind nachfolgend aufgeführt.

Organisation	Gremien-bezeichnung	Gremientitel	Arbeitsgebiet
ISO/IEC	JTC 1/SC 27/WG 5	„Identity Management and Privacy Technologies“	Normung generischer Datenschutztechnologien
CEN	CEN /TC 225	AIDC Technologies	Normung zu RFID, Privacy Impact Assesmment im Bereich RFID
CEN/CENELEC	CEN/CLC/ TC 8	Privacy management in products and services	Normung zu Datenschutzmanagement

Organisation	Gremien-bezeichnung	Gremientitel	Arbeitsgebiet
DIN	NA 043-01-27-05AK	Datenschutztechnologien und Identitätsmanagement	Normung generischer Datenschutztechnologien, Spiegelung der JTC 1/SC 27/WG 5 und CEN/CLC/ JWG 8
DIN	NA 043-01-51 AA	Vernichtung von Datenträgern	Normen zum sicheren Vernichten von Datenträgern
ISO	ISO /TC215	Health Informatics	Medizinische Informatik, Datenschutz im Medizinbereich

5.1.3 Derzeitige Landschaft (Status quo in Bezug auf IT-Sicherheit)

Die Bedeutung und die Herausforderungen des Datenschutzes bei informationsverarbeitenden Systemen wurden erkannt und haben ihren Widerhall in der Normung gefunden. Die Normung im Bereich des Datenschutzes kann grob in drei Teilbereiche untergliedert werden:

- **Rahmenwerke und Architekturen**
- **Schutzkonzepte**
- **Leitfäden zum Inhalt und Bewertung**

Das typische Problem im Spannungsfeld zwischen Datenschutz und Sicherheit ist, dass ein mehr an Sicherheit zwar helfen kann den Zugriff auf Ressourcen, etwa sensitive Daten, zu schützen, um dieses jedoch gewährleisten zu können geht zumeist aber auch einher, dass mehr Daten erfasst werden. Diese Datensammlung kann jedoch dann wiederum ihrerseits ein Datenschutzproblem darstellen. Beispiele für diese Problematik ist die Protokollierung von Zugriffen auf zu schützende Datenbestände. Die Protokollierung kann zwar bei der Kontrolle des Zugriffs auf sensitive Daten helfen, bietet aber ihrerseits die Möglichkeit, die Bewegungen der Akteure detailliert nachzuverfolgen. Dies versetzt protokollierende Stellen in die Lage, ein genaues Persönlichkeitsprofil des Betroffenen zu erstellen bzw. zu nutzen, um den Betroffenen zu überwachen. Aus diesem Grund gilt es auch bei den Standardisierungsbestrebungen, die Interessen des Betroffenen nach „Datenschutz“ und die Interessen der verantwortlichen Stelle nach „Sicherheit“ zu harmonisieren.

5.1.4 Handlungsbedarfe (Normungsbedarfe)

Neben der Grundlagennormung zum Datenschutz besteht nach wie vor großer Normungsbedarf bei Verfahren und Techniken im Sinne von „Best Practices“ zur Umsetzung von gesetzlichen Vorgaben. Insbesondere vor dem Hintergrund der neuen EU-Datenschutzgrundverordnung werden weitere Normungsaufträge der EU-Kommission erwartet, um die EU DSGVO mit Normen zu untermauern. Solche Normen schaffen Vertrauen in gesetzeskonforme Produkte, Dienstleistungen und Services und Rechtssicherheit für Unternehmen, wenn sie entsprechende Anerkennung von den jeweils zuständigen Aufsichtsbehörden erfahren. Identifizierte Themenbereiche, in denen ein Bedarf an Normen zur Umsetzung gesetzlicher Vorgaben gesehen wird sind nachfolgend aufgeführt:

- Dokumentation zu Produkten/Dienstleistungen bezüglich gespeicherter personenbezogener Daten
- technische Verfahren zur Ausübung von Betroffenenrechte (Auskunftsrechte, Löschung, Widerspruch)
- Privacy by Design
- datensparsame Technologien

Einige Themenbereiche, die in der Vorgängerversion der Roadmap aufgeführt wurden sind mittlerweile in Normen verankert, bzw. sind Normen in Entwicklung, die das Thema adressieren. Dies sind im Folgenden:

- Datenverarbeitung im Auftrag
  - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- technische Umsetzung von Einwilligung/Widerruf der Einwilligung
  - ISO/IEC 29184 Guidelines for online privacy notices and consent (in Entwicklung)
- technische Umsetzung von Anonymisierung/Pseudonymisierung
  - EN ISO 25237 Medizinische Informatik – Pseudonymisierung (in Überarbeitung)
- organisatorische Vorkehrungen und Prozesse für ein geordnetes Löschen von Daten
  - DIN 66398 Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten

Die EU Datenschutz-Grundverordnung wurde am 14. April 2016 vom EU-Parlament beschlossen und ersetzt die aus dem Jahr 1995 stammende Datenschutzrichtlinie. Angewandt werden die in ihr enthaltenen gesetzlichen Regelungen ab dem 25. Mai 2018. Die Untermauerung und Konkretisierung der Datenschutzgrundverordnung durch Normen, generisch wie branchen- und sektorspezifisch, wird eine der zentralen Herausforderungen der nächsten Jahre für die Normung auf europäischer Ebene.

5.2 Energieversorgung und -erzeugung

5.2.1 Themenbeschreibung

Die aktuellen gesetzlichen Anforderungen an den sicheren Netzbetrieb aus Sicht der Informationssicherheit, in Form des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) und des IT-Sicherheitskatalogs zum Energiewirtschaftsgesetz (EnWG) §11 Abs. 1a bestätigen die Notwendigkeit der Schaffung eines nachweislich hohen Informationssicherheitsniveaus. Dies zeigt die Notwendigkeit und Nachhaltigkeit der Arbeiten der VDE und DKE Fachgruppen und Gremien zur Standardisierung. Die in diesem Abschnitt beschriebenen Komitees und deren Ergebnisse tragen einen wesentlichen Teil zur Verbesserung des Informationssicherheitsniveaus im Sektor der Energieversorgung bei.

Die IKT-basierte Vernetzung der Komponenten des elektrischen Energienetzes ist eine Voraussetzung für die zukünftige Steuerung und die Beherrschung des Netzes. Im zukünftigen intelligenten Energienetz werden unterschiedliche Segmente bzw. Domänen einschließlich der Endgeräte in Wirtschaft und Haushalt betrachtet. Dazu zählen:

- Energiemanagement
- Smart Meter
- Messstellenbetrieb
- Verteilnetze
- Übertragungsnetze
- Kommunikationsnetze
- Energie-Erzeuger
- Speicher
- Aggregatoren
- Elektromobilität
- Energie-Marktplätze
- zusätzliche Services („Mehrwertdienste“)

5.2.2 Energieversorgung (Smart Grid)

5.2.2.1 aktive Standardisierungsgremien

Auf nationaler Ebene hat sich dabei seit mehr als drei Jahren das DKE-Kompetenzzentrum und der Lenkungskreis mit seinen Fokusgruppen als feste Größe etabliert. Ziel ist die Koordinierung der Normungsthemen im Sektor der Energieversorgung, wie dem Smart Grid in Zusammenarbeit mit den technischen Gremien der DKE und des DIN und verschiedenen Interessenkreisen unter Einbindung der E-Energy-Projekte. Dies schließt somit nicht nur etablierte Normungsgremien ein, sondern auch Verbände, staatliche Institutionen und Gremien der VDE-Fachgesellschaften mit Bezug zu Energieversorgung und Smart Grid. Darüber hinaus begleitet und beobachtet das DKE-Kompetenzzentrum europäische (z.B. CEN/CENELEC) und internationale (IEC) Normungsaktivitäten zum Smart Grid. Einen besonderen Schwerpunkt der Arbeiten des Lenkungskreises bildet dabei die die Energiewende und die Integration der erneuerbaren Energien. Die nachfolgende Tabelle zeigt im Überblick die unterschiedlichen Aktivitäten, die sich bis in die Normungsgremien ziehen, u.a. K261 „Systemaspekte der Stromversorgung und K952 „Netzleittechnik“. Besonders bei diesen Gremien wird der Paradigmenwechsel deutlich: wurden in den letzten Jahren bewährte Produkte und Systeme genormt, findet nun die Normung statt bevor Produkte überhaupt erhältlich sind.

Komitee / Thema	Status / Aktivitäten/ Planungen
K901 „System Komitee Smart Energy“	• Koordinierung der Smart Grid-Normungsaktivitäten in Deutschland, Europa (z.B. CEN/CENELEC) und internationaler Ebene (z.B. IEC) • Gründung einer Task Force „HAN-CLS Schnittstelle“ der die Normungsaktivitäten zwischen den DKE Normungsgremien K716, K952, K461, K261 und dem FNN abstimmt • Begleitung des Abschlussberichtes der M/490 Smart Grid Coordination Group • Mitarbeit bei BSI Task Forces • Mitarbeit bei der BMWi AG „Intelligente Netze und Zähler“ Spiegel zu IEC System Committee „Smart Energy“

Komitee / Thema	Status / Aktivitäten/ Planungen
K901.0.1 „Netzintegration, Lastmanagement und dezentrale Energieerzeugung“	• Weiterentwicklung der Use Cases „DER Integration“ mit AK952.0.17. Die erstellten Use Cases wurden erweitert um das Flexibilitätskonzept und Ampelmodell abzubilden
AK901.0.2 „Smart Home und Metering“	• Unterstützung der Arbeiten zur Definition der Datenmodelle, welche auf der HAN/CLS Schnittstelle des Smart Meter Gateways ausgetauscht werden • Zusammenarbeit mit DKE AK 716.0.1 Informationssicherheit im Smart Home und Building
AK901.0.11 „Smart Grid Informationssicherheit“	• Spiegelung der WG SG-IS und der vier Untergruppen • Link zu DKE/K GAK 952.0.15 • Security in der Elektromobilität und in der „Industrial Area“ • Gründung des „IT-Sicherheit in der Elektromobilität, Schwerpunkt IT Security im Bereich der Ladesäule“ (AK 901.0.115)
K261 „Systemaspekte der Stromversorgung“	• Weiterentwicklung der Use Case Methodik • Micro Grids: Planung, Leitung • Demand Side Energy Resources Interconnection with the Grid • Systemaspekte von el. Speichern • Systemaspekte von DER (Distributed Energy Ressources) Großanlagen
K 952 „Netzleittechnik“	• Prüfung der IEC 61850 aus Sicht der Anwender und verstärktem Schwerpunkt auf USe Cases • IEC 61850, Ed. 2 zu 99 % abgeschlossen, Vorbereitungen zur Ed. 2.1 wurden gestartet • Harmonisierung 61850-CIM wird verstärkt vorangetrieben im AK 952.0.14 „operative Netzführung“ • IT-Security im Smart Grid: Datensicherheit bei XML, Cyber Security Key Management
DKE GAK 952.0.15	• Spiegelgremium zu IEC TC 57 WG15 • Bearbeitung der IEC 62351 • Erarbeitung von Anwendungshinweisen • Begleitung des ISMS-Standards TR ISO/IEC 27019 • Unterstützung und Bewertung europäischer und internationaler Aktivitäten, zum Beispiel der Aktivitäten der SGIS • Kooperation und Abstimmung mit anderen Normungsarbeitskreisen, wie zum Beispiel DKE UK 931.1 und anderen
K 461 „Messeinrichtungen und -systeme für Elektrizität“	• AK 461.0142 Datenmodelle für das Smart Meter Gateway • Verfolgung der BMWi „Netze und Zähler“ insbesondere der Gruppe „KNA Smart Meter“
FNN	• Messystem 2020 • FNN Hinweise zur Anwendung der IEC 61850 (Steuerbox) • FNN Hinweise zu Speichern

5.2.2.2 Derzeitige Normungslandschaft

5.2.2.2.1 EU Mandat M/490 und Folgeaktivitäten

Innerhalb der Arbeiten zum EU-Mandat M/490, dessen 2. Phase Ende des des Jahres 2014 abgelaufen ist spielte Informationssicherheit eine zentrale Rolle. Die „Smart Grid Information Security (SGIS)“ Gruppe beschrieb in ihrem Abschlußbericht, wie Security Standards dazu beitragen ein dediziertes Sicherheitsniveau auf technischer, organisatorischer und prozesstechnischer Ebene im Smart Grid zu erreichen. Als Folgeorganisation hat sich im Januar 2015 die Smart Energy Grid Coordination Group (SEG-CG) gegründet, die Teile der Aktivitäten weiterführt. Darunter das Thema Informationssicherheit in der Untergruppe CyberSecurity and Privacy (CSP).

Hierbei spielen die Anwendung des „Smart Grid Architecture Models (SGAM)“ [*SG-CG/M490/H_Smart Grid Information Security 12/2014]*, die definierten SGIS-Sicherheitslevel und ausgewählte Use Cases die zentrale Rolle, um die unterschiedlichen Sicherheitsanforderungen je SGAM-Domäne / -Zone definieren zu können. Durch Abbildung der betrachteten Security Standards auf das SGAM kann deren Anwendbarkeit identifiziert und System-Designern und –Integratoren geholfen werden, die passenden Standards zur Absicherung ihrer Smart Grid Lösung auszuwählen.

SGIS-Security Level

Die SGIS-Security Level wurden bereits in der ersten Phase des Mandates definiert, um eine Verbindung zwischen Energieversorgungsnetz und Informationssicherheit zu etablieren. Dabei liegt die Stabilität des gesamten europäischen Energieversorgungsnetzes als Basis zugrunde. Die folgende Abbildung zeigt die Zuordnung der Security Level zu Beispielszenarios.

Security Level	Security Level Name	Europeans Grid Stability Scenario Security Level Examples
5	Highly Critical	Assets whose disruption could lead to a power loss above 10 GW Pan European Incident
4	Critical	Assets whose disruption could lead to a power loss from above 1 GW to 10 GW European / Country Incident
3	High	Assets whose disruption could lead to a power loss from above 100 MW to 1 GW Country / Regional Incident
2	Medium	Assets whose disruption could lead to a power loss from 1 MW to 100 MW Regional / Town Incident
1	Low	Assets whose disruption could lead to a power loss under 1 MW Town / Neighborhood Incident

Abbildung 4: SGIS Security level

(Quelle: *[SG-CG/M490/H_Smart Grid Information Security 12/2014])*

Use Cases

Zur Veranschaulichung des Umgangs mit IT-Security in den diversen Domänen werden im SGIS Report vier repräsentative Use Cases ausgewählt und analysiert *[SG-CG/M490/H_Smart Grid*

Information Security 12/2014]. In der Folgeaktivität der SEG-CG/CSP wurde darüber hinaus das Thema dezentrale Energieressourcen und die sichere Unterstation bzgl. der Sicherheit analysiert. Zusätzlich zu den SGIS Security Leveln wurden hier auch die Security Level der IEC 62443 berücksichtigt.

Smart Grid Security Standards

Während in der ersten Phase des Mandates M/490 hauptsächlich Standards für die Smart Grid Kernelemente im Fokus standen, befasst man sich im zweiten Teil mit ausgewählten Standards die auch Bezug zu Nachbardomänen des Smart Grid haben, wie beispielsweise zur Industrieautomation. Zudem werden Standards von ISO, IEC und IETF untersucht, die sich mit der Implementierung von Security Maßnahmen befassen. Auch in der SEG-CG/CSP wird dieser breite Scope beibehalten.

Die betrachteten Standards werden von der SGIS in „Requirement Standards“ und „Solution Standards“ unterteilt und sind in der folgenden Aufzählung genannt:

Requirement standards (beschreiben “Was” gesichert werden muss):

- ISO/IEC 15408 Information technology — Security techniques — Evaluation Criteria for IT 361 security
- ISO/IEC 18045 Information technology — Security techniques — Methodology for IT Security 363 Evaluation
- ISO/IEC 19790 Information technology — Security techniques — Security requirements for cryptographic modules
- ISO/IEC TR 27019 Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
- IEC 62443-2-4 Security for industrial automation and control systems - Network and system security - Part 2-4: Requirements for Industrial Automation Control Systems (IACS) solution suppliers
- IEC 62443-3-3 Security for industrial automation and control systems, Part 3-3: System security requirements and security levels
- IEC 62443-4-2 Security for industrial automation and control systems, Part 4-2: Technical Security Requirements for IACS Components
- IEC 62443-2-1 Security for industrial automation and control systems - Network and system security - Part 2-1: Industrial automation and control system security management system
- IEEE 1686 Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities
- IEEE C37.240 Cyber Security Requirements for Substation Automation, Protection and Control Systems

Solution Standards (beschreiben “Wie” Sicherheit erreicht wird):

- ISO /IEC 15118-2 Road vehicles – Vehicle-to-Grid Communication Interface, Part 2: Technical protocol description and Open Systems Interconnections (OSI) layer requirements

- IEC 62351-x Power systems management and associated information exchange – Data and communication security
- IEC 62056-5-3 DLMS/COSEM Security
- IETF RFC 6960 Online Certificate Status Protocol
- IETF RFC 7252: CoAP Constrained Application Protocol
- IETF draft-weis-gdoi-iec62351-9: IEC 62351 Security Protocol support for the Group Domain of Interpretation (GDOI)
- IETF RFC 7030: Enrollment over Secure Transport
- ISO /IEC 15118: Road vehicles – Vehicle-to-Grid Communication Interface, Part 8 [20]: Physical and data link layer requirements for wireless communication
- ISO / IEC 61850-8-2 [21]: Communication networks and systems for power utility automation - Part 8-2: Specific communication service mapping (SCSM) - Mapping to Extensible Messaging Presence Protocol (XMPP)
- IEC 62743 [23] Industrial communication networks – Wireless communication network and communication profiles - ISA 100.11a
- IETF draft-TLS1.3 TLS Version 1.3

Abdeckung des Smart Grid Umfeldes durch Standards

Die aufgeführten Standards werden in die vier Bereiche der Abbildung 3 eingetragen, um einerseits deren Scope, andererseits den jeweiligen Detaillierungsgrad zu veranschaulichen. Weiterhin verdeutlicht die Lage des Standards innerhalb des Diagramms, ob dieser eher Relevanz für Betreiber und Marktteilnehmer („operator“) oder für Hersteller und Dienstleister („products“) besitzt.

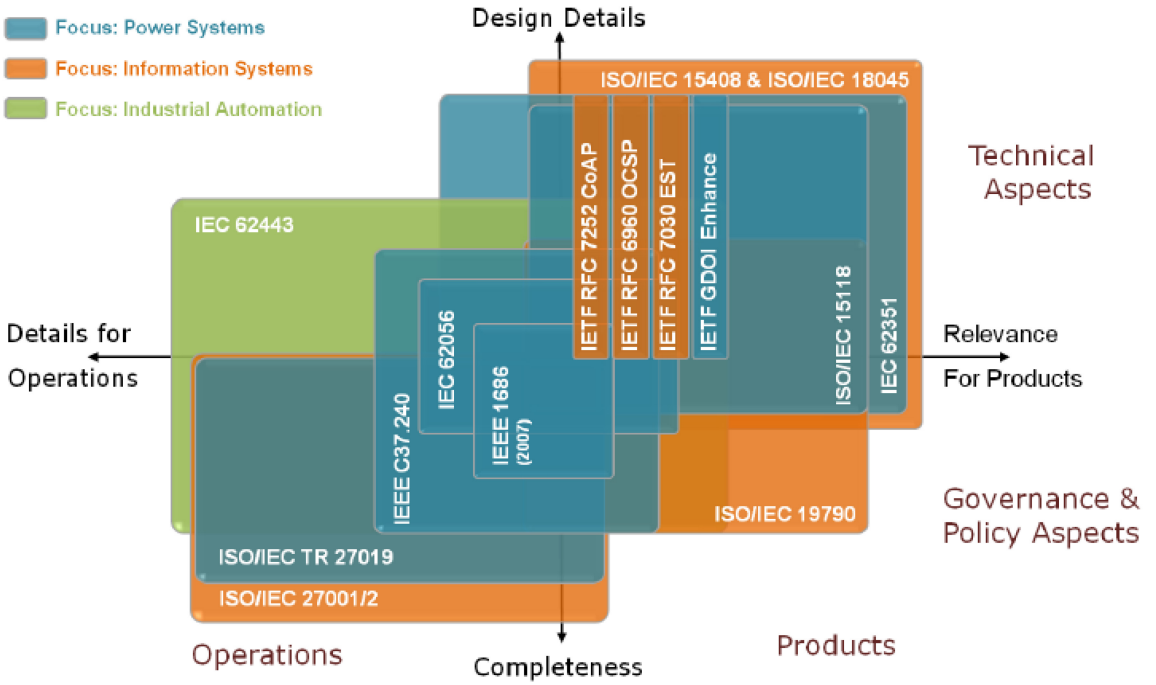


Abbildung 5: Smart Grid Normenlandschaft und deren Kategorisierung

(Quelle: *SEG-CG/CSP Report 12/2016)*

Im Report der SGIS wird auf der beschriebenen Basis eine ausführliche Lückenanalyse der aufgeführten Normen und Standards durchgeführt. Weiterhin findet eine Zuordnung der Standards zu den vier ausgewählten Use Cases statt, um deren praktische Anwendbarkeit zu verifizieren.

5.2.2.2.2 ISO/IEC TR 27019

ISO/IEC 270xx ist ein international anerkanntes Normenwerk zum Thema Informationssicherheitsmanagement (Information Security Management). Organisationen aller Branchen können ihr Informationssicherheitsmanagementsystem (ISMS), also ihre Prozesse und Maßnahmen zur Gewährleistung der Informationssicherheit, nach ISO/IEC 27001 zertifizieren lassen. Die Normen der 27000er-Reihe befassen sich entweder in normativer (d. h. fordernder) oder in informativer (d. h. empfehlender) Weise mit dem Thema Informationssicherheitsmanagement.

Die verschiedenen Dokumente haben dabei unterschiedliche Zielsetzungen und Zielgruppen. Das zentrale Dokument ist die ISO/IEC 27001: Hier werden zum einen die Mindestanforderungen an ein ISMS beschrieben, zum anderen werden in einer tabellarischen Darstellung über 130 Sicherheitsmaßnahmen, die sogenannten „Controls“, beschrieben. Das zweite Hauptdokument, ISO/IEC 27002, enthält Umsetzungshinweise (implementation guidance) für die in ISO/IEC 27001 im Anhang A beschriebenen Controls.

Die ISO/IEC TR 27019 basiert auf ISO/IEC 27002, erweitert diese Norm jedoch um Sektor spezifische Aspekte aus dem Bereich der Energiewirtschaft.

Ziel dieser Sektor spezifischen Erweiterung ist es, den Energieversorgern die Einbindung ihrer Prozesskontroll- (Process Control System, PCS)-systeme und SCADA (Supervisory Control and Data acquisition) in ein ISO/IEC 27000-basiertes ISMS im Unternehmen zu ermöglichen.

Die ISO/IEC TR 27019 wurde von Seiten der deutschen Normungsinstitute DKE und DIN zu einem internationalen Standard entwickelt: Das DKE-Gremium AK 952.0.15 (Spiegelgremium zu IEC TC57/WG15, siehe auch Abschnitt zur IEC 62351) ist verantwortlich für die Informationssicherheit in der Netzleittechnik und initiierte die Aktivitäten in enger Kooperation mit dem DIN-Spiegelgremium zu ISO/IEC JT1/SC 27/WG1 (verantwortlich für die ISO/IEC 27000 Normen). Auch die SGIS-Gruppe aus dem EU-Mandat M/490 unterstützte diese Aktivität massiv und kategorisierte die ISO/IEC TR 27019 als maßgeblichen Lückenschluss in der untersuchten Normungslandschaft ein.

Durch die domänenspezifische Expertise im DKE-Gremium AK 952.0.15 und die Kooperation mit dem BDEW sowie entsprechende Liaisons auf ISO-und IEC-Ebene wird auch für die Zukunft sichergestellt, dass relevante und wichtige Erweiterungen für die PCS-Domäne in die ISO/IEC TR 27019 einfließen werden.

5.2.2.2.3 IEC 62351 Netzführungssysteme und ihr Informationsaustausch – Daten- und Kommunikationssicherheit

Diese Norm wird in nahezu allen internationalen Studien und Untersuchungen als zentraler technischer Standard für die Informationssicherheit in Energienetzen gesehen. Sie wird von der Working Group 15 (WG 15) des Technischen Komitees 57 (TC 57) bei IEC erarbeitet, die seit 1999 die Aufgabe hat, für die vom TC 57 definierten Kommunikationsprotokolle Sicherheitsnormen zu entwickeln. In Deutschland fungiert der „DKE/GAK 952.0.15 DKE-ETG-ITG Informationssicherheit in der Netz- und Stationsleittechnik“ der DKE als nationales, deutsches Spiegelgremium. Dabei wird die

Informationssicherheit als „Ende-zu-Ende-Anforderung“ gesehen, um die Schutzziele in der kritischen Infrastruktur der Netzführungssysteme zu erreichen.

Die adressierte Architektur in diesem Kontext ist in folgender Abbildung gezeigt:

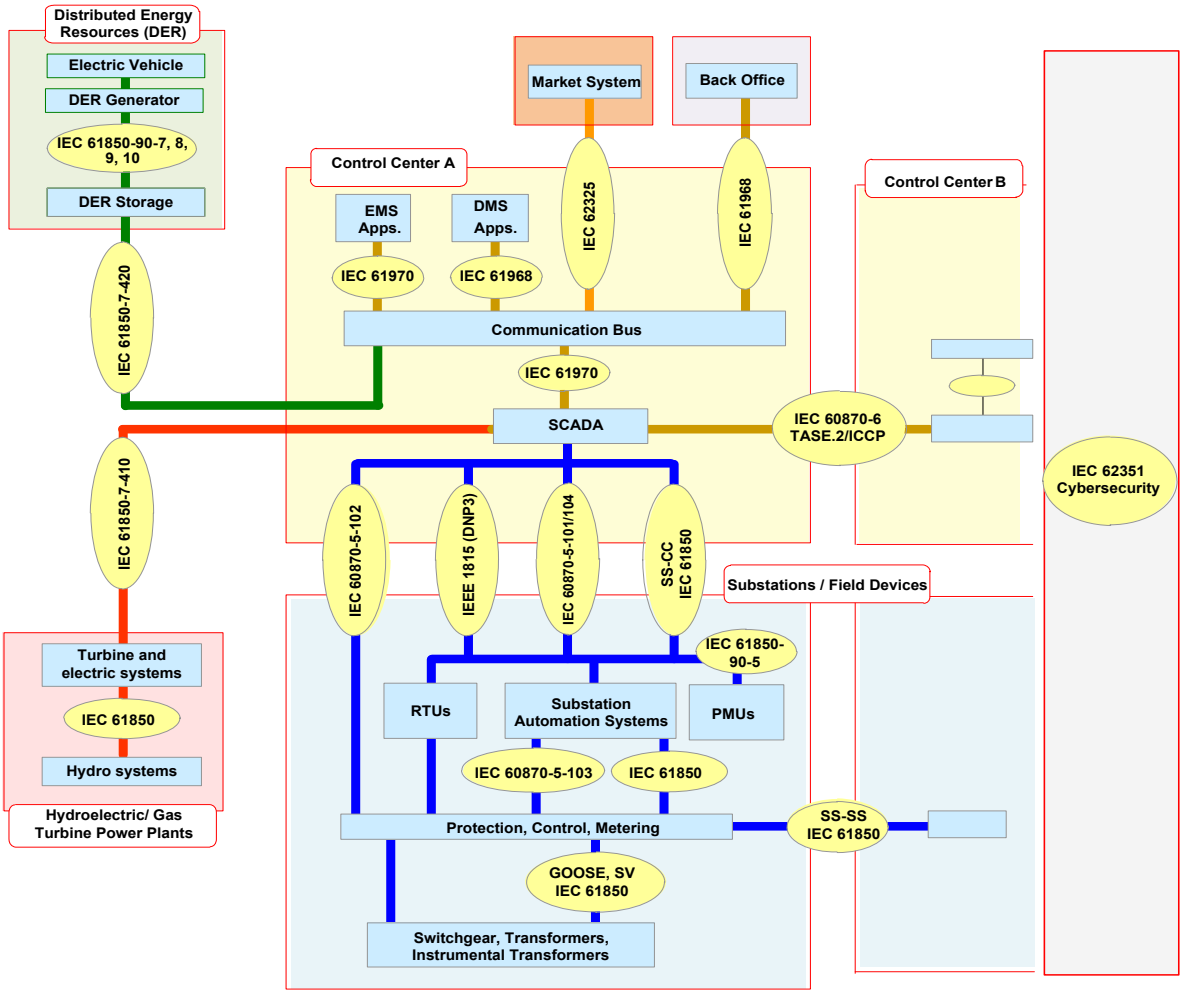


Abbildung 6: IEC TC 57 Architektur von Kommunikationsstandards [Quelle: IEC 62351-10]

Folgende Kommunikationsprotokolle sind bisher durch die diversen Teile der IEC 62351 abgedeckt:

- IEC 62351-3: Informationssicherheit – Profile basierend auf TCP/IP:
- IEC 60870-6 (TASE.2 / ICCP)
- IEC 60870-5 Teil 104
- IEEE 1815 (DNP3) über TCP/IP
- IEC 61850 über TCP/IP
- IEC 62351-4: Informationssicherheit – Profile basierend auf MMS (Manufacturing Message Specification):
- IEC 60870-6 (TASE.2 / ICCP)
- IEC 61850 unter Anwendung des MMS-Profils
- IEC 62351-5: Informationssicherheit – Sicherheit für IEC 60870-5 und Derivate:

- IEC 60870-5, alle Teile
- IEC 61850 unter Anwendung des MMS-Profils
- IEEE 1815 (DNP3)
- IEC 62351-6: Informationssicherheit – Sicherheit für IEC 61850 Peer-to-Peer-Profile:
- IEC 61850 Profile, die nicht auf TCP/IP basieren: GOOSE und SV
- IEC 62351-7: Informationssicherheit – Sicherheit für Netzwerkmanagement:
- Definition einer MIB
- Transport über gesichertes SNMP
- IEC 62351-9: Informationssicherheit – Key Management:
- Definition von Profilen für Zertifikatsmanagementprotokolle
- IEC 62351-14: Informationssicherheit – Sicherheit für Event Logging:
- Definition von Sicherheitsrelevanten Events
- Transport über gesichertes syslog

Die Abbildung 7 zeigt die geschilderten Zusammenhänge.

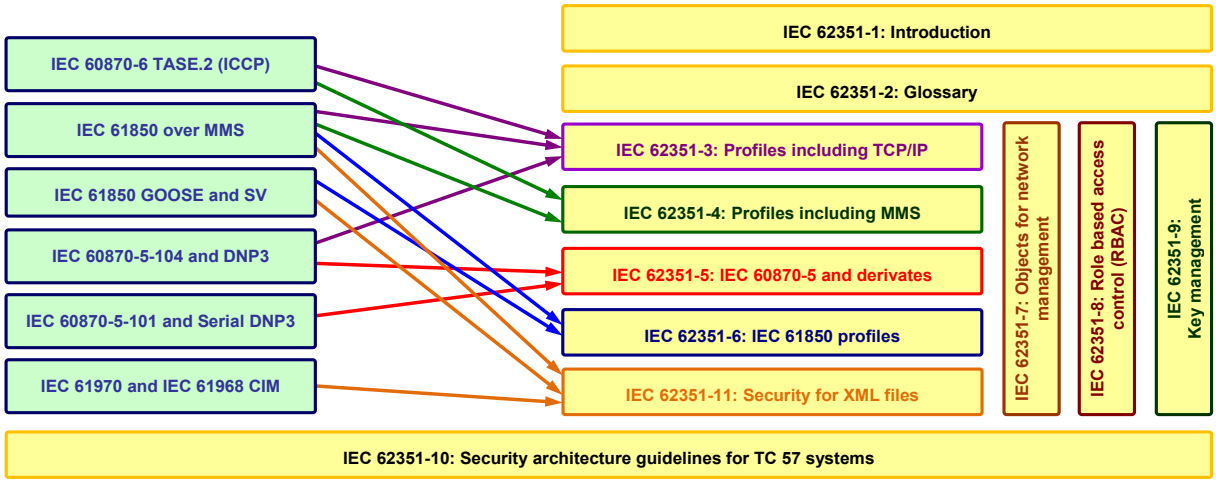


Abbildung 7: IEC TC 57 Kommunikationsstandards und ihre Relation zu den Teilen der IEC 62351 [Quelle: IEC]

Im Folgenden werden die einzelnen Teile der Normenreihe kurz inhaltlich vorgestellt und ein Ausblick auf die potenzielle Weiterentwicklung gegeben. Die Mehrzahl der Teile der IEC 62351 Reihe ist als technische Spezifikation erarbeitet worden. Derzeit läuft eine Überarbeitung von dedizierten Teilen in Richtung „International Standard“.

IEC 62351-1: Einführung

Dieser Teil der Norm liefert einen Überblick und Hintergrundinformationen zum Thema Informationssicherheit in der Energiedomäne und den dort geltenden Besonderheiten. Zudem werden die relevanten Schutzziele (Confidentiality – Integrity – Availability – Non-Repudiation) und

entsprechende Maßnahmen grob vorgestellt, um sich gegen bestimmte Bedrohungen zu schützen, wie in der folgenden Abbildung skizziert:

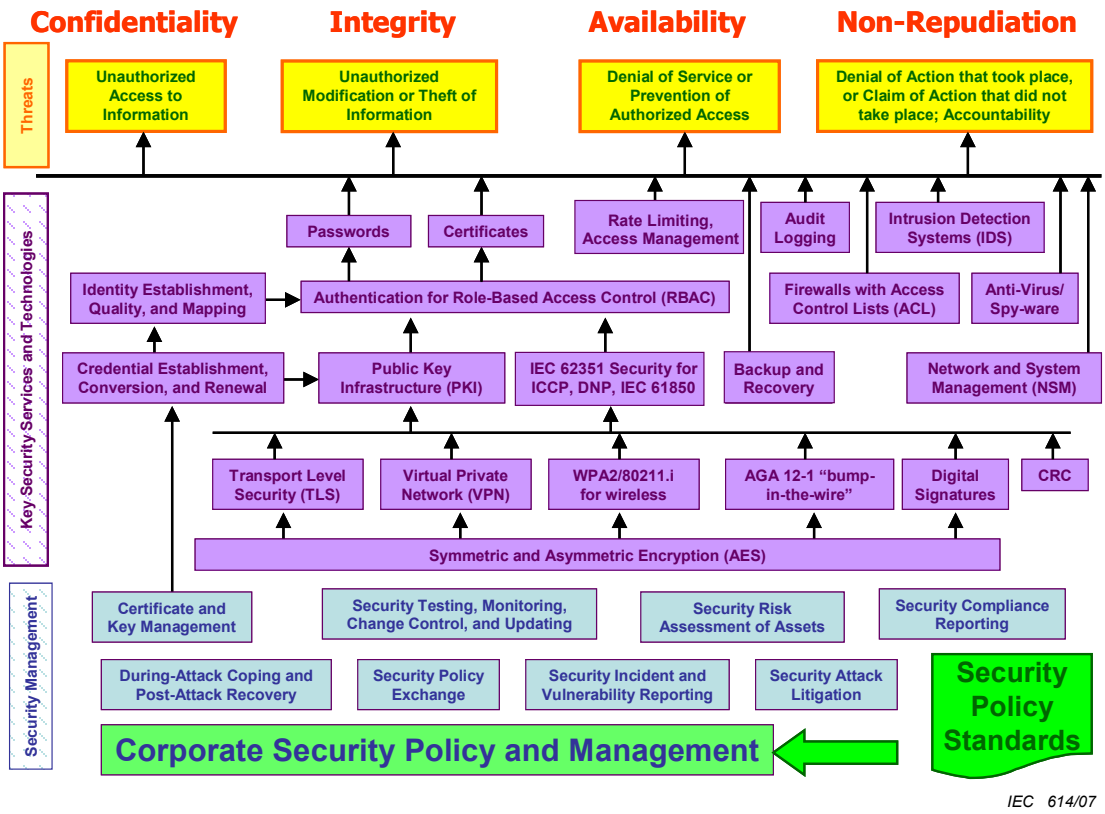


Abbildung 8: Sicherheitsanforderungen, Bedrohungen, Gegenmaßnahmen und Management [Quelle: IEC 62351-1]

IEC 62351-2: Glossar

Dieser Teil der Norm ist frei verfügbar und enthält sämtliche Begriffe und Abkürzungen der gesamten Normenreihe.

IEC 62351-3: Informationssicherheit – Profile basierend auf TCP/IP

Teil 3 der Norm beschäftigt sich mit TCP/IP-basierenden Protokollen der Netzleittechnik. Dafür wird zur Erreichung von Authentisierung, Vertraulichkeit und Integrität der Einsatz von Transport Layer Security (TLS) spezifiziert: Zum Beispiel werden optionale TLS-Bestandteile verbindlich vorgeschrieben und spezielle Anforderungen der Netzleittechnik an die zu nutzenden Zertifikate spezifiziert. Dieser Teil wurde 2014 als IS verabschiedet und beinhaltet nun weitere Funktionalitäten von TLS und eine Aktualisierung der verwendeten Cipher Suites.

IEC 62351-4: Informationssicherheit – Profile basierend auf MMS

Im vierten Teil werden die Sicherheitserweiterungen für Protokolle definiert, die MMS (Manufacturing Message Specification, ISO 9506) einsetzen. MMS wird für Messaging-Systeme mit Echtzeitanforderungen in der Netzleittechnik eingesetzt. Teil 4 definiert dazu TLS-basierte Prozeduren auf der Transport- und Applikationsschicht basierend auf dem Profil aus Teil 3. Derzeit laufen die Arbeiten zum IS, der neben einer Aktualisierung zur Nutzung des neuen IEC 62351-3 auch eine Erweiterung des A-Profils enthält. Diese Erweiterung wird in Form zweier neuer A-Profile beschrieben, deren Anwendung neben klassischem MMS (IEC 61850-8-1) auch die Anwendung über XMPP (IEC 61850-8-2) abdeckt und eine sichere Ende-zu-Ende Beziehung ermöglicht..

IEC 62351-5: Informationssicherheit – Sicherheit für IEC 60870-5 und Derivate

Teil 5 der Normenreihe berücksichtigt die Besonderheiten serieller Kommunikation. Dazu werden Sicherheitsmaßnahmen definiert, um die Integrität von seriellen Verbindungen zu gewährleisten, die einen Keyed-Hash Message Authentication Code (HMAC) verwenden. Weiterhin soll im Teil 5 ein separates Schlüsselmanagement spezifiziert werden, dessen exakte Mechanismen noch in der Diskussion sind. Hierzu ist ein Abgleich mit IEC 62351-9 geplant, um die dort definierten Mechanismen zum Zertifikatsmanagement direkt nutzen zu können.

IEC 62351-6: Informationssicherheit für IEC 61850 Peer-to-Peer-Profile

Die IEC 61850 Norm spezifiziert drei Peer-to-Peer-Multicast-Protokolle, die im LAN einer Trafostation nicht zu routen sind. Prominentester Vertreter ist das GOOSE (Generic Object Orientated Substation Events) Protokoll, das für gesicherte Nachrichtenübermittlung innerhalb von 4 ms zwischen intelligenten Controllern konzipiert wurde. Unter solch harten Echtzeitbedingungen lassen sich nur begrenzte Sicherheitsmaßnahmen umsetzen, da diese einen signifikanten Effekt auf die Verarbeitung haben. Im Teil 6 sind derzeit digitale Signaturen für den Schutz der Multicast-Nachrichten definiert, die sich jedoch mit der feldgerätetypischen Hardware schlecht bis gar nicht umsetzen lassen. Eine alternative Lösung, die anstelle einer gerätespezifischen digitalen Signatur auf die Anwendung eines Gruppenschlüssels zum Errechnen eines Integritätswertes setzt, wurde im technischen Report IEC 61850-90-5 erarbeitet. Dieser Ansatz fließt nun sukzessive in die weitere Bearbeitung der verschiedenen IEC 62351 Teile mit ein. Konkret fließt das Key Management für den Gruppenschlüssel in den Teil IEC 62351-9 mit ein. Der Teil 6 beschreibt dann im Wesentlichen die Anwendung des Gruppenschlüssels auf Nachrichtenebene für GOOSE und SV. Da der Teil 6 eine normative Referenz auf den Teil 4 enthält, erfolgt hier eine parallele Spezifikation beider Teile.

IEC 62351-7: Sicherheit für Netzwerk- und Systemmanagement (NSM) Datenobjektmodelle

Der Fokus im Teil 7 liegt auf dem Netzwerk- und Systemmanagement (NSM) der Informationsinfrastruktur der Energiesysteme. Hierzu hat die WG 15 abstrakte NSM-Datenobjekte für die Kontrolle und Überwachung des Netzwerks sowie angeschlossener Geräte definiert, um zu reflektieren, welche Informationen in einer Leitstelle notwendig sind, um die Informationsinfrastruktur ebenso zuverlässig zu managen wie die Systeme der Energieinfrastruktur. Auf diesen Informationen können typische Managementprotokolle wie SNMP aufsetzen. Durch die Überwachung des Netzwerks sollen Angriffe erkannt und frühzeitige Reaktionen hierauf ermöglicht werden. Derzeit wird dieser Teil auf einen IS aktualisiert. In diesem Kontext sind umfangreiche Änderungen und Erweiterungen an der Definition der Management Information Base (MIB) gemacht worden, um die Zustände dediziert aufnehmen und reporten zu können. Darüber hinaus wurde ein Mapping auf SNMP durchgeführt. SNMP selbst wird in der Version 3 unter Berücksichtigung des User Security Models (USM) verwendet.

IEC 62351-8: Rollenbasierte Zugriffskontrolle für Leitsysteme

Zentrales Thema im Teil 8 der IEC 62351 ist der rollenbasierte Zugangskontrollmechanismus (Role Bases Access Control, RBAC) und dessen Integration in der gesamten Domäne der Energieversorgung. Dies ist unumgänglich, da in Schutzsystemen und Leitwarten Autorisierung und Nachverfolgbarkeit gefordert sind, z. B. um bestimmte Schalthandlungen im Energienetz eindeutig nachvollziehen zu können. Teil 8 definiert dabei drei verschiedene Möglichkeiten, die Rolleninformation zu transportieren, und setzt dabei auf die bisher verwendeten Formate wie z. B. X.509 Zertifikate. Das Dokument wird derzeit zu einem IS erweitert. Dabei werden Erkenntnisse aus dem technischen

Report IEC 62351-90-1 (siehe unten) eingearbeitet sowie eine Erweiterung der existierenden Profile für RBAC eingearbeitet.

IEC 62351-9: Schlüsselmanagement

Dieser Teil befindet sich noch in der Entwicklung und legt fest, wie insbesondere digitale Zertifikate und Schlüsselmaterial generiert, verteilt, widerrufen und behandelt werden sollen, um digitale Informationen und Kommunikation sicher zu schützen. Weiterhin ist im Anwendungsbereich des Standards der sichere Umgang mit symmetrischen Schlüsseln (pre-shared- und Session-Schlüssel) adressiert, insbesondere die Verteilung der Gruppenschlüssel im Kontext des aktualisierten Teil IEC 62351-6. Dabei beschreibt Teil 9 neben typischerweise einzusetzenden Protokollen und Technologien für das Key Management auch eine Reihe von Anwendungsfällen, die diese Technologien benutzen.

IEC 62351-10: Sicherheitsarchitektur

Teil 10 beschreibt im Rahmen eines technischen Reports Security-Architektur-Empfehlungen für Systeme der Netzleittechnik, basierend auf grundlegenden Security-Maßnahmen (Komponenten, Funktionen und ihre Interaktion). Dieser Teil der Norm soll unter anderem System-Integratoren dabei unterstützen, Systeme der Energieerzeugung, -übertragung und -verteilung sicher einzusetzen und die verfügbaren Normen anzuwenden. Die folgende Abbildung zeigt die zugrunde liegende Architektur von IEC TC 57, auf deren Basis Security-Maßnahmen aus dem Umfeld der IEC 62351 anzuwenden sind.

IEC 62351-11: Sicherheit für XML Files

Die Nutzung von XML für den Informationsaustausch nimmt im Bereich der Energieautomatisierung immer mehr zu. Ein Beispiel ist die Nutzung von XML im Kontext der IEC 61970 und in Teilen der IEC 61850. Neben den IEC Standards gibt es auch andere Standards wie IEEE 1815 (DNP3) und IEEE C37.111 (COMTRADE), die XML nutzen. Die mittels dieser Standards übermittelte Information kann sensitive informationen enthalten, die geschützte werden müseen. Daher spezifiziert Teil 11 Mechanismen zum Schutz der XML Dokumente während des Transports, insbesondere:

- Definition eines Mechanismus, um das XML-Quellfile zu authentifizieren und insbesondere die Sensitivität der transportierten Daten zu klassifizieren („taggen“). Dies soll dem Verarbeiter der Information dabei helfen, die Daten auch entsprechend der Sensitivität weiterzuverarbeiten. Damit wird nicht nur der Schutz der Daten während der Kommunikation adressiert, sondern darüber hinaus auch die lokale Weiterverarbeitung und Speicherung.
- Definition eines Mechanismus zur Manipulationserkennung
- Definition der Security-Maßnahmen, so dass maximale Kompatibilität mit den gegenwärtigen CIM, SCL und anderen XML Formaten erreicht wird

Darüber hinaus werden Mechanismen empfohlen zur Sicherstellung des Informationsaustausches über verschiedenen teilnehmer mit unterschiedlichen (auch transitiven) Vertrauensbeziehungen, z.B. Operator Avertraut der Entität B; B vertraut A und C und A will Informationen mit C austauschen, aber hat keine Vertrauensbeziehung zu C.

IEC 62351-12: Resilience in Energiesystemen unter Nutzung von DER Systemen

Teil 10 beschreibt im Rahmen eines technischen Reports Empfehlungen zur Resilience die sowohl auf IT Sicherheitsmaßnahmen als auch auf Engineering und operative Strategien aufsetzen, um die Widerstandsfähigkeit gegen Angriffe, Fehler und Naturkatastrophen, insbesondere bei der

Integration von DER zu erhöhen. Adressiert werden die Anforderungen von den potentiell involvierten Teilnehmern (Besitzer, Betreiber, …). In diesem Teil wird unter anderem ein Mapping der Sicherheitsanforderungen auf die Anforderungen zu den Security Level 2 und 3 der IEC 62443 gemacht.

IEC 62351-13: Empfehlungen zur Berücksichtigung der IT Sicherheit bei der Standadisierung

Dieser technische Report adressiert Entwickler von Standards und Spezifikationen und gibt einen Überblick zur Identifikation von Sicherheitsanforderungen, die dann im Standard durch konkrete technische Maßnahmen adressiert werden sollen. Das Dokument versteht sich in diesem Sinne als Checkliste. Es gibt eine Querbeziehung zu einem IEC übergreifenden Gremium, dem Advisory Committee on Security (ACSec), das eine Security Guideline erstellt, indem ebenfalls Empfehlungen gegeben werden, wie das Thema IT Sicherheit in anderen Standards zu berücksichtigen ist.

IEC 62351-14: Cyber Security Event Logging

Ähnlich dem Teil 7 für das Monitoring werden derzeit im Teil 14 technische Anforderungen für das Thema Logging von sicherheitsrelevanten Ereignissen beschrieben. Hierbei wird zum einen die Definition sicherheitsrelevanten Events, deren Semantik und Struktur definiert. Zusätzlich wird ein Mapping auf syslog für den Transport dieser Daten spezifiziert.

IEC 62351-90-1: RBAC Guidelines

Die in der IEC 62351-8 definierten Mechanismen zur Unterstützung von rollenbasierter Zugriffskontrolle definieren schon spezifische Rollen und die zugeordneten Rechte. Teil 8 erlaubt auch die Definition eigener Rollen, spezifiziert aber nicht wie. Der technische Report IEC 62351-90-1 adressiert dies und definiert auf der einen Seite ein Gruppierung von rechten, die eine leichtere Assoziation zu einer neuen Rolle erlaubt. Darüber hinaus wird ein Mechanismus zum Verteilen der Rollen zu Rechte Information mittels XMPP definiert. Hierbei wird von XMPP das Format und die Semantik genutzt, um die Information in interoperabler Weise auszutauschen. Die technischen Ansätze aus diesem Dokument werden im Kontext der IS Erarbeitung zum IEC 62351-8 mit in die Norm eingearbeitet.

IEC 62351-90-2: Deep Packet Inspection

Ein weiterer technischer Report, der derzeit in der Erarbeitung ist, untersucht Möglichkeiten existierende Maßnahmen zur Inspektion von Verkehrsdaten auch im Kontext verschlüsselter Kommunikation weiter nutzen zu können. Hierzu werden Lösungen untersucht und verglichen, die diese Funktionalität ermöglichen.

5.2.2.3 Schlussfolgerungen und Handlungsbedarfe

Die SGIS stellt in ihrem Bericht fest, dass die relevanten Normen, um eine grundlegende Informationssicherheit im Smart Grid zu etablieren, verfügbar sind. Es wird trotzdem auf die Notwendigkeit der kontinuierlichen Erweiterung bestehender Normen hingewiesen, um Smart-Grid-spezifische Anforderungen an die Informationssicherheit und neue Technologien, Architekturen und Use Cases zu integrieren.

Besonderer Augenmerk soll dabei auf die möglichst einfache Anwendbarkeit von Standards und Richtlinien zur Implementierung von IT-Sicherheit im Smart Grid gelegt werden („Usability“).

Die Handlungsbedarfe aufgrund der aufgedeckten Lücken in den Standards und Normen können dem Report der SGIS entnommen werden [*SG-CG/M490/H_Smart Grid Information Security 12/2014]*.

Hinsichtlich der Weiterführung der SGIS Aktivitäten über die Laufzeit des Mandates M/490 hinaus (Ende ist 12/2014) ist europaweit bereits Einigkeit erzielt worden. Insbesondere soll es im Rahmen der Folgeaktivitäten zu einer abgestimmten Kooperation mit US-amerikanischen Organisationen kommen.

5.2.3 Energieerzeugung (Kerntechnik)

Seit August 2013 gilt die SEWD-IT-Richtlinie in Deutschland als Basis für alle Anlagen der Sicherungskategorie I und II und somit für alle Kernkraftwerke.

SEWD-Richtlinie IT: 2013, Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherheitskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter, VS-NfD, Bundesamt für Umwelt, Naturschutz und Reaktorsicherheit

5.2.3.1 aktive Standardisierungsgremien

Organisation	Gremien-bezeichnung	Gremientitel	Arbeitsgebiet
IEC	SC45A	Instrumentation, control and electrical systems of nuclear facilities	elektrische und elektronische Systeme in Nuklearanlagen
CLC	TC45AX	Instrumentation and control of nuclear facilities	Spiegelung zu IEC SC45A
DKE	UK 967.1	Elektro- und Leittechnik für kerntechnische Anlagen	gesamter Lebenszyklus leittechnischen Systeme in kerntechnischen Anlagen

Die “Nuklear” IEC Standards von IEC SC45A berücksichtigen mit höchster Priorität die Vorgaben der IAEA (International Atomic Energy Agency). Bezüglich Informationssicherheit wird bei IAEA die sogenannte Nuclear Security Series (NSS) laufend erweitert und aktualisiert. Zurzeit gültig ist die IAEA NSS No. 17 “Computer Security at Nuclear Facilities” als top-level Technical Guidance. Diese wird durch die NST045 (in der letzten Stufe vor Veröffentlichung) und die NST047 (Veröffentlichung vermutlich Anfang 2018) ersetzt. Zusätzlich beschreibt der Draft IAEA NST036 “Computer Security of Instrumentation and Control Systems at Nuclear Facilities” über 200 spezifische Security Controls.

5.2.3.2 Derzeitige Normungslandschaft

- IEC 62645 Ed.1.0 (2014) “Nuclear Power Plants – Instrumentation and control important to safety – Requirements for security programmes for computer-based systems". Eine Ed. 2.0 ist in Arbeit und ein CD2 (oder CDV) soll bis Oktober 2017 vorliegen. Die neue Ed. 2.0 lehnt sich stark an die ISO/IEC 27001:2013 an – es gibt z.B. eine 1:1 Kapitelzuordnung. Ebenso findet die IEC 62443 ihre Berücksichtigung.
- IEC 62859 Ed.1.0 (2016) “Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity“. Die Verknüpfung von funktionaler oder nuklearer Sicherheit mit IT-Security ist weltweit und sektorübergreifend ein wichtiges Thema und wir haben dazu eine verabschiedete IEC Norm.

- IEC 63096 “Nuclear power plants - Instrumentation and control and electrical systems – Security Controls”. Für diesen Entwurf wird es bis Oktober 2017 einen ersten CD geben, in dem für alle Controls aus der ISO/IEC 27002:2013 mittels einer 1:1 Übersetzung (Überschriften und Nummerierung im Sinne der ISO/IEC 27009:2016 Empfehlungen für Sektor-spezifische Anwendung) kerntechnische Realisierungsanforderungen für die Phasen Entwicklung, Projektierung und Betrieb einschließlich Legacy Systemen, die bei uns eine große Rolle spielen, definiert werden.
- Weitere Standards zum Informationssicherheits-Risikomanagement und zu Modellierung sicherheitsrelevanter Aspekte stehen auf der Agenda.
- IEC 61500 zu „Data communication in systems performing category A functions“ (also für die höchsten funktionalen Sicherheitsanforderungen) verweist bezüglich Informationssicherheit auf die IEC 62645.

Die Mitarbeit an den IEC SC45A Normen erfolgt über das deutsche Spiegelgremium UK 967.1.

Das CLC TC45AX erstellt selbst keine Normen sondern wählt aus den Normen des IEC SC45A diejenigen aus, die unverändert als europäische Normen (EN) übernommen werden könnten. Die Entscheidung erfolgt über das Abstimmungsverfahren bei CENELEC.

5.2.3.3 Schlussfolgerungen und Handlungsbedarfe

Eine enge Kooperation mit IEEE ist gegeben (Personalunion in IEC/IEEE Gremien).

Es besteht eine Liaison zwischen IEC SC45A WG9 und IEC TC65 bezüglich der Synchronisierung mit IEC 62443-x-x Entwicklungen sowie eine Liaison zwischen IEC SC45A WG9 und ISO/IEC JTC1/SC27 WG1 bezüglich ISO/IEC 270xx.

IEC 60880 für Kategorie A Software (höchste Software-Anforderungen) und IEC 62566 „Development of HDL-programmed integrated circuits for systems performing category A functions“ (höchste Anforderungen für Hardware Definition Language / HDL basierte FPGA-Lösungen) werden bei ihrer jeweiligen Überarbeitung auch auf die IEC 62645 Ed 2.0 verweisen, ebenso wie die IEC 62138 für Kategorie B Software während der gerade laufenden Überarbeitung angepasst wird.

5.3 Industrielle Produktion (Industrie 4.0)

5.3.1 Themenbeschreibung

Heutige Produktionsanlagen sind mit steigender Automatisierung durch vernetzte Rechner-, Mess-, Steuer- und Regelsysteme gekennzeichnet. Damit wird in den beteiligten Industrieanlagen nicht nur die vorhandene Office-IT (e.g. SAP, Windows etc.), sondern auch die Produktion zu einem sicherheitskritischen IT-Komplex. Es wachsen Technologiebereiche zusammen, die zuvor weitgehend autark und separiert waren. Hinzu kommt, dass in der Automatisierungstechnik mehr und mehr auf Standard Hard- und Software (COTS) gesetzt wird und als Kommunikationsmittel offene Standards wie TCP/IP in den Mittelpunkt treten. Allerdings lassen sich die bekannten Sicherheitsmechanismen für TCP/IP aus dem Bereich der Office-IT nicht ohne weiteres in den Produktionsbereich übertragen. Daher gilt es bei Industrie 4.0 die nur schwer vorhersehbaren, komplexen Sicherheitsprobleme aufgrund der Wechselwirkung zwischen Office-IT und Produktions-IT (ähnlich wie beim Smart Grid) zu erfassen und neu zu bewerten. Dabei spielen Normen und Standards eine entscheidende Rolle, um neben dem Sicherheitsbedarf in Produktion und Fertigung, die relevanten Bedrohungen zu erkennen, um zielgerichtet wirksame Maßnahmen abzuleiten und um ein strategisches, ganzheitliches, standardisiertes Konzept für die IT-Sicherheit zu erreichen.

Office- und Industrial-Systeme besitzen im Regelfall unterschiedliche Rahmenbedingungen, innerhalb derer die Security funktionieren (z.B. hinsichtlich Langlebigkeit der Anlagen und proprietär basierte Zonenschutzkonzepte). Ein wichtiger Schwerpunkt der IT-Sicherheit ist die Absicherung des Netzwerks und der Kommunikation eines Unternehmens. Die Industrial Security ergänzt die Security der Produkte, Produktionsmittel und Produktionsprozesse. Es umfasst somit die embedded Industrieplattformen und M2M-Kommunikation im Industriebereich.

Die Industrial Security berücksichtigt insbesondere das Schutzziel „Verfügbarkeit“ aller Komponenten. Störungen der Office-Systeme führen i.d.R. zu einer eingeschränkten Wirkung (Mitarbeiter können nicht arbeiten, wenn Mailserver ausfällt). In der Industrie führt ein ausgefallener Rechner i.d.R. zum Stillstand der Produktionsstätte mit hohen Kosten.

Mit Industrie 4.0 rücken neue Themenfelder und insbesondere ein systemorientiertes Vorgehen in den Fokus. Ebenen- und domänenübergreifende Konzepte müssen entwickelt und genormt werden. Hierzu genügt es nicht, eine übergeordnete Ebene zu etablieren, sondern es erfordert ein insgesamt ganzheitliches Vorgehen sowie eine über die normale Arbeit der Gremien hinausgehende Anstrengung, um die Entwicklung effizient durch Spezifikationen und Normen zu unterstützen. Zentrale Elemente, welche die Basis von Industrie 4.0 sein werden sind:

- Automatisierungstechnik
- Funktionale Sicherheit
- Informations- und Kommunikationstechnik (IKT)
- Informationssicherheit

5.3.2 aktive Standardisierungsgremien

Die Entwicklung konsensbasierter Normen wird von den zuständigen Gremien langfristig und nachhaltig vorangetrieben. In Deutschland sind dies insbesondere DKE und DIN, in Europa ETSI, CENELEC, CEN sowie international IEC und ISO. Neben diesen mit Mandat bedachten Normungsgremien beteiligen sich weitere Gremien durch Ausarbeitung von Spezifikationen und Richtlinien am Vereinheitlichungsprozess für Industrie 4.0 und tragen zur Verbreitung der Informationen bei:

Organisation	Gremien-bezeichnung	Gremientitel	Arbeitsgebiet
DIN	NA 043-01-27 AA	IT-Sicherheitsverfahren	Spiegelkomitee zu ISO/IEC JTC 1/SC 27
DKE	DKE/GK 914	Funktionale Sicherheit elektrischer, elektronischer und programmierbarer elektronischer Systeme (E, E, PES) zum Schutz von Personen und Umwelt	Spiegelkomitee zu IEC TC65/SC 65A/WG 14
DKE	UK 931.1	IT-Sicherheit in der Automatisierungstechnik	Spiegelkomitee zu IEC TC65/WG 10
ISO/IEC	JTC 1/SC 27	IT Security Techniques	Generische IT-Sicherheit/ Informationssicherheits-Managementsysteme
IEC	TC65	Industrial-process measurement, control and automation	industrielle Leittechnik
ETSI	TC Cyber	Technical Committee (TC) Cyber SecurityETSI	develop and maintain the Standards, Specifications and other deliverables to support the development and implementation of Cyber Security standardization within ETSI
ISA	ISA 99	Industrial Automation and Control Systems Security	IT-Sicherheit von Produktionssteueranlagen

5.3.3 Derzeitige Landschaft (Status quo in Bezug auf IT-Sicherheit)

Eine wichtige Rolle bei der Beschreibung der Normungslandschaft wird die Normenreihe IEC 62443, wie bereits beschrieben, einnehmen. Inwiefern alle abzudeckenden Bereiche hierbei hinreichend abgedeckt sind, muss zukünftig im Detail noch erarbeitet werden.

Aus der Aufzählung von Normen, Standards und Richtlinien werden im Folgenden einige wichtige Vertreter näher erläutert.

5.3.3.1 IEC 62443 IT-Sicherheit in der Automatisierungstechnik

Eine zentrale Rolle für die IT Sicherheit im Bereich Industrie 4.0 wird die derzeit in der Entwicklung befindliche Normenreihe IEC 62443 einnehmen.

Die Normenreihe IEC 62443 wird von der IEC/TC 65 in enger Kooperation mit der ISA 99 („International Society of Automation“) spezifiziert. Sie befasst sich mit der IT-Sicherheit in der Automatisierungstechnik und schließt kritische Infrastrukturen wie z. B. die Energiedomäne ausdrücklich mit ein. Die Dokumente der ISA 99 werden dabei dem Abstimmungsprozess der IEC unterzogen, wodurch die ISA 99 Dokumente nahezu identisch zur IEC 62443 sind (ausgenommen Teil 4 der IEC 62443).

Die Europäische Normungsorganisation CENELEC hat beschlossen, die Normen der Reihe IEC 62443 zur IT-Sicherheit in industriellen Automatisierungssystemen und kritischen Infrastrukturen künftig zu übernehmen. Das UK 931.1 der DKE "IT-Sicherheit in der Automatisierungstechnik" erwartet daher ab 2015 die Herausgabe von europäischen Normen der Reihe EN 62443 und von deutschen Normen der Reihe DIN EN 62443 (VDE 0802). Diese Normen werden sowohl für das Fachgebiet der Automatisierungstechnik als auch für das der Netzleittechnik und der Leittechnik für weitere kritische Infrastrukturen grundlegenden Charakter haben.

Wie zuvor erwähnt, hat das amerikanische Normungskomitee ISA 99 die meisten Teile dieser Normenreihe vorbereitet. Sie erscheinen dort als ISA 99.xx.yy. So entspricht ISA 99.00.01 der IEC 62443-1-1. Vorgesehen bzw. erschienen sind, entsprechend des obigen Schemas, die folgende Teile:

- IEC 62443-1-1, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models; Bearbeitungsstand: IEC/TS 62443-1-1 ed1.0 (2009-07), Überarbeitung geplant

Im Unterabschnitt 1.2 der IEC 62443-1-1 "Behandelte Funktionalität" wird klargestellt, dass der Anwendungsbereich der Normenreihe IEC 62443 nicht nur Anlagen der industriellen Automatisierungstechnik umfasst, sondern auch solche in kritischen Infrastrukturen, wie z.B. in der elektrischen Energieübertragung und in Gas- und Wassernetzen. (siehe hierzu auch Kapitel 4.2.4) Die sogenannten grundlegenden Anforderungen werden im Unterabschnitt 5.3 IEC 62443-1-1 eingeführt:

a) Zugriffskontrolle (access control AC): den Zugriff auf ausgewählte Geräte, Informationen oder beides regeln, um vor einer nicht autorisierten Abfrage des Gerätes oder der Information zu schützen;

b) Nutzung kontrollieren (use control UC): die Nutzung ausgewählter Geräte, Informationen oder beides überwachen, um vor nicht autorisiertem Betrieb des Gerätes oder unerlaubter Informationsverwendung zu schützen;

c) Datenintegrität (data integrity DI): die Integrität von Daten in ausgewählten Kommunikationskanälen sicherstellen und so vor nicht autorisiertem Datenaustausch schützen;

d) Datenvertraulichkeit (data confidentiality DC): ausgewählte Kommunikationskanäle vor Mithören schützen, um so die Vertraulichkeit besonderer Daten sicherzustellen;

e) eingeschränkter Datenfluss (restricted data flow, RDF): den Datenfluss in Kommunikationskanälen einschränken, um so vor der Weitergabe von Informationen an nicht autorisierte Senken zu schützen;

f) auf Ereignisse schnell reagieren (timely response TRE): auf Verletzungen der IT-Sicherheit durch Benachrichtigung der zuständigen Stellen rechtzeitig reagieren, die notwendige Sicherung von Beweisen anfordern und automatisch und rechtzeitig in für den Erfolg des Systems kritischen oder sicherheitskritischen Situationen Korrekturmaßnahmen veranlassen;

g) Verfügbarkeit der Mittel und Ressourcen (resource availability RA): die Verfügbarkeit aller Netzwerkressourcen sicherstellen, um so vor Denial-of-Service-Angriffen zu schützen.

Weitere durch diese Publikation eingeführte Konzepte sind die gestaffelte Verteidigung (defense in depth), die Bedrohungs-Risikobeurteilung, die Reife eines IT-Sicherheitsprogramms, IT-Sicherheitsleitlinien, Zonen (Zones) und gesicherte Kanäle (Conduits) (zur Aufteilung des betrachteten Systems) sowie Security-Level (SL).

Diese beschreiben abgestuft den Einsatz, mit dem ein erwarteter Angreifer vorgehen wird:

- SL 1: zufällige Fehlanwendung,
- SL 2: absichtliche Versuche mit einfachen Mitteln,
- SL 3: wie SL2, aber mit Kenntnissen und entsprechenden Mitteln,
- SL 4: wie SL 3 aber mit erheblichen Mitteln.

Je nach der Position im Lebensweg, auf den sich der SL bezieht, wird unterschieden zwischen:

- SL-T (SL target): dieser zu erzielende SL ist ein Ergebnis der Bedrohungs-Risikoanalyse,
- SL-C (SL capable): SL, den ein Gerät oder System erreichen kann, wenn es richtig eingesetzt und konfiguriert wird,
- SL-A (SL achieved): der im Gesamtsystem erreichte und messbare SL.
- IEC 62443-1-2, Industrial communication networks - Network and system security - Part 1-2: Glossary. Bearbeitungsstand: in Entwicklung
- IEC 62443-1-3, Industrial communication networks - Network and system security - Part 1-3: System security compliance metrics. Der Draft Technical Specification (DTS) wurde im ersten Quartal 2014 bei IEC zurückgewiesn
- IEC 62443-2-1, Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program. Bearbeitungsstand: IEC 62443-2-1:2010 (CDV 2Q/15):

  Dieser Teil der Normenreihe wurde vom TC 65 der IEC veröffentlicht. Sie legt die Elemente fest, die zur Einrichtung eines IT-Sicherheitsprogramms notwendig sind. Letzteres ist als Managementsystem zur IT-Sicherheit aufzufassen. Die Elemente betreffen Leitlinien, Vorgehensweisen, Umsetzungen in der Praxis und das Personal. Die Norm enthält weiterhin einen Leitfaden zur Entwicklung dieser Elemente, der jedoch als Beispiel zu verstehen ist und auf den jeweiligen Anwendungsfall angepasst werden muss.
- IEC 62443-2-2, Industrial communication networks - Network and system security - Part 2-2: Implementation guidance for an industrial automation and control system security program. Bearbeitungsstand: geplant
- IEC 62443-2-3, Industrial communication networks - Network and system security - Part 2-3: Patch Management. Bearbeitungsstand: Technical Report (TR) 01/ 2015

- IEC 62443-2-4, Industrial communication networks - Network and system security - Part 2-4: Requirements for IACS solution providers. Bearbeitungsstand: International Standard (IS) im 02/ 2015.

  Sie legt Anforderungen zu IT-Sicherheitsleitlinien, Vorgehensweisen und Praktiken fest, die auf die Lieferanten von industriellen Automatisierungssystemen während des Lebensweges ihrer Produkte anwendbar sind.

- IEC 62443-3-1, Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems. Bearbeitungsstand: IEC/TR 62443-3-1:2009-07.Überarbeitung geplant.

  Dieser Teil stellt verschiedene Techniken zur IT-Sicherheit zusammen und bewertet diese. Diese dienen beispielsweise zur Authentisierung und Autorisierung, zum Filtern, Sperren und zur Zugriffskontrolle, zur Verschlüsselung, zur Validierung von Daten, zur Auditierung, Messung und umfassen auch Werkzeuge zur Überwachung und Erkennung sowie Betriebssysteme.

- IEC 62443-3-2 Industrial communication networks - Network and system security - Part 3-2: Security levels for zones and conduits. Bearbeitungsstand: Committee Draft for Vote (CDV) im dritten Quartal 2016.

- IEC 62443-3-3 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. Bearbeitungsstand: IEC 62443-3-3:08/2013.

  Dieser Teil legt Anforderungen zur IT-Sicherheit von industriellen Automatisierungssystemen entsprechend den grundlegenden Anforderungen (Foundational Requirements, FR) nach IEC 62443-1-1 fest. Zu jeder grundlegenden Anforderung werden dazu eine Reihe von Systemanforderungen (System Requirements, SR) genannt, die erstere näher ausführen. Zu einer Systemanforderung werden ggf. weitere weitergehende Anforderungen aufgeführt (Requirement enhancements, RE). Beispielsweise werden zur grundlegenden Anforderung "Nutzung kontrollieren" (FR 2 - Use Control, UC) zwölf Systemanforderungen genannt, die erste davon ist SR 2.1 "Durchsetzung der Autorisierung". Sie hat zum Inhalt, dass Bediengeräte nur befugt benutzt werden dürfen. Hierzu werden weitergehende Anforderungen genannt, z.B. SR 2.1 RE 2 "Erlaubniserteilung nach Rollen". Sie verlangt, dass Bedienungsbefugnisse nach den Rollen, die ein Benutzer einnimmt, vergeben werden. Die Systemanforderungen und weitergehenden Anforderungen werden entsprechend des erreichbare Security Levels nach IEC 62443-1-1 gefordert (SL-C). Darunter ist der Security Level zu verstehen, den das System erreichen kann, wenn es richtig eingestellt wurde. Die IEC 62443-3-3 erlaubt es somit, bei vorliegendem SL-C die Anforderungen an die Technik des Systems herzuleiten oder bei erfüllten Anforderungen den erreichbaren SL-C zu nennen. Weiterhin werden in dieser Norm Randbedingungen genannt, die typisch für industrielle Automatisierungssysteme sind, beispielsweise der Erhalt von Realzeiteigenschaften bei Erkennung eines IT-Sicherheitsvorfalls, die Aufrechterhaltung von Sicherheitsfunktionen oder der Weiterbetrieb bei Denial-of-Service-Angriffen.

- IEC 62443-4-1 Industrial communication networks - Network and system security - Part 4-1: Product development requirements
  Bearbeitungsstand: ein FDIS ist im vierten Quartal 2016 geplant
- IEC 62443-4-2 Industrial communication networks - Network and system security - Part 4-1: Technical requirements for industrial automation and control system components
  Bearbeitungsstand: ein Document for Comment (DC) ist im ersten Quartal 2015 geplant

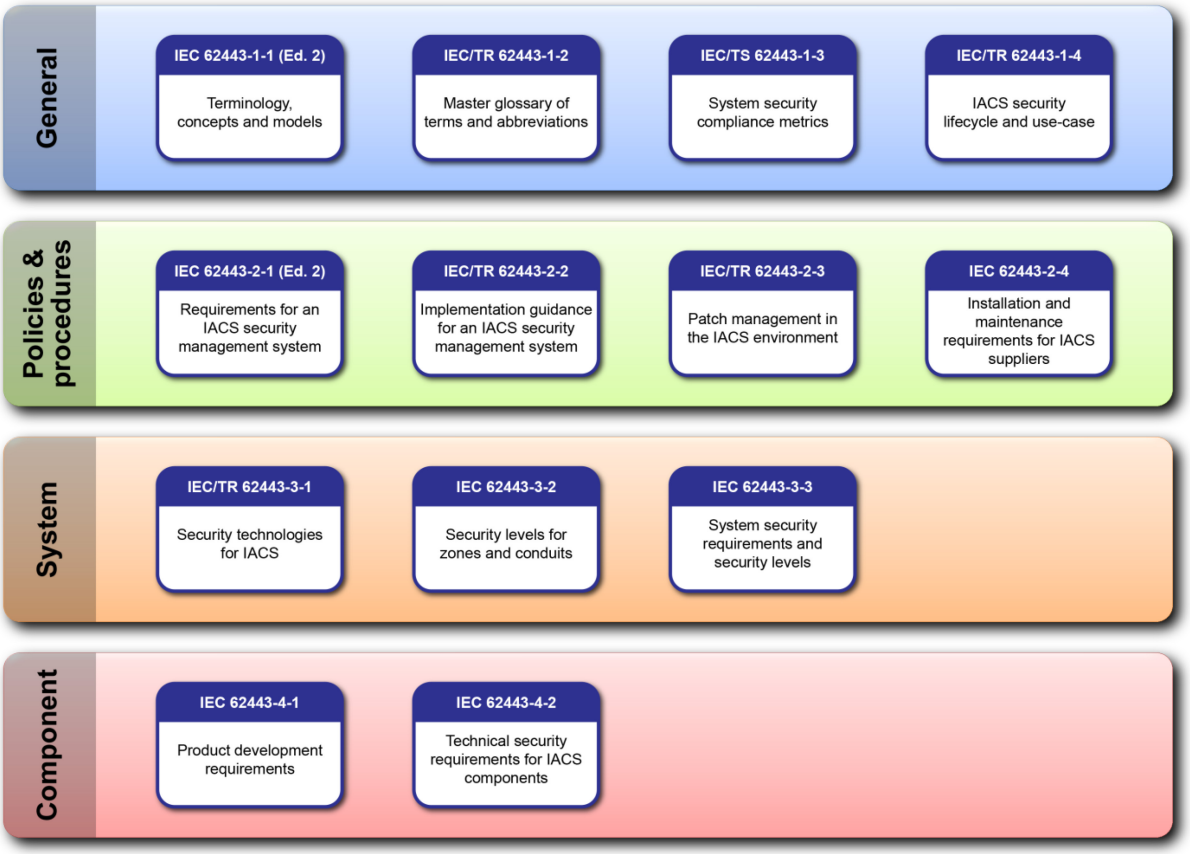


Abbildung 7: Struktur der IEC 62443 Normenreihe

5.3.3.2 Namur-Arbeitsblatt NA 115 - „IT-Sicherheit für Systeme der Automatisierungstechnik: Randbedingungen für Maßnahmen beim Einsatz in der Prozessindustrie“

Bei der Veröffentlichung NAMUR **(Interessengemeinschaft Automatisierungstechnik der Prozessindustrie)** NA 115 (Namur-Arbeitsblatt) „IT-Sicherheit für Systeme der Automatisierungstechnik: Randbedingungen für Maßnahmen beim Einsatz in der Prozessindustrie“ aus dem Jahr 2006 handelt es sich um Erfahrungsberichte und Arbeitsunterlagen aus Sicht der Chemie- und Pharmaindustrie, die keinen Normencharakter haben. Deutlich dargestellt wird die Prioritätenreihenfolge der Schutzziele für Prozess-IT: 1. Verfügbarkeit, 2. Integrität, gefolgt von Authentizität, Vertraulichkeit, Nichtabstreitbarkeit und Überprüfbarkeit. IT-Sicherheit ist in den letzten Jahren ein wichtiges Thema beim Einsatz von Systemen der Automatisierungstechnik geworden. Das hat seine Gründe zum einen in der gegenüber früher erweiterten Funktionalität der

Systeme mit einer immer stärkeren Integration in die IT-Landschaft der Unternehmen, zum anderen hat es seine Ursachen in dem Übergang von proprietären Systemen zu Systemen, die auf Basis von Hardware und Betriebssystemen aus der Standard-IT aufgebaut sind.
Während die stärkere Integration der Systeme die Möglichkeiten für einen Angriff erhöht, ist die Verwendung von Standard-IT-Komponenten als Basis für die Systeme der Grund dafür, dass Angriffe zunehmend erfolgversprechend sind. Letztendlich sind die Systeme der Automatisierungstechnik heute den gleichen Bedrohungen ausgesetzt wie die klassischen IT-Systeme. Ziel dieses NAMUR-Arbeitsblattes ist es, aus Anwendersicht die Randbedingungen im Bereich Automatisierungstechnik für IT-Sicherheitsprodukte darzulegen. Das NAMUR-Arbeitsblatt richtet sich an Hersteller und Systemintegratoren. Es soll ihnen für die Anwendung von Maßnahmen bzw. für das Design neuer Systeme die spezifischen Randbedingungen in der Prozessindustrie vermitteln. Es richtet sich auch an Anwender, die die entsprechenden Kriterien bei Kaufentscheidungen berücksichtigen sollten. Thema des NAMUR-Arbeitsblattes sind sowohl Maßnahmen für heutige Systeme als auch die Entwicklung zukünftiger Systeme der Automatisierungstechnik unter dem Gesichtspunkt IT-Sicherheit.

5.3.3.3 VDI/VDE Richtlinie 2182

Die VDI/VDE-Richtlinie 2182 wurde durch den Fachausschuss 5.22 „Security“ der VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik GMA erarbeitet. Das Ziel war es, wegen der bis dato fehlenden nationalen und vor allem internationalen Normen zum Thema IT-Security eine Diskussionsgrundlage zu schaffen – und zwar aus deutscher Sicht.

Die Richtlinie beschreibt, wie die Informationssicherheit von automatisierten Maschinen und Anlagen durch die Umsetzung von konkreten Schutzmaßnahmen erreicht werden kann; dazu werden Aspekte der eingesetzten Automatisierungsgeräte, Automatisierungssysteme und Automatisierungsanwendungen betrachtet. Auf der Basis einer zwischen Herstellern von Automatisierungsgeräten und -systemen und deren Nutzern (z. B. Maschinenbauer, Integratoren, Betreibern) abgestimmten, gemeinsamen Begriffsdefinition wird eine einheitliche, praktikable Vorgehensweise beschrieben, wie Informationssicherheit im gesamten Lebenszyklus von Automatisierungsgeräten, -systemen und -anwendungen gewährleistet werden kann. Der Lebenszyklus berücksichtigt die Phasen Entwicklung, Integration, Betrieb, Migration und Außerbetriebsetzung.

Das Blatt 1 der Richtlinie definiert dabei ein einfaches, iteratives Vorgehensmodell, das in acht Prozessschritten gegliedert ist. Es stellt mehr oder weniger ein „Good-Practice-Werk“ dar, welches hauptsächlich aus zusammengetragenen offenen Punkten (To-dos) und Erfahrungswerten der Mitglieder besteht. Obwohl neben der VDI/VDE-Gesellschaft für Mess- und Automatisierungstechnik auch weitere Verbände (unter anderem NAMUR, ZVEI, VDMA) die Richtlinie aktiv mitgestaltet haben, ist das Blatt 1 unabhängig von jeglichen Anwendungen und damit auch unabhängig von Smart Grid zu sehen. Bei den Blättern 2.1, 2.2, 3.1, 3.2, 3.3, den sogenannten „Beispielblättern“, spielen zwar beispielhafte Anwendungen der Fabrik- und Prozessautomatisierung eine essenzielle Rolle, Smart Grid bzw. energienahe Themen standen dabei jedoch nicht im Fokus des Fachausschusses 5.22.

Um jedoch Synergiepotenziale zu ermöglichen bzw. zu unterstützen, hat sich der Fachausschuss zur Aufgabe gemacht, seine Ergebnisse und damit letztlich auch das erarbeitete Know-how, der Öffentlichkeit zur Diskussion zu stellen. Im Zuge dessen gab es zum einen zahlreiche Veröffentlichungen (unter anderem regelmäßige Messe-, Diskussionsforen und Workshops). Zum anderen wurden verschiedene Kooperationen mit relevanten DKE-Normungsgremien eingegangen,

so auch mit dem „DKE/GAK 952.0.15 DKE-ETG-ITG Informationssicherheit in der Netz- und Stationsleittechnik“ und dem „DKE/UK 931.1-IT-Sicherheit in der Automatisierungstechnik“. Auf gemeinsamen Sitzungen wird regelmäßig über die Arbeiten des Fachausschusses 5.22 berichtet, mit dem Ziel, die Konzepte der VDI/VDE-Richtlinie 2182 in die internationale Normung einzubringen. Eine weitere Möglichkeit ergab sich durch die Anwendung der Richtlinie selbst und hierbei insbesondere durch die Erstellung weiterer Beispielblätter. Mit dem DKE/AK 952.0.15 wurde unter anderem diskutiert, ein weiteres Beispielblatt zu erstellen, das ein energienahes Thema adressiert.

5.3.3.4 Industrial Control System Security Compendium

Das im Jahre 2013 vom BSI (Bundesamt für Sicherheit in der Informationstechnik) herausgegebene Kompendium hat das Ziel, ein Grundlagenwerk zur IT-Sicherheit von Industrial Control Systems (ICS) zu schaffen. Das ICS Kompendium soll als Basis für den Austausch an der Schnittstelle zwischen IT- und Cyber-Sicherheitsexperten auf der einen und Industriespezialisten auf der anderen Seite dienen und richtet sich demnach an beide Zielgruppen gleichermaßen. Der Inhalt wird sich neben ICS Grundlagen mit einem Best-Practice Guide für Betreiber, mit der Methodik für Audits von ICS-Installationen, dem noch notwendigen Forschungs- und Entwicklungsaufwand auch mit dem Normen- und Standardumfeld beschäftigen. Hier sollte es von Seiten der Normung zukünftig darum gehen, das sektorspezifische Know-How aus den internationalen Normungsgremien mit den Arbeiten des BSI zu synchronisieren, um ein Auseinanderlaufen der Aktivitäten auf nationaler und internationaler Ebene zu verhindern.

Im Jahr 2014 wurde vom BSI zusätzlich das „ICS Security Kompendium - Testempfehlungen und Anforderungen für Hersteller von Komponenten“ herausgegeben. Diese Ergänzung richtet sich an die Hersteller von ICS Komponenten und stellt eine Hilfestellung zur Etablierung eines Security by Design Ansatzes bei der Entwicklung von ICS Komponenten durch Hinweise zu IT-Sicherheitstests und Maßnahmen zur Vermeidung von Schwachstellen zur Verfügung.

5.3.4 Handlungsbedarfe (Normungsbedarfe)

5.3.4.1 Funktionale Sicherheit - IT-Sicherheit

Ein zentraler Aspekt für IT-Sicherheit im Bereich Industrie 4.0 wird das Zusammenspiel zwischen „Funktionaler Sicherheit“ (Safety) und „IT Sicherheit“ (Security) bei der Vernetzung von Automatisierungs- und Produktionssystemen sein.Industrie 4.0 bringt daneben auch die Modularisierung der Produktion mit sich. Das heißt, dass Security- und Safety Konzepte im Zusammenspiel wirksam bleiben müssen, ohne das stets eine Neubewertung notwendig wird. Zusätzlich dürfen Security-Maßnahmen nicht in Konflikt mit Safety-Vorschriften geraten. Die Normenwelt bildet das Zusammenspiel und die Interdependenz noch nicht ab.

Zur Zeit existieren viele verschiedene Gruppen, die intensiv daran arbeiten, die IT-Sicherheit für Safety-relevante Systeme in den diversen Industriebereichen sinnvoll zu etablieren, wobei zum Teil eigene Sichtweisen und Begriffswelten sowie divergente Ansätze entstehen. Dieser Sachverhalt macht einen umfassenden Informationsaustausch notwendig, um die Entwicklung einheitlicher und standardisierter Lösungen zu ermöglichen. Seitens der DKE wird dieser Themenkomplex daher in einem branchenübergreifend besetzten Arbeitskreis („TBINK Ad-Hoc Arbeitskreis IT-Security“) aufgegriffen, um unter Mitwirkung von vorhandener Expertise aus verschiedenen Normungsgremien Ergebnisse schnell in laufende Normungsaktivitäten einzubringen. Die in diesem Gremium erarbeitete VDE Anwendungsregel wird voraussichtlich Anfang 2017 erscheinen.

5.3.4.2 Umfeldanalyse / Normungslandschaft

Der Schutz von Informationen als werthaltige Assets vor Verlust und Missbrauch, die Sicherstellung ihrer zeitgerechten Verfügbarkeit für berechtigte Nutzer und die Einhaltung ihrer Integrität und der Vertraulichkeit sind eine unverzichtbare Grundlage jedes IT-Systems. Mit der Virtualisierung, Flexibilisierung und Verkopplung der firmeninternen Betriebs-, Produktions- und Feldnetzwerken mit dem globalen Netz ergibt sich eine Vielzahl von neuen Herausforderungen an die Informationssicherheit. An vielen Stellen entstehen zur Zeit Aussagen, Anforderungen, Festlegungen und Empfehlungen zur Informationssicherheit. Ansprechpartner sind die Landesdatenschutzbeauftragten, BSI sowie nationale und internationale Normungsorganisationen (z. B. IEC, DKE, DIN) unter aktiver Mitarbeit der relevanten Verbände (BITKOM, VDE, VDI, GMA).

Zur Sicherstellung der Anforderungen aus der industriellen Produktion ist es unbedingt erforderlich, dass eine Landkarte erstellt wird, die die Felder, Anforderungen und angebotenen Lösungsmethoden der Informationssicherheit im Umfeld der industriellen Produktion darstellt und strukturiert.

5.3.4.3 Metriken für Unternehmensübergreifende Wertschöpfungsnetzwerke

Ein wesentliches Merkmal von Industrie 4.0 sind dynamische firmenübergreifende Wertschöpfungsnetzwerke. Eine sichere Kommunikation insbesonders über Unternehmensgrenzen hinweg erfordert die Kenntnis der Fähigkeiten und Möglichkeiten der jeweiligen Teilnehmer. Das schließt neben den funktionalen Fähigkeiten auch den Security-Level mit ein. Die Anforderung eines benötigen Security-Levels muss mit den IT-Sicherheitsfähigkeiten übereinstimmen, ansonsten erfolgt keine Kommunikationsaufbau Eine einheitliche Metrik (z.B. ein abgestuftes Sicherheitsniveaus auf einer Skala) erlaubt die einfachere Einschätzung der sicheren Einsetzbarkeit einer Komponente in einem Gesamtsystem. Zu diesem Zweck müssen geeignete Bewertungsmetriken für die Sicherheitseigenschaften von Komponenten und Systemen erarbeitet und vereinheitlicht werden. Eine einheitliche und kompatible Sicherheitsbewertung von unterschiedlichen Industriekomponenten schafft so die Voraussetzungen für die Berücksichtigung von Sicherheit im Entwurf und im Betrieb von komplexen aus Einzelkomponenten bestehenden Systemen. Die Metrik muss ein Modell beinhalten, das es erlaubt, den Security-Level eines Wertschöpfungsnetzwerkes _automatisch_ zu ermitteln anhand der aktuellen Vernetzung der Teilnehmer des Wertschöpfungsnetzwerkes. Zu dem Zeitpunkt der Integration von Komponenten zu einer Maschine muss sich der resultierende Security-Level aus der Komposition der Komponenten ergeben.

Hier besteht zum einen Forschungsbedarf, um eine praktikable und aussagekräftige Ermittlungsmethode eines Gesamtsicherheitsniveaus zu entwickeln. Im Anschluss besteht Normierungsbedarf, um eine einheitliche und automatisch verarbeitbare Sicherheitsbewertung für eine Vielzahl von Komponenten und Komponentenklassen zu erreichen.

5.3.4.4 Sichere Identitäten im Produktionsumfeld

Für die automatisierte Kommunikation über Unternehmensgrenzen hinweg müssen Techniken und Verfahren festgelegt werden, um kommunizierende Geräte und Systeme zu identifizieren und authentifizieren. Hier gibt es bereits viele Normen und standardisierte Verfahren, jedoch sind weitere Untersuchungen von Nöten, um die geeigneten Verfahren und Techniken auszuwählen um die besonderen Rahmenbedingungen im Bereich der industriellen Produktion wie Echtzeitanforderungen, Safety Aspekte und Langlebigkeit der beteiligten Systeme zu berücksichtigen. Geeignete Techniken sind dann in entsprechenden Normen und Standards vorzugeben.

5.4 Gesundheitsinformationssysteme und Medizintechnik

5.4.1 Themenbeschreibung

Im Laufe der Zeit hat sich die Medizintechnik von der Einzelgeräteanwendung am Patienten immer mehr zu einer (IT-gestützten) Systemanwendung entwickelt. So geht z. B. im Bereich des Operationssaals und der Intensivmedizin der Trend zur Darstellung von digitalen Informationen auf einem Bildschirm, um bei immer komplexeren Behandlungsmethoden schnell durch den Arzt reagieren zu können. Die informationstechnische Vernetzung von Diagnose, Kommunikation und Therapie stellt die Medizintechnik vor besondere Herausforderungen in Bezug auf die IT-Sicherheit. Dieses insbesondere deshalb, weil der Schutz von personenbezogenen Daten und ihrer teils lebensnotwendigen Verfügbarkeit hochsensible Schutzziele darstellen, die sich jedoch teilweise unter anderem auch wegen gesetzlicher Implikationen widersprechen können.

Der weitreichende Scope der Standardisierung von Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen liegt daher auf der Spezifikation von Methoden und Systemen zur Sicherstellung und Verbesserung der Vertraulichkeit, Integrität und Verfügbarkeit von Gesundheitsinformationen. Darüber hinaus in der Bewahrung der eingesetzten Systeme vor negativen Auswirkungen für die Patientensicherheit, der Sicherung des Datenschutzes für persönliche Gesundheitsinformationen des Betroffenen und der Sicherstellung, dass der Nutzer seinen Verantwortlichkeiten in Bezug auf Gesundheitsinformationssystemen nachkommen kann.

Als Besonderheit des Gesundheits- und Sozialwesens (und in der Folge: auch der Medizintechnik) fällt die starke örtliche Fragmentierung der Prozesse und Organisationen auf, was selbst auf den fachlichen und prozessualen Ebenen der Versorgung die Standardisierung mit klassischen Vorgehensweisen erschwert. Dies spiegelt sich in der Informationstechnik für die Versorgungsprozesse natürlich wider und erschwert die klassische Standardisierung.

Um dieser Problemstellung effizient begegnen zu können, hat sich in diesem Zusammenhang die Standardisierung von Elementen der Infrastruktur sowie von grundlegenden Abläufen, die dann generisch spezifiziert werden, bewährt. Durch dieses Vorgehen sind regionale oder fachliche Gruppen in der Lage, aus diesen wiederverwendbaren Architekturen und Diensten die jeweils konkreten technischen Standards abzuleiten und dadurch eine Interoperabilität, die der Sache nach nicht weitergehen kann, als der Konsens der fachlichen Ebene, zu erhalten.

Anmerkung: Die Kritik an der mangelnden Interoperabilität der IT-Systeme im Gesundheitswesen ist zwar inhaltlich richtig, geht jedoch am Kern des Problems vorbei. Dieses insbesondere deshalb, weil das Kernproblem in diesem Bereich der Mangel an kooperierenden Prozessen und einem fehlenden fachlichen Konsens auf der Anwendungsebene ist.

Für die Informationssicherheit in diesem Bereich bedeutet das mithin, dass standardisierende Anwender stets den konkreten organisatorischen Rahmen und die tatsächlich relevanten fachlichen Prozesse beachten müssen, wenn sie aus der Vielfalt der im Folgenden geschilderten Standards ihren konkreten Implementierungsleitfaden (der die eigentliche technische Standard-Spezifikation bildet) aufstellen. Für IT-Systeme im Gesundheitswesen und der Medizintechnik sind deswegen nicht nur technische „Bausteine“ für Informationssicherheit wichtig, sondern auch Modelle und Methoden, die bei der systematischen Spezifikation für den konkreten Einzelfall zu beachten sind. Aus diesem Grund erwähnt der Absatz immer wieder Modelle auf verschiedenen Abstraktionsebenen und bezieht sich

auf moderne Verfahren des Entwurfs und der Realisierung von Diensten, Terminologien, (Objekt-)Datenbanken und Registern.

Neben der Beschreibung von domänenspezifischen Anforderungen, Functional Models und Service Functional Models werden Infrastrukturdienste (Verzeichnisdienste, Terminologiedienste, Policy-Repräsentationen, etc., aber auch Basisdefinitionen wie Ontologien, Terminologien und Vokabularien standardisiert. Auch werden domänenspezifische Ergänzungen zu existierenden domänenübergreifenden Spezifikationen erarbeitet.

Betrachtet man das Problemfeld der Datensicherheit, was international in der Regel den Datenschutz einschließt, können die Grundkonzepte der Kommunikationssicherheit und der Anwendungssicherheit unterschieden werden. (siehe Bild 8)

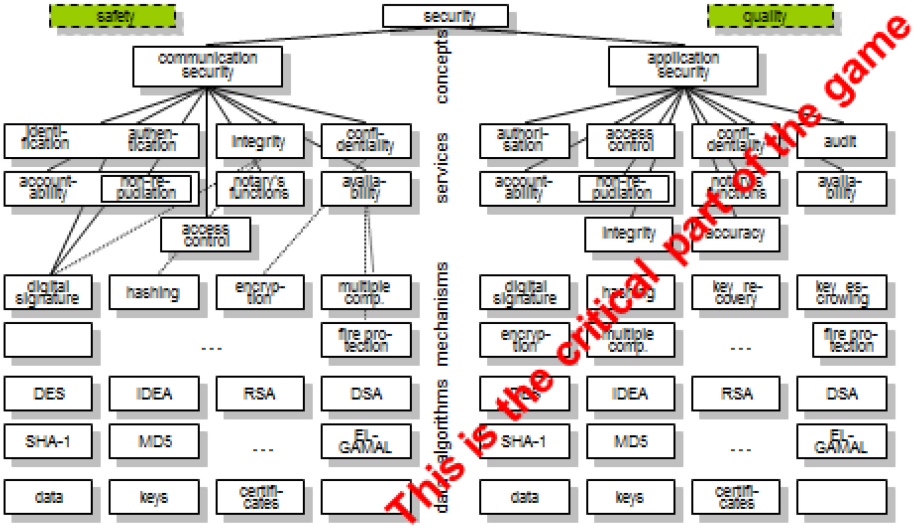


Abbildung 8: Security Concepts (Blobel B, Roger-France F (2001) A Systematic Approach for Analysis and Design of Secure Health Information Systems. International Journal of Medical Informatics 2001; 62 (3): 51-78)

Während die Kommunikationssicherheitsdienste nicht domänenspezifisch sind und deshalb fortgeschrittene Spezifikationen und Lösungen aus anderen Domänen (z.B. Finanzen, Telekommunikation, Administration) nachgenutzt werden können, hängen die Anwendungssicherheitsdienste zum Privilegmanagement, zur Zugriffskontrolle und zur Nutzung der persönlichen Gesundheitsinformationen von domänenspezifischen Regeln (Gesetze, Verordnungen, Regularien der involvierten Organisationen (Staat, Körperschaften der Selbstverwaltung, berufsständige Organisationen, betriebliche Regelungen) ab. Derartige Regeln werden nach ISO 22600 als Policies bezeichnet. ISO 22600 Health informatics – Privilege management and access control bildet in seinen drei Teilen – nicht nur für das Gesundheitswesen – eine Basisspezifikation.

5.4.2 aktive Standardisierungsgremien

Folgende Standardisierungsgremien arbeiten derzeit an Normen, die für den Bereich der Medizintechnik hinsichtlich IT-Sicherheit relevant sind:

Organisation	Gremien-bezeichnung	Gremientitel	Arbeitsgebiet

DIN	NA 063-07-04 AA	Medizinische Informatik — Sicherheit	Sicherheit in der medizinischen Informatik
DKE	UK 811.3	Sicherheit von medizinisch genutzten Geräten / Systemen / Einrichtungen in der vernetzten Anwendung	Betrieb von Medizingeräten in informationstechnischen oder medizinischen Netzwerken
CEN	TC251	Health Informatics	Medizinische Informatik, Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen
ISO	TC215	Health Informatics	Medizinische Informatik, Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen

5.4.3 Derzeitige Landschaft (Status quo in Bezug auf IT-Sicherheit)

Ein besonderer Schwerpunkt der Aktivitäten liegt in der Unterstützung sicherer und datenschutzgerechter Kommunikation und Kooperation zwischen direkt oder indirekt agierenden Einrichtungen des Gesundheits- und Sozialwesen (intersektorale Kommunikation und Kooperation). Dazu werden die notwendigen Infrastrukturdienste (Identifikation, Authentifizierung, Verzeichnisdienste, etc.), Rechtemanagement und Zugriffskontrolle auf der Basis expliziter Policy-Spezifikationen, Rollendefinitionen, Datenschutz- und Datensicherheitsattribute im Kontext des Nachrichten und Dokumentenaustausches, aber auch der Kommunikation von Auszügen elektronischer Gesundheitsakten standardisiert. Rechtemanagement und Zugriffskontrolle einschließlich bezogener Regeln wie der Berücksichtigung des Patientenwillens, Nutzungsbeschränkung und Zweckbindung der Daten stehen als domänenspezifische Anwendungssicherheitsdienste im Zentrum der Aktivitäten der SDOs des Gesundheitswesens.

Die für Deutschland definierte Gesundheitstelematik-Infrastruktur bringt eine Orientierung auf Smart-Card-Technologien und somit spezifische Kartenstandards mit sich.

Da die Akzeptanz der Lösungen entscheidend für eine erfolgreiche Implementierung ist, müssen die Standards die Anforderungen der wichtigsten Stakeholder in diesem Bereich berücksichtigen, deren Bedürfnisse befriedigen und ihnen einen spürbaren Nutzen bringen. Deshalb müssen medizinrelevante Dienste wie die elektronische Gesundheitsakte eine entsprechende Priorität erfahren.

Viele europäische und außereuropäische Länder sind in der Etablierung standardbasierter IKT-Dienste für das Gesundheits- und Sozialwesen weiter fortgeschritten als die Bundesrepublik.

Es ist bekannt, dass Medizingeräte und Gesundheitsinformationssysteme Ziel von Hackern sein können. Davon sind nicht nur Medizingeräte betroffen, die bereits länger im Markt sind. Im Bereich der Anforderungen an die Informationssicherheit spielt der Betreiber eine immer größere Rolle, da er das Netzwerk mit seinen Komponenten „vor Ort“ unter Verwendung einer Vielzahl von unterschiedlichen Komponenten konfiguriert.

Die Sicherheitsbetrachtungen können nur im Systemverbund unter Berücksichtigung von drei Schutzzielen bewertet werden. Diese drei Schutzziele sind: Effektivität, Daten-und Systemsicherheit und die Sicherheit des Patienten. Je nach Use-case der medizinischen Behandlung kann den einzelnen Schutzzielen eine unterschiedliche Bedeutung zugeteilt werden (so ist es z.B. wichtig, dass der behandelnde Arzt immer Zugriff auf die Daten hat, vor allem in Notfallsituationen). Es ist erforderlich, kritische IT-Systeme im Gesundheitswesen einem Risikomanagement zu unterziehen, welches die Aspekte der drei Schutzziele im jeweiligen soziotechnischen Kontext betrachtet und so die medizinische Versorgungsqualität und Patientensicherheit gewährleistet. Bei der Bewertung der Systeme sind nicht nur der Normalbetrieb, sondern auch außergewöhnliche Lagen wie ein Massenanfall von Verletzten, Katastrophen oder Terroranschläge zu betrachten.

IEC 80001-1 beschreibt bereits die Anwendung eines Risikomanagements für den Betrieb von IT-Netzwerken, die Medizinprodukte beinhalten, mit dem die drei Schutzziele bewertet und die optimale Patientenbehandlung sichergestellt werden.

Für Medizinprodukte existiert eine Meldepflicht für Vorkommnisse, um (weitere) Patientenschäden durch einen vergleichbaren Fehler abzuwenden. Die Erkenntnisse aus den Fehlermeldungen fließen sowohl in die Risikobewertung des Herstellers ein, als auch durch die Veröffentlichung und Information der Betreiber in die Risikobewertung der Betreiber. Dies gilt jedoch nicht für Informationssysteme, die nicht unter das Medizinproduktegesetz fallen oder für kritische Ereignisse mit und ohne Patientenschaden, die durch Benutzungsfehler entstehen.

5.4.4 Handlungsbedarfe (Normungsbedarfe)

Paradigmenwechsel in der Organisation und Realisierung des Gesundheits- und Sozialwesens, aber auch in der Technologie wie ubiquitäre Gesundheitsversorgung, personalisierte, präventive, prädiktive, partizipative Systemmedizin vom Molekül übers Genom bis hin zur Gesellschaft, mobile Technologien, der Einsatz sozialer Medien, Big Data und Analytics bringen neue Herausforderungen für Datenschutz, Datensicherheit und IT-Sicherheit mit sich. Dafür müssen standardbasierte Lösungen entwickelt werden. Außerdem nimmt die Integration von biomedizintechnischen und pharmazeutischen Applikationen zu, die unter dem Aspekt der (Daten)Sicherheit betrachtet werden müssen (Medizinproduktegesetz). Auch wächst der Anteil an SOA-basierten Spezifikationen und Webservices. Wo möglich, wären proaktive anstatt der üblichen reaktiven Projekte wünschenswert. Neben den auch in andere Domänen einziehenden Lösungsstrategien wie Security-by-Design, Privacy-by-Design, Security Analytics und Security und Privacy Intelligence spielt im Gesundheitswesen vor allem das Patient Empowerment durch automatisierte oder zumindest werkzeuggestützte Generierung und Durchsetzung individueller Policies eine entscheidende Rolle. Der Schutz die Daten erlangt gegenüber dem Schutz der Geräte und Applikationen eine Priorität.

Die Vielzahl von standardisierten Lösungen, jedoch auch standardisierter IKT-Entwürfe und -Architekturen wirft in der vernetzten Gesundheits-IKT zwei große Fragen auf, nämlich die nach den IKT-Schutzzielen und die Frage nach der Verantwortung für die Einhaltung der IKT-Schutzziele sowie Umsetzung von Teillösungen auf Komponenten-Ebene oder Funktions-Ebene. Eine Abbildung der im Kapitel Industry 4.0 für relevant befundenen IEC 62443-Reihe auf klinische / medizinische IKT wäre demnach dringend geboten, da deren Anerkennung durch die amerikanische Aufsichtsbehörde FDA klare Fakten geschaffen hat – ohne natürlich die verantwortlichen Rollen zu beschreiben. Eine „Übersetzung“ der IEC 62443-Reihe oder zumindest wesentlicher Strukturen daraus auf die

deutschen Verhältnisse wäre wünschenswert, da sie Rechtssicherheit, Transparenz und somit Vertrauen bei allen Beteiligten schaffen könnte.

Im Bereich der Gesundheitstelematik-/Gesundheitsinformatik-SDOs wäre ein personell und finanziell stärkeres Engagement der Bundesrepublik zu empfehlen. Auch wäre eine noch enge Kooperation der verschiedenen Standardisierungsgremien (ISO, CEN, ETSI, CEN-ELEC, aber auch OMG, OASIS, HL7, IHE, etc.) von großem Vorteil. Vorhandene Aktivitäten hierzu sollten gefördert werden. In diesem Kontext wäre eine integrative Struktur analog der formal akkreditierten kanadischen Standards Collaborative, die die nationalen Gremien der SDOs zusammenführt, von unschätzbarem Vorteil. Inzwischen folgen immer mehr Länder diesem Beispiel.

Die Thematik der IT-Sicherheit steht im Bereich der Medizintechnik vor besonderen Herausforderungen. Im Medizinbereich stehen die Verfügbarkeit, Bedienbarkeit und Akzeptanz der Geräte und Services eindeutig im Vordergrund. Einbußen an Bedienbarkeit durch Sicherheitsmaßnahmen sind im Klinikalltag nur schwer vermittelbar. Die Vorstellung, dass durch IT-Sicherheitsvorfälle die Verfügbarkeit von IT Systemen gefährdet ist, ist noch nicht flächendeckend bis auf Anwenderebene vorgedrungen. Normen und Standards können hier die Basis für entsprechende Akzeptanz von Sicherheitslösungen schaffen, wenn die Bedienbarkeit (Usability) beim Design von Sicherheitslösungen von Anfang an berücksichtigt wird. Dies gilt sowohl für die Fehlervermeidung wie auch die Fehlerbeherrschung: Ein Anwender muss sich über den Zustand des von ihm verwendeten Systems bewusst sein um bei korrumpierten Systemen ggf. auf Alternativen umsteigen zu können. Aufgrund der Nähe von Medizintechnik und Informationssysteme im Gesundheitswesen ist eine enge Anlehnung an die DIN EN 62366 wünschenswert. Aufgrund der Heterogenität des soziotechnischen Umfelds beim Betrieb von kritischen IT-Systemen und den daraus entstehenden Risiken im Gesundheitswesen ist es wichtig, aus Fehlern zu lernen. Daher ist der Aufbau oder die Nutzung existierender Fehlermeldesysteme für IT- assoziierte beinahe Behandlungsfehler oder Patientenschäden wünschenswert. Dies sollte auch ausdrücklich Benutzungsfehler einschließen um daraus eine Evidenz für die Weiterentwicklung von Usability-Standards zu erhalten.

Die Einbindung mobiler Endgeräte stellt eine weitere große Herausforderung für den Medizinbereich dar, für die noch keine standardisierten Voraussetzungen zur Einbindung in die Sicherheitsarchitektur bestehen. Hier sind vor allem die internationalen Normungsorganisationen angesprochen möglichst generische Standards und Normen für die weltweite Anwendung zu etablieren. Zusätzlich wird in Zukunft noch eine enge Verbindung zu AAL-Anwendungen notwendig sein, um die Versorgung des Menschen „zu Hause“ sicherstellen zu können. Dabei müssen In einer generell nicht vertrauenswürdigen Umgebung (Zero Trust) alle Ressourcen unabhängig von ihrer Lokalisation und administrativen Zugehörigkeit identifiziert, verifiziert und gesichert, Privilegierung und Zugriffskontrolle für alle Akteure (Personen, Organisationen, Geräte, Applikationen, Komponenten) limitiert und strikt durchgesetzt, und alle Aktionen überwacht und protokolliert werden.

5.5 Elektromobilität

5.5.1 Themenbeschreibung

Um die Vorreiterrolle Deutschlands im Bereich der Elektromobilität im weltweiten Wettbewerb zu erlangen und weiter auszubauen und um die Technologieentwicklung und die Wertschöpfung in Deutschland zu halten, müssen frühzeitig die Entwicklungen und die dahinterliegenden Interessen

zielorientiert weitergeführt und gebündelt werden. Für die erfolgreiche Positionierung der deutschen Wirtschaft ist es in diesem Kontext wichtig, die positiven Effekte der Normung und Standardisierung von Beginn an in den Entwicklungsprozess mit einzubeziehen und damit voll auszuschöpfen.

Die Normung auf dem Gebiet der Elektromobilität ist durch einige Aspekte charakterisiert, die sie von der bisherigen Normung unterscheidet. Die besondere Herausforderung besteht darin, die vielfältigen Aktivitäten unterschiedlicher Branchen und Industriezweige bedarfsgerecht und zielführend zu koordinieren und zu integrieren. Die Elektromobilität ist eine Sprunginnovation, die ein neues, übergreifendes Systemdenken erfordert. Bislang wurden Normen und Standards domänenspezifisch getrennt für die Bereiche der Elektrotechnik/Energietechnik und die Automobiltechnik betrachtet. Gerade für das Zusammenführen dieser Domänen und die sich daraus ergebenden neuen Berührungspunkte und Schnittstellen fehlen bislang eine übergreifende Sichtweise und eine klare thematische Zuordnung.

Im Rahmen der Elektromobilität fallen eine ganze Reihe von Informationen an, die an verschiedenen Stellen erfasst und gespeichert sowie über diverse Kommunikationsschnittstellen zwischen den beteiligten Parteien ausgetauscht werden sollen. Der Gewährleistung einer angemessenen Sicherheit dieser Daten und der jeweiligen Datenverarbeitungssysteme und -netze kommt eine hohe Bedeutung zu. Soweit es sich um personenbezogene Daten handelt, ist die Sicherstellung eines umfassenden Datenschutzes gerade für die breite Akzeptanz der Elektromobilität erforderlich. Datensicherheit und Datenschutz stellen Querschnittthemen dar, die über alle Einzelsysteme und Kommunikationsschnittstellen hinweg behandelt werden müssen.

Die Deutsche Normungs-Roadmap Elektromobilität Version 3.0 (Dezember 2014) stellt eine Fortschreibung der ersten, im Herbst 2010 vorgestellten Deutschen Normungs-Roadmap Elektromobilität dar. Sie greift aktuelle Entwicklungen der Elektromobilität sowie der Rahmenbedingungen auf und stellt diese in Bezug zu laufenden und notwendigen Normungsaktivitäten. Die Deutsche Normungs-Roadmap Elektromobilität enthält das gemeinsame Verständnis aller in die Elektromobilität involvierten Akteure. An der Erstellung waren neben Fahrzeugherstellern, Elektroindustrie, Energielieferanten/Netzbetreibern und Informationsnetzprovidern auch Verbände und Politik beteiligt. Aus diesem Grund stellt die Deutsche Normungs-Roadmap Elektromobilität die deutsche Normungsstrategie für diesen Bereich dar.

Politische Flankierung ist europäisch und international erforderlich

Eine enge Verzahnung von Forschung und Entwicklung, Regulierung und gesetzlichen Rahmenbedingungen mit der Normung ist notwendig. Nationale Normung und Regulierung bestimmter Staaten dürfen eine internationale Vereinheitlichung nicht behindern

Normung muss schnell und international sein

Nationale und internationale Normungskonzepte konkurrieren derzeit miteinander. Aufgrund von internationalen Märkten für Kraftfahrzeuge müssen jedoch von Beginn an internationale Normen angestrebt werden. Dies gilt in gleicher Weise für die Schnittstelle von Fahrzeug und Infrastruktur. Eine alleinige deutsche bzw. europäische Normung für die Elektromobilität wird als nicht ausreichend angesehen. Daher sind eine schnelle Erarbeitung nationaler Vorschläge und der kurzfristigen Umsetzung der in Deutschland erzielten Ergebnisse in der internationalen Normung essenziell.

Koordination und Fokussierung zwingend erforderlich

Elektromobilität ist durch eine Vielzahl an Akteuren und Fachgebieten geprägt. Daher sind eine gremienübergreifende Zusammenarbeit und Koordinierung durch den bestehenden Lenkungskreis EMOBILITY (DKE/ NA Automobil) und die Geschäftsstelle Elektromobilität im DIN wichtig, um Doppelarbeit zu vermeiden. Es sollen keine neuen Gremien geschaffen werden; stattdessen sind die existierenden Gremien in DIN und DKE zu stärken.

Normung muss klar und eindeutig sein

Um Innovationen zu fördern, soll Normung funktionsbezogen sein und Festlegungen hinsichtlich technischer Lösungen vermeiden („performance-based rather than descriptive“). Zur Sicherstellung der erforderlichen Interoperabilität bei Schnittstellennormen (z. B. zwischen Fahrzeug und Netzinfrastruktur) müssen jedoch technische Lösungen festgelegt werden.

Weltweit einheitliche Ladeinfrastruktur ist notwendig (Interoperabilität)

Elektrofahrzeuge müssen „immer und überall“ geladen werden können: Die Interoperabilität von Fahrzeugen verschiedener Hersteller und der Infrastruktur unterschiedlicher Betreiber ist sicherzustellen, ebenso wie eine hinreichende Gewährleistung von Informationssicherheit. Normung und Standardisierung der Ladetechnik und Abrechnung müssen sicherstellen, dass zum Anwender hin eine einheitliche, komfortabel nutzbare und sichere Ladeschnittstelle geschaffen wird. Die Interessen der Nutzer müssen Vorrang haben vor den Interessen einzelner Unternehmen.

Vorhandene Normen müssen genutzt und umgehend weiterentwickelt werden

In den etablierten Domänen Automobiltechnik, Informations- und Kommunikationstechnik und Elektrotechnik existiert bereits eine Vielzahl an notwendigen Normen. Diese müssen entsprechend genutzt und bekannt gemacht werden. Informationen über diese Normungsarbeiten und deren Status sind Bestandteil der Deutschen Normungs-Roadmap Elektromobilität Version 3.0

Darüber hinaus liegt der Schwerpunkt der erforderlichen Arbeiten weniger auf der Initiierung neuer Normungsvorhaben als eher auf der Erweiterung bzw. Anpassung bestehender Normen und Spezifikationen an die Anforderungen der Elektromobilität. Insbesondere bei der Informationssicherheit und Schnittstellenthemen muss eine domänenübergreifende Zusammenarbeit auf internationaler Ebene erfolgen.

Mitwirkung an europäischer und internationaler Normung essenziell

Zur aktiven Einflussnahme und Umsetzung der Ziele ist eine verstärkte Mitarbeit auf nationaler und internationaler Ebene notwendig. Deutsche Unternehmen müssen sich deshalb auch zukünftig engagiert in die deutschen, europäischen und internationalen Normungsarbeiten einbringen. Normungsarbeiten sind als integraler Teil von F&E-Vorhaben zu sehen und somit förderwürdig.

Ein zentraler Aspekt für die Verbreitung der Elektromobilität ist neben der Straßenfahrzeugtechnik und Energieversorgung sowie der erforderlichen Informations- und Kommunikationstechnologie auch die Normung und Standardisierung.

Die bisher weitgehend getrennt betrachteten Domänen Automobiltechnik und Elektrotechnik/Energietechnik sowie Informations- und Kommunikationstechnik (IKT) und damit Informationssicherheit müssen für eine erfolgreiche Elektromobilität zusammenwachsen. Hierfür ist eine langfristige Strategie zu entwickeln, die sowohl die nationalen Belange berücksichtigt als auch der deutschen Wirtschaft den Zugang zu diesem expandierenden internationalen Markt öffnet. Ein Teil dieser Elektromobilitätsstrategie ist die Deutsche Normungs-Roadmap Elektromobilität Version 3.0, die den Bogen spannt vom kurzfristig erforderlichen Normungs- und Standardisierungsbedarf bis

hin zu langfristig angelegten Aktivitäten zur Normung und Standardisierung, aber auch zum Forschungsbedarf.

Es lassen sich die in Abbildung 9 gezeigten Systemkomponenten, Domänen und Unterbereiche identifizieren. Die Produktsicherheit und die Kommunikation stellen Querschnittthemen dar, die alle Systemkomponenten betreffen. Der Normungs- und Standardisierungsbedarf lässt sich in diese Bereiche unterteilen.

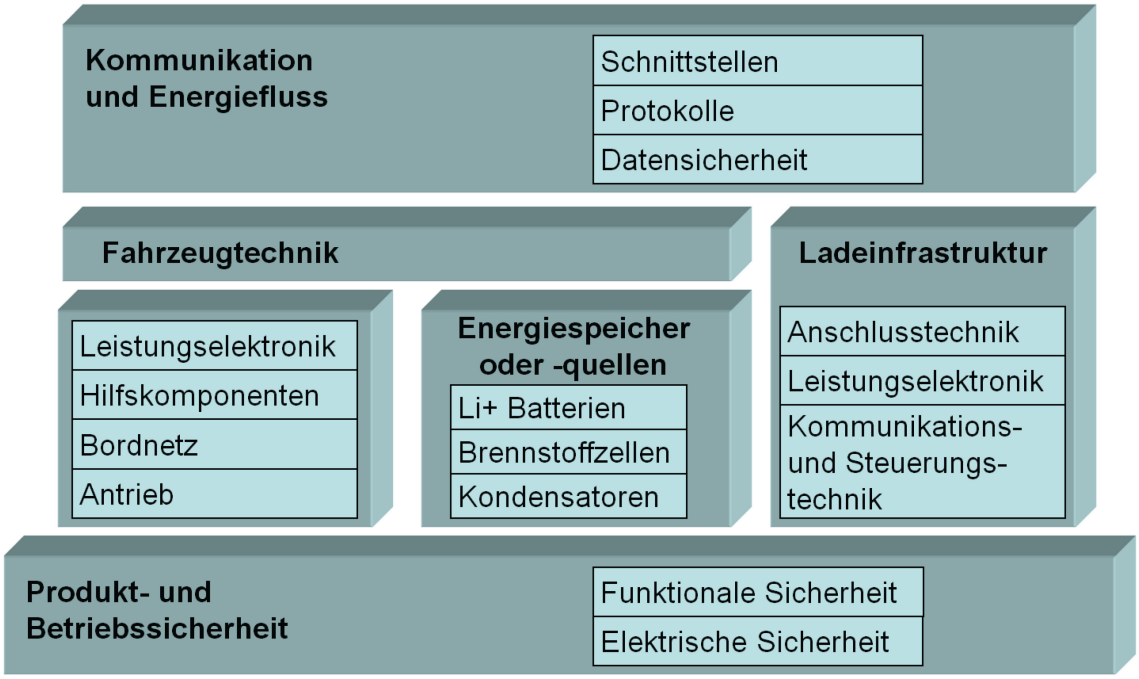


Abbildung 9: Für die Normung relevante Systemkomponenten und Domänen [Quelle: Die deutsche Normungs-Roadmap Elektromobilität – Version 2.0A, DIN/DKE Mai 2013]

5.5.2 aktive Standardisierungsgremien

Folgende Standardisierungsgremien arbeiten derzeit an Normen, die für den Bereich der Elektromobilität hinsichtlich IT-Sicherheit relevant sind:

Organisation	Gremien-bezeichnung	Gremientitel	Arbeitsgebiet
DKE	DKE/AK 901.0.115	Informationssicherheit für Elektromobilität	

5.5.3 Standardisierungsaktivitäten Datensicherheit und Datenschutz

Im Rahmen der Elektromobilität fallen eine ganze Reihe von Informationen an, die an verschiedenen Stellen erfasst und gespeichert sowie über diverse Kommunikationsschnittstellen zwischen den beteiligten Parteien ausgetauscht werden sollen. Der Gewährleistung einer angemessenen Sicherheit dieser Daten und der jeweiligen Datenverarbeitungssysteme und -netze kommt eine hohe Bedeutung zu. Soweit es sich um personenbezogene Daten handelt, ist die Sicherstellung eines umfassenden Datenschutzes gerade für die breite Akzeptanz der Elektromobilität erforderlich. Datensicherheit und Datenschutz stellen Querschnittthemen dar, die über alle Einzelsysteme und

Kommunikationsschnittstellen hinweg behandelt werden müssen. Der essenzielle Charakter dieser Themenfelder und die Vorgaben des nationalen Energiewirtschaftsgesetzes EnWG sind von hoher Bedeutung.

Aufgrund der vielfältigen Kommunikationsschnittstellen zwischen den verschiedenen Systemen sind eine ganze Reihe von Bedrohungen der Informationssicherheit und des Datenschutzes denkbar und zu betrachten. Beispielhaft seien folgende Bedrohungen genannt:

- Angriffe gegen die zentralen Systeme, die der Abwicklung von Energiehandel und Abrechnung dienen, mit dem Ziel der Kompromittierung und Manipulation dieser Systeme.
- Angriffe gegen zentrale Systeme, die der Steuerung der Energienetze dienen, bzw. Angriffe gegen die Smart Grid Infrastruktur mit dem Ziel der Manipulation, insbesondere Störung der Energienetze.
- Angriffe gegen zentrale Systeme, die Servicezwecken dienen (Flottenmanagement, Fahrzeugservice etc.).
- Angriffe gegen die dezentralen Systeme der Ladeinfrastruktur z. B. mit dem Ziel der Manipulation oder des unberechtigten Zugriffs auf Abrechnungsdaten.
- Angriffe gegen Endgeräte in den Fahrzeugen, z. B. Manipulation von Abrechnungsdaten – aber möglicherweise auch zum unberechtigten Zugriff auf Bewegungsdaten des Fahrzeugs.
- Angriffe über fahrzeuginterne Kommunikationsnetze auf hinterlagerte Fahrzeugsysteme (Steuergeräte, Fahrerassistenzsysteme, Kommunikationssysteme, Mehrwertdienste) über die Kommunikationsanbindung zu Ladestationen.
- Verstöße gegen Datenschutzgesetze soweit nicht bereits vorausgehend benannt.

Erfreulicherweise steht im Bereich der Informationssicherheit bereits eine ganze Reihe von international anerkannten und breit angewandten Normen zur Verfügung, die auch im Rahmen der Elektromobilität zur Gewährleistung der Informationssicherheit und des Datenschutzes eingesetzt werden können. Insbesondere sei hier auf die folgenden Normen verwiesen:

• Normenreihe ISO/IEC 270xx Die grundlegende Norm ISO/IEC 27001 beschreibt ein Managementsystem für Informationssicherheit, das allgemein geeignet ist, Informationssicherheitsbelange angemessen zu behandeln und geeignete Maßnahmen zu ergreifen. Die Anwendung dieser Norm ist daher für alle relevanten Bereiche und Betreiber von informationsverarbeitenden Systemen der Elektromobilität zu empfehlen. Darüber hinaus können die im Rahmen der ISO/IEC 27002 beschriebenen Umsetzungsempfehlungen für die Controls der ISO/IEC 27001 direkt auf die Handelsplattformen und kaufmännischen Systeme sowie die hierzu nötigen Kommunikationsnetze und -schnittstellen angewandt werden. Eine darüber hinausgehende Normung scheint uns für diese Bereiche der Elektromobilität nicht erforderlich.

• Sicherung der Kommunikation mit den Energienetz-Steuerungssystemen Zur Sicherung der Kommunikation mit den Steuerungssystemen der Energienetze stehen teilweise bereits Mechanismen innerhalb der hier eingesetzten Kommunikationsprotokolle (insb. IEC 61850) bereit oder werden in zusätzlichen Normen ergänzend definiert (z. B. IEC 62351). Zusätzlich werden im Rahmen der vielfältigen Aktivitäten zur Weiterentwicklung der vorhandenen Energienetze zu „Smart Grids“ die Anwendung und Ergänzung dieser Normen vorangetrieben. Aus Sicherheitssicht sehen wir hier keinen Bedarf für weitergehende Normungsaktivitäten.

• Der technische Report IEC 61850-90-8 beschreibt, wie IEC 61850-7-420 genutzt werden kann, um die wesentlichen Teile der Normen zur E-Mobility (IEC 62196, IEC 61851, IEC 15118) und der IEC 61850-7-420 modelliert werden können. Damit stellen Elektrofahrzeuge eine spezifische Form von DER in der Modellierung dar. Das Dokument beschreibt ein Modell für einen logischen Knoten für Elektrofahrzeuge im Kontext der IEC 61850.

• Die ISO/IEC 15118 spezifiziert ein Kommunikationsprotokoll für das automatische Lastmanagement und automatische Bezahlprozesse im Fahrzeug. Im Wesentlichen beschreibt die ISO 15118 die Kommunikation zwischen Ladeinfrastruktur und Fahrzeug zur Aushandlung eines Ladeprofils und eines dynamischen Ladevorgangs. Darüber hinaus werden noch Dienste für sicheres Bezahlen, Value Added Services und Key Provisioning definiert. Das Thema IT-Sicherheit war von Anfang an Bestandteil dieser Norm, wobei auf bekannte Technologien für den Schutz der ausgetauschten Daten gesetzt wurde: Daher kommen Protokolle wie TLS zum Einsatz auf der Kommunikationsschicht oder aber XML-Security-Maßnahmen auf der Applikationsschicht. Dabei haben vor allem die folgenden Anforderungen Auswirkung auf die Infrastruktur (Secondary Actors):

- Vorgabe der Schlüsselformate (Datenformate, Algorithmen)
- Vorgaben für das Key Provisioning (Generierung von Schlüsselmaterial und auch Revokationsinformation)
- Vorgaben für die signierten Charge Data Records

Die wesentlichen beteiligten Komponenten in der Ladeinfrastrukutur für Plug'n Charge, die nicht Fahrzeug oder Ladesäule sind („Primary Actors"), werden als „Secondary Actors" (Kunde, Ladesäulenbetreiber, Clearing Stelle, Emobility-Provider, Vehicle-to-Grid PKI) in der ISO/IEC 15118 zusammengefasst. Derzeit laufen Arbeiten zur Erweiterung der Norm um auch für induktives Laden anwendbar zu sein. Da hier keine drahtgebundene Kommunikation genutzt wird, sondern auf WLAN gesetzt wird, war eine Neubetrachtung der IT Sicherheit notwendig. Die schon definierten Sicherheitsmechanismen, die oberhalb von TCP/IP angesiedelt sind, sind auch für den Schutz der drahtlosen Kommunikation effektiv. Neu zu beachten ist der in die Ladesäule integrierte Access Point, der generell die Möglichkeit bietet Zugriff auf ein Backend oder das Internet zu bekommen. Hier gibt die derzeit in der Aktualisierung und Erweiterung befindliche Norm Empfehlungen zum Schutz vor Missbrauch insbesondere im Kontext zur Etablierung von Kanälen für die Erbringung von zusätzlichen Diensten (Value Added Service – VAS).

5.5.4 Handlungsbedarfe (Normungsbedarfe)

Ergänzend zu den oben genannten bereits vorhandenen Normen wird speziell für den Bereich der Elektromobilität in folgenden Bereichen Bedarf für weitergehende Normierungsaktivitäten gesehen:

- Sicherung der spezifischen Kommunikationsschnittstellen: Die im Rahmen der Normierungs-aktivitäten zur Elektromobilität festgelegten Kommunikationsschnittstellen sollten über inhärente Sicherungseigenschaften und -mechanismen verfügen. Hierzu gehören z. B. Verfahren zur zuverlässigen Authentifizierung der Kommunikationspartner, zur Sicherstellung der Vertraulichkeit und Integrität der ausgetauschten Daten sowie zur Gewährleistung der Nachvollziehbarkeit von Transaktionen. Relevante Schnittstellen sind z. B. die Kommunikationsschnittstellen zwischen Fahrzeug und Ladestation (IEC 61851-23/24) sowie zwischen Auto und Energienetz (ISO/IEC 15118). Es ist zu prüfen, ob hierzu getrennte Normen entwickelt werden müssen oder ob die Sicherungsmechanismen direkt in der

eigentlichen Norm behandelt werden. Da zur Sicherung der Kommunikationsschnittstellen in der Regel kryptografische Verfahren zum Einsatz kommen, die die Bereitstellung von Schlüsselmaterial für alle Kommunikationspartner erforderlich machen, ist ebenfalls zu prüfen, ob für die Bereitstellung und Verteilung des Schlüsselmaterials an alle Teilnehmer weitergehende Normen erforderlich sind

- Die ISO/IEC 15118 spezifiziert nicht die Absicherung der Kommunikation zwischen Ladesäule und Backend bzw. Grid. Diese Lücke soll im DKE Gremium STD1911.11.5-Informationssicherheit für Elektromobilität bearbeitet und geschlossen werden. Hierbei geht es zum einen, um die Informationssicherheit für den Use Case „Netzintegration der Elektromobilität“. Zum anderen steht die Vereinheitlichung der diversen Rollendefinitionen im Bereich Elektromobilität im Fokus der Arbeiten. Nur durch ein gemeinsames, standardisiertes Rollenverständnis wird es möglich sein, die entsprechenden Kommunikationsbeziehungen zu definieren und entsprechende Schutzmaßnahmen abzuleiten. Aktuell finden Arbeiten zur Entwicklung einer Anwendungsregel zu einer PKI zur Nutzung und Abrechnung von Fahrzeugdiensten statt. Das Gremium AK 901.0.115 „Informationssicherheit für Elektromobilität“ soll dabei als zentraler Ansprechpartner für IT-Sicherheit in der Ladeinfrastruktur fungieren und übergreifenden sowie sektorspezifischen Normungsbedarf ableiten.
- Für die sichere Anbindung der Ladesäulen an das Smart Grid (Backend) werden bestehende und laufende Normungsvorhaben im Bereich der ISO/IEC 15118, IEC 61850 und IEC 62351 einbezogen, ebenso wie die Arbeiten des BSI zum Thema Schutzprofil und Technische Richtlinie (TR3109) für Smart Metering Systeme. Die Definition der Sicherheitseigenschaften von Geräten durch Erstellung so genannter Schutzprofile (Protection Profiles) nach Common Criteria (ISO/IEC 15408) hat sich in vielen Bereichen bewährt. Diese erlauben insbesondere eine neutrale Nachprüfbarkeit und Zertifizierung der Systeme unterschiedlicher Hersteller.

5.6 Smart Home

Ein Smart Home umfasst den privat genutzten Wohn- und Büroinnenraum (im Eigentum / zur Miete; im Mehrfamilienhaus oder Eigenheim; im Bestand und beim Neubau). Das Smart Home umfasst damit auch eine unbegrenzte Entität von Wohnungen mit einer entsprechenden Größe des Gesamtgebäudes (Hochhaus, Wohnblocks), solange der private Bereich tangiert wird und die individuellen Bedürfnisse nach Sicherheit, Komfort und Energieeffizienz der Bewohner befriedigt werden. Hiervon unterscheidet sich das Smart Building als gewerblich genutztes Gebäude. Beim Smart Home steht die Privatperson im Vordergrund. Im Gegensatz dazu wird beim Smart Building das Gebäude in den Fokus gestellt. Die Mechanismen zur Signalisierung sollten dennoch gleich sein. In Band 1 der Studienreihe zur Heimvernetzung des BITKOM (Glasberg & Feldner, 2008) findet sich folgender Definitionsversuch:

Unter den Begriffen Connected Home, Elektronisches Haus, Intelligentes Wohnen, Smart Home, Smart House, etc. verbergen sich eine Reihe von Ansätzen für künftiges Leben, Wohnen und Arbeiten im privaten Wohnbereich. All diesen Begrifflichkeiten gemein ist die Notwendigkeit, den Bewohnern Systeme zur Verfügung zu stellen, die ihre individuellen Bedürfnisse nach Komfort, Sicherheit und Energieeffizienz befriedigen.

Ein Smart Home ist somit mehr als eine Ansammlung einzelner intelligenter Geräte:

1. Die Bedürfnisse der Bewohner/-innen werden durch eine Vielzahl von Sensoren und smarten Geräten erfasst, die eine intuitive Ansteuerung ermöglichen.

2. Die aufgenommenen Informationen werden unter Berücksichtigung des aktuellen Zustandes und der Antizipation potentieller Zustände verarbeitet.

3. Es folgt eine Aktion auf die aufgenommenen Informationen und die darauf basierende Interpretation. Hierzu dient ein ausgereiftes Connected Home Netzwerk, welches ein simples und sicheres Zusammenspiel der Geräte aus den Bereichen der Unterhaltungselektronik (CE), der Informations- und Kommunikationstechnik (IKT), Elektrohaushalt (Herd, Kühlschrank, etc.) und Haustechnik (Alarmanlagen, Heizungs- und Lichtsteuerung, etc.) über Schnittstellen, Software etc. mit Hilfe von drahtgebundenen bzw. drahtlosen Technologien ermöglicht.

In der Vergangenheit wurde das Thema Sicherheit im Smart Home oftmals vernachlässigt, doch auch hier hat sich die Sensibilität für das Thema Sicherheit in den letzten Jahren mit zunehmender Vernetzung deutlich erhöht. Die sichere Erfassung, Speicherung, Verarbeitung und Übermittlung von Daten und Informationen ist mittlerweile eine elementare Voraussetzung für moderne, zukunftssichere und stark vernetzte Smart Home Systeme - vor allem hinsichtlich ihrer Marktakzeptanz. Dabei werden die funktionalen und nicht-funktionalen Anforderungen aus den einzelnen Smart Home Bereichen wie Sicherheit, Komfort, Home Automation, Klima/Heizung/Lüftung, Energiemanagement, oder Ambient Assisted Living (AAL) in enger Zusammenarbeit und Abstimmung mit den jeweils zuständigen Standardisierungs- und Normungsgremien gesammelt und zusammengeführt. Die Anforderungen auf allen Ebenen eines Smart Home Systems, vom einzelnen Sensor bis zum Cloud-Management System mit ihren jeweiligen Anforderungen, sollen berücksichtigt werden.

Für die Normung stellt sich hierbei die Herausforderung, aus den vielen unterschiedlichen Technologien und Insellösungen eine möglichst interoperable und sichere Gesamtlösung zu kreieren, über die ein breites Spektrum von Anwendungsfällen aus Endverbraucher, Hersteller und Service Provider Sicht ermöglicht wird. Die Interoperabilität der unterschiedlichen Technologien im Smart Home soll hierbei über eine Middleware/Gateway-Funktionalität hergestellt werden. Der WAN Schnittstelle dieser Gateways kommt aus IT-Sicherheitsperspektive eine besondere Bedeutung zu, da sie für lokale Geräte eine sichere Möglichkeit bieten muss, um über das WAN zu kommunizieren. In die Sicherheitsbetrachtung sollen schon bestehenden Normen (z. B. aus der Smart Grid Domäne die IEC 62351, ISO/IEC 27002 / TR 27019 und die Ergebnisse der SGIS) einbezogen werden. Besondere Beachtung gilt außerdem den deutschen und europäischen Datenschutzanforderungen da es sich bei Präsenz-, Diagnostischen Daten als auch bei den TV-Sehgewohnheiten um sensitive Informationen handeln kann.

Ziel ist es, einheitliche gruppen- bzw anwendungsspezifische Sicherheitsanforderungen und Normen für alle genannten Produkt- und Anwendungsbereiche im Smart Home zu entwickeln um der Gefahren aus einer zunehmend vernetzten und interoperablen Anwendungswelt adäquat zu begegnen.

Die Anforderung an die gewählten Sicherheitsmechanismen für die Kommunikation innerhalb und außerhalb des Smart Home, orientieren sich an den Grundzielen der Informationssicherheit: Vertraulichkeit, Integrität und Verfügbarkeit, wobei die verschiedenen Anwendungsfälle differenziert zu betrachten sind: Personenbeziehbare Daten stellen beispielsweise eher hohe Anforderungen an

die Vertraulichkeit, während für Safety-relevante Daten die Integrität und Verfügbarkeit der Daten im Fokus steht.

5.6.1 aktive Standardisierungsgremien

Folgende Standardisierungsgremien arbeiten derzeit an Normen, die für den Bereich der Smart Home hinsichtlich IT-Sicherheit relevant sind:

Organisation	Gremien-bezeichnung	Gremientitel	Arbeitsgebiet
DKE	DKE/AK 716.0.1	Normative Beschreibung eines Sicherheitskonzepts für Energiemanagement im Gebäude	
DKE	DKE/AK 713.1.23	Sicherheitstechnik im Smart Home	
DKE	DKE/GUK 715.1	Heim-Elektronik-System (HES)	

5.6.2 Anwendungsregel elektrische Systemtechnik in Heim und Gebäude – IT-Sicherheit und Datenschutz – Anforderungen

Diese Anwendungsregel soll Herstellern, Planern, Errichtern und Prüfstellen Empfehlungen und Richtlinien für die Anforderungen und Schutzniveaus nach aktuellen Stand der Technik bzgl. IT-Sicherheit und Datenschutz von Geräten und Infrastruktur geben. Die hier definierten Schutzniveaus bieten eine Grundlage, um für Geräte und Anwendungsfälle eine differenzierte Sicherheitsbetrachtung durchzuführen und so die anzuwendenden Mindestanforderungen für die IT-Sicherheit und den Datenschutz zu ermitteln. Ziel dieses Dokuments ist es, dem Anwender eine differenzierte Betrachtung der IT-Sicherheitsanforderungen und des Datenschutzes im Heim und Gebäude zu ermöglichen. Daher fokussiert die aktuelle Version hauptsächlich auf die Beschreibung der Anforderungen und stellt diese dem Anwenderkreis zeitnah zur Verfügung, um der zunehmenden Vernetzung im Heim und Gebäude und dem verstärkten Einsatz von Information- und Kommunikationstechnologien gerecht zu werden. In späteren Versionen sollen noch Maßnahmen und weitere Aspekte ergänzt werden. Für diese VDE-Anwendungsregel ist der Arbeitskreis AK716.0.1 „Elektrische Systemtechnik in Heim und Gebäude – IT-Sicherheit“ des Bereichs „Standardisierung“ des VDE zuständig. Es ist geplant diese Anwendungsregel regelmäßig zu aktualisieren, um dem jeweils aktuellen Stand der Technik und etwaigen neuen Bedrohungslagen gerecht zu werden. Zudem sollen in folgenden Versionen auch Maßnahmen und Empfehlungen, bevorzugt auf Basis von existierenden Normen und Standards, für die Erfüllung der Anforderungen definiert werden. Mittelfristig soll es ermöglicht werden einen Konformitätsnachweis zu dieser AR zu erbringen.

5.6.3 Kommunikationssicherheit

Einen Teilaspekt der Informationssicherheit im Smart Home stellt die Kommunikationssicherheit dar, welche die Anforderungen an alle Maßnahmen und Systeme, die den Transport von Daten zwischen zwei Geräten organisieren, beschreibt. Kommunikationssicherheit kann sich dabei sowohl auf Verschlüsselung des Transportwegs als auch auf die Zuverlässigkeit des Transports beziehen. Für die Verschlüsselung des Transportweges gibt es je nach Kommunikationsmedium eine Reihe von

Normen und Standards: Im kabelgebundenen Beim Schlüsselmanagement ist unbedingt darauf zu achten, dass Schlüssel ausgetauscht werden können um im Falle eines Verlustes / Aufdecken des Schlüssels das Kommunikationssystem wieder in einen sicheren Zustand bringen zu können.

Die Zuverlässigkeit der Kommunikation muss folgende Aspekte berücksichtigen:

- Störanfälligkeit der Kommunikation durch erwünschte Teilnehmer
- Störanfälligkeit der Kommunikation durch unerwünschte Teilnehmer
- Maßnahmen zur Informationsübermittlung bei Störung eines Transportweges
- Maßnahmen zur Erkennung und Meldung bei Abbruch einer Kommunikationsverbindung oder Verlust der Kommunikationsmöglichkeit (im Funkbereich werden Verbindungen nur zur direkten Übertragung aufgebaut und anschließend wieder getrennt. Hier muss mittels geeigneter Maßnahmen wie z.B. heartbeats / lifechecks die grundsätzliche Verfügbarkeit regelmäßig überprüft werden).

Je nach Sicherheitslevel und Anwendungsbereich sind dafür entsprechende Maßnahmen zu ergreifen und im Zuge der Weiterentwicklung der Normen im Smart Home zu manifestieren.

Insbesondere müssen bereits erarbeitete Resultate aus der Normung im Bereich der professionellen Brand- und Einbruchstechnik, sowie der Energiebranche und Automatisierungstechnik beachtet und adaptiert (Feinspezifikationen und Profilierung) werden.

5.6.4 Kommunikation über Technologie-Grenzen

Wie bereits erwähnt, ist die Herstellung von Interoperabilität eines der wichtigsten Ziele der Normung und entscheidend für den Erfolg des Smart Home. Für die Auflösung der Technologiegrenzen zwischen den unterschiedlichen Insellösungen muss eine sichere „Übertragungsbrücke“ in Form einer Middleware bzw. eines Gateways realisiert werden, um die sichere Übersetzung zwischen den Technologiedomänen zu gewährleisten. Im Rahmen der Sicherheitsbetrachtung müssen die unterschiedlichen Kommunikationstechnologien für bestimmte Sicherheitsstufen qualifiziert werden. Gerade die Brücke zwischen WAN und LAN muss in der Normung mit großer Sorgfalt betrachtet werden, um das lokale Netz vor Angriffen über die WAN Schnittstelle zu schützen. Beispielsweise gehört die Anbindung an eine Cloud oder einen Service Provider, sowie der Remote Zugriff über das Internet durch den Benutzer auf sein Zuhause zu den Anwendungsfällen, bei denen die WAN Schnittstelle in besonderen Maße abzusichern ist. Für den Remote Zugriff auf das Smart Home, beispielsweise unterwegs über ein Smart Phone, spielt zudem die Ende-zu-Ende Sicherheit ein wichtige Rolle.

5.6.5 Schutzprofil für ein Smart Meter Gateway

[Quelle: Bundesamt für Sicherheit in der Informationstechnik, BSI)

Die zunehmend dezentrale Einspeisung erneuerbarer Energien stellen künftige Energieversorgungssysteme vor eine sehr große Herausforderung. Zum einen erfolgt die Energieeinspeisung durch erneuerbare Energien zu unvorhersehbaren Zeitpunkten, zum anderen können Energieverbräuche zu bestimmten Tageszeiten erhebliche Spitzenlasten erreichen.

Abhilfe sollen nach Vorgabe der Europäischen Union in Zukunft intelligente Netze ("Smart Grids") schaffen, die eine flexiblere und gleichzeitig sichere Energieversorgung ermöglichen können. Im Zuge der Einrichtung solcher Smart Grids kommen beim Verbraucher intelligente Messsysteme (Smart-

Metering-Systeme) zum Einsatz. Durch deren Nutzung erhalten Verbraucher eine höhere Transparenz über den eigenen Energieverbrauch und die Möglichkeit, die Energiekosten über den laufenden Stromverbrauch zu senken.

Aufgrund der Verarbeitung und Zusammenführung personenbezogener Verbrauchsdaten in Messsystemen sowie möglicher negativer Rückwirkungen auf die Energieversorgungssicherheit ergeben sich hohe Anforderungen an den Datenschutz und die Datensicherheit. Bekannt gewordene Hackerangriffe auf intelligente Messsysteme, unter anderem in den USA, und neuere Gefährdungen, wie etwa die Schadsoftware Stuxnet, machen die Notwendigkeit für sichere Lösungen für die Einführung intelligenter Messsysteme in Deutschland deutlich.

In Umsetzung ihres Energiekonzepts wird die Bundesregierung stufenweise für eine intelligente Anbindung von Verbrauchern und Erzeugern an das Energienetz sorgen. Der Anteil der Stromerzeugung aus erneuerbaren Energien soll bis 2020 auf mindestens 35 Prozent und bis 2050 auf mindestens 80 Prozent steigen.

Vor dem Hintergrund der möglichen Bedrohungen hält die Bundesregierung gesetzlich verpflichtende Anforderungen an die Sicherheitsarchitektur von intelligenten Netzen für erforderlich, um sicherzustellen, dass von Anfang an Datenschutz und Datensicherheit gewährleistet werden. Daher wurde das BSI durch das Bundesministerium für Wirtschaft und Technologie im September 2010 mit der Erarbeitung eines Schutzprofils (Protection Profile, PP) sowie im Anschluss einer Technischen Richtlinie (TR-03109) für die Kommunikationseinheit eines intelligenten Messsystems (Smart Meter Gateway) beauftragt, um einen einheitlichen technischen Sicherheitsstandard für alle Marktakteure zu gewährleisten. Sowohl im Energiewirtschaftsgesetz (EnWG), als auch im Energiepaket, das vom Deutschen Bundestag am 30. Juni 2011 beschlossen wurde, sind Schutzprofil und Technische Richtlinie verankert. Das BSI hat seit Anfang 2011 in enger Abstimmung mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), der Physikalisch-Technische Bundesanstalt (PTB) und der Bundesnetzagentur (BNetzA) einen Entwurf zum Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems (Protection Profile for the Gateway of a Smart Metering System) erarbeitet. In mehreren Kommentierungsrunden konnten Verbände aus den Bereichen Telekommunikation, Energie, Informationstechnik, Wohnungswirtschaft und Verbraucherschutz das Schutzprofil umfangreich kommentieren und so an der Weiterentwicklung maßgeblich mitwirken. Seitens der Normung wurden diverse Gremien bei der DKE etabliert, um die nationalen, regulatorischen Anforderungen der Technischen Richtlinie sowohl auf metrologischer Seite als auch im Bereich „Energiemanagement im Smart Home“ mit dem internationalen Normungsaktivitäten in Einklang zu bringen. Diese Arbeiten sind derzeit noch in vollem Gange und von großer Bedeutung. Zum anderen existieren Ansätze in der Normung, das Smart Meter Gateway als Sicherheitsanker in der Liegenschaft zu nutzen, um darüber Mehrwertdienste (z. B. AAL) aus der Smart Home Domäne abzuwickeln.

Aus Sicht des Smart Meter Gateways ist das Smart Home auf Grund seiner inkongruenten Ausprägungen einem unbekannten oder öffentlichen Bereich gleichzusetzen. Die Schnittstelle zwischen Smart Meter Gateway und Smart Home muss daher ähnlich wie die Internet (WAN) Schnittstelle des Smart Meter Gateways abgesichert werden und die Kommunikationsschnittstelle auf unkritische Anwendungsfälle begrenzt werden.

5.6.6 Smart Home und Smart Building

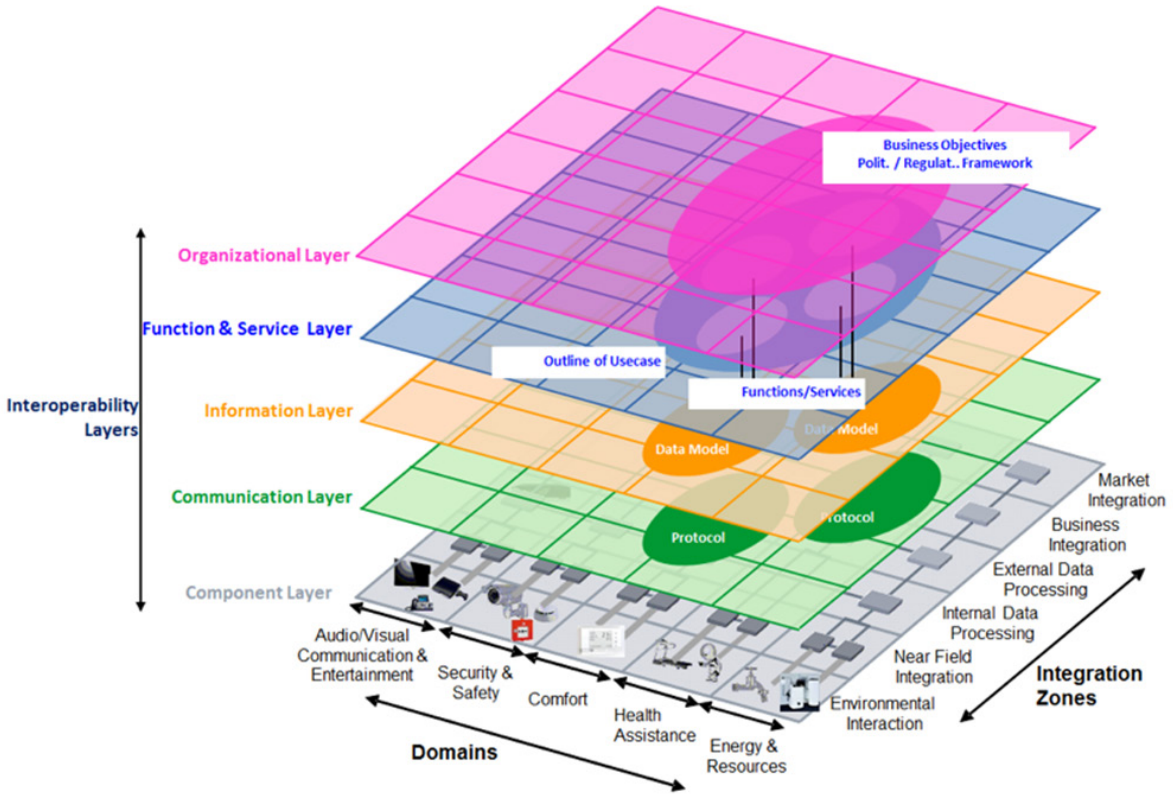
Viele Daten, die im Bereich der Wohnung verarbeitet und gespeichert werden, sind personenbeziehbar bzw. personenbezogen. Um ungewollte Rückschlüsse auf das Verhalten des Bewohners zu vermeiden, ist ein Datenschutzkonzept im Smart Home unerlässlich. Das Prinzip „Privacy-by-Design“ und damit die Vertraulichkeit müssen ein wesentliches Entwurfsziel sein. Dies ist sowohl für die Nutzerakzeptanz als auch durch rechtliche Vorgaben notwendig.

Im Smart Building sind nicht alle Daten personenbeziehbar. D.h. wurde im K901.0.2 in UseCases zwischen UseCases mit Wohnungsbezug und ohne Wohnungsbezug für das Gebäude unterschieden.

Für den privaten Wohnbereich wird – besonders im Zweckbau und Mietwohnungen – die Betriebsführungsverantwortung nicht immer beim Nutzer liegen. Eine Trennung von Nutzer und (Datenschutz-)Verantwortlichem ist daher vorgesehen.

Schutzzonen können die Umgebungsbedingungen beschrieben werden, die als Annahmen in eine Risikoanalyse eingehen. So unterscheidet sich auch die Möglichkeit und die Motivation von Angreifern auf die IT-Sicherheit des Smart Home-Systems. Besonderheit der Anforderungen im Smart Home ist, das Nutzer und Eigentümer (damit Betriebsverantwortlicher) oft identisch sind und Organisatorische Maßnahmen vorrangig auf freiwilliger Basis erfolgen. Allerdings ist dies nicht ausschließlich der Fall, nämlich da nicht wo Dritte eine Betriebsführungsverantwortung übernehmen (z.B. Planer, Errichter, Contractor, Vermieter).

DKE STD1711.0.2 hat hat für den Smart-Home und Building Bereich ein Architektur Framework entwickelt, das an SGAM angelehnt ist.



Es ist geplant dieses Architektur-Framework in der Anwendungsregel des K716.0.1 zur Einordnung der IT-Sicherheits- und Datenschutz Bereiche zu verwenden. So lassen sich Organisatorische Anforderungen und Massnahmen auf dem „Organization Layer“ annordnen, Kommunikationssicherheit auf dem „Communication Layer“ und physische Sicherheit auf dem „Component Layer“. Die Zonen zur Areal-Netz-Bildung (Communication-Layer), Einflussspähre auf Daten (Information-Layer), physische Separation (Component-Layer) wird über Integrations-Zonen abgebildet.Die IT-Sicherheitsbetrachtung in Heim und Gebäude wird dabei in jedem Layer (Organisation/Policy, Service/Funktion, Information, Kommunikation, Log./Phys. Komponenten) durchgeführt.

Dieses Modell soll flexibel genug sein, auch virtualisierte Funktionen (Cloud) unter Datenschutzgesichtspunkten darzustellen und betrachten zu können. Dazu wurden sogenannte Integrationszonen für die Datenverarbeitung eingeführt:

- Umwelt-Interaktionszone (Personen, Sensoren, Aktoren)
- Nahfeld-Zone
- Lokale Zone
- Externe/Ferne Zone
- Unternehmenszone
- Marktzone

Die Nahfeld-Zone kann einer Sensor-nahen Vorverarbeitung entsprechen.

In der Lokalen Zone sind die Daten noch in der direkten Einfluss/Kontrollspähre des Datensubjektes (Wohnung, Gebäude).

So können beispielsweise Anforderungen des Datensubjektes an die Pseudonymisierung/Anonymisierung nach einer Datenintegration und dem Verlassen einer Integrationszone vorgegeben werden.

Im DKE AK 716.0.1 Informationssicherheit im Smart Home und Building wird seit Ende 2014 eine Anwendungsregel erarbeitet, die das Ziel hat die Best Current Practives bei Design, Entwicklung, Inbetriebnahme und Betrieb von vernetzten Komponenten in Heim + Gebäude zu Beschreiben.

Diese Anwendungsregel orientiert sich an der „Threat Landscape for Smart Home and Converged Media“ (ENISA, 2015) und and den Empfehlungen „Security and Resilience of Smart Home Environments“ (ENISA, 2015).

Die Anwendungsregel verwendet die sieben Foundational Requirements und für den SmartHome-Bereich angepasste Security Requirements basierend auf der IEC62443-3-3. Dabei wurden die Security Requirements für Privacy neu aufgenommen.

Im Kontext von Heim und Gebäude werden in Anlehnung an IEC 62443-3-3 vier Schutzniveaus definiert

- SN0: Kein besonderer Schutz gegen Verletzungen der IT-Sicherheit
- SN1: Schutz gegen zufällige und seltene Verletzungen der IT-Sicherheit
- SN2: Schutz gegen absichtliche Verletzungen der IT-Sicherheit durch Angreifer mit durchschnittlichen Kenntnissen öffentlich verfügbaren Informationen
- SN3: Schutz gegen absichtliche Verletzungen der IT-Sicherheit durch Angreifer mit überdurchschnittlichen Kenntnissen und/oder systemspezifischen Kenntnissen

6 aufkommende Normungsfelder

6.1 Ambient Assisted Living - AAL

AAL ist ein sich stetig entwickelndes Thema. Neue Perspektiven, Verantwortlichkeiten und Bedürfnisse werden identifiziert und tragen neben dem heterogenen Umfeld zur Gesamtentwicklung bei. Es ist heute ein hochaktuelles und viel diskutiertes Gebiet mit umfassenden Aktivitäten von der nationalen bis zur europäischen sowie internationalen Ebene. AAL bezeichnet alltagsunterstützende Assistenzlösungen für jedes Alter und jede Umgebung, mit dem Ziel, die Lebensqualität für Menschen in allen Lebensabschnitten und Lebenslagen zu erhöhen. Die Anwendungsbereiche sind sehr vielfältig und generationsübergreifend. Das wiederum bedeutet, dass eine Vielzahl beteiligter Partner aus verschiedenen medizinischen, technologischen, soziologischen, gerontologischen und wirtschaftlichen Bereichen interagieren müssen. Nicht nur das Verständnis unter den Akteuren erfordert gegenseitige Rücksichtnahme. Auch das zwangsweise Interagieren unterschiedlicher Systeme und Komponenten bedarf hoher Anpassungsfähigkeit und vor allem Interoperabilität. Damit einher gehen eine Vielzahl von Spezifikationen, die heute bereits für die Einzelsysteme existent und anwendbar sind.

Das Vorhandensein dieser Spezifikationen allein genügt jedoch noch nicht, um den spezifischen Anforderungen der AAL-Systeme und -produkte gerecht zu werden. Notwendig ist zum Einen, aus den vorhandenen Spezifikationen diejenigen zu identifizieren und auszuwählen, die tatsächlich systemrelevant sind. Zum Anderen gilt es, vorhandene Lücken - insbesondere hinsichtlich der Integration und Interoperabilität der Einzelsysteme, aber auch etwa bezüglich der Ausbildung von Fachkräften und der Qualitätssicherung - zu schließen.

Für die AAL-Umgebung wird eine Infrastruktur benötigt, die sich in vielen Fällen mit der Infrastruktur des Smart Homes überschneidet. G. Demiris et al. bezeichnet das Smart Home als „Residences equipped with technology that enhances safety of patients at home and monitors their health conditions“ (S.88) (G.Demiris et al., Older adults’ attitudes towards and perceptions of “smart home“ technologies: A pilot study, Medical Informatics 29 (2004), 87-94.), was die direkte Verbindung beider Themen verdeutlicht. Aus diesem Grund müssen Absprachen zwischen diesen beiden Domänen erfolgen. Durch geeignete Maßnahmen der Öffentlichkeitsarbeit können zudem Synergien ausgearbeitet werden. Mit Hilfe von Smart Home Technologien finden Sensoren und Aktoren einen Einsatz, um ein höheres Maß an Energieeffizienz, Sicherheit, Komfort und Lebensqualität zu erreichen. Spezifische Anpassung und Nachrüstung der Technik ermöglichen dauerhaft ein höheres Maß an Energieeffizienz, Sicherheit und Komfort. Die Verfügbarkeit mehrerer Technologiekonzepte kann kooperativ vernetzt eingesetzt werden.

Die Verbindung zwischen assistiver Technik und Smart-Home-Anwendungen besteht z. B. in der Anbindung von Sensoren an Entertainment-Anwendungen (z. B. durch Gestensteuerung), um bei Unterstützungsbedarf und eingeschränkter Bewegung das häusliche Umfeld sowie Geräte zu steuern.

Assistive Technologie bezieht sich im Allgemeinen auf diejenige Technik, die es Anwendern ermöglicht, Aufgaben und Bewegungen vereinfacht durchzuführen, die sie ohne diese technischen Geräte nicht oder nur eingeschränkt durchführen könnten. Installierte Sensoren im Haus können Aktivitäten aufzeichnen und gegebenenfalls benötigte Unterstützung anfordern.

Charakteristisch für das AAL-Umfeld ist, dass die Anwendungen nicht nur auf das häusliche Umfeld begrenzt sind, sondern das Umfeld des Betroffenen mit einbeziehen, z. B. wenn dieser mobil ist und

das Haus verlässt. AAL-Methoden dienen damit der Erhöhung der Selbständigkeit, der Sicherheit und somit der Lebensqualität. Auch wenn infolge demografischen Veränderungen die Ausrichtung auf Ältere erforderlich ist, sind doch grundsätzlich alle Generationen angesprochen. So auch junge Familien, die z. B. bei der Beaufsichtigung ihrer Kleinkinder eine IT-technische Unterstützung begrüßen würden.

Der Bedarf für AAL-Entwicklungen ist somit einerseits durch die demografische Entwicklung, andererseits aber durch den steigenden Komfort- und Sicherheitswunsch begründet. Die besonders heterogene Nutzergruppe von AAL- Systemen führt zu einer Vielzahl an funktionalen und nicht-funktionalen Nutzeranforderungen, die von Anfang an berücksichtigt werden müssen. Rechtliche Anforderungen werden vor allem durch Datenschutzgesetze sowie das Medizinproduktegesetz definiert. Die AAL-Funktionen können leicht in entwickelten Smart-Home-Umgebungen zum Einsatz gebracht und hier auch veränderten Bedürfnissen bequem angepasst werden. Da Smart-Home-Technologien und Anwendungen im AAL-Bereich wahrscheinlich schon in naher Zukunft ein besonderes und starkes Marktgeschehen prägen werden, müssen Innovationen in diesen Bereichen heute schon als klare Wettbewerbsvorteil für KMU bewerten werden.

6.1.1 Datenschutz bei AAL

Mit AAL-Technologien und daran gekoppelten AAL-Dienstleistungsangeboten werden viele sensible Daten verarbeitet. Hierzu gehören zum Beispiel Vitalparameterdaten, Daten über soziale Kontakte, häusliche Aktivitäten und Krankheitsdaten. Somit existieren rechtliche Anforderungen u. a. in den Bereichen des Datenschutzes, der informationellen Selbstbestimmung und des Medizinproduktegesetzes. Für einige dieser Bereiche gibt es bereits Gesetze, wie z. B. für die patientenbezogene Datenverarbeitung. Hier sind zunächst die Richtlinien der EU (Richtlinie 95/46/EG,) sowie die nationalen Umsetzungen durch den Bund (Bundesdatenschutzgesetz,) und die Länder (Landesdatenschutzgesetze 1) heranzuziehen. Weitere relevante Gesetze sind unter anderem das Strafgesetzbuch und das Sozialrecht in den relevanten Sozialgesetzbüchern sowie das Grundgesetz. Grundsätze der Datenvermeidung und Datensparsamkeit sind zu berücksichtigen. Außerdem sollte eine Wahlfreiheit zwischen zentraler und dezentraler Speicherung bestehen.

Verdeutlicht werden muss die Unterscheidung zwischen Datenschutz und Datensicherheit. Bereits in der Entwicklungsphase müssen klare Datensicherheitskonzepte festgehalten werden. Des Weiteren ist der Datenschutz in alle Prozesse der Hersteller und Dienstleister zu integrieren.

Weitere Arbeiten auf diesem Feld finden u. a. gerade beim Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein (ULD) statt. Hier wurde die Vorstudie „Juristische Fragen im Bereich altersgerechter Assistenzsysteme“ im Rahmen der Begleitforschung AAL erstell. Anhand abstrahierter Modelle werden die bestehenden Rechtsbeziehungen der Beteiligten identifiziert sowie die Datenflüsse und Verarbeitungsprozesse analysiert und daraus Rechtsfragen abgeleitet. Inwiefern eine Anwendung des MPG für AAL-Systeme und –produkte erforderlich ist, bedarf jedoch noch weiterer Diskussion.

Darüber hinaus werden zurzeit in ISO-Arbeitsgruppen internationale Datenschutzspezifikationen erarbeitet.

Für ein erfolgreiches AAL-Umfeld ist eine hohe Sicherheitsanforderung unabdingbar. Es ist wichtig, sicherheitsrechtliche Fragen bereits im Vorfeld der Entwicklung zu definieren und für eine Sicherheitsarchitektur im AAL-Umfeld zu sorgen.

6.1.2 Entwicklung der AAL-Normungslandschaft im Bereich Informationssicherheit

Im Zuge der Etablierung des System Commitees AAL auf IEC-Ebene wurde bei der DKE das Spiegelgremium K 801 „System Komitee AAL“ gegründet. Nach der konstituierenden Sitzung im Sommer 2015 wurden die Strukturen dieses Gremiums, inklusive aller zugeordneten Arbeitskreise, verabschiedet. Um weiterhin das Querschnittsthema AAL strukturiert bearbeiten zu können und beteiligte Personenkreise entsprechend einzubinden, hat die DKE das ExcellenceCluster AAL gegründet

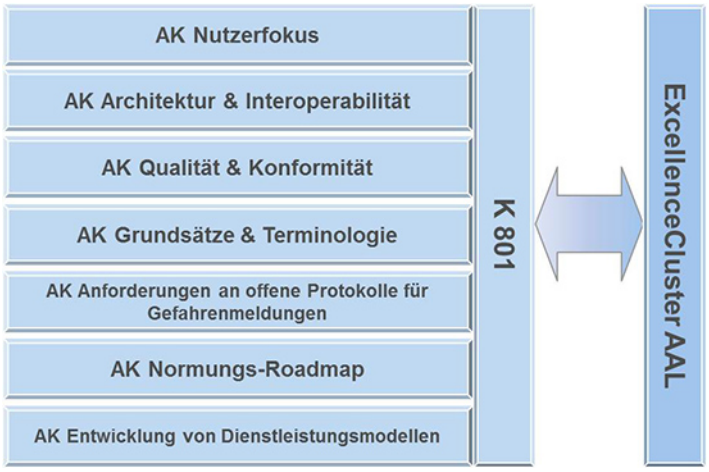


Abbildung 10: Übersicht DKE AAL-Arbeitskreise

Einen weiteren wichtigen Ansatzpunkt im Kontext IT-Sicherheit und Datenschutz stellen auch die Arbeiten des BSI („Bundesamt für Sicherheit in der Informationstechnologie“) zum Thema Smart Metering dar. Das BSI wurde durch das Bundesministerium für Wirtschaft und Technologie im Jahre 2010 mit der Erarbeitung eines Schutzprofils (Protection Profile, PP) sowie im Anschluss einer Technischen Richtlinie (TR) für die Kommunikationseinheit eines intelligenten Messsystems (Smart Meter Gateway) beauftragt, um einen einheitlichen technischen Sicherheitsstandard für alle Marktakteure sicherzustellen. Ausgehend von einer Bedrohungsanalyse für den sicheren und datenschutzfreundlichen Betrieb, legt das Schutzprofil dabei die erforderlichen Mindestsicherheitsanforderungen fest. AAL soll als Mehrwertdienst über diesen Sicherheitsanker in der Liegenschaft geführt werden. Es gilt diesen Ansatz zu untersuchen und die Anforderungen des BSI hinsichtlich der HAN- (Home Area Network) und WAN- (Wide Area Network) Schnittstelle zu berücksichtigen sowie die Ergebnisse normativ zu dokumentieren.

Weiterhin werden aktuell in verschiedenen ISO/IEC-Arbeitsgruppen (wie in JTC1/SC27/WG5) internationale Spezifikationen für den Datenschutz erarbeitet (siehe auch Kapitel 4.1), die auch für AAL von hoher Relevanz sind:

• ISO/IEC 29100 Inormation technology -- Security techniques -- Privacy framework mit der Definition von Datenschutzanforderungen bei der Verarbeitung persönlicher Daten in den Informationssystemen aller Länder,

• ISO/IEC 29101: Eine Datenschutz-Referenzarchitektur (beste Praktiken für konsequente technische Implementierung von Datenschutzprinzipien),

• ISO/IEC 24760-1 Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts, definiert einen Rahmen für das sichere, zuverlässige Datenschutzkonformitäts-Management der Identitätsinformationen

6.2 Smart Cities

Die weltweite Urbanisierung einerseits und die damit verbundene Entleerung ländlicher Regionen anderseits führen zu neuen Herausforderungen an die Struktur-, Angebots- und Ressourcenentwicklung von Siedlungsräumen (in Deutschland und weltweit). Aufgrund neuer, integrativer IT-Lösungen deren Anwendung sich durch alle Lebensbereiche zieht, wurde schnell der Begriff „Smart City“ geboren, unter der Annahme, dass intelligente (vorwiegend IT-unterstützte) Technologien auch in urbanen Lebensräumen für verbesserte Prozesse sorgen. Die Smart City - Diskussion hat sich seither von dieser Beschränkung emanzipiert und bindet weitere Eigenschaften in die Debatten ein; u.a. Bürgerbeteiligung, Nachhaltigkeit, Nutzung des öffentlichen Raums.

Dennoch wird dem Bereich Informationstechnologie eine besondere Rolle zukommen. Durch die IKT-Entwicklung und die damit verbundene Integrationsfähigkeit werden neue intelligente Lösungen in den unterschiedlichen Bereichen durch Verknüpfung von Einzellösungen möglich. Dies führt zu neuen integrierten Technologie-, Service- und/oder Prozesslösungen mit einem hohen Bedarf an das künftige Schnittstellenmanagement.

Das Lenkungsgremium *Smart Cities* veröffentlichte Anfang 2014 eine erste Definition (deutsch/englisch) für den Begriff einer „Smart City“:

„Smart City bezeichnet einen Siedlungsraum, in dem systemisch (ökologisch, sozial und ökonomisch) nachhaltige Produkte, Dienstleistungen, Technologien, Prozesse und Infrastrukturen eingesetzt werden, in der Regel unterstützt durch hochintegrierte und vernetzte Informations- und Kommunikationstechnologien.“

Es gilt dabei, die Chancen dieser Veränderung der breiten Gesellschaft anzubieten, aber gleichzeitig neue Mechanismen für den Schutz der Gesellschaft und der Persönlichkeit zu entwickeln. Das besondere Spannungsfeld dabei, ist die Sicherheit von Daten.

Während eine Weitergabe von Informationen für neue Funktionen unabdingbar wird, muss dennoch dem Anliegen nach Erhalt der Privatsphäre Sorge getragen werden. Dies erfordert ein System mit einem hohen Grad an Privatheit (Privacy), Informationssicherheit (Security) und Funktionssicherheit (Safety) sowie eine hohe Überlebens-, Anpassungs- und Widerstandsfähigkeit (Resilience) und geringe Verletzbarkeit bei Angriffen (Vulnerability). Normungsaktivitäten müssen sich also der Standardisierung grundlegender Sicherheitsmechanismen widmen.

Um die sich daraus ergebenden Chancen für neue Funktionen, Dienste und Geschäftsmodelle nutzbar zu machen, gilt es, neue standardisierte, automatisierte Kommunikationsprozesse bei wichtigen Schnittstellen zwischen Systemen und Infrastrukturen in einem Siedlungsraum zu entwickeln. Um den Risiken dieser Vernetzung entgegenzutreten, die in der potenziellen Verletzung der Privatsphäre auftreten können, die aber auch in einer neuen Form der Angreifbarkeit und Verletzbarkeit von kritischen Infrastrukturen sowie von Einrichtungen durch neue Formen der Cyberkriminalität besteht, sind neue, sichere IT-Architekturen zu definieren.

Die bisherige Praxis von Normungsorganisationen der Themenbehandlung in jeweils zuständigen Normenausschüssen kommt bei Querschnittsthemen wie *Smart Cities* an ihre Grenzen. Diese lassen sich nicht mehr in einzelnen Produkten und Produktgruppen abbilden, sondern stellen komplexe Systeme mit vielen Schnittstellen dar. DIN/DKE haben die natürlichen Grenzen der Normenausschuss-Struktur erkannt und möchten mit den oben dargestellten Gemeinschaftsarbeitskreisen (GAK) neue Diskussionsforen zur Verfügung stellen. Im Besonderen sei

hier der Gemeinschaftsarbeitskreis Sicherheit & Schutz erwähnt, der sich neben den Herausforderungen an die Resilienz von Städten, auch mit Themen der Sicherheit von Kommunikationswegen und Daten beschäftigen wird.

Die Grenzen zwischen den einzelnen Technologiebereichen verschwimmen und können nicht wie bisher in einer vereinfachten Silostruktur dargestellt werden. Bei einer Diskussion über *Smart Cities* beispielsweise müssen allein für neuartige Mobilitätskonzepte unter anderem Architekten, Verkehrsplaner, Stadtplaner, aber auch Hersteller von Telematik Systemen und Fahrzeugen sowie Betreiber von ÖPNV Betreiber an einem Tisch sitzen. Bislang war es möglich, Teile dieser Bereiche weitgehend isoliert voneinander zu betrachten. Um jedoch diese hochkomplexen Themengebiete mit der augenscheinlich wachsenden Anzahl auftretender Schnittstellen – auch im Bereich der Normung – erfolgreich bearbeiten zu können, ist eine systemorientierte Herangehensweise notwendig.

DIN und DKE bemühen sowohl national, als auch international (ISO/IEC) um die Einbringung deutscher Interessen bei diesen systemischen Bemühungen. Weitere Informationen erhalten Sie unter: www.smartcities.din.de

7 Europäische Aktivitäten im Bereich Cybersecurity-Normung

7.1 Cyber Security Focus Group (CSCG)

Seit 2011 existiert ein Beratungsgremium für die obersten Lenkungsgremien von CEN und CENELEC, die Cyber Security Coordination Group (CSCG). Ursprünglich als Beratunggremium für CEn CENLEC und ETSI gegrüdnet ist die CSCG mittlerweile in eine CEN CENELEC Fokus Group umgewandelt worden. Aufgabe der CSCG ist es, die in der Normung vorhandene Expertise zu Cybersecurity zusammen zu bringen, zu bündeln und die Normungsarbeit auf diesem Gebiet durch entsprechende Empfehlungen zu koordinieren. Dabei sollen auch internationale Entwicklungen berücksichtigt werden, indem ein intensiver Informationsaustausch mit außereuropäischen Institutionen angeregt wird. Am 2. April 2014 überreichte eine Delegation der CSCG das erste White Paper mit 9 Empfehlungen zur Standardisierung im Bereich Cybersecurity an die EU-Kommissarin Neelie Kroes. Folgende Empfehlungen wurden darin ausgesprochen:

1. The European Commission (EC) should mandate the CSCG to create a governance framework for the coordination of Cyber Security standardisation within Europe.

2. The EC should establish a clear and common understanding of the scope of Cyber Security, based on an initiative the CSCG plans to launch to clarify the key terms and definitions used in the standardisation of and communication related to Cyber Security within the European Union.

3. The EC should mandate CEN/CENELEC/ETSI to launch an initiative to re-establish the trust of the European citizen in the European digital environment, coordinated by the CSCG and aimed at producing standards to create the most trustworthy environment in the world; this should include privacy and harmonised objectives for education and awareness.

4. The EC should mandate CEN/CENELEC/ETSI to establish an initiative to produce standardised mechanisms for a strong, interoperable, trustworthy and transparent European Public Key Infrastructure and strong cryptographic capabilities for all participants in the European Digital Single Market.

5. The EC should authorise the CSCG to coordinate the standardisation work for a high-level European Cyber Security Label for information and communication technologies (ICT) to protect the European consumer (objective 4 of the EU Cyber Security Strategy).

6. The EC should mandate CEN/CENELEC/ETSI, with the CSCG coordinating appropriate harmonisation with the European regulatory bodies, to extend existing European Cyber Security requirements and evaluation frameworks to ensure adequate Cyber Security throughout the full ICT value chain and to establish an initiative for risk-based standardisation.

7. The EC should authorise the CSCG to create a high-level interface between the CSCG and the European research community to ensure alignment between standardisation and research including industrial research.

8. The EC, with the support of the CSCG, should engage in an industrial forum to harmonise Cyber Security Standards with key international players and stakeholders according to European requirements.

9. The EC, with the support of the CSCG, should launch a targeted global initiative to promote standards appropriate to European requirements for the development of trustworthy ICT products and services as well as Cyber Security solutions.

Erläuterungen und Hintergründe zu den Empfehlungen sind dem White Paper zu entnehmen, welches frei verfügbar ist unter:
http://www.din.de/blob/61520/377b6def0b8679a61c0252b5d1930c52/cscg-white-paper-data.pdf

Die ausgesprochenen Empfehlungen sind grundsätzlicher Natur und sollen die Voraussetzung schaffen, eine effektive, zielgerichtete und harmonisierte Normung im Gebiet Cybersecurity zu ermöglichen. Die Empfehlungen betreffen somit querschnittlich alle auf nationaler Ebene identifizierten und in dieser Roadmap aufgeführten Schwerpunktgebiete.

7.2 ETSI TC Cyber

Eine weitere Entwicklung auf europäischer Ebene, die Auswirkungen auf die IT-Sicherheitsnormung haben wird, ist die Gründung des ETSI TC „Cyber“. Dieses TC bei der europäischen Organisation für die Telekommunikationsnormung (ETSI) soll ETSI Spezifikationen, aber auch EN Normen im Bereich Cybersecurity erarbeiten. Die Aktivitäten des TC Cyber beinhalten die Entwicklung von Normen und Spezifikationen in den folgenden Bereichen:

- Cybersecurity
- Sicherheit von Infrastrukturen, Geräten, Diensten und Protokollen
- Sicherheitshinweise, Leitlinien und operationale Sicherheitsanforderungen für Anwender, Hersteller und Netzwerkinfrastruktur-Betreibern
- Sicherheitswerkzeuge und –techniken zur Sicherstellung von IT-Security
- Erstellung von Sicherheitsspezifikationen und Abgleich mit Arbeiten in anderen ETSI Komitees

8 Kritische Infrastrukturen

Am 17. Dezember 2014 wurde der vom Bundesministerium des Innern eingebrachte Entwurf für ein IT-Sicherheitsgesetz im Bundestag verabschiedet. Es ist am 24. Juli 2015 im Bundesanzeiger veröffentlicht worden und somit ab 25. Juli 2015 in Kraft getreten. In diesem Artikelgesetz wurden u.a das BSI-Gesetz, das Atomgesetz und das Energiewirtschaftsgesetz im Hinblick auf IT-Sicherheit in kritischen Infrastrukturen geändert. Dieses Gesetz hält die Betreiber kritischer Infrastrukturen anhält, branchenspezifische Standards für IT-Sicherheit anzuwenden und z.T. auch durch Zertifizierungen die Einhaltung dieser Standards zu belegen. Am 25.Juli 2015 ist das zuvor vom Deutschen Bundestag beschlossene Gesetz zur Erhöhung der IT-Sicherheit in Kraft getreten. Dieses Gesetz hält die Betreiber kritischer Infrastrukturen dazu an, branchen-spezifische Standards der IT-Sicherheit anzuwenden und auch durch Zertifizierungen die Einhaltung dieser Standards zu belegen. Darüber wird eine Meldepflicht von Sicherheitsvorfällen vorgeschrieben. Die kritischen Infrastrukturen in folgenden Branchen werden durch das Gesetz adressiert:

- Ernährung
- Energie
- Finanz- und Versicherungswesen
- Gesundheit
- Informationstechnik und Telekommunikation
- Medien und Kultur
- Transport und Verkehr
- Wasser

Durch die am 2. Mai 2016 veröffentliche Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz wurden für die Sektoren Energie, Wasser, Ernährung und Informationstechnik und Telekommunikation die Schwellwerte veröffentlich, die die Zuordnung zur Kritischen Infrastruktur bedingen. Jeder Betreiber bzw. Anlage ist selbst verpflichtet zu prüfen, ob eine Zugejhörigkeit zu der

Kritischen Infrastruktur gegeben ist und wenn ja sich zu Registrieren. Die Verordnung für die fehlenden Sektoren soll noch in 2016 kommen.

Im Gesetz werden Mindeststandards und branchenspezifische Sicherheitsstandards zur Anwendung gefordert, bzw. zugelassen und auf den Stand der Technik verwiesen. Zur Beschreibung des Standes der Technik sollte auf bestehende – in der Regel internationale – Normen zurückgegriffen werden. In den adressierten Branchen gibt es zum Teil bereits Strukturen und Normen, die bei der Umsetzung der gesetzlichen Vorgaben zum Einsatz kommen können. Die nachfolgenden Abschnitte geben einen kurzen Überblick. Eine Besonderheit bildet die Energiebranche, da dort die Bundesnetzagentur nach §11a und §11b EnWG getrennt für Energieversorgungsnetze und Energieerzeugungsanlagen je einen Sicherheitskatalog als Mindeststandard veröffentlichen wird, Der für die Netze wurde am 12. August 2015 veröffentlicht und der für die Erzeugungsanlagen wird in 2016 erwartet.

Ernährung

Im Bereich der Ernährung und des Lebensmittelhandels gibt es kein Normungsgremium, welches sich explizit mit dem Thema IT-Sicherheit auseinandersetzt. Auch existieren keine branchenspezifischen IT-Sicherheitsnormen. Da im Lebensmittelhandel hauptsächlich Standard IT-Komponenten zum Einsatz kommen, ist zu vermuten, dass die gängigen generischen IT-Sicherheitsstandards anwendbar sind. Im Bereich der Nahrungsmittelerzeugung könnte von Lösungen aus dem Gebiet der Automatisierungstechnik übernommen werden. Ob branchenspezifische Besonderheiten vorliegen, die bei der IT-Sicherheit berücksichtigt werden müssen, ist noch in einer breiteren Diskussion unter Einbeziehung der interessierten Kreise entlang der Wertschöpfungskette zu klären.

Energie

Gemäß Änderungen des EnWG §11 Absatz 1a und 1b hat die Bundesnetzagentur in Ihrer Rolle als Regulierungsbehörde den Auftrag erhalten, im Benehmen mit dem BSI jeweils einen IT-Sicherheitskatalog für die Netzbetreiber und für die Betreiber von Energie(erzeugungs)anlagen zu erstellen. Der Katalog für die Netzbetreiber liegt bereits vor und beschreibt als eine Kernforderung die Einführung eines Informationssicherheits-Managementsystems (ISMS) gemäß ISO/IEC 27001. Darüber hinaus wird darin gefordert, bei der Implementierung des ISMS die Normen ISO/IEC 27002 und ISO/IEC TR 27019 anzuwenden. Zu bestehenden Gremien und Normen siehe 5.2

Finanz- und Versicherungswesen

Im Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN, dort im Fachbereich 3 befasst sich der Arbeitsausschuss 02 „Bankwesen“ mit der Normung von IT-Sicherheitsaspekten im Banken und Finanzwesen. Dieses Gremium übernimmt auch die Spiegelung des internationalen Gremiums ISO /TC 68/ SC 2 „Sicherheitsaspekte“, welches sich auf internationaler Ebene dieser Thematik annimmt.

Gesundheit

Zu bestehenden Gremien und Normen siehe 4.4

Informationstechnik und Telekommunikation

Im Bereich der IKT gibt es eine Vielzahl von Gremien und Standards. Auf nationaler Ebene ist die Normung im Bereich Telekommunikation bei der DKE angesiedelt, die Grundlagennormung der Informationstechnik im NIA bei DIN. Der Telekommunikationsbereich unterliegt bereits vielfältigen Regulierungen, die teilweise auch im Telemediengesetz festgeschrieben sind. Hingewiesen sei an

dieser Stelle auch auf den IT-Sicherheitskatalog der Bundesnetzagentur, der jedoch nur für den Geltungsbereich des EnWG angewendet werden kann.

Medien und Kultur

In der IT-Sicherheitsnormung sind Besonderheiten der Kultur- und Medienlandschaft bisher wenig diskutiert, dabei hat die Informationstechnik diesen Bereich besonders stark verändert. Informationen werden über „Soziale Netzwerke“ ausgetauscht, Meldungen von unterschiedlichsten Plattformen finden ihren Weg in die Öffentlichkeit und tragen zur Meinungsbildung bei. Manipulierte Meldungen oder Falschmeldungen durch kompromittierte vertrauenswürdige Quellen stellen ernste Gefahren dar. Die informationstechnische Absicherung der Kommunikationskanäle und die Verhinderung von Identitätsdiebstahl muß verstärkt in den Fokus rücken. Die Anwendung bestehender Standards sollte grundlegend analysiert werden, ggf. ist die Entwicklung branchenspezifischer Normen und Standards in einem noch zu gründenden Gremium anzuraten.

Transport und Verkehr

Der Bereich Transport und Verkehr umfasst den Straßen-, Schienen- und Luftverkehr sowie die Schifffahrt. In der Normung sind hier die Normenausschüsse Automobiltechnik, Fahrweg und Schienenfahrzeuge, Luft- und Raumfahrt sowie Schiffs- und Meerestechnik einzubeziehen.

Im Bereich des Luftverkehrs gibt es bereits einen branchenspezifischen Standard, der sich diesem Thema widmet: DIN EN 16495 „Flugverkehrsmanagement - Informationssicherheit für Organisationen im Bereich der Zivilluftfahrt“.

Für elektrische Bahnsignalanlagen wurde bisher der Aspekt der IT-Sicherheit (Security) normativ lediglich in der DIN EN 50159 sowie DIN VDE V 0831-102 behandelt, und zwar dort fast ausschließlich unter dem Gesichtspunkt der Kommunikationssicherheit (für sicherheitsrelevante Systeme im Sinne von Safety). In DIN EN 50126 selbst wird der Aspekt des Schutzes vor „Vandalismus und unvernünftigem menschlichen Handeln“ komplett ausgespart, sowohl in der gültigen Ausgabe als auch im Anwendungsbereich der Revision. In der Praxis hat sich jüngst gezeigt, dass die Verwundbarkeit von IT-Systemen in elektrischen Bahnsignalanlagen gegenüber böswilligen Angriffen möglicherweise unterschätzt wurde. Zwar ist es bisher nur zum Stillstand von Anlagen gekommen, allerdings kann man schwerlich leugnen, dass sich hinter diesen Vorfällen ein größeres Schadenspotenzial verbirgt, zumindest, wenn nicht rechtzeitig vorbeugende Maßnahmen der Gefahrenabwehr ergriffen werden. Bei Bahnsignalanlagen ist neben der Langlebigkeit der Anlagen besonders der Aspekt der flächenhaften Ausdehnung zu berücksichtigen. Derzeit verstärken mehrere Technologietrends und neue Bedrohungsszenarien die Notwendigkeit, dem Thema IT-Sicherheit mehr Aufmerksamkeit als bisher zu widmen:

- auch in Bahnsignalanlagen werden verstärkt handelsübliche Systeme, insb. Betriebssysteme und Übertragungsprotokolle, eingesetzt,
- die Vernetzung der Anwendungen hat stark zugenommen, insbesondere über sog. offene Netze
- in den vergangenen Jahren hat die Anzahl der Angriffe auf IT-Systeme stark zugenommen, insbesondere da Tools für solche Angriffe frei verfügbar sind und ein Markt für entsprechende Aktivitäten entstanden ist,

- die Privatisierung und Öffnung der Märkte hat zu einer komplexeren Situation geführt, insb. bezüglich der Anzahl der beteiligten Partner bzw. Organisationen an den Geschäftsprozessen.

Leider fehlen, von Einzelfällen abgesehen, bisher allgemeine Anforderungen bez. der IT-Sicherheit von elektrischen Bahnsignalanlagen. Ohne diese besteht die Gefahr, dass in Einzelfallentscheidungen unangemessene Anforderungen gestellt werden. Dabei könnten sowohl überhöhte Anforderungen gestellt werden, die die Wirtschaftlichkeit des Eisenbahnbetriebs beeinträchtigen als auch solche, die zumindest zu einer erheblichen Beeinträchtigung des Eisenbahnbetriebs führen können. Eine weitere externe Motivation für die Setzung eines Regelwerks besteht darin, dass das System Eisenbahn eine kritische Infrastruktur darstellt und für diese von verschiedenen Seiten wie z. B. Bundesregierung oder EU Kommission die Forderung nach anwendungsspezifischen IT-Sicherheits-Regelwerken erhoben wurde. Für elektrische Bahnsignalanlagen stellt sich daher die Frage, ob man sich ein eigenes Regelwerk zur IT-Sicherheit geben sollte oder ob man auf vorhandene Regelwerke aufsetzen kann. Erste Untersuchungen haben gezeigt, dass sich insbesondere mit dem Regelwerk der Industrieautomatisierung, das parallel in der IEC 62443 genormt wird, ein hoher Überdeckungsgrad ergibt. Daher soll nicht eine eigenständige Vorgehensweise zur IT-Sicherheit für elektrische Bahnsignalanlagen erstellt werden, sondern die Vorgehensweise nach IEC 62443 soll in die bereits etablierten Regelwerke wie DIN EN 50129 oder EU VO 402/2013 integriert werden. Im Sinne dieser Vorgehensweise wurde DIN VDE V 0831-104 „Elektrische Bahn-Signalanlagen - Leitfaden für die IT-Sicherheit auf Grundlage IEC 62443“ entwickelt. Diese Vornorm stellt einen Leitfaden zur Anwendung der IT-Sicherheit nach IEC 62443 für elektrische Bahnsignalanlagen bereit.

Wasser

Die Struktur der Wasserversorgung weist große Ähnlichkeiten mit der Energieversorgung auf. Der Bundesverband der Energie- und Wasserwirtschaft hat das der ISO/IEC TR 27019 zugrunde liegende BDEW White Paper bereit 2008 veröffentlicht. Es wäre daher zu prüfen, ob ISO/IEC TR 27019 auch im Bereich der Wasserwirtschaft anwendbar ist.

9 Fazit

Die Darstellung der Normungsaktivitäten in den Schwerpunktbereichen zeigt, dass an vielen Stellen Normen und Standards zu den Themen entwickelt werden und die Bereiche normungstechnisch, mit aktiven Gremien und einer funktionierenden Normungsinfrastruktur gut abgedeckt sind. Ein genauer Blick auf die Standards zeigt aber auch, dass der Anteil an gemeinsam, also von verschiedenen Bereichen, genutzten Standards weiterhin relativ gering ist, obwohl der Gegenstand, die Übertragung von Informationen, in allen Bereichen derselbe ist. Dies ist einerseits zwar den speziellen Anforderungen der Bereiche geschuldet, könnte aber auch ein Indikator für eine unklare bzw. ungenügende Trennung von generischen und bereichsspezifischen Aspekten in der Normung sein. Bei einer Wiederholung geneischer Aspekte in den bereichsspezifischen Normen steigt aber die Gefahr von Widersprüchen. Die Heterogenität der Normungslandschaften macht eine IT-Sicherheitstechnische Bewertung zudem schwierig. Dem wird entgegengehalten, das eine unterschiedliche Systemarchitektur in den Bereichen sicherheitserhöhend wirkt, da die Wahrscheinlichkeit, dass ein Schwachpunkt in der Systemkette gleich mehrere Bereiche gefährden würde minimiert wird. Diese gegenläufigen Wirkmechanismen bedürfen einer genaueren

Untersuchung um daraus Schlussfolgerungen für die zukünftige Aufstellung der Normung im Bereich IT-Sicherheit ziehen zu können. Diese Diskussion wird von der Koordinierungsstelle IT-Sicherheit weiter verfolgt und aktiv vorangetrieben werden.

Ein weiteres zukünftiges Handlungsfeld ist die frühzeitige Einbindung der IT-Sicherheit in die Normung bei neuen Themengebieten. Das Stichwort heißt hier Security by Design. Es muss verstärkt darauf geachtet werden, dass neue Bereiche von den Erfahrungen und Vorarbeiten auf dem Gebiet der IT-Sicherheitsstandardisierung profitieren und Kompatibilität zu bestehenden Sicherheitslösungen hergestellt wird, dies alleine schon aus wirtschaftlichen Gesichtspunkten. Die KITS wird sich daher weiter bemühen, Vertreter aus den verschiedenen Bereichen frühzeitig zusammen zu bringen.

Die auf europäischer Ebene neu geschaffenen regulatorischen Rahmenbedingungen werden auch Einfluss auf die zukünftige Normungsarbeit haben. Europäische Verordnungen wie die Datenschutzgrundverordnung bleiben in ihren Regelungsvorgaben zumeist allgemein, hier bietet sich für die Normung vielfache Möglichkeit, die Verordnungsinhalte zu konkretisieren und als Umsetzungshilfe zur Erfüllung gesetzlicher Vorgaben zu dienen. Eine koordinierte Aktivität, einen auf Normen basierten Umsetzungsleitfaden zu erstellen sollte hierbei angeregt werden.