OVE AKTUELL – Informationstechnik

„Energy goes ICT“

März 2020

Sehr geehrte Damen und Herren!

Gerade in der aktuellen Situation, von der wir alle betroffen sind, sind wir mehr denn je auf Informations- und Kommunikationstechnik angewiesen. Mit dem **Newsletter OVE AKTUELL**, diesmal mit dem Schwerpunkt **„Energy goes ICT“**, bieten wir Ihnen gerne eine interessante Lektüre für die Zeit, die Sie gezwungenermaßen zuhause verbringen.

An dieser Stelle finden Sie normalerweise einen **Hinweis zum Veranstaltungsangebot des OVE, aber mit COVID-19 ist alles anders: A**lle **Weiterbildungsangebote und Veranstaltungen des OVE sind bis auf Weiteres ausgesetzt**. Details dazu finden Sie hier.

Wir beobachten die Entwicklungen sehr genau und halten Sie natürlich auf unserer Homepage unter www.ove.at immer auf dem Laufenden. Herzlichen Dank für Ihr Verständnis und bleiben Sie gesund!

Weitere Neuigkeiten aus dem OVE finden Sie am Ende dieses Newsletters.

Energy goes ICT

Virtualisierungstechnologien für das Energienetz

Liebe Leserinnen, liebe Leser,

Die Notwendigkeit, massiv erneuerbare Energie auszubauen, wird an den Stromnetzen nicht spurlos vorübergehen. Die zunehmende dezentrale Erzeugung rückt nun die Smart Grids-Technologien wieder in den Vordergrund. Auch wenn man heute mehr von Digitalisierung spricht, ist Kommunikation ein Schlüsselfaktor für die Integration der erneuerbaren Energien.

Der Beitrag über die Virtualisierung der Energienetze behandelt die flexible Anwendung von Kommunikationstechnologien bei sich ständig ändernden Anforderungen. Virtualisierungstechnologien stellen Funktionalitäten nicht über dezidierte Hardware-Komponenten zur Verfügung, sondern bilden diese in Software ab. Lesen Sie darüber von Dipl.-Ing. Armin Veichtlbauer, FH Salzburg, Dipl.-Ing. Alexander Heinisch, Siemens und Dipl.-Inf.(FH) Ferdinand von Tüllenburg, MSc, Salzburg Research Forschungsgesellschaft.

Im Beitrag von Dr. Oliver Jung, AIT, wird die Software Defined Networks(SDN)-Technologie beschrieben. Er geht dabei auf die Anwendung von SDN für Smart Grids-Kommunikationsnetze ein, wobei die einzelnen Aspekte der Kommunikation und die Sicherheit behandelt werden.

Ein Beispiel einer Netzwerk-Virtualisierung wurde im Projekt VirtueGrid umgesetzt. Über die Forschungsfragen und die entwickelten Lösungskonzepte berichtet Dipl.-Ing. Friederich Kupzog, AIT, in seinem Beitrag.

Ich möchte mich ganz herzlich bei den Autoren für ihre Beiträge bedanken – und lade Sie ein, Ihre Meinung zu einem Thema im Bereich Energy goes ICT per E-Mail an informationstechnik@ove.at oder angela.berger@smartgrids.at direkt an mich zu senden.

Dipl.-Ing. Dr. Angela Berger
OVE-GIT-Arbeitsgruppenleiterin „Energy goes ICT"
Geschäftsführerin Technologieplattform Smart Grids Austria
Kontakt: angela.berger@smartgrids.at

Virtualisierung für Energienetze

Das bestehende Stromnetz befindet sich durch die Integration erneuerbarer Energien in einer bedeutenden Umbruchphase. Speziell das Niederspannungsnetz ist durch die große Anzahl an kleinen Einspeisern in seiner Stabilität gefordert. Informations- und Kommunikationstechnologien (IKT) stellen dabei eine Schlüsseltechnologie zu einer erfolgreichen Transformation in ein „Smart Grid" dar.

Die Anforderungen an eine geeignete IKT-Infrastruktur ändern sich laufend, sei es durch neue Grid Codes und regulatorische Rahmenbedingungen, durch neue Anwendungen und Services oder durch neue Herausforderungen im Bereich Sicherheit (Security) und Verlässlichkeit (Dependability). Gleichzeitig werden Investitionen im Energiebereich langfristig angelegt, mit Lebensdauern im Bereich von Jahrzehnten. Die Lösung dieses Dilemmas liegt für viele beteiligte Stakeholder in der Anwendung geeigneter Virtualisierungstechnologien.

Zielsetzungen

Bei diesen Virtualisierungstechnologien werden benötigte Funktionen der Infrastruktur nicht über eine dedizierte Hardware bereitgestellt, sondern über eine Abstraktionsschicht, die Hardware-Funktionen in Software abbildet. Diese Funktionen können dann flexibel an die jeweiligen geänderten Anforderungen angepasst werden. Das kann verschiedene Vorteile für die Betreiber von Energiesystemen und Energienetzen bringen:

- Aufwände für Konfigurationen oder Rekonfigurationen von Systemkomponenten können verringert werden.
- Bei System-Unterbrechungen durch Wartung oder im Fehlerfall können Steuerungsaufgaben anders verteilt werden.
- Die Situational Awareness bei Fehlern, Überlastsituationen oder im Angriffsfall kann verbessert werden.

Im Folgenden werden nun einige mögliche Ansätze für eine derartige Abstraktion und die damit bereitgestellten Dienste dargestellt.

Virtual (Extensible) LAN (VLAN / VxLAN)

Die wohl einfachste Stufe, Netzdienste zu virtualisieren, stellen VLANs dar. Sie ermöglichen eine leichter durchführbare Strukturierung von unternehmensweiten Netzen, indem auf einer klassischen geswitchten Netzwerkinfrastruktur verschiedene IP-Netze angelegt werden können, die untereinander nur nach selbst festzulegenden Kriterien geroutet werden können. Endgeräte an bestimmten Ports können beliebigen Netzen zugewiesen werden, und damit kann der direkte Zugang zu anderen Geräten auf bestimmte Nutzergruppen eingeschränkt werden.

Der Austausch zwischen diesen Gruppen unterliegt meist strikten Richtlinien, die etwa auf den beteiligten aktiven Netzgeräten in Form von Zugangslisten (Access Control Lists) oder durch Firewalls umgesetzt werden können. Somit können Datenströme verschiedener Nutzergruppen effektiv getrennt und kontrolliert werden.

Da die Verwendung von VLANs nicht standortübergreifend möglich ist, wurde die Erweiterung VxLAN definiert. VxLAN schließt getaggte Ethernet-Frames, wie sie gemäß IEEE 802.1Q für VLAN verwendet werden, in UDP Datagramme ein („Encapsulation“), die dann beliebig über VxLAN Tunnels zu anderen Standorten geroutet werden können. Da VxLANs existierende Netze (im Allgemeinen das Internet) als Basistechnologie („Underlay“) verwenden und deren Funktionalität in geeigneter Weise erweitern, stellen sie ein erstes Beispiel einer so genannten „Overlay“-Technologie dar.

Im Kontext von Energiesystemen können diese Technologien dazu verwendet werden, unterschiedliche Datenströme voneinander zu trennen und damit die wechselseitigen Beeinflussungen zu minimieren. Ein Beispiel dafür ist der Aufbau von virtuell getrennten Netzen für kritische Prozessdaten und weniger kritische Abrechnungsdaten.

Multi-Protocol Label Switching (MPLS)

Die Zuweisung bestimmter Qualitätseigenschaften (etwa die priorisierte Weiterleitung zeitkritischer Steuerbefehle) zu den Datenströmen ist mit VxLAN aber nicht möglich, da das zugrunde liegende Underlay nicht kontrolliert werden kann. Für diesen Zweck wird derzeit häufig MPLS als De-facto - Standard eingesetzt.

MPLS wurde ursprünglich entwickelt, um Router bei der Entscheidung über die Weiterleitung von Paketen zu entlasten, da diese mit MPLS nur deren jeweilige „Labels“ auswerten müssen. Die Route und die Qualitätsanforderungen können aus einer entsprechenden Tabelle abgeleitet und müssen nicht erst dynamisch berechnet werden. Somit können bestimmte Vorteile leitungsvermittelter Übertragungstechnologien auch in paketvermittelten Netzwerken nutzbar gemacht werden.

Aufgrund der hohen Performanz heutiger Geräte ist dieser Vorteil nicht mehr primär; die Eigenschaft jedoch, dass eine Menge gleichartiger Pakete (ein „Flow“) von den Routern auch gleichartig behandelt werden, da sie ja über dasselbe Label verfügen, wird heute oft als Grundlage für ein geeignetes Traffic Engineering genutzt (auch als MPLS-TE bekannt).

Damit ist es möglich, bestimmte Qualitätseigenschaften („Quality of Service“) der Übertragung an die verschiedenen Anforderungen der Anwendungen anzupassen. Das wird im Allgemeinen vertraglich über Service Level Agreements geregelt. Nachteilig ist jedoch, dass die dafür verwendeten MPLS-Pfade im Vorhinein anzulegen sind. Eine an die aktuelle Lastsituation angepasste flexible Weiterleitung (wie z. B. dynamisches Load Balancing) ist damit nicht möglich.

Speziell für den Transport von prozesskritischen Informationen innerhalb eines Netzes können durch MPLS(-TE) Qualitätseigenschaften wie maximale Verzögerung und Paketverluste spezifiziert und im Netz durchgesetzt werden.

Cloud und Edge Computing

Cloud Computing ist eine Technologie, die virtuelle Geräte („Platform as a Service“), Anwendungen („Software as a Service“) oder virtuelle Infrastrukturen („Infrastructure as a Service“) unabhängig von einer konkreten physischen Realisierung anbietet. Rein funktional bietet eine derartige Infrastruktur genau die oben beschriebene Abstraktion, indem sie in der Lage ist, die notwendige Flexibilisierung für Energieversorger, Konsumenten sowie Drittparteien offerieren zu können.

Um die angebotenen Services in einem ausreichenden Maß verfügbar zu machen, bieten die meisten Cloud-Anbieter entsprechende Redundanzen, um die Ausfallsicherheit zu erhöhen. Die Verfügbarkeit liegt jedoch meist nicht im Bereich des jeweiligen Netzbetreibers. Sobald spezielle Anforderungen an Security oder Liability gestellt werden, sollten Plattformen herangezogen werden, die „On-Premises“ betrieben werden können.

Werden Cloud-Dienste eines Dritten konsumiert, so sollte eine detaillierte Analyse der spezifischen Leistungsanforderungen (z. B. Echtzeitfähigkeit) durchgeführt werden, da auch der jeweilige Zugang zum Cloud-Dienst bereitgestellt werden muss. Auch hier stellen viele Cloud-Anbieter Lösungen bereit, um die jeweiligen Zugänge zu optimieren. Dabei werden etwa geographisch verteilte Ressourcen angeboten. Dennoch bleibt ein Zugang, der über eine öffentliche Infrastruktur erfolgt, immer eine schwer berechenbare Größe.

Vielerorts wird daher „Edge Computing“ als geeignete Alternative angesehen, bei der die Funktionalität an den Rand der Cloud verlagert wird. Dieser liegt dann wieder im Bereich der Infrastruktur des Netzbetreibers, der somit kritische Tasks, wie Regelungen oder Verrechnungen, in seinem eigenen Hoheitsbereich behält. Bei der Kopplung verschiedener verteilter Standorte kann dann wieder auf eine öffentlich erreichbare Cloud-Variante zurückgegriffen werden.

Für den Betrieb von Energiesystemen bieten sich (On-Premises-)Cloud-Anwendungen beispielsweise an, um weniger zeit- und betriebskritische Daten zu verarbeiten, wie z. B. Visualisierungen, während zeitkritische Schutzanwendungen auf geeignete Edge-Knoten ausgelagert werden.

Software Defined Networking (SDN)

Konsequent weitergedacht, kann jedoch nicht nur eine Server-Infrastruktur (wie bei einem klassischen Cloud-Service) virtualisiert werden, sondern die gesamte IKT-Infrastruktur, also inklusive aller Zugänge zu entsprechenden Backend-Services in der Cloud. In dem Fall können auch Netzwerkfunktionen wie Routing und in Zukunft immer wichtiger werdende Security Anwendungen, wie Intrusion Detection, durch virtualisierte Komponenten abgearbeitet werden, wodurch die Flexibilität im Vergleich zu MPLS deutlich zunimmt.

Diese virtualisierten Netzwerkkomponenten werden im Allgemeinen per Software angesteuert. Mit SDN können Weiterleitungsentscheidungen für Pakete auf der Basis verschiedener Metadaten wie Quelladressen, QoS-Anforderungen etc. getroffen werden, nicht nur auf Basis der Zieladresse oder des Labels. Jedoch können anwendungsspezifische Informationen und Metadaten nicht als Grundlage der Entscheidungen verwendet werden, da mit SDN nur die Metadaten aus den unteren Schichten des OSI-Modells ausgewertet werden können.

Klassischerweise wird SDN in geswitchten Umgebungen eingesetzt, mit dem Vorteil, eine dedizierte Infrastruktur zu haben, die unter voller Kontrolle des Netzbetreibers steht. Für verteilte Standorte ist eine rein geswitchte Umgebung jedoch nicht praktikabel; dieser Nachteil soll durch „SD-WAN“ ausgeglichen werden. Auch dabei wird eine Overlay-Architektur für verteilte Standorte zur Verfügung gestellt, die privat im alleinigen Zugriff durch die Netzbetreiber bleibt. Das öffentliche Underlay wird dabei über zu definierende Service Level Agreements von einem Infrastrukturanbieter (Carrier) zur

Verfügung gestellt. Das kann auch als ein Cloud-Ddienst interpretiert werden („Network as a Service“), benötigt aber keinen Drittanbieter zum Zugang mehr, da der Zugang Teil des Service Level Agreements ist. Somit ist hier die Liability einfacher zu regeln.

SDN erlaubt also dem Betreiber eines Energiesystems die Kombination von strikter Verkehrstrennung, Qualitätszusicherung sowie Konfigurationsflexibilität mit einer einzigen Technologie.

Programming Protocol-Independent Packet Processors (P4)

Der schwerwiegendste Nachteil von SDN in der klassischen Bedeutung ist die Einschränkung auf Metadaten der unteren Schichten des OSI-Modells (Schichten 2 und 3). Das verhindert Anwendungen wie Application Layer Routing, wo Anwendungsdaten als Grundlage für die Weiterleitung von Paketen verwendet werden.

Mit P4 können diese Nachteile weitgehend umgangen werden. P4 erlaubt eine vollständige Kontrolle der Algorithmik zur Weiterleitung von Paketen („Control Plane“) durch eine geeignete Software. Die Möglichkeiten der Programmierung sind dabei so flexibel, dass P4 als eigene Programmiersprache angesehen wird.

Über die Steuerung der Weiterleitung hinaus können auch die zu sendenden Daten entsprechend weiterverarbeitet werden („Data Plane“). Das ermöglicht etwa Funktionen wie Aggregation auf Ebene der Netzwerkinfrastruktur. Diese Art von Flexibilität bietet sonst derzeit keine andere Technologie zur Virtualisierung von Netzwerkfunktionen.

Jedoch hat auch P4 einige bedeutende Einschränkungen in der Praxis. Einerseits sind entsprechende P4-fähige Infrastrukturen noch selten, andererseits ist die Anwendbarkeit dieser Technologie durch die zunehmende Verwendung von Ende-zu-Ende-Verschlüsselung auch beschränkt, da die verschlüsselten Daten nicht von den Switches interpretiert werden können und somit auch nicht als Grundlage einer Algorithmik zur Entscheidung über die Behandlung einzelner Pakete verwendet werden können.

Ein Netzbetreiber kann P4 beispielsweise dazu nutzen, die Aktivitäten von Feldgeräten zu überwachen, indem auch die Inhalte bzw. Typen der versendeten Informationen der Geräte betrachtet werden. Der Überwachungsvorgang erfolgt dabei transparent auf den Knoten des Kommunikationsnetzes.

Über die Autoren

Dipl.-Ing. Armin Veichtlbauer hat einen Abschluss in „Angewandter Informatik“ der Universität Salzburg. Seine Forschungsschwerpunkte liegen in den Bereichen Netzwerktechnik und Energie-Informatik. Er hat langjährige Erfahrung in Forschungsprojekten und beschäftigt sich aktuell mit dem Testen verschiedener Forschungsprototypen zur Virtualisierung einer geeigneten IKT-Infrastruktur in Niederspannungsnetzen. Er arbeitet aktuell an den Fachhochschulen Salzburg und Oberösterreich.

Dipl.-Ing. Alexander Heinisch hat das Masterstudium „Technische Informatik“ an der Technischen Universität Wien abgeschlossen. Seither befasst er sich eingehend mit den Themenbereichen Embedded Systems, Distributed Computing sowie Dependable Computing. Aktuell ist er als wissenschaftlicher Mitarbeiter in der Forschungsabteilung Corporate Technology im Bereich Smart Grid, Smart Building und Industrial IoT bei Siemens AG Österreich tätig.

Dipl.-Inf. (FH) Ferdinand von Tüllenburg, MSc. hat Allgemeine Informatik an der Technischen Hochschule Regensburg sowie an der Universität Passau studiert. Sein wissenschaftlicher Schwerpunkt liegt im Bereich der Computer-Netzwerke; derzeit erforscht er die Auswirkungen des Einsatzes von Kommunikationstechnologien in Energiesystemen und anderen kritischen Infrastrukturen. Seit 2013 ist er als Forscher bei der Salzburg Research Forschungsgesellschaft mbH beschäftigt.

Dipl.-Ing. Armin Veichtlbauer
Fachhochschule Salzburg GmbH
Zentrum für Sichere Energieinformatik

Dipl.-Ing. Alexander Heinisch
Siemens AG Österreich
CT RDA IOT INN-AT

Dipl.-Inf. (FH) Ferdinand von Tüllenburg, MSc.
Salzburg Research Forschungsgesellschaft mbH
Advanced Networking Center

Software Defined Networks für die Energiebranche

Bei Software Defined Networks (SDN) handelt es sich um eine Technologie, die bereits im Jahr 2005 an der Universität Stanford entstanden ist und in den nachfolgenden Jahren so weiterentwickelt wurde, dass mittlerweile von zahlreichen Netzwerkausrüstern entsprechende Produkte angeboten werden. Der Einsatz von SDN kann auch für die Kommunikation im Smart Grid entscheidende Vorteile in Bezug auf Zuverlässigkeit, Effizienz und Sicherheit mit sich bringen.

Der prinzipielle Ansatz von SDN ist, die Netzwerkintelligenz in einer Netzwerkkomponente, dem SDN-Controller, zu zentralisieren und den Prozess der Weiterleitung von Netzwerkpaketen (Data Plane) vom Routing-Prozess (Controll Plane) zu trennen. Der SDN-Controller als Software-Komponente mit definierten Schnittstellen kann als Plattform für nutzerdefinierte Netzwerk-Anwendungen dienen.

Smart Grid-Kommunikation

Intelligente Stromnetze müssen eine Reihe verschiedener Funktionalitäten und Anwendungen unterstützen, die wiederum spezifische Leistungsanforderungen an die Kommunikationsinfrastruktur haben. Diese Infrastruktur muss eine große Anzahl geografisch verteilter Geräte, wie z. B. Leitgeräte in Umspannwerken, Steuerung für verteilte Erzeugungsanlagen, Smart Meter oder Ladestationen für Elektrofahrzeuge, über verschiedene Distanzen vernetzen. Systeme zur Steuerung des Stromnetzes erfordern eine zuverlässige Datenübertragung bei geringen Latenzzeiten. Im Gegensatz dazu ist die

Hauptanforderung für Anwendungen beim Kunden, wie z. B. Smart Meter, die Skalierbarkeit. Smart Meter-Daten sind in der Regel unempfindlich gegenüber geringer Bandbreite oder hoher Latenz.

SDN in Smart Grids

Der zentrale SDN-Controller ermöglicht es, Netzwerkkomponenten wie Router und Switches durch Manipulation des Verkehrsflusses dynamisch zu konfigurieren, um somit durch die Verhinderung und die Eindämmung von Ausfällen des Kommunikationsnetzes, die Quality of Service (QoS) und Systemstabilität zu verbessern. Unter anderem ermöglicht SDN in Smart Grids:

- Isolierung von Verkehrsklassen und Anwendungen: Mittels SDN lassen sich physische Netzwerkinfrastrukturen in unabhängige virtuelle Netzwerke unterteilen. Man spricht dabei auch, vor allem im Zusammenhang mit 5G, über Netzwerk-Slices. Die verschiedenen Netzwerke unterstützen unterschiedliche Anforderungen in Bezug auf Bandbreite, Latenz und Zuverlässigkeit. Durch diese virtuellen Netze lassen sich auch einzelne Smart Grid-Anwendungen isolieren.
- QoS-Unterstützung: SDN unterstützt QoS-Mechanismen, durch die es möglich ist, beispielswiese zeitkritischen Messungen oder Kontrollkommandos eine höhere Priorität zu geben, z. B. durch Reservierung von Verbindungen zwischen Leitstelle zum Umspannwerk.
- Zuverlässigkeit: Die Zuverlässigkeit von Smart Grid-Kommunikationsnetzen kann durch schnelles Umleiten und Umschalten von ausgefallenen Verbindungen erhöht werden. Die von SDN bereitgestellten Mechanismen ermöglichen im Vergleich zu klassischen Routing-Mechanismen eine geringere Latenzzeit im Falle eines Failover, da die SDN-Mechanismen schneller auf Netzwerkereignisse reagieren können.
- Sichtbarkeit des Kommunikationsnetzes: Der zentrale SDN-Controller erfragt periodisch Statusinformationen von den angeschlossenen SDN-Switches. Dadurch verfügt er über eine vollständige Übersicht aller Datenströme im Netzwerk und weiß über die Anzahl der empfangenen Pakete und Bytes, die verfügbare Bandbreite und die Verbindungen Bescheid. Erfasste Statistiken, die eine Echtzeit-Ansicht des Netzwerkstatus bieten, sind über offene APIs zugänglich und somit eine bequeme Informationsquelle für Anwendungen zur Verkehrsüberwachung.
- Sicherheit: Die Isolierung von Verbindungen ist eine Voraussetzung für sichere Smart Grid-Kommunikationsnetze und wird von einschlägigen Branchenrichtlinien empfohlen. Die Link-Isolation kann darüber hinaus zur Durchsetzung von Richtlinien zur Zugriffskontrolle und zur Implementierung von Einweg-Kommunikation verwendet werden, bei der Nachrichten nur von einer vertrauenswürdigen zu einer weniger vertrauenswürdigen Domäne und nicht umgekehrt gesendet werden können. Darüber hinaus können SDN-Verkehrs-Routing-Funktionen verwendet werden, um böswilligen Verkehr, der von Denial-of-Service-Angriffen oder Netzwerk-Scans stammt, zu blockieren oder umzuleiten.

SDN und Sicherheit

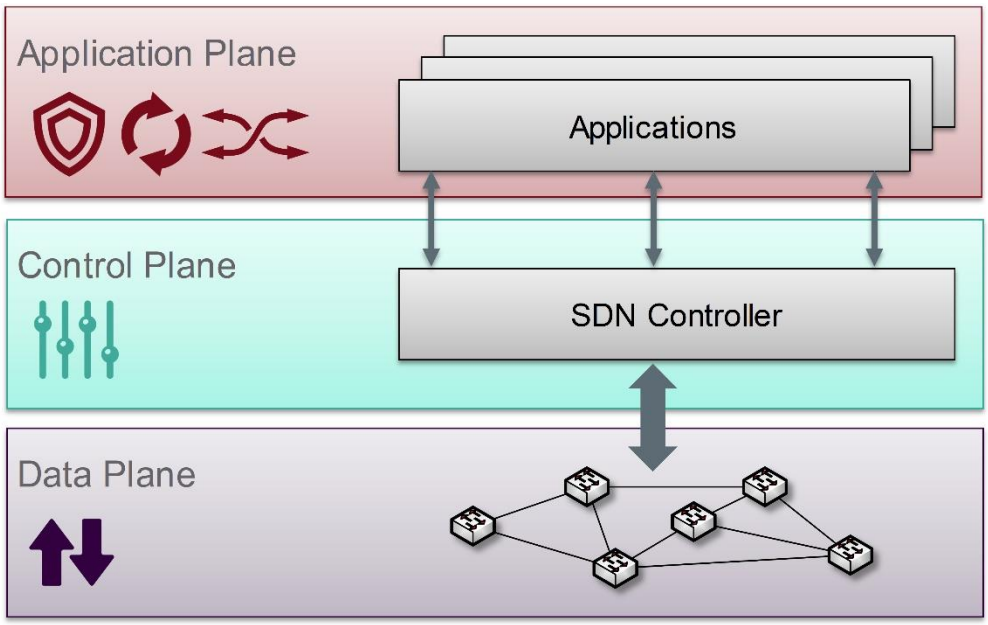
Das SDN-Paradigma kann zwar die Sicherheit von Smart Grid-Kommunikationsnetzen mit neuen Ansätzen zur Verhinderung, Erkennung und Eindämmung von Angriffen verbessern, mögliche negative Einflussfaktoren sollten aber nicht unerwähnt bleiben.

Die Einführung mehrerer Netzwerkanwendungen kann die Systemkomplexität deutlich erhöhen. Sie erschwert es, eine bestimmte Anwendung zu identifizieren, die für die Änderung von Regeln verantwortlich ist.

Die SDN-APIs ermöglichen es andererseits, aufwendige Sicherheitsanwendungen zu implementieren. Die Erfassung von Netzwerkstatistiken, die Isolierung von Netzwerken und die Nutzung der aktiven Angriffsreaktion können erheblich vereinfacht werden.

Der Nachteil des zentralen Controllers besteht darin, dass er einen Single Point of Failure darstellt, was die Systemstabilität potenziell verschlechtert und ein attraktives Ziel für Angreifer ist. Angreifer, die in der Lage sind, den Controller zu kompromittieren, können die volle Kontrolle über das Netzwerk erlangen. Darüber hinaus ist der Controller anfällig für Denial-of-Service-Angriffe, die eine große Anzahl von unbekannten Datenströmen verwenden und damit den Controller überlasten. Dem kann nur zum Teil durch redundante Controller entgegengewirkt werden.

Die zentralisierte Echtzeit-Situationserkennung des Controllers ermöglicht es jedoch auch, Denial-of-Service-Angriffe zuverlässiger zu erkennen und Angriffe durch Neukonfiguration des Netzwerks abzuschwächen, d. h. Pakete, die als Teil eines Angriffs identifiziert werden, können fallen gelassen oder an eine Sicherheitsanwendung umgeleitet werden.



Zusammenfassung

SDN kann somit zahlreiche Vorteile für Smart Grid-Kommunikationsnetze bringen. Dabei stellen die erhöhte Zuverlässigkeit, die leichtere Konfigurierbarkeit und die verbesserte Sicherheit wesentliche Aspekte dar. Einige Verteilnetzbetreiber evaluieren derzeit in Feldversuchen den Einsatz von SDN in ihren Prozessnetzen.

Über den Autor

Dipl.-Ing. Dr. Oliver Jung ist Scientist am Center for Digital Safety & Security des Austrian Institute of Technology. Sein Forschungsschwerpunkt ist die IKT-Sicherheit in Smart Grids.

Dipl.-Ing. Dr. Oliver Jung
AIT Austrian Institute of Technology
Center for Digital Safety & Security

Netzwerk-Virtualisierung im Energiesystemkontext – das Projekt VirtueGrid

Projektübersicht

Zur Integration erneuerbarer Energien in das bestehende Stromnetz stellen Informations- und Kommunikationstechnologien (IKT) eine Schlüsseltechnologie dar. Neben den aktuellen Anwendungen Metering und Billing werden zukünftig auch Stromnetz-Monitoring, -Regelung und dezentrales Energiemanagement eine große Rolle spielen. Unter den neuen Voraussetzungen (große Anzahl neuer Knoten, heterogene Systemelemente in unterschiedlich kritischen Bereichen) müssen die auch bisher geltenden Ziele Verfügbarkeit, Sicherheit, Resilienz und Effizienz der Kommunikationssysteme weiterhin erreicht werden. Eine reine Skalierung der heute für den Verteilernetzbetrieb eingesetzten IKT mit Ergänzung durch ein State-of-the-Art-Sicherheitskonzept reicht dazu nicht aus. Die noch vorwiegend manuellen Verfahren für Maßnahmen, wie Störungsmanagement, Konfiguration neuer vernetzter Komponenten oder Test neuer IT-Komponenten, erweisen sich hier als höchst ineffizient.

Virtualisierungskonzepte aus dem IKT-Bereich, konkret Cloud- und Edge-Computing sowie dynamische virtuelle Local Area Networks oder Software Defined Networking bieten potentielle Lösungen für praktische Kernfragen, wie beispielsweise die Konfiguration neuer Protokoll-Stacks, Cross-Layer-Optimierungen zwischen Energie- und Kommunikationsnetzen, Integration von non-IP-Traffic, Legacy-Komponenten oder der zeitnahen Prüfung der Systemintegrität. Durch Virtualisierung liegen die Komponenten eines dezentralen Automationssystems scheinbar zentral beisammen und können an einer Stelle konfiguriert und betrieben werden. VirtueGrid untersucht, auf welche Weise und wie gut Virtualisierungstechnologien die wesentlichen zukünftigen Anwendungsfälle unterstützen können.

Im Kontext von drei Forschungsfragen werden neue Lösungskonzepte entwickelt:

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?

Eine Evaluierung der entwickelten Konzepte findet dreistufig in Simulation, Labor und einer Feldumgebung im Bereich der Linz Strom und KELAG/KNG statt.

Anwendungsfälle

VirtueGrid geht von einer Hypothese zu potenziellen Anwendungsbereichen von Virtualisierungstechniken aus, die sich im Projektverlauf bestätigt bzw. konkretisiert hat. Die folgenden Entwicklungslinien werden bearbeitet:

1. Kommissionierung und Skalierbarkeit – Der Einsatz von Virtualisierung im Sinne einer scheinbar zentralen Konfiguration aller verteilten Knoten reduziert das Risiko von Ausfällen durch Fehlkonfiguration. Reduktion des Konfigurationsaufwands ist ein wesentlicher Effizienzfaktor. Stand der Technik ist, dass neue Geräte manuell von Technikern konfiguriert

bzw. Vorkonfigurationen angepasst werden. Im Projekt wird eine Verbesserung von Stunden auf Minuten angestrebt.

2. Offenheit für neue Protokollstacks – Einer der wesentlichen Vorteile beim Einsatz von virtualisierten IKT-Komponenten wie Routers, Switches, Zugangstechnik und CPEs für Kommunikationsdienste in kritischen Infrastrukturen ist die Tatsache, dass Protokolle aus der etablierten SCADA-Welt bzw. auch neue Protokoll-Stacks aus den bereits verabschiedeten Standards bzw. den Standards, die gerade im Entstehen sind, mit eingebunden werden können. Nur dann wird eine Transformation zu virtualisierten Kommunikationslösungen möglich sein und auch mittelfristig vom Markt akzeptiert werden. Weiters müssen Architekturen offen sein für Einbindungen von jetzt noch nicht bekannten Protokoll-Stacks, die sich von in Zukunft neu entstehenden Anforderungen ableiten.
3. Integration von Non-IP-Netzwerken und Legacy Komponenten – VirtueGrid erarbeitet Konzepte für die Integration von Komponenten mit Hilfe von SDN, die z. B. Modbus RTU oder IEC 60870-5-101 unterstützen. Ein Fokus liegt hier insbesondere auf Ansätzen für das Routing von Non-IP über IP sowie die Integration von Komponenten ohne Sicherheitsfunktionalität und wie dies durch SDN vereinfacht werden kann, während die Leistungsfähigkeit des Systems verbessert wird.
4. Cross Layer-Optimierung und Grid based Routing – schnelle Wiederherstellung der Telekommunikations-Konnektivität im Fehler- und Angriffsfall. Im SDN-Fall kann schneller und informierter als bei bestehenden Routing-Systemen reagiert werden. Dadurch wird das Gesamtsystem robuster gegen Fehler und Angriffe. Zeiten für die Wiederherstellung der Kommunikation werden von Sekunden auf Millisekunden reduziert. Weiters kann durch eine engere Kopplung von IKT- und Anwendungsschicht in Zukunft robustere Messwertübertragung zum korrekten Endpunkt realisiert werden.
5. Zeitnahe Systemintegritätsüberwachung – proaktive Erkennung von Fehlern und Angriffen im IKT-Netz und ggf. Rückschluss auf außergewöhnliche Ereignisse und Störungen im Stromnetz. Die Erkennung von Angriffen führt, verbunden mit geeigneten Maßnahmen, zu höherer Verfügbarkeit. Es ergeben sich eine deutlich vereinfachte Implementation und Betrieb von z. B. Anomalieerkennung durch Nutzung der Northbound-Schnittstellen der Virtualisierungs-techniken. Einheitliche Schnittstellen für das Aufsetzen von Anomalieerkennungs-Algorithmen machen diese erst sinnvoll einsetzbar.

Im Projekt VirtueGrid werden vier konkrete Anwendungsfälle implementiert, welche die oben diskutierten Themen abdecken.

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 so genannte Generalabfrage der Informationszustand in der neuen betriebsführenden Komponente zu aktualisieren.

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.

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 Daten-Quellen und -Senken über die Stromnetztopologie miteinander verbunden (siehe Abb.) Je nach momentaner Ausprägung der Stromnetztopologie (Stellungen der im Netz enthaltenen Schalter) sind dabei die Daten-Quellen unterschiedlichen Daten-Senken zugeordnet. In der **Fehler! Verweisquelle konnte nicht gefunden werden.**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.

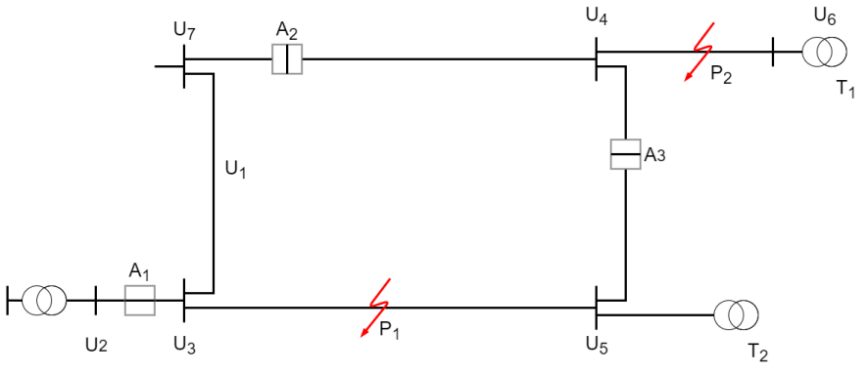


Abb. Basis-Stromnetz-Topologie Anwendungsfall 3 – Grid Based Routing

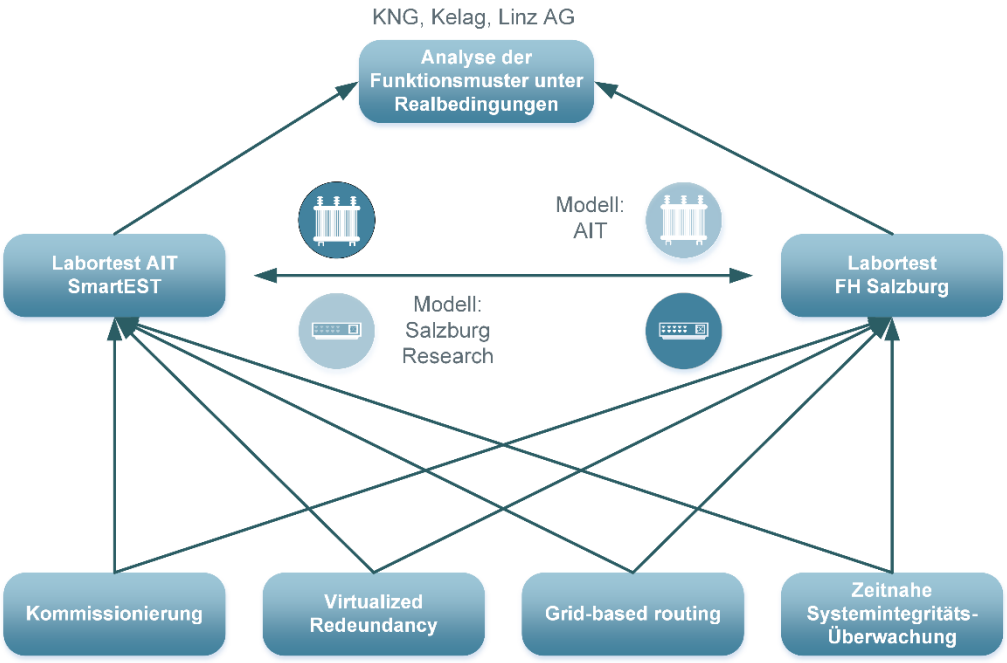
Anwendungsfall 4: Anomaly Detection

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 einen 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 Flow-Statistik 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



Über den Autor

Dipl.-Ing. Dr. Friederich Kupzog ist Head of Competence Unit am Center for Energy des Austrian Institute of Technology. Er koordiniert seit über zehn Jahren Forschungsprojekte im Schnittbereich von Energie- und IKT-Systemen.

Dipl.-Ing. Dr. Friederich Kupzog
AIT Austrian Institute of Technology
Center for Energy

Aktuelles aus dem OVE

Covid-19: Der OVE bleibt auch weiterhin erreichbar

Der OVE unterstützt die Maßnahmen zur Eindämmung des Coronavirus und damit auch die behördlichen Vorgaben zur Reduktion der Sozialkontakte. Damit unsere Mitarbeiterinnen und Mitarbeiter wie gewohnt für Sie erreichbar bleiben, haben wir entsprechende Maßnahmen getroffen.

OIB Richtlinie 6: OVE gegen Benachteiligung der Energieform Strom

Die aktuelle OIB Richtlinie 6 „Energieeinsparung und Wärmeschutz“ benachteiligt in mehreren Punkten die Energieform Strom. Damit Österreichs Klimaziele erreichbar bleiben, bedarf es einer Nachbesserung.

„Klima wenden": Videowettbewerb geht in die heiße Phase

Noch bis Mai läuft der Videowettbewerb von ScienceClip.at. Mit ihren Wissenschaftsvideos zum Thema Klimaschutz können Schülerinnen und Schüler ab der 5. Schulstufe attraktive Preise gewinnen.

Mit freundlichen Grüßen
Ihr OVE Österreichischer Verband für Elektrotechnik

Hinweis: *Nicht immer werden in diesem Newsletter weibliche Formen explizit angeführt. Es wird jedoch ausdrücklich darauf hingewiesen, dass sich alle personenbezogenen Formulierungen grundsätzlich gleichermaßen auf Frauen und Männer beziehen. -*

Impressum:
OVE Österreichischer Verband für Elektrotechnik
Krenngasse 37
8010 Graz