Moderne Energieverteilnetze: Bedrohungen und Gegenmaßnahmen

Carl-Heinz Genzel · Olav Hoffmann · Richard Sethmann

Hochschule Bremen
{carl-heinz.genzel | olav.hoffmann | richard.sethmann}@hs-bremen.de

Zusammenfassung

Das traditionelle deutsche Stromnetz befindet sich im Wandel. Intelligente, vernetzte Steuerungssysteme sollen traditionelle, lokale Steuerungssysteme ersetzen, um verschiedene Herausforderungen in der Netzsteuerung zu kompensieren. Hieraus entstehen neue Anforderungen an die Informationssicherheit von Energieverteilnetzen. Im Forschungsprojekt „Systemsicherheit von Energieversorgungsnetzen bei Einbindung von Informations- und Kommunikationstechnologien“ (SEnCom) wurde deshalb die Informationssicherheit in Energieverteilnetzen der nahen Zukunft untersucht, um mögliche Defizite aufzudecken und Gegenmaßnahmen zu erarbeiten. Diese Veröffentlichung stellt eine Bedrohungsanalyse für dezentrale Standorte in Energieverteilnetzen vor und gibt den Stand der Technik hinsichtlich der Informationssicherheit mit Hilfe bestehender Standards wieder. Auf dieser Basis werden ausgewählte Gegenmaßnahmen für entdeckte Bedrohungen erläutert. Energienetzakteure sollen ermutigt werden, proaktiver mit dem Thema der Informationssicherheit umzugehen.

1 Einleitung

Das traditionelle deutsche Stromnetz (s. Abbildung 1 „Alt“) ist hierarchisch aufgebaut und zentralistisch strukturiert. Elektrizität wird durch Großkraftwerke produziert und an Verbraucher weitergegeben. Das Stromnetz besteht hierfür aus zwei Netzbereichen und vier darin verorteten Spannungsebenen. Der Bereich „Übertragungsnetz“ ist zum Transport des Stroms über große Strecken ausgelegt. Hier befindet sich die höchste Spannungsebene mit 220 kV oder 380 kV. Der Bereich „Verteilnetz“ dient zur Verteilung der Energie vom Übertragungsnetz zum Verbraucher, je nach Energiebedarf. Hieraus ergeben sich drei Spannungsebenen. Die erste Ebene ist die Hochspannung mit 60 kV bis 110 kV. Die zweite Ebene ist die Mittelspannung zwischen 6 kV und 30 kV. Zuletzt kommt die Niederspannung mit 230 V und 400 V.

Diese Hierarchie befindet sich seit der Etablierung von erneuerbaren Energiequellen im Wandel. Erneuerbare Energiequellen werden weitestgehend mit Hilfe dezentraler Energieerzeugungsanlage (DEA) erschlossen und sind aufgrund ihrer Lage häufig an das Verteilnetz angebunden. Hierdurch findet eine teilweise Umkehr der Energieflüsse statt (s. Abbildung 1 „Neu“). Die Energie wird nicht mehr ausschließlich von höheren auf niedrigere Spannungsebenen, sondern in beide Richtungen verteilt. Hieraus entsteht ein dezentrales, bidirektionales Energieversorgungssystem. Das Verteilnetz ist für die hierdurch entstehende Netzlast jedoch nicht flächendeckend ausgelegt. Darüber hinaus sind erneuerbare Energiequellen wie Wind oder Sonne nicht so verlässlich wie traditionelle Energiequellen (z.B. Kohle oder Gas). Dies führt zu einer schwankenden Energieerzeugung im Verteilnetz. Zur Kompensation dieser Herausforderungen

P. Schartner · A. Baumann (Hrsg.) · D•A•CH Security 2017 · syssec (2017) 181-192.

sollen intelligente Steuerungssysteme traditionelle, lokale Steuerungssysteme ersetzen. Intelligente Steuerungssysteme sind im Gegensatz zu den traditionellen Steuerungssystemen miteinander vernetzt, um Informationen über den Netzzustand auszutauschen und autonom, im Sinne des gesamten Energienetzes, handeln zu können. Hierzu wird unter anderem der Ansatz verfolgt, standardisierte Hardware und Software aus der traditionellen Informations- und Kommunikationstechnologie (IKT) für intelligente Steuerungssysteme zu adaptieren, um ein robustes, intelligentes Energienetz zu ermöglich.

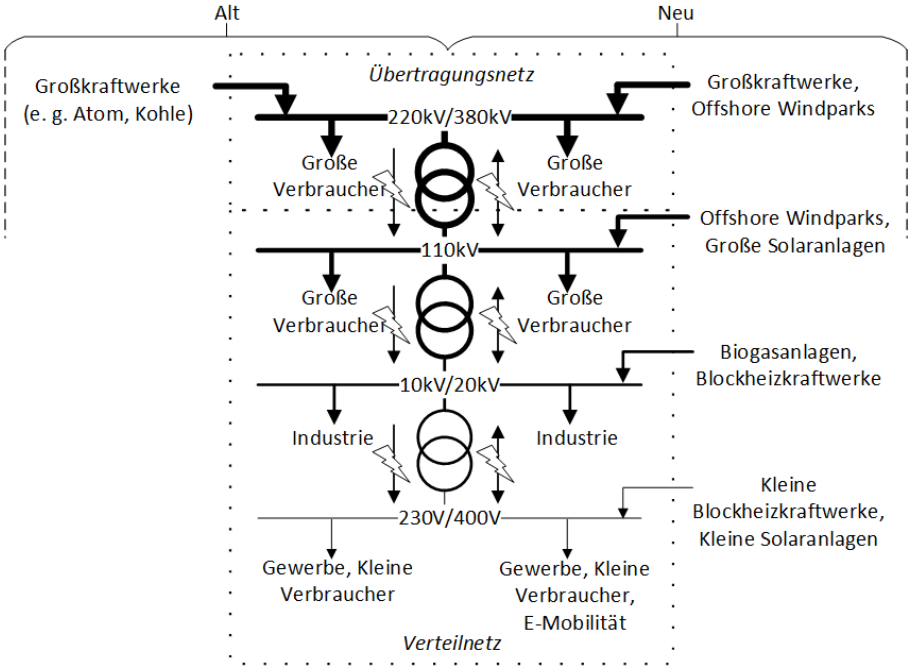

Abb. 1: Struktur des Energienetzes – Alt und Neu

Daraus entstehen neue Anforderungen an die Informationssicherheit von Energienetzen, insbesondere bei Verteilnetzen. Das Energienetz der Zukunft wird aus vielen Endpunkten bestehen, die zum Teil über öffentliche Kommunikationsnetze miteinander verbunden sind, so dass Bedrohungen aus der traditionellen IKT auch für Steuerungssysteme im Energienetz von Bedeutung sein werden. Erste Vorfälle in diesem Zusammenhang, wie der Angriff auf ein Verteilnetz in der Ukraine [LeAC16], sind bereits bekannt. Im Forschungsprojekt SEnCom wurde deshalb die Informationssicherheit in Verteilnetzen der nahen Zukunft untersucht, um mögliche Defizite aufzudecken und Gegenmaßnahmen zu erarbeiten. Die traditionellen Leitsysteme zur Steuerung eines Energienetzes wurden dabei als relativ sicher eingestuft. Der Fokus des Forschungsprojektes lag stattdessen auf den dezentralen Standorten in einem Verteilnetz. Im Folgenden wird hierzu eine Bedrohungsanalyse für dezentrale Standorte vorgestellt. Zu Beginn wird eine exemplarische Architektur für ein Verteilnetz in naher Zukunft als Anwendungsbereich definiert. Danach werden das Vorgehen und die Erkenntnisse aus der Bedrohungsanalyse vorgestellt. Auf dieser Basis werden Einblicke in den Stand der Wissenschaft und Technik zum Schutz von intelligenten Steuerungssystemen im Energienetz mit Hilfe aktueller Standards, Richtlinien und Empfehlungen eingeführt, bevor einzelne ausgewählte Gegenmaßnahmen für entdeckte Bedrohungen erläutert werden. Hierbei sollen Energienetzakteure dazu ermutigt werden, proaktiver mit dem Thema Informationssicherheit umzugehen.

2 Energieverteilnetz in naher Zukunft

Die zukünftigen Ausprägungen der Verteilnetze sind derzeit noch nicht eindeutig abzusehen. Es sind jedoch Rückschlüsse auf die Gestaltung durch bestehende Forschungsprojekte und politische Entwicklungen möglich. Im Forschungsprojekt SEnCom wurde hierzu eine Topologie für ein Verteilnetz in naher Zukunft erstellt. Diese Topologie besteht aus fünf zentralen Elementen, die in Abbildung 2 schematisch, mit Bezug auf die hierarchischen Managementebenen (Zonen) des Smart Grid Architecture Model (SGAM) [CoCE12], dargestellt werden. Die niedrigste Ebene im SGAM ist die Prozessebene (Process). Diese Ebene enthält Komponenten, die direkt an der physikalischen, chemischen oder räumlichen Veränderung von Energie beteiligt sind. In der Feldebene (Field) werden Komponenten zum Schutz, zur Steuerung und zur Überwachung der Prozesse auf der Prozessebene eingeordnet. Über der Feldebene liegt die Stationsebene (Station). Dort befinden sich die Komponenten zur Aggregation von Funktionen und zur Konzentration von Daten für die Verwaltung der tieferen Ebenen. Die darauffolgende Betriebsebene (Operation) umfasst die Komponenten zur Steuerung übergreifender Prozesse in einem Energienetz. Auf der Unternehmensebene (Enterprise) befinden sich Komponenten für organisatorische und wirtschaftliche Aufgaben. Die Marktebene ist die höchste Ebene und vereint Marktfunktionen, wie den Energiehandel. Sie ist nicht Teil des Anwendungsbereichs von SEnCom und daher in Abbildung 2 nicht dargestellt.

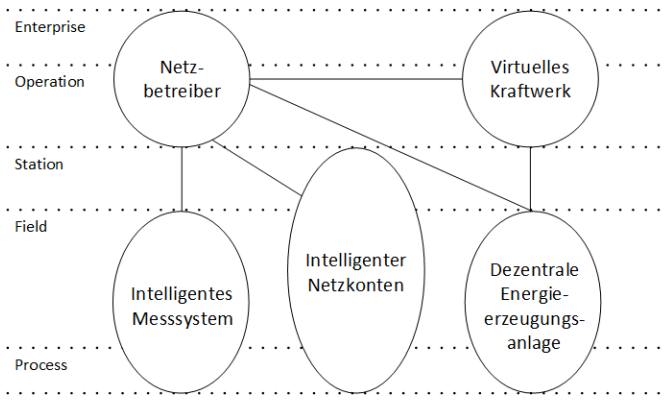

Abb. 2: Komponenten eines Energieverteilnetzes in naher Zukunft im Fokus von SEnCom

Das erste zentrale Element eines Verteilnetzes in naher Zukunft aus Abbildung 2 ist der Verteilnetzbetreiber (VNB), der mit Hilfe eines Leitsystems das Verteilnetz mit seinen Systemen im Feld steuert und überwacht. Er unterhält hierzu auch die notwendige IKT zur Anbindung der einzelnen Systeme im Feld und beschäftigt das benötigte Personal, wie das Bedienpersonal des Leitsystems, das Personal für die Administration der IKT und das Personal für die Integration und Instandhaltung der Systeme im Feld. VNB sind im Energienetz nicht neu, sie bilden jedoch die Basis für zukünftige intelligente Energienetze.

Ein wesentliches Element zur Kontrolle eines Verteilnetzes sind intelligente Netzknoten. Netzknoten enthalten die Systeme im Feld und sind für den Betrieb und die Überwachung des Verteilnetzes mit dem Leitsystem eines VNB verbunden. Ein Netzknoten stellt dabei für gewöhnlich die Grenze zwischen zwei Spannungsebenen dar und enthält die notwendigen Systeme für die Spannungskontrolle, wie z.B. Transformatoren. Während Netzknoten in der Vergangenheit insbesondere für eine lokal eingeschränkte Funktionalität ausgelegt waren, werden zukünftige Netzknoten stärker vernetzt, um intelligente und netzübergreifende Regelungsfunktionen zu ermöglichen.

Ein VNB ist neben den Netzknoten auch an der Steuerung und Überwachung von DEA beteiligt, da DEA die Stabilität eines Verteilnetzes beeinflussen können. Eine DEA ist hierfür ebenfalls mit dem Leitsystem eines VNB verbunden, so dass sie im Sinne der Netzstabilität gesteuert und überwacht werden kann. DEA sind hierbei keine neuen Komponenten im Verteilnetz, sie werden jedoch intelligenter. Dies liegt unter anderem daran, dass der VNB nicht die einzige Partei ist, die eine DEA kontrollieren kann.

Virtuelle Kraftwerke (VKW) entstehen aus der logischen Verknüpfung einzelner DEA mit Hilfe von IKT zu einem Anlagenverbund. Hierbei sollen die Nachteile einzelner erneuerbarer Energiequellen durch eine Kombination unterschiedlicher DEA kompensiert werden (z.B. wetterabhängiges Fotovoltaik mit kontrollierbaren Biogasanlagen). VKW gehören zu den innovativsten Komponenten in einem zukünftigen Verteilnetz. Die Aufgaben des Betreibers sind jedoch vergleichbar mit den Aufgaben eines VNB. VKW besitzen ebenfalls ein Leitsystem, das zum Betrieb und zur Überwachung informationstechnisch mit den DEA verbunden ist. Zudem muss auch entsprechendes Personal, wie das Bedienpersonal des Leitsystems, das Personal für die Administration der IKT und das Personal für die Integration und Instandhaltung der Systeme im Feld vorhanden sein.

Die fünfte, bedeutende Komponente in einem zukünftigen Verteilnetz ist das intelligente Messsystem. Es wird davon ausgegangen, dass ein intelligentes Messsystem neue Anwendungen ermöglicht, die es dem VNB sowie weiteren Energieakteuren erlauben, auf Bereiche des Verbrauchers zuzugreifen und einzelne Komponenten aus der Ferne zu steuern und zu verwalten. Batterien eines Elektrofahrzeugs beim Verbraucher könnten zum Beispiel durch den VNB gesteuert werden, um Unterschiede zwischen Energieerzeugung und -verbrauch zu kompensieren.

3 Bedrohungsanalyse

Auf der Basis der fünf identifizierten Elemente eines Verteilnetzes in naher Zukunft wurde im Forschungsprojekt SEnCom eine Bedrohungsanalyse durchgeführt. Hierzu wurde der Ansatz des Open Web Application Security Project (OWASP) zum Modellieren von Bedrohungen in Anwendungen adaptiert [Open17]. Dieser Ansatz basiert auf der STRIDE-Methode von Microsoft und kann auch für die Modellierung von Bedrohungen in Infrastrukturen eingesetzt werden [Micr09]. Bei dieser Methode werden Bedrohungen mit Hilfe der sechs Bedrohungskategorien „**S**poofing“, „**T**ampering“, „**R**epudiation“, „**I**nformation Disclosure“, „**D**enial of Service“ und „**E**levation of Privilege“ untersucht. STRIDE wurde zudem bereits in früheren Forschungsprojekten zum intelligenten Messsystem erfolgreich eingesetzt [DGSH14]. Die Vorgehensweise bei der Analyse sieht wie folgt aus:

1. Definition eines Anwendungsbereichs (auch „Scope“) für die Analyse
2. Datenflussmodellbildung auf Basis des Verteilnetzes in naher Zukunft
3. Qualitative Bedrohungsanalyse mit Hilfe des Modells und informellen Methoden
4. Orientierung, Identifizierung und Klassifizierung von Bedrohungen mittels STRIDE
5. Validierung durch bekannte Bedrohungsanalysen für das Energienetz (z.B. [Euro13a])

Im Folgenden werden der Anwendungsbereich, wichtige Bedingungen und die Erkenntnisse dieser Analyse näher erläutert.

3.1 Anwendungsbereich

Nicht für alle definierten Elemente eines Energienetzes in naher Zukunft entstehen neue Bedrohungen, die mit dem zunehmenden Einsatz von IKT zusammenhängen. Die Leitsysteme eines VNB sowie eines VKW basieren zum größten Teil auf traditioneller IKT, die bereits durch allgemeine Informationssicherheitsstandards abgedeckt wird (z.B. [Deut15]). Stattdessen wurden dezentrale Standorte, wie Netzknoten und DEA, als Elemente identifiziert, die primär von Veränderungen durch intelligente, vernetzte Systeme betroffen sind und bisher noch nicht ausführlich betrachtet wurden. Intelligente Messsysteme wurden dagegen im Sinne des „Security by Design“ durch das BSI mitgestaltet [Bund13b] und durch die Forschung bereits weiterführend mit Bezug zur Informationssicherheit untersucht [DGHS14]. Der Anwendungsbereich für die Bedrohungsanalyse bezieht sich deshalb vor allem auf dezentrale Standorte. Hierzu wurde ein Datenflussmodell auf der Basis einschlägiger Standards und Richtlinien sowie bestehenden Erfahrungen aus realen Verteilnetzen erstellt (s. Abbildung 3).

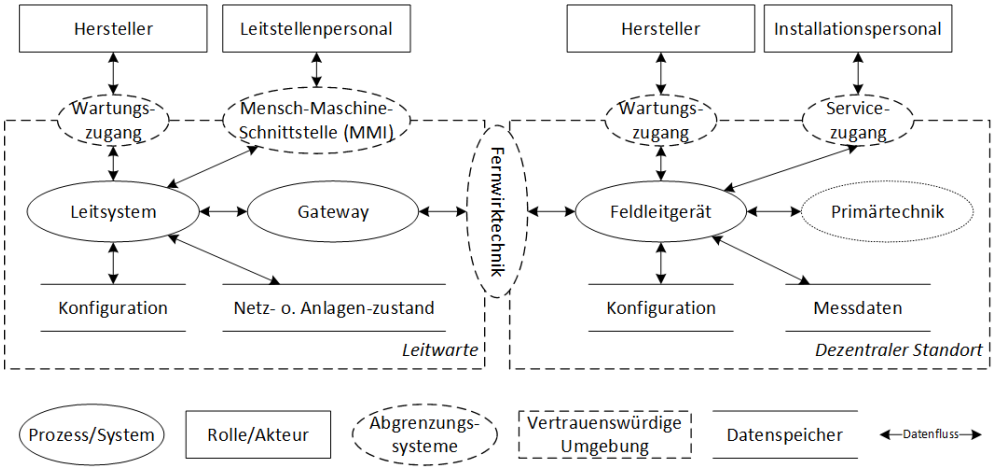

Abb. 3: Datenflussmodell für dezentrale Standorte

Ein dezentraler Standort besitzt demnach eine aufgabenspezifische Primärtechnik, die zur Energietransformation und -weitergabe eingesetzt wird. Die Primärtechnik wird durch ein Feldleitgerät im dezentralen Standort gesteuert und überwacht. Hierzu besitzt das Feldleitgerät entsprechende Konfigurations- und Messdaten. Mit Hilfe der Fernwirktechnik wird die Anbindung an ein Leitsystem umgesetzt, sodass Messdaten von dem Leitsystem abgerufen und Konfigurationsdaten zum Feldleitgerät, unter anderem zur Steuerung, gesendet werden können. Da ein Feldleitgerät und die dazugehörige Primärtechnik üblicherweise in einem klar abgegrenzten Bereich lokalisiert sind (z.B. Raum oder Gebäude), wird davon ausgegangen, dass sich die Komponenten in einem gemeinsamen Vertrauensbereich befinden. Die Fernwirktechnik bildet aus Sicht der IKT die Grenze zu diesem Bereich und dient als logischer Zugangspunkt. Bei dem Vertrauensbereich des dezentralen Standorts wird immer davon ausgegangen, dass dieser weniger vertrauenswürdig ist, als der ebenfalls in Abbildung 3 dargestellte Vertrauensbereich einer Leitwarte mit dem abstrakt dargestellten Leitsystem und einem Gateway zur Übersetzung unterschiedlicher Kommunikationsprotokolle der dezentralen Systeme. Das Leitsystem dient zur Überwachung und Steuerung aller dezentralen Standorte in dessen Aufgabenbereich. Es erfasst hierzu mit Hilfe der dezentralen Messdaten den Zustand eines Netzes (VNB) oder der verwalteten DEA (VKW). Das Leitsystem besitzt zudem Konfigurationsdaten zur übergeordneten Steuerung und zur Anbindung der einzelnen dezentralen Systeme.

Aus Sicht der IKT können verschiedene Rollen aus anderen Vertrauensbereichen über entsprechende Zugangspunkte auf die Komponenten in der Leitwarte und eines dezentralen Standorts zugreifen. Hierzu gehören die Hersteller der eingesetzten Komponenten (Wartungszugang), das Installationspersonal für dezentrale Standorte (Servicezugang) und das Bedienpersonal des Leitsystems (Fernwirktechnik und Mensch-Maschine-Schnittstelle). Es gibt zudem Administratoren, die alle Systeme konfigurieren können. Sie sind in Abbildung 3 nicht dargestellt, um die Lesbarkeit zu verbessern. Administratoren sind für die Konfiguration der dargestellten Systeme inklusive der Abgrenzungssysteme, aber nicht für die Primärtechnik, verantwortlich. Der Zugriff der Administratoren erfolgt dabei aus der vertrauenswürdigen Umgebung der Leitwarte heraus.

3.2 Einschränkungen

Eine Bedrohungsanalyse kann sehr komplex sein, da viele unterschiedliche Komponenten, wie Systeme, Anwendungen, Daten und Benutzer, betrachtet werden müssen. Ein erfolgreicher Angriff kann somit aus diversen Exploits und Sicherheitslücken bestehen. Daher ist es sinnvoll, Rahmenbedingungen zu formulieren, um eine zielgerichtete Analyse zu erreichen.

Die Bedrohungsanalyse soll sich, in Anlehnung an die Gefährdungskategorien aus dem IT-Grundschutz des BSI [Bund08], auf Gefährdungen aus den Kategorien „Vorsätzliche Handlungen“ und „Technisches Versagen“ fokussieren, da angenommen wird, dass die Konvergenz von Energietechnik und IKT in der Verteilnetzebene zu neuen technischen Risiken führt. Die Kategorie „Höhere Gewalt“ liegt dagegen nicht im Fokus, da diese Gefahren unabhängig von den technischen Veränderungen existieren. Zudem wurden die Kategorien „Organisatorische Mängel“ und „Menschliche Fehlhandlungen“ ausgeschlossen, da die Gefahren dieser Kategorien durch den neu eingeführten IT-Sicherheitskatalog (IT-SiKa) [Bund15b] und der damit verpflichtenden Zertifizierung nach ISO/IEC 27001 abgedeckt werden können.

Der Schwerpunkt der Bedrohungsanalyse bezieht sich dabei auf dezentrale Standorte mit dem Fokus auf Bedrohungen an den Außengrenzen und den dort vorhandenen Schnittstellen. Hierzu stehen Angriffe im Mittelpunkt, die das Ziel verfolgen, unerlaubt in die vertrauenswürdige Umgebung eines dezentralen Standortes einzudringen, da ein erfolgreicher Angriff meist mit dem unberechtigten Zugang zu vorhandenen Systemen beginnt. Obwohl dieser Ansatz nicht alle möglichen Angriffspfade betrachtet, kann hierdurch ein wesentlicher Sicherheitsgewinn, bei gleichzeitiger Reduzierung der Analysekomplexität, erreicht werden.

Um die Auflistung trivialer, leicht zu verhindernder Angriffe zu vermeiden, werden zudem folgenden grundlegenden Bedingungen für die Sicherheit eines dezentralen Standorts angenommen. Die eingesetzten Systeme müssen auf dem aktuellen Stand sein und aktiv verwaltet werden. Darüber hinaus müssen Administratoren und Hersteller mit einem privilegierten Zugang zu einzelnen Systemen vertrauenswürdig sein. Hersteller müssen außerdem mindestens die gleichen Sicherheitsanforderungen erfüllen, wie die Umgebungen, auf die sie zugreifen möchten. Zudem muss jeder Zugriff durch einen Hersteller immer von einer für die jeweilige Umgebung verantwortlichen Person explizit erlaubt werden. Dezentralisierte Standorte müssen außerdem zumindest physisch von ihrer Umwelt, z.B. durch Zäune, Gebäude, Räume oder Schränke getrennt sein, so dass der lokale Servicezugang auch nur lokal erreicht werden kann. Angriffe in Form von physischer Gewalt sind zudem nicht Teil der Bedrohungsanalyse, da sie nur durch physische Sicherheitsmaßnahmen verhindert werden können.

3.3 Erkenntnisse

Auf der Basis des vorgestellten Datenflussmodells aus Abbildung 3 wurde eine Bedrohungsanalyse nach STRIDE mit dem Fokus auf dezentrale Standorte und den genannten Einschränkungen durchgeführt. Hierbei wurden die dargestellten Schnittstellen und Systeme jeweils anhand, der durch STRIDE definierten Bedrohungskategorien, analysiert. Die Analyse zeigt, dass DEA im Vergleich zu anderen dezentralen Standorten eine besondere Rolle einnehmen. Dies ist auf die Existenz mehrerer Parteien, mit teilweise gegensätzlichem Interesse und Einfluss auf eine DEA, zurückzuführen (z.B. VNB – Netzstabilität vs. Eigentümer der DEA – Rentabilität). Daher wurde aufbauend auf der allgemeinen Analyse eine spezielle Analyse für DEA durchgeführt. Es wurden insgesamt 58 Bedrohungen erkannt, neun dieser Bedrohungen sind nur für DEA relevant. Die Bedrohungen wurden dabei nicht gewertet, sondern aufgrund der Kritikalität eines Verteilnetzes als gleichermaßen wichtig eingestuft. Mit insgesamt 19 Bedrohungen beziehen sich die meisten Bedrohungen auf die Sicherheit von Feldleitgeräten. Dies war zu erwarten, da Feldleitgeräte besonders stark von dem Wandel zu einem intelligenten Energienetz betroffen sind. Es zeigt sich, dass Funktionalität und Vernetzung häufig wichtiger als Informationssicherheit sind, so dass schon einfache Sicherheitsmechanismen, wie eine ausgereifte Zugriffskontrolle und eine sichere Übertragung von Daten fehlen. Die meisten Bedrohungen aus der Analyse fallen daher in die STRIDE-Kategorie „Information Disclosure“ (18), gefolgt von der Kategorie „Tampering“ (11). Aufgrund fehlender kryptografischer Sicherheitsmaßnahmen in eingebetteten Systemen, wie den Feldleitgeräten, sind Man-In-The-Middle-Angriffe möglich. Zudem erleichtern unsichere lokale Passwörter und gemeinsam genutzte Zugangsdaten den unberechtigten Zugriff. Durch die meist geringen Systemressourcen sind Denial-Of-Service-Angriffe außerdem leicht umzusetzen. Die bekannten Sicherheitslösungen aus der traditionellen IKT sind hierbei, aufgrund längerer Lebenszyklen und geringerer Systemressourcen der Steuerungssysteme, nicht einfach übertragbar.

Eine weitere Erkenntnis besteht in der Priorisierung der allgemein anerkannten Sicherheitsziele, Vertraulichkeit, Integrität und Verfügbarkeit. Die Manipulation von Mess- und Steuerungsdaten kann zu einem Systemausfall führen. Die Integrität der Daten ist daher besonders wichtig. Dagegen ist der Verlust von Daten außerhalb gesetzlicher Datenschutzbestimmungen weniger kritisch. Die Verfügbarkeit der Systeme ist aus heutiger Sicht am wenigsten relevant, so lange die Ausfallzeit begrenzt ist. Die meisten Systeme im Feld können, über einen begrenzten Zeitraum, autark funktionieren. Hinzu kommen zudem physikalische Effekte, die einfache elektrotechnische Fehler im Netz ausgleichen. Dies führt zu der folgenden Priorisierung der genannten Sicherheitsziele mit Ähnlichkeit zu den Anforderungen im Umfeld der Industrie 4.0 [Bund16]: 1) Integrität, 2) Vertraulichkeit, 3) Verfügbarkeit.

4 Empfehlungen

Im Rahmen der Bedrohungsanalyse wurden nationale und internationale Standards, Richtlinien und Empfehlungen untersucht, um zu evaluieren, welche Bedrohungen und Gegenmaßnahmen für das intelligente Energienetz bereits bekannt sind. Die Untersuchung zeigt, dass für die, in der Bedrohungsanalyse erkannten, Bedrohungen bereits Gegenmaßnahmen durch eine Kombination der untersuchten Dokumente existieren. Im Folgenden wird daher ein kurzer Überblick über die als relevant eingestuften Standards, Richtlinien und Empfehlungen gegeben, bevor einzelne eigene Empfehlungen zu Sicherheitsmaßnahmen erläutert werden, die Aufgrund der Bedrohungsanalyse als besonders wichtig oder in den Standards als unterrepräsentiert angesehen werden.

4.1 Standards

Durch die Aktualität des Themas Smart Grid gibt es diverse Standards, Richtlinien und Empfehlungen verschiedener Nationen und Verbände, die sich mit intelligenten Energienetzen auseinandersetzen. Das Oldenburger Forschungs- und Entwicklungsinstitut für Informatik-Werkzeuge und Systeme (OFFIS e.V.) hat hierzu einen zusammenfassenden Überblick in zwei Teilen veröffentlicht (vgl. [RUB+10, URB+10]). Davon ausgehend wurden zwei Gruppen von Dokumenten, nach einer eingehenden Recherche, als besonders relevant eingestuft, da diese sich insbesondere auf Verteilnetze beziehen.

Zum einen sind es die Empfehlungen der European Network and Information Security Agency (ENISA). Die ENISA hat in einem zeitlichen Abstand, neben einer sogenannten Bedrohungslandkarte [Euro13a], zwei Dokumente mit Sicherheitsempfehlungen für das Smart Grid herausgegeben. Das erste Dokument [Euro12] besteht hierbei aus einer Sammlung von Sicherheitsmaßnahmen aus unterschiedlichen Standards sowie aus verschiedenen weiteren Dokumenten, wie beispielsweise von anderen staatlichen Organisationen oder Organisationen der Wissenschaft. Das zweite Dokument [Euro13b] baut auf den Vorarbeiten des ersten Dokuments auf und konsolidiert die Informationen zu einer Teilmenge von Mindestanforderungen an die Informationssicherheit. Diese Empfehlungen der ENISA fassen verschiedene internationale sowie nationale Standards zusammen und bilden daher eine Basis für intelligente Energienetze in der Europäischen Union. Abbildung 4 zeigt einen Teil der Standards und Richtlinien, die durch die ENISA berücksichtigt werden. Aufgrund der Verflechtungen zwischen den Dokumenten besteht bei der Abbildung aber kein Anspruch auf Vollständigkeit.

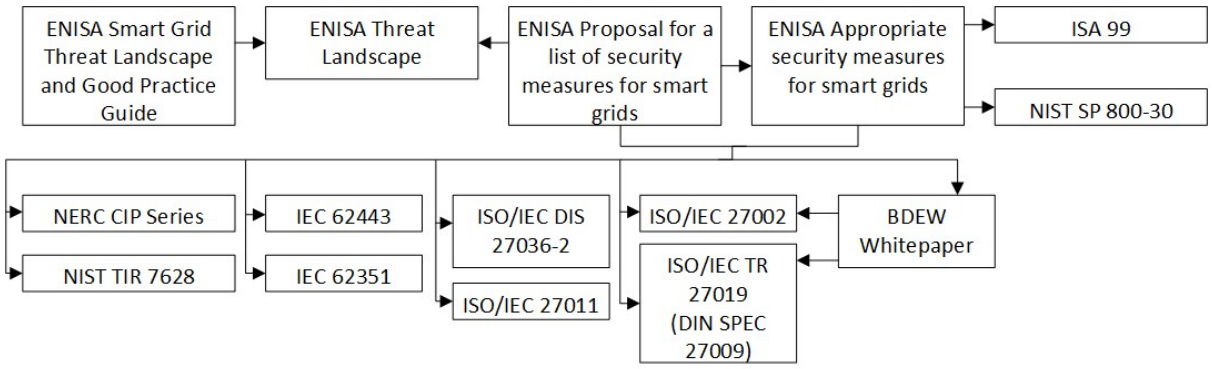

Abb. 4: Relevante Dokumente der ENISA und beeinflussende Standards

Die Vorgaben der ENISA sind jedoch nur Empfehlungen. Im Gegensatz dazu sind die VNB in Deutschland dazu verpflichtet, den IT-SiKa umzusetzen [Bund15b]. Der IT-SiKa hat daher eine besondere Relevanz für das Verteilnetz. Der IT-SiKa verpflichtet VNB ein Informationssicherheitsmanagementsystem (ISMS) auf Basis der internationalen Normenfamilie ISO/IEC 27000 (u.a. [Deut15, Deut14]) einzuführen. Der IT-SiKa referenziert zudem weitere Richtlinien, wie das BDEW-Whitepaper [Bund15a] und das ICS-Security-Kompendium [Bund13a] im Zusammenhang mit dem IT-Grundschutz [Bund08] des BSI. Abbildung 5 zeigt einen Teil der Dokumente, die durch den IT-Sicherheitskatalog berücksichtigt werden. Aufgrund der Verflechtungen zwischen den Dokumenten besteht auch hier kein Anspruch auf Vollständigkeit.

Die genannten Standards, Richtlinien und Empfehlungen ergeben eine weitreichende Wissensbasis zum Thema Informationssicherheit in intelligenten Energienetzen, die in Kombination, wie eingangs erwähnt, bereits alle erkannten Bedrohungen aus der durchgeführten Bedrohungsanalyse mit entsprechenden Gegenmaßnahmen abdecken.

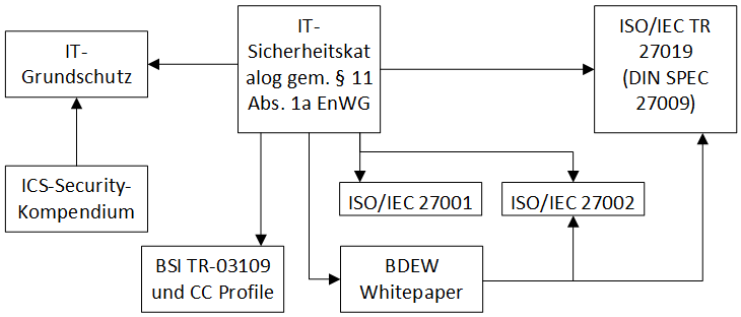

Abb. 5: Der IT-Sicherheitskatalog und beeinflussende Standards

Untersuchungen der Praxis im Rahmen des Forschungsprojektes SEnCom haben hierzu gezeigt, dass bei großen VNB viele dieser Vorgaben bereits berücksichtigt werden. Kleinere und mittlere VNB berücksichtigen diese dagegen häufig nur teilweise und in manchen Bereichen gar nicht. Die Ursachen hierfür liegen unter anderem in den historisch gewachsenen und dadurch heterogenen Infrastrukturen, die durch die langen Lebenszyklen in der Prozesstechnik zustande kommen. In vielen Fällen sind proprietäre Systeme und Kommunikationsprotokolle sowie veraltete Übertragungsmedien zu finden. Zum Schutz der Systeme in der Prozesstechnik wird hierbei häufig eine strikte Trennung von öffentlichen Kommunikationsnetzen, wie dem Internet, verfolgt. Zukünftig wird sich diese Air-Gap allerdings schließen, was die Sicherheitsanforderungen an diese Systeme stark erhöhen wird. Des Weiteren setzen VNB in der Prozesstechnik auf Systeme, die sich über Jahre bewährt haben. Hier ergibt sich zukünftig die Herausforderung, dass diese Systeme trotzdem in der Lage sind, den Stand der Technik im Bereich der Informationssicherheit abbilden zu können.

Die wichtigste Empfehlung besteht daher darin, dass das Bewusstsein für Informationssicherheit im Energiesektor gestärkt wird und bestehende Standards, Richtlinien und Empfehlungen besser verbreitet werden, so dass bekannte Sicherheitsmaßnahmen auch Anwendung finden. Dabei muss Informationssicherheit als ein andauernder Prozess verstanden werden, der von allen beteiligten berücksichtigt wird. Hierzu gehört unter anderem die Aufforderung an Energienetzakteure entsprechende Sicherheitsanforderungen an die Hersteller der beteiligten Steuerungssysteme in einem Energienetz weiterzugeben. Hersteller müssen sich dagegen den neuen Sicherheitsanforderungen stellen und bestehende Lösungen für den Energiesektor an den Stand der Technik anpassen, da die Umsetzung einiger bekannter Sicherheitsmaßnahmen bereits an der Verfügbarkeit technischer Lösungen scheitert.

4.2 Monitoring

Aufgrund der Erkenntnisse aus der Bedrohungsanalyse besteht eine zentrale Herausforderung für sichere Verteilnetze der nahen Zukunft in der Überwachung der heterogenen IKT im Feld. Durch die zunehmende Integration von IKT sind Störungen nicht mehr ausschließlich auf die Primärtechnik zurückzuführen. Stattdessen können Fehler zukünftig häufiger bei der IKT auftreten. Dies wird bereits durch aktuelle Ereignisse verdeutlicht [LeAC16]. Die Überwachung der IKT wird jedoch in der Praxis derzeit nur wenig adressiert. Hierdurch entsteht eine Art „Blinder Fleck“, der zufolge hat, dass zukünftige Störquellen im Stromnetz nicht mehr mit bisherigen Mitteln zu identifizieren sind. Es besteht die Gefahr, dass eine Störung, die ursprünglich durch die IKT verursacht wird, aufgrund einer fehlenden Überwachung nicht auf die IKT zurückgeführt werden kann. In der Folge ist eine zuverlässige Fehlerdiagnose erst durch auf-

wendige Verfahren vor Ort möglich. Höhere Ausfallzeiten sind eine mögliche Folge. Eine Ursache für die geringe Überwachung von IKT kann fehlendes Bewusstsein oder Know-how sein. Dies gilt vor allem für kleinere VNB. Eine andere wichtige Ursache ist auf die Hersteller der Systeme im Feld zurückzuführen. Eine Untersuchung verschiedener Systeme aus dem Feld hat gezeigt, dass viele Geräte aktuell nur geringe Überwachungsmöglichkeiten bieten. Standardisierte Methoden wie Syslog sind kaum verbreitet, am häufigsten ist noch das Simple Network Management Protocol zu finden, zum Teil sind Überwachungsmöglichkeiten gar nicht vorhanden. Dies muss sich ändern, da VNB zukünftig in der Lage sein müssen, IKT und Prozesstechnik gleichermaßen zu überwachen. Entsprechende Anforderungen sind auch in den untersuchten Standards, Richtlinien und Empfehlungen zu finden (z.B. [Bund15a, Bund13a]).

4.3 Zugangs- und Integritätsschutz

Eine besondere Situation im Verteilnetz stellen dezentrale Standorte dar. Sie wurden im Rahmen des Forschungsprojektes SEnCom als besonders kritisch identifiziert, da sie unter anderem an schwer zu kontrollierenden Orten stehen und einem, teilweise sogar berechtigten, Zugriff durch Dritte ausgesetzt sind. Für dezentrale Standorte ist ein effektiver Zugangs- und Integritätsschutz daher von besonderer Bedeutung. Physische Maßnahmen zur Zugangskontrolle sind hierbei heute am häufigsten vertreten. Sie stellen die Basis für einen erfolgreichen Schutz dar. Teilweise werden auch logische Maßnahmen, wie der Zugangsschutz durch Anmeldevorgänge an Systemen, bereits umgesetzt. Zukünftig sollten aber noch weitere logische Maßnahmen eingesetzt werden, die aktuell nur bei wenigen, meist großen, VNB zu finden sind. Hierzu sind ebenfalls entsprechende Anforderungen in den untersuchten Standards, Richtlinien und Empfehlungen zu finden (z.B. [Bund15a, Bund13a]). Ein wichtiger Punkt ist der Einsatz zentraler Identitäts- und Zugangsmanagementsysteme (Identity and Access Management), um die Nutzerverwaltung zu vereinfachen und Anmeldevorgänge besser überwachen zu können. Der Zugang zu Kommunikationsnetzen sollte zudem mit logischen Maßnahmen wie IEEE 802.1X ergänzend geschützt werden. Hardwarebasierte Schutzmaßnahmen aus dem Bereich Trusted Computing ermöglichen darüber hinaus die Überwachung der Integrität einzelner, besonders kritischer Systeme. Dies kann die Vertrauenswürdigkeit und die Zuverlässigkeit von intelligenten Energienetzen wesentlich verbessern [DGHS14].

5 Zusammenfassung und Ausblick

Die Energiewende hat einen großen Einfluss auf die Verteilnetze, da DEA überwiegend an Verteilnetzen angebunden werden. Die Energie wird hierdurch nicht mehr von den obersten Spannungsebenen zu den niedrigeren Spannungsebenen, sondern in beide Richtungen verteilt. Hieraus entsteht ein dezentrales, bidirektionales Energieversorgungssystem, das mit Hilfe von intelligenten Systemen gesteuert werden soll. Es entwickeln sich intelligente Verteilnetze, die informationstechnisch nicht mehr durch ein Air-Gap von ihrer Umgebung getrennt sind und neue Anforderungen an die Informationssicherheit stellen. Die vorgestellte Bedrohungsanalyse verdeutlicht dies. Eine Recherche in bestehenden Standards, Richtlinien und Empfehlungen kommt darüber hinaus zu demselben Ergebnis, da die untersuchten Dokumente bereits die wesentlichen Bedrohungen und notwendigen Gegenmaßnahmen enthalten. In der Praxis werden die bestehenden Informationen jedoch nur teilweise beachtet und angewandt. Dies führt zu dem Schluss, dass bestehende Standards, Richtlinien und Empfehlungen noch nicht flächendeckend zu den allgemein anerkannten Regeln der Technik im Energiesektor gehören.

Für die Zukunft ist mit Hilfe von Erfahrungen aus der Praxis erkennbar, dass insbesondere die Überwachung der IKT in intelligenten Verteilnetzen eine wichtige Rolle spielen wird. Heute werden vor allem die energietechnischen Parameter eines Verteilnetzes überwacht, in der Zukunft müssen auch informationstechnische Parameter genauer überwacht werden, um einen „Blinden Fleck“ bei der Fehlersuche zu vermeiden. Die vorgestellte Betrachtung fokussiert sich dabei besonders auf dezentrale Standorte im Verteilnetz, da der Schutz dieser Standorte im Allgemeinen als schwieriger, im Vergleich zu zentralen Unternehmensniederlassungen, angesehen wird. DEA wurden in diesem Zusammenhang gesondert betrachtet, weil unterschiedliche Parteien einen Zugriff auf DEA haben können. Hierzu gehören insbesondere der Eigentümer, der VNB und gegebenenfalls der Betreiber eines VKW. Der Zugangs- und der Integritätsschutz für dezentrale Standorte, und DEA im speziellen, stellen daher neben der Überwachung besondere Schwerpunkte dar.

Zusammenfassend lässt sich feststellen, dass die notwendigen Informationen zur Etablierung eines sicheren intelligenten Energienetzes bereits vorhanden sind. Um dieses Wissen jedoch in die allgemein anerkannten Regeln der Technik im Energiesektor zu überführen, ist ein fortlaufender Austausch im Sinne des Wissens- und Technologietransfers zwischen Anwendern, Herstellern und Domänenexperten notwendig. Hierzu wird aktuell eine Zusammenfassung der vorgestellten Standards, Richtlinien und Empfehlungen erstellt, die mit Hilfe einfacher praktischer Beispiele zur Orientierung und zur Weiterbildung für den Bereich Informationssicherheit in intelligenten Energienetzen beitragen soll. Der Wissenstransfers muss dabei durch den Technologietransfer zur Entwicklung sicherer Steuerungssysteme für das intelligente Energienetz ergänzt werden. Bekannte Sicherheitslösungen für traditionelle IKT sollten für den Einsatz im intelligenten Energienetz adaptiert werden. Insbesondere die Steuerungssysteme im Feld müssen als „Next-Generation“- Steuerungssystem durch die Integration genereller Sicherheitsmaßnahmen und spezieller Sicherheitssysteme besser geschützt werden. Hierbei ist zu prüfen, welche Ansätze zur Integration in Frage kommen. Sicherheitsmaßnahmen, die Teil eines Steuerungssystems sind, sind schwerer zu umgehen, nutzen aber die gleichen Systemressourcen wie die primären Systemfunktionen. Externe Sicherheitsmaßnahmen sind unabhängig von den Systemressourcen eines Steuerungssystems, können dafür aber leichter umgangen werden. Ergänzend dazu sollten domänenspezifische Überwachungslösungen entwickelt werden, die aus der Leitwarte heraus ein konvergiertes Lagebild über ein intelligentes Energienetz, ohne spezialisiertes Wissen zu IKT und Informationssicherheit, ermöglichen.

Literatur

[Bund08] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise, Version 2.0. BSI (2008).

[Bund13a] Bundesamt für Sicherheit in der Informationstechnik: ICS-Security-Kompendium. BSI (2013).

[Bund13b] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie BSI TR-03109-1 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems. BSI (2013).

[Bund15a] Bundesverband der Energie- und Wasserwirtschaft e.V: Whitepaper- Anforderungen an sichere Steuerungs- und Telekommunikationssysteme. BDEW (2015).

[Bund15b] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz. BNetzA (2015).

[Bund16] Bundesministerium für Wirtschaft und Energie: IT-Sicherheit für die Industrie 4.0 – Abschlussbericht. BMWI (2016).

[CoCE12] European Committee for Standardization (CEN) and European Committee for Electrotechnical Standardization (CENELEC) and European Telecommunications Standards Institute (ETSI): Smart Grid Reference Architecture, Version 3.0. Smart Grid Coordination Group (2012).

[Deut14] Deutsches Institut für Normung: Informationstechnik – Sicherheitsverfahren – Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002 (ISO/IEC TR 27019:2014). DIN (2014).

[Deut15] Deutsches Institut für Normung: Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC 27001:2013 + Cor. 1:2014). DIN (2015).

[DGHS14] K.-O. Detken, C.-H. Genzel, O Hoffmann, R. Sethmann: Absicherung von Smart-Meter-Umgebungen mit Trusted Computing. In: P. Schartner, P Lipp: D.A.CH Security 2014: Bestandsaufnahme, Konzepte, Anwendungen und Per-spektiven, syssec-Verlag (2014).

[Euro12] European Union Agency for Network and Information Security: Appropriate security measures for smart grids - Guidelines to assess the sophistication of security measures implementation. ENISA (2012).

[Euro13a] European Union Agency for Network and Information Security: Smart Grid Threat Landscape and Good Practice Guide. ENISA (2013).

[Euro13b] European Union Agency for Network and Information Security: SMART GRID TASK FORCE 4 EG2 DELIVERABLE 5 - Proposal for a list of security measures for smart grids. ENISA (2013).

[LeAC16] M. R. Lee, M. J. Assante, T. Conway: TLP: White - Analysis of the Cyber Attack on the Ukrainian Power Grid – Defense Use Case. Electricity Information Sharing and Analysis Center (2016).

[Micr09] Microsoft Corporation: IT Infrastructure Threat Modeling Guide. Microsoft Solution Accelerators (2009).

[Open17] Open Web Application Security Project: Application Threat Modeling. https://www.owasp.org/index.php/Application_Threat_Modeling, Abruf: (2017).

[RUB+10] S. Rohjans, M. Uslar, R. Bleiker, J. González, M. Specht, T. Suding, T. Weidelt: Survey of Smart Grid Standardization Studies and Recommendations. In: 2010 First IEEE International Conference on Smart Grid Communications, SmartGridComm (2010), S. 583-588.

[URB+10] M. Uslar, S. Rohjans, R. Bleiker, J. González, M. Specht, T. Suding, T. Weidelt: Survey of Smart Grid standardization studies and recommendations — Part 2. In: Innovative Smart Grid Technologies Conference Europe (ISGT Europe), IEEE PES (2010), S 1-6.