Modellierung von Sicherheitsschichten und -Zonen für eine Sichere IKT-Infrastruktur in Energie-Effizienz-Verbünden

Verteilte Steuerungen im intelligenten Stromnetz sicher und resilient gestalten.

Marius Stübs[1], Maximilian Blochberger[1], Hannes Federrath[1], Raoul Pascal Pein[2], Edith Kirsch[3], Roman Tschepat[4]

Abstract: Die Steuerung von verteilten Energieanlagen und Verbrauchern wird heutzutage bereits stark automatisiert. Unter anderem wird dadurch in Echtzeit sichergestellt, dass Abweichungen von geplanten Stromerzeugungs- und Verbrauchsmengen kompensiert werden können. Ein hoher Grad an Automatisierung und vernetzter Kommunikation muss allerdings immer mit entsprechenden Sicherheitskonzepten einhergehen. Wir stellen eine Systematik vor, mit der sich die Bedrohungen durch böswillige und fehlerhafte Komponenten im Kommunikations- und Steuerungssystem verteilter Energieanlagen einordnen und strukturieren lassen. Dazu werden vier Ebenen beschrieben, in die sich Angriffe und Schutzmaßnahmen kategorisieren lassen. Mittels dieser Ebenen lassen sich zu verteidigende Angriffsflächen identifizieren und schließlich reduzieren. Unter Verwendung der Systematik wird ein Bedrohungsszenario analysiert und dafür eine Schutzmaßnahme entwickelt und evaluiert.

Keywords: Intelligente Stromnetze, IKT-Sicherheit, Netzwerksicherheit, Resilienz, ITSM

1 Transformation des Energienetzes

Die Zahl verteilter Energieanlagen im Stromnetz nimmt stetig zu [De07]. Die Integration von verteilten Energieanlagen bringt neue Herausforderungen für die Steuerung des Stromnetzes mit sich [MMNQ13]. Intelligente Stromnetze (engl. Smart Grids) nutzen Informations- und Kommunikationstechnologie (IKT), um eine verbesserte Überwachung und Steuerung im Vergleich zu herkömmlichen Stromnetzen zu ermöglichen [Fu17]. Sie bestehen aus verteilten Energieanlagen, Energiespeichern und Steuergeräten [MMIK17]. Dabei können sie entweder am öffentlichen Stromnetz angeschlossen sein oder im Inselmodus betrieben werden, indem sie vom öffentlichen Stromnetz getrennt sind und die Frequenz und Spannung des Stromnetzes selbst steuern [Ba14]. Es kann vorteilhaft sein, diese Steuerung durch ein dezentrales System aus verteilten Energieanlagen zu realisieren, da es möglicherweise fehlertoleranter gegenüber einem zentralisierten System sein kann und außerdem besser skalierbar ist [De07]. Solch eine Steuerung braucht eine

[1] Universität Hamburg, Sicherheit in verteilten Systemen, {nachname}@informatik.uni-hamburg.de
[2] HAMBURG ENERGIE GmbH, Billhorner Deich 2, 20539 Hamburg, pascal.pein@hamburgenergie.de
[3] QSC AG, Weidestraße 122b, 22083 Hamburg, edith.kirsch@qsc.de
[4] cbb software GmbH, Isaac-Newton-Straße 8, 23562 Lübeck, roman.tschepat@cbb.de

offene Kommunikationsinfrastruktur, um die steigende Dezentralität der Energieproduktion und Speicherung zu unterstützen [MMNQ13]. Jedoch wird durch diese offene Architektur des Netzes die Angriffsfläche erhöht [SYA14]. Etwa könnte die Steuerung der Energieanlagen manipuliert werden, um sie in einen unsicheren Zustand zu bringen [HM17], zum Beispiel durch Denial-of-Service-Angriffe (DoS-Angriffe) oder das Einspielen falscher Daten [Fu17]. Daraus entstehende Fehlfunktionen können zu einer Überspannung und zu einem Stromausfall führen [HM17].

Da mit dem IT-Sicherheitsgesetz und dem IT-Sicherheitskatalog der BNetzA gesetzliche Anforderungen an die Informationssicherheit für kritische Infrastrukturen im Energiesektor gestellt werden, entsteht unmittelbarer Handlungsbedarf für alle Verbünde von Energieanlagen ab einer Nennleistung von 420 MW [Bsi16]. Allerdings ist eine Ausweitung des Gültigkeitsbereichs auf kleinere Energieverbünde perspektivisch abzusehen.

1.1 Virtuelle Kraftwerke

Eine zentrale Rolle bei der Koordination verteilter Energieanlagen spielen die sogenannten virtuellen Kraftwerke. Ein virtuelles Kraftwerk ist eine Softwarelösung zur Überwachung und Übersicht der angeschlossenen Stromerzeuger im Sinne einer lokalen Leitwarte. Ein weiterer Kernaspekt ist zumeist die Bündelung der erzeugten Leistung der verteilten Stromerzeuger zum gemeinsamen Vertrieb eines gemeinsamen Produkts auf den Strommärkten [PRS08].

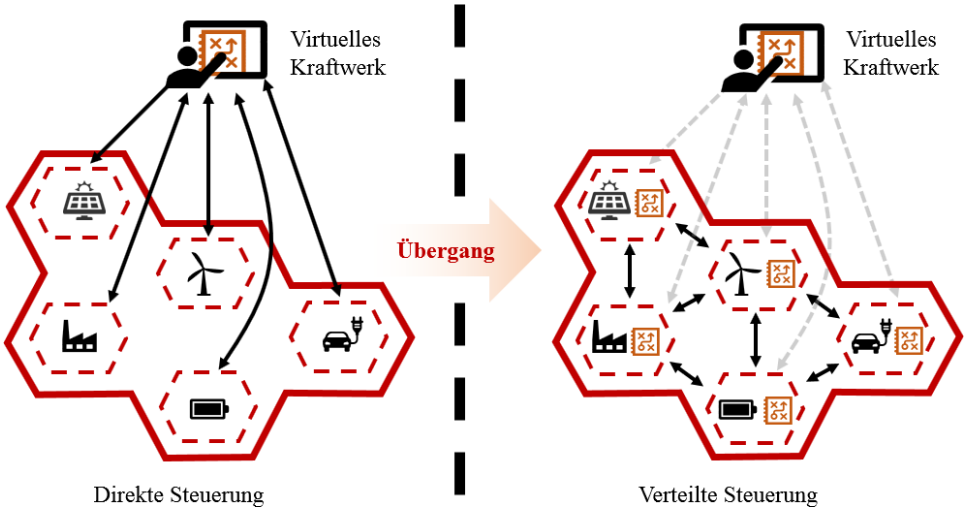

Abbildung 1 - Virtuelles Kraftwerk im Wandel

Virtuelle Kraftwerke bestehen aus einem Leitsystem und unterschiedlichen energieerzeugenden Anlagen und Stromspeichern. Dezentrale Stromerzeugungsanlagen, senden ihre Messdaten an ein Leitsystem. Von diesem Leitsystem aus werden, entsprechend dem klassischen „Industrie 4.0"-Modell (vgl. Abbildung 1, links), steuernde Daten an eine Anlage versendet. Bislang waren produzierende Anlagen abgeschlossene Systeme, ihre Steuerung und Überwachung fand in räumlicher Nähe statt. Durch die Einrichtung von Leitsystemen mit einer Anbindung an das Internet entstehen neue Herausforderungen für die Informationssicherheit.

Organisatorische Zersplitterung: Die Anbindung vieler kleiner Anlagen, die unterschiedlichen Zuständigkeiten unterliegen und nicht zentral verwaltet werden. Das Identitäts- und Vertrauensmanagement wird komplexer, weil jede Anlage über Organisationsgrenzen hinweg kryptographisch verifiziert werden muss.

Verlagerung OT nach IT: Die Einführung zusätzlicher IT-Geräte bei der Anlagensteuerung, die Aufgaben aus der Echtzeitsteuerung übernehmen.

Sichere Anbindung ans Internet: Kontrollmöglichkeiten durch eine Leitwarte und Datenaustausch zwischen verteilten Anlagen erhöhen die Angriffsoberfläche. Wenn Fahrpläne aufgrund von Echtzeitinformationen dynamisiert werden, müssen die gesteuerten Anlagen erreichbar sein und eine latenzfreie Anbindung gewährleistet werden.

Rechtliche Vorgaben: Die Anbindung vieler kleiner Anlagen erfordert Rechtssicherheit bezüglich der technischen Voraussetzung und der Verantwortlichkeiten bei Fehlern und Störungen.

Unabhängig von der Art der Übertragung und dem eingesetzten Medium der Übermittlung liegt genau hier eine hohe Anfälligkeit für unerwünschte Eingriffe oder Zugriffe durch unberechtigte Dritte. Die direkte Manipulation der Anlage, das Nutzen des Übertragungsweges von der Anlage, das Nutzen des Übertragungsweges von der Anlage zur Leitstelle zu Spionagezwecken oder der Außerkraftsetzung des Leitsystems können das nationale Stromnetz beeinflussen und die Versorgungssicherheit beeinträchtigen.

1.2 Dezentralisierung und Autonomie verteilter Energieanlagen

Businesslogik und Entscheidungen auf Basis von Messwerten und Optimierungszielen verlagern sich weg von der zentralen Leitwarte hin zu einer dezentralen Entscheidung in der einzelnen Energieanlage (vgl. Abbildung 1). Diese Dezentralisierung macht es allerdings schwieriger, Systemdienstleistungen zu erbringen, die eine globale Sicht auf den Netzzustand erfordern. Hier wird es notwendig sein, Aggregatoren zu etablieren, die zumindest für Teilnetze ermöglichen, z.B. Plausibilitätsprüfungen und Anomalieerkennung durchzuführen, einerseits, und andererseits teilzentrale Systemdienstleistungen zu erbringen.

Der Trend geht zur Anbindung von Anlagen an TCP/IP-basierte Fernwirkprotokolle und einer Anbindung an das Internet-of-Energy. Die Verlagerung von Businesslogik in die Anlagen führt zu einer stärkeren Abhängigkeit von der grundsätzlichen Erreichbarkeit aus dem Internet zwischen den einzelnen Anlagen. Daraus resultiert mit jeder erreichbaren Schnittstelle eine potentiell vergrößerte Angriffsoberfläche. Unterschieden wird hier zwischen operativer Technologie (OT) und Informations-Technologie (IT), die wie in Abbildung 2 dargestellt zusammenspielen. Die Unterscheidung zwischen OT und IT ist traditionell gewachsen, verliert aber durch die Anbindung von Anlagen über Kommunikationsverbindungen mit niedrigen Latenzen, immer mehr an Bedeutung. Die Übertragung von Messwerten und Steuersignalen zwischen der Energieanlage und deren Leitwarte findet dabei zunehmend über Internetkommunikation statt. Insbesondere Kleinstanlagen, wie etwa ein einzelnes Windrad im Besitz einer Dorfgemeinschaft, werden oft direkt vom Besitzer verwaltet, während die Steuerung an externe Dienstleister bzw. Energieunternehmen weitergegeben wird. Das bedeutet eine Vermischung von OT und IT bzw. eine Transformation der eigentlichen IT-Aufgaben hin in den Aufgabenbereich von OT.

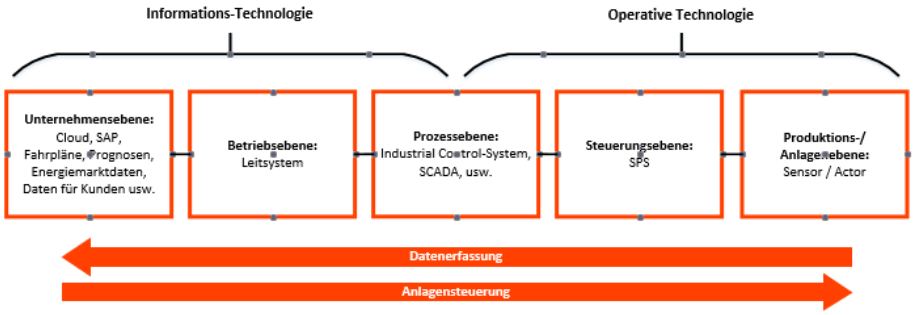

Abbildung 2 - Anwendungsbereiche von IT- und OT-Systemen

2 Sicherheitsanforderungen

Bei der Entwicklung zeitgemäßer Sicherheitsstandards beschränkt sich die staatliche Unterstützung zunehmend auf eine Lenkungsfunktion, ohne gesetzliche Vorschriften zu erlassen. Diese Strategie ermöglicht den beteiligten Betreiberfirmen die Umsetzung innovativer Sicherheitskonzepte, die in manchen Fällen die Neuorganisation ganzer wirtschaftlicher Bereiche zur Folge hat, wofür ein ausreichender Zeitrahmen die Voraussetzung ist. Ein Nachteil dieser Vorgehensweise kann die „organisatorische Zersplitterung“ sein, wenn Informationen und Vorgehensweisen nicht ausgetauscht, abgeglichen und optimiert gebündelt werden. Diese kann durch Abgrenzungen verstärkt werden, um zum Beispiel wirtschaftliche Ziele einer Organisation nicht zu gefährden. Es

besteht auch die Gefahr, dass Aspekte der IT-Sicherheit und der Informationssicherheit vernachlässigt und den wirtschaftlichen Interessen untergeordnet werden.

Die vom BSI und von der ISO definierten Anforderungen [Bsi19, Iso13] sind zu unspezifisch für den Energiesektor, um daraus konkrete Maßnahmen ableiten zu können. Deshalb ist es für einzelne Unternehmen empfehlenswert, sich explizit mit den eigenen branchenspezifischen Rahmenbedingungen auseinander zu setzen und aus den generischen Vorgaben und daran angelehnte Branchenstandards wie etwa relevante BDEW Whitepaper [Bdew08, Bdew18] eine maßgeschneiderte Sicherheitsrichtlinie zu erstellen.

2.1 Sicherheitsanforderungen an intelligente Stromnetze

Anlagen in virtuellen Kraftwerken werden häufig von kleinen und mittleren Stadtwerken, kommunalen Unternehmen oder Unternehmen ohne Energie-Schwerpunkt (z.B. Wohnungsbaugesellschaften) betrieben. Diese können meist keine Spezialisten für die IKT-Sicherheit vorhalten und sind in vielen Fällen von externen Beratern abhängig. So wurden beispielweise generische Anforderungskataloge erarbeitet, die beim Einkauf von Fremdsystemen angewendet werden können [Bdew08]. Die sichere Einrichtung und der Betrieb der Anlagen erfordern allerdings spezifische Fachkenntnisse.

Typischerweise vergrößern die Betreiber von virtuellen Kraftwerken ihren Verbund schrittweise. In frühen Stadien ist ein strukturiertes Sicherheitsmanagement unwirtschaftlich und kaum umsetzbar. Für größere Verbünde ist es unerlässlich. Der Betrieb der übergeordneten Leitsysteme erfordert einen strukturierten Prozess, um auf Fehler, Sicherheitslücken oder Angriffe schnell zu reagieren.

Die aktuelle Forschung im Bereich virtueller Kraftwerke hat bereits zahlreiche Untersuchungen verteilter Steuerungsalgorithmen hervorgebracht, die sich mit Sicherheitsaspekten beschäftigen. Die dabei zugrunde gelegten Schutzziele beschränken sich gemeinhin auf die Kommunikationsverbindung zwischen grundsätzlich vertrauenswürdigen Kommunikationspartnern, beschreiben also Anforderungen an Authentisierung, Autorisation, Echtzeitanforderungen oder noch spezifischere Robustheitseigenschaften. Im Bereich der IT-Sicherheit sind allgemein die drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit [Bek14, KPP14] üblich. Im Bereich der Integrität ist das Unter-Schutzziel der Nachweisbarkeit hervorzuheben, da besonders im Energiesektor die nachträgliche Nachvollziehbarkeit von Problemen und die feste Verankerung von Verantwortlichkeiten von grundlegender Bedeutung ist. Als übergeordnetes Schutzziel steht die Versorgungssicherheit, das heißt eine stabile und unterbrechungsfreie Stromversorgung zu gewährleisten.

2.2 Security by Design

Sicherheit sollte ein fester Teil von Softwareentwicklung und IKT-Konzeption sein und von Planungsbeginn an berücksichtigt werden. Ein solches Vorgehen wird durch das Befolgen von Designprinzipien, z.B. von BSI und OWASP [Bsi06, Owa16], gefördert und nennt sich "Security by Design". In Tabelle 1 sind Prinzipien aufgeführt, für die in diesem Dokument konkrete Umsetzungsschritte beschrieben werden.

Tabelle 1: „Security-by-Design" Prinzipien

BSI	OWASP	Beschreibung
Economy of mechanism	Keep security simple	Der Funktionsumfang der Anwendung soll so einfach wie möglich gehalten werden. Bevorzugt sind Whitelist-Verfahren und Standards zu nutzen.
Complete mediation	Principle of defense in depth	Objektzugriffe sollten auf mehreren unabhängigen Ebenen geprüft werden.
Segregation of duties	Separation of duties	Besonders sicherheitsrelevante Aktionen sollten nur von mehreren Personen/Rollen gemeinsam durchführbar sein und Administratoren sollten nicht die Rechte eines regulären Nutzers erhalten
Least privilege	Principle of least privilege	Anwender und Systemkomponenten sollten nur die absolut notwendigen Rechte und Ressourcen für die Erledigung ihrer Aufgaben erhalten.
Least common mechanism		Es sollten bevorzugt lokale Ressourcen verwendet werden. Der Austausch mit anderen Akteuren sollte minimiert und reglementiert werden.
Psychological acceptability		Sicherheitsmechanismen dürfen die Bedienbarkeit nicht zu sehr einschränken und sollten den Anwendern verständlich gemacht werden.
Compromise recording		Eine Protokollierung ist unerlässlich, um Angriffe erkennen oder nachvollziehen zu können.
	Establish secure defaults	Das System sollte sichere Standardwerte nutzen, auch wenn diese für den Anwender „unbequem" sind. Änderungen sollten bewusst durchgeführt werden.
	Fail securely	Algorithmen sollten bei auftretenden Fehlern einen sicheren und definierten Zustand erzeugen.
	Don't trust services	Externe Dienste sind nicht vertrauenswürdig. Sämtliche eingehenden Daten sollten geprüft werden.

2.3 Mehrseitige Sicherheit

Am intelligenten Stromnetz nehmen verschiedene Akteure mit unterschiedlichen Schutzinteressen teil. Daher werden mehrseitige Anforderungen an die Sicherheit gestellt. Diese Anforderungen können zueinander im Konflikt stehen [Fed99]. Das Zusammenwirken verschiedenartiger Systeme kann ebenfalls unterschiedliche potentiell konfliktbehaftete Sicherheitsanforderungen nach sich ziehen. So ist beispielsweise die Verfügbarkeit von Teilnehmern im Stromnetz von der Verfügbarkeit von Teilnehmern im Kommunikationsnetz getrennt zu betrachten. Die Versorgungssicherheit sollte auch dann gegeben sein, wenn die Kommunikation der Teilnehmer eingeschränkt ist. Bei physischer Aufteilung des Stromnetzes in Teilnetze hingegen können die Teilnetze ggf. noch miteinander kommunizieren und eine gemeinsame Strategie für optimalen Inselbetrieb entwerfen.

3 Sicherheitsschichtenmodell verteilter Systeme

Eine Schwäche traditioneller Sicherheitskonzepte ergibt sich aus ihrer binären Unterscheidung zwischen vertrauenswürdigen und nicht-vertrauten Kommunikationspartnern. In einer zukünftigen agilen Umgebung, die in intelligenten Stromnetzen immer stärker Einzug halten, verwischt diese Grenze. Umso mehr wird die Bewertung von Kommunikationspartnern anhand ihres Verhaltens, d.h. legitim versus bösartig oder fehlerhaft, relevant, was sich allerdings schlecht im Vornherein feststellen lässt. Die Zugehörigkeit von Energieanlagen zu einem oder mehreren virtuellen Kraftwerken kann über Marktplattformen oder andere Steuerungsmechanismen dynamisch wechseln.

Abbildung 3 zeigt, wie die verschiedenen Ebenen der Sicherheitsbetrachtung zusammenspielen. In diesem Kontext bietet die Einbeziehung einer kollaborativen Sicherheitsebene bei der Bewertung von Sicherheitsanforderungen eine zusätzliche Orientierung [Stü18]. Komponenten können in Falle eines virtuellen Kraftwerks IoT-Geräte, Dienste eines Leitsystems, Clients usw. sein.

3.1 Komponenten- und Kommunikationssicherheit im Zonenmodell

An dieser Stelle werden die Schichten „Gegenseitige Authentisierung“ und „Korrekt arbeitende Komponenten“ aus Abbildung 3 näher erläutert. Als Grundlage dient ein VK mit direkter Steuerung (siehe Abbildung 1). Abbildung 4 zeigt eine mögliche Anbindung einer Energieanlage an IKT-Systeme, die unterschiedlichen Verantwortlichkeiten unterliegen und somit eine deutlich größere Angriffsoberfläche bieten als technisch notwendig.

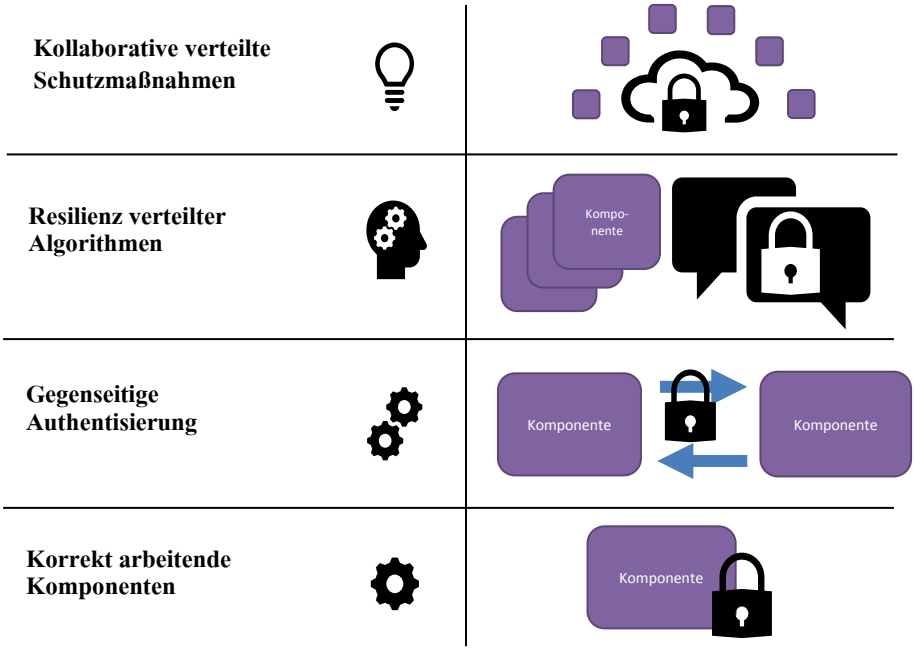

Abbildung 3 - Ebenen verschiedener Sicherheitskonzepte

Im Folgenden wird ein hierarchisches Sicherheitsmodell beschrieben, das ähnliche Grundzüge wie das formalisierte Modell von Biba [Bib75] trägt. Dieses gewährleistet die Integrität der verarbeiteten Daten und ist mit „read up, write down“ die Umkehr des Vorgängermodells Bell-LaPadula („read down, write up“) [LCM84], welches primär Vertraulichkeit gewährleistet. Beide Modelle zeichnen sich jedoch dadurch aus, dass Datenflüsse entgegen der Hauptrichtung praktisch nicht realisierbar sind.

Ein möglicher Ausweg wird von Clark-Wilson [CW87] vorgeschlagen. Ein System verarbeitet darin nur Daten, die sich in einem nachgewiesen gültigen Zustand befinden. Für externe Daten existieren jedoch Mechanismen, um sie zu verifizieren. Zustandsänderungen werden jeweils über eine unabhängige Transaktionskontrolle abgesichert (*Separation of duties*).

Ein Leitsystem sollte über mehrere Sicherheitszonen mit unterschiedlichen Vertrauensebenen hinweg betrieben werden (siehe Abbildung 6). Dadurch werden zusammengehörige Komponenten gruppiert und weitgehend von anderen Bereichen getrennt. Unbeabsichtigte oder vorsätzliche Fehlfunktionen können sich nicht

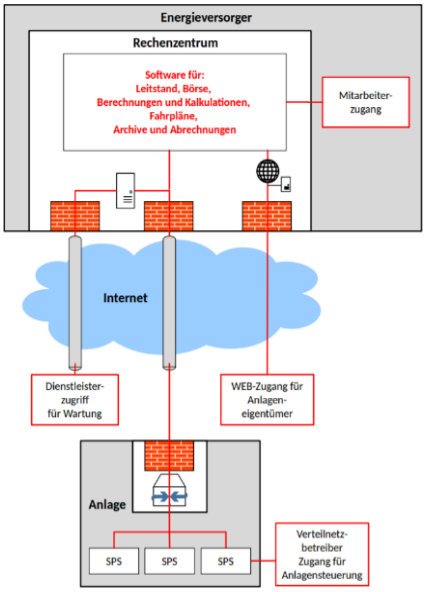

Abbildung 4 – Anbindung einer Energieanlage in die IKT-Infrastruktur

unkontrolliert ausbreiten (*Fail securely*). Um Fehler und Angriffe nachvollziehen zu können, sollten entsprechende Ereignisse protokolliert werden *(Compromise recording*).

Datenflüsse zwischen Sicherheitszonen finden dabei nur in einem vorher festgelegten Rahmen statt. Es sollte stets gewährleistet werden, dass der Kommunikationspartner bekannt ist. Dies gilt besonders bei der Verwendung verteilter Algorithmen, da Steuerbefehle nicht zwangsläufig nur von einem zentralen Leitsystem initiiert werden. Dies lässt sich über geeignete kryptographische Verfahren, wie digitale Signatursysteme und Public-Key-Infrastruktur realisieren. Die Komplexität der ausgetauschten Daten sollte so gering wie möglich gehalten werden, damit fehlerhafte oder manipulierte Daten effizient erkannt und zurückgewiesen werden können (*Keep security simple*, *Least common mechanism, Don't trust services*).

Die Zugriffsberechtigungen zwischen den Zonen sollten dabei vorrangig von Zonen höherer Sicherheit auf Zonen geringerer Sicherheit modelliert sein. Verbindungen in Gegenrichtung sollten nur genutzt werden, wenn dies für das Erreichen einer akzeptablen Nutzbarkeit unvermeidbar ist. Diese Datenströme sollten klar definiert und automatisch prüfbar sein. Beispielsweise muss es Anwendern möglich sein, Aktionen durchzuführen, die zu ihrem Aufgabenbereich gehören. Dabei darf es keine Rolle spielen, ob der Anwender sich in einer Zone befindet, die weniger sicher ist. Hier ist eine Lösung zu nutzen, die die Arbeit ermöglicht, ohne die Sicherheit des Gesamtsystems über Gebühr zu gefährden (*Psychological acceptability*).

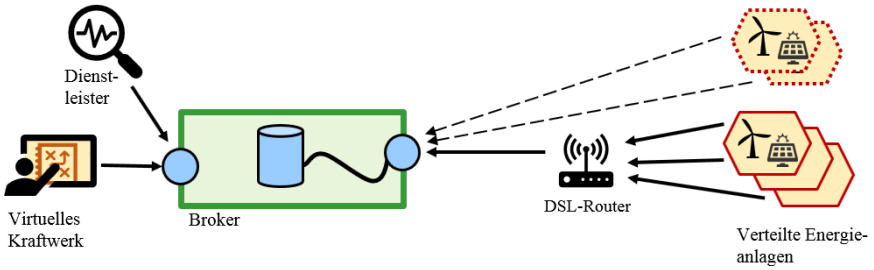

Abbildung 5: Broker zwischen Leitsystem und Anlage

Gleiches gilt für den Verbindungsaufbau als sicherheitskritischem Akt. Für Anlagen in Zonen mit höherer Sicherheitsstufe sollte das Prinzip eines Brokers eingesetzt werden, um direkte Kommunikationsverbindungen von Außen zu vermeiden. Broker werden über eine ausgehende Internetverbindung kontaktiert, so dass die Energieanlage selbst keine eingehenden Verbindungen anzunehmen braucht. Wird die verwendete Firewalllösung entsprechend konfiguriert, kann so die Angriffsoberfläche der einzelnen Anlage deutlich reduziert werden. Dieses Vorgehen ist in Abbildung 5 dargestellt.

Bei der Anbindung von Anlagen wird empfohlen, eine vom ISP bereitgestellte Verbindung mit Multiprotocol Label Switching (MPLS) zu verwenden, so dass öffentlicher IP-Adressen vermieden werden. Zudem sollten alle genutzten Verbindungen zumindest über ein VPN oder über TLS abgesichert sein. Auf diese Weise wird die verbleibende Angriffsoberfläche aus dem Internet minimiert.

Das hier vorgestellte Sicherheitszonenmodell (vgl. Abbildung 66) besitzt somit keine angreifbaren Dienste, die direkt über eine Internetverbindung erreichbar sind. Jedoch werden in der Realität Kompromisse vonnöten sein, um die Benutzbarkeit und Akzeptanz des Systems zu gewährleisten. Ein Beispiel hierzu ist der Zugriff durch Kunden auf die Webschnittstelle, um Wartungsintervalle einzutragen. Eine verpflichtende VPN-Verbindung erhöht die Sicherheit zu Lasten des Bedienkomforts (*Psychological acceptability*).

3.2 Resilienz verteilter Algorithmen

In verteilten Systemen ist das Auftreten fehlerhafter oder böswilliger Prozesse kaum noch zu vermeiden. Verteilte Algorithmen sind zentrale Angriffsziele von Angreifern, die als valide Teilnehmer im Netzwerk auftreten. Es gibt zwei verschiedene Arten von potentiellen Angriffen [Fu17]:

1. Das Ändern oder Hinzufügen von Informationen, auch False-Data-Injection genannt.
2. Das Blockieren von Kommunikationswegen oder Diensten, auch Denial-of-Service genannt.

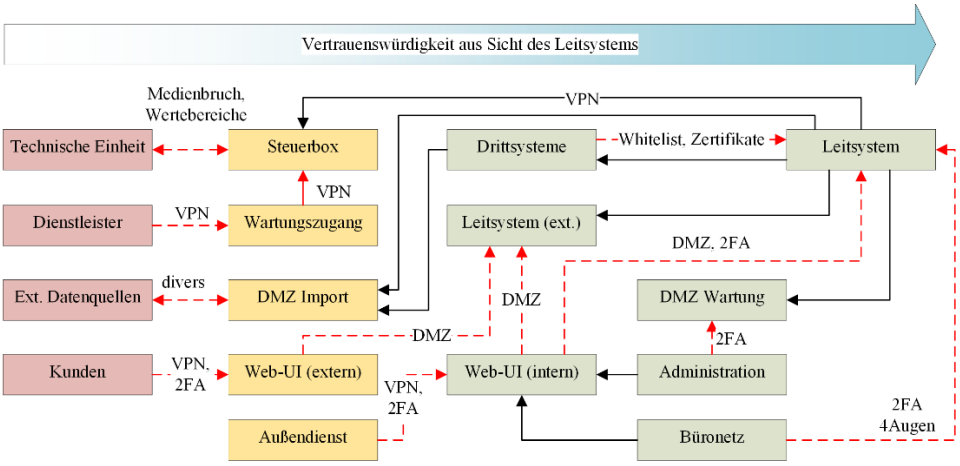

Abbildung 6 - Sicherheitszonen aus Sicht des Leitsystems

Dabei ist die Intention des Angreifers unerheblich, d.h. ob die schädlichen Aktivitäten böswillig, fahrlässig oder irrtümlich durchgeführt werden. So können authentifizierte Teilnehmer z.B. durch defekte Sensoren, die fehlerhafte Messwerte liefern, das durch den verteilten Algorithmus errechnete gemeinsame Ergebnis verfälschen. Maßnahmen dieser Sicherheitsschicht limitieren die Auswirkungen von Ausfall oder Fehlverhalten einzelner Komponenten, etwa durch Plausibilitätsprüfungen von Messwerten oder durch Bildung von Erwartungswerten *(Don't trust services, Fail securely, Establish secure defaults).*

3.3 Kollaborative Schutzmechanismen

Auf dieser Ebene sind diejenigen Herausforderungen einzuordnen, die a) sich auf heterogene Systeme mit Anlagen beziehen, die sich in Rechenkapazität, Speicher-vermögen oder anderen Dimensionen unterscheiden, b) ermöglichen, dass Energieanlagen sich dynamisch anmelden oder abmelden, c) unterschiedliche Qualität der verfügbaren (Sensor-)Daten berücksichtigen, d) sich auf entsprechende Werkzeuge für Authentisierung und Zuordenbarkeit von Aktionen beziehen, als auch e) die auf Vertrauensmanagement und verteilte Sicherheitsmanagementkonzepte beziehen. Die Ebene der kollaborativen Sicherheit muss dabei Daten aus unterschiedlichen Quellen zusammenführen und enthält optimalerweise Echtzeit-Maßnahmen wie Plausibilitäts-prüfungen, Vertrauensmanagement, Topologiemaßnahmen und Angriffserkennung.

Auf dieser Ebene werden Denial-of-Serivce-Angriffe und False-Data-Injection-Angriffe erkannt, um daraufhin geeignete Gegenmaßnahmen wie etwa auch Minderung von Vertrauen bei der Berechnung gemeinsamer Mittelwerte einzusetzen oder auch

Anpassungen der Kontrollstruktur und Kommunikationstopologie vorzunehmen, etwa um Knotenpunkte zu entlasten oder Teilnehmer mit geringer Vertrauenswürdigkeit an den Rand der Topologie zu verschieben oder ganz aus dem System auszuschließen [Stü18].

4 Bedrohungsszenario und Sicherheitsbetrachtung

Sowohl im VK mit zentralem Leitsystem als auch bei verteilten Systemen sollte die Anlage die Authentizität und Integrität der Steuerungsbefehle überprüfen können. So soll verhindert werden, dass potentielle Angreifer Befehle manipulieren können oder fehlerhafte Befehle ungeprüft umgesetzt werden.

Hierfür muss der Befehl bei Initialisierung vom berechtigten Benutzer signiert werden. Die Rollen bzw. die Rechte und der öffentliche Schlüssel eines Benutzers werden ihm von einer als vertrauenswürdig angesehenen CA bestätigt. Das Leitsystem kann daher die Identität und somit auch die Rechte bzw. Rollen prüfen (*Principle of defense in depth, Principle of least privilege, Segregation of duties*).

Eine vorgeschaltete Komponente („Verifikator“) soll gültige Nachrichten erkennen und den enthaltenen Steuerbefehl an den eigentlichen Protokollumsetzer weiterreichen. Die Gültigkeit der Nachricht soll allein auf Grund der angefügten Sicherheitsinformationen (Signatur und Zertifikat) auf Gültigkeit überprüft werden können. Die Nachricht enthält alle Informationen, die die Anlage benötigt, um die Nachricht ohne zusätzliche Informationen von Außen zu verifizieren. Einzig das Root-Zertifikat der CA muss vorab

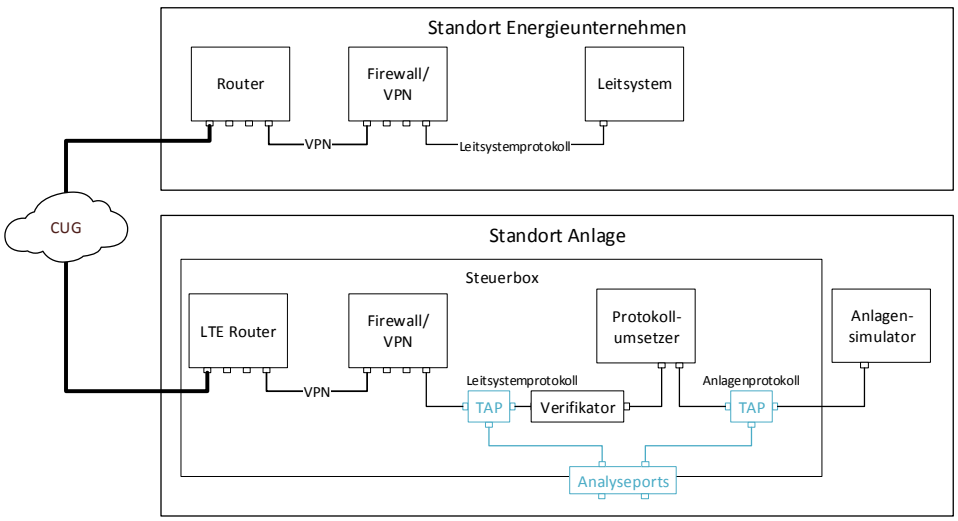

Abbildung 7 - Aufbau der Gesamtstrecke zwischen Leitsystem und simulierter Anlage

in der Anlage bekannt sein. Nachrichten, die einen Fehler in der Verifikation nach sich ziehen, müssen verworfen, und ein Logeintrag mit der jeweiligen Aktion muss generiert werden.

Implementation

Das gewählte Szenario ist die Übertragung eines Sollwertes an den Protokollumsetzer, der den Befehl in das native Protokoll der Anlage übersetzt (vgl. Abbildung 7). Die erste prototypische Umsetzung des Konzeptes sieht die isolierte Verifizierung einzelner Nachrichten auf Seite der Anlage vor. Es wird insbesondere geprüft, ob das Konzept anlagenseitig praxistauglich ist. Dazu werden Laufzeitinformationen in Abhängigkeit von verschiedenen kryptografischen Verfahren und der zusätzlichen Verifikation gemessen.

simulierter Anlage. Die Standorte sind über CUG und ein eigenes VPN sicher verbunden. Die Steuerbox ist ein abschließbarer Schaltschrank, der vom Leitsystembetreiber vorgegeben wird. Sie ist als vermittelnde Instanz zwischen die Endpunkte geschaltet und dient als wesentliches Sicherheitselement auf der Anlagenseite. Für belastbare Untersuchungen des Laufzeitverhaltens sind „Test Access Points“ (TAP) in die Signalwege integriert, die eine genaue Überwachung der Datenpakete erlauben.

5 Zusammenfassung

Die IKT-Sicherheitsanforderungen an die Absicherung von Energieanlagen befinden sich im Wandel. Eine besondere Herausforderung stellt dabei die Dezentralisierung und Digitalisierung der Steuersysteme dar, für die eine unterbrechungsfreie Anbindung an Kommunikationssysteme immer wichtiger wird. Auf Basis von Sicherheitsschichten und unter Betrachtung einer Systematik von Sicherheitszonen wird in dieser Arbeit eine Methodik vorgestellt, die die zukünftige Entwicklung bezüglich der erwarteten Dezentralisierung der Energieerzeugung miteinbezieht. Die untersuchten Sicherheitsaspekte und die abgeleiteten Umsetzungsmaßnahmen bieten wirksame Bausteine zur Skalierung eines Informationssicherheits-Managements für wachsende Energieanlagenverbünde.

Literaturverzeichnis

[Ba14] Bani-Ahmed, Abedalsalam; Weber, Luke; Nasiri, Adel; Hosseini, Hossein: Microgrid communications: State of the art and future trends. In: Renewable Energy Research and Application (ICRERA), 2014 International Conference on. IEEE, S. 780–785, 2014.

[Bdew08] Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW): Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme, 2008, Überarbeitet 2018, online: https://www.bdew.de/service/anwendungshilfen/whitepaper-anforderungen-sichere-steuerungs-telekommunikationssysteme/

[Bdew18] BDEW. „Branchenspezifischer Sicherheitsstandard für die Verteilung von Fernwärme (B3S VvFw)“ Abgerufen am 5. April 2019 unter: https://www.bdew.de/media/documents/Awh_20180503_B3S-Verteilung-Fernwaerme.pdf

[Bek14] Chakib Bekara. “Security Issues and Challenges for the IoTbased Smart Grid”. In: Procedia Computer Science 34 (2014).

[Bib75] Biba, K. J. “Integrity Considerations for Secure Computer Systems”, MTR-3153, The Mitre Corporation, (1975).

[Bsi06] BSI. „BSI-Leitfäden zur Entwicklung sicherer Webanwendungen“ (2013) Abgerufen am 5. April 2019 unter https://www.bsi.bund.de/DE/Publikationen/Studien/Webanwendungen/index_htm.html

[Bsi16] BSI-KritisV (2016), Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV).

[Bsi19] Bundesamt für Sicherheit in der Informationstechnik. „IT-Grundschutz Kompendium“. Reguvis (2019).

[CW87] David D. Clark, David R. Wilson: „A Comparison of Commercial and Military Computer Security Policies“. IEEE Symposium on Security and Privacy (1987).

[De07] Deconinck, Geert; Rigole, Tom; Beitollahi, Hakem; Duan, Rui; Nauwelaers, Bart;Van Lil, Emmanuel; Driesen, Johan; Belmans, Ronnie; Dondossola, Giovanna: Robustoverlay networks for microgrid control systems. In: Proc. Workshop on Architecting Dependable Systems (WADS 2007), co-located with 37th Ann. IEEE/IFIP Int. Conf.on Dependable Systems and Networks (DSN 2007), Edinburgh, Scotland (UK). S.148–153, 2007.

[Fed99] Hannes Federrath. Sicherheit mobiler Kommunikation: Schutz in GSM-Netzen, Mobilitätsma-nagement und mehrseitige Sicherheit. DuD Fachbeiträge, Vieweg, Wiesbaden (1999).

[Fu17] Fu, Rong; Huang, Xiaojuan; Sun, Jun; Zhou, Zhenkai; Chen, Decheng; Wu, Yingjun:Stability analysis of the cyber physical microgrid system under the intermittent DoSattacks. Energies, 10(5):680, 2017.

[HM17] Hossain-McKenzie, Shamina Shahrin: Protecting the power grid: strategies againstdistributed controller compromise. Dissertation, University of Illinois at Urbana-Champaign, 2017.

[Iso13] ISO. „ISO/IEC TR 27019: Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry“. (2013)

[KPP14] Nikos Komninos, Eleni Philippou, and Andreas Pitsillides. “Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures”. In: IEEE Communications Surveys & Tutorials 16.4 (2014).

[LCM84] Landwehr, Carl E., Constance L. Heitmeyer, and John McLean. A Security Model for Military Message Systems. No. NRL-8806. NAVAL RESEARCH LAB WASHINGTON DC, 1984.

[MMIK17] Monteiro, Kate; Marot, Michel; Ibn-Khedher, Hatem: Review on microgrid commu-nications solutions: a named data networking–fog approach. In: Ad Hoc Networking Workshop (Med-Hoc-Net), 2017 16th Annual Mediterranean. IEEE, S. 1–8, 2017.

[MMNQ13] Macana, Carlos Andrés; Mojica-Nava, Eduardo; Quijano, Nicanor: Time-delay effect onload frequency control for microgrids. In: Networking, Sensing and Control (ICNSC),2013 10th IEEE International Conference on. IEEE, S. 544–549, 2013.

[Owa16] OWASP. „Security by Design Principles“ (2016) Abgerufen am 5. April 2019 unter https://www.owasp.org/index.php/Security_by_Design_Principles

[PRS08] D. Pudjianto, C. Ramsay und G. Strbac. “Microgrids and virtual power plants: Concepts to support the integration of distributed energy resources”. In: Proceedings of the Institution of Mechanical Engineers, Part A: Journal of Power and Energy 222.7 (2008), S. 731–741. DOI: 10.1243/09576509JPE556.

[Stü18] Marius Stübs. “Towards Emergent Security in Low-Latency Smart Grids with Distributed Control”. In: Proceedings of the 2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (Smart-GridComm 2018).

[SYA14] Sargolzaei, Arman; Yen, Kang; Abdelghani, Mohamed N: Delayed inputs attack on loadfrequency control in smart grid. In: ISGT 2014. IEEE, S. 1–5, 2014.

[WG18] Weidenhammer, Detlef, and Rocco Gundlach. „Wer kennt den ‚Stand der Technik‘?“ Datenschutz und Datensicherheit-DuD 42.2 (2018): 106-110.