VDE-POSITIONSPAPIER

SMART GRID SECURITY

Energieinformationsnetze und -systeme

ITG

VDE

VDE-Positionspapier

Smart Grid Security

Energieinformationsnetze und -systeme

Autoren

Dr.-Ing. Jörg Benze, T-Systems Multimedia Solutions GmbH, Dresden

Dr. Andreas Berl, Universität Passau, Passau

Dr. Kai Daniel, RWE Deutschland AG, Essen

MMag. Dr. Günther Eibl, Fachhochschule Salzburg, Salzburg

FH-Prof DI Mag. Dr. Dominik Engel, Fachhochschule Salzburg, Salzburg

Dipl. Inf. Andreas Fischer, Universität Passau, Passau

FH-Prof. Prof. Dr. (habil) Ulrich Hofmann, Fachhochschule Salzburg, Salzburg

Dipl.-Phys. Andreas Kießling, energy design & management consulting, Leimen

Dr.-Ing. Stefan Köpsell, Technische Universität Dresden, Dresden

Dr.-Ing. Lucie Langer, AIT Austrian Institute of Technology GmbH, Wien

Prof. Dr. Hermann de Meer, Universität Passau, Passau

DI Christian Neureiter, Fachhochschule Salzburg, Salzburg

Dipl.-Inf. Michael Niedermeier, Universität Passau, Passau

DI (FH) Thomas Pfeiffenberger, Salzburg Research Forschungsgesellschaft mbH

Dipl.-Wirtsch.-Inform. (FH) Michael Pietsch, CONSULECTRA Unternehmensberatung GmbH, Hamburg

DI Armin Veichtlbauer, Fachhochschule Salzburg, Salzburg

Impressum

VDE VERBAND DER ELEKTROTECHNIK
ELEKTRONIK INFORMATIONSTECHNIK e.V.

Stresemannallee 15 · 60596 Frankfurt am Main
Telefon 069 6308-0 · E-Mail service@vde.com · http://www.vde.com

Bildnachweis ©: Titel, Siemens/Grafik: Markus Kellermann Graphik-Design, Schwielowsee-Caputh
Design: www.schaper-kommunikation.de

Dezember 2014

Inhalt

Abbildungsverzeichnis

Management Summary

Das elektrische Energieversorgungssystem durchläuft gegenwärtig eine Transformation zu einem Energiesystem mit dem Vorrang an erneuerbaren, volatilen Energien sowie den Trends zu einer lastfernen und im hohen Maße zunehmenden dezentralen Erzeugung.

Hierdurch ergeben sich Veränderungen im Netz und in der Netztopologie, die u. a. dadurch gekennzeichnet sind, dass die Prozessdatenverarbeitung (PDV) und die Bürokommunikation (IT) schleichend mehr und mehr zusammenwachsen (auch als OT/IT-Integration bezeichnet). Desweiteren sind Prozesssteuerungssysteme dezentraler Anlagen zunehmend über das Internet erreich- und konfigurierbar. Hierdurch ergeben sich neue Bedrohungsszenarien, die es bis dato nicht gab, auf die jedoch zukünftig reagiert werden muss.

Das Positionpapier beleuchtet zunächst neue Sicherheitsziele und Sicherheitsanforderungen, die sich in Folge der Markt- und Netzintegration und der zunehmenden OT/IT-Integration ergeben. Anschließend werden Angreifermodelle und Schutzmaßnahmen erläutert; ferner werden Test und Testverfahren vorgestellt, mittels denen man eine Sicherheitsevaluierung von Energieinformationsnetzen vornehmen kann. Aufbauend darauf werden die aktuell diskutierten Smart Grid Topologien betrachet und Design-Empfehlungen für Sicherheitssysteme, einerseits für bestehende historisch gewachsene Architekturen, andererseits für den Entwurf neuer Architekturen, vorgestellt; denn Sicherheitsaspekte müssen beim Entwurf neuer Systeme essentieller Bestandteil der Topologie sein.

Abschließend werden spezifische Handlungsempfehlungen für Politik, Standardisierung, Energieversorger, Hersteller und Wissenschaft/Forschung zum Aufbau sicherer IKT-Infrastrukturen für die Energieversorgungssysteme vorgestellt.

1. Einleitung

Das bisherige fossile und nukleare Energiesystem wurde insbesondere durch die zentralisierte Energiegewinnung sowie zentralisierte Steuerungsmechanismen und Systemverantwortung bestimmt. Daraus resultierte die gute Planbarkeit der Erzeugung. Das Verteilungsnetz stellte die benötigte Energie den Kunden unidirektional bereit, wobei der Kunde selbst im System eine passive Rolle spielte.

Um die ökologischen und energiepolitischen Ziele erfolgreich umzusetzen, gilt es nun die Säulen eines neuen Gesamtkonzeptes zu bestimmen. Ihre Tragkraft basiert auf dem Gedanken, dass die Energiewende nicht nur als Pflicht und unter Kostenaspekten betrachtet werden sollte, sondern sich aus diesem historischen Prozess neue Chancen für die zukünftige Wirtschaftskraft des Landes ergeben. Diese neuen Chancen für vielfältige Beteiligte werden durch die Erschließung von Energiepotentialen aus zentralen Lagen sowie auch die Erschließung dezentraler Erzeugungs- und Speicherpotentiale bei Bürgern und Unternehmen sowie Kommunen und Regionen eröffnet.

Die Teilnehmer am Energienetz als Erzeuger sowie als Verbraucher und damit als sogenannte **Prosumenten** wachsen in eine aktive Rolle, womit die Wertschöpfung in den Regionen gestärkt wird. Ein daraus resultierender wachsender Grad an **Partizipation** am Energiesystem mit regionalen Ausgleich- und Austauschmechanismen wiederum führt zu einer zunehmenden **Vielfalt** von Energieflüssen unterschiedlichster Quellen und Energieträgerarten in der Verbindung von Strom, Wärme, Gas sowie den Treibstoffen des Verkehrs. Die zentrale Erzeugung wird zunehmend durch die dezentrale Erzeugung ergänzt, wodurch bidirektionale Energieflüsse entstehen, die neue Prozesse und Formen der **Organisiertheit** erfordern. Erneuerbare Energien bringen aber auch eine zunehmende **Volatilität** der Erzeugung in das Gesamtsystem, womit die Planbarkeit abnimmt und neue Prognosemethoden erforderlich sind.

Dabei wird eine hohe Versorgungssicherheit weder allein durch ein zentralisiertes System noch durch regionale Egoismen entstehen. Ein zellularer Ansatz unterstützt dabei, die zunehmende **Komplexität** der Systemführung zu beherrschen, **Subsidiarität und globale Verbundenheit** zu vereinen sowie **Sicherheit und Datenschutz** im Gesamtsystem zu erhöhen. Die Komplexitätsbeherrschung gelingt dabei insbesondere durch neue Markt- und Netzfunktionen zur Flexibilisierung des Gesamtsystems im Rahmen eines Ampelmodells. Dabei werden rein marktbasierte Funktionen dem Grünbereich, die Priorität von Netzfunktionen im Störungsfalle dem Rotbereich und Abstimmungen zwischen Markt und Netz dem Gelbbereich zugeordnet.

Neue Energieaggregationsfunktionen für Mengen von Kleinanlagen, neue Flexibilitäts- und Netzunterstützungsfunktionen umfassen dabei Demand Response-Verfahren zur anreizbasierten Verbrauchssteuerung, die Marktintegration erneuerbarer, dezentraler Energien in virtuelle Kraftwerke, neue Systemdienstleistungen im Verteilungsnetz in Interaktion mit Liegenschaften, neue Formen der dezentralen, automatisierten Regelung im Verteilungsnetz sowie neue Energiedienstleistungen (Smart Metering, Anlagen-Contracting, usw.).

Für Teile dieser Funktionen wird eine gemeinsame IKT-Infrastruktur im Smart Grid als Enabler benötigt. Wer sollte die Erweiterung der notwendigen IKT-Infrastruktur für neue Markt- und Netzmechanismen vornehmen? Die Vielzahl der Akteure und der Komponenten in einem komplexen, vernetzten sowie zentral und dezentral verbundenen System erfordert das Vorantreiben einer standardisierten Kommunikation sowie die Gewährleistung von Informationssicherheit und Datenschutz. Die dafür notwendige IKT-Infrastruktur vernetzt eine kritische Infrastruktur. Um die Versorgungssicherheit in gewohnter Weise auch unter den neuen Bedingungen zu erhalten, sollte die IKT-Infrastruktur durch einen verantwortlichen Akteur, wie beispielweise den Verteilungsnetzbetreiber (VNB) als Betreiber einer intelligenten Energieinfrastruktur, gestaltet werden, wobei dies Dienstleister für die VNBs umsetzen können. Gemeinsame, diskriminierungsfrei bereitgestellte Smart-Grid-Infrastrukturen aus elektrotechnischer und informationstechnischer Vernetzung verbessern dabei gleichzeitig die Wirtschaftlichkeit von Geschäftsmodellen verschiedener Marktakteure.

Zusätzlich sind die durch die Transformation des Energiesystems entstehenden neuen Möglichkeiten des Energiemarktes in Verbindung mit dem Einsatz von IKT-Technologien zur Vernetzung der Energiekomponenten (Erzeuger, Speicher, Verbraucher) von Marktakteuren im Smart Grid hochrelevant. Dafür wurde auch der Begriff „Smart Market“ geprägt. Dies umfasst ebenso neue Marktmechanismen zur Aggregation der Energiemengen vielfältiger, dezentraler Energieanlagen sowie auch das Angebot von Leistungsflexibilitäten in der Erzeugung, in der Speicherung und in der Nutzung von Energie verschiedener Energieträger (Elektrizität, Gas, Wärme, Verkehr) sowie neuartige Dienstleistungen, die durch die Informationen und die Vernetzung im Smart Grid verfügbar werden. Ein Beispiel für eine mögliche Dienstleistung besteht darin, die Energieeffizienzpotentiale in Haushalten automatisiert ständig zu bewerten und diese wirtschaftlich zu nutzen.

Im Rahmen dieser Marktpotentiale entstehen somit auch völlig neue Fragestellungen und Herausforderungen bezüglich der Daten, die

einerseits für die Schaffung von Marktchancen zur Verfügung gestellt werden, jedoch andererseits aufgrund ihres Personenbezugs oder ihrer Kritikalität eines besonderen Schutzniveaus bedürfen. Hier sind aktuell neben der Nutzerakzeptanz auch rechtliche Grundsätze zu betrachten, da diese eine Weitergabe von Nutzerdaten aufgrund von §9 Abs. 1 EnWG verbieten. Um die Weiterverarbeitung dieser Daten trotzdem zu ermöglichen, ist zunächst eine Bewertung der Daten in Bezug auf deren Kritikalität (Gefahr für die Energieinfrastruktur an sich) und Personenbezug (Gefahr für den Datenschutz und rechtliche Konsequenzen) unerlässlich. Danach müssen neuartige Bewertungs- und Anonymisierungsmethoden untersucht werden, die als Ausgangspunkt die Offenlegung der Daten auf eine „nicht diskriminierende Weise“ (gemäß §9 Abs. 2 EnWG) nutzen. Darüber hinaus stellt der Schutz der Privatsphäre eine wesentliche Voraussetzung für die Übertragung von energiebezogenen Daten dar. Mit Hilfe von Smart Metern können detaillierte Verbrauchsinformationen gesammelt und zu individuellen Verbrauchsprofilen zusammengesetzt werden. Die Erfassung und Verarbeitung dieser personenbezogenen Daten muss im Sinne der informationellen Selbstbestimmung für den Verbraucher transparent, durch ihn freigeben und sperrbar sowie kontrollierbar sein.

Durch die Einführung von Informations- und Kommunikationstechnologie in der Stromversorgung entstehen auch neuartige Bedrohungsszenarien. Die Kommunikation im Smart Grid, die in einem Energieinformationsnetz stattfindet, muss neben Dienstgüteanforderungen vor allem Anforderungen im Bereich der IT-Sicherheit und Widerstandsfähigkeit erfüllen. Da es sich bei Energienetzen um kritische Infrastrukturen handelt, werden auch Fragen der funktionalen Sicherheit aufgeworfen. Angriffe auf Energieinformationssysteme oder Ausfälle von Kommunikationssystemen und wesentlicher Systemfunktionen können zu Stromausfällen führen und stellen damit eine akute Gefahr für Unternehmen sowie öffentliche Einrichtungen dar. Längerfristige Störfälle können die gesamte Versorgungsinfrastruktur und in weiterer Konsequenz auch Leib und Leben bedrohen. Durch eine mögliche Verflechtung zwischen Energie- und IT-Systemen im Rahmen des Smart Grids entsteht eine gegenseitige Abhängigkeit dieser beiden Netze, die im Falle eines großflächigen Stromausfalls zu erheblichen Problemen führen kann. Das Szenario einer Wiederinbetriebnahme dieses Systems, als Schwarzstart bezeichnet, ist allein aufgrund der komplexen Abhängigkeiten im heutigen Stromnetz schon eine Herausforderung. Im zukünftigen Energiesystem stellt sich durch die Durchdringung mit IT-Systemen bis in den Niederspannungsbereich und hin zu Millionen von Liegenschaften eine nochmals größere Herausforderung. Nicht zuletzt spielt natürlich auch die Akzeptanz seitens der Verbraucher eine wichtige Rolle, die von der Benutzbarkeit, der Zuverlässigkeit und

der Sicherheit der Smart Grid Technologien abhängt. Ein zukünftiges Smart Grid muss all diesen Herausforderungen gerecht werden. Durch seine Rolle als kritische Infrastruktur spielt dabei die Sicherheit eine wesentliche Rolle. Es ist daher notwendig einerseits geeignete Sicherheitsanforderungen zu formulieren und andererseits neue Konzepte und Schutzmaßnahmen zur Absicherung dieser Infrastruktur zu entwickeln.

Zur Betrachtung dieser Themen wurde das Positionspapier folgendermaßen gegliedert. In Kapitel 2 werden die Infrastruktur und die fachlichen Besonderheiten des erweiterten Energieinformationsnetzes und -systems detailliert beschrieben. Kapitel 3 beschäftigt sich mit den Sicherheitszielen und Sicherheitsanforderungen in Folge der Markt- und Netzintegration erneuerbarer Energien und schafft den Übergang zu Schutzmaßnahmen in den folgenden Kapiteln. Wichtige Aspekte, die bei den Sicherheitsanforderungen berücksichtigt werden müssen, stellen sowohl der Schutz der Prosumenten, der Marktakteure und ihrer Komponenten im Energiesystem sowie der Infrastruktur selbst dar. Kapitel 4 erläutert im Anschluss Sicherheitsmaßnahmen im erweiterten Energieinformationssystem. Dabei werden zunächst Sicherheitsziele und Angreifermodelle gegenübergestellt, bevor nachfolgend Schutzmaßnahmen erläutert werden. In Kapitel 5 werden die aktuell diskutierten Smart Grid-Topologien betrachtet. Unterschieden wird zwischen zentral geführten und dezentralen/zellularen Systemen. Weitere in diesem Kapitel abgedeckte Teilbereiche beinhalten Kommunikationstechnologien sowie deren Sicherheits- und Zugriffsverfahren. Kapitel 6 entwickelt aus den zuvor diskutierten Technologien und Ansätzen aktuelle Empfehlungen und zieht das Fazit für ein sicheres Energieinformationsnetz und -system als gemeinsame Grundlage im Smart Grid.