Projekt: eSafeNet

Ein Demonstrator für das Internet der Energie

Ein intelligentes Stromnetz erfordert eine neue Infrastruktur, „intelligente" Dienstleistungen und ein ganzheitliches Sicherheitskonzept

Durch das Erneuerbare-Energien-Gesetz und den Wandel in der Energieversorgung ergeben sich immer neue Herausforderungen. Aufgrund der zunehmenden Einspeisung durch fluktuierende Erneuerbare-Energie-Erzeugungsanlagen ist der Ausbau von Energienetzen in Kopplung mit einer sicheren, schnell verfügbaren, energieeffizienten und wirtschaftlichen Informations- und Kommunikationstechnologie unabdingbar[1]. Im Rahmen des Forschungsprojekts ‚eSafeNet' werden verschiedene Funk- und Kabelübertragungstechnologien auf ihr Potenzial für das Internet der Energie untersucht. Des Weiteren wird eine Dienstleistungsplattform für Smart Services entwickelt. Ein interaktiver Demonstrator wird kreiert, der die Lösungsansätze für eine sichere Informations- und Kommunikations- sowie Energieinfrastruktur erlebbar darstellen soll. Das Vorhaben 03ET7549A der Forschungsvereinigung *FIR e. V. an der RWTH Aachen* wird über den *PTJ* durch das *Bundesministerium für Wirtschaft und Energie (BMWi)* aufgrund eines Beschlusses des Deutschen Bundestages gefördert.

Die aktuellen Klima- und Energieziele der Europäischen Union sowie der Bundesrepublik Deutschland erfordern neben der Steigerung der Anzahl von Energieerzeugungsanlagen für EE (erneuerbare Energien) auch die Bewältigung weiterer daraus resultierender technischer und operativer Herausforderungen, wie den Ausbau der Energienetze[1]. Durch die Weiterentwicklung zu Smart Grids und den Smart-Meter-Roll-out steigen neben dem Datenvolumen auch die Verletzlichkeit und Verwundbarkeit des Energienetzes durch gezielte Hackeraktivitäten oder Manipulationsversuche. Daher ist die Einführung einer sicheren und jederzeit verfügbaren Kommunikationsinfrastruktur für den Betrieb eines Energienetzes mit intelligenten Sensoren und Messstellen unabdingbar[2]. Im Rahmen des Forschungsprojekts ‚eSafeNet' werden dazu Lösungsansätze entwickelt und in einem interaktiven Demonstrator dargestellt, um die Ergebnisse auf das Energienetz übertragen zu können. Im Folgenden wird die Projektidee vor- und die Umsetzung des Demonstrators dargestellt.

Intelligente Stromnetze erfordern eine neue Kommunikations- und Energieinfrastruktur

Im Rahmen des Forschungsprojekts ‚eSafeNet' wurden zunächst die steigenden Anforderungen an die Kommunikations- und Energieinfrastruktur identifiziert. Aufgrund der zunehmenden Einbindung dezentraler Erneuerbare-Energie-Erzeugungsanlagen in virtuelle Kraftwerke erfordert die zukünftige Informations- und Kommunikationsinfrastruktur einen bidirektionalen Informationsfluss. Zugleich ist ein hohes Maß an Verfügbarkeit, Zuverlässigkeit, Echtzeitdatenübertragung, Energieeffizienz und Sicherheit im Rahmen der Energiewende unabdingbar.

Daher wurden verschiedene kabellose und kabelgebundene Kommunikationstechnologien auf ihr Potenzial im Internet der Energie überprüft. Neben der Wirtschaftlichkeit sind insbesondere lokale Unterschiede zu berücksichtigen. Die Verfügbarkeit kabelloser Übertragungstechnologien ist regional sehr unterschiedlich. Zudem müssen die Technologien hinsichtlich weiterer Kriterien, wie bspw. Gebäudetopologie und Baudichte, auf ihr Einsatzpotenzial überprüft werden, sodass der Lösungsansatz nicht aus einer gesamteinheitlichen Technologie besteht, sondern sich individuelle standortabhängige und teilweise sogar kombinierte Technologien ergeben. In dem vernetzten Demonstrator (s. Bild 1, S. 26) wird die Kombination verschiedener Übertragungstechnologien dargestellt. So werden Energieerzeugungsdaten einer Windenergieanlage mittels LTE-Übertragung in der Dienstleistungsplattform dargestellt. Zudem findet eine Übertragung der Energieverbrauchsdaten aus dem Smart Meter der *Demonstrationsfabrik Aachen* mittels 5G statt, sodass sich durch die Einbindung verschiedener Komponenten in den Demonstrator eine modellhafte Abbildung des Energienetzes ergibt.

Neben dem Wandel und den steigenden Anforderungen an die Kommunikationsinfrastruktur erfordert die Energiewende auch die Anpassung der Energieinfrastruktur. Im Rahmen der Klimapolitik wer-

[1] Schulz 2016, S. 19 – 35

[2] Sichler 2014, S. 436 – 494

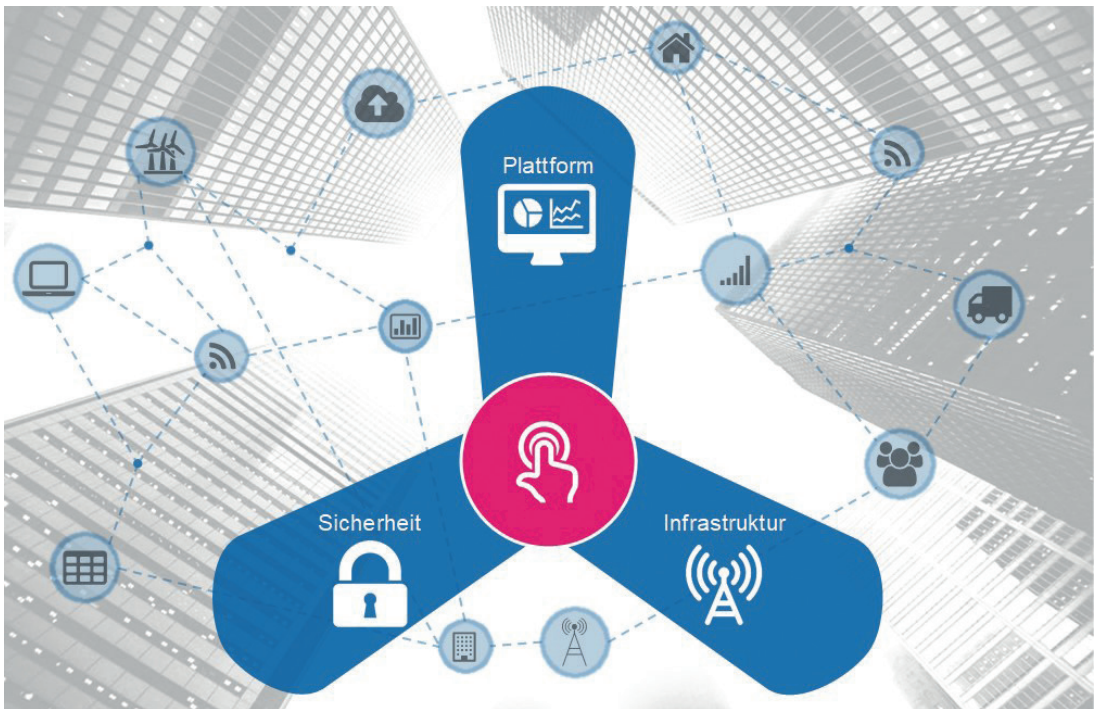


Bild 1: Interaktiver Demonstrator (eigene Darstellung)

den zunehmend fossile Kraftwerke durch die Einbindung dezentraler erneuerbarer Energieerzeugungsanlagen ersetzt.

Aufgrund der fluktuierenden Einspeisung werden diese durch virtuelle Kraftwerke gesteuert und das Energienetz zu Smart Grids weiterentwickelt. Insbesondere die zunehmende Einbindung von Windenergieanlagen in Norddeutschland und von Photovoltaikanlagen in Süddeutschland erfordern den Speicher- und Netzausbau, um auch bei Dunkelflauten die Versorgungssicherheit zu gewährleisten. Zur bildhaften Darstellung des zukünftigen Energienetzes werden in dem Demonstrator die Komponenten wie Solarmodul, Solarregler, Speicher (Blei-Akku), Wechselrichter, Verbraucher und Webbox zur Übertragung der Last- und Erzeugungsdaten aufgebaut.

Eine innovative Dienstleistungsplattform mit Smart Services

Im Forschungsprojekt ‚eSafeNet' werden zudem die Potenziale einer dedizierten Kommunikationsinfrastruktur mittels Mobilfunk- und kabelgebundener Übertragungstechnologien untersucht, um die Interaktion zwischen Verbraucher, Netzbetreiber und Betreiber der Energieerzeugungsanlagen zu ermöglichen. Zur Darstellung der Wirtschaftlichkeit und Generierung von Smart Services durch die Übertragungstechnologien werden diese in einer Dienstleistungsplattform dargestellt.

Als mögliche innovative Dienstleistungen werden bspw. Predictive-Maintenance- (insbes. für Windenergieanlagen) sowie Monitoring- und Alertsysteme zur Lokalisierung kritischer Netzteile eingebunden. Zugleich werden auch die Echtzeitdaten über Erzeugung und Verbrauch in der Plattform dargestellt. In dem Demonstrator können interaktiv verschiedene Angriffsszenarien auf die Dienstleistungsplattform mit Echtzeitdaten aus Erzeugung und Verbrauch bzw. auf das Energienetz simuliert werden.

Die Transformation zum Internet der Energie erfordert neue Sicherheitskonzepte

Durch die zunehmende Vernetzung und Entwicklung eines Smart Grids steigen die Risiken durch verschiedene Angriffsmöglichkeiten auf das Infrastruktur- und Versorgungsnetz, in denen das Energienetz manipuliert oder sogar in seiner Gesamtheit außer Betrieb genommen werden könnte. Cyber-Security gewinnt zunehmend an Bedeutung, sodass im Rahmen des Projekts auch entsprechende Anforderungen und Spezifikationen für ein ganzheitliches Daten- und Kommunikationskonzept im Internet der Energie zu definieren und in dem Demonstrator einzubinden sind.

Nachfolgend werden einige der im Projektrahmen identifizierten Angriffsszenarien vorgestellt:

- Cyber-Attacken, Advanced-Persistent-Threats (APT) und unbekannte Bedrohungen stellen aktive Hackerangriffe dar, die das Energienetz manipulieren oder außer Betrieb setzen können. Derartige Angriffe lassen sich durch den Einsatz eines Security-Network-Operations-Centers (SNOC) und durch das Programm Pandora FMS (Pandora Flexible Monitoring System) verhindern; zudem kann vorab eine Prüfung auf Unterwanderung erfolgen.
- Bei Denial-of-Service-Attacken (DoS) finden Angriffe zur Blockierung von Diensten statt. Bei einem Distributed-Denial-of-Service (DDoS)

werden massenhaft Datenpakete an den Server geschickt, die teilweise auch als Ablenkungsmanöver dienen, um Schadsoftware für Datendiebstahl zu installieren. DDoS-/DoS-Attacken können ebenfalls mittels SNOC abgewehrt werden.

- Neben webbasierten Angriffsszenarien sind auch physische und organisatorische Angriffe zu berücksichtigen, bei denen durch Vandalismus, Datenmanipulation, Datendiebstahl und Man-in-the-Middle-Angriffe das Energienetz gefährdet werden kann. Als Abwehrmaßnahme ist dafür ein Security-Organisationskonzept unabdingbar, bei dem Verschlüsselungen und Zugangskontrollen auf den Service-Ports sowie Videoüberwachungen und Personen- bzw. Zugangskontrollen erfolgen.

Das zukünftige Energienetz generiert innovative Dienstleistungen

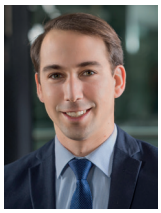
Die Projektergebnisse und der Demonstrator verdeutlichen, dass die zukünftige Informations- und Kommunikationsstruktur für das Internet der Energie aus standortabhängigen und individuellen Lösungen besteht, in denen verschiedene kabellose und kabelgebundene Übertragungstechnologien miteinander kombiniert werden. Zugleich ergibt sich Potenzial für neue Technologien, aus denen sich Smart Services als innovative Energiedienstleistungen im Internet der Energie entwickeln lassen. So können zukünftig bspw. Gebäude mit PV-Anlagen als Prosumer agieren und ihren Überschussstrom mittels Blockchain-Technologie an ihre Nachbarn verkaufen. Der Demonstrator befindet sich zurzeit in der Entwicklung und wird demnächst im Cluster Smart Logistik in Aachen ausgestellt sowie zukünftig auf verschiedenen Messen präsentiert.

Literatur

Schulz, D.: Elektrische Energieversorgung. In: Energiewende – Quo vadis? Beiträge zur Energieversorgung. Hrsg.: F. Joos. Springer Vieweg, Wiesbaden [u. a.] 2016, S. 19 – 35.

Sichler, R.: Smart und sicher – geht das? In: Smart Market. Vom Smart Grid zum intelligenten Energiemarkt. Hrsg.: C. Aichele; O. D. Doleski. Springer Vieweg, Wiesbaden 2014, S. 463 – 494.

Ansprechpartner:



Vasco Seelmann, M.Sc.
Wissenschaftlicher Mitarbeiter
FIR, Bereich Informationsmanagement
Tel.: +49 241 47705-512
E-Mail: Vasco.Seelmann@fir.rwth-aachen.de

Markus Schwank
Studentische Hilfskraft
FIR, Bereich Informationsmanagement

Frederick Birtel, M.Sc.
Wissenschaftlicher Mitarbeiter
FIR, Bereich Dienstleistungsmanagement
Tel.: +49 241 47705-204
E-Mail: Frederick.Birtel@fir.rwth-aachen.de

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Projekttitel: eSafeNet

Projekt-/Forschungsträger: BMWi; PtJ

Förderkennzeichen: 03ET7549A

Assoziierte Projektpartner: Power Plus Communications AG; psm Nature Power Service & Management GmbH & Co. KG; Quantec Systems GmbH

Projektpartner: Forschungscampus FEN; Ericsson GmbH; Institute for Automation of Complex Power Systems (ACS) – RWTH Aachen; Kalinowski Consulting GmbH; QSC AG; Software AG; SOLIT SYSTEMS GmbH; Stadtwerke Mainz AG

Internet: e-safe-net.de