Energieforschungsprogramm

Publizierbarer Endbericht

Programmsteuerung:
Klima- und Energiefonds

Programmabwicklung:
Österreichische Forschungsförderungsgesellschaft mbH (FFG)

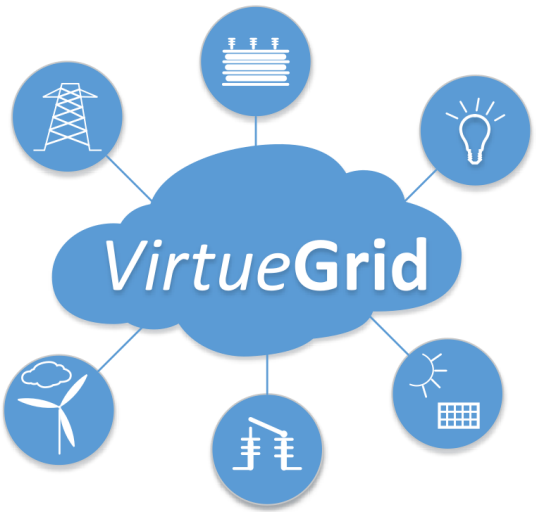
Endbericht
erstellt am
31/07/2020

VirtueGrid

Virtualisierung
für resiliente und sichere
Smart Grid-Kommunikationsnetze

Ziele, Methode,
Lessons Learned und Schlussfolgerungen

Projektnummer: 858873



Ausschreibung	3. Ausschreibung Energieforschungsprogramm
Projektstart	01/05/2017
Projektende	30/04/2020
Gesamtprojektdauer (in Monaten)	36 Monate
ProjektnehmerIn (Institution)	AIT Austrian Institute of Technology GmbH
AnsprechpartnerIn	Friederich Kupzog
Postadresse	Giefinggasse 4, 1210 Wien
Telefon	+43 50550 6059
Fax	
E-mail	friederich.kupzog@ait.ac.at
Website	www.ait.ac.at

VirtueGrid

Virtualisierung
für resiliente und sichere Smart Grid-Kommunikationsnetze

AutorInnen:
Friederich Kupzog, AIT
Armin Veichtlbauer, FH Salzburg
Alexander Heinisch, Siemens AG Österreich
Ferdinand von Tüllenburg, Salzburg Research
Oliver Langthaler, FH Salzburg
Ulrich Pache, FH Salzburg
Oliver Jung, AIT
Reinhard Frank, Siemens AG Deutschland
Peter Dorfinger, Salzburg Research
Georg Linhard, LINZ AG

Inhaltsverzeichnis

1 Einleitung

Informations- und Kommunikationstechnologien (IKT) spielen eine Schlüsselrolle bei der Integration erneuerbarer Energien in die bestehende Stromnetzinfrastruktur. Anwendungen wie Montoring von Verteilungsnetzen, die Steuerung von Feldgeräten und verteiltes Energiemanagement stehen neben herkömmlichen Anwendungen wie *supervisory control and data acquisition* (SCADA), Metering und Abrechnung immer mehr im Fokus. Mit den weltweiten Bemühungen zur Reduzierung der Treibhausgasemissionen [1] werden neue Anforderungen an bestehende Energiesysteme gestellt. Hierzu gehört beispielsweise die Notwendigkeit einer Sektorkopplung oder die Umsetzung von Energiegemeinschaften [2]. Dies führt zur Integration einer großen Anzahl von zusätzlichen Systemelementen. Die neuen Lösungen müssen den bestehenden Anforderungen an Verfügbarkeit, Sicherheit, Ausfallsicherheit und Effizienz entsprechen.
Unter diesen Umständen scheint es völlig unzureichend, lediglich die bestehenden IKT-Systeme des heutigen Verteilungsnetzbetriebs zu skalieren und sie mit einem Sicherheitskonzept zu erweitern [3]. Die etablierten und derzeit angewendeten Verfahren für Aspekte wie Ausfallmanagement, Konfiguration neu integrierter Netzwerkkomponenten oder Testen neuer IT-Netzwerksegmente sind in der Regel manuell und zeitaufwändig. Dies gilt insbesondere für ein stark IKT-abhängiges Stromnetzbetriebsszenario. Virtualisierungskonzepte aus dem IKT-Bereich wie Edge- und Cloud-Computing sowie dynamische virtuelle lokale Netzwerke und Software Defined Networking (SDN) eröffnen eine potenzielle Gelegenheit für praktische Schlüsselfragen in der IKT von Stromversorgungssystemen [4] [5] [6].
In diesem Forschungsprojekt analysieren wir, wie und wie gut Virtualisierungskonzepte aus dem IKT-Bereich relevante Anwendungsfälle für die Energieverteilung verbessern können. Der Fokus liegt dabei auf der Virtualisierung von Kommunikationsaspekten, nicht jedoch auf der Virtualisierung von Komponenten oder Systemen. Gegenstand der Untersuchung sind Kommunikationsaspekte wie der Einsatz neuer Protokoll Stacks, eine übergreifenden Optimierung zwischen Energie- und Kommunikationsnetzwerken, der Integration von Nicht-IP-Verkehr, Legacy-Komponenten, sowie Online-Integritätsprüfungen von Energie- und IKT-Systemen. Durch eine virtualisierte Lösung können Komponenten eines verteilten Steuerungssystems an einem scheinbar zentralen Ort konfiguriert und betrieben werden.
Um die potenziellen Vorteile von Virtualisierungsansätzen im Kontext der IKT von Stromversorgungssystemen systematisch zu untersuchen, untersuchen wir die folgenden vier konkreten Anwendungsfälle und implementieren Prototypen:

1.1 Anwendungsfall 1: Virtualised Redundancy

In der Automatisierung von elektrischen Anlagen sind kritische Komponenten typischerweise aus Verfügbarkeitsgründen redundant ausgeführt. Dabei wird die Redundanz mithilfe verschiedener Funktionen unter Verwendung von standardisierten Protokollen wie IEC60870-5-104 realisiert.

Diese Redundanz wird applikationsspezifisch realisiert und ist somit nicht protokollunabhängig einsetzbar. Das spezifische Protokoll kann im Projektkontext VirtueGrid als „Legacy Protokoll“ angesehen werden.
Ziel des Anwendungsfalls ist es, durch Virtualisierung eine applikationsunabhängige und somit weitgehend protokollunabhängige Redundanzlösung zu schaffen. Die Umschaltung von einer zur anderen aktiven Komponente geschieht auf SDN-Ebene. Folgende Rahmenbedingungen sind für eine virtuelle Lösung zu berücksichtigen: Während des Umschaltvorganges zwischen der betriebsführenden zur Standby-Komponente darf die Kommunikation kurzzeitig ausfallen. Nach der erfolgten Umschaltung ist jedoch durch eine sogenannte Generalabfrage der Informationszustand in der neuen betriebsführenden Komponente zu aktualisieren.

1.2 Anwendungsfall 2: Commissioning

Der Anwendungsfall Commissioning prüft verschiedene Funktionen in einem Prozessnetzwerk. Das Prozessnetzwerk dient der Übertragung von Daten von Aktoren, Sensoren, Videoanlagen oder auch Sprachanlagen, welche sich im Feld befinden, an eine Zentrale. Wesentlich ist, dass die Daten hinsichtlich verschiedener Parameter wie Bandbreite, Latenz, Verfügbarkeit oder Klassifizierung sehr unterschiedlich sind. Das Netzwerk dient primär der Automatisierung von kritischen Infrastrukturen wie zum Beispiel Stromnetz, Gasnetz, Wassernetz oder auch dem öffentlichen Verkehr.

Es wird davon ausgegangen, dass in naher Zukunft die Anzahl der Endgeräte, welche an dieses Netzwerk angeschlossen werden, sehr stark steigen wird und daher Anforderungen in Richtung hoher Verfügbarkeit, Sicherheit und Flexibilität sehr bedeutsam werden. Durch die Virtualisierung können solche Anforderungen im Zuge von Netzwerkerweiterungen, dem Anbinden neuer Endgeräte, Provisionierung neuer Kommunikationsprofile aber auch Rückbau von Netzteilen wesentlich unterstützt und damit auch erfüllt werden.

1.3 Anwendungsfall 3: Grid-based routing

Anwendungsfall 3 betrachtet ein Szenario mit mehreren Daten-Quellen (z.B. Spannungs-Messpunkte) und mehreren Daten-Senken (z.B. Transformator-Steuerungen), die über mehrere Umspannwerke verteilt sind. Elektrisch sind diese Datenquellen und Senken über die Stromnetztopologie miteinander verbunden (siehe Abbildung 1). Je nach momentaner Ausprägung der Stromnetztopologie (Stellungen der im Netz enthaltenen Schalter) sind dabei die Daten-Quellen unterschiedlichen Daten-Senken zugeordnet. In **Fehler! Verweisquelle konnte nicht gefunden werden.**1 kann der Messpunkt je nach Schalterstellung für die Spannungssteuerung in T1 oder T2 relevant sein.

Der Anwendungsfall 3 zielt damit zugleich auf Forschungsfrage 1 (Minimieren des Konfigurationsaufwands) sowie Forschungsfrage 2 (Verschiebung von Prozessen dezentraler Regelungssysteme und Graceful Degradation) ab. Es werden unterschiedliche Szenarien für die Umsetzung evaluiert. Als Referenz dient eine Pub/Sub basierte Version bei der alle Daten in die „Cloud“ übermittelt werden. Eine weitere Variante basiert auf Software-defined-Networking, um das Umleiten der Datenströme im Feld zu ermöglichen. Außerdem ist als Möglichkeitsstudie eine dritte Variante, die P4 verwendet, angedacht. Die SDN-Variante wird im dritten Projektjahr noch in Richtung „Verschiebung von Prozessen“ ergänzt werden.

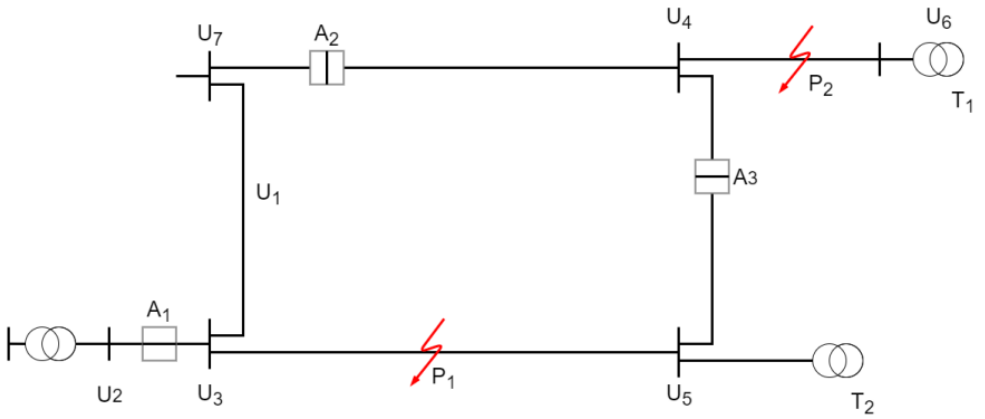


Abbildung 1. Basis-Stromnetz-Topologie Anwendungsfall 3 - Grid-Based Routing. (Ti sind Stufentrafos, Ai sind Schalter und Ui sind Messpunkte für Spannungen)

1.4 Anwendungsfall 4: Anomaly detection

Im Anwendungsfall Anomaly Detection wird ein System entwickelt, mit dessen Hilfe Anomalien des Stromnetzes durch Analyse verfügbarer Informationen aus dem Kommunikationsnetz erkannt werden können. Dabei wird die Analyse des Datenverkehrs auf Basis der Flow-Statisitik im SDN-Switch vorgenommen. Der SDN Controller sammelt die Informationen aller Switches und führt die Anomaly Detection Applikation für die anschließende Analyse durch, um Abweichungen zu gespeicherten Verkehrsprofilen des entsprechenden Flows zu erkennen. Ziel ist es, nicht nur Anomalien, die ein Hinweis auf bösartige Angriffe darstellen, sondern auch defekte und fehlerhaft konfigurierte Komponenten zu erkennen.
Für die Anomalieerkennung werden Ansätze aus zwei unterschiedlichen Bereichen untersucht: Zum einen Principal Component Analysis (PCA) auf Basis von Entropiewerten aus der SDN Flowstatistik und zum anderen die Analyse mit Hilfe eines künstlichen neuronalen Netzes. Beide Ansätze werden mit Hilfe von künstlich erzeugten Flows, mittels Flows aus einem echten Netz sowie im Testbed evaluiert.

Die Anforderungen an den Use Case Anomaly Detection sind:

- Zuverlässige Erkennung von Angriffen wie beispielswiese Flooding oder Scans
- Zuverlässige Erkennung nicht autorisierter Endgeräte
- Erkennung ausgewählter Fehlerereignisse

2 Forschungsfragen und Methode

Um die Auswirkungen von Virtualisierungstechniken auf Systeme der Stromnetz-Automatisierung systematisch zu bewerten, werden in dieser Arbeit die folgenden drei Forschungsfragen analysiert:

Forschungsfrage 1: Mit welchem Ansatz lässt sich der Konfigurationsaufwand bei der zuverlässigen und sicheren Integration zusätzlicher intelligenter Stromnetzkomponenten sowie Patch-Management mithilfe von Virtualisierung (scheinbar zentraler Konfiguration) minimieren?

Forschungsfrage 2: Auf welche Weise lässt sich bei freier Verschiebung von Prozessen dezentraler Regelungssysteme im IKT-Fehlerfall bis hin zum IKT-Ausfall die Systemzuverlässigkeit erhöhen bzw. Graceful degradation auf Anwendungsebene realisieren?

Forschungsfrage 3: Wie unterstützt Software-Defined Networking als ein Ansatz zur Netzwerk-Virtualisierung die Situationserkennung im IKT-Netz, d.h. die proaktive Erkennung von Überlast, Fehlern und Angriffen und wie kann eine schnelle Wiederherstellung der Telekommunikations-Konnektivität im Fehler- und Angriffsfall erfolgen?

Anschließend analysieren wir konventionelle und virtualisierungsbasierte Technologien, die verfügbar sind oder sich derzeit in der Entwicklung befinden. Um diese Fragen an konkreten Systemen untersuchen zu können, wurde folgende Methodik gewählt: In einem ersten Schritt wurden praktisch relevante Anwendungsfälle vom Projektteam bestehend aus Netzbetreibern, Lösungsanbietern und Forschern identifiziert. Dies hat zu der Liste der Anwendungsfälle geführt, wie in der Einleitung dargestellt. Für jeden der vier Anwendungsfälle wurde eine theoretische Lösung entwickelt und bewertet: Wie werden Planungs- und Betriebsprozesse durch die Lösung verändert und welche Auswirkungen haben diese Änderungen? In allen vier Fällen wurden anschließend vielversprechende Ansätze umgesetzt. Für die Bewertung dieser wurde ein experimenteller Prüfstand in Simulationen, im Labor und in einer realen Feldumgebung eingerichtet, in dem die anfängliche Hypothese der Machbarkeit und Auswirkung der Virtualisierungsansätze validiert werden konnte.

3 Stand der Technik

Kommunikationsnetzwerke spielen im Zusammenhang mit SCADA-Systemen eine wichtige Rolle für den Transport von Sensorwerten von den Feldgeräten zu den Leitsystemen und die Übertragung der Steuerbefehle in umgekehrter Richtung. Für gewöhnlich unterhalten Stromnetzbetreiber für ihre Steuerungs- und Überwachungssysteme dedizierte Kommunikationsnetze. Aus architektonischer Sicht folgen diese Kommunikationsnetze den wesentlichen Entwurfszielen Skalierbarkeit in Bezug auf die Anzahl der angeschlossenen Anlagen, Betriebssicherheit in Bezug auf die Robustheit gegenüber Ausfällen des Kommunikationsnetzes und Interoperabilität in Bezug auf die Diversität der angeschlossenen Geräte.

Folglich basieren die Kontroll- und Überwachungsnetze in der Regel auf Standardtechnologie: Auf dem physical Layer basieren die drahtgebundenen Netzwerke in der Regel auf Kupferleitungen und - zunehmend gebräuchlicher – Glasfasern. Die Kabelverläufe folgen in der Regel (aber nicht zwingend) den Stromleitungswegen. Auch Powerline-Kommunikation wird häufig verwendet. Etwas weniger verbreitet sind drahtlose Verbindungen mit Richtfunk. Hier befinden sich die Funkstationen in der Regel an besonders exponierten Orten. Um die Anforderung an die Betriebssicherheit zu erfüllen, bilden die Netze typischerweise eine Ring-of-Ring-Topologie (siehe Abbildung 2). Auf diese Weise ist jeder Kommunikationsendpunkt über mindestens zwei Wege erreichbar. Um Interoperabilität und Skalierbarkeit aus Sicht des Kommunikationsprotokolls zu gewährleisten, werden die Netze typischerweise mit bewährter Layer-2-Netzwerktechnologie (vulgo LAN-Netze) betrieben [7].

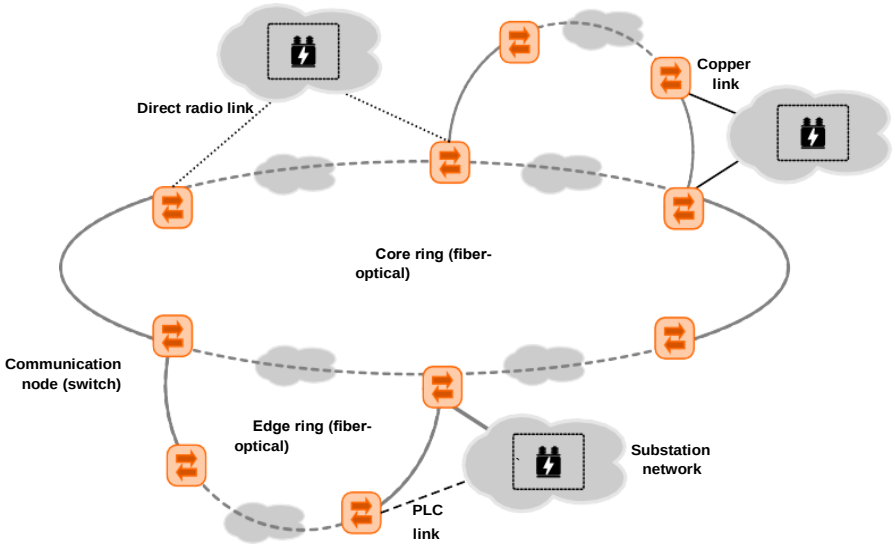


Abbildung 2. Eine schematische Darstellung einer typischen Ring-of-Ring-Topologie, bestehend aus einem Kernring und mehreren Randringen, die die Feldstationen entlegener Netzgebiete anbinden. Die Ringe basieren oft auf Glasfasertechnologie, während die Speichenverbindungen zu den Feldstationen verschiedene Layer-1-Technologien verwenden können.

3.1 Kommunikationstechnologien für Stromnetzautomatisierung

Kommunikationsnetze umspannen große geographische Bereiche, verbinden dabei eine große Anzahl von Knoten und sind Teil einer Reihe von Applikationen. Aus Sicht des Netzwerkmanagements werden Lösungen benötigt, die den Betrieb des dieser Netze hinsichtlich der ursprünglichen Entwurfsziele ermöglichen. Virtual (Extensible) Local Area Networks (VLANs / VxLANs) ermöglichen die Aufteilung einer großen Layer 2 Domäne in kleinere Segmente. Diese Segmente enthalten eine Teilmenge der verfügbaren Verbindungen und Kommunikationsknoten des Netzes. VLAN wird so üblicherweise verwendet, um die Datenströme unterschiedlicher Anwendungen zu trennen und deren gegenseitige Beeinflussung zu minimieren. Dabei wird die Ethernet Erweiterung IEEE 802.1Q verwendet, die bis zu 4096 Netzwerksegmente ermöglicht. Durch das Wachstum von Rechenzentren und Cloud-Strukturen hat sich diese Limitierung jedoch als problematisch herausgestellt. Um darüber hinaus höhere Skalierbarkeit zu ermöglichen, wurde VxLAN entwickelt [8]. Außerdem ermöglicht es VxLAN, mehrere LANs über Weitverkehrsnetze (WANs) wie das Internet unter Verwendung von Kapselung auf einfache Weise miteinander zu verbinden. VxLAN Endpunkte bilden ein Overlay Netz über das WAN (wie z.B. das Internet), wodurch die Layer 2 Pakete transparent zwischen den LANs getunnelt werden.

Während VLAN und VxLAN im Kontext der Überwachung und Steuerung von Energienetzen großflächig ausgerollt worden sind, hat die Dezentralisierung der Energieversorgung zu einer fortschreitenden Digitalisierung sowie zu einer Veränderung der Steuerungs- und Überwachungsprozesse geführt. Daraus haben sich neue Anforderungen ergeben, die mit VLAN und VxLAN nicht mehr erfüllt werden können. Dies trifft insbesondere auf gestiegene Anforderungen hinsichtlich der Verlässlichkeit der Datenströme zwischen SCADA Systemen und Feldgeräten zu.

Für diese Datenströme bestehen bestimmte Anforderungen an die Übertragungsqualität. Dies betrifft z.B. Überwachungsfunktionen wie Wide Area Monitoring Systems (WAMS), welche strikte Zeitsynchronisierung zwischen den Sensoren erfordern oder einige Schutzfunktionen, die definierte Anforderungen an Latenz und Paketverluste haben. Diese Anforderungen können von VLAN und VxLAN nicht erfüllt werden, weshalb Multiprotocol Label Switching MPLS Einzug in einige SCADA Netze gehalten hat. Das MPLS Protokoll ermöglicht Protokollunabhängigkeit, Netzwerkressourcenmanagement und Fehlerschutz. Das Grundprinzip des Protokolls ist Packet Labeling, bei dem die zu einer bestimmten Anwendung oder einem bestimmten Datenfluss gehörenden Pakete mit einem Label zur eindeutigen Identifikation markiert werden. Die weiterleitenden Knoten (MPLS Router) setzen eine vordefinierte Behandlung dieser Pakete basierend auf konfigurierbaren Regeln um. Diese Regeln können z.B. bestimmen, auf welchen Pfaden Pakete weitergeleitet werden oder welchen Anteil an der verfügbaren Bandbreite diesen Paketen zugeteilt wird.

MPLS ermöglicht damit die Definition einer bestimmten Übertragungsqualität für unterschiedliche Datenflüsse. Dazu wurde MPLS mit einer Traffic Engineering Funktion (MPLS-TE) erweitert. Darüber hinaus gibt es Erweiterungen für Pfadredundanz mit schneller Pfadumschaltung (MPLS Fast Reroute, MPLS-FRR). Dieser Mechanismus erlaubt das Umschalten zwischen redundanten Pfaden, sobald einer dieser Pfade unterbrochen wird. Verglichen mit dem traditionellen Rapid Span-

ning Tree Protokoll, können die Umschaltzeiten signifikant reduziert und dadurch Latenzanforderungen besser eingehalten werden.

3.2 Software-defined Networking

SDN basiert auf einer Netzwerkdesign-Philosophie, welche die Separierung der Data Plane von der Control Plane propagiert. Dies ermöglicht programmgesteuertes Netzwerkmanagement und effiziente Netzwerkkonfiguration (siehe Abbildung 3). Die Änderung der Netzwerkkonfiguration in traditionellen, nicht SDN Netzwerken verursacht hohen Aufwand und erfordert viel Zeit. Durch die programmierbaren Schnittstellen die SDN zur Verfügung stellt können Netzwerkkomponenten von einer zentralen Stelle, dem SDN Controller, aktualisiert werden und komplexe Netzwerkmanagement Aufgaben können einfacher durchgeführt werden. SDN Software Interfaces bieten größere Flexibilität für das Netzwerkmanagement sowie die Kontrolle über das Verhalten des Netzwerks. Dies ermöglicht feingranular abgestimmtes Traffic-Engineering [9], [10]. Änderungen am Netzwerk müssen nicht mehr Gerät für Gerät erfolgen, sondern können auf das gesamte Netzwerk auf einmal angewendet werden. SDN eröffnet auch Möglichkeiten zur Netzwerkvirtualisierung und erhöht die Sicherheit in Netzwerken, da sämtliche Netzwerkkomponenten für den Kontroller jederzeit sichtbar sind.

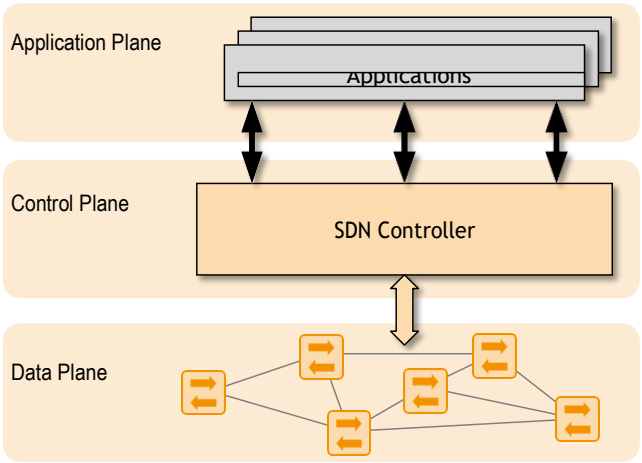


Abbildung 3. SDN Architektur

Die Verwendung von SND in Smart Grids ist ein gut untersuchtes Gebiet. SDN bietet für die Smart Grid Kommunikation viele Vorteile. Rehmani et al. [11] identifizieren einige der Hauptmotive für die Verwendung von SDN in Smart Grids.

- Trennung von unterschiedlichen Verkehrsarten
- Qualitiy of Service
- Virtual Network Slicing
- Erhöhung der Zuverlässigkeit der Kommunikation in Smart Grids

- Schnelle Fehlererkennung und -behebung
- Frühe Verschiebung von Lasten, um Spannungszusammenbrüche zu verhindern
- Einfacheres Netzwerkmanagement und erhöhte Interoperabilität
- Reduktion der Komplexität bei der Integration elektrischer Fahrzeuge

Aydeger et al. [12] schlagen ein SDN basiertes Inter-Umspannwerk-Kommunikationsnetzwerk vor, um die Zuverlässigkeit des Smart Grids zu erhöhen. Hierzu werden die SDN Controller hierarchisch angeordnet: Der globale Controller verwaltet den Verkehr zwischen den Umspannwerken und wird vom Betreiber des Smart Grids an einer zentralen Stelle in seinem Netz platziert. Lokale SDN Controller werden in den Umspannwerken betrieben, um dort den lokalen Verkehr zu verwalten. Die Zuverlässigkeit wird durch redundante Links erhöht.
Die Fähigkeit zur Selbstreparatur eines Smart Grids kann, wie in [13] gezeigt wird dadurch verbessert werden, dass Verkehr von kompromittierten PMUs umgeleitet wird. PMUs werden verwendet um die Spannung und die Phase von Übertragungsleitungen zu überwachen. Phasor data concentrators (PDCs) empfangen Daten von mehreren PMUs und senden die gesammelten Messdaten an die Steuerzentrale. Wenn ein PDC durch eine Cyber-Attacke kompromittiert wurde beeinträchtigt dies die Überwachungsmöglichkeiten des Smart Grids erheblich, bis hin zum Verlust der Überwachungsmöglichkeit. Dieses Problem wird durch die Umleitung der Daten von PMUs an unkompromittierte PDCs durch das SDN behoben.
Dorsch et al. schlugen in [14] einen fehlertoleranten Mechanismus für SDN basierte Smart Grids vor, der sowohl die Zeit für die Linkfehlererkennung und Linkfehlerbehebung minimiert, als auch die Wege auf denen der Verkehr durch das Netzwerk geleitet wird nach der Linkfehlerbehebung optimiert. Um Linkfehler zu erkennen wurden Bidirectional Forwarding Detection als auch Heartbeat-Mechanismen des SDN Controllers eingesetzt. Für die Wiederherstellung der Links wurden OpenFlow Fast Failover Groups verwendet. Der SND Controller wurde für die Optimierung der Pfade nach Wiederherstellung der Links verwendet. Hierbei wurden, um die optimale Leistung der neuen Pfade sicherzustellen, Verbindungen mit geringerer Auslastung, Verbindungen mit höherer Auslastung vorgezogen.
Fast Failover Groups wurden auch von Pfeiffenberger et al. [15] verwendet, um die Zuverlässigkeit des Multicastverkehrs zu erhöhen, welcher in Umspannwerken zum Einsatz kommt. Dies wurde durch die Verringerung der Paketverluste erreicht, die zwischen einem Linkausfall und dessen Behebung auftraten.
Der SDN Controller hat einen kompletten Überblick über das Netzwerk. Dieser Umstand kann eingesetzt werden um Verkehr effizient, entlang optimaler Pfade, durch das Netzwerk zu leiten. In [16] wird ein OpenAMI Routingschema vorgeschlagen um den Verkehr auf dem schnellsten Weg durch das Netzwerk einer Advanced Metering Infrastructure (AMI) zu leiten, wobei Loadbalancing zum Einsatz kommt. Durch den Einsatz von OpenAMI konnten niedrige Ende-zu-Ende Verzögerung als auch höherer Durchsatz erreicht werden.
Der komplette Überblick über das Netzwerk, den ein SDN Controller bietet, wird auch verwendet, um die Sicherheit von Smart Grids zu erhöhen. In [17], wird ein netzwerkbasiertes Intrusion Detection System für SDN basierte SCADA Systeme vorgestellt. Dieses System verwendet SDN um die

Kommunikation zwischen Stromnetzkomponenten zu überwachen und Netzwerkinformationen sowie periodisch Netzwerkstatistiken zu sammeln. Die gesammelten Daten werden in einem One-Class Klassifizierungsalgorithmus verwendet, um schädlichen Verkehr zu identifizieren.
Zhang et al. [18] behaupten, dass die Verwendung von SDN erhebliche Vorteile für Smart Grid Kommunikationsnetze mit sich bringt. Besonders die Vereinfachung der Netzwerkkonfiguration und des Netzwerkmanagements, domänenübergreifendes Content-Based Networking sowie Virtualisierung und Isolierung von Verkehr bieten erhebliche Vorteile.
Cahn et al. [19] schlagen vor, Probleme welche in Kommunikationsnetzen von Umspannwerken auftreten, durch die Verwendung von SDN zu lösen. Hierfür wird eine Software-Defined Energy Communication Network (SDECN) Architektur vorgestellt, welche die Fähigkeit zur Selbstkonfiguration besitzt und viele bekannte Probleme in der Verwaltung von Umspannwerken beheben kann. Es wird betont, dass die schiere Zahl unterschiedlicher Intelligent Electronic Devices (IED), welche verschiedene Bereiche des Umspannwerkes überwachen und kontrollieren und welche hauptsächlich auf Layer 2 Kommunikation setzen, die Netzwerkkonfiguration sehr komplex werden lassen. Das SDECN kann den Konfigurationsaufwand erheblich reduzieren, unterstützt Layer 2 Multicast Gruppen und vereinfacht die Inbetriebnahme neuer IEDs im Netzwerk.
SDN Eigenschaften wie bessere Netzwerküberwachung und einfache Rekonfigurierbarkeit können verwendet werden um ausgefeilte Systeme für die Isolierung von Netzwerkverkehr sowie komplexe Network Security Anwendungen zu implementieren, um die Netzwerksicherheit zu erhöhen. Ein zentraler SDN Controller vergrößert jedoch die Angriffsfläche. Der Bereich der SDN Security ist in [20] und [21] zusammengefasst.

3.3 Programming Protocol-independent Packet Processors (P4)

Obwohl SDN die Programmierbarkeit auf der Steuerebene ermöglicht, verfügen OpenFlow-Switches immer noch über eine Datenebene mit fester Funktion, die lediglich konfiguriert, aber nicht wirklich programmiert werden kann. Da OpenFlow nur bestimmte Protokolle und Headerfelder unterstützt, beschränkt sich der Controller-Betrieb auf die Verwaltung von Flusstabellen und die Verarbeitung von Paketen, die von den OpenFlow-Switches empfangen werden. Dies folgt einem Bottom-up-Ansatz, bei dem SDN-Entwickler die Steuerebene auf der Grundlage der festen Funktionalität einer SDN-fähigen Datenebene erstellen müssen.
P4 bietet jedoch programmierbare Datenebenen, mit denen das Verhalten der Datenebene auf einer abstrakten Schicht definiert werden kann. Dadurch werden sowohl die Steuer- als auch die Datenebene programmierbar.
Programmierbare Data Planes stellen grundlegende Funktionen bereit, z. B. Match-Action-Tabellen und Mechanismen zur Header-Manipulation, die konfiguriert und verkettet werden können, um eine spezifische Weiterleitungspipeline zu bilden. Die Spezifikation der Paketverarbeitung wird unabhängig von der Vermittlungshardware, d.h. sie ist über verschiedene Zielsysteme hinweg portierbar.
Diese Flexibilität bringt viele Vorteile mit sich. Die Entwicklung von Netzwerkhardware kann von der Netzwerkfunktionsprogrammierung entkoppelt werden. Anstatt sich auf Hardwareentwick-

lungsprozesse mit langen Zyklen zu konzentrieren, können neue Funktionen von Entwicklern einfach entwickelt und bereitgestellt werden. Darüber hinaus können Fehler in der Bearbeitung behoben werden, ohne auf Aktualisierungen warten zu müssen. Programmierbare Datenebenen vereinfachen daher agile Entwicklungsprozesse mit einfachem Prototyping, schnellen Entwurfszyklen und einfacher Bereitstellung.

Die P4-Technologie wird im Rechenzentrumsbereich und in Dienstanbieternetzwerken erweitert. Dennoch ist es für Smart-Grid-Netze an bestimmten Orten auch relevant, spezielle lokale Probleme zu lösen. Programmierbare Datenebenen, wie sie von P4 bereitgestellt werden, können die Verzögerungswerte mit Hardware-Kapselungsmethoden für eine Tunnelarchitektur von Standort zu Standort verbessern. Die Umwandlung komplexer und rechenintensiver Prozesse wie Internet Protocol Security-Tunneling in Hardware über eine programmierbare Weiterleitungsebene führt zu einer optimierten Standort-zu-Standort-Konnektivität.

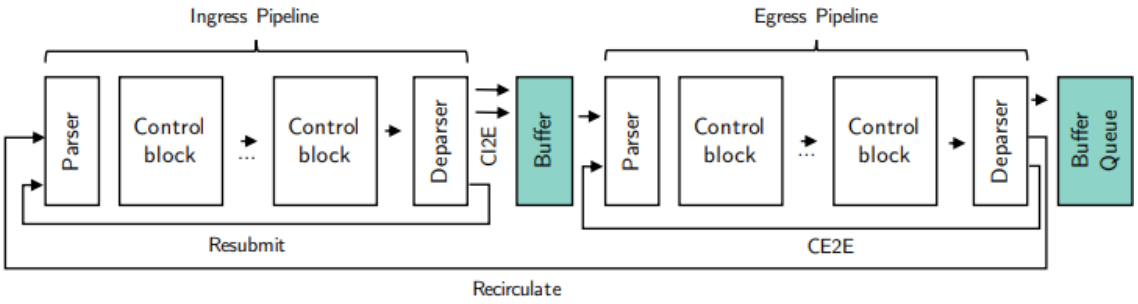


Abbildung 4. P4 Architektur

Wie in Abbildung 4 dargestellt, ermöglicht die P4-Architektur die Analyse, Änderung und Einführung aller Arten von Paket-Headern, sowohl standardisierten also auch proprietären Headern. Die Header oder Informationsfelder können überall im Datenrahmen eingefügt werden. Dies bietet die Flexibilität, zusätzliche Informationen nicht über Softwareprozesse, sondern über Hardware und damit mit Drahtgeschwindigkeit auf bestimmten Hardwarezielen in Datenpakete einzuführen.

4 Virtualisierungstechniken und deren Anwendbarkeit im Kontext der Stromnetzautomatisierung

Ziel dieses Abschnitts ist es, einen Überblick über bestehende Virtualisierungskonzepte im IKT-Bereich zu geben und deren Anwendbarkeit auf die genannten Anwendungsfälle (anwendungsprotokollunabhängige Redundanz, Kommissionierung, Grid-basiertes Routing und Anomaly Detection) zu bewerten. Im Rahmen der State-of-the-Art-Analyse wurde bereits in einem früheren Stadium der Forschungsarbeit eine Vorauswahl getroffen, mit dem Ergebnis, dass die folgenden Virtualisierungskonzepte für die Realisierung der genannten Anwendungsfälle in Betracht kommen: VLAN/VxLAN, MPLS, Cloud- und Edge-Computing, SDN und P4. Basierend auf der Anwendbarkeit dieser Technologien auf die Anwendungsfälle wurde eine gemeinsame Meta-Architektur entwickelt.

Die Virtualisierung kann an mehreren Stellen in einer umfassenden IKT-Infrastruktur erfolgen. Sie alle müssen berücksichtigt werden, um die besten Lösungen für die genannten Anwendungsfälle zu finden und eine geeignete Meta-Architektur abzuleiten. Im Folgenden wird ein kurzer Überblick über mögliche Ansätze gegeben und bewertet, wie gut diese den Anforderungen der Anwendungsfälle entsprechen.

4.1 Gerätevirtualisierung

Zunächst einmal ist der einfachste Ansatz die Virtualisierung physischer Systeme, seien es Endsysteme, die als IED am Smart Grid teilnehmen, oder Netzwerkknoten als Teil der Kommunikationsinfrastruktur. Einige der Geräte können durchaus auch als virtuelle Maschinen realisiert werden (z.B. Backend-Server, die auf einem Hypervisor laufen), während andere Geräte eine physische Interaktion mit der echten Welt erfordern (z.B. Sensoren und Aktoren im Feld), so dass diese nicht einfach ersetzt werden können.
Bei der Nutzung öffentlicher Kommunikationsinfrastrukturen wie dem Internet als „Underlay“ Infrastruktur sind auch die beteiligten aktiven Netzwerkkomponenten (Router, Switches) nur schwer zu ersetzen, da die Pakete ja durch irgendein Gerät weitergeleitet werden müssen. Dennoch ist Virtualisierung in vernetzten Umgebungen nichts Ungewöhnliches [22]. In ihrer einfachsten Form werden virtuelle Verbindungen durch Technologien wie „Link Aggregation definiert“, bei der mehrere physische Verbindungen zu einer logischen Verbindung mit größerer Kapazität aggregiert werden.
Eine weitere sehr verbreitete Technologie sind virtuelle lokale Netzwerke (VLANs), bei denen es sich um logisch getrennte IP-Netzwerke handelt, die sich über eine geswitchte Infrastruktur erstrecken. Darüber hinaus ist es möglich, VLANs auch vollständig virtuell einzurichten, d.h. nicht in realen Infrastrukturen (z.B. können VLANs in einer virtuellen Netzwerkumgebung in einem Hypervisor gehostet werden). So sind auch die beteiligten Switches als virtuelle Switches („v-Switches“) realisiert. In der Praxis ist eine Koexistenz von realen und virtuellen Infrastrukturen sehr häufig [22].
Das Konzept der virtuellen Maschinen (VMs) erlaubt die flexible Verteilung dieser VMs auf eine vorhandene Hardware. Änderungen der realen Hardware wirken sich nicht notwendigerweise auf die VMs aus, solange die Anforderungen der jeweiligen VMs durch die reale Infrastruktur erfüllt werden kann. Umgekehrt können bei Bedarf weitere VMs auf derselben Hardware betrieben werden, solange die Performance der zugrunde liegenden Infrastruktur ausreicht.
Änderungen im Steuerungsprozess von elektrischen Systemen (sei es aufgrund von regulatorischen Änderungen, aufgrund von sich ändernden Anforderungen durch den elektrischen Teil der Infrastruktur, oder aus irgendwelchen anderen triftigen Gründen) können so auf derselben physikalischen Infrastruktur abgebildet werden. Dies macht die Gerätevirtualisierung besonders nützlich für redundanzbezogene Anwendungsfälle (wie z.B. die anwendungsprotokollunabhängige Redundanz oder das Grid-basierte Routing).
In der Netzwerktechnik hat in den letzten Jahren eine Technologie zunehmendes Interesse gefunden, die eine Abstraktion der Hardwareressourcen in logische Teile erlaubt, die über Service Level

Agreements angefordert werden können. Diese Technologie ist als „Network-Slicing“ [23] bekannt, wobei die Slices Teile der physisch verfügbaren Bandbreite sind, die einem anfordernden Benutzer oder einer Anwendung zugeordnet werden. Gegenwärtig liegt der Schwerpunkt im Bereich der zellbasierten 5G-Funkkommunikation. Dies macht Network Slicing für Anwendungen im Niederspannungsnetz interessant, da hier oft keine Festnetzkommunikation zur Verfügung steht.

4.2 Funktionale Virtualisierung

Virtualisierung kann aber auch auf rein funktionaler Ebene betrachtet werden. Dabei ist es nicht wichtig, *wo* Funktionen ausgeführt werden, sondern nur *unter welchen Qualitätsbedingungen* (z.B. in welcher Zeit, wie korrekt, etc.). Dies wird oft als Cloud Computing bezeichnet [24], da der Standort kein entscheidender Faktor ist. Für Edge Computing trifft das nicht wirklich zu [24], da der Standort am „Rand“ (eben der „Edge“) des öffentlichen Netzes einen wichtigen Einfluss besitzt, etwa auf Eigenschaften wie Vertrauenswürdigkeit oder Echtzeitfähigkeit.
Diese funktionale Virtualisierung kann für jede Art von Diensten verwendet werden, die innerhalb der IKT-Lösung benötigt wird. Sie kann etwa für Anwendungen wie die Rechnungsstellung gelten, bei der die Funktionalität durch Cloud-Software („Software as a Service“) bereitgestellt wird. In diesem Fall müssen Haftungsfragen im Voraus geklärt werden; auch hier wiederum in der Regel durch die Definition rechtsverbindlicher Service Level Agreements.
Dasselbe gilt auch für Netzfunktionen („Network Function Virtualisation“). So können beispielsweise Routingfunktionen (Application Layer Routing) oder Sicherheitsfunktionen (Intrusion Detection) virtualisiert eingesetzt werden. Häufig sind diese virtualisierten Funktionen an virtualisierte Geräte gebunden, die in Cloud- oder Edge-Umgebungen existieren können („Platform as a Service“) oder die Teil einer kompletten virtuellen Infrastruktur sind („Infrastructure as a Service“).
Diese Funktion ist besonders vorteilhaft für den Anwendungsfall Anomaly Detection, da Anomalien in der Netzwerkinfrastruktur durch solche virtualisierten Funktionen leicht erkannt werden können. Diese Erkennung basiert nicht nur auf Signaturen, sondern kann auch unbekannte Ausreißer unabhängig von deren Ursprung erfassen. Solche Anomalien können absichtlich von einigen Angreifern erzeugt werden (etwa bei DoS Attacken), aber auch unabsichtlich auftreten, etwa durch unsachgemäße Ressourcennutzung oder durch Fehler im elektrischen Netzwerk.
Die Funktionalitäten in einer Abstraktionsschicht, wie sie durch die Virtualisierung bereitgestellt wird, zu kapseln, wo immer dies möglich ist, hat insbesondere für kritische Infrastrukturen wie das Smart Grid viele Vorteile. Der erste und offensichtlichste Vorteil ist die zusätzliche Flexibilität, da Ressourcen bei Bedarf den logischen Knoten zugeordnet werden können. Softwarefunktionen in definierten und abgegrenzten „Sandboxes“ zu kapseln (containerbasierte Virtualisierung) bietet zusätzlich ein besseres Sicherheitshandling, da der Zugriff auf die Container in jeder gewünschten Weise eingeschränkt werden kann.
Darüber hinaus stehen Orchestrierungswerkzeuge für die Zusammenarbeit dieser Container zur Verfügung (z.B. Kubernetes). Damit ist es möglich, große Software-Rollouts, Replikation von Diensten, Upgrades von Diensten und sogar topologieabhängige Verteilung von Komponenten zu

verwalten. Somit profitieren Anwendungsfälle wie Kommissionierung mit hohen Anforderungen an die Skalierbarkeit immens von diesen Virtualisierungstechnologien.

4.3 Overlay Netze

In der Vergangenheit basierten viele kritische Infrastrukturen auf dedizierte IKT Ressourcen. Die aufkommende Konvergenz von IT und OT[1] führt jedoch zu gemischten Systemen, wo dedizierte Teile mit öffentlichen IKT Infrastrukturen interagieren. Dazu gehören „Public Cloud“ Systeme, aber auch öffentliche IP-Verbindungen zu diesen Cloud-Diensten oder zur „Customer Premises“ Domäne, etc. Es versteht sich von selbst, dass Sicherheit, Leistung und Zuverlässigkeit Themen für solche hybriden Systeme sind.
Dies gilt insbesondere für Niederspannungsnetze, wo der IP-basierte Netzzugang oft nur über eine begrenzte Bandbreite verfügt. Die meisten Verteilnetzbetreiber verfügen über stark verteilte Netze, was eine angemessene Kommunikationsinfrastruktur zwischen verschiedenen Standorten erfordert. Schließlich benötigen Drittorganisationen, die Anwendungen wie Abrechnung oder Eigenverbrauchsoptimierung zur Verfügung stellen, einen effizienten und sicheren Zugang sowohl zu den Kunden als auch zu den Betreibern.
Daraus ergeben sich widersprüchliche Anforderungen: Die Ressourcen müssen öffentlich verfügbar sein, aber der Zugang muss auf sichere und eindeutige Weise erfolgen. Die übliche Lösung für diesen Konflikt ist die Einführung von „Overlay“ Architekturen [25]. Ein privates Overlay-Netzwerk (mit eingeschränktem und kontrolliertem Zugang) verwendet eine öffentliche Underlay-Infrastruktur, die die grundlegende Konnektivität bereitstellt. Dieses verbreitete Architekturmuster stellt eine Abstraktion der physischen Infrastruktur und kann somit per se als eine Virtualisierungstechnologie betrachtet werden.
Praktische Anwendungen davon sind virtuelle private Netzwerke (VPNs), die eine sichere Fernkonnektivität bieten können, oder VxLANs, die eine Standort-zu-Standort-Kopplung mehrerer VLANs mit unterschiedlichen IP-Bereichen ermöglichen. Der Hauptvorteil hierbei ist die strikte Trennung der Verkehrsströme. Sollen auch Quality of Service (QoS) Aspekte wie Latenz, Paketverlust oder Durchsatz berücksichtigt werden, kann dies durch MPLS realisiert werden.
Mit MPLS können verteilte Anwendungen wie die Steuerung von Niederspannungsnetzen in kritischen Infrastrukturen eingesetzt werden, da MPLS ausreichend kurze Reaktionszeiten für Steuerungsaufgaben bietet. Für die in dieser Forschungsarbeit am häufigsten betrachteten Anwendungsfälle ist jedoch neben der Trennung von Verkehrsströmen und QoS-Bereitstellung ein dritter Aspekt wichtig: die Flexibilität von Systemkonfigurationen bzw. Neukonfigurationen. Diese Flexibilität wird durch SDN bereitgestellt.
Im Zusammenhang mit Overlay-Netzwerken über bestehende (Legacy) Netzinfrastrukturen wurde eine Technologie namens Software Defined Wide Area Network (SD-WAN) [26] entwickelt. Üblicherweise bilden SDN-fähige Router die Schnittstelle zwischen dem Legacy-Netzwerk und der SDN-Welt. Der Zweck dieser Geräte besteht darin, eine Abstraktion des Legacy-Netzwerks für die

[1] Integration von Informationstechnologien mit operationalen Technologien (IT/OT)

SDN „Control Plane“ bereitzustellen. Dadurch bleiben Änderungen am Legacy-Netzwerk, wie unterschiedliche Pfade, Routen oder Technologien, für die SDN-Ebene transparent. Technisch gesehen wird die Abstraktion und Transparenz durch Paket-Enkapsulierung erreicht, wenn der Netzwerktraffic über die Underlay-Infrastruktur gesendet wird.
Darüber hinaus haben Änderungen am Overlay-Netz keine Auswirkungen auf das Underlay-Netz. Beispielsweise ist die Implementierung neuer End-to-end Netzwerkprotokolle im Overlay-Netz möglich, ohne dass diese Protokolle vom Underlay-Netz verstanden werden müssen. Dies ermöglicht auch die vereinfachte Einführung neuer Anwendungen innerhalb des Firmennetzwerks.
Ein Nachteil von SD-WAN (wie bei allen Overlay-Lösungen) ist, dass es auf das Underlay-Netz angewiesen ist und nur über sehr begrenzte Überwachungs- und Konfigurationsmöglichkeiten des darunter liegenden Underlay-Netzes verfügt („Network as a Service“). Dies kann potenziell zu Verletzungen der Service Level Agreements führen. In diesem Zusammenhang können Technologien wie Network Slicing [23] interessant sein, da sie versprechen, ein Underlay-Netzwerk mit konfigurierbaren Service Level Agreements bereitzustellen.

5 Implementierung und Analyse der Fallstudien

In diesem Kapitel werden der Entwurf, die Implementierung und die Ergebnisse der Evaluierung von vier domänenrelevanten Anwendungsfällen für die Virtualisierung in Netzleitsystemen vorgestellt. Die Auswahl der Anwendungsfälle erfolgte aus der Perspektive des Verteilnetzbetriebs und aus den Anforderungen, die sich aus der Integration erneuerbarer Energien in das bestehende Stromnetz ergeben.

5.1 Kommissionierung

Der Anwendungsfall Kommissionierung befasst sich mit der Integration von intelligenten Feldgeräten (in diesem Zusammenhang als „Controller“ bezeichnet) in das TCP/IP-basierte OT-Netzwerk eines Energieversorgungsunternehmens, das als „Prozessnetz“ bezeichnet wird. Diese Controller bestehen aus speicher-programmierbaren Steuerungen (SPSen), Aktoren und Sensoren; Smart Meter sind typische Beispiele für solche Geräte. Controller stellen somit Gateways zwischen dem Prozessnetz und dem Feldnetz dar und nehmen an beiden teil. Häufig müssen sie zwischen Feldbussystemen und Ethernet-LANs übersetzen.
In einer klassischen Umgebung wird ein Prozessnetz als eine Reihe von Ethernet-basierten LANs realisiert [27]. Die LANs werden lokal eingerichtet (z.B. einer Verteilerstation) und intern mit Switches verbunden. Router werden verwendet, um die verschiedenen LANs einer Station zu koppeln und Verbindungen zu anderen Stationen sowie zu weiteren Netzwerkinfrastrukturen herzustellen (diese Infrastrukturen umfassen das IT-Netzwerk des Versorgungsunternehmens sowie die Internetverbindung). Das Routing erfolgt jedoch üblicherweise nicht mehr auf einer dedizierten Infrastruktur (wie es in früheren Installationen der Fall war).

Da das Prozessnetz nicht mehr isoliert ist, muss in Bezug auf Sicherheits- und Datenschutzfragen besondere Vorsicht geboten sein. Tatsache ist, dass heutzutage die meisten Prozessnetze modernste Sicherheitsmechanismen wie Firewalling, Filterung, Intrusion Detection, Authentifizierung, Autorisierung (z.B. rollenbasierte Zugriffskontrolle), Verschlüsselung, etc. verwenden. Mit der massiv steigenden Anzahl von Controllern ist dies eine zunehmende Herausforderung. Traditionelle Methoden wie die portbasierte Zugriffskontrolle nach IEEE 802.1X scheinen für solch umfassende Netzwerkinfrastrukturen zu leichtgewichtig zu sein.

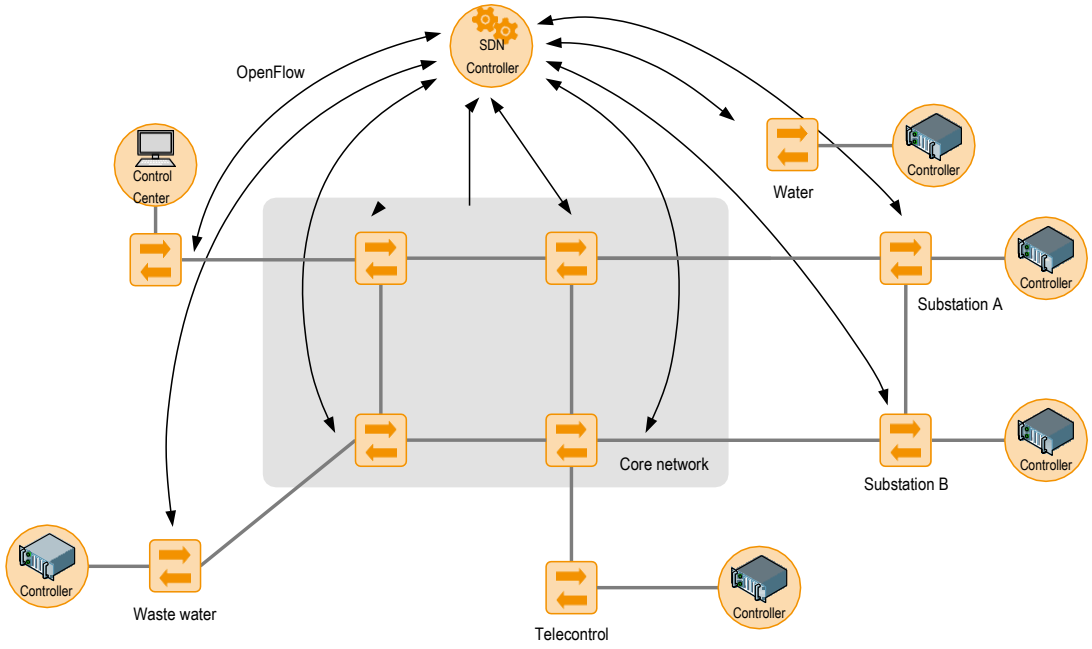


Abbildung 5. Setup eines SDN-basierten Prozessnetzes

Es wurden mehrere Szenarien definiert, die eine aktuelle Herausforderung für Prozessnetze darstellen:

- Integration einer neuen Controller-Instanz
- Trennung eines Controllers (Entfernung oder Austausch)
- Installation einer neuen Switch
- Abweichendes oder fehlerhaftes Verhalten eines Controllers

Die Herausforderung umfasst die Identifizierung der Controller, die sich um eine Integration in das Prozessnetz bewerben, die Zuweisung geeigneter Rollen, die Definition der mit diesen Rollen verbundenen Zugriffsrechte, das „Policy Enforcement“ (also die Durchsetzung von Richtlinien zur Gewährleistung des legalen Zugriffs bei gleichzeitiger Sperrung aller unberechtigten Anfragen), die Bearbeitung von Datenaustauschanfragen, die Aufrechterhaltung der Dienstverfügbarkeit und die Wartung der Prozessnetz-Infrastruktur.
Um einen flexiblen und sicheren Ansatz zu gewährleisten, wurde eine SD-WAN-Implementierung eines Prozessnetzes unter Testbedingungen vorgenommen (vgl. Abbildung 5). Dabei wurde eine

kommerzielle Lösung[2] als Basistechnologie verwendet. Der gewählte SD-WAN-Ansatz bietet mehrere Vorteile im Zusammenhang mit dem vorliegenden Anwendungsfall Kommissionierung:

- SD-WAN bietet eine Flexibilität, die mit den üblichen SDN-Ansätzen vergleichbar ist für große Overlay-Netzwerke
- SD-WAN kann für die Konfiguration neuer Geräte verwendet werden (sichere automatische Zero-Touch-Bereitstellung)
- SD-WAN kann zur Gewährleistung von QoS verwendet werden
- SD-WAN kann für die strikte Verkehrstrennung von kritischem und unkritischem Verkehr in derselben Netzwerkinfrastruktur verwendet werden (wie SDN für lokale Installationen)
- SD-WAN kann zum Aufbau eines Quarantänebereichs für neu eingesetzte Geräte verwendet werden
- SD-WAN kann für die Servicebereitstellung und Serviceverschiebung innerhalb der Netzwerkinfrastruktur verwendet werden

Somit stellt SD-WAN alle genannten Anforderungen für den Anwendungsfall Kommissionierung bereit. Da dieser Ansatz bisher jedoch noch nicht in einer realen Prozessnetzumgebung verwendet wurde, können insbesondere Skalierbarkeitsprobleme nur auf der Basis der kleinskalierten Testumgebung abgeschätzt werden.
Tabelle 1 zeigt die gemessenen Konfigurationszeiten für die einzelnen Konfigurationsmethoden. Die Zeiten für die letzte Methode (SDN mit Nutzung APIs) wurden geschätzt.

Tabelle 1. Konfigurationsaufwand Commissioning auf dem Praxistest

Methode	Konfiguration Layer 3 Konnektivität	Konfiguration Layer 2 Konnektivität
Klassische Konfiguration	30 Minuten pro NAD L3	5 Minuten pro SGD
Klassische Konfiguration mit Port-basierter Zugriffsmethode	30 Minuten pro NAD L3	2 Wochen Konfiguration der Managementsysteme 15 Minuten pro NAD L2
SDN ohne Nutzung APIs	60 Minuten für alle SGD	4 Wochen Konfiguration der Managementsyteme 15 Minuten pro NAD L2
SDN mit Nutzung APIs	60 Minuten für alle SGD	8 Wochen Konfiguration der Managementsysteme und Programmierung auf Basis der API

Verknüpft man diese Zeiten mit der Anzahl der zu konfigurierenden Smart Grid Devices, so lässt sich feststellen, dass alle Methoden linear verlaufen, mit Ausnahme „SDN mit Nutzung APIs“.

[2] https://www.nuagenetworks.net/

Hierbei ist der erhöhte Integrationsaufwand ein Einmalaufwand, da die Konfiguration der einzelnen Access-Ports nicht mehr notwendig ist. Dabei wurde angenommen, dass pro Netzwerkdevice 7 Smart Grid Devices verbinden.

5.2 Protokollunabhängige Redundanz

Dieser Abschnitt enthält die Hauptmotivation, die erstellte Lösung sowie die wichtigsten Ergebnisse aus der Anwendung der Konzepte beschrieben von von Tüllenburg et al. [28].
Dieser Anwendungsfall beschäftigt sich mit Fehlerumschaltvorgängen für Fernwirk- und Überwachungssysteme in elektrischen Verteilnetzen. Die mit solchen Systemen assoziierten Komponenten sind üblicherweise redundant ausgeführt. Beim Ausfall einer Komponente sind definierte Umschaltvorgänge für einen zuverlässigen Wechsel zur redundanten Komponente innerhalb festgelegter Zeitgrenzen verantwortlich. Die Neuerung des vorgeschlagenen Ansatzes besteht im Einsatz von Software Defined Networking (SDN) für die Fehlererkennung und Durchführung der Umschaltung.

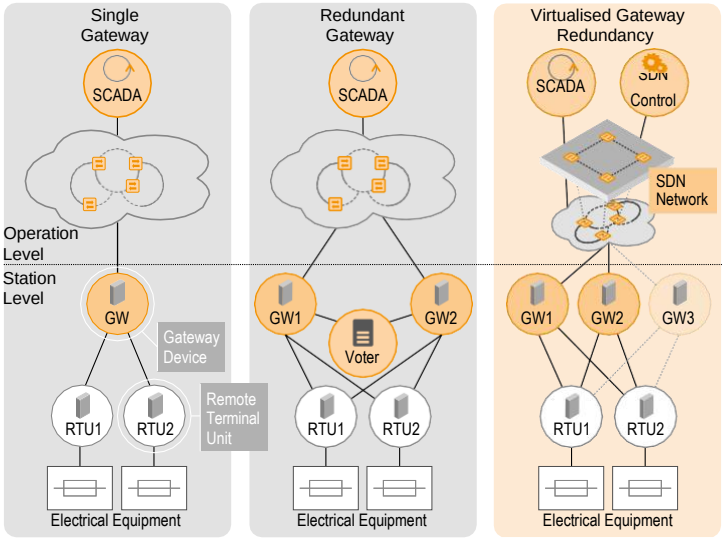


Abbildung 6. Der Ansatz für protokollunabhängige Redundanz verbessert die Flexibilität der Implementierung von Gateway-Redundanz und gewährleistet die Trennung der Belange

Üblicherweise werden Fernwirk- und Überwachungssysteme im Bezug auf das Smart Grid Architecture Model (SGAM) in zwei Zonen umgesetzt: “Station” und “Operation”. Die Zone “Operation” gruppiert die für die Überwachung der Feldgeräte erforderliche Infrastruktur unter Verwendung zentraler Steuerungskomponenten. Diese Zone beinhaltet insbesondere Kommunikationsnetze und SCADA Systeme. Die Zone “Station” hingegen umfasst die zur Steuerung und Überwachung notwendigen Geräte in den Feldstationen. Abgesehen von einem Kommunikationsnetz, werden in der Zone “Station” Intelligent Electronic Devices (IEDs) und Remote Terminal Units (RTUs) eingesetzt, die bestimmte Funktionen zur Steuerung und Überwachung implementieren. Eine bestimmte Komponente in der Zone “Station”, die Gateway Komponente, ist für die Verbindung der Zonen

“Station” und “Operation” verantwortlich und damit kritisch für die Fernwirk- und Überwachungsfunktionen. Dieses Gerät ist im Fokus dieses Anwendungsfalls.

Abbildung 6 zeigt drei Varianten zur Verbindung von SCADA und Feldstationen. Im linken Szenario kommt nur ein einziges Gateway für die Verbindung von Feldgeräten mit dem SCADA System zum Einsatz. In diesem Fall führt der Ausfall des Gatways zum Verlust jeglicher Fernwirk- und Überwachungsfunktionalität der dahinterliegenden RTUs und IEDs, ein klassischer Single Point of Failure.

Typischerweise wird in solchen Fällen (wie im mittleren Szenario dargestellt) heutzutage auf Redundanz und Voter-basiertes Ausfallmanagement zurückgegriffen. Hierbei bestimmt eine Voter Komponente das aktive der verfügbaren Gateways basierend auf seiner Konfiguration hinsichtlich definierter Leistungsindikatoren. Sobald diese Indikatoren für das alternative Gateway jene des aktiven Gateways übertreffen, wechselt der Voter zum alternativen Gerät. Ein Beispiel für einen solchen Indikator ist die Kommunikationsqualität zwischen Gateway und SCADA System. Dieser Ansatz führt jedoch zu einer Überschneidung von Belangen, da der Voter (welcher im Grunde einen Teil des SCADA Systems darstellt) den internen Zustand der Gateways kennen muss, welche jedoch im Wesentlichen Kommunikationsgeräte (wie ein Switch oder ein Router) sind. Dadurch werden künstliche Abhängigkeiten zwischen dem SCADA System, dem Kommunikationsnetz, den Kommunikationsprotokollen und dem Ausfallmanagement geschaffen.

Beim rechts dargestellten Ansatz für protokollunabhängige Redundanz hingegen findet durch den Einsatz von SDN eine Trennung dieser Belange statt. In diesem Fall wird SDN zur Überwachung des Kommunikationsverhaltens zwischen den Gateways und dem SCADA System eingesetzt. Dadurch können Ausfälle (nicht funktionsfähige oder nicht antwortende Gateways) erkannt werden und ein unmittelbarer Wechsel zu einem anderen Gateway durchgeführt werden. Das SCADA System muss in diesem Fall nicht benachrichtigt werden. Nach dem Wechsel zu einem anderen Gateway muss jedoch die Verbindung auf Anwendungsschicht neu initialisiert werden, da der Zustand der Verbindung auf dieser Ebene mit SDN nicht überwacht werden kann. Die Evaluierung dieses Ansatzes hat gezeigt, dass der Prozess der Erkennung (von Hard- und Softwarefehlern) und der Umschaltung unter Verwendung von SDN binnen maximal 5 Sekunden abgeschlossen werden kann. Für die meisten Anwendungen in der Fernwirk- und Überwachungstechnik wird dies als ausreichend angesehen. Darüber hinaus werden auf Anwendungsebene beliebige Protokolle unterstützt, was die Flexibilität der Lösung im Hinblick auf zukünftige Szenarien verbessert.

Für die Implementierung des Ausfallmanagements wurden zwei unterschiedliche Technologien betrachtet: OpenFlow4 und die Netzwerk-Programmiersprache P4. Zunächst wurde hierbei ein Vergleich der beiden Technologien aus theoretischer Sicht angestellt. Während beide Technologien eine schnelle Erkennung von Unterbrechungen der physischen Netzwerkverbindungen ermöglichen, ist die Erkennung nicht reagierender Gateways komplexer. Bei OpenFlow können hierfür Anschlussmetriken (Byte- und Paketzählung) herangezogen werden, um die Aktivität der Verbindung zwischen Gateway und SCADA System zu analysieren. Im konkreten Fall werden die zwischen Gateway und SCADA System ausgetauschten Nachrichten des 104 Protokolls analysiert, um ein nicht antwortendes Gateway zu erkennen. Sobald SCADA Anfragen nicht zeitgereicht vom Gateway beantwortet werden, wird eine Umschaltung durchgeführt. Mit P4 könnte darüber

hinaus prinzipiell der Inhalt der übertragenen Pakete analysiert und manipuliert werden. Dies würde eine Extraktion semantischer Informationen aus dem 104 Paketheader ermöglichen, wodurch Anfrage und Antwort semantisch in Zusammenhang gebracht werden können. Dies würde die Zuverlässigkeit der Erkennung von nicht antwortenden Gateways verbessern. Da der 104 Verkehr in der Praxis jedoch üblicherweise mit Transport Layer Security (TLS) verschlüsselt übertragen wird, kann dieser Vorteil von P4 allerdings nicht genützt werden. Aus diesem Grund wurde eine schneller umsetzbare Implementierung auf Basis von OpenFlow gewählt.

5.3 Grid Based Routing

Cyber-physikalische Systeme wie ein Smart-Grid bestehen typischerweise aus 2 Netzwerken. Auf der einen Seite das Kommunikations- und auf der anderen Seite im Fall des Smart-Grid, das Energienetz. Obwohl die beiden Netze oft gemeinsam verbaut werden, kann die Topologie dieser Netze meist nicht als ident angesehen werden.
Abbildung 7 zeigt zwei Netzsegmente in denen Informationen zwischen den Komponenten ausgetauscht werden müssen. Die Zugehörigkeit der Komponenten zu einem Netzsegment bzw. die Relevanz von Informationen einer Komponente für eine andere kann anhand des aktuellen Netzzustandes dynamisch berechnet werden. Es ist, zum Beispiel, abhängig vom Zustand des Schalters S_3 (offen oder geschlossen) ob Messwerte, die vom Spannungssensor U_3 durchgeführt werden, relevant für die Trafostellungen von T_1 sind. Ist S_3 geschlossen so sind diese, durch die physikalische Verbindung der beiden Komponenten, relevant. Bleibt S_3 wie in der Abbildung dargestellt jedoch geöffnet, so besteht keine physikalische Abhängigkeit zwischen den Komponenten und die Messungen von U_3 sind rein für T_2 von Relevanz.
Im Fall einer Änderung im Energienetz kann es daher schnell dazu kommen, dass auch eine Änderung der Kommunikationspfade zwischen den Komponenten im System notwendig wird. Diese Änderung kann durch eine geplante Umschaltung im Netz, eine Erweiterung des Verteilnetzes, das Hinzukommen bzw. wieder Wegschalten von zusätzlichen Erzeugern und/oder Verbrauchern, als auch teilweise Netzausfälle hervorgerufen werden.

Das Problem dabei besteht darin, dass die oben beschriebene reaktive Rekonfiguration der Kommunikationskomponenten, um Informationen entsprechend zu filtern bzw. von vorne herein nur an die richtigen Endpunkte weiterzuleiten, wenn diese nur teilautomatisiert oder gar manuell passiert, sehr aufwändig und dadurch auch fehleranfällig ist. Eine Alternative hierfür wäre die Filterung der Daten in den Komponenten selbst. Abgesehen von sicherheitskritischen Bedenken, würde dies jedoch auch bedeuten, dass jede Komponente grundlegendes Wissen über den Zustand des Energienetzes haben muss, um entsprechende Filter anzupassen, was wiederum die Komplexität und den Wartungsaufwand der Endpunkte erhöht.

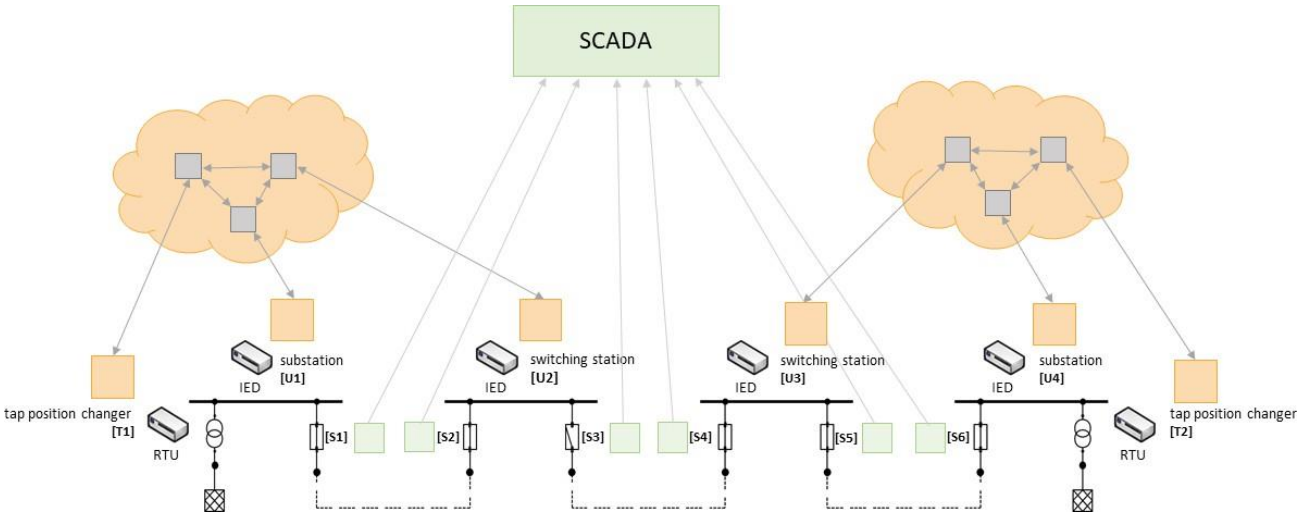


Abbildung 7. Beispielhafte Darstellung eines Mittelspannungsnetz (T_i sind Stufentrafos, S_i sind Schalter und U_i sind Messpunkte für Spannungen)

Verwendet man Virtualisierungskonzepte so kann diese erhöhte Komplexität von der Anwendung in gemeinsam verwendete Subsysteme verschoben werden. Dabei sendet und empfängt die Anwendung ihre Daten an bzw. von einem einzelnen, dezidierten, virtuellem Endpunkt, wodurch die korrekte Verteilung sowie Filterung der Informationen für die Anwendung an sich komplett transparent bleibt, und somit anstelle eines komplexen Kommunikationsproblems, eine Punkt zu Punkt Verbindung entsteht. Änderungen im Stromnetz und daraus resultierende Änderungen im Kommunikationsnetz können in den virtualisierten Subsystemen entsprechend, ohne Wissen der Applikationen auf den Endgeräten umgesetzt werden.
Im Projekt wurden sowohl eine SDN als auch eine broker-basierte Lösung als Proof-of-Concept umgesetzt. Wie in Abbildung 8 gezeigt haben wir dafür das Problem in drei Subsysteme unterteilt. Das Applikationssubsystem stellt die Anwendungsebene im klassischen Sinn dar. Darin werden applikationsspezifische Use Cases wie zum Beispiel das Berechnen der Trafostellungen, oder das Monitoring von Spannungen auf Abgängen realisiert. Das Message-Delivery-Subsystem bildet die notwendige Abstraktion für das Verteilen und Filtern von Daten, um dies für die Applikationen transparent zu gestalten. Das Umsetzen von Zuständen im Stromnetz auf die entsprechenden Regeln in der Kommunikationsinfrastruktur wird vom Decision-Subsystem durchgeführt, welches diese Regeln dann anschließend an das Message-Delivery-Subsystem weitergibt.

In der SDN basierten Implementierung, haben wir SDN Switches als Ingress-Gateways zum Kommunikationsnetz installiert. Jede Komponente ist mit genau einem dieser Ingress-Gateways verbunden, und die komplette Kommunikation dieser Komponente läuft über dieses. Pakete, die vom Gateway empfangen werden, werden von diesem wenn notwendig dupliziert sowie die Sender- und Empfangsadressen modifiziert, sodass die Pakete entsprechend der aktuellen, im Decision-Subsystem berechneten, Routingkonfiguration im Kommunikationsnetz weiter geroutet wer-

den. Obwohl dieser Ansatz im allgemeinen transparent für die Applikationen ist, und bis auf die Ingress-Gateways keine neue Hardware installiert werden muss, gibt es bei der Verteilung von Nachrichten in m-zu-n (n > 1) Verbindungen einige Einschränkungen auf Transportebene. Sollen mehrere Komponenten die Daten empfangen, so ist eine Duplizierung dieser notwendig. Dadurch ist der Einsatz von verbindungsorientierten Protokollen (wie TCP oder darauf aufbauend TLS/SSL) nicht, ohne expliziter Behandlung dieses Falles auf der Applikationsebene, möglich.

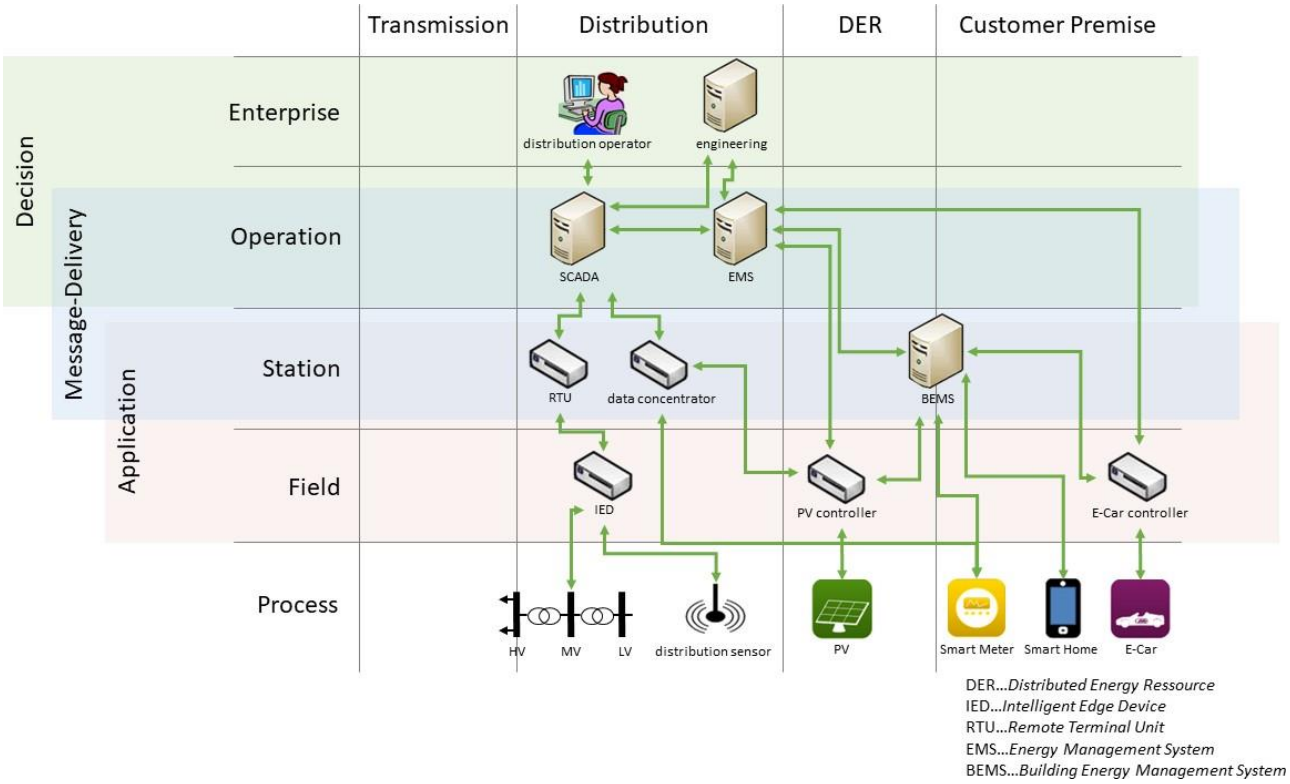


Abbildung 8. Subsysteme auf das Smart Grid Architecture Model (SGAM)

Bei der broker-basierten Lösung wurde das, auf dem MQTT Protokoll aufbauende Framework, coaty-io verwendet. Dabei senden, wie auch bereits bei der SDN basierten Lösung, die Anwendungen IEC 60870-5-104 Nachrichten an ein Ingress-Gateway, welches diese, in für das Framework verarbeitbare JSON Nachrichten, übersetzt und entsprechend der aktuellen Konfiguration aus dem Decision-Subsystem an Egress-Gateways weiterleitet. Diese führen eine Rückübersetzung der JSON Nachrichten auf IEC 60870-5-104 Nachrichten durch und leiten diese schlussendlich an die Empfangskomponenten weiter.

Im Vergleich zur SDN basierten Implementierung unterstützt dieser Ansatz das Senden von Nachrichten von einem Sender zu mehreren Empfängern, bzw. im allgemeineren m-zu-n (n > 1) Verbindungen, auch für verbindungsorientierte Protokolle. Weiters wird keine spezielle neuer Hardware für diesen Ansatz benötigt, da die Verteilkomponenten wie z.B. der Broker entweder in der

Cloud oder auf einem Server im Unternehmensnetz laufen. Ein weiterer Vorteil, ist das zentrale Management der Komponenten im Message-Delivery-Subsystem.

5.4 Anomalie-Erkennung

Einer der Hauptvorteile, die SDN mit sich bringt, ist die Sichtbarkeit aller mit dem SDN-Controller verbundenen Switches. SDN-Controller, wie z.B. der beliebte ONOS-Controller, fragen regelmäßig die Flow-Tabellen aller verbundenen Switches ab. Im Falle von ONOS werden diese Flow-Informationen standardmäßig alle 5 Sekunden abgefragt und mit hoher Genauigkeit bereitgestellt. Damit sind umfassende Informationen über alle in den Switches vorhandenen Flows verfügbar, die eine ideale Quelle für sicherheitsbezogene Analysen darstellen. Flow-Informationen werden häufig zur Erkennung von Sicherheitsvorfällen wie beispielsweise Denial-of-Service (DoS)-Angriffe oder das Scannen von IP-Adressen oder Ports. Der Hauptnachteil der Flow-basierten Analyse im Vergleich zur4 paketbasierten Analyse ist jedoch die potentiell erhöhte Anzahl falsch positiver und negativer Ergebnisse aufgrund der geringeren Auflösung der Flow-Daten.
Anomalien, die z.B. durch Cyber-Angriffe oder Netzwerkfehler verursacht werden, haben gemeinsam, dass sie die Verteilung von IP-Paket-Headerfeldern wie Quell- und Zieladresse oder TCP-Ports verändern. Im Zusammenhang mit der Erkennung von Anomalien stellen diese Felder wichtige Informationen dar, die das Verkehrsverhalten charakterisieren. Im Falle eines DoS-Angriffs, z.B. durch Flooding, ist zu erwarten, dass die Anzahl der an das Opfer gerichteten Pakete ansteigt und sich damit die Verteilung der Headerfelder verändern wird. Auch ein Port-Scan, bei dem ein einzelner Host verschiedene Ziel-IP-Adressen und Ports von einer einzigen IP-Adresse aus scannt, wird sich entsprechend bemerkbar machen.
Für die Anomalieerkennung auf Basis von Flow-Informationen gibt es zahlreiche Ansätze. Im Rahmen von VirtueGrid wurden Algorithmen untersucht, die auf künstlichen neuronalen Netzen basieren [29]. Das System besteht aus einem Classifier, einem Autoencoder sowie einer Vor- und Nachverarbeitungsstufe [30]. Während der Vorverarbeitung werden die Flow-Einträge einer vordefinierten Zeitspanne verwendet, um den Netzzustand zu bestimmen. Die Flows werden in Batches unterteilt, die aus einer festen Anzahl von Flow-Einträgen bestehen und anschließend zum Aufbau des so genannten Partiellen Netzzustands (PNS) verwendet werden. Jeder PNS besteht aus 45 Merkmalen, die so ausgewählt wurden, dass sie ein typisches Netzverhalten repräsentieren. Beispiele dafür sind die Entropie der beobachteten IP-Adressen oder TCP-Ports.
Wie in Abbildung 9 dargestellt, wird der PNS zur weiteren Verarbeitung zwei neuronalen Netzen zugeführt, einem Classifier und dem Autoencoder. Der Classifier führt eine Mehrklassen-Anomalie-Erkennung durch, indem er sowohl die Art des Angriffs als auch die angriffsfreie Flows klassifiziert. Die Rolle des Autoencoders besteht in erster Linie darin, die Anzahl der Fehlalarme zu reduzieren. Anders als der Classifier, kann der Autoencoder nur zwischen normalen und anormalen Verkehr unterscheiden.
Für die endgültige Klassifizierung werden in der Nachbearbeitungsphase die Ergebnisse des Classifiers und des Autoencoders kombiniert. In Abhängigkeit das vom Autoencoder geschätzten

Rekonstruktionsfehler wird die Ausgabe des Classifiers angepasst, um die Anzahl der Fehlalarme reduzieren.

Da Flow-Informationen eines Live-SDN-Netzes nicht zur Verfügung standen, wurden Verkehrsdaten von zwei nicht-SDN-Netzen zur Bewertung des Systems herangezogen: a) der synthetische CICIDS 2017-Datensatz [31] zur Evaluierung von Intrusion Detection Systemen und b) Daten aus einem SCADA-Netzwerk mit IEC 60870-5-104-Verkehr. Da der SCADA-Verkehrsdatensatz keine Angriffe enthielt, wurden sie unter Verwendung des Angriffsverkehrs aus dem CICIDS 2017-Datensatz hinzugefügt. Beide Datensätze wurden in einem ersten Schritt auf die Flow-Information, einschließlich der sieben Merkmale (Quell-IP und TCP-Port, Ziel-IP und TCP-Port, Anzahl der Pakete, Anzahl der Bytes und Lebensdauer eines Flow), reduziert, die im SDN verfügbar sind.

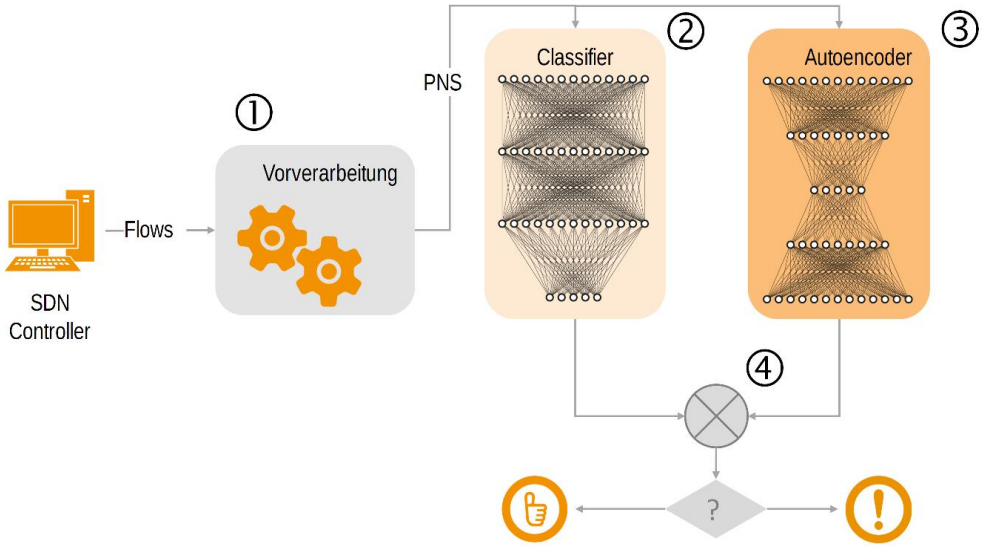


Abbildung 9: Schematische Darstellung (1) Vorverarbeitung, (2) Classifier, (3) Autoencoder, (4) Zusammenführung und finale Bewertung

Für beide Datensätze zeigt unser System eine gute Performance. Für den CICIDS 2017-Datensatz gewannen wir eine Rate von Fahlalarmen von 0,57 % bei einer Erkennungsrate von 95,19 %. Bei Verwendung des SCADA-Datensatzes erreichte die Erkennungsrate 100 % ohne jegliche Fehlalarme.

Wir konnten zeigen, dass mit den über das OpenFlow-Protokoll im SDN bereitgestellten Flow-Statistik effizient genutzt werden können, um Veränderungen in der Verteilung von Verkehrseigenschaften zu erkennen und so Anomalien zu identifizieren. Um jedoch spezifische Headerfelder in der Flow-Statistik zu berücksichtige, ist es erforderlich, ein Flow-Matching für diese Headerfelder durchzuführen. Die Extraktion von Headerfeldern ist mit OpenFlow auf Informationen der Schicht 2 bis Schicht 4 beschränkt.

Um Zugang zu den Informationen der Anwendungsschicht zu erhalten, wurde Deep Packet Inspection mit P4 evaluiert. Wie bereits erwähnt, kann die P4-Programmierung für softwaredefinierte Netzwerke einige Vorteile bringen. Die erweiterten Fähigkeiten von P4 wurden bisher jedoch kaum genutzt, um auf die Anwendungsdaten von SCADA-Paketen zuzugreifen.

Daher haben wir evaluiert, inwieweit P4 sinnvoll verwendet werden kann, um auf beliebige Anwendungsdaten in IEC 60870-5-104-Paketen zur Intrusion Detection zuzugreifen. Mit diesem Ziel vor Augen wurden neben einem P4-Parser, der es ermöglicht, die Felder aus der Nutzlast von IEC 60870-5-104-Paketen zu extrahieren, Mechanismen zur Intrusion Detection implementiert. Ziel war es, die Funktionalität des Parsers zu beurteilen, und zu demonstrieren, welche Vor- und Nachteile P4 gegenüber Alternativen wie beispielsweise dem Intrusion Detection System Snort hat. Die Evaluierung der implementierten Lösungen zeigte, dass P4 in Bezug auf Parsen und Intrusion Detection die gewünschte Funktionalität bereitstellen kann. Es wurde jedoch eine starke Reduzierung des Datendurchsatzes beobachtet.
Diese Reduzierung liegt ist erster Linie daran, dass für die Implementierung nur das Softwaremodelles eines P4-Switches Verwendung fand. Das sogenannte Behavioural Model 2 wurde eingesetzt, da keine P4-Hardware-Plattform zur Verfügung stand. Mit geeigneter P4-fähiger Hardware sind deutlich Leistungssteigerungen zu erwarten.

6 Ergebnisse und Analyse

Mit der Implementierung der vier beschriebenen Anwendungsfälle konnten Erkenntnisse zur Anwendung von Virtualisierungstechniken im Kontext von Stromversorgungssystemen gewonnen werden. Rückblickend kann man sagen, dass die Technologiereife bei Antragstellung durchaus richtig eingeschätzt worden war. Bei einigen der untersuchten Virtualisierungsanwendungen sind noch mehrere Jahre Entwicklungsarbeit absehbar bis zur kommerziellen Anwendung (siehe z.B. Probleme bei P4). Die technische Umsetzung hat auf Prototypenebene – bis auf einige Verzögerungen – jedoch sehr gut funktioniert.
Eine flexible und kostensparende Nutzung von Hardware, die in der IT-Domäne ein Treiber von Virtualsierung ist, ist in der hier betrachteten Anwendungsdomäne noch nicht so stark fortgeschritten. In Bezug auf die Technologiereife kann man durchaus Vergleiche anstellen mit der Eisenbahnsicherungstechnik, wo ebenfalls hohe Zuverlässigkeit und robuste Technik benötigt wird.
Grundsätzlich kann aufgrund der Forschungsarbeiten und Implementierungen im Projekt festgestellt werden, dass mit SDN eine valide, IP-basierende virtualisierte Kommunikation für Smart Grid-Anwendungen in gesicherter Form verfügbar ist. Anwendungen können hierauf aufgebaut werden, wie es im Projekt geschehen ist. Die Technologiereife von P4 hingegen erschien noch nicht ausreichend für den Praxiseinsatz, hier ist mehr Entwicklungsarbeit notwendig.

Es konnte gezeigt werden, dass neben SDN auch Cloud-basierte Ansätze zur Lösung von komplexen Routingproblemen herangezogen werden können. Darüber hinaus konnten in einigen Szenarien gegenüber dem reinen SDN (Open Flow) Ansatz Lösungen erzielt werden, die mit SDN alleine gar nicht umsetzbar wären. Es ist jedoch herausfordernd, im Energieverteilungssektor eine breite Masse an Anwendungsfällen auf genereller Ebene zu beschreiben, die klar einen greifbaren

Vorteil aus der Virtualisierung ziehen. Verbesserungen liegen oft im Detail und hängen mit sehr spezifischen Problemstellungen zusammen.

Für spartenintegrierte Betreiber ergibt sich generell ein höheres technologisches Potential als für Flächennetzbetreiber. Die SDN-Technologie generell sowie SD-WANs im speziellen wird für die Netzbetreiber immer wichtiger, dies hat sich auch während des Projektverlaufs in anderen Bereichen außerhalb des Projektes gezeigt. Das bedeutet, dass sich die Relevanz über die Projektlaufzeit stark gesteigert hat, v.a. im Data Center Bereich WLAN für die Authentifizierung. Es konnte auch ein spürbarer Rückfluss aus dem Projekt in die operativen Bereiche der an der Arbeit beteiligten Betreiber festgestellt werden.

6.1 Antworten auf die Forschungsfragen

Diese Arbeit konzentrierte sich insbesondere auf die im Abschnitt Methodik definierten Forschungsfragen. Erwartete Vorteile von Virtualisierungsansätzen, bei denen erstens der Konfigurationsaufwand durch Einkapselung der Komplexität in virtualisierte Netzwerkschichten reduziert wird, zweitens eine bessere Zuverlässigkeit erzielt wird, die durch verbesserte Fähigkeiten zum erneuten Lokalisieren von Funktionen erreicht wird, und drittens eine bessere Kenntnis des Systemstatus. Tabelle 1 gibt einen Überblick über die Ergebnisse und Antworten, die aus den Implementierungen der Studienfälle gewonnen wurden.

Die folgende Tabelle fasst die Anwendungsfall-spezifischen Ergebnisse zu den drei Forschungsfragen zusammen.

Anwendungsfall	*Forschungsfrage 1: Konfigurationsaufwand bei Integration zusätzlicher Stromnetzkomponenten sowie Patch-Management minimieren?*	*Forschungsfrage 2: Systemzuverlässigkeit erhöhen bzw. Graceful degradation realisieren?*	*Forschungsfrage 3: SDN als Ansatz zur Netzwerk-Virtualisierung die Situationserkennung im IKT-Netz? Wie kann eine schnelle Wiederherstellung der Konnektivität im Fehler- und Angriffsfall erfolgen?*
Virtualised Redundancy	Abstraktion von Adressierungsinformationen durch SDN reduziert Netzwerkkonfigurationsaufwand und Fehlerpotenzial. In der SDN-basierten VirtueGrid-Implementierung müssen redundante Gateways nicht mehr individuell konfiguriert werden, auch ist kein Voter mehr notwendig.	Mithilfe von SDN lässt sich de-fakto Funktionalität auf eine Nachbarkomponente übertragen. Faktisch werden Kommunikationspfade im Anlassfall umkonfiguriert. In diesem Anwendungsfall ist das System sogar „fail operational“. Umschaltzeiten konnten auf maximal 5 Sekunden beschränkt werden (Kabelbruch: unter 1s), somit bleibt das SCADA System voll verfügbar. Die im Projekt implementierte SDN-Lösung ist jedoch für stärker zeitkritischen Datenverkehr (z.B. Regelung) nicht einsetzbar.	Eine SDN-basierte Variante von Fail-over Funktionalität wurde erfolgreich umgesetzt, um neben Netzwerkausfällen auch Fehler im Kommunikationsverhalten von Komponenten aufzudecken. SDN bietet standardisierte Schnittstelle für Netzwerkmonitoring die sowohl für die Überwachung der Netzwerkinfrastruktur als auch des Kommunikationsverhaltens genutzt werden kann. Analyse des Kommunikationsverhaltens könnte aber durch den Einsatz von P4 (zumindest potenziell falls keine Verschlüsselung vorhanden) verbessert werden.
Commissioning	Die Anwendbarkeit von kommerziell verfügbare Lösungen für andere Domänen für die Anwendung im Stromnetzkontext wurde im Projekt verifiziert. Durch eine Overlay-SDN-Lösung ist das Ausrollen von neuen Netzbereichen ohne manuelle Eingriffe möglich. Die automatische Konfiguration von Diensten mit vorgefertigten Templates verkürzt die Konfigurationszeit ebenso wie vereinheitlichte Netzkonfigurationen und einheitliche Security Policies. Dadurch ergibt sich insgesamt die Realisierung von neuen Diensten in sehr kurzer Zeit.		
Grid-based Routing		Sowohl mit SDN- als auch Brokerage-Ansätzen ist das Verändern von Kommunikationsbeziehungen zwischen Prozessen nach Bedarfsfall ohne Wissen der Anwendungen veränderbar. Hier war das Problem mit einem Broker einfacher zu lösen und hat besser in eine SCADA Architektur gepasst (z.B. wären sonst Dummy-Adressen für Feldkomponenten notwendig gewesen). Die Verschiebung von Funktionalität lässt sich durch App-Orchestrierungsansätze (Kubernetes, bzw. K3s) umsetzen, z.B. unter der Annahme, dass gewisse Apps in allen Netzsegmenten aktiv sein müssen.	Der Anwendungsfall betrachtet hier vor allem die Reaktion auf Vorfälle im IKT- und Stromnetz. Die Broker-Lösung kann bei partiellen Stromnetzüberlasten, sowie Ausfällen einzelner Übertragungsleitungen, nach einer notwendigen Netzumschaltung durch intelligentes Routing die Daten an die korrekten Endpunkte (Trafostationen, Überwachungsapps) weiterleiten. Eine automatisch getriggerte Umschaltung wurde hier nicht umgesetzt, kann aber mit der entwickelten Lösung ebenfalls umgesetzt werden.
Anomaly Detection	Die zentrale Verwaltung von Policies beim Einsatz eines SDN-Controller erleichtert nicht nur die Rekonfiguration im laufenden Betrieb, sondern auch die Einbindung von neuen Komponenten. Die Integration neuer Komponenten kann vom Controller erkannt werden und entsprechenden Policies für z.B.für Routing und QoS können angewendet werden. Unter Sicherheitsaspekten sind die Möglichkeit der Netzwerksegmentierung und Zugangskontrolle zu erwähnen		Durch die regelmäßige Abfrage der Flow-Statistik kann ein SDN-Controller über den aktuellen Status aller SDN-fähigen Switches im Netzwerk verfügen. Daraus lassen sich Informationen zu Überlast, Fehlern und Angriffen ableiten. Für die Anwendung von Algorithmen zur Anomalieerkennung auf Basis Flow-Informationen gibt es zahlreiche Beispiele. Im Rahmen von VirtueGrid konnte gezeigt werden, dass diese Ansätz auch auf Flow-Statistiken aus dem SDN anwendbar sind.

6.2 Virtualisierungsarchitektur

Durch eine Zusammenfassung der verschiedenen im Projekt angewandten Virtualisierungsansätze zu einer Meta-Architektur wird deutlich, in welchen Bereichen welche Virtualisierungstechniken eingesetzt wurden. Die gesamte Meta-Architektur ist in Abbildung 10 dargestellt. Die Komponenten des Kommunikationsnetzes befinden sich auf der linken Seite, während die angeschlossenen Stromnetzkomponenten, wie z.B. Transformatoren mit Stufenschalter und Sensoren, auf der rechten Seite zu sehen sind. Dargestellt ist ein typischer städtischer Versorger, bei dem das Kommunikationsnetz auch für die Steuerung des Gasnetzes und der Wasserversorgung genutzt wird. SDN ist in der Lage, ein breites Spektrum von Anwendungsfällen auf effiziente Weise zu unterstützen. Durch seine Verwendung können die Komplexität und Effizienz der eingesetzten Kommunikationslösungen erheblich reduziert werden. Die verschiedenen Anwendungsfälle lassen sich als separate SDN-Anwendungen auf dem SDN-Controller implementieren. Abhängig von der implementierten Netzwerktopologie können SDN-Switches von einem zentralen Controller gesteuert werden, der für die Verwaltung des SDN-Netzwerks als Ganzes verantwortlich ist.

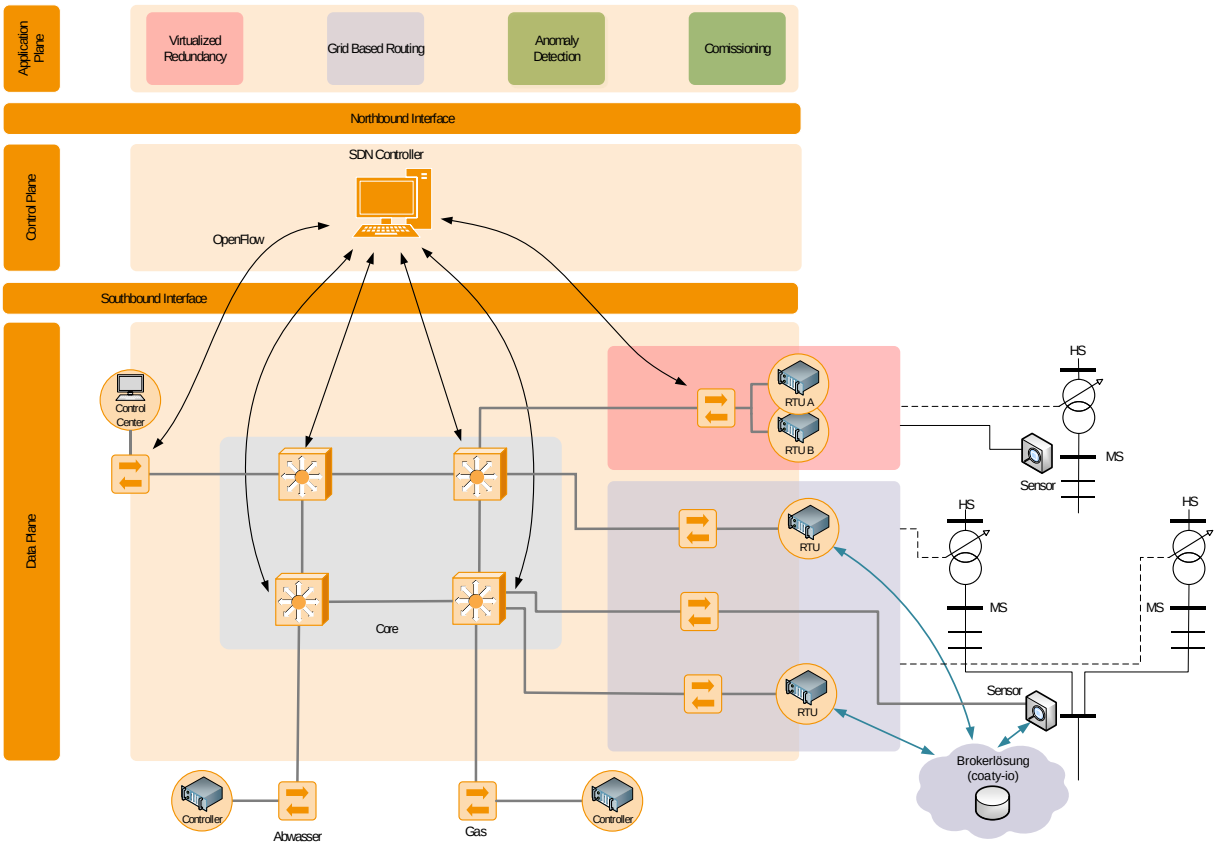


Abbildung 10: VirtueGrid Meta-Architektur

In Abbildung 10 sind die verschiedenen Applikationen in der Data Plane farbig hinterlegt. Während die Application Protocol Independent Redundancy (rot) und Grid Based Routing (violett) mit dedizierten Komponenten der Data Plane interagieren, findet in den Anomaly Detection (hellgrün) und Comissioning (dunkelgrün) die Kommunikation im Prinzip mit allen SDN-Switches im Netzwerk statt. Im vorliegenden Fall werden die Core-Switches als SDN-Switches von einem zentralen SDN-Controller gesteuert.

7 Schlussfolgerungen

Das Projekt VirtueGrid hat gezeigt, welche Rolle Virtualisierungsansätze übernehmen können, um im Kontext der Digitalisierung von Energieinfrastruktur die Systemkomplexität sowie die Konfigurationsaufwände bei Aufbau und Betrieb von Kommunikationsnetzen aus Betreibersicht zu verringern. Automatisierungstechnik spielt eine immer wichtigere Rolle für den Betrieb von elektrischen Verteilnetzen, jedoch bedeutet eine zunehmende Verwendung von IKT-Systemen und Kommunikationsstrecken auch eine Erhöhung der Systemkomplexität, des Engineering-Aufwands beim Aufbau und bei Wartung und Betrieb. Virtualisierungstechniken können diese steigende Systemkomplexität leichte beherrschbar machen. Durch die Implementierung von vier konkreten Anwendungsfällen war es möglich, allgemeine Schlüsse über den Nutzen (und die Grenzen) von Virtualisierungsansätzen zu ziehen.

Bereits zur Entwurfszeit von Automatisierungsanwendungen erlaubt beispielsweise die Verwendung von SDN, Funktionalitäten wie Redundanzbereitstellung und Redundanzaktivierung zu kapseln, so dass sie nicht mehr im Einzelfall auf Anwendungsebene entworfen werden müssen, sondern als Fähigkeit der Kommunikationsebene automatisch zur Verfügung steht. Mit Overlay-SDN ist es möglich, das Netzwerkmanagement von Fernwirk- und Prozessnetzwerken zu vereinfachen, virtuelle Netzwerktypen auf einer gemeinsamen Infrastruktur einfacher einzurichten bzw. zu verwalten, und neue Knoten ins Netz einfacher einzubringen. Insbesondere spartenintegrierte Betreiber, die neben Stromnetzen auch andere Infrastrukturen wie öffentlichen Verkehr, Fernwärme- oder Gasnetze betreiben, stehen vor der Herausforderung, große Mengen neuer Kommunikationsendpunkte für zusätzliche Sensoren und Aktuatoren „in die Fläche“ zu bringen.

Zur Betriebszeit des Systems erlauben Anwendungen aus dem Cloud- oder Edge-Bereich, die Systemkomplexität zu verringern, beispielsweise durch anpassen der Kommunikationspfade entweder im Netzwerk oder in einem zentralen (ggf. redundanten) Broker, so dass Sensorwerte in einem dynamisch betriebenen Stromnetz immer zum jeweils richtigen Controller gelangen. Darüber hinaus kann die Systemintegrität des IKT-Netzes, aber auch indirekt des Stromnetzes, leichter überwacht werden, wenn auf die einheitlichen Monitoring-Schnittstellen z.B. von SDN-Controllern zurückgegriffen wird.

Die Implementierung von Virtualisierungskonzepten in bestehenden Netzen und Automatisierungssystemen ist mit vergleichsweise geringem Aufwand umsetzbar. Nicht alle Router müssen z.B. getauscht werden, um SDN zu ermöglichen, sondern nur die Geräte am Anfang und am Ende der Kommunikationsstrecke. Broker-Lösungen eignen sich gut, um existierende SCADA-Systeme einfach zu erweitern.

8 Publikationen aus dem Projekt

I. Tobias Gawron-Deutsch, Florian Kintzler, Friederich Kupzog, Ferdinand von Tüllenburg, Ulrich Pache (2018): Grid Based Routing – VirtueGrid SDN Whitepaper. 2018 Global Internet of Things Summit (GIoTS), Bilbao, 2018, pp. 1-6.

II. Ferdinand von Tüllenburg, Jia Lei Du, Georg Panholzer (2018): Universelles Messaging für Smart Grid Anwendungen. Smart Energy Systems Week Austria (SESWA), Wien, 2018.

III. Armin Veichtlbauer, Florian Kintzler (2018): VirtueGrid - Virtualisierung in digitalisierten Energiesystemen. In: Tagungsband des 9. Symposiums Communications for Energy Systems (ComForEn 2018), Puch/Salzburg, Okt. 2018

IV. Armin Veichtlbauer, Ulrich Pache, Oliver Langthaler, Helmut Kapoun, Chritian Bischof, Ferdinand von Tüllenburg, Peter Dorfinger (2018): Enabling Application Independent Redundancy by Using Software Defined Networking. 10th int. congress on ultra modern telecommunications and control systems (ICUMT), Moscow, 2018.

V. Ferdinand von Tüllenburg, Peter Dorfinger, P., Armin Veichtlbauer, et al. (2019): Virtualising redundancy of power equipment controllers using software-defined networking. In: Energy Informatics 2, 14 (2019)

VI. Alexander Heinisch (2019): Potenziale von Virtualisierungsansätzen für die Netzsteuerung, Vortrag bei der ComForEn2019, 14.10.2019

VII. Oliver Langthaler (2019): Local Energy Community Systems and the Impact on Prosumers and the Smart Grid. In: Proceedings of the 8th DACH+ Conference on Energy Informatics (EI 2019), Puch/Salzburg, Sep. 2019

VIII. Fabian Knirsch, Oliver Langthaler, Dominik Engel (2019) Trust-less electricity consumption optimization in local energy communities. In: Proceedings of the 8th DACH+ Conference on Energy Informatics (EI 2019), Puch/Salzburg, Sep. 2019

IX. Workshop Software Defined Networking für Energienetze ComForEn 2019, Wien 14. - 15. Oktober 2019

X. Oliver Jung, Paul Smith, Julian Magin, Lenhard Reuter (2019): Anomaly Detection in Smart Grids based on Software Defined Networks. In SMARTGREENS (pp. 157-164).

XI. Lenhard Reuter, Oliver Jung, Julian Magin (2020): Neural network based anomaly detection for SCADA systems, ICIN 2020, Paris, 24.-27. Februar 2020

XII. Friederich Kupzog, Armin Veichtlbauer, Alexander Heinisch, Ferdinand von Tüllen-

burg, Oliver Langthaler, Ulrich Pache, Oliver Jung, Reinhard Frank, and Peter Dorfinger (2020): Impact of Virtualisation Techniques in Power System Control Networks, eingereicht bei MDPI Electronics, im Begutachtungsprozess

XIII. Alexander Heinisch et al., (2020): Grid Based Routing, eingereicht bei MDPI Electronics, im Begutachtungsprozess

9 Literaturverzeichnis

1. Capros, P.; Kannavou, M.; Evangelopoulou, S.; Petropoulos, A.; Siskos, P.; Tasios, N.; Zazias, G.; DeVita, A. Outlook of the EU energy system up to 2050: The case of scenarios prepared for European Commission's "clean energy for all Europeans" package using the PRIMES model. Energy strategy reviews 2018, 22, 255–263.
2. Brown, T.; Schlachtberger, D.; Kies, A.; Schramm, S.; Greiner, M. Synergies of sector coupling and transmission reinforcement in a cost-optimised, highly renewable European energy system. Energy 2018, 160, 720–739.
3. Skopik, F.; Smith, P., Smart Grid Security; Elsevier, 2015.
4. Kim, J.; Filali, F.; Ko, Y.B. Trends and potentials of the smart grid infrastructure: From ICT sub-system to SDN-enabled smart grid architecture. Applied Sciences 2015, 5, 706–727.
5. Chekired, D.A.; Khoukhi, L.; Mouftah, H.T. Decentralized cloud-SDN architecture in smart grid: A dynamic pricing model. IEEE Transactions on Industrial Informatics 2017, 14, 1220–1231.
6. Pfeiffenberger, T.; Du, J.L.; Arruda, P.B.; Anzaloni, A. Reliable and flexible communications for power systems: Fault-tolerant multicast with SDN/OpenFlow. 2015 7th International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2015, pp. 1–6.
7. von Tüllenburg, F.; Dorfinger, P.; Veichtlbauer, A.; Pache, U.; Langthaler, O.; Kapoun, H.; Bischof, C.; Kupzog, F. Virtualising Redundancy of Power Equipment Controllers Using Software-Defined Networking. Energy Informatics 2019, 2, 14. doi:10.1186/s42162-019-0086-y.
8. Naranjo, E.F.; Salazar Ch, G.D. Underlay and Overlay Networks: The Approach to Solve Addressing and Segmentation Problems in the New Networking Era: VXLAN Encapsulation with Cisco and Open Source Networks. 2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM); IEEE: Salinas, 2017; pp. 1–6. doi:10.1109/ETCM.2017.8247505.
9. Aydeger, A. Software Defined Networking for Smart Grid Communications. Master's thesis, Florida International University, 2016.
10. Hu, F.; Hao, Q.; Bao, K. A survey on software-defined network and openflow: From concept to implementation. IEEE Communications Surveys & Tutorials 2014, 16, 2181–2206.
11. Rehmani, M.H.; Davy, A.; Jennings, B.; Assi, C. Software Defined Networks-Based Smart Grid Communication: A Comprehensive Survey. IEEE Communications Surveys and Tutorials 2019, 21, 2637–2670, [1801.04613]. doi:10.1109/COMST.2019.2908266.

12. Aydeger, A.; Akkaya, K.; Cintuglu, M.H.; Uluagac, A.S.; Mohammed, O. Software defined networking for resilient communications in Smart Grid active distribution networks. 2016 IEEE International Conference on Communications, ICC 2016. Institute of Electrical and Electronics Engineers Inc., 2016, pp. 1–6. doi:10.1109/ICC.2016.7511049.
13. Lin, H.; Chen, C.; Wang, J.; Qi, J.; Jin, D.; Kalbarczyk, Z.T.; Iyer, R.K. Self-healing attack-resilient PMU network for power system operation. IEEE Transactions on Smart Grid 2018, 9, 1551–1565. doi:10.1109/TSG.2016.2593021.
14. Dorsch, N.; Kurtz, F.; Girke, F.; Wietfeld, C. Enhanced fast failover for software-defined smart grid communication networks. 2016 IEEE Global Communications Conference, GLOBECOM 2016 - Proceedings. Institute of Electrical and Electronics Engineers Inc., 2016, pp. 1–6. doi:10.1109/GLOCOM.2016.7841813.
15. Pfeiffenberger, T.; Du, J.L.; Arruda, P.B.; Anzaloni, A. Reliable and flexible communications for power systems: Fault-tolerant multicast with SDN/OpenFlow. 2015 7th International Conference on New Technologies, Mobility and Security - Proceedings of NTMS 2015 Conference and Workshops. Institute of Electrical and Electronics Engineers Inc., 2015, pp. 1–6. doi:10.1109/NTMS.2015.7266517.
16. Montazerolghaem, A.; Moghaddam, M.H.Y.; Leon-Garcia, A. OpenAMI: Software-Defined AMI Load Balancing. IEEE Internet of Things Journal 2018, 5, 206–218. doi:10.1109/JIOT.2017.2778006.
17. d. Silva, E.G.; d. Silva, A.S.; Wickboldt, J.A.; Smith, P.; Granville, L.Z.; Schaeffer-Filho, A. A One-Class NIDS for SDN-Based SCADA Systems. 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), 2016, Vol. 1, pp. 303–312.
18. Zhang, J.; Seet, B.C.; Lie, T.T.; Foh, C.H. Opportunities for Software-Defined Networking in Smart Grid. 2013 9th International Conference on Information, Communications Signal Processing, 2013, pp. 1–5. doi:10.1109/ICICS.2013.6782793.
19. Cahn, A.; Hoyos, J.; Hulse, M.; Keller, E. Software-defined energy communication networks: From substation automation to future smart grids. 2013 IEEE International conference on smart grid communications (SmartGridComm). IEEE, IEEE, 2013, pp. 558–563. doi:10.1109/SmartGridComm.2013.6688017.
20. Dacier, M.C.; Konig, H.; Cwalinski, R.; Kargl, F.; Dietrich, S. Security Challenges and Opportunities of Software-Defined Networking. IEEE Security & Privacy 2017, 15, 96–100. doi:10.1109/MSP.2017.46.
21. Scott-Hayward, S.; Natarajan, S.; Sezer, S. A Survey of Security in Software Defined Networks. IEEE Communications Surveys & Tutorials 2016, 18, 623–654.

doi:10.1109/COMST.2015.2453114.

22. Chowdhury, M.K.; Boutaba, R. A survey of network virtualization. Computer Networks 2010, 54, 862–876.
23. Zhou, X.; Li, R.; Chen, T.; Zhang, H. Network slicing as a service: enabling enterprises' own software-defined cellular networks. IEEE Communications Magazine 2016, 54, 146–153.
24. Pan, J.; McElhannon, J. Future edge cloud and edge computing for internet of things applications. IEEE Internet of Things Journal 2017, 5, 439–449.
25. Lua, E.K.; Crowcroft, J.; Pias, M.; Sharma, R.; Lim, S. A survey and comparison of peer-to-peer overlay network schemes. IEEE Communications Surveys & Tutorials 2005, 7, 72–93.
26. Yang, Z.; Cui, Y.; Li, B.; Liu, Y.; Xu, Y. Software-defined wide area network (SD-WAN): Architecture, advances and opportunities. 2019 28th International Conference on Computer Communication and Networks (ICCCN). IEEE, 2019, pp. 1–9.
27. Budka, K.C.; Deshpande, J.G.; Thottan, M.; others. Communication networks for smart grids; Springer, 2016.
28. von Tüllenburg, F.; Dorfinger, P.; Veichtlbauer, A.; Pache, U.; Langthaler, O.; Kapoun, H.; Bischof, C.; Kupzog, F. Virtualising Redundancy of Power Equipment Controllers Using Software-Defined Networking. Energy Inform 2019, 2, 14.
29. Dawoud, A.; Shahristani, S.; Raun, C. Deep Learning for Network Anomalies Detection. 2018 International Conference on Machine Learning and Data Engineering (iCMLDE); IEEE: Sydney, Australia, 2018; pp. 149–153. doi:10.1109/iCMLDE.2018.00035.
30. Reuter, L.; Jung, O.; Magin, J. Neural network based anomaly detection for SCADA systems. 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN); 2020.
31. Sharafaldin, I.; Lashkari, A.H.; Ghorbani, A.A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. ICISSP, 2018.

10 Abkürzungsverzeichnis

AMI	Advanced Metering Infrastructure
BEMS	Building Energy Management System
DER	Distributed Energy Resources
DoS	Denyal of Service
EMS	Energy Management System
GOOSE	Generic Object Oriented Substation Event
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IP	Internet Protocol
IT	Information Technology
JSON	JavaScript Object Notation
LAN	Local Area Network
LV	Low Voltage
MPLS	Multi-Protocol Labal Switching
MQTT	Message Queuing Telemetry Transport
MV	Medium Voltage
ONOS	Open Network Operating System
OSI	Open Systems Interconnection
OT	Operational Technology
P4	Programming Protocol-independent Packet Processors
PDC	Phasor Data Concentrator
PMU	Phasor Measurement Unit
PNS	Partial Network State
QoS	Quality of Service
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SDECN	Software-Defined Energy Communication Network
SDN	Software Defined Network

SD-WAN	Software Defined Wide Area Network
SGAM	Smart Grid Architecture Model
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSN	Time Sensitive Network
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
VxLAN	Virtual (Extensible) Local Area Network
WAMS	Wide Area Monitoring Systems

11 Kontaktdaten

ProjektleiterIn:

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH
Friederich Kupzog
friederich.kupzog@ait.ac.at

Oliver Jung
oliver.jung@ait.ac.at

Projektpartner:

FH SALZBURG

Oliver Langthaler
oliver.langthaler@fh-salzburg.ac.at

Ulrich Pache
ulrich.pache@fh-salzburg.ac.at

SIEMENS AG ÖSTERREICH

Alexander Heinisch
alexander.heinisch@siemens.com

SALZBURG RESEARCH

Ferdinand von Tüllenburg
ferdinand.tuellenburg@salzburgresearch.at

Peter Dorfinger
peter.dorfinger@salzburgresearch.at

NOKIA

Andreas Petritsch
andreas.petritsch@nokia.com

KELAG

Frédéric Gierlinger
frederic.gierlinger@kelag.at

KÄRNTEN NETZ

Georg Wurzer
georg.wurzer@kaerntennetz.at

LINZ STROM

Georg Linhard
g.linhard@linzag.at