

Industrial IoT für Smart Grid-Anwendungen im Feld

T. Gawron-Deutsch IEEE, K. Diwold, S. Cejka, M. Matschnig, A. Einfalt

Die Energiewende bewirkt eine Transformation des Energiesystems, die zu großen Herausforderungen für den Verteilernetzbetrieb führt. Dies ist der Tatsache geschuldet, dass bis dato passive Verteilernetz-Abschnitte, welche historisch reine Verbraucher waren, nunmehr durch dort verortete dezentrale Erzeugung und proaktive Netzteilnehmer – wie Photovoltaikanlage, Speicher und E-Mobility – aktiv Einfluss auf den Netzbetrieb nehmen. Durch die Integration und den Einsatz intelligenter Automatisierung sollen diese Netzabschnitte in Zukunft aktiv gesteuert werden. Das daraus resultierende Gesamtsystem stellt ein cyber-physikalisches System dar, dass durch einen hohen Komplexitätsgrad gekennzeichnet ist und die elektrische und algorithmische Welt mittels geeigneter IKT-Infrastruktur koppelt. Es ist davon auszugehen, dass die Steuerung und Automatisierung in solchen Systemen immer individueller wird. Dafür bedarf es flexibler und (hinsichtlich Installation und Wartung) einfach zu bedienender Automatisierungssysteme, die es den Betreibern von Verteilernetzen erlauben, individualisierte Lösungen nahtlos in ihren Netzen zu integrieren. Dieser Beitrag beschreibt einen Systemansatz, der aufbauend auf einer Industrial Internet-of-Things(IoT)-Plattform die Interaktion der notwendigen physikalischen Modelle und Anwendungen realisiert und somit zur Lösung dieser Herausforderungen eingesetzt werden kann.

Schlüsselwörter: Smart Grid; Industrial IoT; Cyber-Physical System; massiv verteilte Systeme

Industrial IoT for Smart Grid in-field analytics.

Currently an increased integration of distributed energy resources and prosumers into the distribution system can be observed. These new resources range from renewable energy resources such as PV-systems, to storage systems, and e-mobility charging stations. This trend is coined under the term “Energiewende” and presents a challenge for the system operators, as the grid-level (where the integration of these entities happens) was initially designed for distribution purposes only and was thus operated passively. In order to mitigate and solve resulting problems, intelligent automation systems can be used to actively operate these grids. The resulting system constitutes a cyber physical system, which is characterized by a high degree of complexity and connects the electrical and the algorithmic world, using a suitable ICT infrastructure. As the control and automatization of such systems becomes more and more individual, flexible and simple to use (regarding installation and maintenance) automation systems are required, which allow the operator the seamless integration of individualized solutions into their grids. This article describes a system approach that is based on industrial Internet-of-Things technology and allows realizing the required interaction between the physical models and applications; thus presenting a solution to solve these challenges.

Keywords: Smart Grid; industrial IoT; Cyber-Physical System; massively distributed systems

Eingegangen am 19. Februar 2018, angenommen am 5. Mai 2018, online publiziert am 7. Juni 2018
© Springer-Verlag GmbH Austria, ein Teil von Springer Nature 2018



1. Einleitung

Unter dem mittlerweile etablierten Begriff „Energiewende“ versteht man im Allgemeinen den Übergang von der nicht-nachhaltigen Nutzung von fossilen Energieträgern sowie der Kernenergie zu einer nachhaltigen Energieversorgung, weitestgehend basierend auf der Nutzung erneuerbarer Energien. Die effiziente Umsetzung der „Energiewende“ gilt als eine der wichtigsten gesellschaftspolitischen Herausforderungen, um einerseits im globalen Maßstab Klimaziele einhalten zu können, aber auch um andererseits lokal eine lebenswerte Umwelt sicherzustellen [1]. Nach den ersten Jahren der konzentrierten, großtechnischen Nutzung von erneuerbaren Energieträgern, z. B. durch Windparks, hat sich zuletzt vor allem die massiv verteilte Erzeugung durch PV-Anlagen – großteils im Niederspannungsnetz – etabliert. Hinzu kommt nun der allgemeine Trend der Substitution von bisher fossilen Energieträgern, z. B. für Raumwärme und Individualmobilität, durch elektrifizierte Anwendungen. PV-Anlagen in Kombination mit Wärmepumpen und zunehmend auch Ladestellen für E-Fahrzeuge führen zu neuen Herausforderungen für den Verteilernetzbetrieb.

Für die Netzplaner ändern sich die bisherigen Regeln bezüglich Gleichzeitigkeit, Richtung des Lastflusses, etc. Deshalb müssen Methoden zur Netzauslegung an die neuen Situationen angepasst werden. Dezentrale Erzeugungsanlagen bzw. neue Lasten führen vorwiegend in ländlichen Netzen zu lokalen Spannungsschwankungen („U-Problem“). Fluktuierende Erzeugung und hohe Energiepreisdynamik (z. B. spotmarktgeführte Tarife) können sprunghafte Auslastungsspitzen der Netzinfrastruktur nach sich ziehen. Dezentrale Erzeugung in Kombination mit Starklasten mit hoher Gleichzeitigkeit (z. B. Elektromobilität und Wärmepumpe) können zur nicht abgesicherten Überlastung einzelner Kabelabschnitte führen („I-Problem“).

Gawron-Deutsch, Tobias, Siemens AG Österreich, Siemensstraße 90, 1210 Wien, Österreich (E-Mail: tobias.gawron-deutsch@siemens.com); **Diwold, Konrad**, Siemens AG Österreich, Siemensstraße 90, 1210 Wien, Österreich; **Cejka, Stephan**, Siemens AG Österreich, Siemensstraße 90, 1210 Wien, Österreich; **Matschnig, Martin**, Siemens AG Österreich, Siemensstraße 90, 1210 Wien, Österreich; **Einfalt, Alfred**, Siemens AG Österreich, Siemensstraße 90, 1210 Wien, Österreich

Die Erkenntnis für Verteilernetzbetreiber ist, dass sie massiven Netzausbau zur Beherrschung dieser Herausforderung betreiben, was allein aufgrund der Personalressourcen und verfügbarer Investitionsmittel nicht einfach durchführbar sein wird. Daher müssen Betriebsmittel näher an ihren Belastungsgrenzen betrieben werden. Gegenwärtig werden Niederspannungsnetze passiv betrieben und deshalb müssen sie mit mehr Sicherheitsreserven geplant werden als es eigentlich notwendig wäre. Erst ein aktiver Betrieb, der mehr Transparenz bis in die Niederspannungsnetze schafft ermöglicht die Verkleinerung der Sicherheitsreserven. Durch gezielten Einsatz von intelligenter Automatisierungstechnik kann der Netzausbau vermieden oder zumindest genügend Zeit gewonnen werden, um einen effizienteren Netzausbau zu ermöglichen.

Ein intelligentes Stromnetz, welches die skizzierten Herausforderungen mittels intelligenter Automatisierungstechnik bewerkstelligt ist ein klassisches Beispiel eines cyber-physikalischen Systems [2]. Dieser Beitrag beschreibt einen Systemansatz namens iSSN2020 (intelligent Secondary Substation Node), der aufbauend auf einer Internet-of-Things(IoT)-Plattform die Interaktion der notwendigen physikalischen Modelle und Anwendungen realisiert und somit zur Lösung der oben skizzierten Herausforderungen eingesetzt werden kann.

2. Systemanforderungen

Wie aus den Herausforderungen hervorgeht, muss dieses Automatisierungssystem einfach im Feld zu implementieren sein (Plug & Play bzw. Plug & Automate) und sich flexibel an die sich rasch ändernden Rahmenbedingungen anpassen lassen. Wie in früheren Arbeiten vorgestellt [3–5], wurde ein System entworfen, das durch die Nutzung einzelner, abgeschlossener Applikationen eine individuelle Anpassung der notwendigen Funktionalität erlaubt. So ist eine prototypische Implementierung eines auf Industrial IoT basierenden Automatisierungssystems unter Verwendung der existierenden SICAM A8000 Produktfamilie¹ entstanden.

Dieser Beitrag beschreibt ein Anwendungsszenario für dieses zukunftsweisende Automatisierungskonzept für intelligente Verteilernetze. Im Zuge des Projekts iNIS (intelligent Network Information System) erfolgt derzeit zum Funktionsnachweis im Smart Grid Testbed der ASCR (Aspern Smart City Research) ein Proof of Concept. Im Wesentlichen wird dabei die Flexibilität der Applikationsumgebung auf dem intelligenten Automatisierungsgerät – im IoT Kontext als „EDGE-Device“ bezeichnet – gezeigt. Ein Betrieb vollständig ohne zentrale Koordination birgt jedoch auch Nachteile.

In der klassischen Literatur [6] werden drei Arten von verteilten Kommunikationsnetzen unterschieden: zentral, dezentral und verteilt. Ersteres entspricht der klassischen Architektur in der Mittelspannung, in der Fernwerkstationen an eine Zentrale angeschlossen sind. Bei dezentralem Aufbau gibt es nach wie vor einen zentralen Knoten, zu dem die anderen Knoten hierarchisch verbunden sind. In dieser Taxonomie wird ein verteiltes Kommunikationsnetz durch gleichberechtigte Knoten, die vermascht verbunden sind, aufgebaut. Alle drei Arten haben Auswirkungen auf die Anforderungen an die Knoten und die möglichen Anwendungen.

Der zentrale Ansatz eignet sich besonders für die Integration in bestehende Infrastruktur. Dadurch, dass alle Knoten direkt mit der Zentrale verbunden sind, können sie einfach gestaltet sein, ihre Mindestanforderung ist die Datenkommunikation zur Zentrale. Für ein räumlich weit verteiltes System wie ein Smart Grid ist die Anbindung

aller Komponenten an eine Zentrale mit hohen Kosten verbunden. Auch müssen, wenn die aktuelle Gestaltung von Mittelspannungssystemen als Referenz herangezogen wird, alle Daten in die Zentrale übermittelt und dort verarbeitet werden.

Der dritte Ansatz – verteilt – hat hohe Anforderungen an die Knoten. Da es keine Zentrale gibt, müssen die Knoten gemeinsam eine Strategie aussuchen und sie umsetzen. Das bedeutet, dass ein einzelner Knoten mehr Information haben und verarbeiten können muss, als für seine eigentliche Aufgabe (z. B. als Trennstellenschalter) notwendig wäre. Der Austausch der zusätzlichen Information ist auch mit einem erhöhten Kommunikationsaufwand verbunden. In seiner extremsten Ausprägung ist dieser Ansatz ein selbstorganisierendes System, welches schwer zu modellieren und konträr zur gegenwärtigen Betriebsphilosophie der Verteilernetzbetreiber ist. Ein selbstorganisierendes System ist aus Anwendersicht eine Blackbox, bei der, analog zu neuronalen Netzen, nur das Ergebnis, aber nicht der Weg zum Ergebnis betrachtet werden kann. Das Wie und das Warum sich das System so und nicht anders verhalten hat, sind nicht beantwortbar. Ein Verteilernetzbetreiber arbeitet mit einem „Betriebshandbuch“, in dem genau festgelegt ist, wie die Betriebsmittel einzusetzen sind.

Es gibt allerdings eine kleine Menge an Anwendungen, für die der verteilte Ansatz von Bedeutung ist: wenn topologisch benachbarte Knoten eine konkrete Aufgabe mit sehr kurzen Reaktionszeiten zu erfüllen haben. Dazu zählen Fault Localisation and Restauration, adaptiver Schutz und die Durchführung einer zentral geplanten Rekonfiguration des Stromnetzes.

Der für das Smart Grid relevanteste Ansatz ist der dezentralisierte (auch hierarchische). Hier existiert nach wie vor eine Zentrale, die die Strategie vorgibt. Die Knoten entlang der Hierarchie leiten daraus ihre Taktik ab. Das hat zur Folge, dass „Intelligenz“ (d. h. Algorithmen und Entscheidungshoheit) von der Zentrale in die Feldebene abgegeben wird. Die somit (teil-)autonomen Knoten können schneller reagieren und auch andere, hierarchisch ihnen untergeordnete Knoten, koordinieren. Im Gegensatz zum zentralen Ansatz wird mehr Rechenleistung für die Knoten erforderlich. Im Gegenzug wird die Zentrale entlastet und nur mehr die Daten an die Zentrale weitergeleitet, die für diese von Relevanz sind. Das sind typischerweise Kennzahlen, Status und außergewöhnliche Ereignisse.

Analog zu der Verschiebung von Zentral zu Dezentral (und teilweise zu Verteilt) wird auch ein Paradigmenwechsel bezüglich der Automatisierungspyramide beobachtet [7]. Die strikte Aufteilung in die verschiedenen Ebenen verschiebt sich in Richtung einer vermaschten Struktur, bei der Teilfunktionalitäten der einzelnen Ebenen miteinander direkt interagieren (auch über ehemals nicht benachbarte Ebenen hinweg).

Das Projekt MASGrid [8] hat sich mit einer verteilten Struktur für den Betrieb eines Smart Grids beschäftigt. Die resultierende Architektur entspricht in der obigen Terminologie einem dezentralisierten Ansatz. Nur durch eine Hierarchie kann ein Multiagentensystem gestaltet werden, das den sicheren Betrieb des Stromnetzes ermöglicht. Die allgemeinere Fragestellung – wie viel Dezentralisierung, wie viel Zentralisierung ist notwendig – wurde unter anderem im Forschungsprojekt ICT4RobustGrid [9] bearbeitet.

Um diese Fragestellung nicht nur in einer theoretischen Arbeit, sondern an einem realen System zu bearbeiten, wird im Proof of Concept der Vorteil der sich aus einer zentralen, analytischen Untersuchung in Kombination einer Datenvorverarbeitung auf den EDGE-Devices gezeigt. Hierbei werden Kennzahlen, die von vielen EDGE-Devices stammen, verarbeitet und daraus Parameter abgeleitet. Bei der Gestaltung des Proof of Concept wurden sowohl ein Prozessziel als auch ein Funktionsziel verfolgt.

¹ <http://w3.siemens.com/smartgrid/global/de/produkte-systeme-loesungen/stationsautomatisierung/stationsautomatisierung/Pages/SICAM-A8000.aspx>.

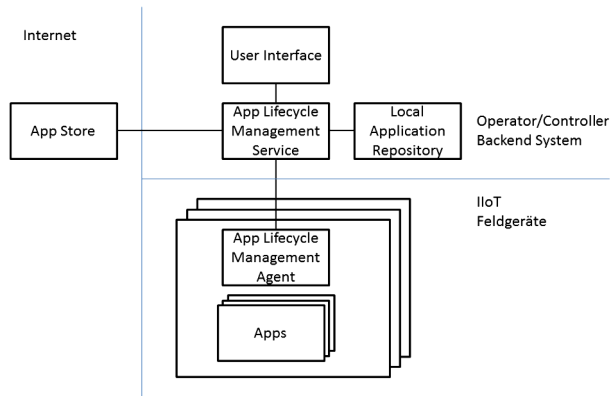


Abb. 1. System-Architektur der iSSN 2020 Industrial IoT-Plattform

Prozessziel: Es soll der gesamte Ablauf gezeigt werden, der notwendig ist, damit ein Operator (= eine Kombination aus Leitwarte-techniker und Systemadministrator) eine App installieren und starten kann, die Ergebnisse der App angezeigt bekommt und sie schlussendlich wieder deinstallieren kann.

Funktionsziel: Es soll gezeigt werden, wie eine Analyse-App am Gerät mit einer Analyseanwendung im Backend sinnvoll miteinander interagieren können. Es werden gleichzeitig zwei Konfigurationsarten demonstriert:

- Es soll der Vorteil der zentralen Datenanalyse und der Ableitung von Konfigurationsparametern gezeigt werden. Verteilte intelligente Geräte im Feld liefern dafür Daten und erst über die „Welt-sicht“ der zentralen Instanz im Backend kann eine entsprechende für alle geltende Konfiguration gefunden werden.
- Es soll eine individuelle Konfiguration gefunden werden. Dazu werden im ersten Schritt nur Daten in das Backend geliefert. Aus diesen Daten wird automatisiert eine individuelle Konfiguration erstellt. Diese kann dann auf eine operative App, „personalisiert“ für ein bestimmtes Netz, geladen werden.

3. IIoT-Plattform

Wir unterscheiden in diesem Beitrag zwischen (consumer) IoT und industrial IoT (IIoT). Unter ersterem verstehen wir Geräte, die mit einem Cloud-Dienst verbunden sind, „best-effort“ Quality-of-Service haben, immer mit dem Internet verbunden sind und bei denen ein Ausfall im Normalfall maximal einen Komfortverlust bedeutet. Weiters gibt es nur sehr reduzierte (meisten vordefinierte) Interaktionsmöglichkeiten zwischen Geräten in einem System in dem es einen Dienstanbieter und einen Kunden gibt (aus Kundensicht); Interaktionen zwischen mehreren Systemen und verschiedenen Dienst-anbietern sind nicht, oder nur sehr beschränkt, vorgesehen. Dem gegenüber steht das IIoT – zu den wichtigsten Eigenschaften zählen wir, dass Geräte hier eine höhere Verfügbarkeit aufweisen müssen, auch bei Ausfall der Kommunikation weiter funktionieren, längere Produktlebenszyklen ermöglichen, den Betrieb in einem massiv ver-teilten System unterstützen, sowie die Geräte Teil eines „System of Systems“ sind. Weiters muss es möglich sein die Konfiguration den individuellen Bedürfnissen der Domäne/des Kunden mit möglichst geringen Kosten anzupassen. Die vergleichsweise geringen Stück-zahlen, der hohe Bedarf an Anpassung an die jeweilige Anwendung verbunden mit dem Kostendruck sind eine besondere Herausfor-derung. Im consumer IoT Umfeld wird dem Kostendruck durch sehr hohe Stückzahlen und nur wenige Ausprägungen begegnet.

Die Systemarchitektur der Industrial IoT-Plattform zur Realisierung einer Secondary Substation Node, ist in Abb. 1 dargestellt. Die

Systemkomponenten und Services werden folgend im Detail be-schrieben. Der Fokus liegt hierbei auf den Funktionalitäten, die für die nachfolgend beschriebene Anwendung benötigt werden. Die Kommunikation zwischen den einzelnen Komponenten ist IP-basiert und es werden Standardinternetprotokolle wie XMPP oder REST-Interfaces verwendet. Als Betriebssystem auf den Feldgeräten wird ein Linux mit einem Real-Time-Patch verwendet.

3.1 Application Lifecycle Management Service

Eine Komponente im zentralen Backend ist das Application Lifecycle Management zur Verwaltung von Softwarekomponenten (kurz Apps) auf Geräten im Feld. Folgende – in [4] als Application Pro-visioning Tasks bezeichnete – Lifecycle-Management-Funktionalitäten wurden identifiziert:

- Installieren eines Anwendungs-Moduls
- Starten des Anwendungs-Moduls
- Stoppen des Anwendungs-Moduls
- Deinstallieren des Anwendungs-Moduls
- Information über den Status der (installierten) Anwendungs-Module
- Konfiguration des Anwendungs-Moduls (im laufenden Betrieb)
- Update des Moduls (im laufenden Betrieb)

Je nach Anwendungsfall und der verwendeten Hardware unter-scheidet sich die Implementierung der oben genannten Module. Die Java-basierte Umsetzung eines Frameworks welches die genannten Funktionalitäten zur Verfügung stellt, wird in [3, 4] detailliert bespro-chen. Es besteht aus einem Web-Dashboard auf Backendseite, über welches die Applikationen und deren Konfiguration auf dem Feld-gerät verwaltet werden und der geräteseitigen Gegenstelle, welche die Java Applikationen startet, stoppt und konfiguriert. Die Kommu-nikation zwischen Backend-System (UI) und dem Feldgerät wurde in dieser Umsetzung über das Extensible Messaging and Presence Pro-tocol (XMPP) realisiert. Es wurde bei der Konzeptionierung darauf geachtet, dass Alternativen wie REST-Schnittstellen und das MQTT-Protokoll (Message Queue Telemetry Transport) ebenfalls verwendet werden können.

Wie in Abb. 1 ersichtlich ist, existiert im zentralen Backend neben der Kernkomponente (Application Lifecycle Management Service) und der grafischen Benutzeroberfläche auch ein lokales Applikations- und Lizenzarchiv. Das User Interface am Backend ver-waltet beliebig viele Feldgeräte und bietet die Möglichkeit zum ein-fachen Verwalten der Apps; sie können von hier installiert, gestar-tet, konfiguriert, gestoppt und wieder deinstalliert werden. Um eine neue Funktionalität auf das Feldgerät zu bringen wird das EDGE-Device und die dort zu installierende Applikationen ausgewählt und dadurch der Installationsprozess gestartet. Da nicht in jedem An-wendungsfall davon ausgegangen werden kann, dass die Feldgerä-te permanent mit dem Backend verbunden sind, wurden zwei Lö-sungen konzipiert: Push- und Pull-Betrieb. Im Push-Betrieb wird von einer kontinuierlichen Verbindung ausgegangen und die Komman-dos werden sofort an das Gerät übertragen. Demgegenüber steht der Pull-Betrieb: hier wird die Interaktion periodisch durch das Gerät initiiert und die Befehle werden mit entsprechender Zeitverzögerung durchgeführt.

Ein wichtiges Element in consumer IoT ist die Möglichkeit mit-tels eines Application Stores (z. B. Google Play-Store) Apps auf das Gerät zu installieren. In dem iSSN2020-Ansatz verfolgen wir die Phi-losophie, dass externe Systeme nicht auf die Feldgeräte zugreifen dürfen. Dies erfordert eine alternative Architektur für Application Stores. In Abb. 1 ist der AppStore im Internet und somit außer-halb des Backends angesiedelt. Da ein Push-Betrieb – im AppSto-re eine App kaufen und diese direkt ins Backend/aufs Gerät spielen

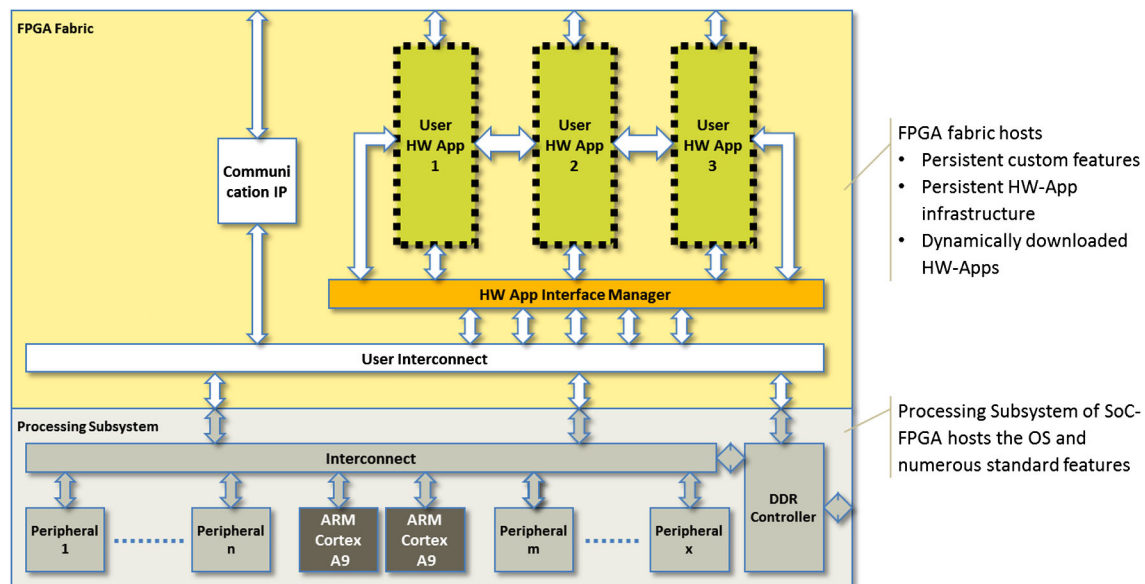


Abb. 2. FPGA-Architektur der iSSN 2020

– nicht erlaubt ist, gibt es zwei alternative Möglichkeiten, wie die App und die dazugehörige Lizenz ins Backend eingespielt werden kann. Die erste ist der manuelle Import. Hier wird die App gekauft, anschließend die entsprechenden Dateien heruntergeladen, auf das Backendsystem kopiert und dort über die grafische Benutzeroberfläche importiert. Der Vorteil hier ist, dass das Backend strikt vom Internet entkoppelt sein kann. Die zweite Alternative ist ein Pull-Betrieb. Dafür ist eine eigene Komponente im Backend vorgesehen, die regelmäßig im AppStore überprüft, ob neue/aktualisierte Apps und Lizenzen verfügbar sind. Diese werden dann automatisch ins System übernommen und können entsprechend weiter verarbeitet werden. Neben der nahtlosen Integration hat dieser Ansatz den Vorteil, dass Updates von Apps automatisch im Backend angezeigt und zur Verfügung gestellt werden können.

Damit die beschriebene Lösung anwendungsfallunabhängig ist, wurde darauf geachtet, dass alle Komponenten über definierte Schnittstellen verfügen und die Kommunikationsprotokolle austauschbar sind.

3.2 Application Lifecycle Management Agent

Auf Geräteseite wurde ein generischer Application Lifecycle Management Agent entwickelt, der durch den Aufruf definierter umsetzungsspezifischer Skripte die genannten Modulimplementierungen unterstützt. In der Implementierung für die iSSN auf der SICAM A8000 Familie können damit sowohl hardware-unterstützte Apps auf dem FPGA (Field Programmable Gate Array), als auch Software-Apps in LXC (LinuxContainers) Containern gemanagt werden. Zur Implementierung der Funktionalität „Information über den Status der (installierten) Anwendungs-Module“ ist ein periodischer Health-Check der Applikationen vorgesehen.

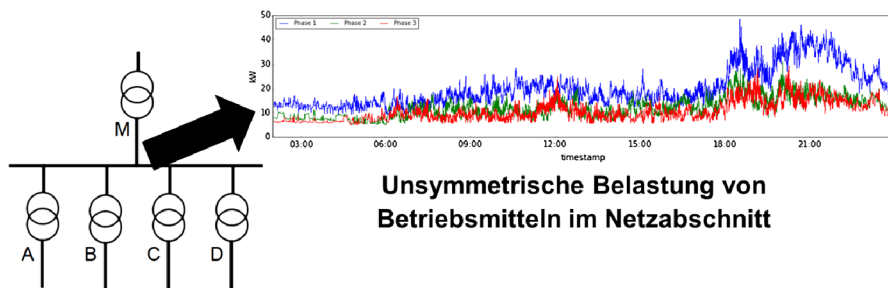
3.3 Hardware-Anwendungen (als flexible Beschleuniger für Software-Anwendungen)

Wie zuvor beschrieben, werden neben Software Applikationen auch Hardware-unterstützte Applikationen auf der iSSN eingesetzt. Diese Applikationen werden mittels Field Programmable Gate Arrays realisiert [10]. Ein zentraler Bestandteil der zugrunde liegenden Hardware-Plattform ist daher ein System-on-a-Chip (SoC) FPGA,

welcher neben dem eigentlichen Dual Core Prozessor Subsystem, auch über einen rekonfigurierbaren Bereich verfügt. Das Prozessor Subsystem besteht aus zwei ARM Cortex A9, dem Speicherkontroller (DDR Controller), verschiedenen Peripheriemodulen wie Zeitgeber oder Schnittstellen und einem Bus. In dem rekonfigurierbaren FPGA-Teil werden in erster Linie echtzeitkritische Systemfunktionen realisiert (Communication IP), wobei aber gleichzeitig ein Teil der verfügbaren Logik zur Unterstützung von SW-Apps vorgesehen ist. Diese Anforderung bedingt, dass analog zur SW-App auch die entsprechenden FPGA-Teile dynamisch nachgeladen werden müssen. Die beschriebene Funktionalität wird durch Ausnutzung des „Dynamic Partial Reconfiguration“ Mechanismus des verwendeten FPGA-Bausteines realisiert. Dabei wird die frei programmierbare FPGA-Fläche in Partitionen aufgeteilt, welche im Betrieb, d. h. ohne sich wechselseitig zu beeinflussen, rekonfiguriert werden können (siehe Abb. 2).

In der aktuellen Anwendung wurde somit das klassische Applikationskonzept dahingehend erweitert, dass für jede SW-Applikation auch die Möglichkeit besteht, einen Teil des FPGA zu nutzen. Die zusätzliche HW-Funktionalität wird dabei in Form eines FPGA-Ladefiles zusammen mit dem SW-Image der App via Application Lifecycle Management auf das Feldgerät geladen, installiert und gegebenenfalls deinstalliert. Die Interaktion der SW-App mit der zugehörigen HW-App kann auf unterschiedliche Arten erfolgen, beispielsweise über File-IO, Memory-mapped oder einen Device-Treiber.

Im iSSN Umfeld, bzw. der Substation Automation finden sich vielfältige Anwendungsszenarien für HW-Applikationen. Besonders im Bereich der Messdatenerfassung und Aufbereitung können rechenintensive Aufgaben in das FPGA ausgelagert werden. Konkret wurden eine exemplarische HW-App zur Umsetzung einer Teilfunktion des später beschriebenen Grid-Watch-Dogs realisiert. Dabei handelt es sich um eine Floating-Point-Engine zur KPI-Berechnung (Key Performance Indicator). In Zukunft ist geplant auch anspruchsvollere HW-Apps wie ein neuronales Netz zur Vorhersage von Betriebszuständen im Niederspannungsnetz umzusetzen.



Unsymmetrische Belastung von Betriebsmitteln im Netzabschnitt

Abb. 3. Dezentrale Ermittlung der Leistungsasymmetrie in einem Mittelspannungsnetzabschnitt (beispielhafter Tagesverlauf der Wirkleistungsflüsse auf den drei Phasen eines urbanen Niederspannungsnetzabschnitts)

4. Smart Grid-Cyber-Physical-System-Anwendung im Kontext einer intelligenten Ortsnetzstation

Mit Hilfe der dargestellten IoT-Plattform soll im Folgenden eine relevante Anwendung des Systems dargestellt werden. Die Anwendung basiert auf folgendem Szenario: Ein Verteilernetzbetreiber betreibt in der Regel eine Vielzahl von Niederspannungsnetzen [11]. Um Auslastungsgrad und Verluste zu optimieren, möchte dieser eine möglichst ausgeglichene Belastung der drei Phasen sicherstellen. Um das verfügbare Investitionsbudget möglichst effizient einsetzen zu können ist es unabdingbar einen Überblick über auftretende Probleme zu bekommen. Die Asymmetrie der Leistung in diesen Netzen ist von den in den Netzen installierten Erzeugern und Verbrauchern bestimmt. Durch die Volatilität von Erzeugung und Verbrauch kann die Asymmetrie einzelner Netze signifikant schwanken und das Asymmetrieverhalten unterscheidet sich netzabhängig.

Um nun für den Netzabschnitt eines Mittelspannungsnetzes M (in Abb. 3 skizziert) die Top 1-%-Leistungsasymmetrie der unterlagerten Niederspannungsnetze A, B, C und D zu ermitteln, kann bei entsprechender, im Niederspannungsnetz installierter Monitoringinfrastruktur, eine Aufzeichnung der Leistungsdaten (beispielsweise am Niederspannungstransformator und in ausgewählten Netzverteilerkästen) erfolgen. Diese Aufzeichnung kann im Nachgang für die Netzplanung herangezogen werden. 1 % ist hier ein willkürlich gewählter Wert, der je nach realem Bedarf entsprechend angepasst werden kann.

Da die Anzahl der durch einen Verteilernetzbetreiber zu betreuenden Netze mit abfallender Spannungsebene stark ansteigt [11], würde die Speicherung aller an den Transformatoren aller Niederspannungsnetze anfallenden Leistungswerte eine signifikante Datenmenge darstellen. Abhängig von der dem Verteilernetzbetreiber zur Verfügung stehenden IKT (Informations- und Kommunikationstechnik) Infrastruktur, kann die Übertragung und Speicherung dieser Daten signifikante Betriebskosten mit sich führen. Im konkreten Anwendungsfall muss die gewählte Lösung sowohl die Betriebskosten als auch die Investitionskosten berücksichtigen.

Die Errechnung solcher spezifischen, für Planung und Betrieb relevanten, KPIs wie Asymmetriebewertungen kann aber auch durch lokale, in einer intelligenten Ortsnetzstation instanziierten Anwendungen dezentral und verteilt durchgeführt werden. Hierzu werden die an den einzelnen Ortsnetzstationen vorliegenden Asymmetrieverhalten mittels individueller, durch das Backend vorgegebener Schwellenwerte überwacht. Bei einer Überschreitung des Schwellenwerts erfolgt eine Übermittlung der Asymmetriewerte an das Backend. Anhand der eingehenden Asymmetriewerte können die Schwellenwerte in den einzelnen Ortsnetzstationen angepasst werden unter Berücksichtigung der Werte die durch andere Ortsnetzstationen eingehen. Die Verwendung eines solchen dezentralen Ansatzes reduziert das Übertragungsaufkommen und damit einhergehend die notwendige Bandbreite. Außerdem reduziert sich dadurch

der backendseitige Speicheraufwand signifikant, da es nur bei Bedarf zur Datenübertragung kommt.

Zur Realisierung dieses Anwendungsfalls bedarf es iSSN-seitig mehrerer Anwendungen:

- **Measurement Applikation (MeaApp):** Diese Applikation stellt die south-bound Schnittstelle zu den im Netz installierten Grid-Monitoring-Devices (GMD) und Sensoren (und damit dem elektrischen Teil des Cyber Physical Systems) dar. Andere Anwendungen können über einen Subscribe Mechanismus zur Verfügung stehende Datenpunkte erfragen bzw. abonnieren und werden bezüglich neuer Messwerte zu diesen Datenpunkten von der MeaApp informiert.
- **Grid Watch Dog (GWD):** Diese Anwendung übernimmt das Netzmonitoring auf Basis der durch die MeaApp bereitgestellten Messwerte. Durch definierte Regeln können einfache KPIs im Netz ermittelt werden wie beispielsweise das Über- beziehungsweise Unterschreiten definierter Schwellenwerte. Die Definition der KPIs erfolgt durch den Nutzer in Form von Regeln welche einer DSL (Domain-Specific-Language) entsprechen. Bei Eintreten eines KPIs erfolgt die Benachrichtigung spezifizierter Nutzer (beispielsweise ein Leitwarten-Alert) bzw. nachgelagerter Applikationen (beispielsweise Abregelungsmechanismen). Das Update am GWD ausgeführter KPIs kann durch ein Update aus dem Backend erfolgen.
- **Hardware-unterstützte Berechnung komplexer Kennwerte (GWD-HW-App):** Wie im Kapitel IIoT-Plattform bereits beschrieben verfügt die verwendete Hardware-Plattform über einen SoC FPGA, welcher für echtzeitkritische Systemfunktionen, bzw. zur Auslagerung rechenintensiver Prozesse genutzt werden kann. Durch den GWD können nur sehr simple KPIs realisiert werden. Dies ist der Tatsache geschuldet, dass die durch die MeaApp eingehenden Messwerte nur die phasenscharfe Spannungs- und Leistungswerte des unterlagerten elektrischen Netzes darstellen. Die Errechnung komplexerer Kennzahlen aus den eingehenden Messwerten (beispielsweise ein zusammengefasster KPI mit Gewichtungen für einzelne Asymmetrien von Spannung oder Strom) ist mathematisch anspruchsvoll und kann somit einen Großteil der einer Applikation zur Verfügung stehenden Ressourcen beanspruchen. Zur Entlastung des Systems können solche Berechnungen auf den FPGA ausgelagert werden. Im vorliegenden Fall wird im GWD durch eine HW-App die Errechnung von Stromasymmetrie realisiert. Das ermöglicht die Überwachung zusätzlicher KPIs (seitens des GWDs) hinsichtlich dieser komplexen Werte.

Außerdem ist backend-seitig eine Analytics-Applikation notwendig die die eingehenden Asymmetriewerte analysiert und auf Basis der eingegangenen Werte die Schwellenwerte der einzelnen GWD-Instanzen anpasst.

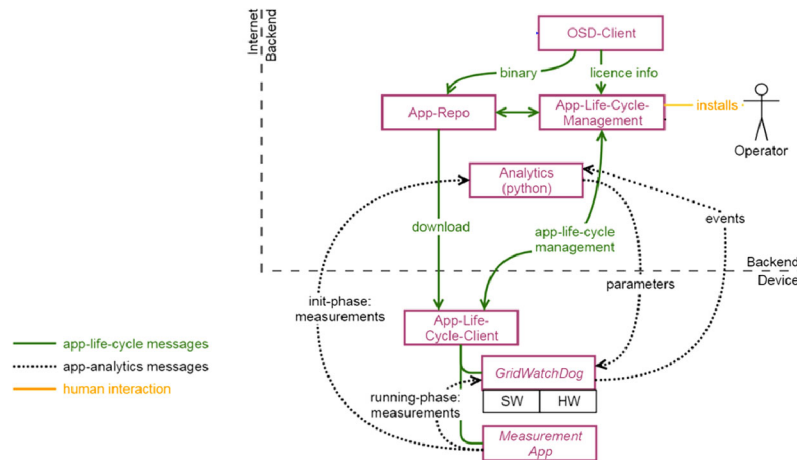


Abb. 4. Systembild dezentrale Ermittlung von Asymmetrieverhalten in einem Mittelspannungs-Netzabschnitt

4.1 Umsetzung

Die benötigten Anwendungen wurden als Microservices spezifiziert [12]. Dieses Architekturmuster wurde bewusst gewählt um die Dienste weitgehend von einander zu entkoppeln. Die Kommunikation zwischen den iSSN Anwendungen ist nicht durch die IoT-Plattform spezifiziert, je nach Anwendungsfall können zum Austausch zwischen den Applikationen unterschiedliche Protokolle zur Anwendung kommen. Im vorliegenden Fall erfolgt der Informationsaustausch zwischen den Komponenten mittels Representational State Transfer (REST). REST stellt kein spezifisches Kommunikationsprotokoll beziehungsweise Standard dar, sondern definiert ein Webservice Paradigma zur Definition von Applikationsschnittstellen, wobei Interaktionen zwischen Anwendungen mittels atomarer Operatoren des HTTP Protokolls realisiert werden [13]. Die Spezifikation der Schnittstellen erfolgte mittels Swagger, einer Tool-sammlung zum Design, Bau und Dokumentation von RESTful Web Services [14]. Durch den Einsatz von LXC Containertechnologie im Kontext der IoT-Plattform sind die Anwendungen umsetzungsagnostisch und wurden sowohl in Java als auch in Python implementiert. Auch diese Anwendung wurde als Microservice mit entsprechenden REST-Schnittstellen konzipiert und implementiert. Die HW-App wurde GWD-seitig dahingehend integriert, dass die GWD-Applikation eingehenden Messwerte für den Einsatz auf dem FPGA vorbereitet und die Durchführung FPGA-basierender Berechnungen initiiert.

4.2 Prozessablauf

Im Folgenden soll der Prozessablauf des Anwendungsfalls skizziert werden, die Systeminteraktion ist in Abb. 4 dargestellt.

4.3 Prozess: Installation und Verwaltung

Der Ablauf beginnt mit der Installation der Anwendungen auf den intelligenten Ortsnetzstationen (die dabei durchgeführten Interaktionen sind in Abb. 4 in der Farbe Grün dargestellt). Dazu wird durch den Operator das backend-seitige Dashboard geöffnet. Dieses zeigt die für die Ortsnetzstationen verfügbaren Anwendungen, welche im App-Repository hinterlegt sind, an. In das Backend importiert werden sie durch die im Abschn. 3 beschriebene Komponente, die einen Pull-Betrieb mit einem (hier fiktiven) AppStore realisiert (OSD-Client - Online Software Delivery). Anschließend weist der Operator über das Dashboard an, die Anwendungen MeaApp, GridWatchDog (Software- und HW-App) auf spezifischen Ortsnetzstationen zu installieren. Diese Anweisungen werden durch das App-Life-Cycle-Management durchgeführt. Vor der Installation erfolgt eine Über-

prüfung der auf den einzelnen Ortsnetzstation, installierten Anwendungen mittels des lokalen App-Life-Cycle-Clients. Sofern die Applikationen dort noch nicht instanziiert sind erfolgt die Anweisung an den App-Life-Cycle-Client die Anwendungen zu installieren. Dieser finale Schritt ist notwendig, um etwaige Inkonsistenzen in der Datenhaltung im Backend bei einem Pull-Betrieb des Clients auszu-schließen. Schlussendlich bezieht der Client die Anwendungen aus dem App-Repository und installiert und instanziiert sie auf dem entsprechenden Feldgerät.

4.4 Prozess: Anwendungsverlauf

4.4.1 Initialisierungsphase

Nach der Installation der Applikationen erhält die Measurement-App kontinuierlich Messdaten von den im elektrischen Netz installierten GMDs und Sensoren. Da an diesem Punkt noch keine Schwellenwerte für die GridWatchDog-Applikationen vorliegen, werden die eingehenden Messdaten in der Initialisierungsphase direkt an die Analytics Anwendung im Backend übermittelt. Auf Basis der initial erhaltenen Messwerte erfolgt in der Backend Analytics App eine erste Schwellenwertberechnung für die an den einzelnen Stationen installierten GridWatchDog-Applikationen. Diese Schwellenwerte werden in Form von Parametern an die entsprechenden GWD-Instanzen übermittelt.

4.4.2 Betriebsphase

Auf Basis der eingegangenen Regeln findet GWD-seitig eine Subscription auf die benötigten Messdatenpunkte statt. Bei eingehenden Messwerten (durch MeaApp) erfolgt die Errechnung der Asymmetrie (durch GridWatchDog-HW-App) und die Überprüfung hinsichtlich der Schwellenwertüberschreitung (durch GridWatchDog-SW-App). Bei einer Schwellenwertüberschreitung wird die Analytics-Applikation im Backend mittels Event über die Überschreitung informiert. Auf Basis dieser Werte können Backend-seitig die Schwellenwerte der einzelnen GridWatchDogs angepasst um schlussendlich aus dem gesamten Netzgebiet nur die Top 1-%-Asymmetriewerte zu erhalten.

4.5 Ergebnisse

Nach einem erfolgreichen Test des vorgestellten Ansatzes im Labor wurde ein Langzeittest der Anwendung im Smart Grid Testbed der ASCR gestartet. Die ersten Tests der Anwendung im Labor deuten

darauf hin, dass die dezentrale Berechnung der benötigten Kennzahlen mit den vorgeschlagenen Methoden möglich ist. Der Einsatz einer FPGA-basierten Berechnung komplexer Kennwerte führt zu einer signifikanten Reduktion der durch die Applikationen benötigten CPU-Rechenleistung (Central Processing Unit).

Die Verwendung eines solchen dezentralen Ansatzes reduziert das Übertragungsaufkommen und damit einhergehend die notwendige Bandbreite. Außerdem reduziert sich dadurch der backendseitige Speicheraufwand signifikant, da es nur bei Bedarf zur Datenübertragung kommt. Das derzeitige Preismodell etablierter Cloud-Anbieter basiert auf der Anzahl der in die Cloud übertragenen Nachrichten. Normalerweise stehen einem Nutzer, je nach Abonnement, eine gewisse Anzahl an Nachrichten pro Tag/Stunde, zur Verfügung. Bei Überschreitung des Nachrichtenkontingents entstehen für den Nutzer weitere Kosten. Im Falle der Übertragung von Asymmetrien, bzw. Messwerten zur Errechnung von Asymmetrien, wird die Anzahl der aus dem Feld eingehenden Messdaten durch die Art des Messgeräts, bzw. dessen Übertragungsintervall, sowie die Anzahl der im Netz installierten Messgeräte definiert. Das Übertragungsintervall gängiger Messgeräte liegt derzeit im Bereich von Sekunden bzw. weniger Minuten. Die Anzahl der im Netz installierten Messgeräte hängt stark von der Netztopologie ab, wobei zur Erfassung von Asymmetrien zumindest am Transformator und idealerweise an den Abgängen Messgeräte installiert sind.

Wird die Asymmetrie in der intelligenten Ortsnetzstation berechnet fällt pro Netz eine Übertragung einer Kennzahl pro Überwachungsintervall an. Wenn die Asymmetrie im Backend errechnet wird, so muss pro Messgerät die Anzahl der Messungen pro Intervall mal drei (=die drei Phasen) übertragen werden.

Beispiel Verteilnetzbetreiber mit 500 Niederspannungsnetzen und durchschnittlich 5 Messgeräten im Feld mit moderatem Übertragungsintervall von einer Minute sowie sechs Messungen pro Minute:

- Asymmetrie und Auswahl der Top 1 % wird im Backend durchgeführt: 15.000 Nachrichten pro Minute
- Asymmetrie wird im Feld errechnet, Auswahl der Top 1 % wird im Backend durchgeführt: 500 Nachrichten pro Minute
- Asymmetrie wird im Feld errechnet, Parameter für Bestimmung der Top 1 % wird an die Feldgeräte übermittelt (der in dieser Arbeit vorgestellte Systemansatz): ~5 Nachrichten pro Minute

Die Werte in dieser Aufzählung konnten durch die ersten Ergebnisse des Feldtestes bestätigt werden. Der aktuelle Feldtest besteht aus einem Feldgerät – weiterführende Untersuchungen bezüglich der Skalierung sind für nachfolgende Projekte geplant.

Die Anzahl der Nachrichten pro Minute für den letzten Ansatz kann nicht präzise angegeben werden. Bei Bedarf müssen neue Parameter an die Feldgeräte übertragen werden (500 Nachrichten pro Aktualisierung). Je nach Einstellung der Systemparameter findet diese Anpassung unterschiedlich oft statt. Die Bestimmung der Top 1-%-Asymmetrievorfälle ist als Schiebefensterverfahren mit einem Zeithorizont von 48 h realisiert. Bei einer hinreichend großen Abweichung von 1 % wird automatisch die Aktualisierung der Parameter angestoßen. Durch die sich daraus ergebende Trägheit des Systems ist die Anzahl der Nachrichten für die Parameteraktualisierung viel kleiner als die Anzahl der gesendeten Asymmetrievorfälle. Aus diesem Grund sind sie für den oben angestellten Vergleich eine vernachlässigbare Größe.

Die Cloud-Betreiber-Kosten für die Übermittlung der Nachrichten sind selbst im Falle von 15.000 Nachrichten pro Minute mit weniger als €10,-/Monat (Preisabschätzung auf Basis der Preisangaben von AWS, Azure und Google IoT) vernachlässigbar. Es ist davon auszugehen, dass neben einer Anwendung wie Asymmetriemeldung

auch Basisdienste wie Überwachung der Betriebsmittel und weitere Anwendungen auf den Feldgeräten laufen werden. Die Summe der von den einzelnen Anwendungen benötigten Nachrichten und die übertragene Datenmenge sind dann ein Vielfaches des in diesem Beispiel anfallenden Volumens. Als ein Beispiel seien hier Power-Quality-Messungen angeführt: je nach gewählter Ausprägung fallen hier nicht 18 Messungen pro Minute sondern bis zu 12.000 Messungen pro Minute an. Hier ist eine entsprechende Vorverarbeitung der Daten im Feld auf einem EDGE-Device eine vielversprechende Alternative zum konstanten Versenden der Daten in die Zentrale.

5. Zusammenfassung und Ausblick

Im vorliegenden Artikel wurde eine IIoT-Plattform zur Anwendung in einem cyber-physischen System dargestellt. Die Plattform wurde hinsichtlich ihres industriellen Einsatzes entwickelt und basiert auf bewährten Hardware- und Softwarekomponenten. Die Plattform ermöglicht leichte Installation und Management individueller Softwaremodule mittels eines auf Plug and Automate [5] ausgerichteten Device Management.

Das beschriebene Applikations-Framework ist bislang nur als Softwareprototyp im Zuge von internen als auch kooperativen Forschungsaktivitäten umgesetzt worden; es läuft aber auf als Produkt erhältlichen Komponenten. Durch die Forschungsaktivitäten im Rahmen des Projekts iNIS – intelligent Network Information System und des verfügbaren Smart Grid Testbeds der ASCR (Aspern Smart City Research) in der Seestadt Aspern ist nun ein Langzeittest dieses Applikations-Frameworks möglich. Durch die praktischen Felderfahrungen können die verbleibenden Schritte bis hin zu einer Realisierung einer IIoT basierten Niederspannungsnetzautomatisierung unterstützt werden.

Danksagung

Das Projekt iNIS wird aus Mitteln des FFG-Forschungsprogramms IKT der Zukunft (2. Call) unter der Nummer (849902) gefördert, und der Proof of Concept wird im Testbed der ASCR in Aspern durchgeführt.

Literatur

1. Kühne, O., Weber, F. (2018): Bausteine der Energiewende – Einführung, Übersicht und Ausblick. In Bausteine der Energiewende (S. 3–19). Wiesbaden: Springer.
2. Karnouskos, S. (2011): Cyber-physical systems in the SmartGrid. In 2011 9th IEEE international conference on industrial informatics, INDIN.
3. Cejka, S., Hanzlik, A., Plank, A. (2016): A framework for communication and provisioning in an intelligent secondary substation. In 2016 21st IEEE international conference on emerging technologies and factory automation, ETFA.
4. Faschang, M., Cejka, S., Stefan, M., Frischenschlager, A., Einfalt, A., Diwold, K., Pröbstl Andrén, F., Strasser, T., Kupzog, F. (2017): Provisioning, deployment, and operation of smart grid applications on substation level. Comput. Sci. Res. Dev., 32(1), 117–130.
5. Einfalt, A., Cejka, S., Diwold, K., Frischenschlager, A., Faschang, M., Stefan, M., Kupzog, F. (2017): Interaction of smart grid applications supporting plug & automate for intelligent secondary substations. CIREN, Open Access Proc. J., 2017(1), 1257–1260.
6. Baran, P. (1964): On distributed communications networks. IEEE Trans. Commun. Syst., 12(1), 1–9.
7. VDI/VDE – Gesellschaft für Mess- und Automatisierungstechnik (Hrsg.) (2013): Cyber-Physical Systems: Chancen und Nutzen aus Sicht der Automation. Berlin: VDI/VDE.
8. Prostejovsky, A., Merdan, M., Andren, F., Strasser, T. (2012): MASGrid: a Multi-Agent-based Smart Grid control approach. Talk: Dritte Fachkonferenz Kommunikation für Energienetze der Zukunft – Smart Grids werden Realität! ComForEn 2012, Wels, 2012-09-05. OVE-Schriftenreihe (Bd. 65, S. 90–96). OVE – Österreichischer Verband für Elektrotechnik/Austrian Electrotechnical Association, Wien. ISBN: 978-3-85133-072-4.
9. Faschang, M., Xypolytou, E., Meisel, M., Wendt, A., Kaufmann, T., Litzlbauer, M., Marchgraber, J., Bibl, M., Prostejovsky, A., Gawron-Deutsch, T., Kienesberger, G. (2015): Transition roadmap—from centralized to massively decentralized grid control systems, Nov. 2014. In Dipl.-Ing., Bakk. techn. Marcus Meisel (Hrsg.), Wissenschaftlicher Bericht für die FFG. Eigenverlag des Institut für Computertechnik der TU Wien, Energy&IT Group, Wien. 75 S., ISBN: 978-3-200-04337-4.
10. Hauck, S., DeHon, A. (2010): Reconfigurable computing: the theory and practice of FPGA-based computation (Bd. 1). Amsterdam: Elsevier.

11. Schuster, T. (2014): Auswirkungen der unsymmetrischen Belastung im Niederspannungsnetz für dezentrale Energieeinspeiser. In Tagungsunterlagen Eninnov 2014, Graz.
12. Nadareishvili, I., Mitra, R., McLarty, M., Amundsen, M. (2016): Microservice architecture: aligning principles, practices, and culture. Sebastopol: O'Reilly Media, Inc.

13. Fielding, R. (2000): Architectural styles and the design of network-based software architectures. Dissertation.
14. Surwase, V. (2016): REST API modeling languages—a developer's perspective. Int. J. Sci. Technol. Eng., 2(10), 634–637.

Autoren



Tobias Gawron-Deutsch

ist Projektleiter für nationale und internationale F&E-Projekte bei Siemens AG Österreich und Experte im Bereich Smart Grid. Tobias Deutsch wurde 1975 in Wien geboren. Er absolvierte an der Technischen Universität Wien das Diplomstudium Informatik, das er mit einer Diplomarbeit im Bereich Robotik abschloss. Danach arbeitete er als Forschungsassistent am Institut für Computertechnik an der Elektrotechnischen Fakultät der Technischen Universität Wien, wo er auch seine Dissertation verfasste. Das Doktoratsstudium beendete er erfolgreich im Mai 2011. Seit Oktober 2011 forscht er bei Siemens im Bereich Smart Grids mit Schwerpunkt auf IKT sowie an Industrial IoT-Themen.



Konrad Diwold

erhielt 2007 einen Master in Künstlicher Intelligenz von der Vrije Universiteit Amsterdam (Niederlande). Von 2008 bis 2011 war er wissenschaftlicher Mitarbeiter in der Arbeitsgruppe Parallelverarbeitung und komplexe Systeme an der Universität Leipzig (Forschungsschwerpunkt: Biologisch inspirierte Algorithmen). Im Jahr 2012 erhielt er den Doktor der Informatik von der Universität Leipzig.

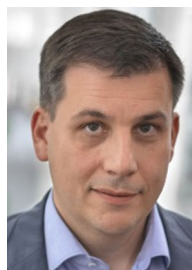
Von 2011 bis 2014 war er als wissenschaftlicher Mitarbeiter am Fraunhofer Institut für Windenergie und Energiesystemtechnik (Kassel, Deutschland) in der Abteilung Verteilnetzbetrieb tätig (Forschungsschwerpunkt: intelligente Integration erneuerbarer Energien in den Verteilnetzbetrieb). Seit 2015 arbeitet Konrad Diwold in der Siemens Corporate Technology (Wien, Österreich) und forscht in den Bereichen Smart Grid und Smart Building.



Stephan Cejka

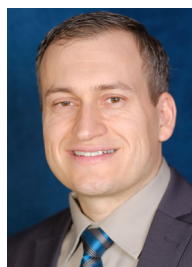
ist seit 2014 bei Siemens AG Österreich in einer Forschungsabteilung für Smart Grids und Smart Buildings als Research Scientist tätig. 2013 erhielt er den Bachelor of Science in Software & Information Engineering von der Technischen Universität Wien, 2016 wurde er Magister der Rechtswissenschaften an der Universität Wien. Er ist derzeit im Masterstudium Software Engineering & Internet Computing an der Technischen Universität Wien sowie im Doktoratsstudium Rechtswissenschaften an der Universität Wien inskribiert. Seine Forschungsschwerpunkte liegen im Bereich der verteilten Systeme,

me, Datenspeicherung und Datenschutz in Smart Grids und Smart Buildings.



Martin Matschnig

ist zertifizierter Projektleiter für nationale und internationale F&E-Projekte bei Siemens AG Österreich und Experte mit Schwerpunkt Chip Design und Hardware Security. Martin Matschnig wurde 1975 in Wien geboren. Er studierte an der Technischen Universität Wien das Diplomstudium der Elektrotechnik. Während des Studiums arbeitete er als Computer-Servicetechniker und absolvierte mehrere Berufspraktika. Nach dem ausgezeichneten Abschluss des Studienganges Computertechnik trat er 2001 in den Dienst der Siemens AG ein. Beginnend als Hardware-Entwickler, beschäftigte er sich mit Verifikation von eingebetteten Systemen und sicherheitskritischen Anwendungen, sowie Security Aspekten im Bereich der Elektronik. Aktuell arbeitet er als Projektleiter für internationale, kooperative Forschungsprojekte.



Alfred Einfalt

ist Projektleiter für nationale und internationale F&E-Projekte bei Siemens AG Österreich und Experte im Bereich Energietechnik und Smart Grid. Alfred Einfalt wurde 1980 in Zwettl, Niederösterreich, geboren. Nach dem erfolgreichen Abschluss der HTL für Elektronik und Automatisierung mit Auszeichnung begann er 2001 das Elektrotechnik-Studium an der TU Wien. Während dieser Zeit absolvierte er mehrere Praktika bzw. leistete Werkvertragstätigkeiten bei einem der führenden außeruniversitären Forschungseinrichtungen, dem AIT Austrian Institute of Technology. Nach dem ausgezeichneten Abschluss des Studienganges Energietechnik 2006 war er als wissenschaftlicher Mitarbeiter und später als Universitätsassistent am Institut für Elektrische Anlagen und Energiewirtschaft an der TU Wien tätig. Neben der Lehrtätigkeit arbeitete er aktiv und auch in koordinierender Rolle an diversen Forschungsprojekten im Umfeld von Smart Grid. Mit der Dissertation zum Thema „Versorgungssicherheit nachhaltiger, autonomer Micro Grids“ beendete er 2011 sein Doktoratsstudium und auch die Tätigkeit an der TU Wien. Seitdem arbeitet er als Projektleiter für F&E-Projekte und Energietechnik-experte mit Fokus auf energietechnische Modellierung, Simulation und DMS (State Estimation, Distribution Network Operation).