

VI. Bericht Arbeitspaket. 6

Analyse der Cybersicherheit

Mitglieder:

Prof. Dr. Djaffar OULD ABDESLAM, UHA

Bushra CANAAN, UHA

Yosra KADRI, UHA

Abderrazek BADJI, UHA



Interreg



Cofinancé par
l'Union Européenne
Kofinanziert von
der Europäischen Union

Rhin Supérieur | Oberrhein

VI.1. Kontext und Zielsetzung

Da sich die Oberrheinregion auf den Weg zu einer treibhausgasfreien Wirtschaftszone begibt, sind die Integrität, Zuverlässigkeit und Widerstandsfähigkeit ihrer zugrunde liegenden Energiesysteme von zentraler Bedeutung für den Erfolg dieser Initiative. Das Projekt CO2InnO unterstützt diesen Wandel durch die Demonstration und Bewertung klimaneutraler Technologien, darunter wasserstoffbasierte Kraft-Wärme-Kopplungsanlagen (KWK), nachhaltige Mobilitätslösungen und intelligente Energieinfrastrukturen. Diese Innovationen sind zwar umweltfreundlich, führen jedoch zu einer neuen Komplexität und digitalen Verflechtung, wodurch die Bedeutung der Cybersicherheit erheblich zunimmt.

In diesem Zusammenhang trägt das Arbeitspaket 6 (WP6) zur Cybersicherheit in Energiesystemen direkt zum sicheren und nachhaltigen Betrieb der wichtigsten Demonstratoren des Projekts bei. Es stärkt außerdem das Vertrauen der Interessengruppen, unterstützt die Einhaltung gesetzlicher Vorschriften und stellt sicher, dass der Übergang zur Klimaneutralität nicht nur technisch und wirtschaftlich machbar, sondern auch sicher und gesellschaftlich akzeptiert ist. Cybersicherheit ist ein Querschnittsthema, das alle wichtigen Komponenten des CO2InnO-Projekts betrifft. Die Echtzeit-Steuerungssysteme der Wasserstoff-KWK-Demonstratoren, die intelligente Ladeinfrastruktur für Elektromobilität und der datenintensive Betrieb moderner Energienetze basieren alle auf digitalen Systemen, die potenziell anfällig für Cyberangriffe sind. Eine Beeinträchtigung der Cybersicherheit in einem dieser Systeme könnte die Energieversorgung stören, die öffentliche Sicherheit gefährden, das Vertrauen der Nutzer untergraben und die übergeordneten Projektziele gefährden.

Durch die explizite und systematische Auseinandersetzung mit Cybersicherheit legt dieses Arbeitspaket den Grundstein für eine widerstandsfähige und vertrauenswürdige Energieinfrastruktur in der Oberrheinregion. Es unterstützt den „Living Lab“-Ansatz des CO2InnO-Projekts, indem es Cybersicherheitsaspekte in die technischen, rechtlichen und sozialen Dimensionen der Energiewende einbezieht. Die gewonnenen Erkenntnisse dienen auch als reproduzierbares Modell für andere Regionen, die ähnliche Transformationen durchführen.

Das Hauptziel dieses Arbeitspakets ist die Untersuchung, Entwicklung und Bewertung von Cybersicherheitsstrategien, die die Umsetzung dezentraler, digitaler und nachhaltiger Energielösungen unterstützen. Der Schwerpunkt liegt auf der Identifizierung von Schwachstellen, dem Verständnis der Bedrohungsdynamik und dem Vorschlag robuster, kontextspezifischer Erkennungs- und Abwehrstrategien.

Die Arbeit gliedert sich in drei miteinander verbundene Teilaufgaben:

6.1. Simulationsmodell eines realistischen Mikronetzes, einschließlich Berichterstattung über verschiedene Aspekte des Modelldesigns, zur Veranschaulichung der Herausforderungen bei seiner Entwicklung. Dazu gehört eine detaillierte Analyse der architektonischen Entscheidun-

gen, technischen Einschränkungen, Bedenken der Interessengruppen und rechtlichen Verpflichtungen. Der Bericht fasst die während der Projektdurchführung gewonnenen Erkenntnisse zusammen und enthält umsetzbare Empfehlungen für zukünftige Implementierungen.

6.2. KI-basierte Analyse zur Früherkennung von Cyberbedrohungen, die den Bedarf an proaktiven und adaptiven Sicherheitsmaßnahmen berücksichtigt. Ziel ist es, ein maschinelles lernbasiertes System zu entwickeln und zu evaluieren, das in der Lage ist, Anomalien und potenzielle Eindringversuche anhand von Betriebsdaten aus Komponenten des Energiesystems zu erkennen. Diese Aufgabe unterstützt die Automatisierung und Skalierbarkeit des Cybersicherheitsmanagements in komplexen, datenreichen Umgebungen.

6.3. Bericht über Sicherheitsaspekte in modernen intelligenten Zählern mit einer vergleichenden Analyse, wie sich unterschiedliche nationale und regionale Ansätze zur Datenerfassung und zum Datenschutz auf die Cybersicherheit auswirken. Diese Aufgabe untersucht, wie Politik, Regulierung und Markttrends die Gestaltung, den Einsatz und die Akzeptanz der Infrastruktur für intelligente Zähler beeinflussen, wobei der Schwerpunkt auf dem europäischen Kontext und der Oberrheinregion liegt.

Es ist zu beachten, dass das Arbeitspaket auch zwei zusätzliche Teilaufgaben umfasst, die nicht in den Geltungsbereich dieses Dokuments fallen. Teilaufgabe 6.4, die einen aktuellen Überblick über die Regulierung der Integration von cyber-physischer Sicherheit in Energiesysteme gibt, wird in dem speziellen Bericht des Partners HS Kehl behandelt. Ebenso wird Teilaufgabe 6.5, die sich auf die gesellschaftliche Akzeptanz intelligenter und vernetzter Geräte in Energiesystemen konzentriert, in dem Bericht des Partners KIT-DFIU vorgestellt. Folglich behandelt dieser Abschlussbericht ausschließlich die ersten drei Teilaufgaben.

Diese Aufgaben sind in die übergeordneten Forschungs- und Entwicklungsziele des CO2InnO-Projekts eingebettet und liefern wichtige Rückmeldungen für technische, rechtliche und gesellschaftliche Arbeitsbereiche. Die Ergebnisse stellen sicher, dass Cybersicherheit nicht als isoliertes technisches Problem behandelt wird, sondern als wichtiger Faktor für Innovation, Integration und Nutzerengagement.

Die Cybersicherheit von Energiesystemen hat in den letzten Jahren zunehmend Aufmerksamkeit auf sich gezogen, insbesondere mit dem Wachstum von Smart Grids, IoT-fähigen Geräten und dezentraler Energieerzeugung. Die Forschung hat Schwachstellen in Systemarchitekturen, Kommunikationsprotokollen und älteren Komponenten aufgezeigt. Darüber hinaus zeigen Studien, dass Cyberangriffe auf die Energieinfrastruktur immer häufiger, gezielter und raffinierter werden.

Im Bereich der intelligenten Messung haben Bedenken hinsichtlich Datenintegrität, Datenschutz und Fernausnutzung zu unterschiedlichen nationalen Ansätzen geführt, wodurch eine fragmentierte Regulierungslandschaft entstanden ist. Unterdessen entwickelt sich künstliche Intelligenz zu einem leistungsstarken Werkzeug für die Erkennung von Eindringlingen, deren

Wirksamkeit jedoch stark von der Qualität der Trainingsdaten, der kontextuellen Anpassung und der Fähigkeit abhängt, harmlose Anomalien von echten Bedrohungen zu unterscheiden. Trotz dieser Fortschritte bestehen weiterhin Lücken bei der Integration der Cybersicherheit in die frühzeitige Planung von Energiesystemen, insbesondere bei neuartigen Konfigurationen wie Wasserstoff-KWK. Auch gibt es nur wenige empirische Untersuchungen zur Wechselwirkung zwischen nationalen politischen Rahmenbedingungen und sicherheitsrelevanten Designentscheidungen bei Smart-Metering-Infrastrukturen.

Das Arbeitspaket basiert auf den folgenden Arbeitshypothesen.

- Dezentrale und datengesteuerte Energiesysteme erfordern grundlegend neue Ansätze für die Cybersicherheit. Die Hypothese lautet, dass traditionelle perimeterbasierte Sicherheitsmodelle unzureichend sind und dass integrierte, adaptive und datengestützte Modelle erforderlich sind.
- KI kann die Erkennung von Bedrohungen in dynamischen Energieumgebungen erheblich verbessern. Es wird erwartet, dass Methoden des maschinellen Lernens Cyber-Bedrohungen früher und genauer erkennen können als regelbasierte Systeme, vorausgesetzt, sie werden mit domänenrelevanten Daten trainiert und für Energieanwendungen kontextualisiert.
- Nationale Unterschiede in der Politik im Bereich Smart Metering wirken sich auf die Cybersicherheit aus. Diese Hypothese untersucht, wie unterschiedliche rechtliche und regulatorische Rahmenbedingungen in Deutschland und Frankreich die technische Konfiguration und Sicherheitslage von Smart-Metering-Systemen beeinflussen.

Basierend auf diesen Hypothesen verfolgt das Arbeitspaket die folgenden Teilziele.

- Dokumentation und Bewertung der Designherausforderungen und Lösungen im Zusammenhang mit der Cybersicherheit in den Demonstratoren des Projekts
- Untersuchung der KI-basierten Erkennung und Abwehr von Bedrohungen unter Verwendung projektspezifischer Daten und Szenarien.
- Analyse und Vergleich der Auswirkungen verschiedener nationaler Smart-Metering-Richtlinien auf die Cybersicherheit, mit Schwerpunkt auf Datenerfassung und Datenschutz.

VI.2. Methodik

Dieses Arbeitspaket kombiniert vier sich ergänzende Forschungsstränge, die sich sowohl mit aktuellen als auch mit neuen Herausforderungen in dezentralen Energiesystemen befassen. Der erste Teil enthält eine detaillierte Beschreibung des Entwurfs, der Umsetzung und der

Simulation eines realen Mikronetz-Demonstrators am „IUT de Mulhouse“ in UHA. Der Schwerpunkt liegt auf der Architektur des physischen Systems, der Integration erneuerbarer Energien und den ersten Schritten zur Entwicklung eines digitalen Zwillings als Grundlage für zukünftige cyber-physische Sicherheitsanwendungen. Dieses reale Mikronetz dient als vielseitiger Betriebsrahmen, der die Reproduzierbarkeit und zukünftige Einsatzszenarien für regionale Infrastrukturen im Oberrhein und in ganz Europa unterstützt.

Auf dieser Grundlage untersucht der zweite Teil KI-basierte Techniken zur Erkennung cyber-physischer Bedrohungen in Mikronetzumgebungen. Er beschreibt die Entwicklung und Erprobung von Deep-Learning-Modellen, insbesondere von LSTM-Rekurrenten Neuronalen Netzen, zur Erkennung von Anomalien in kritischen Energieflüssen. Dieser Teil zeigt auf, wie KI das Situationsbewusstsein verbessern und Frühwarnmechanismen für cyber-physische Störungen in dezentralen Energiesystemen bereitstellen kann.

Der dritte Teil konzentriert sich auf intelligente Messinfrastrukturen und die damit verbundenen Herausforderungen für die Cybersicherheit, insbesondere im Zusammenhang mit der grenzüberschreitenden Interoperabilität und den regionalen politischen Zielen im Oberrheinraum. Er untersucht den aktuellen Stand der Einführung intelligenter Zähler in Frankreich, Deutschland und der Schweiz, beleuchtet die technischen und rechtlichen Hindernisse, die deren Einführung beeinträchtigen, und analysiert die Schwachstellen, die sich aus der zunehmenden digitalen Vernetzung ergeben.

Der vierte Teil erweitert schließlich den Umfang der Arbeit, indem er die Aspekte Digitalisierung, Cybersicherheit und Resilienz eines hypothetischen wasserstoffbasierten Kraft-Wärme-Kopplungssystems (KWK) untersucht. In direktem Zusammenhang mit den übergeordneten Zielen des CO2InnO-Projekts dokumentiert er die potenziellen Architekturen, Schwachstellen und KI-gesteuerten Minderungsstrategien für wasserstoffbasierte Energieinfrastrukturen.

Zusammen bilden diese vier Stränge ein Kontinuum der europäischen Energiewende und verbinden heutige erneuerbare Mikronetze, KI-gestützte cyber-physische Sicherheit, die digitale Backbone-Infrastruktur für intelligente Zähler und zukünftige wasserstoffbasierte Systeme zu einem klimaneutralen, interoperablen und cyber-resilienten Rahmenwerk.

VI.2.1. Entwurf und Simulation eines realen Mikronetzes

Das Mikronetzsystem am „IUT de Mulhouse“ dient als modularer und flexibler Demonstrator für die Integration dezentraler erneuerbarer Energien. Es wurde entwickelt, um typische städtische Einsatzszenarien nachzubilden und gleichzeitig fortgeschrittene Forschung zu Steuerung, Simulation und cyber-physikalischer Sicherheit zu ermöglichen. Das physische System integriert Photovoltaik (PV)-Erzeugung, stationäre und mobile Energiespeicher, Stromumwandlungsgeräte und kommunikationsfähige Steuerungen.

Dieses Mikronetz steht im Einklang mit den übergeordneten Zielen des Projekts, nämlich der Erreichung von Klimaneutralität, der Förderung der dezentralen Erzeugung erneuerbarer

Energien und der Verbesserung der Widerstandsfähigkeit digitalisierter Energiesysteme. Die Entwurfsmethodik legt den Schwerpunkt sowohl auf operative Flexibilität als auch auf Hardware-Validierung, um sicherzustellen, dass die Ergebnisse auf reale Einsätze anwendbar sind und gleichzeitig für zukünftige Forschungsarbeiten in der Oberrheinregion und darüber hinaus skalierbar bleiben.

VI.2.2. **Struktur des Mikronetzes und Auswahl der Ausrüstung**

Der Mikronetz-Demonstrator umfasst modulare Erzeugungs-, Speicher- und Umwandlungseinheiten, die die aktuellen Einsatzpraktiken in kleinen städtischen und halbstädtischen Energienetzen widerspiegeln. Die installierte PV-Gesamtleistung beträgt 6,6 kWp und verteilt sich auf mobile und stationäre Anlagen, um Vergleichsanalysen und unterschiedliche Betriebszenarien zu ermöglichen. Diese diversifizierte Solarinfrastruktur unterstützt die Erfassung heterogener Datensätze, die für das Training von Algorithmen zur Anomalieerkennung und das Testen adaptiver Regelungsstrategien von entscheidender Bedeutung sind.

Das PV-Subsystem umfasst zwei Hauptkategorien von Anlagen. Die dynamischen PV-Tracker bestehen aus zwei unabhängig voneinander betriebenen Strukturen mit jeweils vier Solarmodulen und zwei Mikro-Wechselrichtern. Diese Tracker sind mit integrierten MPPT-Reglern (Maximum Power Point Tracking) ausgestattet, um die Energiegewinnung zu optimieren. Die mechanische Betätigung erfolgt über zwei Getriebemotoren, während integrierte Anemometer und Fernsteuerungssysteme ein sicheres Einfahren bei widrigen Wetterbedingungen gewährleisten. Im Gegensatz dazu bieten statische PV-Anlagen eine feste Solarstromerzeugungskapazität. Dazu gehört eine Fahrradunterstandsanlage mit acht festen Modulen, die auf einer Fläche von 13,2 m² eine Leistung von 2,16 kWp liefern. Durch die Kombination von mobilen und festen PV-Einheiten bildet das System „ die Vielfalt der städtischen Solaranwendungsszenarien nach und bereichert den Betriebsdatensatz des Mikronetzes.

Das Speichersubsystem verfügt ebenfalls über eine duale Struktur. Stationäre Batteriepacks bestehen aus zwei Modulen mit jeweils fünf Batterien und einer Gesamtkapazität von 24 kWp. Diese Batterien ermöglichen Energiespeicherung, Lastenausgleich und Spitzenlastabdeckung innerhalb des Mikronetzes. Ergänzt wird dieser stationäre Speicher durch ein mobiles Elektrofahrzeug (EV) mit einer 6,1-kWp-Batterie an Bord.

Für die Stromumwandlung und -steuerung integriert das Mikronetz mehrere Geräte.

- Mikro-Wechselrichter sind für die dynamischen PV-Tracker vorgesehen, die jeweils MPPT-Algorithmen für eine optimale Solarenergiegewinnung implementieren.
- Zwei einphasige DC/AC-Wechselrichter übernehmen die Umwandlung von Gleichstrom in netzkompatiblen Wechselstrom und gewährleisten so die Interoperabilität mit dem Versorgungsnetz.

- Für Speichersysteme werden bidirektionale DC/DC-Wandler eingesetzt, die über Proportional-Integral-Algorithmen (PI) mit Anti-Sättigungsmechanismen gesteuert werden, um ein stabiles Lade- und Entladeverhalten zu gewährleisten.

Die allgemeine Gesamtarchitektur des Mikronetz-Demonstrators und die darin fließenden elektrischen Ströme sind in Abbildung 1 unten dargestellt.

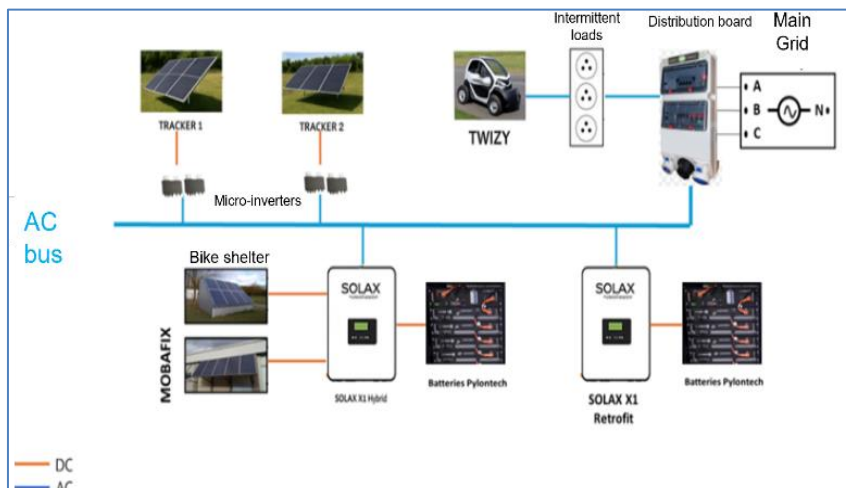


Abbildung VI-1: Allgemeine Architektur des Mikronetz-Demonstrators

VI.2.3. Modellierung und Simulation physikalischer Komponenten

Das Energiesystem und seine Komponenten werden mit MATLAB/Simulink unter Verwendung der Simscape Power Systems-Bibliothek modelliert. Die Simulationsumgebung kann sowohl als digitales Modell als auch als Plattform für die Erkennung von Anomalien und cyber-physikalische Experimente dienen.

Für die PV-Zellmodellierung wird jedes Photovoltaikmodul anhand eines elektrischen Äquivalenzmodells dargestellt, das auf Herstellerparametern, Sonneneinstrahlungsprofilen und Umgebungstemperatur basiert. Diese Modellierung ermöglicht eine genaue Vorhersage der Leistungsabgabe und unterstützt die Echtzeit-Verhaltensprognose.

Für MPPT wurde aufgrund seiner Einfachheit und Effektivität der Perturb-and-Observe-Algorithmus (P&O) ausgewählt. Er wird digital innerhalb des Simulationsrahmens implementiert, um die Regelungsleistung bei unterschiedlicher Sonneneinstrahlung zu bewerten.

Für die Batteriemodellierung wurde ein nichtlineares dynamisches Modell aus der SimPowerSystems-Batteriemodellbibliothek verwendet, um die Klemmenspannung zu simulieren und den Ladezustand (SoC) der Batterie zu schätzen. Dieses Modell unterstützt die Schätzgenauigkeit für Lade- und Entladeprofile. DC/DC-Wandler wurden so modelliert, dass sie bidirektionale Leistungsflüsse mit PI-basierter Regelung für die Stromregelung widerspiegeln. DC/AC-Wechselrichter verwendeten PWM-Strategien (Pulsweitenmodulation), um sinusförmige Ausgangsleistungen in Netzqualität zu synthetisieren.

Alle Steuerungsfunktionen werden über ein zentrales Framework koordiniert, das einen zuverlässigen Betrieb gewährleistet und eine externe Überwachung der Energieflüsse ermöglicht. Die Infrastruktur eignet sich daher gut für die spätere Integration von Digital-Twin-Technologien, die auf Echtzeit-Datenerfassung und -analyse basieren.

VI.2.4. Entwicklung digitaler Zwillinge

Aufbauend auf Modellierung, Simulation und Steuerungsvalidierung wurden Anstrengungen zur Entwicklung eines digitalen Zwillings (DT) des Mikronetzes unternommen. In Anerkennung der wachsenden Bedeutung digitaler Zwillinge für die Verbesserung der cyber-physischen Sicherheit wurde eine Literaturrecherche zu digitalen Zwillingen von Mikronetzen (MGDTs) durchgeführt. Diese Recherche konzentrierte sich auf ihre potenzielle Rolle bei der Verbesserung der Widerstandsfähigkeit gegen cyber-physische Bedrohungen und der Integration künstlicher Intelligenz für vorausschauende und adaptive Steuerung. Die Ergebnisse dieser Arbeit mündeten in einem detaillierten Artikel, der derzeit einem Peer-Review-Verfahren unterzogen wird und eine Klassifizierung von MGDTs nach Sicherheitsfunktionen vorschlägt sowie die Möglichkeiten für die Integration von KI in digitale Zwilling-Frameworks für die Cyber-Resilienz von Mikronetzen untersucht. Die Studie zeigt auch zukünftige Forschungsrichtungen auf, insbesondere in Richtung intelligenterer und sicherheitsorientierterer MGDTs.

Als praktischer Schritt zur Implementierung eines digitalen Zwillings des Mikronetz-Demonstrators in UHA wurden Benchmark-Bemühungen initiiert, um über mehrere Tage und unter unterschiedlichen Wetterbedingungen Echtzeit-Leistungsflussdaten zu sammeln. Abbildung 2 zeigt ein Beispieldiagramm der Mikronetz-Produktion und des Mikronetz-Verbrauchs, das über einen Zeitraum von 7 Stunden am 3. April 2025 erfasst wurde.

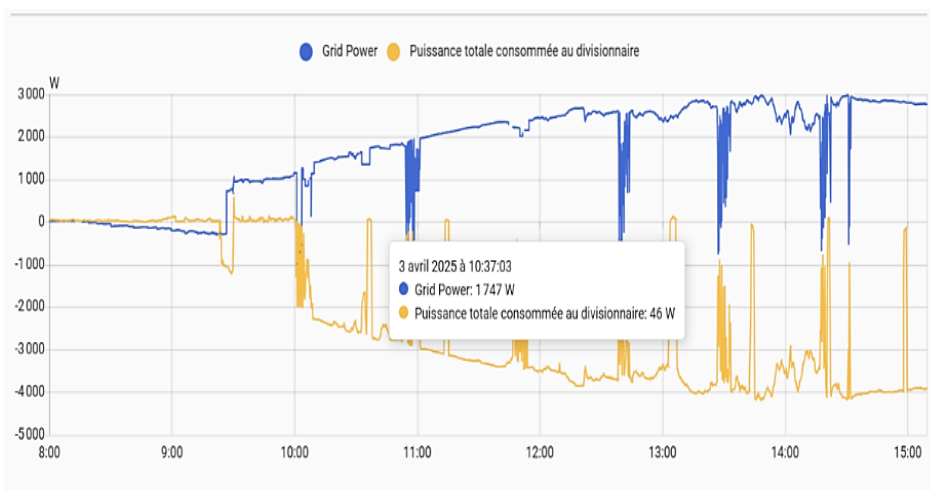


Abbildung VI-2 : Echtzeit-Diagramme zur Stromerzeugung und zum Stromverbrauch

Der daraus resultierende hochauflösende Datensatz erfasst das Systemverhalten in verschiedenen Betriebszuständen und dient zwei wichtigen Zwecken. Erstens bietet er eine empirische

Grundlage für die Entwicklung eines dynamischen, datengesteuerten digitalen Zwillings, der die sich entwickelnden Betriebsbedingungen des physischen Mikronetzes widerspiegeln kann. Zweitens unterstützt er das Training und die Validierung von KI-basierten Modellen zur Anomalieerkennung, Vorhersage oder Optimierung und schließt damit die Lücke zwischen aktuellen Mikronetz-Steuerungsstrategien und zukünftigen intelligenten cyber-physikalischen Frameworks.

Diese ersten Schritte in der Entwicklung digitaler Zwillinge bilden eine Roadmap für den Übergang des Mikronetz-Demonstrators zu einer fortschrittlicheren Forschungsplattform für cyber-physische Resilienz. Durch die Kombination einer sorgfältig instrumentierten physischen Infrastruktur mit Live-Daten-Benchmarking wird die Grundlage für die Integration KI-gesteuerter Funktionen geschaffen, die prädiktive Analysen, fortschrittliche Intrusion Detection und verbesserte Cybersicherheit ermöglichen.

VI.2.5. KI-basiertes Erkennungssystem für die Überwachung cyber-physikalischer Anomalien

Um die Sicherheit und Zuverlässigkeit des Mikronetzes zu gewährleisten, wurde ein Deep-Learning-basiertes Erkennungssystem unter Verwendung eines rekurrenten neuronalen Netzwerks mit Long Short-Term Memory (LSTM) entwickelt. LSTM-Modelle wurden aufgrund ihrer überlegenen Fähigkeit ausgewählt, langfristige Abhängigkeiten in Zeitreihendaten zu verarbeiten und das bei traditionellen rekurrenten neuronalen Netzen (RNNs) häufig auftretende Problem des verschwindenden Gradienten zu überwinden. Ihre Gated-Architektur ermöglicht es dem Netzwerk, relevante Informationen selektiv zu speichern und irrelevante Eingaben zu verwerfen, wodurch die Genauigkeit zukünftiger Vorhersagen verbessert wird. Das LSTM arbeitet in einem Closed-Loop-Modus und nutzt vergangene Ein- und Ausgänge, um den aktuellen Systemzustand zu schätzen, was seine Robustheit bei der Erkennung subtiler Anomalien, die durch cyber-physische Angriffe verursacht werden, verbessert.

Dieser Ansatz baut auf einer früheren Arbeit auf, die Teil des RES-TMO-Interreg-Projekts war, bei dem ein neuronales Netzwerk mit einem nichtlinearen autoregressiven Modell mit exogenen Eingaben (NARX) als intelligentes Erkennungssystem zur Überwachung des Wirkleistungsaustauschs am Point-of-Common-Coupling (PCC) eingesetzt wurde. Während das NARX-Netzwerk Anomalien in einfacheren Konfigurationen durch den Vergleich von vorhergesagten und tatsächlichen Sensorwerten erfolgreich erkannte, zeigte es Einschränkungen bei der Anwendung auf komplexere Steuerungssysteme mit mehrstufigen Batteriemanagementsystemen (BMS). Diese Einschränkungen ergaben sich unter anderem aus dem Problem des verschwindenden Gradienten, das die Fähigkeit des Netzwerks beeinträchtigte, langfristige Abhängigkeiten zu lernen.

Das aktuelle LSTM-basierte System wurde unter zwei Hauptkategorien von Angriffsszenarien

evaluiert. Die erste Kategorie umfasste Cyberangriffe wie False Data Injection (FDI) und Replay-Angriffe, bei denen kompromittierte Kommunikationskanäle es Angreifern ermöglichen, übertragene Messwerte zu verändern. Die zweite Kategorie zielte auf die physikalische Ebene ab, wo ein Eindringling das Batteriesteuerungsprogramm manipulieren konnte, um schädliche Auswirkungen zu verursachen. Zusammen ermöglichten diese Szenarien eine umfassende Bewertung der Fähigkeit des Systems, sowohl cyberphysische als auch physische Eingriffe in das Mikronetz zu erkennen und darauf zu reagieren.

VI.2.6. Intelligente Messinfrastruktur und Integration in KWK-Systeme

Der methodische Ansatz zur Untersuchung intelligenter Messsysteme im Rahmen des CO2InnO-Projekts kombinierte regulatorische, technische und betriebliche Perspektiven, um ein ganzheitliches Verständnis ihrer Rolle in zukünftigen dezentralen Energiesystemen zu ermöglichen. Es wurde eine vergleichende Analyse der Richtlinien und Praktiken für den Einsatz intelligenter Zähler in Frankreich, Deutschland und der Schweiz durchgeführt, wobei ein besonderer Schwerpunkt auf der Region Oberrhein lag. Diese Bewertung umfasste die Überprüfung der aktuellen Messinfrastrukturen, wie beispielsweise das französische Linky-System und die Gazpar-Gaszähler, die Wize-Technologie verwenden. Diese Ergebnisse wurden dann mit den sich entwickelnden Anforderungen der Sektorkopplung abgeglichen, wobei betont wurde, wie sich die Messinfrastrukturen weiterentwickeln müssen, um nicht nur elektrische Daten, sondern auch multivektoriellen Energieflüsse wie Wasserstoff zu berücksichtigen.

Die Methodik wurde dann erweitert, um zu untersuchen, wie intelligente Messinfrastrukturen die Integration von wasserstoffbasierten Kraft-Wärme-Kopplungsanlagen (KWK) unterstützen können. Dieser Schritt konzentrierte sich darauf, die zusätzlichen Datenanforderungen von KWK-Anlagen zu identifizieren, wie z. B. die Überwachung des Wasserstoffflusses, des Drucks und der Emissionen, und zu bewerten, wie IoT-fähige Kommunikationstechnologien wie LoRaWAN diese Anlagen innerhalb intelligenter Netze verbinden könnten. Während LoRa praktische Vorteile für dezentrale Systeme bietet, erfordern seine bekannten Sicherheitsbeschränkungen eine gezielte Risikobewertung, um Schwachstellen in Kommunikations-, Steuerungs- und Sicherheitssystemen zu beheben. Anhand einer szenariobasierten Modellierung wurde veranschaulicht, wie Cyberangriffe auf digitale Überwachungs- oder Sicherheitskontrollschleifen zu physischen Gefahren wie Kettenausfällen oder Explosionen eskalieren können. Durch die Abstimmung dieser methodischen Erkenntnisse mit dem breiteren politischen und implementierungstechnischen Kontext der intelligenten Messung im Oberrhein schuf die Forschung einen kohärenten analytischen Rahmen, der die Bereitschaft der digitalen Infrastruktur mit der sicheren und widerstandsfähigen Implementierung von Wasserstoff-KWK-Anlagen verbindet.

VI.2.7. Cybersicherheit und Resilienz von wasserstoffbasierten KWK-Systemen

Während sich der Mikronetz-Demonstrator auf aktuelle Technologien im Bereich der erneuerbaren Energien konzentriert, richtet das CO2InnO-Projekt den Blick auch auf zukünftige Infrastrukturen, die Wasserstoff als wichtigen Energieträger integrieren. Wasserstoffbasierte KWK-Systeme werden als wichtiger Bestandteil klimaneutraler Energienetze angesehen, da sie sowohl elektrische als auch thermische Energie liefern und gleichzeitig die Sektorkopplung zwischen Strom, Wärme und Mobilität ermöglichen. Die zunehmende Digitalisierung der Wasserstoff-Energieinfrastrukturen bringt jedoch neue Risiken mit sich, sodass Cybersicherheit und Resilienz zu wichtigen Forschungsbereichen werden.

Dieser Teil der Arbeit untersucht die Auswirkungen einer hypothetischen wasserstoffbasierten KWK-Anlage auf die Cybersicherheit. Der Schwerpunkt liegt auf konzeptionellen Architekturen, potenziellen Schwachstellen und Strategien zur Risikominderung, die in die zukünftige Konzeption und Entwicklung einfließen können.

Wasserstoff-KWK-Anlagen unterscheiden sich in mehrfacher Hinsicht von herkömmlichen KWK-Anlagen. Die Verwendung von Wasserstoff als Brennstoff führt zu einer neuen Betriebsdynamik, einschließlich der Notwendigkeit fortschrittlicher Speicherlösungen, komplexer Sicherheitsmanagementsysteme und sensibler Kommunikationsnetzwerke zur Überwachung von Druck, Temperatur und Gaszusammensetzung. Die Integration dieser Systeme in umfassendere Smart Grids erfordert sichere Schnittstellen zu SCADA-Systemen (Supervisory Control and Data Acquisition), cloudbasierten Energiemanagementplattformen und IoT-fähigen Sensoren. Jede dieser digitalen Schnittstellen vergrößert die Angriffsfläche für potenzielle Cyberbedrohungen. Abbildung 3 veranschaulicht die Integration von KWK in die Energieinfrastruktur und die damit verbundenen potenziellen Angriffsvektoren.

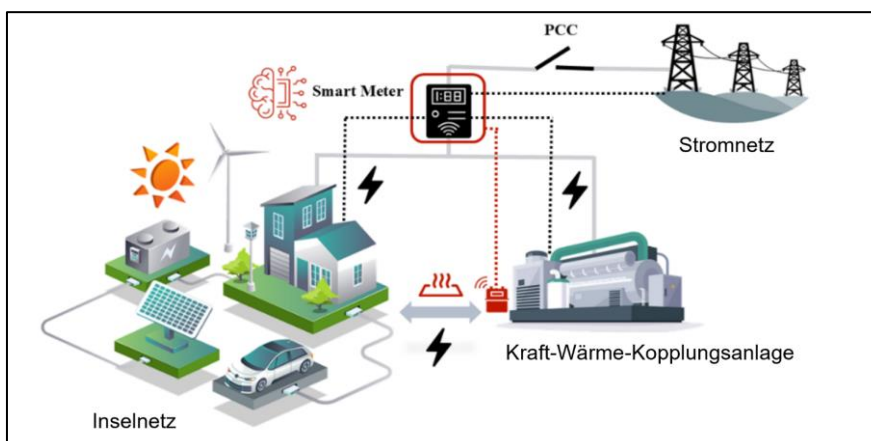


Abbildung VI-3 : CHP-Integration in Energiesysteme und Angriffsvektoren für Cybersicherheit

Cyber-physische Angriffe auf Wasserstoff-KWK könnten erhebliche Folgen haben, die von Betriebsstörungen bis hin zu physischen Sicherheitsrisiken reichen. Dazu gehört die Manipulation von Drucksensoren oder Durchflussregelventilen, was zu unsicheren Betriebsbedingungen

führen kann. Störungen der Echtzeit-Regelkreise können zu Ineffizienzen oder erzwungenen Abschaltungen führen, während die Fälschung von Datenströmen das Vorhandensein von Fehlern verschleiern und die Reaktionszeiten verzögern kann. Über die direkten physischen Konsequenzen hinaus könnten solche Angriffe auch die Integrität von Markttransaktionen gefährden und das Vertrauen der Stakeholder in Wasserstoffenergiesysteme untergraben.

Um diesen Risiken zu begegnen, untersucht die Studie, wie künstliche Intelligenz und digitale Zwillingstechnologien die Cybersicherheit verbessern können. Konzeptionelle Rahmenwerke veranschaulichen, wie KI in digitale Zwillinge integriert werden könnte, um eine kontinuierliche Überwachung und Erkennung von Anomalien zu ermöglichen. Ein solcher Ansatz würde es dem System ermöglichen, normale Betriebsmuster zu lernen und automatisch Abweichungen zu melden, die auf Cyberangriffe oder Fehler hindeuten könnten.

Resilienzstrategien für Wasserstoff-KWK gehen auch über die Erkennung von Anomalien hinaus. Sichere Kommunikationsprotokolle, Intrusion-Detection-Systeme und Redundanz in kritischen Steuerungskomponenten sind wichtige Maßnahmen, um sicherzustellen, dass eine Wasserstoff-KWK unter cyber-physikalischem Stress einen sicheren Betrieb aufrechterhalten kann. Darüber hinaus erfordert die Resilienz auf Systemebene koordinierte Reaktionsstrategien, die die KWK in die umgebenden Energienetze integrieren und sicherstellen, dass Störungen eingedämmt werden und eine schnelle Wiederherstellung erfolgt.

Unter Berücksichtigung dieser Elemente im Rahmen des CO2InnO-Projekts zeigt die Arbeit, dass Cybersicherheit für Wasserstoff-KWK keine isolierte Herausforderung ist, sondern Teil einer umfassenderen Energiewende. Die sichere Integration von Wasserstoffinfrastrukturen in digitalisierte Smart Grids erfordert eine Kombination aus robustem Hardware-Design, sicheren Softwarearchitekturen und intelligenter Überwachung auf Basis KI-gesteuerter Modelle.

VI.3. Ergebnisse

In diesem Abschnitt werden die Ergebnisse aus vier sich ergänzenden Bereichen vorgestellt. Der erste Teil befasst sich mit der Betriebsleistung des Mikronetz-Demonstrators unter verschiedenen Bedingungen und hebt dessen Fähigkeit hervor, Stabilität aufrechtzuerhalten, ein optimales Energiemanagement zu gewährleisten und auf Netzereignisse zu reagieren. Aufbauend auf dieser Validierung untersucht der zweite Teil den Einsatz von KI-basierten Techniken, insbesondere LSTM-Deep-Learning-Modellen, zur Erkennung cyber-physischer Bedrohungen im Mikronetzbetrieb. Diese Ergebnisse zeigen, wie eine fortschrittliche Anomalieerkennung die Widerstandsfähigkeit sowohl gegen digitale Eingriffe als auch gegen böswillige physische Eingriffe verbessern kann. Der dritte Teil analysiert die politischen und praktischen Rahmenbedingungen für Smart Metering in der Oberrheinregion und erweitert die Diskussion um regulatorische und grenzüberschreitende Integrationsherausforderungen. Der letzte Teil

stützt sich auf die vorangegangenen Diskussionen, um die Herausforderungen der Cybersicherheit und Digitalisierung von sektorverbundenen Infrastrukturen anzugehen, wobei der Schwerpunkt speziell auf wasserstoffbasierten KWK-Systemen liegt. Anhand eines anschaulichen Szenarios für einen cyber-physischen Angriff werden die Risiken hervorgehoben, die durch die zunehmende Vernetzung entstehen, und die Notwendigkeit einer integrierten KI-gestützten Überwachung und robuster Sicherheitsstrategien unterstrichen. Zusammengefasst bieten diese Ergebnisse einen ganzheitlichen Überblick über die physische und digitale Widerstandsfähigkeit zukünftiger dezentraler Energieinfrastrukturen.

VI.3.1. Leistungsvalidierung des realen Mikronetz-Demonstrators

Das Mikronetzsystem in UHA wurde entwickelt, um dezentrale erneuerbare Energiequellen, Speichereinheiten und Flexibilität auf der Nachfrageseite zu integrieren und dabei einen zuverlässigen Betrieb sowohl im netzgebundenen als auch im Inselbetrieb zu gewährleisten. Die in MATLAB/Simulink erzielten Simulationsergebnisse zeigen die Fähigkeit der Mikronetz-Steuerungsstrategien, dynamische Bedingungen, Netzstörungen und unterschiedliche Last- und Erzeugungsprofile zu bewältigen.

VI.3.2. Robustheit der Netzsynchrosation

Zur Bewertung der Stabilität der Phasenregelschleife (PLL) des Wechselrichters wurden zwei Netzfehlerszenarien simuliert. Zunächst wurde eine tiefe Spannungsabsenkung mit einer Amplitudenreduzierung von 90 % für 1 Sekunde angelegt. Wie in Abbildung 4 dargestellt, führte die Spannungsabsenkung zu keinem Verlust der PLL-Verriegelung. Der Wechselrichterstrom i_g blieb phasenausgerichtet und stabil mit minimaler harmonischer Verzerrung.

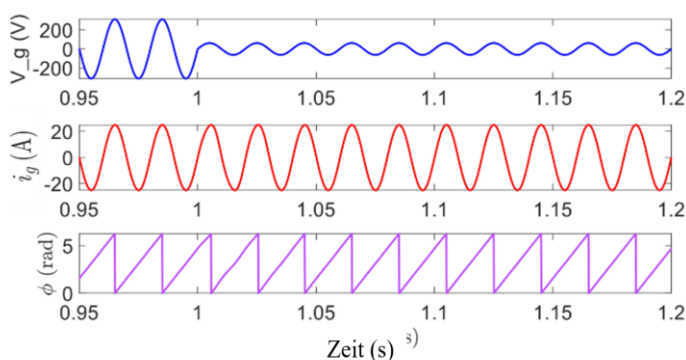


Abbildung VI-4 : Reaktion auf 90 % Spannungsabfall, Spannungs-, Strom- und Phasenwellenformen

Für das zweite Fehlerszenario wurde ebenfalls nach 1 Sekunde ein plötzlicher Phasensprung im Netz eingeführt. Die PLL verfolgte und korrigierte das verzerrte Netzsignal erfolgreich innerhalb eines Netzyklus mit minimalem Überschwingen, wie in Abbildung 5 zu sehen ist. Die schnelle Konvergenz verhinderte das Auftreten unerwünschter Zirkulationsströme und schützte empfindliche Lasten vor vorübergehender Instabilität.

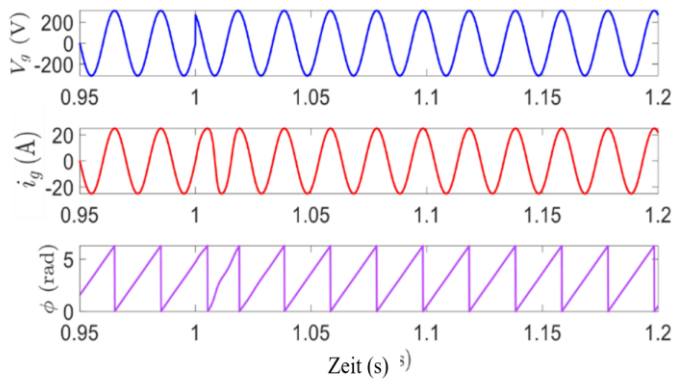


Abbildung VI-5 : PLL-Reaktion auf Phasensprung

Diese Tests bestätigten eine starke Synchronisationsresilienz unter schweren Störungen.

VI.3.3. Normalbetrieb bei variablen Sonneneinstrahlungswerten

Ein zeitlich variierendes Leistungsstrahlungsprofil reproduzierte Bedingungen bei klarem Himmel, Schwankungen und Verschattung. Abbildung VI-6 zeigt, wie die PV-Stromerzeugung den Strahlungsmustern genau folgte. Die Ergebnisse des kompletten Systems, dargestellt in Abbildung VI-7, bestätigen, dass der Strom I_g der Referenz mit einer akzeptablen Reaktionszeit perfekt folgt. Die Amplitude von I_g stimmt ebenfalls mit der Referenz überein und spiegelt das Sonneneinstrahlungsprofil wider. Die Spannungen V_g und U_{dc} behalten ihre Anfangswerte bei, was eine korrekte Regelung der Gleichstrom-Bussspannung belegt.

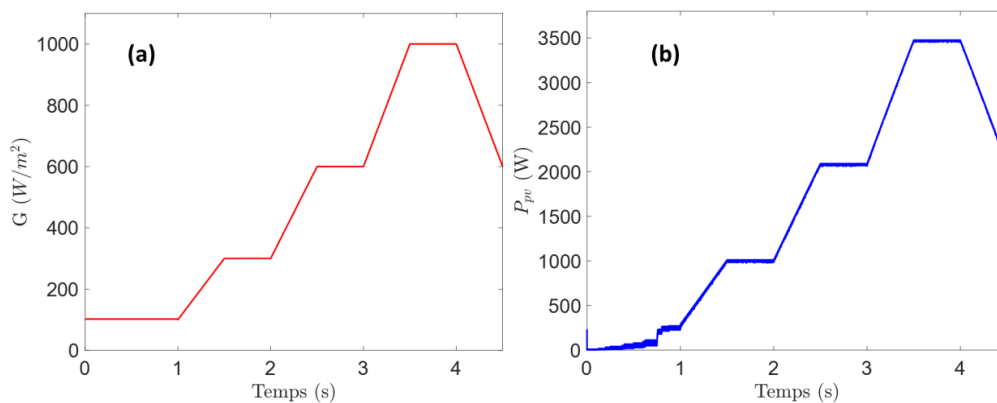


Abbildung VI-6 : Stationäre PV-Modulproduktion unter wechselnden Sonnenbedingungen (a) Strahlungsprofil (b) Solarstromerzeugungprofil

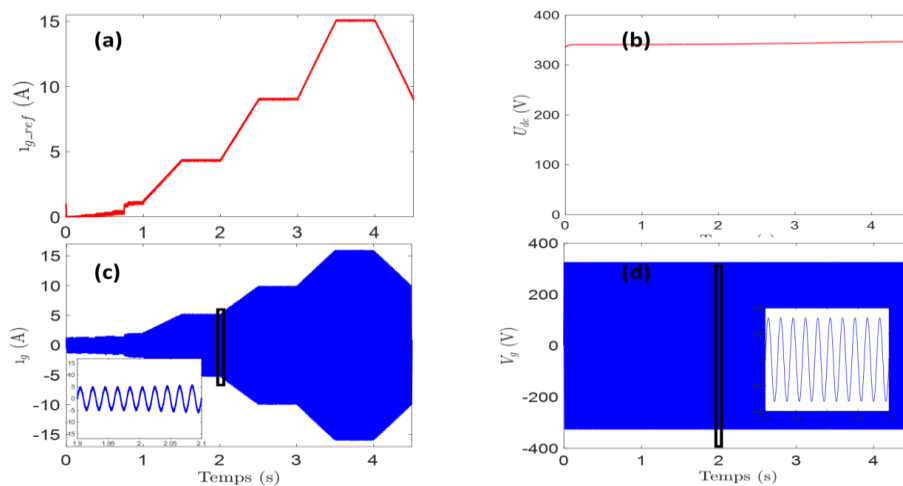


Abbildung VI-7 : Ergebnisse der Wechselrichterleistung. (a) Netzreferenzstromprofil (b) Gleichstrom-Bussspannung (c) Netzwechselstrom (d) Netzspannung

Dies deutet auf eine effektive Regelung und eine stabile Stromabgabe auch bei schwankenden erneuerbaren Eingängen hin.

VI.3.4. Energiemanagementstrategie

Um die Leistung des implementierten Energiemanagementsystems zu validieren, wurde über mehrere Tage hinweg eine eingehende Beobachtungsstudie unter verschiedenen Betriebsbedingungen durchgeführt, ein e Szenarien mit und ohne Anschluss eines Elektrofahrzeugs (EV). Wichtige elektrische Parameter wie Spannung, Strom und Leistungsabgabe der Photovoltaikmodule (PV) sowie die Wechselrichterleistung wurden kontinuierlich an mehreren Punkten der Anlage gemessen. Diese Messungen ermöglichten eine detaillierte Bewertung der gesamten Energieverfügbarkeit, des Ladezustands der Batterien, des Gesamtverbrauchs und der bidirektionalen Energieflüsse zwischen dem Mikronetz und dem externen Versorgungsnetz.

Die Analyse bestätigte, dass das Hybridsystem den direkten Einsatz lokal erzeugter Solarenergie zur Versorgung der Last priorisiert, wobei die Wechselrichter so konfiguriert sind, dass sie den PV-Strom zu den Verbrauchsstellen leiten, bevor andere Ressourcen in Anspruch genommen werden. Wenn die PV-Produktion nicht ausreichte, ergänzten die Batteriepacks nahtlos die Energieversorgung und sorgten so für Ausgewogenheit und Kontinuität. Nur in Fällen, in denen sowohl die PV-Erzeugung als auch die Batteriereserven unzureichend waren, bezog das Mikronetz Strom aus dem externen Netz. Darüber hinaus bestätigte die Studie, dass das Laden der Batterien streng auf die überschüssige Solarstromproduktion beschränkt war, was das Ziel der Maximierung des Eigenverbrauchs und der Minimierung der Abhängigkeit von externen Quellen untermauerte. Diese Ergebnisse belegen die Wirksamkeit der umgesetzten Energiemanagementstrategie bei der Optimierung der Ressourcennutzung und der Aufrechterhaltung eines stabilen Betriebs unter dynamischen Last- und Erzeugungsbedingungen.

Diese Ergebnisse bestätigen, dass der Mikronetz-Demonstrator sowohl unter gestörten als

auch unter normalen Netzbedingungen Stabilität gewährleisten kann, während sein Energiemanagement-Framework die lokale Nutzung erneuerbarer Energien effektiv maximiert und Zusatzdienste unterstützt.

VI.3.5. LSTM-basierte Erkennungsleistung für cyber-physische Angriffe

In diesem Abschnitt werden die Ergebnisse des Trainings des LSTM-basierten Erkennungssystems vorgestellt und dessen Leistung unter verschiedenen cyber-physikalischen Angriffsszenarien, die auf das Mikronetz abzielen, bewertet. Die Analyse konzentriert sich zunächst auf die Fähigkeit des Modells, die Wirkleistung am gemeinsamen Kopplungspunkt (Ppcc) unter normalen Betriebsbedingungen zu lernen und vorherzusagen, gefolgt von seiner Reaktion auf Cyberangriffe auf die Kommunikationsebene und physische Eingriffe auf der Steuerungsebene.

VI.3.6. LSTM-Trainingsergebnisse

Das LSTM-basierte Erkennungssystem wurde so trainiert, dass es den Ppcc direkt vorhersagt und den Zwischenschritt der Schätzung des Batteriezustands umgeht. Dieser direkte Ansatz erwies sich als vorteilhaft für die Erkennung mehrerer Betriebsbedingungen, da er die Erkennung von Angriffen auch dann ermöglicht, wenn das Batteriemanagementsystem (BMS) unter komplexen Steuerungsschemata arbeitet. Es wurden drei Konfigurationen getestet, deren Ergebnisse in den Vergleichsdiagrammen in Abbildung VI-8 dargestellt sind. In ersten Tests wurde ein Netzwerk mit einer einzigen LSTM-Schicht aus 200 versteckten Einheiten in Kombination mit einer vollständig verbundenen Schicht verwendet und mit einem Datensatz von 1000 Sekunden trainiert. Diese Konfiguration (Istm1) lieferte zwar im Allgemeinen genaue Ergebnisse, es wurden jedoch geringfügige Störungen und gelegentliche Fehleinschätzungen beobachtet.

Diese Ungenauigkeiten konnten deutlich reduziert werden, als der Trainingsdatensatz auf 4000 Sekunden erweitert wurde, was zu einer verbesserten Leistung der zweiten Konfiguration (Istm2) führte. Die besten Ergebnisse wurden jedoch mit einer tieferen Architektur erzielt, die aus zwei gestapelten LSTM-Schichten (Istm3) bestand und eine optimale Schätzleistung erzielte. Die Trainingsergebnisse von Istm3 zeigten unter normalen Bedingungen hochstabile Vorhersagen mit minimalen Abweichungen.

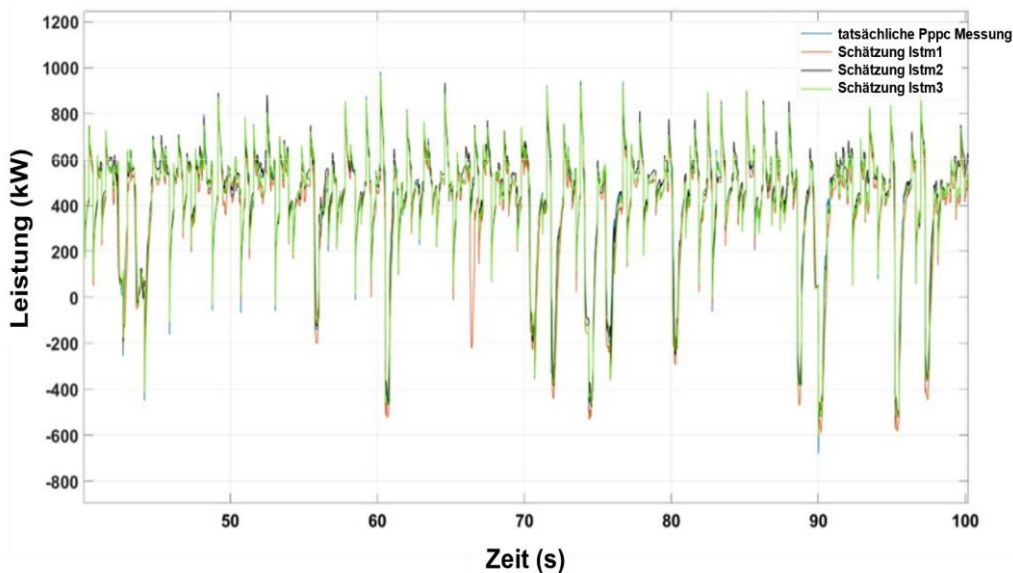


Abbildung VI-8 : Vorhergesagte Leistung der drei Konfigurationen im Vergleich zur tatsächlichen Messung

Abbildung VI-9 zeigt die Leistungsindikatoren Root Mean Square Error (RMSE) und Loss von Istm3 im Detail.

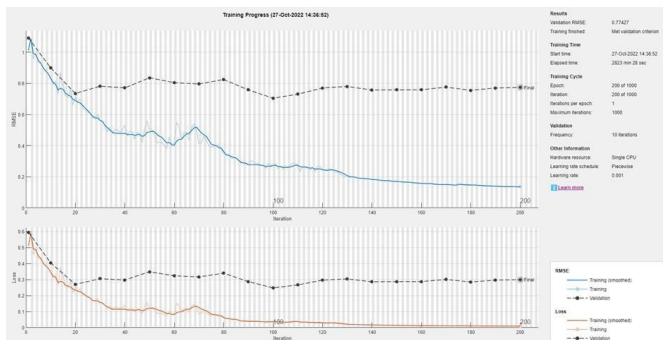


Abbildung VI-9 : Trainingsergebnisse der Istm3-Konfiguration

VI.3.7. Cyber-physische Angriffsszenarien und Bewertung

Sobald das Modell eine stabile Basisleistung erreicht hatte, wurde es unter verschiedenen cyber-physikalischen Angriffsszenarien bewertet.

Für den FDI-Angriff (False Data Injection) auf die PV-Produktion wurde in der 20. Sekunde des Tests ein Überproduktionssignal injiziert. Diese Art von Angriff ahmt betrügerisches Verhalten nach, das darauf abzielt, Förderprogramme durch künstliche Aufblähung der gemeldeten PV-Erzeugung zu manipulieren. Der Angriff verursachte eine sofortige Abweichung zwischen dem physikalisch gemessenen Ppcc und dem von LSTM geschätzten Signal, die in Abbildung VI-10 (a) und im Fehlerdiagramm in Abbildung VI-10 (b). Im Gegensatz zu vorübergehenden Störungen, die in der Regel isolierte Fehlerspitzen erzeugen, führte dieser Angriff zu einer anhaltenden Diskrepanz zwischen gemessenen und geschätzten Werten, was auf eine absichtliche Manipulation der Daten hindeutet.

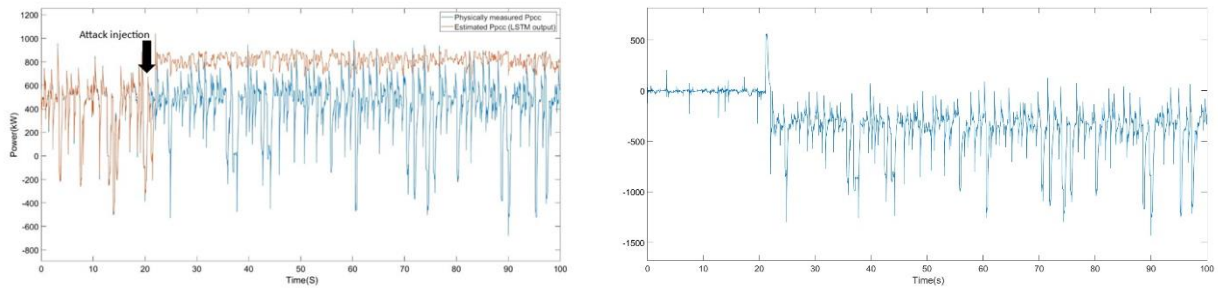


Abbildung VI-10 : LSTM-Vorhersage vor und nach der FDI-Angriffsinjektion (a) Signaldiagramm (b) Fehlerdiagramm

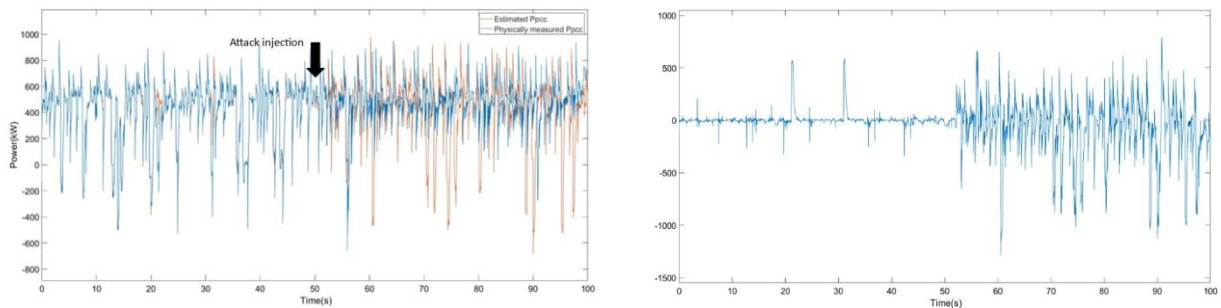


Abbildung VI-11 : LSTM-Vorhersage vor und nach der Injektion des Replay-Angriffs (a) Signaldiagramm (b) Fehlerdiagramm

Anschließend wurde in der 50. Sekunde eines weiteren Tests ein Replay-Angriff durchgeführt. In diesem Szenario wurde ein zuvor aufgezeichnetes PV-Produktionsprofil aus günstigen Bedingungen wiedergegeben, um das System in die Irre zu führen. Solche Angriffe sind besonders schwierig, da die injizierten Messungen einer vollkommen gültigen Verteilung folgen, die aus demselben System stammt. Trotzdem konnte das LSTM-Modell die Anomalie erfolgreich erkennen, wie die anhaltende Abweichung zwischen den Echtzeitmessungen und den vorhergesagten Werten zeigt (Abbildung VI-11 (a)). Diese Diskrepanz war in der Fehlergrafik in Abbildung VI-11(b) noch deutlicher zu erkennen, wo die kontinuierliche Abweichung den Angriff klar von normalen Betriebsschwankungen unterschied.

Über Cyberangriffe hinaus wurde das System auch auf physikalische Eingriffe getestet, insbesondere auf ein Szenario mit erzwungener Ladung. Hier gab der Angreifer einen Befehl aus, der die BMS-Beschränkungen umging und das Laden der Batterie unter ungünstigen Bedingungen initiierte. Diese Manipulation, zwang die Batterie, Energie zu beziehen, obwohl sie dies nicht sollte, was das Mikronetz belasten oder sogar zu einer Verschlechterung des Speichersystems führen konnte. In diesem Test verursachte der Befehl zum erzwungenen Laden eine deutliche Abweichung der gemessenen Ppcc-Kurve vom geschätzten Signal, wie in Abbildung 12 dargestellt, was die Fähigkeit des LSTM unterstreicht, Anomalien über die Kommunikationsebene hinaus zu erkennen.

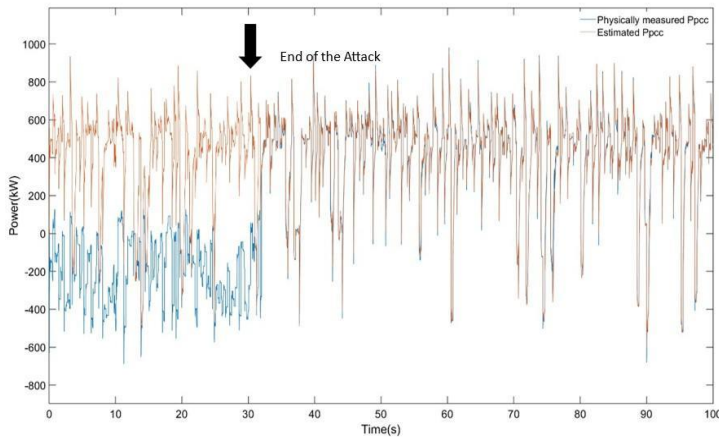


Abbildung VI-12 : Erzwungener Ladeangriff auf die Batterie bis zur 30. Sekunde

Insgesamt bestätigen diese Ergebnisse, dass das LSTM-basierte Erkennungssystem effektiv zwischen vorübergehenden Störungen und konsistenten Abweichungen unterscheiden kann, die auf cyber-physische Angriffe hindeuten. Seine Fähigkeit, sowohl cyber-verursachte falsche Daten als auch physikalisch induzierte Betriebsanomalien zu erkennen, macht es zu einem robusten Werkzeug zur Verbesserung der Sicherheit von Mikronetzen.

Diese Fähigkeit ist besonders relevant, wenn man die Integration komplexerer Infrastrukturen in Betracht zieht, wie z. B. wasserstoffbasierte KWK-Systeme, bei denen das Zusammenspiel zwischen digitaler Überwachung und physischer Sicherheit noch kritischer wird. Die nachgewiesene Robustheit des LSTM-Ansatzes bietet eine solide Grundlage für die Ausweitung ähnlicher Erkennungsstrategien zum Schutz zukünftiger sektorverbundener Energienetze.

VI.3.8. Vergleichende Analyse der Politik und Praxis im Bereich Smart Metering im Oberrhein

Über die operative Validierung des Mikronetz-Demonstrators und die KI-basierte Sicherheitsanalyse hinaus untersuchte das Projekt die breitere Digitalisierungslandschaft dezentraler Energiesysteme durch intelligente Messtechnologien. Es wurde eine vergleichende Studie zum aktuellen Stand der intelligenten Messinfrastrukturen in den Ländern des Oberrheins durchgeführt.

Die Oberrheinregion, die Teile Frankreichs, Deutschlands und der Schweiz umfasst, bietet einen einzigartigen Kontext, da sie unterschiedliche nationale Rechtsrahmen innerhalb eines geografisch vernetzten Energiemarktes umfasst. Es wurden mehrere grenzüberschreitende Initiativen zur Harmonisierung der Energiepolitik und -praxis ins Leben gerufen.

Das Programm Interreg VI-A Frankreich-Deutschland-Schweiz (2021–2027) zielt darauf ab, intelligente Energiesysteme, einschließlich intelligenter Netze und IKT-Systeme, zu entwickeln, um die Energiewende und die ökologische Nachhaltigkeit in der Region zu fördern (Europäische Kommission, 2021).

Ein weiteres bemerkenswertes Projekt ist die Smart Border Initiative zwischen Frankreich und

Deutschland, die sich auf die Integration von Smart-Grid-Technologien konzentriert, um die Energieeffizienz und die Sektorkopplung in den Regionen Saarland (DE) und Lothringen (FR) zu verbessern. Diese Initiative zielt darauf ab, kostengünstige Lösungen zur Verbesserung der Sicherheit und zur Förderung von Investitionen in erneuerbare Energien anzubieten (Europäische Kommission, 2019).

Trotz dieser gemeinsamen Bemühungen bestehen weiterhin Diskrepanzen zwischen den politischen Absichten und der praktischen Umsetzung. Während Frankreich beispielsweise durch sein Linky-Programm erhebliche Fortschritte bei der Einführung intelligenter Zähler erzielt hat, kam es in Deutschland aufgrund rechtlicher und bürokratischer Herausforderungen zu Verzögerungen, sodass laut jüngsten Bewertungen nur eine Durchdringungsrate von 14 % erreicht wurde (De Paola et al., 2023). Die Schweiz hingegen hat eine gesetzliche Vorgabe für eine Abdeckung von 80 % mit intelligenten Zählern bis 2027, hatte aber nach den neuesten Daten nur 20 % erreicht, was auf eine erhebliche Lücke zwischen den politischen Zielen und den tatsächlichen Fortschritten hindeutet (Brightly Energy, 2024).

Öffentlich-private Partnerschaften (ÖPP) haben eine entscheidende Rolle bei der Förderung der Sicherheit intelligenter Stromnetze in der Region gespielt. In Frankreich wurde bei der Einführung der intelligenten Gaszähler Gazpar durch GRDF die Wize-Technologie eingesetzt, ein Protokoll für ein energiesparendes Weitverkehrsnetz, das in Zusammenarbeit zwischen öffentlichen Versorgungsunternehmen und privaten Unternehmen wie Suez und Sagemcom entwickelt wurde. Diese Partnerschaft ermöglichte die Integration sicherer, effizienter Kommunikationstechnologien in die nationale Gasmessinfrastruktur (Wize Alliance, o. J.).

In ähnlicher Weise ist die Smart Border Initiative ein Beispiel für grenzüberschreitende ÖPP, bei der Enedis (FR) und Energis-Netzgesellschaft mbH (DE) zusammenarbeiten, um ein intelligentes Stromnetz zu implementieren, das Flexibilität in Verbindung mit intelligenter Mobilität und Energieeffizienz integriert und damit die Sicherheit erhöht und Investitionen in erneuerbare Energien fördert (Europäische Kommission, 2019).

Zusammenfassend lässt sich sagen, dass die praktischen Auswirkungen für grenzüberschreitende Projekte erheblich sind. Die französischen Systeme sind technisch bereit für schnelle datengesteuerte Dienste, stehen jedoch aufgrund unterschiedlicher Datenformate und Sicherheitsprotokolle vor potenziellen Interoperabilitätsproblemen mit deutschen und schweizerischen Zählern. Deutsche Systeme legen den Schwerpunkt auf Cybersicherheit und Datenschutz, verzögern jedoch die vollständige Realisierung digitaler Flexibilitätsmärkte. Schweizer Implementierungen betonen die Integration mehrerer Energiearten, bleiben jedoch aufgrund der kantonalen Verwaltung fragmentiert.

Für transnationale Initiativen wie CO2InnO ist die Harmonisierung von Datenstandards und Interoperabilitätsanforderungen von entscheidender Bedeutung. Ohne ein gemeinsames Datenaustauschprotokoll und kompatible Sicherheitszertifizierungssysteme wird die Integration

von Smart-Metering-Daten in regionale Mikronetze zu einer mühsamen Angelegenheit. Diese Heterogenität könnte die Schaffung grenzüberschreitender Demand-Response-Programme behindern oder die Einführung von KI-basierten regionalen Energieoptimierungstools verzögern.

VI.3.9. Cybersicherheit und Digitalisierung in Wasserstoff-KWK-Systemen

Nach der vergleichenden Analyse der Smart-Metering-Strategien und -Praktiken in der Oberrheinregion wird deutlich, dass die zukünftige Entwicklung von Smart Grids nicht allein auf die Strommessung beschränkt sein kann. Die Integration von wasserstoffbasierten Kraft-Wärme-Kopplungsanlagen (KWK) ist ein entscheidender Schritt zur Förderung der Sektorkopplung und zur Stärkung der Widerstandsfähigkeit dezentraler Energiesysteme. Im Rahmen des CO2InnO-Projekts werden diese Anlagen als strategische Ressourcen angesehen, die die intermittierende Erzeugung erneuerbarer Energien ergänzen und gleichzeitig flexible, bidirektionale Energieflüsse unterstützen. Ihr Einsatz bringt jedoch zusätzliche Komplexität mit sich, insbesondere im Hinblick auf die cyber-physische Sicherheit, da diese Systeme auf umfangreiche digitale Überwachungs- und Kommunikationsinfrastrukturen angewiesen sind.

VI.3.10. Auswirkungen der Integration intelligenter Messsysteme auf die cyber-physische Sicherheit

Wasserstoff-KWK-Anlagen sind zunehmend auf IoT-fähige Sensorplattformen angewiesen, um Echtzeit-Einblick in Leistungskennzahlen, Wasserstoffdurchflussraten, Druckniveaus und Emissionen zu erhalten. Die LoRaWAN-Technologie (Long Range Wide Area Network) hat sich als kostengünstige und energieeffiziente Lösung für die Anbindung dieser verteilten Anlagen an zentrale Managementplattformen etabliert. Auf Anlagenebene eingesetzte LoRa-Gateways können Telemetriedaten übertragen, sodass Betreiber die Leistung optimieren und die Einhaltung von Sicherheitsstandards gewährleisten können. LoRa bietet zwar große Vorteile in Bezug auf Reichweite und geringen Stromverbrauch, hat aber im Vergleich zu kabelgebundenen oder zellularen Alternativen auch inhärente Sicherheitsbeschränkungen. Statisches Schlüsselmanagement, begrenzte Verschlüsselungsmöglichkeiten und Anfälligkeit für Replay- oder Jamming-Angriffe schaffen potenzielle Angriffspunkte für böswillige Akteure. Mit der zunehmenden Verbreitung von Wasserstoff-KWK-Anlagen wird die Robustheit der IoT-Kommunikationssicherheit zu einem Eckpfeiler für die Gewährleistung der Betriebsintegrität und -sicherheit.

Diese Risiken sind nicht nur theoretischer Natur. Cyberangriffe auf Wasserstoff-KWK-Anlagen können schnell von digitalen Sicherheitsverletzungen zu schweren physischen Zwischenfällen führen. So könnte beispielsweise ein Angriff, bei dem ein Gaskonzentrationsensor manipuliert wird, eine gefährliche Wasserstoffansammlung verschleiern, insbesondere wenn gleichzeitig

die Belüftungs- oder Sicherheitssysteme beeinträchtigt sind. In solchen Fällen könnten unentdeckte Lecks zu Explosionen mit verheerenden Folgen für die Sicherheit von Menschen, die Umwelt und die umliegende Infrastruktur führen. Ebenso können Denial-of-Service-Angriffe auf SPS- oder SCADA-Systeme die Strom- und Wärmeerzeugung unterbrechen und kritische Einrichtungen wie Krankenhäuser oder Industriestandorte gefährden, wo eine unterbrechungsfreie Stromversorgung unerlässlich ist. Subtilere Manipulationen, wie die Veränderung von Druckregelkreisen oder die Kompromittierung von Firmware-Updates durch Angriffe auf die Lieferkette, können zu mechanischen Ausfällen oder einer langfristigen Verschlechterung der Systemzuverlässigkeit führen.

Mehrere anschauliche Szenarien verdeutlichen diese Risiken. Ein koordinierter Angriff auf den Betrieb von Brennstoffzellen könnte beispielsweise die Betreiber irreführen, indem falsche Normalwerte angezeigt werden, während ein versteckter Überhitzungsprozess einen thermischen Durchbruch auslöst. In einem anderen Fall könnte ein Man-in-the-Middle-Angriff auf netzintegrierte KWK-Anlagen die Laststeuerungssignale manipulieren und damit sowohl die lokale als auch die regionale Energiebilanz destabilisieren. Die Deaktivierung der Notabschaltlogik während der Wartung könnte dazu führen, dass ein Wasserstoffleck zu einer Explosion eskaliert, während Kompromittierungen der vorgelagerten Lieferkette zeitgesteuerte Logikbomben einführen könnten, die den Ventilbetrieb nach und nach stören.

Diese Beispiele sind zwar hypothetisch, entsprechen jedoch bekannten Schwachstellen in industriellen Energiesystemen und unterstreichen die dringende Notwendigkeit integrierter Cybersicherheitsmaßnahmen bei der Konzeption, Bereitstellung und dem Betrieb von Wasserstoff-KWK-Anlagen. Da Smart Grids weiterentwickelt werden, um diese neuen Anlagen zu integrieren, muss das Zusammenspiel zwischen digitaler Konnektivität und physischer Sicherheit sorgfältig gesteuert werden. Die Ergebnisse unterstreichen die Notwendigkeit mehrschichtiger Sicherheitsstrategien, risikobewusster architektonischer Entscheidungen und starker regulatorischer Rahmenbedingungen zum Schutz der zukünftigen Wasserstoffwirtschaft.

VI.3.11. Illustratives Szenario für einen cyber-physischen Angriff auf Wasserstoff-KWK-Anlagen

Um potenzielle Schwachstellen in zukünftigen Wasserstoffenergiesystemen zu untersuchen, wurde ein illustratives Szenario entwickelt, das eine mittelgroße 500-kW-5-MW-KWK-Anlage umfasst, bestehend aus einem Elektrolyseur, Speichertanks, einer Turbine und einer SCADA-Integration. Das Szenario zeigt, wie ein koordinierter Cyberangriff die Schwachstellen des Steuerungssystems ausnutzen könnte, um unsichere Betriebsbedingungen auszulösen, und wie eine KI-gestützte Überwachung in Verbindung mit einem digitalen Zwilling solche Risiken mindern könnte.

In diesem Szenario verschafften sich die Angreifer über kompromittierte Fernwartungszu-

gangsdaten unbefugten Zugriff auf das Netzwerk der Anlage. Sobald sie sich in der Betriebstechnologiemgebung befanden, nutzten sie schwache Zugriffskontrollrichtlinien aus, um ihre Berechtigungen zu erweitern und Schreibzugriff auf kritische Prozessvariablen zu erhalten. Als erstes manipulierten sie den Modbus/TCP-Kommunikationskanal, der die speicherprogrammierbaren Steuerungen (SPS) der Anlage mit der SCADA-Schnittstelle verbindet. Durch das Senden manipulativer Pakete gaben sie böswillige Befehle aus, die wichtige Sicherheitssensoren zur Überwachung des Drucks und der Temperatur der Wasserstoffspeicher deaktivierten. Gleichzeitig speisten sie falsche „normale“ Messwerte in die SCADA-Mensch-Maschine-Schnittstelle (HMI) ein und verschleierten so die Tatsache, dass der tatsächliche Druck im Speichertank aufgrund der absichtlichen Überlastung des Elektrolyseurs allmählich über die Sicherheitsgrenzwerte anstieg.

Aus betrieblicher Sicht sahen die Anlagenbetreiber keine Anomalien, da das SCADA-Dashboard weiterhin die Nennwerte anzeigte. In Wirklichkeit wurden die Speichertanks jedoch über ihren Auslegungsdruck hinaus befüllt, was ein latentes Risiko für eine katastrophale Explosion darstellte. Ein solcher Angriff könnte, wenn er ungehindert bleibt, zu Wasserstofflecks, Brandgefahren und potenziell schweren Schäden an Personen und Infrastruktur führen.

Das im Projekt vorgesehene Cybersicherheits-Framework integriert eine KI-gestützte Überwachungsebene, die eng mit einem digitalen Zwilling des KWK-Systems gekoppelt ist. Die KI-Anomalieerkennung-Engine analysiert mehrere Datenströme, darunter Netzwerkverkehr, Benutzerauthentifizierungsprotokolle und Prozess-Variablenzeitreihen. In diesem Fall würde das System unregelmäßige Anmeldeuster erkennen, wie z. B. eine Fernverbindung außerhalb der üblichen Wartungsfenster in Kombination mit ungewöhnlichen Befehlssequenzen, die auf sicherheitskritische Register abzielen. Diese Cyber-Indikatoren würden bereits eine Sicherheitswarnung niedriger Stufe auslösen.

Parallel dazu prognostiziert der physikalisch basierte digitale Zwilling des KWK-Systems kontinuierlich die zu erwartenden Prozessverläufe unter normalen Bedingungen. Anhand des Elektrolyseur-Lastprofils und der Umgebungsbedingungen berechnet der digitale Zwilling beispielsweise die zu erwartenden Wasserstoffproduktionsraten und die entsprechende Druckentwicklung im Speichertank. Im Angriffsszenario würden die tatsächlichen Sensorwerte, die nun manipuliert sind, erheblich von den vom Modell vorhergesagten Werten abweichen. Diese Diskrepanz zwischen der Vorhersage des Zwillings und den von SCADA gemeldeten Daten würde eine Anomaliewarnung auf höherer Ebene auslösen.

Bei Erkennung der Anomalie würde eine automatisierte Reaktion das betroffene Netzwerksegment isolieren, indem kompromittierte Benutzeranmeldedaten widerrufen und externe Verbindungen blockiert würden. Das System würde außerdem auf redundante Backup-Sensoren zurückgreifen, die direkt mit einer isolierten Sicherheits-SPS verbunden sind. Wenn die Backup-Daten einen abnormalen Tankdruck bestätigen würden, würde die Steuerungslogik eine

kontrollierte Abschaltung des Elektrolyseurs einleiten, um einen weiteren Überdruck zu verhindern. In extremen Fällen könnten mechanische Sicherheitsventile unabhängig von Softwarebefehlen aktiviert werden. (Die Abbildung veranschaulicht den mehrschichtigen Prozess der Angriffserkennung und -abwehr, der Netzwerkanalyse, KI-Anomalieerkennung und digitale Zwilling-Validierung kombiniert.

Dieses Szenario veranschaulicht, wie eine fortschrittliche KI-gesteuerte Anomalieerkennung in Kombination mit einer physikbasierten Validierung digitaler Zwillinge die Cybersicherheit von Wasserstoff-KWK-Anlagen verbessern könnte. Es unterstreicht, wie wichtig es ist, cyber-physische Resilienzmaßnahmen in kritische Energieinfrastrukturen zu integrieren, bevor solche Anlagen weit verbreitet sind.

VI.3.12. **Diskussion**

Die kombinierten Ergebnisse der Validierung des Hybrid-Mikronetzes in Mulhouse, der LSTM-basierten Erkennungsexperimente, der vergleichenden Smart-Metering-Analyse und des illustrativen Cybersicherheitsszenarios für Wasserstoff-KWK-Anlagen zeichnen ein facettenreiches Bild der sich wandelnden Energielandschaft.

Die Simulation eines realen Mikronetzes hat gezeigt, dass dezentrale hybride Energiesysteme auch unter Störungsbedingungen zuverlässig erneuerbare Energien integrieren und lokale Netzdienste bereitstellen können. Durch die Priorisierung lokal erzeugter Solarenergie, den dynamischen Ausgleich von Batteriespeichern und die nahtlose Interaktion mit dem Hauptnetz bei Bedarf hat das System seine Fähigkeit zur Aufrechterhaltung der Betriebskontinuität unter Beweis gestellt. Diese Validierung hat jedoch auch gezeigt, dass die für ein intelligentes Energiemanagement und den Fernbetrieb erforderliche zunehmende Digitalisierung zwangsläufig die potenzielle Angriffsfläche solcher Infrastrukturen vergrößert.

Aufbauend auf dieser Erkenntnis wurde das LSTM-basierte Erkennungssystem als fortschrittliche cyber-physische Sicherheitsschicht für den Betrieb von Mikronetzen evaluiert. Die Ergebnisse zeigten, dass das Deep-Learning-Modell Cyber- und physische Anomalien, darunter falsche Dateneingaben, wiederholte Messprofile und erzwungenes Laden von Batterien, selbst unter komplexen Batteriemangementbedingungen effektiv identifizierte. Tiefere Netzwerkarchitekturen, die auf erweiterten Datensätzen trainiert wurden, erfassten langfristige Abhängigkeiten in der Systemdynamik genauer, minimierten Fehlalarme und verbesserten gleichzeitig die Empfindlichkeit gegenüber subtilen Angriffsmustern. Diese Ergebnisse unterstreichen das Potenzial der KI-gesteuerten Anomalieerkennung zur Stärkung der Widerstandsfähigkeit von Mikronetzen gegenüber sich entwickelnden Bedrohungen.

Auf einer breiteren regionalen Ebene zeigte die vergleichende Analyse der Smart-Metering-Richtlinien in der Oberrheinregion sowohl Chancen als auch Herausforderungen für die Skalierung solcher intelligenter Systeme auf. Frankreich zeigt Stärke bei der schnellen Einführung, Deutschland legt Wert auf strenge Sicherheitsstandards und die Schweiz konzentriert sich auf

die sektorübergreifende Integration. Diese Vielfalt führt jedoch auch zu einer regulatorischen und technischen Fragmentierung, die den nahtlosen Betrieb transnationaler Mikronetze behindern könnte. Die Harmonisierung digitaler Infrastrukturen, Sicherheitsprotokolle und Datenverwaltung ist daher nicht nur für die Strommessung von entscheidender Bedeutung, sondern auch für die Integration komplexerer Anlagen wie wasserstoffbasierter KWK-Systeme, die auf einer umfassenden IoT-gestützten Überwachung und bidirektionaler Kommunikation beruhen. Schließlich veranschaulicht das Cybersicherheitsszenario für Wasserstoff-KWK, wie sich diese Schwachstellen in zukünftigen sektorübergreifenden Infrastrukturen manifestieren könnten. Angriffe auf Wasserstoff-KWK-Anlagen, die von gefälschten Sensordaten bis hin zu manipulierten Laststeuerungssignalen reichen, könnten sich von digitalen Verstößen zu schweren physischen Zwischenfällen eskalieren. Dies unterstreicht die Notwendigkeit mehrschichtiger Sicherheitsstrategien, die ein robustes Systemdesign, fortschrittliche Erkennungsmechanismen wie LSTM-basierte Modelle und koordinierte Regulierungsrahmen kombinieren. Um solche Risiken zu mindern, muss die cyber-physische Sicherheit nicht als isoliertes Add-on, sondern als integraler Bestandteil der Konzeption, Bereitstellung und des Betriebs von dezentralen Energiesystemen der nächsten Generation behandelt werden.

Letztendlich erfordert die Schaffung widerstandsfähiger, kohlenstoffarmer und intelligenter Energienetze einen ausgewogenen Ansatz. Physische Robustheit muss durch cyber-physische Widerstandsfähigkeit, KI-gestützte Überwachung und harmonisierte digitale Infrastrukturen ergänzt werden. Nur wenn diese Dimensionen gemeinsam angegangen werden, können zukünftige Energiesysteme zuverlässige, nachhaltige und sichere Dienstleistungen sowohl für lokale Gemeinschaften als auch für transnationale Regionen erbringen.

VI.4. Probleme und Risiken

Während der Umsetzung des Projekts traten mehrere technische und kontextbezogene Herausforderungen auf, insbesondere im Zusammenhang mit der Integration von wasserstoffbasierten Kraft-Wärme-Kopplungsanlagen (KWK) und deren Digitalisierung. Obwohl viele dieser Risiken bis zu einem gewissen Grad vorhersehbar waren, erforderten ihre praktischen Auswirkungen adaptive Strategien, um die Kontinuität und Relevanz der Forschung sicherzustellen.

Eine der größten Herausforderungen hängt mit den Eigenschaften von Wasserstoff als Energieträger zusammen. Wasserstoff ist hochreaktiv und unterliegt besonderen Sicherheitsauflagen, insbesondere bei klein- bis mittel n Anwendungen in städtischen oder halbstädtischen Umgebungen. Die Lagerbedingungen, das Druckmanagement und die Wechselwirkung von Wasserstoff mit anderen Elementen in den Brennkammern erfordern eine präzise Steuerung. Selbst geringfügige Abweichungen bei Temperatur, Druck oder Durchfluss können die Systemstabilität beeinträchtigen oder Sicherheitsrisiken mit sich bringen. In beengten städtischen

Gebieten, in denen die Nähe der Infrastruktur und die Bevölkerungsdichte das Risiko eines technischen Ausfalls erhöhen, werden diese Risiken noch verstärkt.

Diese Sicherheitsbeschränkungen wirkten sich direkt auf den Umfang der cyber-physikalischen Sicherheitsprüfungen aus. Während ursprünglich vorgesehen war, dass wasserstoffbasierte KWK-Anlagen als Testumgebungen für integrierte Sicherheitsexperimente dienen könnten, erwies sich die Durchführung solcher Tests in Umgebungen mit brennbaren Gasen als nicht durchführbar. Das Potenzial für unbeabsichtigte Wasserstofflecks, Überdruck oder Entzündungsereignisse bedeutete, dass eine absichtliche Simulation von cyber-physischen Angriffen unter realistischen Betriebsbedingungen nicht durchgeführt werden konnte. Das Fehlen einer angemessen kontrollierten und isolierten Testumgebung schränkte die Möglichkeit, diese Systeme absichtlichen cyber-physischen Stressszenarien auszusetzen, weiter ein.

Zusätzlich zu den sicherheitsbezogenen Hindernissen ergab sich eine kritische Einschränkung aus dem aktuellen Stand der Smart-Metering-Infrastruktur. Die in der Projektregion eingesetzten Smart Meter sind in erster Linie für elektrische Parameter wie Spannung, Strom und aktive/reaktive Energieflüsse ausgelegt. Der Betrieb von wasserstoffbasierten KWK-Anlagen hängt jedoch auch von nicht-elektrischen Daten wie Temperatur, Druck und Wasserstoffdurchflussraten ab. Ohne die Möglichkeit, solche Daten nativ zu erfassen und in bestehende Smart-Metering-Plattformen zu integrieren, war es unmöglich, die angestrebte vollständige digitale Darstellung der KWK-Anlagen zu erreichen. Diese Lücke behinderte sowohl die Fähigkeit zur Echtzeit-Überwachung cyber-physikalischer Vorgänge als auch die Erstellung umfassender Datensätze, die für KI-basierte Modelle zur Erkennung von Anomalien erforderlich sind.

Darüber hinaus stieß eine geplante Zusammenarbeit mit der Partnerorganisation HKA zur cyber-physikalischen Sicherheitsanalyse ihrer wasserstoffbasierten KWK-Anlage auf unerwartete Hindernisse. Der von der HKA unterhaltene Prüfstand war in erster Linie für die Forschung im Bereich Energieeffizienz und Wärmemanagement konzipiert. Es fehlten die für die Integration von Smart Metern und externe Cybersicherheitstests erforderlichen Hardware- und Kommunikationsebenen. Die Nachrüstung dieser Infrastruktur hätte umfangreiche Modifikationen erfordert, sowohl für die Sicherheitszertifizierung als auch für die Kompatibilität mit externen digitalen Überwachungssystemen, was den verfügbaren Zeit- und Ressourcenrahmen des Projekts überschritten hätte.

Die Situation offenbarte eine interessante Dualität in der Konnektivität von Wasserstoff-KWK-Systemen. Einerseits behindert die mangelnde Integration mit intelligenten Mess- und Fernkommunikationsnetzen die Energieoptimierung und das dynamische Management. Wenn beispielsweise KWK-Anlagen parallel zu variablen erneuerbaren Energiequellen betrieben werden, schränkt das Fehlen detaillierter Verbrauchs- und Produktionsdaten die Fähigkeit des Systems ein, Ressourcen effizient zuzuweisen, Energieengpässe zu antizipieren oder voraus-

schauende Wartungsmaßnahmen zu planen. Diese Trennung schränkt das Betriebsmanagement ein und untergräbt das Potenzial für eine KI-gesteuerte Optimierung, die auf hochauflösenden, domänenübergreifenden Daten basiert.

Andererseits bot genau diese mangelnde Konnektivität einen zufälligen Schutz. Da diese KWK-Anlagen nicht ständig externen digitalen Netzwerken ausgesetzt sind, sind sie von Natur aus weniger anfällig für Cyberangriffe aus der Ferne, Spionage oder Systemmanipulationen. Diese Isolation kann als kurzfristige Schutzmaßnahme angesehen werden, die besonders in kritischen Infrastrukturen wie Krankenhäusern, industriellen Mikronetzen oder kommunalen Dienstleistungen relevant ist, wo Wasserstoff-KWK eine wichtige Rolle bei der Verbesserung der Widerstandsfähigkeit spielt. Dieser Schutzeffekt ist jedoch nur vorübergehend. Da Energiesysteme zunehmend stärker sektorübergreifend gekoppelt werden, erfordern die regulatorischen Anforderungen eine umfassende digitale Integration von Wasserstoffsystemen, einschließlich der Überwachung von Gasflüssen, Emissionen und Wärmeaustausch. In dieser Phase wird sich die Risikooberfläche zwangsläufig vergrößern.

Um diese miteinander verflochtenen technischen und digitalen Herausforderungen zu mindern, wurde der Ansatz des Projekts angepasst. Anstelle von umfassenden experimentellen Simulationen cyber-physischer Angriffe auf in Betrieb befindliche Wasserstoff-KWK-Anlagen wurde ein hypothetisches, aber technisch fundiertes Angriffsszenario betrachtet. Dies ermöglichte eine konzeptionelle Analyse von Erkennungs- und Abwehrstrategien, ohne die physische Sicherheit zu gefährden.

Trotz dieser Anpassungen konnten bestimmte Einschränkungen im Rahmen des aktuellen Projektumfangs nicht vollständig überwunden werden. So konnte beispielsweise das Fehlen integrierter intelligenter Messgeräte für wasserstoffspezifische Parameter nicht behoben werden, ohne die bestehenden Messinfrastrukturen auf regulatorischer Ebene neu zu gestalten. Ebenso bedeutet die Unmöglichkeit, Live-Cyber-Physik-Stresstests durchzuführen, dass einige Aspekte der Resilienz, insbesondere solche, die gekoppelte Kaskadenausfälle betreffen, eher theoretischer Natur bleiben und nicht empirisch validiert werden können.

Dennoch lieferten diese Herausforderungen wertvolle Erkenntnisse. Sie unterstrichen, wie wichtig es ist, Wasserstoff-KWK-Anlagen von Anfang an unter Berücksichtigung der Cybersicherheit zu konzipieren, um sowohl einen sicheren Betrieb als auch eine sichere Digitalisierung zu gewährleisten. Sie machten auch deutlich, dass dringend interoperable intelligente Messsysteme benötigt werden, die in der Lage sind, multivektoriellen Energiedaten zu erfassen, darunter Wasserstoffströme, thermische Variablen und Emissionskennzahlen. Diese Erkenntnisse werden in die Übergangsstrategie für eine sichere KWK-Integration in zukünftigen Forschungsphasen einfließen, wobei die Erfordernisse der Optimierung, Sicherheit und Resilienz gegeneinander abgewogen werden.

VI.5. Abweichungen

Es gab nur wenige Abweichungen vom ursprünglichen Projektplan, die in erster Linie auf technische und infrastrukturelle Einschränkungen im Zusammenhang mit Wasserstoff-KWK-Anlagen zurückzuführen waren. Diese Änderungen erforderten zwar Anpassungen bei der Durchführung einiger Aktivitäten, beeinträchtigten jedoch nicht grundlegend die Gesamtziele des Projekts. Stattdessen führten sie zu einer Neugestaltung bestimmter Teilziele und einer Neuausrichtung des Forschungsschwerpunkts auf eher konzeptionelle und strategische Ergebnisse.

Die erste Abweichung betraf die geplante experimentelle cyber-physische Sicherheitsanalyse einer wasserstoffbasierten KWK-Anlage in Zusammenarbeit mit HKA. Ursprünglich sollte diese Anlage als Live-Testumgebung dienen, um unter kontrollierten Bedingungen Netzwerkangriffe, Sensor-Spoofing und Prozessmanipulationsangriffe zu simulieren. Nach einer detaillierten technischen Bewertung stellte sich jedoch heraus, dass der Prüfstand nicht für die Integration mit externen intelligenten Messgeräten oder Fernüberwachungssystemen ausgelegt war. Darüber hinaus machte es das Fehlen sicherheitszertifizierter Umgebungen unmöglich, absichtlich abnormale Wasserstoffbetriebsbedingungen ohne erhebliches Risiko herbeizuführen.

Um dieser Einschränkung zu begegnen, verlagerte sich das Projekt auf eine theoretische Angriffsfallstudie. Anstelle von Live-Experimenten entwickelte das Team ein digital twin-gesteuertes Szenario eines hypothetischen Eindringens in ein Wasserstoffspeichersystem. Dies ermöglichte eine detaillierte Untersuchung potenzieller Angriffswege, KI-basierter Erkennungsstrategien und mehrschichtiger Abwehrmaßnahmen, ohne physische Vermögenswerte oder Personal zu gefährden. Dieser Ansatz war zwar nicht so empirisch reichhaltig wie Live-Tests, lieferte jedoch wertvolle Einblicke in die cyber-physische Risikolandschaft und fundierte Empfehlungen für zukünftige Anforderungen an die Forschungsinfrastruktur.

Im Hinblick auf die Integration fortschrittlicher KI stellte die Implementierung von LSTM-Modellen in der Simulink-Umgebung eine zusätzliche Komplexität dar. Obwohl LSTMs für die Zeitreihenanalyse sehr effektiv sind, ist ihr Einsatz in Echtzeitumgebungen noch nicht ganz einfach. Die Unterstützung von MATLAB für die LSTM-Inferenz basiert auf einem zustandsbehafteten Vorhersageblock, der .mat-Dateiformate verwendet, die nicht mit Code-Generierungs-Workflows kompatibel sind. Diese technische Einschränkung verhindert, dass das Modell zu ausführbarem C-Code kompiliert werden kann, um es auf Echtzeit-Simulatoren oder eingebetteten Systemen einzusetzen. Zwar gibt es verschiedene Alternativen wie Python-basierte Implementierungen, doch würde ihre Integration in RT-Lab oder eingebettete Mikrocontroller zusätzliche Entwicklungs- und Anpassungsarbeiten erfordern, die über den Rahmen dieses Projekts hinausgingen. Daher wurde kein HIL-Test des LSTM-Modells durchgeführt. Stattdessen konzentrierte sich die Arbeit darauf, die Leistung von LSTM in Offline-Tests und im Vergleich

zum NARX-Modell zu demonstrieren.

Eine weitere Abweichung ergab sich aus den Einschränkungen der aktuellen Smart-Metering-Infrastruktur. Der ursprüngliche Plan sah einen umfassenden Datensatz vor, der elektrische und nicht-electrische Variablen, einschließlich Wasserstoffströme, Druckniveaus und thermische Daten, aus integrierten KWK-Anlagen kombinierte. Da die verfügbaren Smart Meter jedoch nur für Stromparameter optimiert waren, konnte das Projekt keine vollständige Datenerfassung erreichen.

Die Auswirkungen dieser Abweichung wurden durch die Umstellung auf eine konzeptionelle Bewertung der Vorteile fortschrittlicher Überwachungs- und Steuerungsstrategien gemildert. Dieser Ansatz führte zwar zu einer gewissen Abstraktion, hob jedoch die strukturellen Lücken in der aktuellen Smart-Metering-Politik und -Technologie hervor und stärkte die vergleichende Analyse der regionalen Praktiken im Oberrheingebiet.

Schließlich führte die Dualität der begrenzten Konnektivität in Wasserstoff-KWK-Systemen zu einer konzeptionellen Verschiebung in der Projektdarstellung. Ursprünglich wurde davon ausgegangen, dass eine vollständige digitale Integration zweifellos von Vorteil für die Cyber ität ist. Im Laufe des Projekts wurde jedoch deutlich, dass eine teilweise Isolation derzeit einen vorübergehenden Vorteil in Bezug auf die Cyber ität bietet. Dieses differenzierte Verständnis bereicherte die abschließenden Empfehlungen und unterstrich die Notwendigkeit eines schrittweisen und sicheren Übergangs zu einer umfassenden Digitalisierung anstelle einer sofortigen vollständigen Konnektivität.

Insgesamt führten diese Abweichungen zu einer Neuausrichtung bestimmter Forschungsaktivitäten, stärkten aber letztlich die strategische Relevanz des Projekts. Sie deckten kritische technologische und politische Lücken auf, die geschlossen werden müssen, bevor Wasserstoff-KWK-Anlagen sicher in digitalisierte Mikronetze integriert werden können. Während einige Teilziele neu formuliert wurden, blieb das übergeordnete Projektziel, resiliente, nachhaltige und intelligente Energiesysteme voranzutreiben, unverändert.

VI.6. Aussichten

Die im Rahmen dieses Projekts durchgeführten Arbeiten haben eine solide konzeptionelle und methodische Grundlage für die cyber-physische Sicherheit von hybriden Mikronetzsystemen geschaffen, insbesondere von solchen, die wasserstoffbasierte Kraft-Wärme-Kopplungsanlagen (KWK) integrieren. Gleichzeitig haben sie mehrere Bereiche aufgezeigt, in denen weitere Forschung und technologische Entwicklung erforderlich sind, um die verbleibenden Lücken zu schließen und das volle Potenzial sicherer, digital integrierter und widerstandsfähiger Energiesysteme auszuschöpfen. Die Aussichten für die zukünftige Arbeit sind daher sowohl technischer als auch strategischer Natur und erfordern koordinierte Fortschritte in den Bereichen

Überwachungsinfrastruktur, cyber-physische Testumgebungen, künstliche Intelligenz zur Erkennung von Anomalien und politische Rahmenbedingungen, die eine sichere Integration von Wasserstoffenergiesystemen in umfassendere Smart-Grid-Architekturen unterstützen.

Ein vorrangiger Bereich der zukünftigen Forschung liegt in der Verbesserung der intelligenten Messfunktionen für Multivektor-Energiesysteme. Bestehende intelligente Messinfrastrukturen sind überwiegend für elektrische Parameter wie Spannung, Strom und Leistungsfaktor ausgelegt und bieten wenig Einblick in nicht-elektrische Aspekte, die für den sicheren und effizienten Betrieb von Wasserstoff-KWK-Anlagen unerlässlich sind. Die zukünftige Entwicklung muss sich daher auf Messungstechnologien konzentrieren, die gleichzeitig die Wärmeabgabe, die Wasserstoffdurchflussraten, die Druckniveaus und die Bedingungen in der Brennkammer erfassen können, während gleichzeitig die Kompatibilität mit bestehenden Standards für den Datenaustausch im Netz gewährleistet bleibt. Dieser domänenübergreifende Sensoransatz wird die Grundlage für eine aussagekräftige Echtzeitüberwachung und die zuverlässige Erkennung abnormaler Betriebsmuster bilden.

Die vergleichende politische Analyse der Smart-Metering-Praktiken in der Oberrheinregion weist auch auf wichtige zukünftige Richtungen in den Bereichen Governance und Standardisierung hin. Das derzeitige Flickwerk aus Vorschriften und technischen Standards für Smart Meter und Wasserstoffenergiesysteme schafft Hindernisse für Interoperabilität, Datenaustausch und koordinierte Sicherheitsmaßnahmen. Zukünftige Forschungs- und Politikarbeiten sollten daher darauf abzielen, harmonisierte grenzüberschreitende Standards für die Multivektor-Messung und die Zertifizierung der Cybersicherheit zu entwickeln. Solche Standards würden nicht nur die Integration von Wasserstoff-KWK in regionale Mikronetze erleichtern, sondern auch koordinierte Reaktionen auf neue cyber-physische Bedrohungen ermöglichen.

Neben Hardware-Innovationen müssen auch die Kommunikationsprotokolle und Datenmodelle, die diesen Zählern der nächsten Generation zugrunde liegen, weiterentwickelt werden. Sichere, standardisierte Datenformate, die Gas-, Wärme- und Strommessungen in ein einheitliches Rahmenwerk integrieren können, werden für die Interoperabilität von entscheidender Bedeutung sein. Dies ist besonders wichtig in grenzüberschreitenden Regionen wie dem Oberrhein, wo unterschiedliche Rechtsordnungen unterschiedliche technische Standards anwenden können. Durch die Verfolgung einer harmonisierten und robusten Messarchitektur können zukünftige Studien viele der derzeitigen blinden Flecken beseitigen, die das Betriebsbewusstsein in KWK-Systemen einschränken.

Ein weiterer wichtiger Ansatzpunkt für zukünftige Untersuchungen ist die Schaffung kontrollierter Versuchsumgebungen für die cyber-physikalische Sicherheitsforschung im Bereich Wasserstoff. Derzeit birgt die Untersuchung der Auswirkungen von absichtlichen Cyberangriffen oder versehentlichen Fehlfunktionen auf den Betrieb von Wasserstoff-KWK-Anlagen erhebliche Sicherheitsrisiken. Die hohe Entflammbarkeit von Wasserstoff in Verbindung mit den

komplexen thermodynamischen Prozessen bedeutet, dass selbst geringfügige Manipulationen zu gefährlichen Folgen führen können. Diese Einschränkung erfordert spezielle Laboreinrichtungen mit fortschrittlichen Sicherheitsvorkehrungen. Solche Umgebungen müssten physische KWK-Hardware mit redundanten Überwachungs-, Gasetektions-, Belüftungs- und ausfallsicheren Abschaltmechanismen kombinieren, um die sichere Simulation von ansonsten gefährlichen Szenarien zu ermöglichen.

Ergänzend zu physischen Testanlagen sollten auch virtualisierte Simulationsumgebungen ausgebaut werden. Hochpräzise Simulationswerkzeuge, die sowohl die physikalischen Prozesse innerhalb einer KWK-Anlage als auch die damit verbundenen Steuerungs- und Kommunikationsebenen nachbilden können, bieten eine alternative Plattform für die Untersuchung komplexer Szenarien, ohne dass Personal oder Infrastruktur gefährdet werden. Hardware-in-the-Loop-Ansätze (HIL) könnten die Lücke zwischen rein virtuellen Umgebungen und realer Hardware schließen und es Forschern ermöglichen, realistische Cyberangriffe zu simulieren und deren Auswirkungen auf die Betriebsparameter von Wasserstoff-KWK-Anlagen zu überwachen. Diese hybriden Ansätze werden das Spektrum der experimentellen Bedingungen, die sicher getestet werden können, erheblich erweitern.

Eng damit verbunden ist die Weiterentwicklung von digitalen Zwillingen, die auf Wasserstoff-KWK-Systeme zugeschnitten sind. Digitale Zwillinge sind auf genaue und hochauflösende Datenströme angewiesen, um das Betriebsverhalten zu modellieren und Störungen in Echtzeit zu simulieren. Das Fehlen umfassender Sensordaten in diesem Projekt schränkte die Konzeption und Implementierung digitaler Zwillinge ein, insbesondere wenn es um die Darstellung der dynamischen Prozesse innerhalb der Wasserstoffverbrennungskammern ging. Zukünftige Forschungsarbeiten sollten sich vorrangig auf die Kopplung fortschrittlicherer physikalischer Modelle mit umfangreicheren Daten aus der Praxis konzentrieren, damit digitale Zwillinge als leistungsstarke Prognosewerkzeuge sowohl für die Betriebsoptimierung als auch für Cybersicherheitstests dienen können. Verbesserte digitale Zwillinge würden es Forschern auch ermöglichen, komplexe Wechselwirkungen zwischen Wasserstoff-KWK-Anlagen und anderen dezentralen Energiequellen innerhalb eines Mikronetzes systematisch zu untersuchen, einschließlich potenzieller Kaskadeneffekte von Störungen oder Angriffen.

Darüber hinaus muss die Sicherheit der Kommunikationskanäle, die KWK-Anlagen mit übergeordneten Mikronetz-Managementsystemen verbinden, weiter untersucht werden. Da die digitale Integration von KWK-Systemen unvermeidlich ist, wird die Angriffsfläche zunehmen, sodass die Entwicklung und Validierung sicherer Kommunikationsprotokolle unerlässlich ist. Zukünftige Forschungsarbeiten sollten sich auf Verschlüsselungsschemata und Intrusion-Detection-Systeme konzentrieren, die in Echtzeit arbeiten können, ohne übermäßige Rechenlast auf ressourcenbeschränkte industrielle Steuerungen auszuüben.

Ein verwandter Forschungsbereich ist die Widerstandsfähigkeit von KI-basierten Überwachungssystemen selbst. Mit fortschreitender digitaler Integration von KWK-Anlagen könnten die KI-Modelle, die diese Systeme steuern oder überwachen, selbst zum Ziel von Angriffen werden. Zukünftige Forschungsarbeiten müssen sich mit der Robustheit und Cybersicherheit von KI befassen, um sicherzustellen, dass Erkennungsalgorithmen nicht durch sorgfältig ausgearbeitete falsche Dateneingaben leicht getäuscht oder manipuliert werden können. Dies erfordert einen ganzheitlichen Ansatz, der die KI-Entwicklung mit sicheren Kommunikationsprotokollen, vertrauenswürdigen Ausführungsumgebungen und strengen Validierungsrahmenwerken kombiniert.

Eine weitere langfristige Perspektive ist die schrittweise Integration von KWK-Anlagen in koordinierte Energiemanagement-Frameworks. Derzeit arbeiten viele KWK-Anlagen in isolierten oder halbisolierten Modi mit begrenzter oder gar keiner digitalen Konnektivität. Diese Isolation hat zwar vorübergehend einen Puffer gegen Cyber-Bedrohungen aus der Ferne gebildet, verhindert aber auch, dass die Anlagen effektiv zur Optimierung auf Systemebene beitragen können. Zukünftige Arbeiten sollten sich mit schrittweisen Integrationsstrategien befassen, die es KWK-Anlagen ermöglichen, an Demand-Response-Mechanismen, Netzausgleichsdiensten und Sektorkopplungsinitiativen teilzunehmen und gleichzeitig strenge Sicherheitsgrenzen einzuhalten. Dies wird einen schrittweisen Übergang beinhalten, bei dem Sicherheitsmaßnahmen parallel zu jeder neuen Konnektivitätsebene eingesetzt werden.

Die Entwicklung von Strategien zur Erkennung und Abwehr hypothetischer Cyberangriffe auf Wasserstoff-KWK-Anlagen ist ebenfalls ein vielversprechendes Gebiet für zukünftige Forschungsarbeiten. Die in diesem Projekt entwickelte hypothetische Fallstudie, in der ein Angreifer Steuersignale manipuliert, um unsichere Druck- und Temperaturbedingungen zu erzeugen, kann zu einer umfassenderen Bibliothek von Bedrohungsszenarien erweitert werden. Diese Szenarien können dann als Grundlage für die Entwicklung automatisierter Reaktionsmechanismen dienen, die in der Lage sind, kompromittierte Subsysteme zu isolieren, kontrollierte Abschaltungen auszulösen oder Betriebsmodi dynamisch neu zu konfigurieren, um Schäden zu minimieren.

Der mittel- und langfristige Einsatz von Wasserstoff-KWK in städtischen Energiesystemen wird zwangsläufig die Komplexität der Wechselwirkungen zwischen dezentralen Ressourcen erhöhen. Da KWK-Anlagen mit Photovoltaik, Speichersystemen und Fernwärmenetzen integriert werden, steigt das Potenzial für Kettenausfälle. Zukünftige Forschungsarbeiten sollten sich daher auf Multi-Energie-Systemmodelle konzentrieren, die sowohl cyberphysische als auch physische Interdependenzen explizit berücksichtigen. Solche Modelle würden wertvolle Einblicke in die Ausbreitung von Fehlern oder Angriffen in miteinander verbundenen Netzwerken liefern und dabei helfen, kritische Knotenpunkte zu identifizieren, auf die sich Sicherheitsmaßnahmen konzentrieren sollten.

Schließlich sollten die Zukunftsaussichten auch Schulungen und Kapazitätsaufbau für Betreiber und Ingenieure umfassen, die zunehmend digitalisierte KWK-Systeme verwalten werden. Während die technologische Entwicklung von entscheidender Bedeutung ist, bleibt der Faktor Mensch ein kritischer Bestandteil des sicheren Betriebs. Die Entwicklung von Schulungsmodulen, simulationsbasierten Übungen und Zertifizierungssystemen für Betreiber wird sicherstellen, dass die Belegschaft angemessen darauf vorbereitet ist, neu auftretende cyber-physische Risiken in Wasserstoff-KWK-Umgebungen zu erkennen, darauf zu reagieren und sie zu verhindern.

Insgesamt sind die Perspektiven für weitere Studien vielschichtig und umfassen die Entwicklung fortschrittlicher Sensor- und Messtechnologien, die Schaffung sicherer Versuchs- und Simulationsplattformen, die Verfeinerung von Kommunikationsprotokollen und Integrationsstrategien sowie die Angleichung der regulatorischen Rahmenbedingungen. Durch die systematische Auseinandersetzung mit diesen Bereichen kann die zukünftige Forschung die Unsicherheiten und Einschränkungen, mit denen der sichere Einsatz von Wasserstoff-KWK-Systemen derzeit konfrontiert ist, erheblich reduzieren und so zu einer widerstandsfähigen, optimierten und dekarbonisierten Energiezukunft beitragen.

VI.7. Empfehlungen

Auf der Grundlage der im Laufe des Projekts gewonnenen Erkenntnisse lassen sich mehrere Empfehlungen formulieren, die sowohl als Leitfaden für die nächsten Forschungsschritte als auch für die Entwicklung einer umfassenderen Politik und Roadmap für die sichere Integration von Energiesystemen dienen können.

Auf der Ebene der Forschung und technologischen Entwicklung wird empfohlen, die domänenübergreifende Smart-Metering-Infrastruktur als grundlegende Voraussetzung für die Digitalisierung von Wasserstoff-KWK-Systemen zu priorisieren. Ohne die Möglichkeit, elektrische, thermische und chemische Parameter nahtlos zu messen und zu integrieren, können weder fortschrittliche digitale Zwillingmodelle noch KI-basierte Anomalieerkennung ihr volles Potenzial entfalten. Öffentliche Forschungsförderprogramme und Industriepartnerschaften sollten daher die Entwicklung und den Einsatz von Messlösungen der nächsten Generation unterstützen, die sowohl den betrieblichen als auch den Cybersicherheitsanforderungen entsprechen. Diese Geräte sollten speziell für Multi-Energie-Umgebungen konzipiert und mit bestehenden Strommessinfrastrukturen kompatibel sein, während sie gleichzeitig Funktionen zur Erfassung nicht-elektrischer Parameter hinzufügen, die für die Sicherheit und Effizienz von Wasserstoff-KWK-Anlagen entscheidend sind.

Parallel dazu ist es unerlässlich, spezielle cyber-physische Testanlagen für Wasserstoffenergiesysteme einzurichten. Diese Anlagen sollten reale KWK-Hardware, hochpräzise virtuelle

Umgebungen und fortschrittliche Sicherheitssysteme kombinieren, um kontrollierte Tests sowohl von zufälligen als auch von böswilligen Ausfallszenarien zu ermöglichen. Solche Infrastrukturen würden nicht nur die Forschung zu Erkennungs- und Minderungsstrategien beschleunigen, sondern auch eine vertrauenswürdige Umgebung für die Validierung von KI-Modellen, Kommunikationsprotokollen und integrierten Überwachungslösungen bieten, bevor diese in Betriebsnetzen eingesetzt werden.

Aus Sicht der Regierungsführung sind harmonisierte Rechtsrahmen erforderlich, um die Interoperabilität und Sicherheit regionaler Energiesysteme zu gewährleisten. In der Oberrheinregion sollte die grenzüberschreitende Zusammenarbeit verstärkt werden, um technische Standards für intelligente Messsysteme, Cybersicherheitszertifizierung und Datenschutz anzugleichen. Die Entwicklung einheitlicher Leitlinien für die Datenerfassung, den Datenaustausch und den Datenschutz würde ein einheitliches Sicherheitsniveau gewährleisten und gleichzeitig kooperative Ansätze zur Energieoptimierung ermöglichen. Koordinierte politische Maßnahmen würden die sichere Integration von Wasserstoff-KWK-Anlagen in bestehende Mikronetze erleichtern und gleichzeitig die Widerstandsfähigkeit gegen cyber-physische Bedrohungen gewährleisten.

Darüber hinaus sollte die digitale Integration von Wasserstoff-KWK-Systemen in sorgfältig gesteuerten Phasen erfolgen. Anstatt sofort eine vollständige Konnektivität anzustreben, die die Systeme unnötigen Risiken aussetzen würde, sollte ein schrittweiser Ansatz verfolgt werden. Jede Phase der verstärkten Integration sollte mit strengen Sicherheitstests, Redundanzplanung und Schulungen für das Bedienpersonal einhergehen. Diese schrittweise Strategie würde es ermöglichen, Schwachstellen zu identifizieren und schrittweise zu beheben, wodurch systemische Schwächen bei der Erweiterung des Netzes verhindert würden.

Darüber hinaus sollte der Entwurf und die Einführung sicherer Kommunikationsprotokolle für Wasserstoff-KWK-Anlagen ausdrücklich priorisiert werden. Zukünftige Integrationsbemühungen werden unweigerlich den Fluss von Betriebsdaten zwischen KWK-Anlagen und Überwachungssystemen erhöhen und neue Angriffsvektoren schaffen, wenn sie ungeschützt bleiben. Forschungs- und Politikbemühungen sollten sich daher auf die Validierung von leichtgewichtigen Verschlüsselungs-, Authentifizierungsmechanismen und Intrusion-Detection-Systemen konzentrieren, die auf industrielle Energieumgebungen zugeschnitten sind.

Auf strategischer Ebene wird außerdem empfohlen, Cybersicherheitsaspekte in das Lebenszyklusmanagement von Wasserstoff-KWK-Anlagen einzubeziehen, vom Entwurf und der Beschaffung bis hin zum Betrieb und zur Stilllegung. Beschaffungsrichtlinien sollten Geräte und Software bevorzugen, die strenge Sicherheitsstandards erfüllen, und langfristige Wartungsstrategien sollten regelmäßige Sicherheitsaudits, Updates und Schulungen für das Betriebspersonal umfassen.

Schließlich sollte die politische Roadmap zur Förderung der Integration von Wasserstoff-KWK-

Anlagen explizit die Ziele der cyber-physischen Sicherheit und der Energiewende miteinander verknüpfen. Wasserstoff spielt zwar eine entscheidende Rolle bei der Dekarbonisierung von Energiesystemen und der Verbesserung der lokalen Widerstandsfähigkeit, doch muss seine digitale Integration mit gleicher Aufmerksamkeit für Sicherheit und Schutz erfolgen. Politische Maßnahmen sollten daher multidisziplinäre Forschungskonsortien fördern, die Energieingenieure, Cybersicherheitsexperten, Regulierungsbehörden und Sozialwissenschaftler zusammenbringen, um sicherzustellen, dass zukünftige Wasserstoffsysteme nicht nur nachhaltig, sondern auch sicher sind und das Vertrauen aller Beteiligten genießen.

Diese Empfehlungen bilden zusammen einen kohärenten Weg in die Zukunft, der Forschung, Entwicklung und politische Maßnahmen zu einer einheitlichen Strategie für die sichere Integration von Wasserstoff-KWK-Systemen verbindet. Durch die Priorisierung fortschrittlicher Messtechnologien, kontrollierter Versuchsinfrastrukturen, harmonisierter Vorschriften, einer schrittweisen Digitalisierung und sicherer Kommunikationsprotokolle können die Beteiligten die derzeitigen Einschränkungen schrittweise überwinden und sicherstellen, dass Wasserstoff-KWK zu einem zuverlässigen und widerstandsfähigen Bestandteil der sich wandelnden Energielandschaft wird.

VI.8. Tabelle zur Zielerreichung

Ziel (Ergebnis)	Erreicht?
6.1. Bericht, in dem die verschiedenen Aspekte der Gestaltung des Mikronetzmodells erläutert, die zu bewältigenden Herausforderungen hervorgehoben und Empfehlungen für das weitere Vorgehen gegeben werden.	Ja
6.2. KI-basiertes Analysesystem zur Früherkennung von Cyber-Bedrohungen.	Ja
6.3. Bericht über Sicherheitsaspekte moderner intelligenter Zähler, in dem Markteinflussfaktoren und nationale Trends bei der Anpassung verschiedener Richtlinien zur Informationsbeschaffung verglichen werden.	Ja