Übersicht

Dennis Rösch*, André Kummerow, Stephan Ruhe, Kevin Schäfer, Cristian Monsalve und Steffen Nicolai

IT-Sicherheit in digitalen Stationen: Cyber-physische Systemmodellierung, -bewertung und -analyse

Cybersecurity in digital substations: Cyber-physical system modelling, assessment and analysis

https://doi.org/10.1515/auto-2020-0077
Empfangen 30. April 2020; angenommen 7. Juli 2020

Zusammenfassung: Die Digitalisierung der Stationsautomatisierung eröffnet neue Anwendungspotentiale für intelligente Stationsfunktionen in elektrischen Energiesystemen. Die Vernetzung und der Einsatz von IEC 61850 als vereinheitlichter Kommunikationsstandard ist eine wichtige Voraussetzung, erhöhen aber gleichzeitig die Anfälligkeit für IT-Angriffe. Zur Untersuchung der IT-Sicherheit digitaler Stationen wird hierfür eine neu konzipierte cyberphysische Echtzeit-Co-Simulationsplattform vorgestellt. Auf Basis einer Referenzarchitektur eines IP-basierten Umspannwerks wird die Modellierung, Bewertung und Analyse digitaler Stationen für gestörte und ungestörte Betriebsfälle sowie unter Beachtung von IT-Angriffen ermöglicht. Daraufhin werden Ansätze zur Resilienzbewertung sowie Maßnahmen zur IT-Sicherheit für den operativen Betrieb, z. B. die Erkennung cyber-physischer Anomalien, aufgezeigt.

Schlagwörter: Digitale Station, Co-Simulation, IT-Sicherheit, Resilienz, Anomalieerkennung, Cyberphysische Systeme

***Korrespondenzautor: Dennis Rösch,** Fraunhofer IOSB, IOSB-AST Ilmenau, Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung, Abteilung Energiesysteme, Am Vogelherd 90, 98693 Ilmenau, Deutschland, E-Mail: dennis.roesch@iosb-ast.fraunhofer.de
André Kummerow, Stephan Ruhe, Kevin Schäfer, Cristian Monsalve, Steffen Nicolai, Fraunhofer IOSB, IOSB-AST Ilmenau, Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung, Abteilung Energiesysteme, Am Vogelherd 90, 98693 Ilmenau, Deutschland, E-Mails: andre.kummerow@iosb-ast.fraunhofer.de, stephan.ruhe@iosb-ast.fraunhofer.de, kevin.schaefer@iosb-ast.fraunhofer.de, cristian.monsalve@iosb-ast.fraunhofer.de, steffen.nicolai@iosb-ast.fraunhofer.de

Abstract: The increasing digitalization within station automation enables new applications for intelligent functionalities in substations of electrical power systems. For this, the utilization of IEC 61850 as unified communication standard is a key requirement but also changes the vulnerability for cyber-attacks. For cyber-security investigations of digital substations a cyber-physical real-time co-simulation platform is introduced. A reference architecture of an IP-based substation is presented and enables the modelling, assessment and analysis of digital substation within disturbed and undisturbed grid situations as well as under consideration of cyber-attacks. Based on this, novel approaches and methods for resilience assessment of digital substations and cyber-security measures for operations, e. g. the detection of cyber-physical anomalies, are described and discussed.

Keywords: digital substation, co-simulation, cyber-security, resilience, anomaly-detection, cyberphysical-systems

1 Einleitung

1.1 IT-Sicherheit in der Energieversorgung

Die Energieversorgung mit ihrer weitreichenden gesellschaftlichen und volkswirtschaftlichen Bedeutung steht im Allgemeinen als kritische Infrastruktur im besonderen Fokus möglicher IT-Angriffe. Nach [1] sind dabei unterschiedliche Entwicklungen in der Informations- und Kommunikationstechnik (IKT) wie die Steigerung des Vernetzungsgrades, die erhöhte IT- Durchdringung sowie das Verschwinden von Netzgrenzen zu verzeichnen. Die weitreichende Digitalisierung von zentralen und dezentralen Prozessen führt dazu, dass die Funktionsfähigkeit der Versorgung maßgeblich daran gebunden ist, dass die umliegende IT-Infrastruktur funktionsfähig bleibt und aus-

getauschte Informationen sowohl Störungs- als auch Manipulationsfreiheit aufweisen. Infolge der tieferen Durchdringung und Vernetzung von IT- und OT-Systemen (Operational Technology) geht die Abschottung prozessnaher OT-Geräte von unternehmensweiten IT-Geräten verloren und erfordert eine ganzheitliche Betrachtung beider Domänen. Dabei wird unter OT diejenige Hardware und Software verstanden, welcher zur Überwachung und Kontrolle von physikalischen Prozessen benötigt wird. IT-Systeme haben demgegenüber keinen direkten Einfluss auf physikalische Prozesse. Eine Einschätzung der Kritikalität der Energieversorgung in Bezug auf IT-Angriffe hat beispielsweise das BSI aufgezeigt [2]. Generell sind für die klassischen IT-Prozesse drei Schutzziele nach dem CIA Triad (angelehnt an z. B. BSI Grundschutz-Kompendium [1]) anzuwenden. Dadurch muss sichergestellt werden, dass Daten folgende drei Eigenschaften mit absteigender Priorität aufweisen:

- Vertraulichkeit (Confidentiality),
- Integrität (Integrity) und
- Verfügbarkeit (Availability).

Im Gegensatz zu bisherigen Anforderungen für Automatisierungssysteme sind die Schutzziele auf prozessnahe OT-Systeme in genannter Priorität analog zur vorliegenden IKT-Infrastruktur anzuwenden. Durch die zunehmende Durchdringung der IT steht dabei die Vertraulichkeit von Daten im unmittelbaren Zusammenhang mit der (korrekten) Funktionsweise der OT-Systeme. Dadurch verschiebt sich der klassische Fokus einer hohen Verfügbarkeit hinzu einer stärkeren Betrachtung von Vertraulichkeit von Informationen.

Für die unterschiedlichen Schwachstellen bzw. Einfallstore und möglichen Angriffsmotivationen hat das BSI gezielt Angriffsmethoden und –mittel entlang der sogenannten Cyber-Kill-Chain beschrieben. Hierzu zählen vor allem grundlegende Angriffstypen, welche in den ersten Phasen eines IT-Angriffs eingesetzt werden (z. B. Identitätsdiebstahl, Spam oder Phishing-Schadprogramme). Diese passiven Angriffsarten dienen vorrangig dem Einstieg in IT-Systeme, indem als Einfallstor vor allem die Mitarbeiter im Unternehmen als Schwachstelle ausgenutzt werden. Ein initialer Eintritt in ein IT-System ist immer zwingend notwendig, um weitere Schritte wie beispielsweise den Zugriff auf OT-Systeme aus Sicht des Angreifers ausführen zu können. Durch das Überwinden dieser Hürde sind die prozessnahen Strukturen erreichbar und lassen sich durch unterschiedliche aktive IT-Angriffsarten gezielt und nachhaltig stören. Diese nachgelagerten und zielgerichteten Angriffe gehen unmittelbar einher mit teilweise signifikanten Schäden innerhalb des angegriffenen Systems (z. B. Versorgungsausfälle oder Verluste der Frequenz- oder Spannungsstabilität in Energiesystemen). Sehr relevante Angriffsarten insbesondere für prozessnahe IKT-Infrastrukturen oder OT-Systeme sind die sogenannten „Advanced Persistent Threats“ (APT). Hierunter werden fortgeschrittene und andauernde Bedrohungen verstanden, welche gezielt den Durchgriff von öffentlich erreichbaren IT-Systemen zu prozessrelevanten OT-Systemen ausnutzen. Hierbei handelt es sich i. d. R. um einen koordinierten mehrstufigen Angriff, der durch verschiedene Werkzeuge gestützt wird. Die Gefahrenlage durch APT-Angriffen stuft das BSI als weiter steigend ein.

1.2 Potentielle Bedrohungen und IT-Sicherheitsmaßnahmen

Die Digitalisierung und Vernetzung innerhalb elektrischer Stationen bietet zwar einerseits Vorteile aus Anwendersicht, bringt prinzipiell aber auch neue Sicherheitsrisiken mit sich. Insbesondere in Kommunikationsstandards für die Stationsautomatisierung (z. B. IEC 61850) finden IT-Sicherheitsmaßnahmen keine hinreichende Berücksichtigung [3]. Im Vergleich zu älteren Kommunikationsstandards und –infrastrukturen nach beispielsweise IEC 60870 erlaubt der auf Interoperabilität ausgelegte IEC 61850 eine Öffnung der Kommunikation zur netzwerkbasierten Umsetzung verschiedener Automatisierungs- und Monitoringfunktionen. Es werden so mehr offene Schnittstellen geschaffen, welche zwangläufig verstärkt in den Fokus der IT-Sicherheit rücken und einen erhöhten Absicherungsbedarf im Vergleich zu früheren Kommunikationsstandards nach sich ziehen. Zum Beispiel ermöglicht die im IEC 61850 eingesetzte Multicast-Verteilungstechnik einen schnellen Echtzeit-Informationsaustausch ohne großen Konfigurationsaufwand zwischen Stationskomponenten. Offene Gruppenzugehörigkeiten und Zugänge stellen jedoch signifikante IT-Sicherheitsschwachstellen dar, welche es einem Angreifer theoretisch ermöglichen, einen Zugriff auf das interne Stationsnetzwerk zu erhalten und Nachrichtenpakete zu erfassen und zu modifizieren. So könnten zum Beispiel Leistungsschalter der Schaltanlage ohne Autorisierung der Leitstelle ausgelöst werden. Des Weiteren könnten in Folge von Paketmanipulationen überhöhte Strom- und Spannungswerte an IEDs übertragen werden und dort zu unerwünschten Betriebszuständen oder Fehlfunktionen führen [4]. Bleiben diese Manipulationen auf Stationsebene unerkannt, so könnten verfälschte Spannungs- und Strommessungen auf Leitsystemebene den Systembetrieb und die Systemstabilität negativ beeinträchtigen. Der Bedarf an zusätzlicher

Tab. 1: Übersicht passiver IT-Angriffe nach [5].

IT-Angriff	Erklärung
Paket-Analyse oder Sniffing	Lesen und Analysieren von Inhalten von TCP/IP Paketen. Analyse auch hinsichtlich der Struktur und Assets im Netzwerk.
Port Scanning	Überwachung und Testen von offenen oder unsicher konfigurierten Ports von Systemen
Side-Channel Angriff	Beobachtung von Implementierungen

Tab. 2: Übersicht aktiver IT-Angriffe nach [5].

IT-Angriff	Erklärung
DoS / DDoS	Flutung des Netzwerkverkehrs (z. B. ARP-Anfragen, IPv4-Pakete) zur Herbeiführung von Kommunikationsverzögerungen oder -unterbrechungen
Man-in-the-Middle	Imitation eines legitimierten Clients oder Servers zur Einspeisung manipulierter Daten in das Netzwerk z. B. durch Änderung der Routing-Tabellen
Data Spoofing / False Data Injection	Einspeisung manipulierter Datenpakete (z. B. Messwerte, Statusinformationen, Steuerbefehle, Zeitstempel), im Speziellen auch Manipulation von GPS Signalen
Zeitverzögerungsangriffe	Herbeiführen von Zeitverzögerungen bei der Nachrichtenübertragung z. B. durch Umleitung der Nachrichtenpakete
Packet-Drops / Message Reordering	Modifizierung von Datenpaketen zur Unlesbarkeit
Malicious Code Injection	Einschleusung ausführbarer Schadprogramme oder Manipulation existierender Programmierskripte auf dem Zielsystem
Manipulierung von Konfigurationsdateien (IEC 61850 SCL)	Manipulation vorhandener Konfigurationsdaten zur Änderung des Systemkonfiguration, wie z. B. Schnittstellenbeschreibungen oder auch im Speziellen IEC 61850 SCL-Dateien

Absicherung der Kommunikation wird vom Standard IEC 62351 adressiert und in Abschnitt 3.3 näher thematisiert.

Neben den generellen Bedrohungen, die vom BSI definiert sind, werden nachfolgend potentielle aktive und passive Angriffsarten aufgeführt. Die passiven Angriffe beschreiben vor allem Verletzungen gegen den Datenschutz, nehmen aber auch eine wichtige Rolle bei der Informationsgewinnung für Angreifer ein. Dahingegen nehmen aktive Angriffe direkt Einfluss auf den Prozess z. B. durch Datenmanipulationen. Bei einem zielgerichteten mehrphasigen Angriff spielen zumeist passive als auch aktive Angriffe eine Rolle. Einige im Bereich der Stationsautomatisierung typische aktive und passive IT-Angriffsarten sind in Tab. 1 und Tab. 2 dargestellt.

Zur Vermeidung von IT-Angriffen im operativen Betrieb stehen verschiedene passive und aktive IT-Sicherheitsmaßnahmen zur Verfügung. Passive IT-Sicherheitsmaßnahmen unterbinden den Zugang auf vulnerable Systeminformationen und -komponenten u. a. durch Zugriffskontrollen (z. B. Autorisierungs- und Authentifizierungsmechanismen), Zugriffsbeschränkungen, Informationsverschlüsselung und -separation [6–9]. Demgegenüber gehen aktive IT-Sicherheitsmaßnahmen davon aus, dass ein Systemzugriff seitens des Angreifers bereits erfolgt und passive IT-Sicherheitsmaßnahmen entsprechend umgangen wurden. Ziel aktiver IT-Sicherheitsmaßnahmen ist die Detektion laufender oder bereits erfolgter IT-Angriffe durch Analyse aller netzwerkbezogener Informationen. Dies erfolgt hauptsächlich durch Einsatz Host- oder Netzwerk-basierter Intrusion Detection Systeme (HIDS bzw. NIDS). Je nach eingesetzten Erkennungsverfahren können diese weiter unterteilt werden in Spezifikations-, Signatur- und Anomalie-basierte Verfahren [10–16]. Die hier nachfolgend vorgestellten Ansätze zur Absicherung der Kommunikationswege (siehe Abschnitt 3.3) und der Anomalieerkennung (siehe Abschnitt 3.4) spielen eine wesentliche Rolle in der Resilienzbewertung digitaler Stationen (siehe Abschnitt 3.2).

2 Referenzarchitektur digitaler Stationen

2.1 Aufbau der Infrastruktur und Kommunikationswege

Nachfolgend wird ein Referenzansatz digitaler Stationen als IP-basiertes Umspannwerk zwischen der Mittel- und Hochspannungsebene in Energienetzen mit dem Ziel ei-

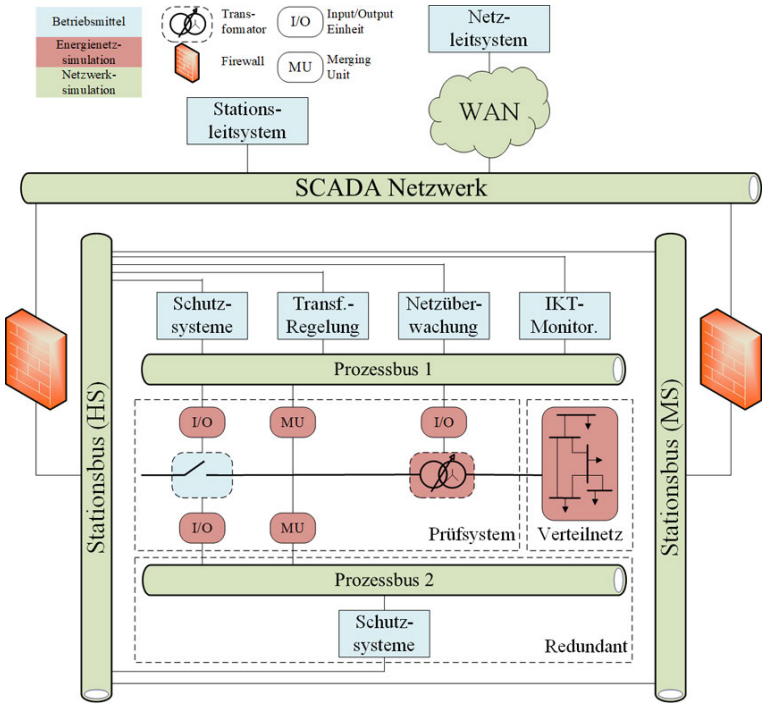

Abb. 1: Digitale Station aufgeteilt in reale Betriebsmittel, Energienetzsimulation und Netzwerksimulation.

ner einheitlichen Kommunikation nach IEC 61850 vorgestellt. Ziel ist die Nachbildung eines realitätsnahen Aufbaus inkl. detaillierter Abbildung notwendiger Stationskomponenten und Kommunikationsstrecken. Diese Referenzarchitektur ermöglicht somit umfassende Versuche in der IT- und OT-Domäne unter Laborbedingungen, welche auf reale Prozesse übertragbar sind. Den prinzipiellen Aufbau zeigt Abb. 1.

Für die Betrachtung wird der Ausschnitt eines Leitungsstranges einer Umspannstation auf der Oberspannungsseite als Modell umgesetzt. Die Speisung sowie Abnahme erfolgt über angegliederte Netze, die für die weitere Betrachtung der digitalen Station nicht relevant sind und daher nicht weiter beschrieben werden. Der dargestellte Leitungsabzweig umfasst wesentliche Elemente wie Leistungsschalter, Messeinrichtungen sowie den Transformator inklusive Stufensteller, um alle möglichen Typen von Mess- und Statussignale zu generieren und Stellgrößen bereitzustellen. Um das System zunächst möglichst einfach zu halten, wird auf die Modellierung von Trennern, Kupplungen sowie der Sammelschienensysteme auf Hoch- sowie Mittelspannungsebene verzichtet. Alle Komponenten sollen das Übertragungsprotokoll IEC 61850 durch die drei verschiedenen Kommunikationsarten MMS, GOOSE, Sampled Values je nach Anwendung unterstützen. Jegliche Messgrößen des Netzes werden durch verteilte Messeinrichtungen, den Merging Units (MU), erfasst und über Sampled Values übertragen. Die Spannungs- und Strominformationen auf Hoch- und Mittelspannungsseite werden von weiteren Systemen wie Schutz-, Steuer- und Überwachungssystemen oder anderen intelligenten Geräten (IEDs) genutzt. Zur Überwachung und Steuerung der Primärtechnik wie Transformatoren und Leistungsschaltern werden GOOSE-Meldungen in beiden Richtungen verwendet, um Status- und Steuerinformationen zu verarbeiten. Für die Ankopplung des Prozesses in überlagerte Leitsysteme wird die MMS Kommunikation des IEC 61850 Standards verwendet, welche durch seine Client-Server Architektur mit dem IEC 60870-5-104 vergleichbar ist. Pilotprojekte zur vereinheitlichten Kommunikation in vernetzten Umspannwerken mittels IEC 61850 werden in verschiedenen Publikationen vorgestellt [17–20]. Gemäß der Norm IEC 61850 wird die Netzwerkumgebung für die unterschiedlichen Informationsarten in verschiedene Bussysteme aufgeteilt. Es werden drei grundlegende Netzwerkebenen vorgestellt.

Auf dem **Prozessbus** werden alle Daten übertragen, die zwischen verschiedenen Input-Output-Einheiten und Merging Units auf der Prozessseite mit überlagerten IEDs hochfrequent über das Multicast-Prinzip ausgetauscht werden. Gemessene und abgetastete Daten werden über IEC 61850 Sampled Values übertragen, nach IEC 61850-9-2. Diese sind ungefilterte Daten für verschiedene Berechnungen sowie Aggregations- und Steuerungsaufga-

ben auf der Stationsebene. Dabei wird zwischen Datenquelle und IED ein Publish-Subscriber-Modell verwendet. Abgesehen von diesen Abtastwerten senden die IEDs, wiederum über ein Publish-Subscriber Modell, Steuer- und Statuswerte an die Betriebsmittel über IEC 61850-8-1 GOOSE. Im vorgestellten Ansatz sind zwei redundante Prozessbusse mitsamt redundanten Schutzsystemen vorgesehen. Dies erhöht die Funktionsfähigkeit und senkt die Gefahr von Prozessstörungen im Falle von Hardware-Fehlern oder IKT-Ausfällen. Wie auch in Abb. 1 dargestellt, sind an einem zweiten Prozessbus sehr wichtigen Systeme redundant angeschlossen, um deren Ausfallsicherheit entsprechend zu erhöhen. Im Falle einer Beschädigung oder eines Fehlers im Prozessbus 1 oder diesen Komponenten kann der zweite Prozessbus den Prozess fortsetzen. Eine Validierung und Erkennung von Fehlern auf Prozessebene ist hierfür zwingend erforderlich.

Daten, die zwischen IEDs an übergeordnete Steuerungsinstanzen wie ein SCADA-System ausgetauscht werden, sind im **Stationsbus** gebündelt und konzentriert. Getrennt durch zumeist Firewalls oder andere Sicherungsschichten ist das SCADA Netzwerk mit dem Aufbau der Unterstation verbunden. SCADA- und Datenbanksysteme erhalten ihre Informationen über IEC 61850 MMS-Meldungen aus dem zugrundeliegenden Prozess. Der Übergang von Stationsbus zu dem **SCADA Netzwerk** stellt aus Sicht der IT-Sicherheit einen sehr wichtigen Punkt dar, aufgrund der nahezu unvermeidlichen Zugänglichkeit der SCADA Netzwerke über öffentliche Netze und der Datenübertragung über TCP/IP-basierte Protokolle. Im Bereich der Hoch- und Höchstspannungsnetze sind autarke Kommunikationsinfrastrukturen der Netzbetreiber heute Stand der Technik. Im Zuge der Digitalisierung und der zunehmenden Verbreitung von Automatisierungstechnik werden weitere Spannungsebenen informationstechnisch an die bestehenden Infrastrukturen angeschlossen. Ein breitflächiger Ausbau des eigenen Glasfasernetzes ist aufgrund der hierfür erforderlichen Größe und Knotenanzahl im Mittel- und Niederspannungsbereich nur sehr schwer zu realisieren. Eine effiziente Möglichkeit ist daher die Nutzung der öffentlichen Infrastrukturen, so dass auch bei Einführung des Funkstandards abgelegene Regionen und Funklöcher abgedeckt werden können.

2.2 Intelligente Monitoring-, Regelungs- und Schutzanwendungen

Für die dargestellten Anwendungsfälle einer digitalen Station mit Realisierung eines IEC 61850 Prozessbusses werden klassische Schutz-, Regelungs- und Monitoring-Anwendungen neu konzipiert. Sämtliche Messdaten für Spannungs- und Stromwerte an unterschiedlichen Messstellen im Umspannwerk werden den IEDs auf der Prozessebene zur Verfügung gestellt. Hierdurch wird der Verkabelungsaufwand verkleinert. Es werden ausschließlich Netzwerkdaten verwendet – analoge Messsignale sind nicht notwendig. Hierdurch werden die IEDs direkt mit dem Prozessbus verbunden und erhalten die notwendigen Daten, die für unterschiedliche Funktionalitäten verwendet werden. In der Übertragung von Messwerten gibt es eine Anpassung des „reinen“ IEC 61850-9-2 Standards zu Sampled Values. Um den vereinheitlichten Einsatz unter verschiedenen Herstellern zu garantieren, wurde dieser in der sogenannten „Light Edition“ in IEC 61850-9-2LE näher spezifiziert [21]. Diese Einigung definiert zwei feste Übertragungsraten und eine feste Datenstruktur für zu übertragende Nachrichten. Es wird jeweils von einem Messpunkt ausgegangen, bei dem Informationen über die drei Leiterspannungen und dem Neutralleiter übermittelt werden, ebenso wie die Ströme auf den jeweiligen Phasen. Zwei unterschiedliche Betriebsmodi sind definiert, die sich in der Abtastung unterscheiden. Es wird differenziert zwischen 4 kHz-Abtastung oder verallgemeinert mit 80 Werten pro Sinus-Schwingung (Beachtung der Grundfrequenz 50 Hz vs. 60 Hz) und der 12.5 kHz-Abtastung mit 256 Werten pro Sinusperiode. Der gängigste Modus, der für viele Anwendungen ausreicht, ist die 4 kHz Abtastung, welche unter Einschränkungen die Übertragung über kupferbasierte Leitungen erlaubt. Für die Abtastung mit 12.5 kHz ist die Übertragung aus Performance Gründen nur über Lichtwellenleitern möglich. Nachfolgende Anwendungen und Funktionen (siehe Tab. 3) sind durch die Nutzung des Prozessbusses im Vergleich zur konventionellen analogen Messung angepasst und auf die Anforderungen der vorhanden Sampled Values erweitert [22–24]. Erweiterungen besonders in Bezug auf passive Monitoring-Möglichkeiten des Prozessbusses werden sind in Kapitel 3 weiter erläutert.

2.3 Kopplung zur Leitsystemebene

Ausgehend von der Stations- und Prozessbuskommunikation auf Basis IEC 61850 GOOSE und SV werden zur Kommunikation zwischen digitaler Station und Leitwarte überwiegend gerichtete, TCP/IP-basierte Übertragungsprotokolle verwendet. Traditionell kommt hierfür das adressorientierte Fernwirkprotokoll IEC 60870-5-104 zum Einsatz mit weitreichender Unterstützung gängiger Übertragungssequenzen wie z. B. Befehlsübermittlungen oder sponta-

Tab. 3: Übersicht klassischer Funktionalitäten innerhalb von Stationen und Änderungen durch den Prozessbus.

Funktion	Konventionell	Prozessbus-basiert
Spannungsregelung	hierarchische Regelungskonzepte auf Basis analoger Messwerte und analoger oder protokollbasierter Ansteuerungen	SV-basierter Messwerte, i. d. R. über eigene Merging Unit integriert
Schutzfunktionen – Distanzschutz – Differentialschutz – Transformatorschutz	analoge Messung von Spannungs- und Stromsignalen Auswertung und protokollbasierte oder analoge Ansteuerung von Schutz- bzw. Leistungsschaltern	SV-basierte Messwerte für verschiedene Schutzfunktionen mit GOOSE-basierter Ansteuerung nachgelagerter Schutz- und Leistungsschalter
Monitoring – Power-Quality – Netzzustand – Phasor-Messung	analoge Messung und Auswertung von Spannungs- und Stromsignalen, netzwerktechnische Anbindung an höhere Ebenen	SV-basierte Messwerte mit Auflösungsgrenzen und Beschränkung abbildbarer Oberwellen oberhalb der Abtastfrequenz

Tab. 4: Übersicht ACSI-Services für IEC 61850-8-1 (MMS) Kommunikation.

ACSI-Service	Beschreibung
SETBRCBVALUES, GETBRCBVALUES	Schreiben bzw. Lesen der Reporting-Konfiguration
LOGICALDEVICEDIRECTORY, LOGICALNODEDIRECTORY, GETDATASETDIRECTORY	Lesen der Verzeichnisse von logischen Geräten und Knoten sowie einer vordefinierten Datenkollektion
GETDATAVALUES, GETDATASETVALUES, GETALLDATAVALUES	Lesen von Datenattributen eines Datenobjekts, einer Datenkollektion sowie eines logischen Knotens
SETDATAVALUES	Setzen von Datenattributen eines Datenobjekts

ne sowie zyklische Messwertabfragen [25]. Im Zuge der Etablierung des IEC 61850 Standards erfolgt die Kopplung zwischen Leitwarten- und Stationsebene über IEC 61850-8-1 MMS Kommunikation und ermöglicht im Vergleich zum IEC 60870-5-104 Standard die Nutzung umfassender Kommunikationsdienste. Grundlage hierfür ist ein objektorientiertes IEC 61850 Datenmodell zur Abbildung aller relevanten Stationskomponenten und –funktionen. Der Informationsaustausch zwischen Leitwarte und Station erfolgt über die Nutzung verschiedener Dienste des Abstract Communication Service Interface (ACSI) zur Erfassung und Änderung aller wesentlichen Stationsparameter sowie netzbezogener Größen. Eine entsprechende Übersicht liefert nachfolgend Tab. 4. Weiterführende Informationen finden sich unter [26].

IEC 61850-8-1 (MMS) und IEC 60870-5-104 Protokolle dienen dem Austausch von SCADA-Informationen in Überwachungsrichtung (Messwerte, Statusinformationen, Parameter) und Steuerungsrichtung (Sollwerte, Befehle). Darüber hinaus werden insbesondere in der Übertragungsnetzebene zeitlich hochaufgelöste Phasormessungen von PMUs (engl.: Phasor Measurement Units) verwendet, um die Überwachungs- und Steuerungsmöglichkeiten vor allem im dynamischen Zeitbereich deutlich zu verbessern [27]. Hierzu werden PMU-Sensoren zur Messung von Spannungs- und Stromphasoren sowie zusätzlicher Frequenzinformationen im Netz verteilt. Die Übertragung der mit GPS Zeitstempel versehenen Daten erfolgt über das TCP/IP-basierte IEEE C37.118 Protokoll (seit 2018: IEC 60255-118-1-2018 [28]). Typische Übertragungsraten liegen dabei im Bereich von 10 bis 50 Messungen pro Sekunde [29].

Für die Umsetzung der IEC 61850-8-1 Kommunikation werden kommerzielle Softwarelösungen zur Erstellung und Verwaltung von IEC 61850 Clients und Servern eingesetzt. Darüber hinaus besteht die Möglichkeit mit einem Gateway IEC 61850-8-1 und IEC 60870-5-104 Komponenten direkt miteinander zu verbinden. IEC 60870-5-104 Clients und Server stehen alternativ als Java®-basierte Softwaremodule zur Verfügung [30]. Für die IEEE C37.118 Kommunikation kommen Python®-basierte Client- und Server-Lösungen zum Einsatz auf Basis von [31].

3 Simulation und Analyse gesicherter, digitaler Stationen

3.1 Untersuchungen auf Basis von cyber-physischen Echtzeit-Co-Simulationen

Die vorgestellten Strukturen im Bereich der Energieversorgung zeigen, dass eine immer größer werdende Abhängigkeit zur Kommunikationsinfrastruktur besteht. Hier spielen die Übertragungsstrecken zwischen elektrischen Betriebsmitteln, Systemen und Komponenten eine besondere Rolle, aber auch deren Implementierung in Kommunikationsinfrastrukturen. Erst die Integration von Netzwerkkomponenten mitsamt Schnittstellen, Konfigurationen und Schwachstellen in eine gemeinsame Simulationsumgebung ermöglicht eine umfassende Analyse und Bewertung der IT-Sicherheit von Energieversorgungsstrukturen. Im Vordergrund der Analysen bezüglich der IT-Sicherheit sind allgemeine Fragestellungen, wie die externe Erreichbarkeit der Systeme, die Möglichkeit der Manipulation von Konfigurationen und der Datenabgriff, bzw. die Datenmanipulation ausgetauschter Daten. Auch klassische Angriffsmuster aus dem Bereich der IT, wie DoS Attacken, stellen Herausforderungen für OT-Strukturen dar. Die Auswirkungen durch Eingriffe in der Netzwerkebene auf die elektrische Ebene sind essentiell für Risikoabschätzungen von IT-Angriffen. Eine isolierte Laborumgebung ohne natürlich auftretende Störungen oder externe Einflüsse stößt hier auf gewisse Grenzen, wodurch Erweiterungen des Netzwerks mitsamt simulierten Nebeneinflüssen auf Netzwerkebene durch Simulationssysteme notwendig werden.

Zur Untersuchung der unterschiedlichen Fragestellungen und Bewertung der gesamtheitlichen IT-Sicherheit von digitalen Strukturen, wird eine **cyber-physische Echtzeit-Co-Simulationsplattform** vorgestellt, die eine Synthese aus zwei dynamischen Simulationsebenen und der Integration von realen Betriebsmitteln und Komponenten ermöglicht. Durch die Anforderung der Einbindung von realen Komponenten und der Untersuchung von dynamischen Phänomenen, ausgelöst durch IT-Sicherheitsvorfälle, aber auch durch elektrische Wechselwirkungen, leitet sich die Anforderung von dynamischen Betrachtungen unter Einhaltung von Echtzeit-Bedingungen ab.

Gesamtkonzept

Der vorgestellte Gesamtaufbau der digitalen Station inkl. der Kopplung zu überlagerten Leitsystemen steht im Gesamtenergienetz mit verschiedenen Spannungsebenen für exemplarisch herausgezogene Bestandteile. Für eine Gesamtintegration sind unterschiedliche Messpunkte und Übertragungsprotokolle sowie -mechanismen zu berücksichtigen. Diese können aber nicht alle in der gleichen Detailtiefe modelliert und simuliert werden. Der hier präsentierte Ansatz beschreibt eine Mischform aus Simulationsobjekten aus einer Energienetzsimulation, einer Netzwerksimulation und real eingebunden Hardware-Komponenten. Einige Objekte und Teile eines Energienetzes werden lediglich im elektrischen Verhalten simuliert und geben den Netzzustand über nicht weiter betrachtete Schnittstellen an die übergeordnete Leitebene. Andere Teile des Netzes stehen mehr im Fokus und werden detaillierter modelliert und simuliert. Hierdurch rücken neben der elektrischen Betrachtung auch andere Aspekte und besonders die Kommunikationsebene des Prozesses in den Vordergrund. Ein gebündeltes Untersuchungsobjekt ist die bereits eingeführte digitale Station. Für die hier vorgestellte Betrachtung wird eine sogenannte Co-Simulation umgesetzt. Aus der Co-Modellierung der beiden Ebenen – elektrisches Netz und Kommunikationsnetzwerk – wird ein gemeinschaftliches Simulationssystem aufgebaut. Durch die Integration von Hardware-in-the-Loop Ansätzen lässt sich der Gesamtaufbau in drei unterschiedliche Bereiche aufteilen.

Elektrische Netzsimulation Das Herzstück der vorgestellten Untersuchungen bildet eine Echtzeit-Netzsimulation eines elektrischen Netzes auf unterschiedlichen Spannungsebenen. Zur präzisen Abbildung transienter Netzvorgänge, insbesondere kritischer Netzbetriebssituationen, wird eine hochaufgelöste dynamische Simulation notwendig. Die Netzsimulation, hier umgesetzt durch die Software HYPERSIM von OPAL-RT, läuft auf einer Hardwareplattform und hat eine minimale Abtastung von 50 µs. Über die Simulation können verschiedene Schnittstellen umgesetzt werden. Analoge und digitale Schnittstellen ermöglichen dabei unterschiedliche Umsetzungen von Hardware-in-the-Loop Ansätzen. Hierbei werden direkte Verbindungen zwischen dem „Device under Test“ und der Simulationsplattform hergestellt und durch einen zwischengeschalteten Leistungsverstärker wird das Betriebsmittel elektrisch in die Simulation eingebunden. Neben dieser elektrischen Einbindung besteht die Möglichkeit, über kommunikationstechnische Übertragungsprotokolle weitere Schnittstellen zur Simulation zu schaffen. Diese Kommunikationsschnittstellen stehen

in dem vorliegenden Beitrag im Vordergrund. Die energietechnischen Protokolle, wie das IEC 61850, bieten die Möglichkeit, den vorgestellten Ansatz der digitalen Station oder der dynamischen Leitwarte umzusetzen.

IKT-Netzsimulation Die Netzwerksimulation wird in dem vorgestellten Ansatz durch eine ereignisbasierte Simulationssoftware umgesetzt, in diesem Fall durch den diskreten Event-Simulator OMNeT++. Netzwerktopologien werden mitsamt den Netzwerkkomponenten aufgebaut, wodurch beispielsweise das Routing und die Absicherung von Datenströmen abgedeckt werden können. Innerhalb der Netzwerksimulation lassen sich im Online-Betrieb externe Schnittstellen einrichten. Ein Informationsaustausch wird so über die energietechnischen Übertragungsprotokolle umgesetzt, welche bereits eingeführt wurden. Der Standard IEC 61850 steht mit seinen unterschiedlichen Kommunikationsarten auch hier im Fokus. Die Gegenstellen für dieses Protokoll können innerhalb der Simulationsumgebung konfiguriert werden und den Datenaustausch mit der Energienetzsimulation oder den real vorliegenden Betriebsmitteln und Systemen umsetzen. In einem ersten Schritt erfolgt der Aufbau eines Netzwerkes auf Prozessebene mit den Schnittstellen zu überlagerten Ebenen (z. B. Stationsbus). Vereinfachte Schutzalgorithmen und Logiken zur Auswertung auf Prozessebene können entworfen und integriert werden. Spätere Untersuchungen zur kommunikationstechnischen Anbindung der Prozessebene bzw. des Stationsbusses an überlagerte SCADA und Unternehmens-Ebenen ermöglichen nähere Einflüsse von genutzten öffentlichen Netzwerken oder der Übertragung von Daten an entfernte Leitstellen zu identifizieren und abzubilden.

Hardware-in-the-Loop Simulation Für viele Untersuchungen spielt die Integration von realer Hardware eine essentielle Rolle zu Untersuchungen bezüglich deren Funktionsfähigkeit in abgebildeten Infrastrukturen. Aber auch aus Sicht der IT-Sicherheit ist die Integration von Komponenten relevant zur Abbildung der realen Schwachstellen und Manipulationsmöglichkeiten. Wird ein reales Betriebsmittel in den Prozess integriert, so können auch unterschiedliche Ebenen eines Betriebsmittels abgebildet, integriert und simuliert werden. In vorigen Arbeiten wurde bereits ein teil-virtualisiertes Betriebsmittel eingeführt [32], dessen Verhalten in eine Kommunikationsebene und elektrische Ebene aufgeteilt wurde. Ein reales Betriebsmittel kann elektrisch in ein Simulationssystem eingebunden werden, während seine Datenübertragung simulativ umgesetzt wird. Andererseits kann das elektrische Verhalten auch simuliert und die realen Datenübertragungsschnittstellen werden weiterhin betrieben. Hierdurch lassen sich verschiedene Varianten abbilden. Ein Beispiel eines solchen Betriebsmittels ist der Leistungsschalter, welcher den realen Schaltvorgang physisch durchführen kann. Die zur Auslösung des Schaltvorganges notwendigen Daten für die Schutzsysteme werden durch die Echtzeitsimulation des elektrischen Netzes bereitgestellt.

Neben reinen Betriebsmitteln spielen auch Schutz- und Monitoringsysteme eine große Rolle. Diese Systeme werden ebenfalls als reale Hardware Systeme eingebunden. Durch die vorgestellte Speisung mit Daten des Prozessbusses kann folglich auch auf die elektrische Verbindung und die Messung von realen Größen verzichtet werden. Eine reine Speisung durch Simulationsdaten und hier umgesetzte Merging Units ist ausreichend. Durch den Prozessbus können auf Basis der zur Verfügung stehenden Messdaten unterschiedliche Monitoring- und Schutzfunktionalitäten prototypisch aufgebaut und weiterentwickelt werden.

Kopplung zur Gesamt Co-Simulation

Die Kopplung der beiden Simulationssysteme geschieht über einen parallelen Informationsaustausch. Analog zu den vorgestellten Arten teil-virtualisierbarer Betriebsmittel wird die Integration der IKT Netzwerkabbildung in die Energienetzsimulationen in unterschiedliche Kopplungsformen unterteilt [33]:

- Hardware-in-the-Loop,
- emulierte IKT Hardware,
- simulierte IKT Hardware und
- vollständige Simulation.

Bei der Kopplung sind unterschiedliche Aspekte zu beachten, wie die Harmonisierung der Modellierungen, die systemtechnische Stabilität und die Zeitsynchronisierung bis hin zu einer vereinheitlichten Zeitbasis. Einen Überblick über verschiedene, domänenübergreifende Ansätzen und Projekte zur Entwicklung von Co-Simulationsumgebungen gibt [34]. Die Unterscheidung in diskrete und kontinuierliche Modellierung kommt bei der Synthese von elektrischer Netzsimulation und eventbasierter Netzwerksimulation zum Tragen, wodurch der Ansatz einer hybriden Co-Simulation benötigt wird. Schwierigkeiten und Herausforderungen bei der Kopplung von hybriden Co-Simulationssystemen und insbesondere der Notwendigkeit einer gemeinsamen Zeitbasis, bzw. zeitbasierten Synthese, zeigt beispielhaft [35].

Die beiden Kommunikationsarten der Norm IEC 61850 – Sampled Values und GOOSE – werden für die Datenübertragung zwischen beiden Simulationssystemen verwendet. Diese Nachrichten werden jeweils im vorliegenden

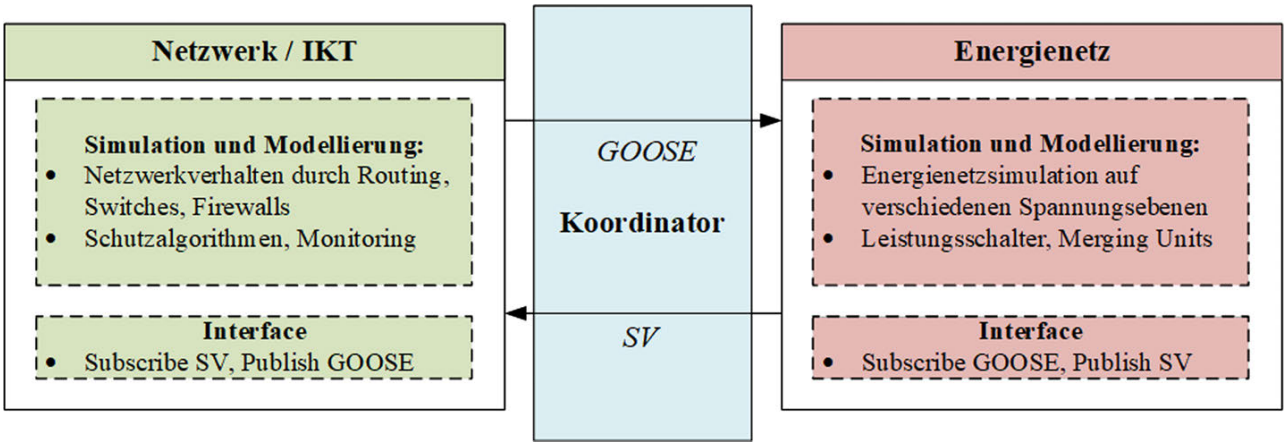

Abb. 2: Koordination der beiden Simulationsebenen innerhalb der Co-Simulation unter Nutzung von IEC 61850 Nachrichten.

Simulationssystem generiert. Ein einfacher Anwendungsfall beschreibt die Kopplung eines Leistungsschalters an ein Schutzsystem unter der Verwendung von Prozessbus-Daten, in welchem beide Simulationsebenen verwendet werden. Die Energienetzsimulation berechnet Werte für dreiphasige Spannungen und Ströme in definierten Knoten im Stromnetz. Diese Werte werden über Sampled Values durch das beschriebene Publisher-Subscriber Prinzip übertragen. Innerhalb der HYPERSIM Simulation wird ein vorhandener IEC 61850-9-2LE Publisher verwendet und sendet die Daten an die Netzwerksimulation. In der aufgebauten OMNeT++ Umgebung wird hierfür über die INET Erweiterung ein SV-Subscriber definiert und integriert. Die Netzwerksimulation selbst sendet GOOSE-Nachrichten an die Energienetzsimulation, um beispielsweise Leistungsschalter zu steuern. Diese Nachrichten müssen in der Energienetzsimulation von GOOSE-Subscribern verarbeitet werden. Auch hier kommen wieder bereits vorhandene Module zum Einsatz. Für die zeitliche Synchronisation der beiden Systeme gilt es einen Koordinator zu entwerfen [33, 34]. Die prinzipielle Funktionsweise des Koordinators zeigt Abb. 2.

Der **Koordinator** übernimmt dabei die Kontrolle der Simulationszeit und den Datenaustausch zwischen den Systemen. Der zweite Aspekt kann in dem beschriebenen Kontext zunächst vernachlässigt werden, da Standardprotokolle zum Einsatz kommen und somit kein dedizierter Datenaustausch über den Koordinator definiert und implementiert werden muss. Der Koordinator stellt jedoch Anforderungen an die Simulationszeit und muss diese folglich von beiden Systemen überwachen. Passende Schnittstellen und Übertragungsarten können von den beiden Systemen genutzt werden. Unterschiedliche Ansätze zur Orchestrierung nach Master-Slave Verfahren über beispielsweise das Functional Mock-Up Interface (FMI) oder High-Level Architecture (HLA) sind bereits veröffentlicht mit noch bestehenden Herausforderungen an die Zeitsynchronisierung und der externen Ansteuerung der eventbasierten Netzwerksimulation [36, 37]. Neben Master-Slave Konzepten sind in der Literatur Ansätze zu Punkt-basierten und Event-gesteuerten Koordinierungsansätzen zu finden. Der Entwurf der Kopplung und Koordinierung ist maßgeblich von den Berechnungsobjekten abhängig und ist Gegenstand künftiger Untersuchungen, um die Stabilität und Zeitsynchronität der Co-Simulation in unterschiedlichen dynamischen Anwendungsfällen sicherzustellen. Vor allem durch die Dynamik und Echtzeit-Anforderungen des vorgestellten Ansatzes stoßen bekannte und verbreitete Ansätze nach Master-Slave Prinzip an Grenzen. Simulationen auf getrennten Hardwareplattformen werden durch die Rechenfähigkeit des Masters (hier Netzwerksimulation) limitiert. Weiterhin werden Echtzeit-Bedingungen verletzt, wenn die Slave Simulation jeweils neu durch den Master angestoßen werden muss.

3.2 Resilienzbewertung digitaler Stationen

Die Resilienz spielt bei Stromnetzen eine immer größer werdende Rolle. Bei den vorliegenden Betrachtungen wird nachfolgende allgemeine Definition für den Begriff der Resilienz verwendet:

Allgemeine Def.: „Resilienz ist die Fähigkeit, tatsächlich oder potentiell widrige Ereignisse abzuwehren, sich darauf vorzubereiten, sie einzukalkulieren, sie zu verkraften, sich davon zu erholen und sich ihnen immer erfolgreicher anzupassen. Widrige Ereignisse sind menschlich, technisch sowie natürlich verursachte Katastrophen

oder Veränderungsprozesse, die katastrophale Folgen haben“. [38]

Nach konventionellen Betrachtungen der Resilienz wird zumeist nur die Energiebereitstellung betrachtet [39, 40]. Durch die bereits beschriebenen Wandlungen in der Energieversorgung und –verteilung wird jedoch klar, dass eine reine Betrachtung von Energieerzeugungseinheiten und Energieträgern für die Beurteilung von Resilienz nicht ausreichend ist. Im Besonderen die Kommunikation und der Nachrichtenaustausch über unterschiedliche Kommunikationswege und unter Nutzung unterschiedlicher Übertragungsprotokolle trägt maßgeblich zur Funktionsfähigkeit der Prozesse bei und folglich sind Betrachtungen der Resilienz von Infrastrukturen eng gekoppelt mit Betrachtungen der IT-Sicherheit. Eingriffe, Störungen oder andere Ereignisse auf Seite der Kommunikation müssen ebenso betrachtet werden wie klassische Ausfallszenarien für die Energieverteilung, wie physische Schäden an Teilen der Infrastruktur. Aus diesem Grund muss für eine Beurteilung der Resilienz die IKT-Infrastruktur mit betrachtet werden. Dies erfordert eine Analyse und Bewertung von Auswirkungen auf kritische Infrastrukturen bei Beeinflussungen der IKT Infrastruktur. Notwendige Ansätze zur übergreifenden Auswirkungsanalyse von IKT auf das Energienetz sind durch den Ansatz der Co-Simulation vorgestellt. Für eine strukturierte Resilienzbewertung auf Basis von simulativen Untersuchungen gilt es ein Phasenmodell zu implementieren in Anlehnung an [41–43], siehe Abb. 3.

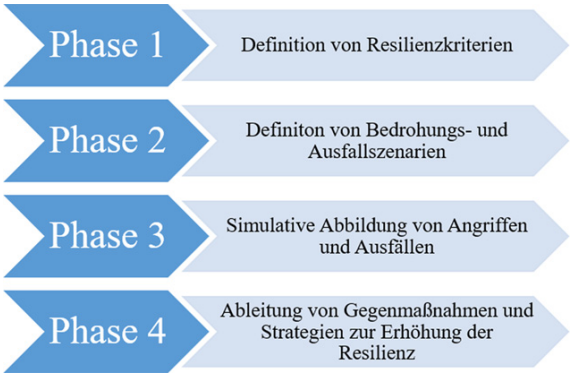

Abb. 3: Phasenmodell der simulationsgestützten Resilienzbewertung nach [43].

Innerhalb von **Phase 1** sind quantitative und qualitative Kriterien zu definieren, um Aussagen über die Resilienz treffen zu können. Hierzu können beispielsweise die Wiederaufbaufähigkeit oder –zeit, Kosten-Nutzen-Verhältnisse bei der Integration von Redundanzen oder Ähnliches zählen, mit gleichzeitiger Definition geeigneter Bewertungsmaße. Die **Phase 2** beschreibt die Identifikation von potentiellen Bedrohungen und Ausfällen auf Basis einer systematischen Beschreibung der vorliegenden Infrastruktur. Nachdem die potentiellen Bedrohungen identifiziert und definiert sind, ist die Beschreibung und Analyse des potentiellen Schadens für das System notwendig, um nach den zuvor definierten Resilienzkriterien in **Phase 3** eine Auswertung treffen zu können. Die Auswirkungen von IT-Angriffen, aber auch von technischen Störungen im Kommunikationsnetz auf das elektrische Verhalten von Betriebsmitteln, können durch genannte Simulationen abgeschätzt werden. Auf Basis der simulativen Untersuchungen werden die Auswirkungen von Ausfällen und Angriffen in **Phase 4** betrachtet und Gegenmaßnahmen abgeleitet. Iterativ können die Phasen 3 und 4 wiederholt werden, bis die gesetzten Resilienzkriterien nach Phase 1 hinreichend erfüllt sind. Die Identifikation von Störungen, bzw. Anomalien, und externen Eingriffen im IKT-Netzwerk steht nach Definition der Resilienz ebenso im Fokus. Aufbauend auf der Erkennung von Störungen können reaktive Maßnahmen nach dem Emergency-Response-Vorgehen definiert und entworfen werden. Neben dieser reaktiven Betrachtung ermöglicht die simulative Untersuchung auch im Planungsprozess aktiv im Vorfeld gegen vorliegende Bedrohungen zu agieren, durch beispielsweise dem Aufbau von Redundanzen in der Kommunikationsinfrastruktur oder Absicherung von kritischen Kommunikationspfaden (siehe Abschnitt 3.3).

Für die resiliente Auslegung von digitalen Stationen nach den vorgestellten Schritten der Resilienzbewertung stehen unterschiedliche Aspekte im Fokus. Essentiell für digitale Stationen ist die Fähigkeit, Angriffe und Fehlfunktionen auf der Prozess- und Leitebene zu identifizieren. Hierauf wird in Abschnitt 3.4 näher eingegangen und verschiedene Lösungsansätze präsentiert werden. Im Sinne der Resilienz spielt der Planungsprozess und Konfigurationsprozess von IKT-Infrastrukturen eine wichtige Rolle. Für die Auslegung der IKT-Infrastruktur werden bestehende Bedrohungsszenarien definiert und daraus Anforderungen abgeleitet, wie beispielsweise einer redundanten Auslegung des Prozessbusses zur Erhöhung der Ausfallssicherheit von Schutzfunktionalitäten und einem teilweise redundanten Aufbau des Stationsbusses zur Absicherung kritischer Verbindung zum SCADA Netzwerk. Hier vorgestellte Analysen durch Simulationen ermöglichen es, gewisse Szenarien abzubilden und die Resilienzfähigkeit im Planungsprozess zu bewerten und gezielt umzusetzen, ähnlich wie in [41] beschrieben.

3.3 Passive Absicherung der Kommunikationswege

Wie in Abschnitt 1.2 beschrieben, unterscheidet man bei den Maßnahmen zur Absicherung von IT-Systemen zwischen aktiven und passiven Methoden. Die nachfolgend beschriebenen Mittel stellen passive Ansätze zur Absicherung von Kommunikationswegen im Kontext der digitalen Station dar. Sie dienen daher in der ersten Phase des IT-Angriffes dazu, dem Angreifer die Aufklärung des Zielsystems zu erschweren. In dieser Phase sammelt der Angreifer wichtige Informationen über die Infrastruktur der digitalen Station, die Kommunikationspartner und -protokolle und kann darauf aufbauend weitere Schritte planen. Wird dieser Informationsgewinn beschränkt bzw. unterbunden, können spätere koordinierte und mehrstufige IT-Angriffe verhindert oder zumindest erschwert werden.

In Tab. 1 und Tab. 2 wurden Beispiele von aktiven und passiven IT-Angriffen vorgestellt. Maßnahmen zur Erhöhung der passiven IT-Sicherheit, wie beispielsweise der Einsatz von Verschlüsselung oder Authentifizierungszertifikaten, bieten erhöhten Schutz gegenüber Angriffstypen beider Kategorien. Zum Beispiel verhindert die Verschlüsselung von IEC 61850 Paketen den Einblick in die stationsinterne Kommunikationsstruktur und deren Messwertübertragung. Dagegen bietet der Einsatz von digitalen Zertifikaten auf Basis einer Public-Key-Infrastruktur, wie beispielsweise X.509, Schutz gegenüber den Angriffstypen Man-in-the-Middle, Data Spoofing oder False Data Injection (vgl. mit Tab. 2).

Mit der Normreihe IEC 62351 wurden Methoden eingeführt, um die CIA-Kriterien aus Abschnitt 1.1 für eine sichere Datenkommunikation innerhalb der digitalen Station zu gewährleisten. Diese setzt vor allem auf die Umsetzung einer Ende-zu-Ende-Absicherung des Datenverkehrs für die TCP/IP-basierten Protokolle IEC 61850 GOOSE, MMS und SV [3]. Dabei wird auf das hybride Verschlüsselungsprotokoll Transport Layer Security (TLS) gesetzt, welches eine erforderliche gegenseitigere Authentifizierung von Client und Server auf Basis von X.509-Zertifikaten voraussetzt. Dies hat zur Folge, dass jedes übermittelte Paket mit einem Sitzungsschlüssel chiffriert wird, sodass es dem Angreifer unmöglich gemacht wird, Daten auszulesen oder unbemerkt zu manipulieren. Weiterhin stellt die Authentifizierung mittels digitaler Zertifikate zum Sitzungsbeginn sicher, dass kein Angreifer die Identität des Gegenübers annehmen kann, wie es beispielsweise während eines Man-in-the-Middle-Angriffes geschieht. Mit der Authentifizierung der Identität des Gegenübers wird daher sichergestellt, dass ein Datenaustausch nur zwischen den vorgesehenen Kommunikationspartner stattfindet. Weiterhin sollen mit dem Einsatz von virtuellen LAN (VLAN) für GOOSE und MMS sowie Authentifizierungsmechanismen für SNTP der IEC 61850 Standard sicherer gestaltet werden. Aufgrund der schnellen Übertragungszeitanforderung könnten die meisten kryptografischen Verfahren z. B. auf Basis von RSA-Signaturen insbesondere für GOOSE möglicherweise nicht praktikabel sein, da diese durch rechenintensive Operationen die Übertragungszeit der Pakete deutlich erhöhen [44].

Für die Umsetzung einer passiv gesicherten IEC 61850 MMS Kommunikation zwischen Leitsystemen und der digitalen Station stehen Sicherheits-Plug-Ins zur Verfügung, welche bedarfsweise aktiviert werden können zur Absicherung der Client-Server-Verbindung. Darüber hinaus besteht ebenfalls die Möglichkeit einer passiven Absicherung der IEEE C37.118 Kommunikation durch Aufbau und Nutzung einer performanten TLS-Verschlüsselung. Bezüglich der Kommunikation auf Basis von IEC 61850 GOOSE und SV Paketen wird auf den Einsatz aktiver IT-Sicherheitsmaßnahmen (siehe Abschnitt 3.4) gesetzt.

3.4 Cyber-physische Anomalieerkennung

Neben der passiven Absicherung der Kommunikation durch Authentifizierungs- und Verschlüsselungsmaßnahmen ist die aktive Erkennung von IT-Angriffen ein wichtiger Baustein gesicherter, digitaler Stationen. Die cyber-physische Anomalieerkennung geht dabei über klassische IDS-Ansätze [10–15, 45, 46] hinaus und analysiert sowohl netzwerk- als auch prozessbezogene Informationen. Hierzu werden herkömmliche SCADA-Daten (z. B. IEC 61850-8-1 oder IEC 60870-5-104) um zeitlich hochaufgelöste Messungen im Netz verteilter PMU-Sensoren und lokaler IEC 61850-9-2 Sampled Values aus dem Prozessbus ergänzt. Dies ermöglicht eine automatische Situationserkennung auf Basis statistischer Verfahren oder unter Nutzung künstlicher Intelligenz. Durch die zusätzliche Einbeziehung und Analyse des Netzwerkverkehrs der prozessbezogenen Kommunikation können gestörte bzw. manipulierte Informationen erkannt und von physikalischen Ereignissen unterschieden werden. Dies ist eine wichtige Voraussetzung für eine umfassende cyber-physischen Situationsbewertung.

Allgemein können Anomalien als von einem definiertem Normalverhalten abweichende Prozess- oder Signalcharakteristiken bezeichnet werden [47, 48]. Eine zentrale Herausforderung der Anomalieerkennung ist die Bewertung der Kritikalität hinsichtlich des zugrundeliegenden Prozesses, da nur ein bestimmter Teil detektierter Anomalien eine Gegenreaktion bzw. Handlung erfordern.

Die übergeordnete Zielstellung der cyber-physischen Anomalieerkennung ist die Detektion kritischer Netzbetriebssituationen unter Berücksichtigung von IT-Angriffen zur Vermeidung von Versorgungsausfällen oder Stabilitätsverlusten. Aufgrund der hohen Systemkomplexität heutiger Energieversorgungssysteme ergibt sich eine hohe Anzahl und Vielfalt möglicher cyber-physischer Situationen bzw. Ereignisse, die zu berücksichtigen sind – siehe auch [5]. Zu physikalischen Anomalien können Power-Quality Ereignisse (z. B. Flicker, Spannungseinbrüche), Fehlfunktionen (z. B. Sensorausfälle, Fehlparametrierungen) oder auch Betriebsstörungen (z. B. Anlagenausfälle, Kurzschlüsse) zählen. Virtuelle Anomalien umfassen vorrangig IT-Angriffe in Form von:

- Dateninspektionen zum Auslesen vulnerabler Systeminformationen (z. B. reconaissance attack),
- Datenmanipulationen zur Veränderung von Messwerten, Status- und Zeitstempelinformationen sowie Netzbetriebsmittelparametern (z. B. false data injection, timing based attacks) und
- Kommunikationsstörungen zur Unterbrechung oder Verzögerung von Kommunikationsprozessen (z. B. denial-of-service attack) oder auch das Einschleusen historischer oder manipulierter Netzwerkpakete (z. B. replay attacks).

Prinzipiell können derartige IT-Angriffe über passive Sicherheitsmaßnahmen (siehe Abschnitt 3.3) vermieden bzw. erschwert werden. Zusätzlich ermöglicht die aktive Überwachung von Netzwerkpaketen (z. B. PMU- und SCADA-Telegramme) die Detektion und Unterscheidung virtueller Anomalien. Hierbei bietet sich der Einsatz spezifikationsbasierter Verfahren (z. B. Whitelists, Blacklists, Regelwerke) sowie anomaliebasierter Verfahren (z. B. die statistische Erkennung von Messwertanomalien oder Unregelmäßigkeiten im Netzwerkverkehr) an. Zur Erkennung cyber-physischer Anomalien werden mehrere Detektoren bzw. unterschiedliche Verfahren miteinander kombiniert. Über eine geeignete Meta-Analyse (z. B. Fuzzy-Modell) können die Ergebnisse aggregiert und für eine ganzheitliche cyber-physische Situationserkennung genutzt werden. Je nach erkannter Angriffsart bzw. Anomalie können darauf aufbauend gezielte Gegenmaßnahmen (z. B. Bildung von Ersatzwerten, Aktivierung von Notfallprozeduren, Nutzung redundanter Kommunikationswege, Sperrung von Ports) eingeleitet werden. In den folgenden Ausführungen werden Lösungsansätze zur Erkennung und Klassifikation physikalischer Anomalien kurz vorgestellt. Für eine detaillierte Beschreibung der entwickelten Verfahren wird an dieser Stelle auf die Primärliteratur verwiesen. Entsprechende Ansätze zur Detektion virtueller Anomalien befinden sich aktuell in der Entwicklung.

In [49] wurde ein Online-Analyseverfahren zur Erkennung von *Anomalien auf Basis von IEC 61850-9-2 Sampled Values* entwickelt. Hierbei werden Spannungsbeträge bei zeitlich hoher Abtastung (80 Samples pro Netzperiode) ausgewertet zur Erkennung von Netztransienten mit Fokus auf Power Quality Kriterien. Hierzu wird ein zweistufiges Verfahren bestehend aus einem regelbasierten Klassifikator und einem Klassifikator auf Basis von Spannungsgradienten umgesetzt, siehe auch Abb. 4. Dabei wird mittels Fouriertransformation ein ungestörtes Referenzsignal auf Basis der erfassten Grundfrequenz ermittelt und mit dem Messsignal verglichen.

Zur Erkennung und Bewertung physikalischer *Anomalien auf Basis von PMU-Messungen* wurde in [50] ein statistisches Analyseverfahren entwickelt. Hierbei werden Signalauswertungen im Zeit- und Frequenzbereich (z. B. Wavelet-Dekomposition) für einzelne PMU-Messkanäle (z. B. Spannungsamplitude) durchgeführt. Durch Vergleich aktueller Analysen mit historischen Ergebnissen wird ein Anomaliegrad bestimmt, welcher je nach Ausprägung fünf verschiedenen Anomaliestufen (normal bis extrem) zugeordnet werden kann. Die prinzipielle Funktionsweise zeigt Abb. 5.

Zur besseren Veranschaulichung zeigt Abb. 6 einige simulierte Frequenz- und Spannungssignalverläufe für unterschiedliche Anomaliegrade bzw. Anomaliestufen.

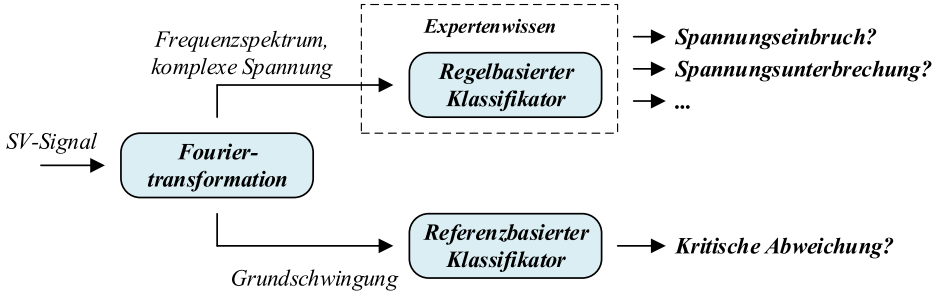

Abb. 4: Prinzipielle Funktionsweise der SV-basierten Anomalieerkennung nach [49].

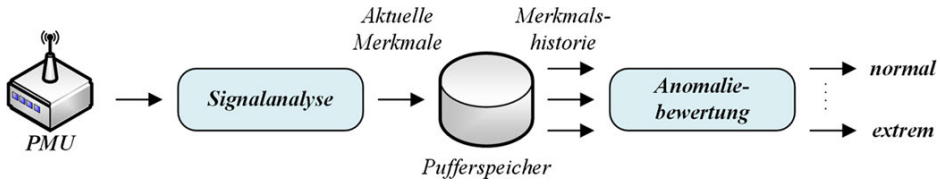

Abb. 5: Prinzipielle Funktionsweise der PMU-basierten Anomalieerkennung nach [50].

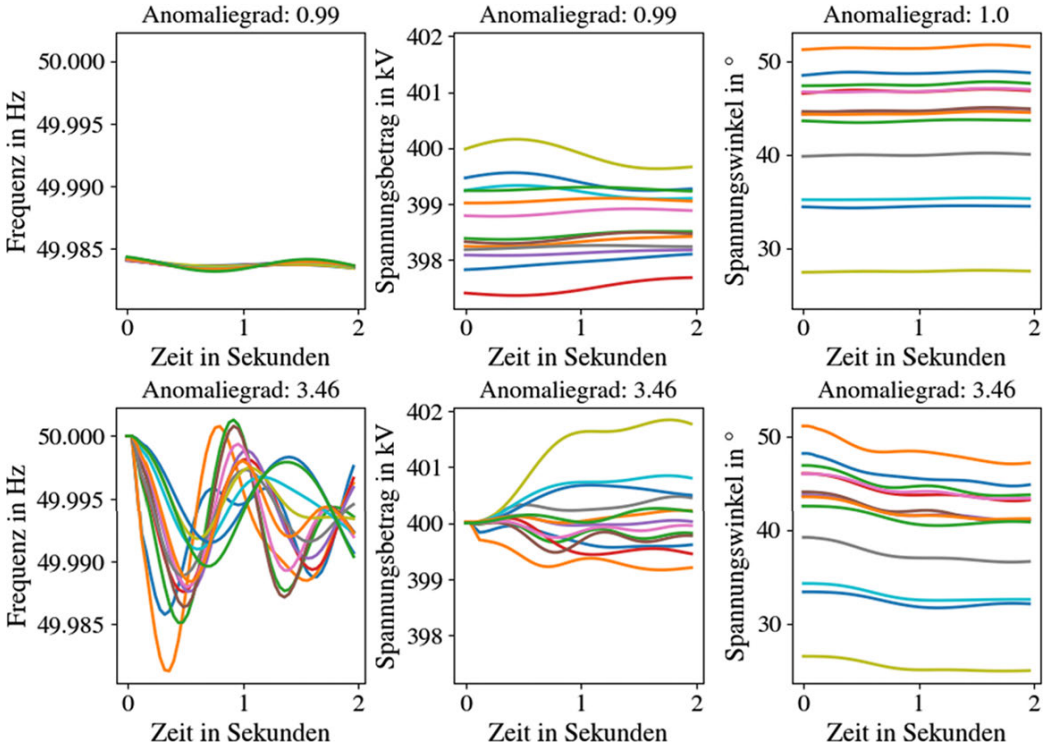

Abb. 6: Exemplarische Anomaliebewertungen von PMU-Beispielsignalen.

Die automatische *Identifikation und Lokalisierung von Betriebsstörungen* auf Basis maschineller Lernverfahren ist aktuell Gegenstand vieler Untersuchungen [51–53]. Unter Bereitstellung einer geeigneten Trainingsdatenbasis kann somit ein Großteil physikalischer Anomalien erkannt und vordefinierten Klassen zugeordnet werden. Im Gegensatz zu den vorherigen Ansätzen können somit Gegenmaßnahmen bereits im Vorfeld für verschiedene Fehler- oder Anomalietypen definiert und im Fall einer Detektion ausgeführt werden. In [50, 54] wurden entsprechende Klassifikationsverfahren entwickelt durch Analyse von Frequenz- und Spanungsmessungen hochaufgelöster PMU-Daten. Über dynamische Netzsimulationen werden dabei für definierte Ausfallszenarien Lernbeispiele zur Verfügung gestellt und für das Training der Klassifikationsmodelle verwendet werden. Je nach Anzahl vorhandener PMU-Messungen kann die Identifikation und Lokalisierung von Betriebsstörungen auf Leit- oder Stationsebene erfolgen. Bisherige Untersuchungen auf Übertragungs- und Verteilnetzebene umfassen u. a. die folgenden Betriebsstörungen:

- Kraftwerksausfälle,
- Ausfälle von EE-Anlagen,
- (partielle) Lastabwürfe,
- Kurzschlüsse und
- Leitungsausfälle.

Einige exemplarische Ausfallsimulationen sind in Abb. 7 für verschiedene Arbeitspunkte (stationärer Netzbetriebspunkt) veranschaulicht.

Zu den bisher untersuchten Lernverfahren gehören u. a. Support-Vektor-Maschinen, Entscheidungsbäume und Künstliche Neuronale Netze. Die prinzipielle Funktionsweise liefert Abb. 8. Die vom Klassifikationsmodell gelie-

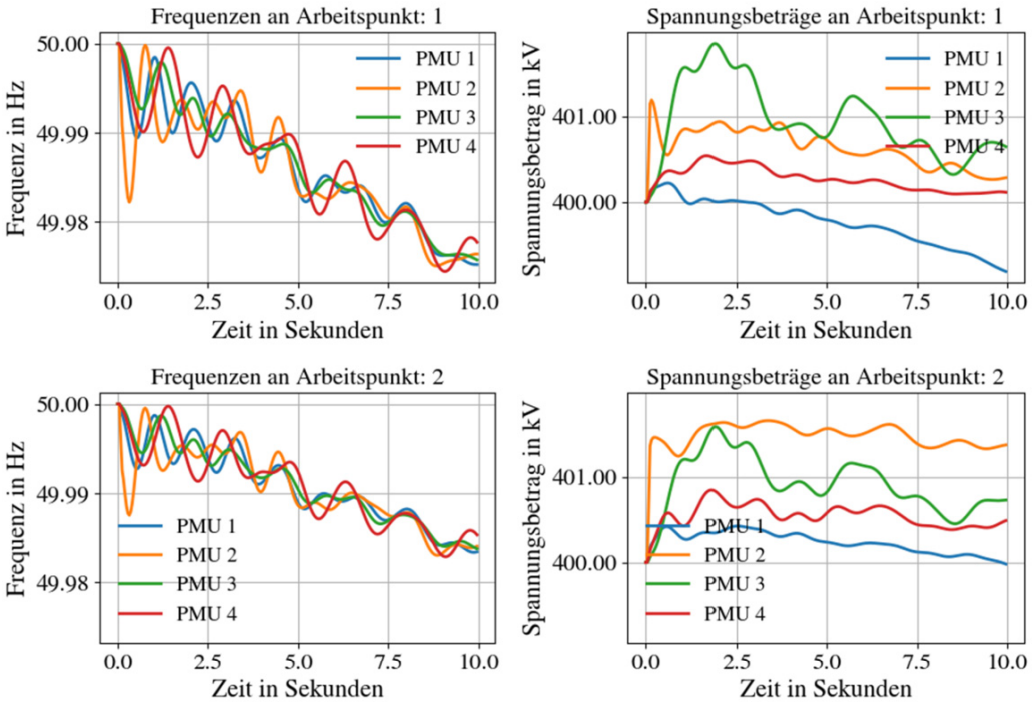

Abb. 7: Simulierte PMU-Signale an zwei stationären Netzbetriebspunkten (hier Arbeitspunkte) für den Ausfall eines PV-Kraftwerks.

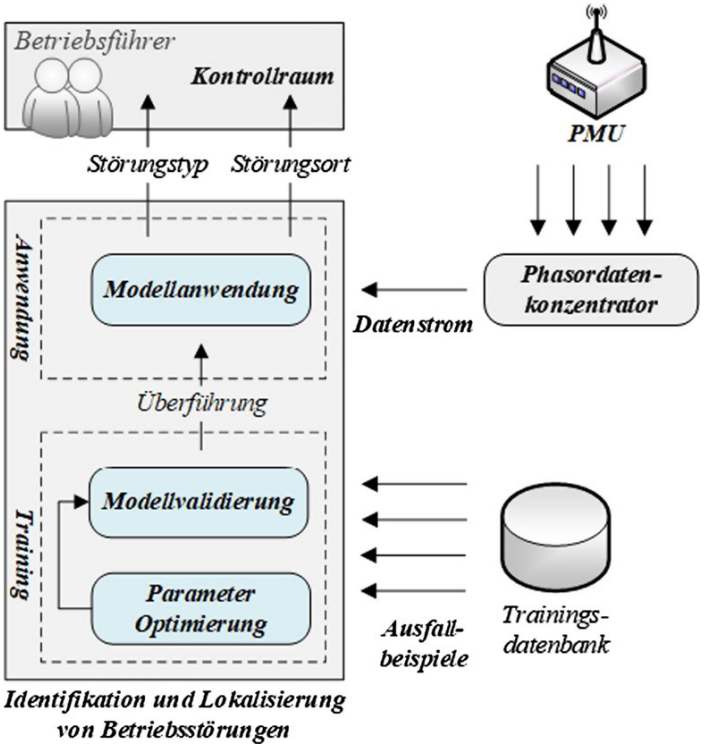

Abb. 8: Prinzipielle Funktionsweise der PMU-basierten Identifikation und Lokalisierung von Betriebsstörungen nach [50, 54].

ferten Informationen über Störungsort und Störungstyp können der Netzbetriebsführung zur Aktivierung passender Gegenmaßnahmen und Erhaltung der Versorgungsstabilität zur Verfügung gestellt werden. In [54] konnten für einige Klassifikationsverfahren Ausführungszeiten unterhalb von 9 ms und Klassifikationsgenauigkeiten zwischen 98-100 % erreicht werden.

4 Zusammenfassung und Ausblick

Der Einsatz digitaler Stationen auf Basis IEC 61850 bietet erstmalig eine vereinheitliche Kommunikation und Datenmodellierung auf Prozess-, Stations- und Leitebene und ermöglicht neue Schutz-, Regelungs- und Monitoring-Anwendungen. Aus Sicht der IT-Sicherheit und zur Erfüllung der allgemeinen Schutzziele (CIA Triad) sind entsprechende Einfallstore und strukturelle Schwachpunkte in digitalen Stationen neu zu bewerten und zu analysieren. Hierzu sind nach Abschnitt 1.2 ausgehend von dem Cyber-Kill-Chain Modell verschiedene aktive und passive IT-Angriffsarten zu berücksichtigen, da vorhandene Kommunikationsstandards in der Stationsautomatisierung IT-Sicherheitsmaßnamen nur unzureichend abbilden.

Zur Modellierung, Bewertung und Analyse der IT-Sicherheit in digitalen Stationen wird in Kapitel 2 eine Referenzarchitektur auf Basis eines IP-basierten Umspannwerks auf Verteilnetzebene vorgeschlagen. Dabei wird eine vereinheitlichte Kommunikation auf Basis IEC 61850 zwischen allen Stationskomponenten auf den Ebenen Prozessbus, Stationsbus und SCADA-Netzwerk umgesetzt. Der Prozessbus ist dabei redundant ausgeführt und erlaubt neben der Integration klassischer Stationsfunktionen wie Spannungsregelungs- oder Monitoring-Anwendungen eine zusätzliche Absicherung systemkritischer Funktionen (z. B. Schutzanwendungen). Zur Kopplung an überlagerte Leitsysteme stehen neben der IEC 61850 Kommunikation auch weitere Client-Server-basierte Übertragungsprotokolle wie IEC 60870-5-104 oder IEEE C37.118 zur Verfügung.

Zur umfassenden Untersuchung des dynamischen Systemverhaltens digitaler Stationen in gestörten und ungestörten Betriebssituationen sowie unter Berücksichtigung von IT-Angriffen wird eine cyber-physische Echtzeit-Co-Simulationsplattform vorgeschlagen (vgl. Abschnitt 3.1). Hierbei werden verschiedene Simulationsebenen unter Einbeziehung realer Betriebsmittel mittels präziser und hochdynamischer Echtzeitsimulationen in IT- und OT-Domäne abgebildet. Dies umfasst die elektrische Netzsimulation auf Basis von HYPERSIM von OPAL-RT mit zusätzlicher Unterstützung von Hardware-in-the-Loop Integrationen. Des Weiteren wird eine IKT-Netzwerksimulation über den diskreten Event-Simulator OMNeT++ zur Abbildung verschiedener Netzwerktopologien durchgeführt. Über einen parallelen Informationsaustausch auf Basis von IEC 61850 GOOSE und SV erfolgt die Kopplung und Synthese der elektrischen Netzsimulation mit der eventbasierten Netzwerksimulation über ein hybrides Co-Simulationssystem. Zur Aufrechterhaltung der Stabilität und Zeitsynchronität der Co-Simulation werden verschiedene Koordinierungsansätze beschrieben.

Die cyber-physische Echtzeit-Co-Simulationsplattform ist eine wichtige Voraussetzung zur Resilienzbewertung digitaler Stationen in Abschnitt 3.2. Dabei wird ein ganzheitliches, vierstufiges Phasenmodell vorgestellt zur Definition und Auswertung quantitativer und qualitativer Resilienzkriterien, der Identifikation potentieller Bedrohungen und Ausfälle und der Ableitung passender Gegenmaßnahmen. Hierzu gehören Maßnahmen aus Abschnitt 3.3 zur passiven Absicherung der Kommunikationswege zwischen digitaler Station und überlagerten Leitsystemen über Verschlüsselungstechnologien und Authentifizierungszertifikate. In Abschnitt 3.4 werden darüber hinaus verschiedene aktive IT-Sicherheitsmaßnahmen zur Erkennung cyber-physischer Anomalien vorgestellt. Ausgehend von einer kurzen Systematisierung physikalischer und virtueller Anomalien werden hierzu mehrere Online-Analysemethoden zur Detektion und Klassifikation von Anomalien auf Basis von IEC 61850 Sampled Values und IEEE C37.118 PMU-Daten eingeführt sowie exemplarische Ergebnisse beschrieben.

Weiterführende Arbeiten umfassen die weitere Umsetzung und Erprobung der cyber-physischen Echtzeit-Co-Simulationsplattform mit besonderem Fokus auf die effiziente Kopplung der verschiedenen Simulationsebenen. Darüber hinaus sind Technologien zur passiven Absicherung der Kommunikation innerhalb des Prozess- und Stationsbus zu prüfen. Bezüglich der cyber-physischen Anomalieerkennung erfolgen aktuell detaillierte Untersuchungen zur Entwicklung eines hybriden Netzwerk-IDS zur Detektion von IT-Angriffen in IEC 61850 MMS und IEEE C37.118 Datenpaketen. Ähnliche Arbeiten sind zur Auswertung von IEC 61850 GOOSE Telegrammen geplant. Im Rahmen der Digitalisierung von Stationen werden darüber hinaus Ansätze und Methoden der Nutzung Digitaler Zwillinge in Verteilnetzen untersucht. Dadurch können digitale dynamische Systemabbilder von Netzstrukturen oder auch Stationskomponenten in die bestehende Simulationsplattform integriert werden und ermöglichen eine engere Verzahnung zwischen technischem Prozess und Simulationsmodell.

Literatur

1. Bundesamt für Sicherheit in der Informationstechnik, *IT-Grundschutz-Kompendium*. Köln: Reguvis Bundesanzeiger Verlag; Bundesanzeiger Verlag, 2020.
2. Bundesamt für Sicherheit in der Informationstechnik (BSI), Ed., "Die Lage der IT-Sicherheit in Deutschland 2019," Broschüre BSI-LB19/508, Oct. 2019.
3. Power systems management and associated information exchange – Data and communications security, 62351-1, 2007.
4. J. Hong, C.-C. Liu and M. Govindarasu, "Integrated Anomaly Detection for Cyber Security of the Substations," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1643–1653, 2014, doi: 10.1109/TSG.2013.2294473.
5. A. Kummerow et al., "Challenges and opportunities for phasor data based event detection in transmission control centers under cyber security constraints," in *2019 IEEE Milan PowerTech*, Milan, Italy, Jun. 2019 – Jun. 2019, pp. 1–6.
6. Guidelines for smart grid cybersecurity: National Institute of Standards and Technology, 2014.
7. V. Delgado-Gomes, J. F. Martins, C. Lima and P. N. Borza, "Smart grid security issues," in *2015 9th International Conference on Compatibility and Power Electronics (CPE 2015): Costa da Caparica, Portugal, 24–26 June 2015*, Costa da Caparica, Portugal, 2015, pp. 534–538.
8. S. Sridhar, A. Hahn and M. Govindarasu, "Cyber–Physical System Security for the Electric Power Grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, 2012, doi: 10.1109/JPROC.2011.2165269.
9. Y. Yan, Y. Qian, H. Sharif and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," *IEEE Commun. Surv. Tutorials*, vol. 14, no. 4, pp. 998–1010, 2012, doi: 10.1109/SURV.2012.010912.00035.
10. U. Adhikari, "Event and intrusion detection systems for cyber-physical power systems," Dissertation, Department of Electrical and Computer Engineering, Mississippi State University, Mississippi State, Mississippi, 2015.
11. M. H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita, "Network Anomaly Detection: Methods, Systems and Tools," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 1, pp. 303–336, 2014, doi: 10.1109/SURV.2013.052213.00046.
12. M. Cheng, "Anomaly Detection in Cyber Physical Systems," Seattle, WA, Dec. 11 2018.
13. A. Khraisat, I. Gondal, P. Vamplew and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecur*, vol. 2, no. 1, p. 384, 2019, doi: 10.1186/s42400-019-0038-7.
14. C.-C. Liu, A. Stefanov, J. Hong and P. Panciatici, "Intruders in the Grid," *IEEE Power and Energy Mag.*, vol. 10, no. 1, pp. 58–66, 2012, doi: 10.1109/MPE.2011.943114.
15. A.-S. K. PATHAN, *State of the art in intrusion prevention and detection*. [Place of publication not identified]: CRC Press, 2016.
16. A. Ahmed et al., "Cyber Physical Security Analytics for Anomalies in Transmission Protection Systems," in *2018 IEEE Industry Applications Society Annual Meeting (IAS)*, Portland, OR, Sep. 2018 – Sep. 2018, pp. 1–8.
17. H. Lei, C. Singh and A. Sprintson, "Reliability Modeling and Analysis of IEC 61850 Based Substation Protection Systems," *IEEE Trans. Smart Grid*, vol. 5, no. 5, pp. 2194–2202, 2014, doi: 10.1109/TSG.2014.2314616.
18. S. Mohagheghi, J. Stoupis and Z. Wang, "Communication protocols and networks for power systems-current status and future trends," in *2009 IEEE/PES Power Systems Conference and Exposition*, Seattle, WA, USA, Mar. 2009 – Mar. 2009, pp. 1–9.
19. Y. Zhang, A. Sprintson and C. Singh, "An integrative approach to reliability analysis of an IEC 61850 digital substation," in *2012 IEEE Power and Energy Society General Meeting*, San Diego, CA, Jul. 2012 – Jul. 2012, pp. 1–8.
20. M. Golshani, G. A. Taylor and I. Pisica, "Simulation of power system substation communications architecture based on IEC 61850 standard," in *2014 49th International Universities Power Engineering Conference (UPEC)*, Cluj-Napoca, Romania, Sep. 2014 – Sep. 2014, pp. 1–6.
21. C. Brunner, "Implementation Guideline for Digital Interface to Instrument Transformers using IEC 61850-9-2".
22. G. R. Allen and R. Cheung, "Integration of protection, control and monitoring functions for transmission and distribution substations," *IEEE Trans. Power Delivery*, vol. 13, no. 1, pp. 96–101, 1998, doi: 10.1109/61.660859.
23. Q. Huang, S. Jing, J. Li, D. Cai, J. Wu and W. Zhen, "Smart Substation: State of the Art and Future Development," *IEEE Trans. Power Delivery*, vol. 32, no. 2, pp. 1098–1105, 2017, doi: 10.1109/TPWRD.2016.2598572.
24. J. Ma, T. Wang, J. Wu and Z. Wang, "Integration of protection and control systems for smart substation," in *2010 5th International Conference on Critical Infrastructure (CRIS)*, Beijing, China, Sep. 2010 – Sep. 2010, pp. 1–5.
25. *Fernwirkeinrichtungen und -systeme – Teil 5-104: Übertragungsprotokolle – Fernwirkeinrichtungen und -systeme – Teil 5-104: Übertragungsprotokolle – Zugriff für IEC 60870-5-101 auf Netze mit genormten Transportprofilen*, DIN EN 60870-5-104:2006 (IEC 60870-5-104:2006).
26. *Kommunikationsnetze und -systeme für die Automatisierung der elektrischen Energieversorgung – Teil 8-1: Spezifische Abbildung von Kommunikationsdiensten (SCSM) – Abbildungen auf MMS (nach ISO 9506-1 und ISO 9506-2) und ISO/IEC 8802-3*, IEC 61850-8-1:2011, 2011.
27. C. Brosinsky, A. Kummerow, A. Naumann, A. Kronig, S. Balischewski and D. Westermann, "A new development platform for the next generation of power system control center functionalities for hybrid AC-HVDC transmission systems," in *2017 IEEE Power & Energy Society General Meeting: 16–20 July 2017*, Chicago, IL, 2017, pp. 1–5.
28. *60255-118-1-2018 - IEEE/IEC International Standard – Measuring relays and protection equipment – Part 118-1: Synchrophasor for power systems – Measurements*. [Place of publication not identified]: IEEE, 2018.
29. *IEEE standard for synchrophasor data transfer for power systems*. New York: Institute of Electrical and Electronics Engineers, 2011.
30. *j60870 Overview – IEC 60870-5-104 – OpenMUC*. [Online]. Available: https://www.openmuc.org/iec-60870-5-104/ (accessed: Jun. 15 2020).
31. S. Sandi, B. Krstajic and T. Popovic, "pyPMU — Open source python package for synchrophasor data transfer," in *2016 24th Telecommunications Forum (TELFOR): Belgrade, Serbia, November, 22–23, 2016: proceedings of papers = XXIV*

Telekomunikacioni forum TELFOR 2016; zbornik radova, Belgrade, Serbia, 2016, pp. 1–4.
32. S. Ruhe and D. Rösch, "Design of a cyber-physical energy laboratory," in *Proceedings of International ETG Congress 2019: 08. – 09.05.2019 in Esslingen am Neckar*: VDE VERLAG GMBH Berlin Offenbach, 2019, pp. 153–158.
33. P. Palensky, A. A. van der Meer, C. D. Lopez, A. Joseph and K. Pan, "Cosimulation of Intelligent Power Systems: Fundamentals, Software Architecture, Numerics, and Coupling," *EEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 34–50, 2017, doi: 10.1109/MIE.2016.2639825.
34. C. Gomes, C. Thule, D. Broman, P. G. Larsen and H. Vangheluwe, "Co-simulation: State of the art," Feb. 2017. [Online]. Available: http://arxiv.org/pdf/1702.00686v1.
35. F. Cremona, M. Lohstroh, D. Broman, E. A. Lee, M. Masin and S. Tripakis, "Hybrid co-simulation: it's about time," *Softw Syst Model*, vol. 18, no. 3, pp. 1655–1679, 2019, doi: 10.1007/s10270-017-0633-6.
36. Jens Dede, Koojana Kuladinithi, Anna Foerster, Okko Nannen and Sebastian Lehnhoff, "OMNeT++ and Mosaik: Enabling Simulation of Smart Grid Communications."
37. "High_Level_Architecture_For_Simulation."
38. K. Thoma, Ed., *Resilien-Tech: "Resilience-by-Design"; Strategie für die technologischen Zukunftsthemen*. München: Utz, 2014.
39. S. Byfield, Ed., *Das Energiesystem resilient gestalten: Maßnahmen für eine gesicherte Versorgung*. München, Halle (Saale), Mainz: acatech – Deutsche Akademie der Technikwissenschaften; Deutsche Akademie der Naturforscher Leopoldina e.V. – Nationale Akademie der Wissenschaften; Union der Deutschen Akademien der Wissenschaften e.V, 2017. [Online]. Available: http://nbn-resolving.org/urn:nbn:de:gbv:3:2-106010.
40. M. Panteli and P. Mancarella, "The Grid: Stronger, Bigger, Smarter?: Presenting a Conceptual Framework of Power System Resilience," *IEEE Power and Energy Mag.*, vol. 13, no. 3, pp. 58–66, 2015, doi: 10.1109/MPE.2015.2397334.
41. S. Byfield, Ed., *Das Energiesystem resilient gestalten: Maßnahmen für eine gesicherte Versorgung*. München, Halle (Saale), Mainz: acatech – Deutsche Akademie der Technikwissenschaften; Deutsche Akademie der Naturforscher Leopoldina e.V. – Nationale Akademie der Wissenschaften; Union der Deutschen Akademien der Wissenschaften e.V, 2017. [Online]. Available: http://nbn-resolving.org/urn:nbn:de:gbv:3:2-106010.
42. Z. Bie, Y. Lin, G. Li and F. Li, "Battling the Extreme: A Study on the Power System Resilience," *Proc. IEEE*, vol. 105, no. 7, pp. 1253–1266, 2017, doi: 10.1109/JPROC.2017.2679040.
43. R. K. Mathew, A. S, and K. S, "Resilience assessment of Electric Power Systems: A scoping study," in *2016 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, Bhopal, India, Mar. 2016 – Mar. 2016, pp. 1–4.
44. S. M. Farooq, S. M. S. Hussain and T. S. Ustun, "Performance Evaluation and Analysis of IEC 62351-6 Probabilistic Signature Scheme for Securing GOOSE Messages," *IEEE Access*, vol. 7, pp. 32343–32351, 2019, doi: 10.1109/ACCESS.2019.2902571.
45. U. Adhikari, "Event and intrusion detection systems for cyber-physical power systems," Dissertation, Department of Electrical and Computer Engineering, Mississippi State University, Mississippi State, Mississippi, 2015.
46. R. Khan, A. Albalushi, K. Mclaughlin, D. Laverty and S. Sezer, "Model based Intrusion Detection System for Synchrophasor Applications in Smart Grid," in 2018. Accessed: Feb. 16 2018.
47. V. Chandola, A. Banerjee and V. Kumar, "Anomaly detection," *ACM Comput. Surv.*, vol. 41, no. 3, pp. 1–58, 2009, doi: 10.1145/1541880.1541882.
48. M. A.F. Pimentel, D. A. Clifton, L. Clifton and L. Tarassenko, "A review of novelty detection," *Signal Processing*, vol. 99, pp. 215–249, 2014, doi: 10.1016/j.sigpro.2013.12.026.
49. D. Rösch, S. Ruhe, K. Schäfer and S. Nicolai, "Local anomaly detection analysis in distribution grid based on IEC 61850-9-2 LE SV voltage signals," in *2019 International Conference on Smart Energy Systems and Technologies (SEST)*, Porto, Portugal, Sep. 2019 – Sep. 2019, pp. 1–6.
50. A. Kummerow, C. Brosinsky, C. Monsalve, S. Nicolai, P. Bretschneider and D. Westermann, "PMU-based online and offline applications for modern power system control centers in hybrid AC-HVDC transmission systems," in *Proceedings of International ETG Congress 2019: 08. – 09.05.2019 in Esslingen am Neckar*: VDE VERLAG GMBH Berlin Offenbach, 2019, pp. 405–410.
51. M. Biswal, S. M. Brahma and H. Cao, "Supervisory Protection and Automated Event Diagnosis Using PMU Data," *IEEE Trans. Power Delivery*, vol. 31, no. 4, pp. 1855–1863, 2016, doi: 10.1109/TPWRD.2016.2520958.
52. A. K. Singh and M. Fozdar, "Supervisory Framework for Event Detection and Classification using Wavelet Transform," in *Institute of Electrical and Electronics Engineers, Power & Energy Society et al. 2017 – IEEE PES General Meeting*, pp. 1–5.
53. R. Yadav, A. K. Pradhan and I. Kamwa, "Real-Time Multiple Event Detection and Classification in Power System using Signal Energy Transformations," *IEEE Trans. Ind. Inf.*, p. 1, 2018, doi: 10.1109/TII.2018.2855428.
54. A. Kummerow, C. Monsalve, S. Nicolai and P. Bretschneider, "Simultaneous online identification and localization of disturbances in power transmission systems," in *2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, Bucharest, Romania, Sep. 2019 – Oct. 2019, pp. 1–5.

Autoreninformationen

M. Sc. Dennis Rösch
Fraunhofer IOSB, IOSB-AST Ilmenau,
Fraunhofer-Institut für Optronik,
Systemtechnik und Bildauswertung,
Abteilung Energiesysteme,
Am Vogelherd 90, 98693 Ilmenau,
Deutschland
dennis.roesch@iosb-ast.fraunhofer.de

Dennis Rösch, M. Sc., ist wissenschaftlicher Mitarbeiter des Fraunhofer IOBS-AST. Hauptarbeitsgebiete: Modellierung und Simulation von Energie- und Kommunikationsnetzen, IT-Sicherheit von Energienetzen und –systemen

M. Sc. André Kummerow
Fraunhofer IOSB, IOSB-AST Ilmenau,
Fraunhofer-Institut für Optronik,
Systemtechnik und Bildauswertung,
Abteilung Energiesysteme,
Am Vogelherd 90, 98693 Ilmenau,
Deutschland
andre.kummerow@iosb-ast.fraunhofer.de

André Kummerow, M. Sc., ist wissenschaftlicher Mitarbeiter des Fraunhofer IOBS-AST. Hauptarbeitsgebiete: Einsatz maschineller Lernverfahren zur Überwachung von Energienetzen, Kommunikation und IT-Sicherheit in Energienetze

M. Sc. Cristian Monsalve
Fraunhofer IOSB, IOSB-AST Ilmenau,
Fraunhofer-Institut für Optronik,
Systemtechnik und Bildauswertung,
Abteilung Energiesysteme,
Am Vogelherd 90, 98693 Ilmenau,
Deutschland
cristian.monsalve@iosb-ast.fraunhofer.de

Cristian Monsalve, M. Sc., ist wissenschaftlicher Mitarbeiter des Fraunhofer IOBS-AST. Hauptarbeitsgebiete: Modellierung und Simulation elektrischer Netze, Integration von erneuerbaren Energien in elektrischen Netzen, Kommunikation für Energiesysteme.

M. Sc. Stephan Ruhe
Fraunhofer IOSB, IOSB-AST Ilmenau,
Fraunhofer-Institut für Optronik,
Systemtechnik und Bildauswertung,
Abteilung Energiesysteme,
Am Vogelherd 90, 98693 Ilmenau,
Deutschland
stephan.ruhe@iosb-ast.fraunhofer.de

Stephan Ruhe, M. Sc., ist wissenschaftlicher Mitarbeiter des Fraunhofer IOBS-AST. Hauptarbeitsgebiete: Modellierung und Simulation elektrischer Netze, Power-Hardware-in-the-Loop und echtzeitbasierte Simulationen, Erweiterung der Netzautomatisierung durch digitalisierte Infrastrukturen und neue Methoden zur Zustandserfassung

Dipl.-Ing. Steffen Nicolai
Fraunhofer IOSB, IOSB-AST Ilmenau,
Fraunhofer-Institut für Optronik,
Systemtechnik und Bildauswertung,
Abteilung Energiesysteme,
Am Vogelherd 90, 98693 Ilmenau,
Deutschland
steffen.nicolai@iosb-ast.fraunhofer.de

Dipl.-Ing. Steffen Nicolai ist Leiter der Gruppe „Elektrische Energiesysteme“ des Fraunhofer IOBS-AST und stellv. Leiter der Abteilung „Energiesysteme“. Hauptarbeitsgebiete: Projekt- und Konsortialleitung von Verbundprojekten im Bereich des sicheren und automatischen Betriebs elektrischer Energienetze und Cybersicherheit in der Energieversorgung. Strategische Entwicklung von Forschungsthemen im Bereich IT-Sicherheit in der Digitalen Station.

M. Sc. Kevin Schäfer
Fraunhofer IOSB, IOSB-AST Ilmenau,
Fraunhofer-Institut für Optronik,
Systemtechnik und Bildauswertung,
Abteilung Energiesysteme,
Am Vogelherd 90, 98693 Ilmenau,
Deutschland
kevin.schaefer@iosb-ast.fraunhofer.de

Kevin Schäfer, M. Sc., ist wissenschaftlicher Mitarbeiter des Fraunhofer IOBS-AST. Hauptarbeitsgebiete: Modellierung elektrischer Betriebsmittel, Echtzeitbasierte Simulation elektrischer Netze, Kommunikationsprotokolle digitaler Umspannwerke, Entwurf von IDS-Verfahren zur Überwachung der IT-Sicherheit