Smart Grid LAB Hessen

Abschlussbericht

29. JUNI 2023

EUROPÄISCHE UNION
Investition in Ihre Zukunft
Europäischer Fonds
für regionale Entwicklung

HESSEN
Hessisches Ministerium
für Wirtschaft, Energie,
Verkehr und Wohnen

1. Einleitung

Im Rahmen der in Deutschland eingeleiteten Energiewende wächst der Bestand an erneuerbaren Stromerzeugungsanlagen [1]. Künftig soll die Endenergie Elektrizität, sowie die in den Sektoren Mobilität und Wärme (bzw. Kälte) angewendeten Endenergieträger aus regenerativen Primärquellen gewonnen werden.

Dabei liegt der Schwerpunkt auf Windkraft- und Photovoltaikanlagen (PV-Anlagen). Ende 2021 waren etwa 59 GW PV-Anlagenleistung, etwa 57 GW onshore und etwa 7 GW offshore Windanlagenleistung in Deutschland installiert [2]. Im Jahr 2022 beschloss der Bundestag, die Photovoltaik-Leistung bis 2040 auf 400 GW und Windenergieanlagen an Land auf 160 GW auszubauen. [3]. Beide sind volatil und intermittierend.

Abbildung 1 beschreibt den Wandel des konventionellen Energiesystems zu einem intelligenten Stromnetz (Smart Grid). Es wird durch eine Steuerung der Erzeugung, Speicherung und dem Verbrauch von Energie im Stromnetz der Stromfluss kontrolliert. Dafür ist eine Vernetzung von Erzeugungsanlagen, großen Verbrauchen und digitalisierten Netzen für einen Informationsaustausch notwendig. Die Informationen werden in einem Energiemanagement ausgewertet und steuern entsprechend die Komponenten. [4]

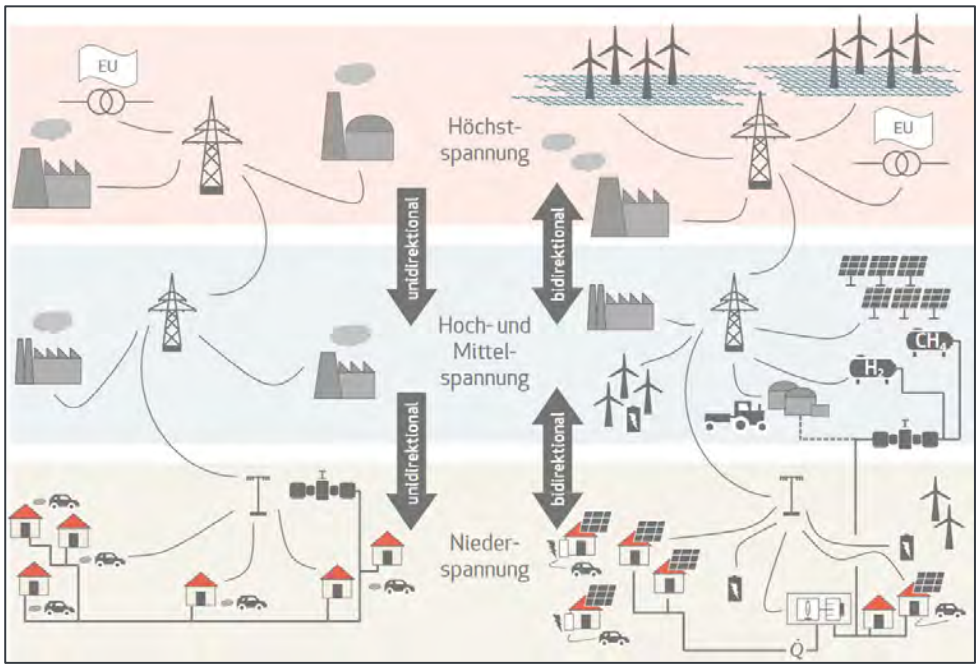


Abbildung 1: konventionelles Energiesystem vs. Smart Grid [5].

In der alten Energiestruktur (in der Abbildung links) gibt es Großkraftwerke, die zentral in Übertragungsnetze einspeisen. Von hier aus wird der Strom unidirektional bis zu den Haushalten im Niederspannungsnetz verteilt. Die Haushalte waren ausschließlich Verbraucher. Des Weiteren gab es eine klare Trennung der Sektoren (Haushalte mit Strom und Warmwasser, Gewerbe, Handel und Dienstleistungen (GHD), Industrie und Verkehr).

Die rechte Seite der Abbildung 1 zeigt eine bidirektionale Stromversorgung und zunehmende Kopplung der Sektoren. Die privaten Haushalte tragen ebenfalls zur Energiegewinnung durch PV-Anlagen bei und verfügen über weitere Smarte Komponenten wie E-Mobile, Batteriespeicher und Wärmespeicher. Es wird von Prosumern gesprochen.

Die Transformation des Verteilnetzes stellt das Verteilnetz vor neue Herausforderungen. Die Nutzung von regenerativen Energien als Primärenergiequelle bedeutet eine Bereitstellung von volatiler elektrischer Leistung aus hauptsächlich Wind und Sonne. Es kommt zu zeitweisen hohen Einspeiseleistungen. Die leistungsstarke Volatilität zeigt sich aber nicht nur auf der Erzeugerseite, sondern zunehmend auch auf der Verbraucherseite. Das Laden von Elektrofahrzeugen und die Verwendung von elektrischen Wärmepumpen führen zu hohen Entnahmeleistungen im Verteilnetz.

Die Elektrifizierung von weiteren, z.B. gewerblichen Sektoren bringt zudem neue und unbekannte Lastgänge mit sich. Diese könnten jedoch das Potential haben als flexible Lasten das Netz zu unterstützen. Hierzu ist eine großflächige mess- und steuerungstechnische Erfassung nötig. Die Herausforderung liegt darin, Zeit und Ort der Erzeugung mit Zeit und Ort des Bedarfs dynamisch abzugleichen. Daraus resultieren vielfältige Herausforderungen für das künftige Energienetz. Z.B. führen hohe Leistungsspitzen zu Spannungsänderungen und es kann zu Verletzungen des zulässigen Spannungsbandes kommen.

Im Forschungsprojekt Smart Grid LAB Hessen sollen die Herausforderungen der Energiewende im Verteilnetz untersucht und Lösungen für ein stabiles und optimiertes Verteilnetz ermittelt wurden. Das Laborstromnetz ist über eine intelligente Ortsnetzstation am Mittelspannungsnetz angebunden und bildet ein Niederspannungsnetz mit den künftig zu erwartenden Quellen und Senken nach. Es umfasst – real oder in Nachbildung durch Stromrichter – Lademöglichkeiten für Elektrofahrzeuge, Batteriespeicher, Hausanschlüsse, Wärmepumpen und Photovoltaikanlagen (Abbildung). Insbesondere können acht Wechselrichterpaare im 4-Quadranten Betrieb arbeiten und simulieren damit sehr flexibel sowohl Erzeuger als auch Verbraucher.

Das Labornetz wurde mit Messsystemen, automatisierbaren Schaltern und Controllern ausgestattet. Alle Komponenten des Labors wurden über Kommunikationsprotokolle vernetzt und können darüber dann angesteuert werden. Zur Messdatenverarbeitung und für Schalthandlungen wurde ein Leitsystem implementiert. Umschaltungen im Labornetz ermöglichen es, verschiedene Topologien im Teststromkreis zu testen. Außerdem wurden netzdienliche Betriebsmittel, wie ein Spannungsregler, ins Labornetz integriert, um die Wirkungen und Nutzungsvorteile zu untersuchen. Parallel dazu wurden Messdatenverarbeitungssysteme mit verschiedenen Kommunikationsprotokollen und verschiedenen Cloud Systemen errichtet.

Die Untersuchungen im Forschungsprojekt sollen aufzeigen, wie sich das Netz in bestimmten Lastflusssituationen verhält und inwiefern durch Regel- und Steuerungsmaßnahmen das Netz beeinflusst werden kann. Mit geschlossener Kupplung entspricht das Labornetz einem Smart Grid, kann aber durch Trennung vom öffentlichen Netz als autarkes Inselnetz (Mikronetz) betrieben werden, in dem lokale Erzeugungskomponenten und Batteriespeicher die Verbraucher versorgen.

Anhand der Untersuchungen werden Kriterien für den Einsatz im realen Netz abgeleitet und ein Leitfaden für resiliente Smart Grids für Verteilnetze erstellt werden. Diese Aufgaben sind der in der Abbildung grafisch dargestellt.

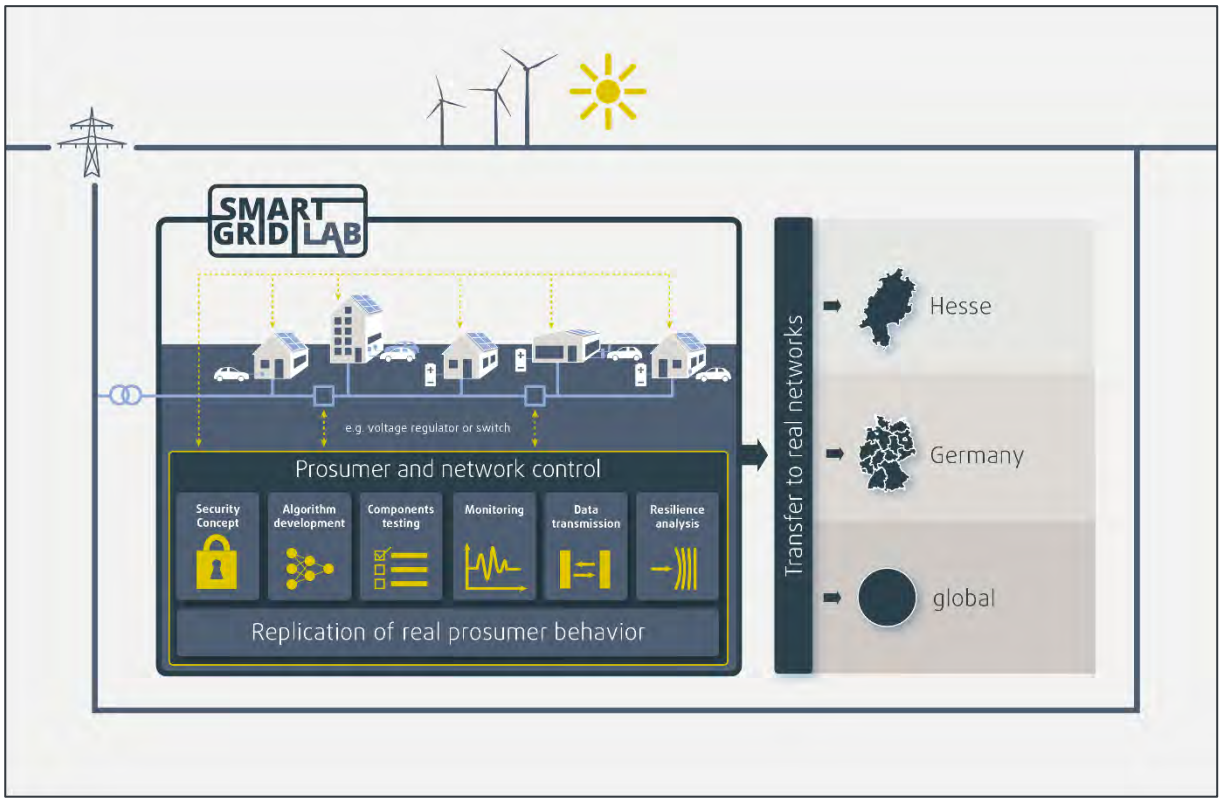


Abbildung 2: Projektgrafik.

Neben diesem funktionsorientierten Vorgehen, das die dynamischen Reserven bestehender Netzstrukturen für den Betrieb erschließt, bildet die Untersuchung von Sicherheit und Resilienz von Information Technology (IT) und Operational Technology (OT) einen Schwerpunkt des Projekts. Wie können Fehler im – autonom arbeitenden – Algorithmus erkannt werden, die durch Hacker, Manipulation von Daten oder auch Ausfall und Fehlfunktion von Sensoren, entstehen erkannt, behoben oder zumindest eingegrenzt werden. Welche Soft- und Hardwarestrukturen können hier unterstützen und welche Systemarchitekturen sind am besten geeignet? Durch die Nutzung der dynamischen Reserven des Netzes wird dessen Übertragungsfähigkeit erhöht. Die Zuverlässigkeit dieser neuen Betriebsweise hängt damit direkt mit der Sicherheit und Resilienz des unterlagerten IT-/OT-Systems zusammen.

Zu dem Konsortium welches von der Hochschule Darmstadt geleitet wird, gehören die Projektpartner Ingenieurbüro Pfeffer, JEAN MÜLLER, QGroup und Tractebel und das House of Energy an und bringen ihre Perspektiven aktiv mit ein.

Hochschule Darmstadt

Die Hochschule Darmstadt entwickelt zukünftige Verbrauchs- und Erzeugungsszenarien und nutzt die Erkenntnisse für das reale hessische Verteilnetz.

House of Energy

Das House of Energy etabliert einen wissenschaftlich-technischen Beirat, der die Projektpartner berät. In diesem werden Unternehmensvertreter aus den Gebieten Energieversorgung und Netzbetrieb, technische Überwachung und Zertifizierung, Personensicherheit und Energierecht mitwirken.

Ingenieurbüro Pfeffer GmbH

Das Ingenieurbüro Pfeffer ist für die Errichtung des Labors verantwortlich und stellt dazu auch eigene Infrastruktur zur Verfügung. Es erarbeitet Lösungen zur Verarbeitung von Daten intelligenter Ortsnetzstationen und deren Integration in Leitwarten und Cloudlösungen.

Jean Müller GmbH

Jean Müller entwickelt und fertigt vernetzungsfähige Niederspannungsschaltgeräte für die Smart-Grid Infrastruktur.

QGroup GmbH

Der Multilevel Security Hersteller QGroup betrachtet die Resilienz, um Risiken durch Cyberangriffe einzuschränken. Dabei werden Segregationsanforderungen hinsichtlich der IT/OT Versuchsstellungen, der eingesetzten Betriebsmittel, ihrer Vernetzung und Steuerung über Sicherheitsgrenzen untersucht.

Tractebel

Der Projektpartner Tractebel bringt seine Erfahrungen aus internationalen Energieinfrastruktur-Projekten ein und sorgt für Übertragbarkeit des Projektes auf den nationalen und internationalen Kontext.

1.1 Smart Grid

Das Hauptziel der Einführung von Smart Grids ist eine nachhaltige, sichere und wettbewerbsfähige Energieversorgung bei gleichzeitiger Aufrechterhaltung sicherer, stabiler und effizienter Systeme in Bezug auf Kosten und Energie. Es gibt keine allgemeingültige Definition für ein Smart Grid, sondern zahlreiche Definitionen verschiedener Organisationen. Die IEEE definiert ein Smart Grid als ein revolutionäres Unterfangen, das neue Kommunikations- und Steuerungsmöglichkeiten, Energiequellen, Erzeugungsmodelle und die Einhaltung von gerichtsübergreifenden Regulierungsstrukturen beinhaltet [6] während die IEA es als ein Stromnetzsystem definiert, das digitale Technologie zur Überwachung und Steuerung des Stromtransports aus allen Erzeugungsquellen einsetzt, um den unterschiedlichen Strombedarf der Endverbraucher zu decken [7]. Laut IEC ist Smart Grid ein Begriff, der eine Verbesserung des Stromnetzes umfasst, um den unmittelbaren Herausforderungen der nahen Zukunft gerecht zu werden, und eine Vision für ein zukünftiges Stromsystem auf lange Sicht mit einem erhöhten Maß an Beobachtbarkeit und Kontrollierbarkeit eines komplexen Stromsystems bietet [8].

Ein Smart Grid ist ein System, das sich aus verschiedenen Teilsystemen zusammensetzt und verschiedene Informations- und Kommunikationstechnologien mit Steuerungen und Sensoren verbindet, um sowohl den Versorgungsunternehmen als auch den Verbrauchern mehrere Vorteile zu bieten. Es gibt zahlreiche Beweggründe für die Einführung eines Smart Grids, die für eine Vielzahl von Akteuren gelten, darunter Versorgungsunternehmen, Energiedienstleister, Regulierungsbehörden, Verbrauchern, Prosumern und Regierungen. Abbildung 3 zeigt einige der Vorteile der Einführung von Smart Grids.

Smart Grids können durch neue Technologien wie FLISR (Fehlerortung, Isolierung und Systemwiederherstellung), ADMS (fortschrittliche Verteilungsmanagementsysteme), der Automatisierung von Umspannwerken, Zweiwegekommunikation bei dynamischen Bedingungen und Selbstheilungsfunktionen die Sicherheit und Zuverlässigkeit der Stromversorgung verbessern, was wiederum die Betriebskosten senkt und die Effizienz erhöht. Durch diese zusätzliche

Echtzeitbeobachtung und -steuerung können Erweiterungsinvestitionen vermieden oder hinausgezögert werden, was zu wirtschaftlichen Vorteilen führt. Aus ökologischer Sicht können die Treibhausgasemissionen durch die Umstellung von zentraler auf variable erneuerbare Energien, welche durch Smart Grids ermöglicht werden, reduziert werden.

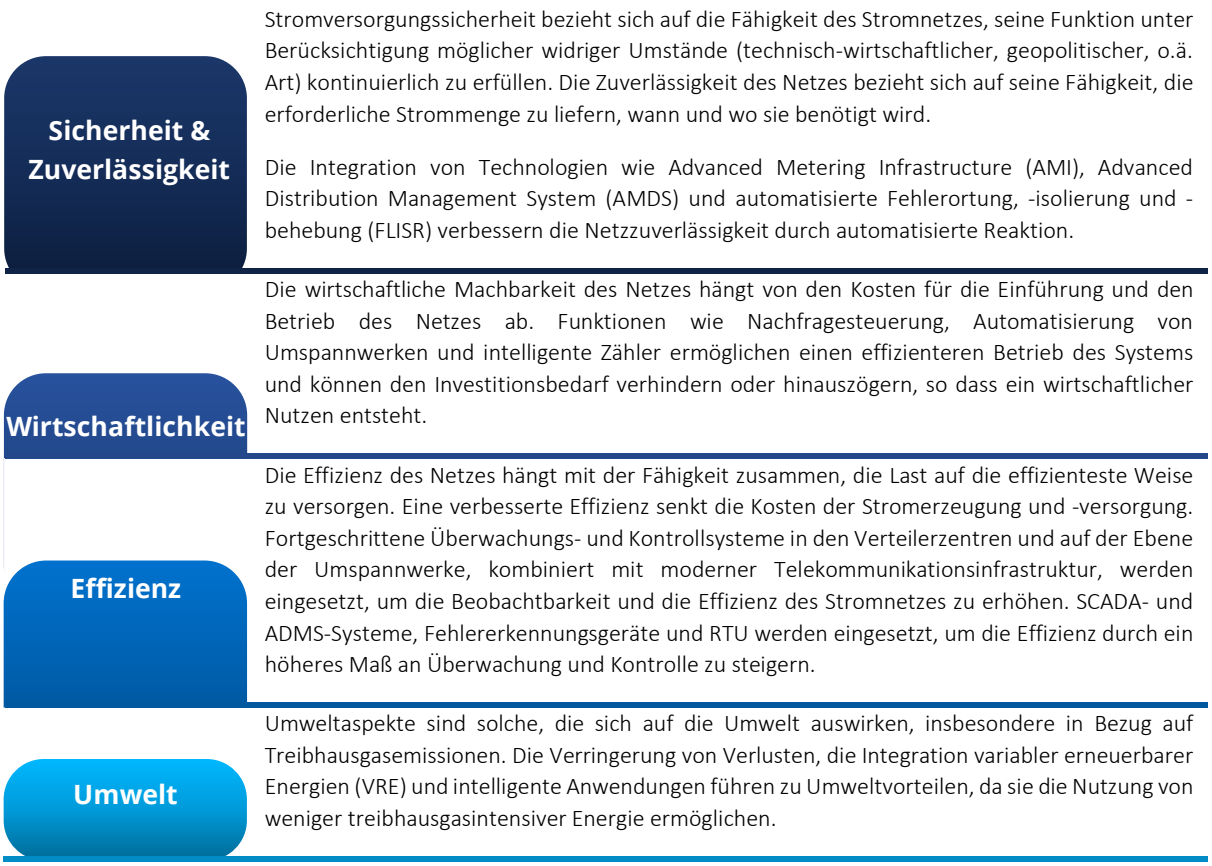


Abbildung 3: Vorteile von Smart Grids.

Die Vorteile der Smart Grids ergeben sich aus den Hauptfunktionen der Technologien. Diese Vorteile können in die folgenden Kategorien eingeteilt werden: Wirtschaftlichkeit, Zuverlässigkeit, Effizienz und Umwelt. Tabelle 1 zeigt die Vorteile für die verschiedenen Kategorien von Interessengruppen auf.

Tabelle 1: Vorteile des Smart Grids für Stakeholder.

INTERESSENTEN	MOTIVATIONEN DER SMART GRID IMPLEMENTIERUNG

VERBRAUCHER	**ZUVERLÄSSIGBARKEIT**: • Verbessertes Serviceniveau. • Das Management von Nachfragespitzen (oder Nachfragesteuerung) führt zu einem zuverlässigeren Dienst. **WIRTSCHAFTLICHKEIT**: • Verbesserte Verbrauchstransparenz führt zu geringerem Verbrauch und damit zu niedrigeren Stromrechnungen. • Fähigkeit zur Teilnahme an Flexibilitätsmärkten durch virtuelle Kraftwerke. • Aggregation von DERs und Monetarisierung dieser Anlagen. **EFFIZIENZ**: • Verbesserte Abrechnungsgenauigkeit und Zuverlässigkeit. **UMWELT:** • Bessere Möglichkeiten zur Beschaffung von Energie aus dezentraler VRE. • Ermöglicht das Aufladen von E-Fahrzeugen und damit eine Verringerung der verkehrsbedingten Treibhausgasemissionen.
NETZBETREIBER	**ZUVERLÄSSIGKEIT**: • Verringerung der Zahl der Ausfälle durch verbesserte Überwachungs- und Spitzenverschiebungsfunktionen. • Verkürzung der Störungsdauer (z. B. automatische Fehlersuche und -behebung). • Höhere Kundenzufriedenheit und bessere Kundenbeziehungen. • Aktives Energiemanagement der dezentralen Stromerzeugung, das die Nachfragespitzen reduziert und so die Belastung des Netzes verringert und Störungen abmildert. **WIRTSCHAFTLICHKEIT**: • Höhere Einnahmen aufgrund geringerer Stromverteilungsverluste. • Senkung der Betriebskosten durch verbesserte Abrechnungs- und Ertragsverwaltung. • Möglichkeiten für zusätzliche Einnahmequellen durch neue Märkte wie Einführung und Betrieb von Kleinstnetzen und neue Geschäftsmodelle wie tageszeitabhängige Tarife. • Senkung der Betriebskosten durch verstärkte Automatisierung. • Verringerung oder Verzögerung von Investitionen in den Netzausbau.

	• Implementierung fortschrittlicher Asset-Management-Modelle, die die Auslastung der Anlagenressourcen maximieren und die Zuverlässigkeit erhöhen. **EFFIZIENZ**: • Verringerung der wirtschaftlichen und technischen Verluste. • Steigerung der Effizienz und Beobachtbarkeit durch verbesserte Automatisierungs- und Überwachungstechnologien. • Verbesserte Betriebsmanagementsysteme verlängern die Lebensdauer der Anlagen. **UMWELT:** • Ermöglicht die verstärkte Integration von intermittierenden erneuerbaren Ressourcen. • Geringere Emissionen durch weniger Verluste. • Ermöglichung der Elektrifizierung neuer Lasten (z. B. E-Mobilität, hocheffiziente Heizsysteme wie elektrische Wärmepumpen).
ÜBERTRAGER	**ZUVERLÄSSIGKEIT**: • Wide Area Monitoring (z.B. Phasor Measurement Unit) verbessert die Stabilität des Systems. • Höhere Planungsgenauigkeit der Investitionen durch detailliertere Systemdaten. • Die Selbstheilung durch Automatisierung ermöglicht es dem Netz, sich dynamisch zu rekonfigurieren, um sich von Ausfällen von Netzkomponenten, Naturkatastrophen, Störungen usw. zu erholen. • Die Echtzeitsteuerung und -überwachung auf der Grundlage eines schnellen und genauen Datenaustauschs über das Netz verbessert die Zuverlässigkeit und Sicherheit des Systems und optimiert gleichzeitig die Übertragungsanlage. **WIRTSCHAFTLICHKEIT**: • Senkung der Betriebskosten durch verstärkte Automatisierung. • Durch die Verlagerung von Spitzenlasten werden Investitionskosten reduziert und/oder verschoben. • Dezentrale Erzeugung und Speicherung schaffen neue Marktchancen (z. B. Flexibilitätsmarkt). • Die Abflachung des Lastprofils minimiert die Betriebs- und Wartungskosten (O&M).

	EFFIZIENZ: • Geringere Überlastungen bei der Übertragung verbessern die Effizienz des Systems und verringern den Re-Dispatch. • Ermöglicht EMS- und Netzanwendungsfunktionen höherer Ordnung wie AGC, wirtschaftliches Dispatch, optimaler Leistungsfluss usw. **UMWELT:** • Ermöglicht die verstärkte Integration diskontinuierlicher erneuerbarer Ressourcen und reduziert dadurch die Treibhausgasemissionen.

1.2 Smart Grid Technologien

Das Smart Grid integriert mehrere Technologien, die die Effizienz und Sicherheit des Stromnetzes erhöhen. Gemeinsam sorgen diese Technologien für eine Kommunikation, die Überwachungs- und Steuerungsmöglichkeiten bietet. Dies führt jedoch auch zu komplexeren Systemen. In diesem Abschnitt werden die wichtigsten Smart-Grid-Technologien, ihre Anwendungen, Vorteile und die erforderliche Infrastruktur kurz beschrieben.

1.2.1. Zwei-Wege Kommunikationstechnologien

Die Informations- und Kommunikationstechnologie (IKT) ist der Baustein für einen sicheren, stabilen und wirtschaftlichen Netzbetrieb. Zusammen mit Sensor- und Messgeräten ermöglicht die IKT ein hohes Maß an Überwachung und Kontrolle der Prozesse und Anlagen im Stromnetz. Die Zwei-Wege-Kommunikation überträgt Informationen und Daten zwischen verschiedenen Geräten innerhalb des Stromnetzes. Im Allgemeinen gibt es zwei Arten von Kommunikationstechnologien, die in Stromversorgungssystemen verwendet werden: drahtgebundene oder drahtlose Kommunikation. Je nach Technologie liegen unterschiedliche Hardwareanforderungen, Reichweiten, Kosten und Zuverlässigkeit vor.

Kommunikationskabel werden eingesetzt, um Kommunikationskanäle zwischen zwei Enden (Sende- und Empfangsseite) aufzubauen, die physisch durch Kabel verbunden sind. Es gibt verschiedene Arten von Kommunikationskabeln: Twisted Pair, Koaxialkabel und Glasfaserkabel. Die Wahl des Kabeltyps hängt von der Anwendung und ihren Anforderungen ab. Digitale Daten können mit Geschwindigkeiten von bis zu 200 Gbit/s übertragen werden, mit einer Bandbreite von bis zu 4,7 GHz. Die Reichweiten beginnen bei 100 m und reichen bis zu 80 km.

Bei der drahtlosen Kommunikation werden Kommunikationskanäle zwischen zwei oder mehr Enden aufgebaut, die nicht physisch miteinander verbunden sind. Es gibt verschiedene Arten der drahtlosen Kommunikation, z. B. über Satelliten, Mobilfunknetze, ZigBee, WiMAX usw. Daten können mit einer Geschwindigkeit von bis zu 1000 Gbit/s und einer Bandbreite von bis zu 3 GHz übertragen werden. Die Reichweite reicht von 10 m bis zu 6.000 km.

Kommunikationskabel gelten im Allgemeinen als sicherer als drahtlose Kommunikationsnetze. Informationen können nur am Ende der Kabel abgefangen werden, während bei der drahtlosen

Kommunikation Informationen zwischen den Sende- und Empfangsknoten abgefangen werden können. Da in Stromnetzen nur die Netzbetreiber Zugang zu den Sende- und Empfangsknoten haben, bieten Kommunikationskabel ein sicheres Mittel zur Informationsübertragung innerhalb der Stromnetze. Andererseits bietet die drahtlose Technologie eine kostengünstige und flexible Lösung für die Kommunikation ohne die Kosten für die Kabel. Drahtlose IKT ist eine vielversprechende Lösung für die Datenübertragung, wenn strenge Verschlüsselungstechniken angewendet werden.

Im Rahmen des Projekts Smart Grid LAB Hessen hat die Tractebel Engineering GmbH einen kurzen Überblick über moderne Informations- und Kommunikationstechnologien in Stromnetzen veröffentlicht. Weiterführende Informationen zu diesem Thema liefert ein veröffentlichtes Paper in dem international Journal of Smart Grid [9].

1.2.2. Netzautomatisierungstechnologie

Bei der Netzautomatisierung werden Sensor-, Mess-, Steuerungs- und Kommunikationstechnologien eingesetzt, um den Betrieb des Stromnetzes und die Prozesse in Umspannwerken zu automatisieren. Eine Studie in [10] zeigt, dass die Netzautomatisierung die Möglichkeiten der Fehlerortung, -isolierung und -wiederherstellung verbessert hat und daher weniger und kürzere Ausfälle zu verzeichnen waren. Darüber hinaus wurden durch die Überwachung der Anlagen die Betriebskosten gesenkt und die Zahl der Anlagenausfälle verringert, was wiederum zu weniger Netzausfällen führte.

In alten Umspannwerken war die Sekundärseite der Feldgeräte (Leistungsschalter, Trennschalter, Mess- und Leistungstransformatoren usw.) über Kabel fest mit elektromechanischen Relais verbunden. Die Relais waren mit den SCADA-Systemen zur Überwachung und Fernsteuerung der Feldgeräte verbunden.

Abbildung 4 veranschaulicht die Automatisierungsebenen in modernen Umspannwerken. Die Prozessebene enthält die Mess- und Leistungstransformatoren, Schaltanlagen und andere verschiedene Sensoren. Die Feldebene besteht aus der Stationssteuerung und den intelligenten elektronischen Geräten (IED). IED ist ein digitales Relais, das als Schutz-, Mess-, Fehlererfassungs- und Steuergerät fungiert. Es enthält eine Signalverarbeitungseinheit, einen Mikroprozessor und eine Kommunikationsschnittstelle [11].

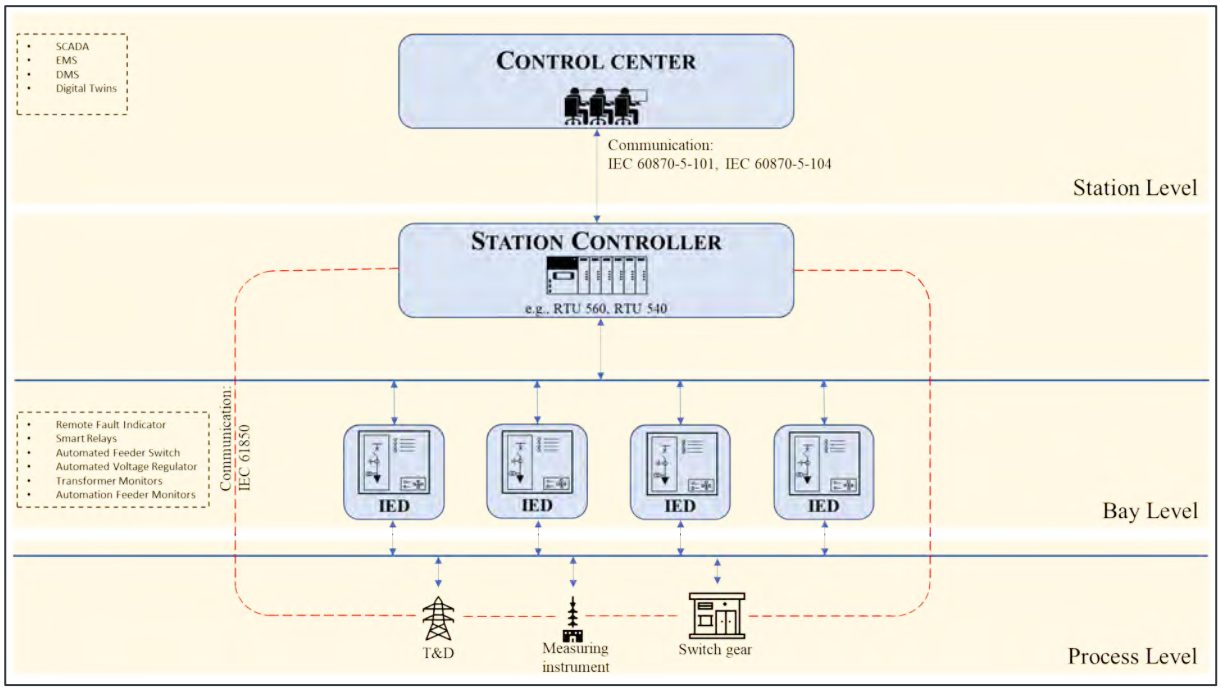


Abbildung 4: Automatisierungsebenen bei modernen Umspannwerken.

Remote Terminal Units (RTU) sind die Schnittstelle zwischen der Prozessebene und der Stationsebene. Die Hauptfunktion besteht darin, die Signale von den Feldsensoren und -Aktoren zu überwachen und jede Änderung an die Leitstelle zu melden.
Die Netzautomatisierung umfasst verschiedene Anwendungen wie Selbstheilung, Überwachung, Demand Side Response, Verteilungsmanagementsysteme, Smart Homes und Vehicle-to-Grid. Im nächsten Abschnitt werden diese Smart-Grid-Anwendungen erörtert.

1.3 Smart Grid Anwendungen

Die Fähigkeit, die Anlagen auf der Erzeugungs-, Übertragungs- und Verteilungsebene zu überwachen und zu steuern, ist einer der Hauptvorteile der Smart Grids gegenüber den herkömmlichen Netzen. Dies ist nur möglich, wenn die IKT bidirektional, in Echtzeit und zuverlässig arbeitet.

1.3.1. Selbstheilung

Bei der Selbstheilung werden Geräte zur Fehlerortung, Isolierung und Wiederherstellung von Diensten (FLISR) eingesetzt, um die Zuverlässigkeit und Verfügbarkeit des Netzes zu verbessern. Dazu gehören automatische Abzweigschalter und Wiedereinschaltvorrichtungen, Leitungsüberwachungsgeräte und Kommunikationstechnologien. FLISR ermöglicht die Rekonfiguration des Stromflusses im Falle von Störungen, um die Anzahl der betroffenen Kunden zu verringern und somit die Zuverlässigkeit und Verfügbarkeit des Netzes zu erhöhen. Die IKT bildet das Rückgrat dieser Smart-Grid-Anwendung. Eine Fallstudie des US-Energieministeriums aus dem Jahr 2016 hat gezeigt, dass die Zahl der von Stromausfällen betroffenen Kunden durch den Einsatz von FLISR um 55 % reduziert werden konnte [10]. Darüber hinaus wurde der System Average Interruption Duration Index (SAIDI) um 58 % gegenüber der Zeit vor der Einführung der FLISR-Anwendung verbessert.

1.3.2. Netzüberwachung und -steuerung

Die Netzüberwachung und -steuerung erfolgt über Supervisory Control and Data Acquisition (SCADA). SCADA ist eine Anwendung, die Software- und Hardwarekomponenten umfasst, die hauptsächlich aus speicherprogrammierbaren Steuerungen (SPS), Remote Terminal Units (RTU) und Sensoren bestehen, um unternehmenskritische Daten innerhalb des T&D-Netzes an lokalen oder entfernten Standorten in Echtzeit zu erfassen, zu überwachen und zu steuern. SCADA-Systeme sind skalierbare, konfigurierbare und integrierte Systeme, die je nach den Erfordernissen der Situation modifiziert werden können und einige Schlüsselparameter aufweisen:

- Überwachung, Steuerung und Analyse von Echtzeit-Prozessdaten aus dem T&D-Netz (Spannung, Frequenz, Status und Alarme von Geräten usw.)
- Kommunikation und Fernsteuerung verschiedener Geräte
- Direkte Schnittstelle über Human Machine Interface (HMI) mit verschiedenen Feldgeräten (RTUs, Schutzrelais IED, Leistungsschalter, Stromzähler usw.)
- Aufzeichnung und Protokollierung von historischen Daten und Ereignisse
- Klare Sichtbarkeit über die Grenzen des T&D-Netzes hinweg
- Höhere Zuverlässigkeit und Produktivität
- Reduziert die O&M-Reaktionszeit und die Betriebskosten

1.3.3. Advanced Metering Infrastructure (AMI)

AMI kombiniert intelligente Zähler, bidirektionale Kommunikationsnetze und Datenverwaltungssysteme, um eine zuverlässige und effiziente Stromerzeugung und -verteilung zu gewährleisten. Es sammelt Messdaten von drahtlosen Sensoren im gesamten Smart Grid, verarbeitet sie und sendet sie an das Versorgungsunternehmen. Auf der Grundlage dieser Daten können die Versorgungsunternehmen die Erzeugung und den Verbrauch ausgleichen, so dass die Kosten für den Einsatz teurer Spitzenstromerzeuger zur Deckung des Spitzenbedarfs vermieden werden können. Darüber hinaus senkt AMI die Kosten für Messung und Abrechnung und gibt dem Kunden mehr Kontrolle über den eigenen Stromverbrauch und die Kosten [12].

Abbildung 5 zeigt eine Anwendung zur intelligenten Verbrauchsmessung mit AMI. Die ferngesteuerte und automatische Verbrauchsmessung ist eine wichtige Anwendung, die mit herkömmlichen Messsystemen nicht möglich ist. Intelligente Geräte, Hausautomatisierungs- und Sicherheitsanwendungen, Ladestationen für Elektrofahrzeuge sowie dezentrale Erzeugungsanlagen, wie z. B. PV-Anlagen, senden Verbrauchs- und Erzeugungsdaten an das Home Energy Management System (HEMS), wo sie analysiert und an den intelligenten Zähler weitergeleitet werden. Der intelligente Stromzähler speichert die kWh-Zählerstände in regelmäßigen Abständen (in der Regel alle 15-60 Minuten) und sendet sie dann zweimal täglich an das Versorgungsunternehmen. Das Home Area Network (HAN) ist ein geschlossenes Kommunikationsnetz, in dem alle Haushaltsgeräte einschließlich des intelligenten Zählers verbunden sind. Die Kommunikation innerhalb des HAN erfolgt über das Kommunikationsprotokoll ZigBee. AMI bietet die Flexibilität, Nachfragespitzen abzumildern und zu reduzieren.

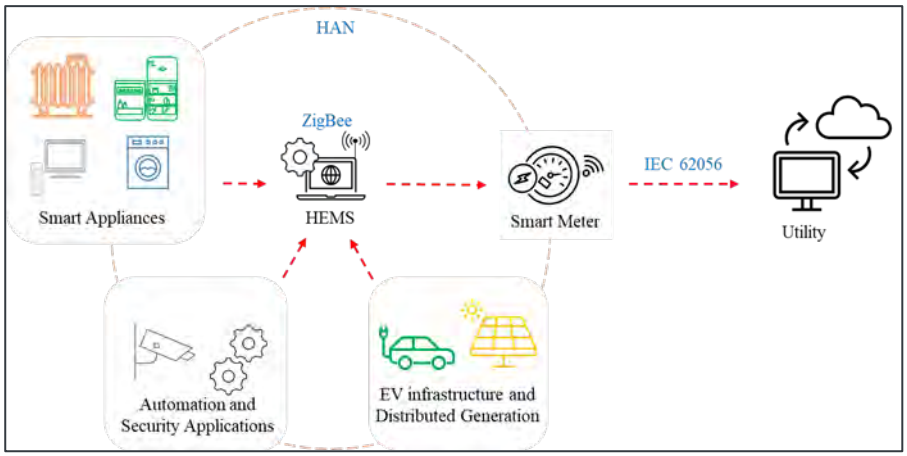


Abbildung 5: Intelligente Verbrauchsmessung.

1.3.4. Demand Side Response (DSR)

DSR nutzt flexible Lasten, verteilte Erzeugung und Speichersysteme, um verschiedene Dienste wie Lastverschiebung, Spitzenkappung, dynamisches Energiemanagement, Auffüllen von Tälern und Verbesserung der Energieeffizienz zu leisten [11]. Zu den flexiblen Lasten, die auch als intelligente Geräte (Smart Appliances) bezeichnet werden, gehören Wärmepumpen, Waschmaschinen, Kühl- und Gefrierschränke, Geschirrspüler sowie Elektrofahrzeuge (EV). Flexible Lasten sind elektronische Haushaltsgeräte mit Kommunikationsfähigkeiten. Durch die Verwendung dynamischer Preise und Preissignale können intelligente Geräte den Startzeitpunkt ändern oder den Betrieb zu einem späteren Zeitpunkt unterbrechen, um Spitzenzeiten zu vermeiden. Vor dem Start eines Vorgangs eines intelligenten Geräts (z. B. Waschen, Kühlen usw.) muss der Benutzer einige Parameter wie die Endzeit oder die gewünschte Temperatur eingeben. Das Gerät arbeitet dementsprechend und beendet den Prozess zur angegebenen Zeit oder hält die Temperatur innerhalb der vom Benutzer eingegebenen Werte. Dies minimiert die Unannehmlichkeiten im Tagesablauf des Benutzers und bietet Anreize, während das Versorgungsunternehmen die Spitzenlast reduziert und den Einsatz teurer Stromerzeugungsanlagen, oder die Notwendigkeit einer Netzverstärkung vermeidet. Auf diese Weise schaffen intelligente Geräte eine Win-Win-Situation für beide Parteien, den Kunden und das Versorgungsunternehmen.

Andere intelligente Geräte wie Beleuchtungssysteme, Soundsysteme und Unterhaltungsgeräte sowie Hausautomatisierungssysteme können die Energieeffizienz von Haushalten verbessern und den Gesamtenergieverbrauch senken. Auch dies schafft eine Win-Win-Situation für beide Seiten, den Kunden und das Versorgungsunternehmen.

1.3.5. Distribution Management Systems (DMS)

DMS ist eine Smart-Grid-Anwendung, die zur Überwachung, Steuerung und Optimierung der Leistung von Verteilungsnetzen eingesetzt wird. Sie ermöglicht eine aktive Steuerung der Lastnachfrage sowie integrierte Verteilerenergieressourcen und eine effektivere Nutzung der Verteilernetzanlagen [11]. In Verteilungsnetzen ist das DMS immer mit SCADA-Systemen verbunden, in denen Datenerfassung, Ereignisverarbeitung und Steuerungsprozesse stattfinden.

1.3.6. Zusammenfassung

Die aktuellen Herausforderungen des Stromnetzes wie der stark steigende Strombedarf und die alternde Infrastruktur erfordern intelligente Lösungen und Technologien. Die Integration der Netzüberwachung und -steuerung ermöglicht die Digitalisierung und Echtzeitüberwachung, um die Zuverlässigkeit des Netzes zu erhöhen. Die Integration dezentraler erneuerbarer Energiequellen (DRES) trägt zur Verringerung der Stromverluste und damit zur Senkung der Betriebskosten sowie zur Erhöhung der Zuverlässigkeit des Netzes bei. AMI erhöht die Flexibilität des Netzes durch DSR und nutzt die Netzressourcen, wodurch die Betriebskosten gesenkt werden.

2. Aufbau des Smart Grid LAB

Der Aufbau des Labors lässt sich in zwei Teilen unterscheiden. Der erste Teil ist die Primärtechnik und betrifft den Aufbau der nachzubildenden Netzstrukturen auf der Niederspannungsebene. Der zweite Teil besteht aus der Sekundärtechnik. Es sind die Komponenten zu analysieren, welche Komponenten bei Verteilnetzbetreibern gängig sind. Das Leitsystem und die Anbindungen in verschiedene Cloudlösungen bauen dann darauf auf.

2.1 Primärtechnik

Die Primärtechnik besteht aus drei wesentlichen Kapiteln. Das erste Kapitel beschreibt wie und auf welcher Grundlage das Labornetz erzeugt erstellt wurde. Das zweite beinhaltet die Auswahl und Bestellung der Komponenten für die Primärtechnik.

2.1.1. Labornetz

Grobkonzept

In der Projektskizze wurde schon ein erster Wurf für das Grobkonzept getätigt, siehe Abbildung 6. Mit 16 Wechselrichtern (in der Skizze Stromrichter genannt) die verschiedensten „Lastfälle (z.B. Wohngebäude, Elektroladesäule, gewerbliches Gebäude) und Einspeisefälle (Batterie, Solaranlage)“ [13] nachzubilden. Es entstehen so zwei Stromkreise, den Test- und den Energiestromkreis.

Der Energiestromkreis bildet die Energieversorgung bzw. die Energierückführung für die Wechselrichter. Um diesen Kreis zu entkoppeln und die Verunreinigungen durch die Wechselrichter zu wird eine Drosselspule eingesetzt.

In der Projektskizze ist der Teststromkreis mit „vier Kabelabschnitten, fünf fernsteuerbaren Lasttrennschaltern zur Segmentierung, vier Spannungslängsreglern, 16 Stromrichtern (20 kW) mit Gleichstromzwischenkreis und Anbindung und den Energie-Stromkreis, Messsensoren und Stellungsmeldungen, Steuerung und Datenerfassung (SCADA), Schutzrelais mit Parameteradaption, Datenimport“ [13] beschrieben. Es ergeben sich acht Wechselrichterpaare.

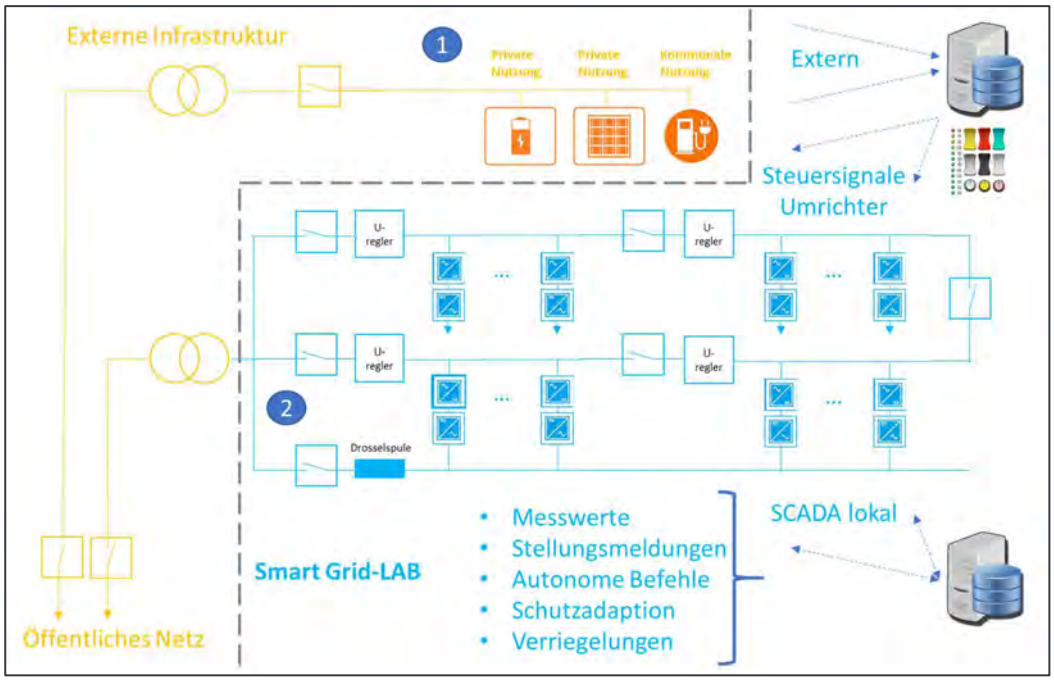


Abbildung 6: Struktur der geplanten Ortsnetzstation und externen Infrastruktur (ockergelb) sowie des Smart Grid-LAB [13].

Feinkonzept

Der Energiestromkreis ist in seiner Funktion und Umsetzung in der Feinplanung unverändert, es wurde nur die Drosselspule ausgelegt. Dafür waren die Leistungen der Wechselrichter ausschlaggebend.

Für die Feinplanung kam der Gedanke auf, dass eine Strangverschaltung ohne Impedanzen zu keinen nennenswerten Spannungsabfällen führt und es in der Realität Verzweigungen in den Niederspannungsnetzen vorkommen. Aus diesem Grund wurde ein Benchmarking durchgeführt. Als Referenznetze wurden vor allem die Studie „SimBench“ der TU Dortmund und Studien der TU Dresden herangezogen.

Netztopologien nach SimBench

Die Ergebnisse im Projekt SimBench zeigen Modelle des Niederspannungsnetzes, welche in Deutschland durchschnittlich zu finden sind. In einer Fallstudie [14] werden ca. 8000 Netzgebiete in sechs Netztopologien zusammengefasst. Dieses Cluster wird als Basis der Netztopologien verwendet. Es wird zwischen drei ländlichen, zwei halbstädtischen und einem städtischen Netz unterschieden. In den Modellen werden Transformatoren der Größe 160, 250 und 630 kVA verwendet. Es wird von einer durchschnittlichen Last pro Haushalt von 2 kW ausgegangen. Die ländlichen Modelle sind mit Leitungen mit einem Kabelquerschnitt von 150 mm2 und die vorstädtischen und städtischen Modelle mit 240 mm2 ausgelegt. In der Leitungslänge sind die einzelnen Netzanschlüsse nicht berücksichtigt (vom Strang zum endgültigen Verbraucher). Es wird jeweils das Netz verwendet, welche die kürzeste Strecke zum Zentrum der Gemeinde aufweist. [14]

Abbildung 7 zeigt eine Tabelle der sechs geclusterten Netztopologien und deren Netzparameter. Zu erkennen ist, dass bei dem ländlichsten Netz (LV 01) die Distanz zwischen den Abgängen mit 40 m (560 m/13 Abgänge) am größten ist und die Gesamtlänge des Netzes gering. Die Last pro Verbraucher liegt bei ca. 6 kW bei einer Gesamtlast von 80 kW. Die Erzeugung mit insgesamt 160 kW bei vier Erzeugern liegt pro Erzeuger mit 40 kW hoch. Insgesamt ist die Anzahl der Verbraucher gering.

Das ländliche Netz (LV 02) unterscheidet sich zu LV01 in der Hinsicht, dass die Leitungslänge das 2,6-fache der Leitungslänge entspricht und die Gesamtlast von 202 kW bei 99 Verbrauchern anliegt. Die Erzeugung pro Erzeuger liegt bei ca. der Hälfte im Vergleich zu LV01. Pro Erzeuger ergibt sich eine Einspeisung von 18 kW bei insgesamt 145 kW.

Die Cluster LV 03 und LV 04 weisen jeweils ähnliche Parameter auf, welche sich nur in der Hinsicht unterscheiden, dass LV 04 das dreifache an Einspeisung besitzt und somit auch das dreifache der anderen Parameter im Vergleich zu LV 03 aufweist. Ein signifikanter Unterschied stellt jedoch die Einspeisung dar. Während in dem Modell von LV 03 eine gesamte Einspeisung von 190 kW bei 17 Erzeugern zu finden ist, weist LV 04 nur eine Einspeisung mit 6,5 kW auf. Die Last pro Verbraucher entspricht bei LV 04 das Doppelte wie in LV 03. Die Distanz zwischen den Verbrauchern liegt bei ca. 20m, was die Hälfte der Distanz von LV 01 entspricht. Für die weiteren Untersuchungen wird das Modell LV 04 herangezogen.

Das Modell LV 05 wird der Vorstadt zu geordnet und unterscheidet sich nicht gravierend zu LV 06. Das Netz LV 06 weist eine kürzere Gesamtlänge auf und bei ungefähr gleicher Anzahl von Verbrauchern kommt LV 06 zu einer Distanz zwischen den Verbrauchern von 10 m. Das Modell Stadt weist somit die kürzeste Strecke zwischen den Verbrauchern auf im Vergleich zu den anderen Netztopologien. Insgesamt weist das Netz eine hohe Anzahl an Verbrauchern auf, was zu einer hohen Gesamtlast führt. Die Last pro Verbraucher liegt bei 4 kW, was im Vergleich zu den anderen Lasten mittelmäßig einzuordnen ist. Die Einspeisungen sind in dem Stadt Modell gering und liegen bei einer Gesamteinspeisung von 57 kW bei fünf Erzeugern.

	LV 01	LV 02	LV 03	LV 04	LV 05	LV 06
Cluster	rural 3	rural 2	rural 1	semi-urban 2	semi-urban 1	urban
Transformer S_r [kVA]	160	250	400	400	630	630
Number of feeders	4	4	9	3	6	7
Overall linelength [km]	0.56	1.47	2.35	0.75	1.79	1.08
Number of loads	13	99	118	41	104	111
Overall load [kW]	80	202	331	243	409	441
Number of DER	4	8	17	1	9	5
Installed DER power [kW]	160	145	190	6.5	137	57

Abbildung 7: Parameter der Netzmodelle nach SimBench [15].

In der Untersuchung sind in den Netztopologien drei bis neun Einspeisungen im Netz zu finden. In dem Laboraufbau wird maximal eine Einspeisung realisiert. Die Parameter werden auf die Anzahl der Einspeisungen und auf die Anzahl der Verbraucher skaliert. Für die weitere Analyse der Netztopologie für das Smart Grid Lab werden die Netzmodelle LV 01, LV 02, LV 04 und LV 06 weiter untersucht und mit den Ergebnissen aus [15] verglichen. Die Leitungslänge vom Strang bis zum Hausanschluss ist nicht berücksichtigt.

Im Vergleich zu [16] ist dort die Leitungslänge vom Strang bis zum Hausanschluss mit 15 m in der Gesamtleitungslänge enthalten.

Bei Muffenanschlüssen liegt die durchschnittliche Hausanschlusslänge bei 12 m und beim Anschluss über einen Kabelverteilerkasten bei 32 m. [17]

Netztopologien nach Forschungsarbeiten der TU Dresden [16]

In der Untersuchung der TU Dresden [16] werden Niederspannungsnetze auf Basis von Niederspannungsnetzen in Deutschland geclustert. Es wird zwischen unverzweigten Netzen und Netzen mit Verzweigung unterschieden (siehe Abbildung 8). Bei der Leitungslängenangabe sind die Längen der Netzanschlüsse mit 15m von Strang zum Hausanschluss berücksichtigt. Für den Vergleich zu [15] werden die 15m von der Distanz zwischen den Verbrauchern subtrahiert.

Bei der Unterscheidung der Fälle sind die folgenden Parameter wie folgt definiert:

B0= Strangnetz ohne Verzweigungen

B1= Strangnetz mit einer Verzweigung

B2= Strangnetz mit zwei Verzweigungen

B3= Strangnetz mit drei Verzweigungen

lBx= Leitungslänge auf dem Hauptstrang (x=0,1,2,3)

ltotal= gesamte Leitungslänge (Hauptstrang mit Verzweigungen)

nDP Bx= Anzahl der Verbraucher auf dem Hauptstrang

dDP= Abstand zwischen den Verbrauchern

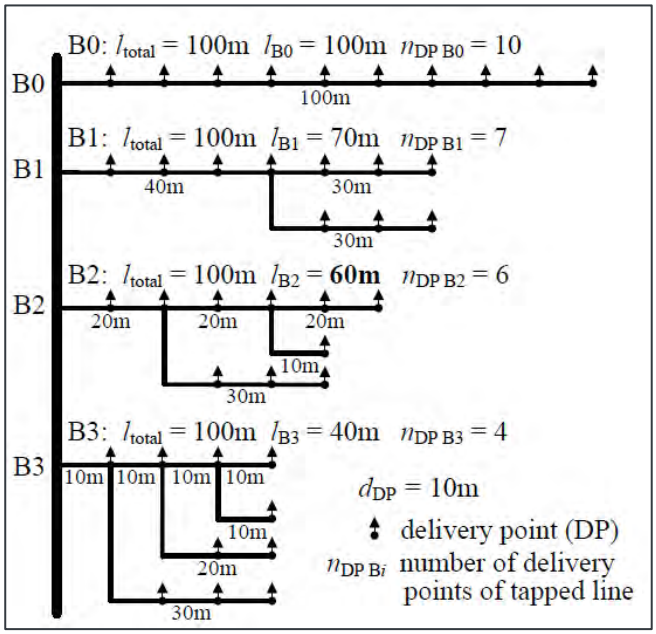


Abbildung 8: Netztopologien B0, B1, B2 und B3 [16].

In der Abbildung 9 ist eine Tabelle zur Unterscheidung der Netzparameter für die Netztopologien B0, B1, B2 und B3 zu sehen. Jede Typologie wird nach Einspeisungstyp kurz, mittel und lang differenziert, wobei es zwei kurze Einspeisungstypen gibt mit der Unterscheidung ein Verbraucher bzw. mehrere Verbraucher. Innerhalb dieser Differenzierung werden Netze nach den Parametern nDP Bx und dDP unterschieden. Zusätzlich sind bei jeder Typologie die Parameterkombination in einen „guten Fall", „durchschnittlichen Fall" und einem „schlechtem Fall" zugeordnet.

TABLE III. PARAMETERS FOR BENCHMARK FEEDERS – CABLE

	d_{DP}	$n_{DP\,B0}$	l_{B0}	$n_{DP\,B1}$	l_{B1}	$n_{DP\,B2}$	l_{B2}	$n_{DP\,B3}$	l_{B3}
short	60	1	60	*good case*					
	120	1	120	*average case*					
	80	2	160	*worse case*					
	80	3	240	2	160	*good case*			
	50	6	300	4	200	*average case*			
	40	10	400	7	280	*worse case*			
mid	40	15	600	10	400	9	360	*good case*	
	35	20	700	14	490	11	385	*average case*	
	30	25	750	17	510	14	420	*worse case*	
long	30	*30*	*900*	*good case*		15	450	12	360
	30	*40*	*1200*	*average case*		21	630	16	480
	30	*50*	*1500*	*worse case*		26	780	20	600

all lengths and distances in m

Abbildung 9: Parameter für Benchmark Einspeiseleitungen [16].

Für die weiteren Untersuchungen für die Netztopologie des Smart Grid Labs werden die Parameter aus [15] als Grundlage verwendet und mit den Parametern aus Abbildung 28 abgeglichen. Daraus sollen Gemeinsamkeiten gefunden und mit den Möglichkeiten des Smart Grid Labs umgesetzt werden.

Im Smart Grid LAB Hessen ist es angedacht gewesen nur einen Strang von Niederspannungsnetzen abzubilden. Um ganze Netz aus der Niederspannung abbilden zu können, wäre ein größeres Labor notwendig. Die Qualität der Ergebnisse würde dadurch jedoch nicht steigen, weil Engpässe, bestehend aus Spannungsbandverletzungen und Überbeanspruchung, je Strang betrachtet werden müssen. Und eine Überbeanspruchung des Ortsnetztransformators, lässt sich durch eine Übertragung der Gleichzeitig des einzelnen Stranges ermitteln.

Aus den oben genannten Arbeiten wurden vier Kategorien für das Smart Grid LAB Hessen abgeleitet.

Land, Dorf, Vorstadt und Stadt

Netztopologie Land

Nach der Untersuchung [15] weist das ländliche Netz eine Netztopologie ohne Verzweigung auf. In Abbildung 10 ist das Netz LV 01 zu sehen, welches ländliche Netztopologien nachbildet. Zum Vergleich wird der blaue Strang mit drei Abgängen für Land 1 und der grüne Strang mit vier Abgängen für Land 2 verwendet. Bei einer Gesamtlänge von 560 m und 13 Verbrauchern ergibt sich unter der Berücksichtigung der Kabelquerschnittumrechnung (von NAYY 150 m² zu 240 m² / Faktor 1,648) eine Distanz zwischen den Abgängen von 71 m. Bei vier Lasten ergibt sich eine Gesamtnetzlänge von 284 m.

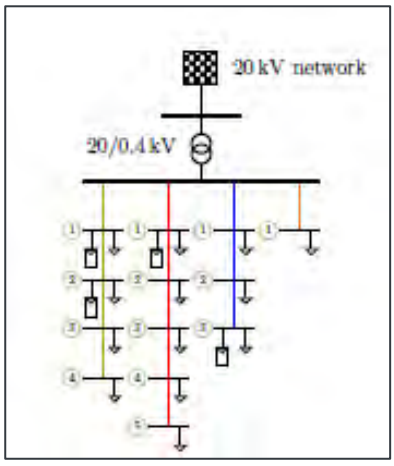


Abbildung 10: Netztypologie Land [15].

Nach den Netztopologien [16] fällt das Strangnetz ohne Verzweigung in die Topologie B0 (Abbildung 11). Bei fünf Abgängen liegt die Distanz zwischen den Verbrauchern bei 50 m, das heißt abzüglich der 15m welche bei dem vorherigen Referenznetz nicht berücksichtigt sind, 35 m und umfasst eine Gesamtlänge von 240 m-300 m bei 3-6 Lasten. Damit liegt das Netz laut der Tabelle im guten bis durchschnittlichen Fall. Zu den anderen Netzparametern liegen keine Angaben vor.

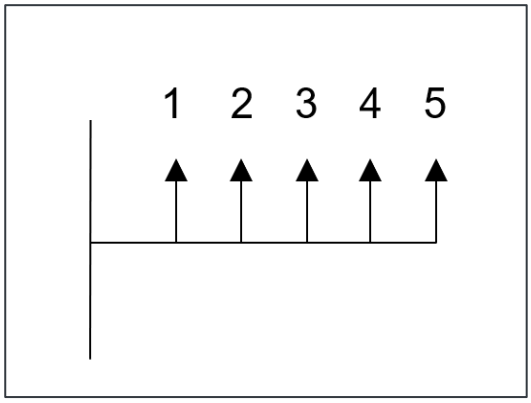


Abbildung 11: Netztopologie in Anlehnung an [16] ohne Verzweigung.

Im Vergleich der Netztopologien ergeben sich folgende Distanzen zwischen den Verbrauchern und Leitungslängen für die Netztopologie Land, welche in Tabelle 2 dargestellt sind. Die Netztopologie Land weist keine Netzverzweigungen auf und hat nach [15] eine Last pro Verbraucher von 6 kW bei einer Gesamtlast von 80 kW und eine Einspeisung von 160 kW, wobei eine Einspeisung bei 40 kW liegt.

Tabelle 2: Vergleich der Netzlänge bei einem Kabelquerschnitt von 240mm2 zwischen [15] (LV01), [16] (B0) und Smart Grid Lab Netztopologie Land1 und Land2.

	Referenznetz TU Dortmund [15]	**Referenznetz TU Dresden [16]**	**SGL Land 1**	**SGL Land 2**
Distanz zwischen Abgängen [m] (Mittelwerte)	71	35	71	73
Gesamtlänge* [m]	284 (*bei 4 Lasten)	240-300 (*bei 3-6 Lasten)	285 (*bei 4 Lasten)	295 (*bei 4 Lasten)

In der Abbildung 12 sind zwei Varianten von Netztopologien für die ländliche Region für das Smart Grid Lab dargestellt. Es wird eine Gesamtlast von 25 kW über die Wechselrichter hinzu geschaltet. Die 25 kW ergeben sich aus der Überlegung, dass pro Verbraucher 6 kW Last anliegt. Das Netz hat eine Gesamtlänge von 285 m bzw. 295 m.

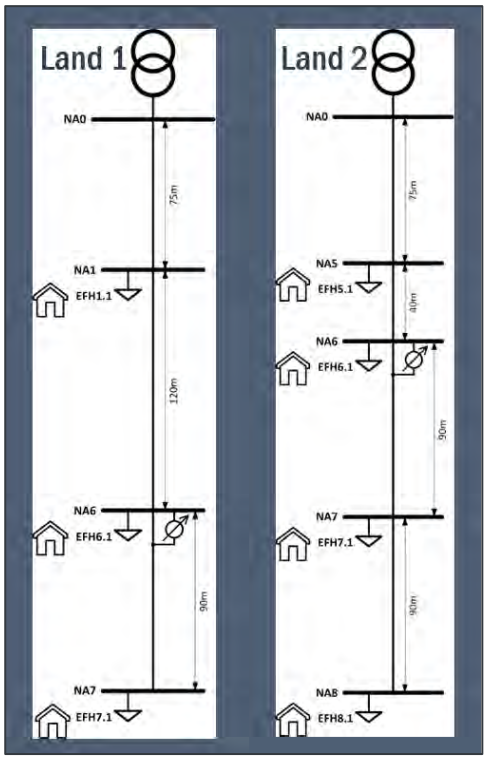


Abbildung 12: Netztopologien Land 1 und Land 2.

Netztopologie Dorf – einfach verzweigt

Als Referenznetz wird der grüne Strang von LV 02 verwendet. (siehe Abbildung 13). Dieses Referenznetz bildet dörfliche Netze mit einfachen Verzweigungen nach. Bei einer Gesamtlänge von 1470 m und 99 Verbrauchern ergibt sich unter der Berücksichtigung der Kabelquerschnittumrechnung (Faktor 1,648) eine Distanz zwischen den Abgängen von 24,72 m. Bei 22 Lasten ergibt sich eine Gesamtlänge von 543,84 m. Die 22 Verbraucher sind mit jeweils 2,04 kW angeschlossen. Insgesamt ergibt sich für den grünen Strang einen Verbrauch von 44,8 kW.

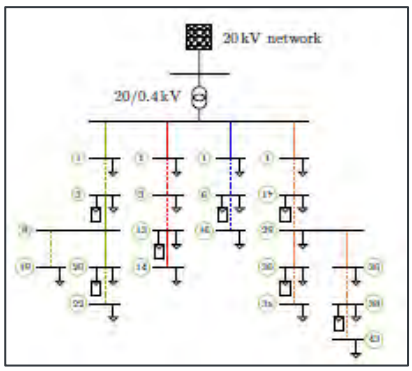


Abbildung 13: Netztopologie LV02 Land/ Vorstadt [15].

Nach den Netztopologien [16] fällt das Strangnetz mit einer Verzweigung in die Topologie B1 (Abbildung 14).

Bei 20 Abgängen am Hauptstrang ergibt sich eine Distanz zwischen den Abgängen von 20 m (35 m-15 m). Mit 20 Abgängen und 20 m Distanz beträgt die Gesamtlänge der Leitung 400 m. Damit liegt das Netz laut der Tabelle 3 im durchschnittlichen Fall. Zu den anderen Netzparametern liegen keine Angaben vor.

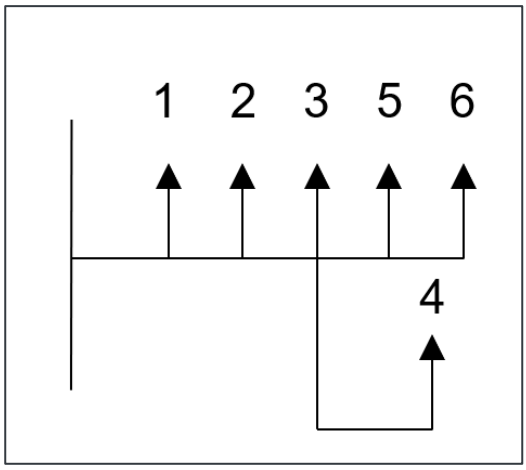


Abbildung 14: Netztopologie in Anlehnung an [16] mit einer Verzweigung.

Für die Netztopologie Dorf ergeben sich folgende Netzlängen im Vergleich (Tabelle 3). Es werden zwei Netztopologien mit den Netzabschnitten verschaltet mit jeweils einer Verzweigung (Abbildung 15). Die Netztopologie Dorf 1 hat eine Gesamtlänge von 490 m bei 22 m Distanz zwischen den Abgängen. Die zweite Netztopologie umfasst eine Gesamtlänge von 545 m bei 25 m Distanz zwischen den Abgängen. Im zweiten Netz kann die Last, aufgrund der höheren Anzahl von Netzabschnitten, höher eingestellt werden als in der ersten Netztopologie. Die Anzahl der Verbraucher bzw. der Netzabschnitte sind im zweiten Netz nach dem Spannungsregler höher und können hier höhere Spannungsabweichungen verursachen. Das Netz wird mit einer Gesamtlast von 44 kW bei insgesamt 22 Lasten belastet und bildet so ein durchschnittlich ausgelastetes Netz nach [15].

Tabelle 3: Vergleich der Netzlänge bei einem Kabelquerschnitt von 240mm2 zwischen [15] (LV02), [16] (B1) und Smart Grid Lab Netztopologie Dorf1 und Dorf2.

	Referenznetz TU Dortmund [15]	**Referenznetz TU Dresden [16]**	**SGL Dorf 1**	**SGL Dorf 2**
Distanz zwischen Abgängen [m] (Mittelwerte)	24,72	20	22	25
Gesamtlänge* [m]	543,8 (*bei 22 Lasten)	400 (*bei 20 Lasten)	490 (*bei 22 Lasten)	545 (*bei 22 Lasten)

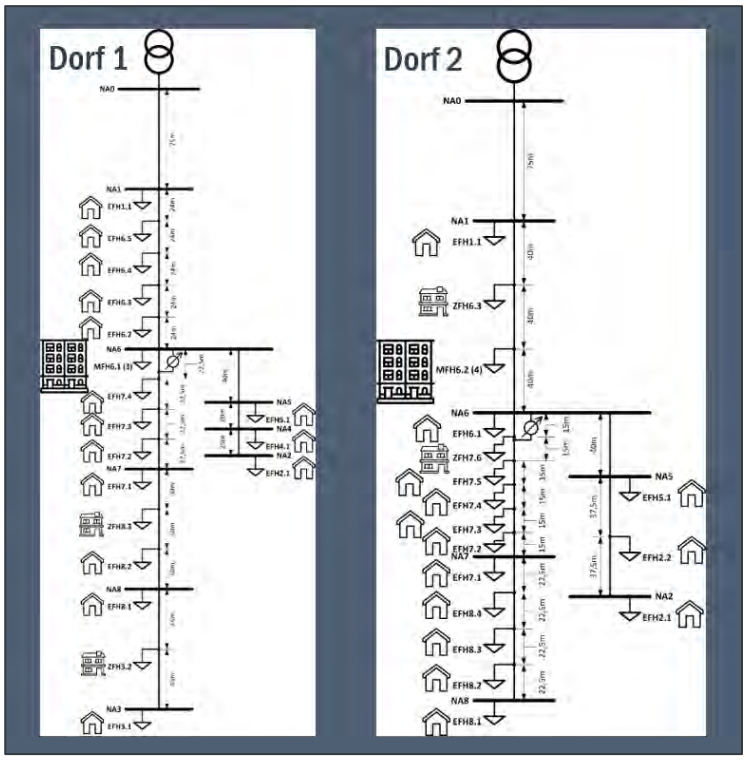


Abbildung 15: Netztopologien Dorf 1 und Dorf 2.

Netztopologie Vorstadt – mehrfach verzweigt

Zur Nachbildung der Netztopologie Vorstadt wird aus dem Referenznetz nach [15] der blaue Strang zur Referenz verwendet. In Abbildung 16 ist das Referenznetz LV04 für die Topologie Vorstadt dargestellt. Die Netztopologie Vorstadt weist eine höhere Verzweigung auf, als die Netztopologien Land und Dorf. Mit einer Gesamtlänge von 750 m und 41 Verbrauchern liegt die Distanz zwischen den Verbrauchern im Durchschnitt bei 18,29 m. Für den blauen Strang ergibt sich eine Gesamtlänge von 475 m. Bei einer Gesamtlast von 243 kW lässt sich eine Leistung von 5,9 kW pro Verbraucher errechnen. Für den blauen Strang ergibt sich eine Gesamtlast von 153,4 kW bei 26 Lasten.

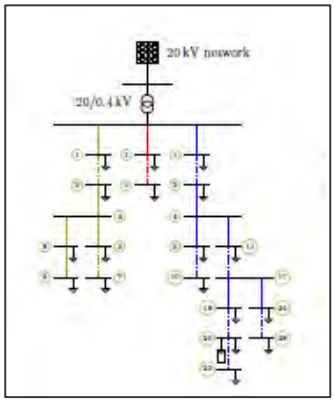


Abbildung 16: Netztopologie LV04 Vorstadt [15].

Nach dem Referenznetz aus [16] entspricht die Topologie Vorstadt der Topologie B2 aus [16]. Diese Netztopologie weist zwei Verzweigungen auf (siehe Abbildung 17). Bei 26 Lasten am Hauptstrang, wie aus dem vorherigen Referenznetz mit blauem Strang, ergibt sich aus [16] eine Distanz zwischen den Abgängen von 15 m (30 m-15 m). Bei 40 Abgängen beträgt die Gesamtleitung 600 m.

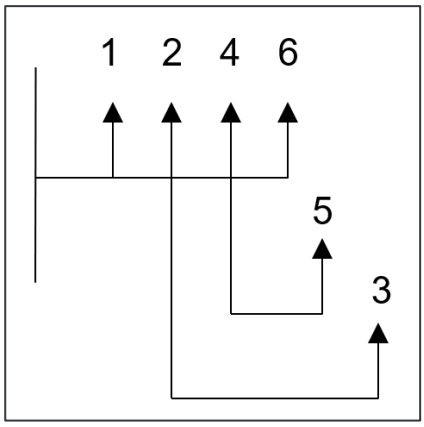


Abbildung 17: Netztopologie in Anlehnung an [16] mit zwei Verzweigungen.

Für die dritte Netztopologie Vorstadt werden zwei Varianten mit jeweils zwei Netzverzweigungen für das Smart Grid Lab entworfen (Abbildung 18). Die Leitungslängen sind in der Tabelle 4 im Vergleich dargestellt. Die Distanz zwischen den Verbrauchern liegt nach den Untersuchungen in [15] bei durchschnittlich 18m und in [16] bei 15m. Bei 26 Lasten wird eine Gesamtlast von 154 kW simuliert. Es liegt pro Last ein Verbrauch von 6 kW an und simuliert so ein durchschnittliches Netz der Netztopologie Vorstadt. In der Netztopologie Vorstadt 1 liegt die Distanz zwischen den Verbrauchern bei 21 m bei einer Gesamtlänge von 545 m. Für die Topologie Vorstadt 2 wird eine Distanz von 19 m zwischen den Verbrauchern gewählt und eine Gesamtlänge von 490 m bei 26 Lasten.

Tabelle 4: Vergleich der Netzlänge bei einem Kabelquerschnitt von 240mm2 zwischen [15] (LV04), [16] (B2) und Smart Grid Lab Netztopologie Vorstadt1 und Vorstadt2.

	Referenznetz TU Dortmund [15]	**Referenznetz TU Dresden [16]**	**SGL Vorstadt 1**	**SGL Vorstadt 2**
Distanz zwischen Abgängen [m] (Mittelwerte)	18	15	21	19
Gesamtlänge* [m]	475 (*bei 26 Lasten)	600 (*bei 40 Lasten)	545 (*bei 26 Lasten)	490 (*bei 26 Lasten)

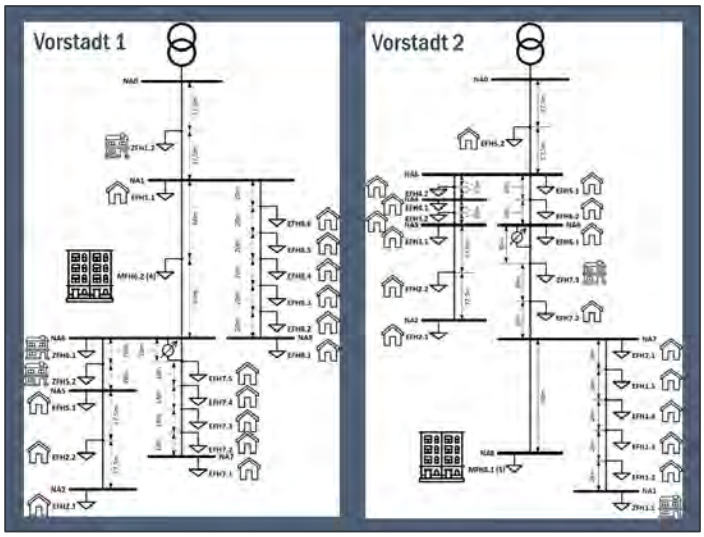


Abbildung 18: Netztopologien Vorstadt 1 und Vorstadt 2.

Netztopologie Stadt

Für die Netztopologie Stadt wird aus dem Referenznetz nach [15] der lila Strang aus LV06 (Abbildung 19) als Referenz zur Verschaltung der Netzabschnitte verwendet. Die Netztopologie Stadt weist am meisten Verzweigungen auf im Vergleich zu den anderen Topologien. Die Gesamtlänge liegt für LV06 bei 1080 m mit 111 Verbrauchern. Die Distanz zwischen den Verbrauchern liegt durchschnittlich bei 10 m. Der lila Strang umfasst insgesamt 39 Lasten, wobei mehrere Lasten an einem Abgang zusammengefasst werden. Bei 39 Lasten ergibt sich eine Gesamtlänge von 390 m. Die Gesamtlast beträgt 441 kW für insgesamt 111 Verbrauchern. Bei 39 Lasten beträgt die Last für den lila Strang 155 kW. Pro Verbraucher liegt eine durchschnittliche Last von 3,9 kW an.

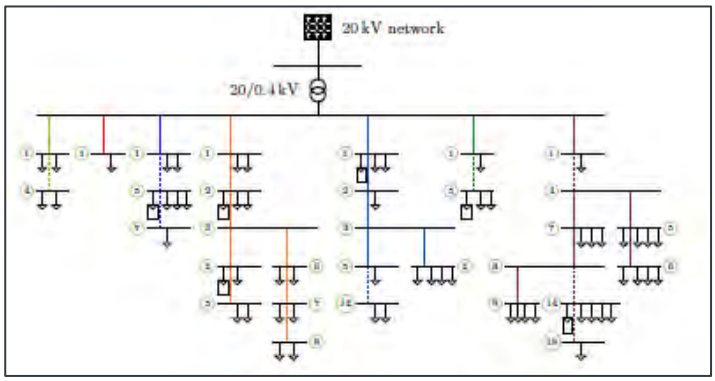


Abbildung 19: Netztopologie LV06 Stadt [15].

Nach dem Referenznetz von [16] entspricht die Netztopologie Stadt der Topologie B3 und weist drei Verzweigungen vom Hauptstrang auf (Abbildung 20). Bei ca. 40 Lasten, wie im vorherigen Referenznetz, beträgt die Distanz zwischen den Verbrauchern 15 m (30 m-15 m). Die Gesamtlänge ergibt sich dann zu 600 m.

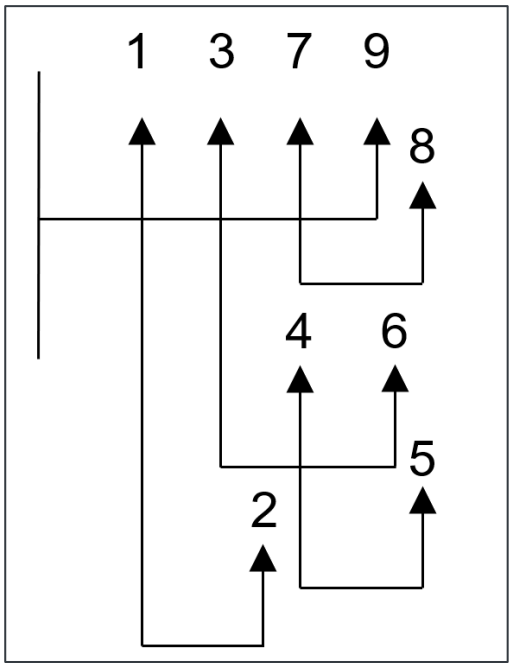


Abbildung 20: Netztopologie in Anlehnung an [16] mit drei Verzweigungen.

Eine durchschnittliche Distanz zwischen den Verbrauchern liegt nach dem Vergleich zwischen 10-15 m. Im Smart Grid Lab wird eine durchschnittliche Distanz von 9 m realisiert. Die Gesamtlänge beträgt 360 m und orientiert sich damit an dem Referenznetz nach [15]. In der Netztopologie Stadt wird eine Gesamtlast von 155 kW bei insgesamt 39 Lasten simuliert. Das entspricht einer durchschnittlichen Last von 3,9 kW pro Verbraucher. Die Leitungslängen sind in der Tabelle 5 im Vergleich dargestellt.

Tabelle 5: Vergleich der Netzlänge bei einem Kabelquerschnitt von 240mm2 zwischen [15] (LV06), [16] (B3) und Smart Grid Lab Netztopologie Stadt.

	Referenznetz TU Dortmund [15]	**Referenznetz TU Dresden [16]**	**SGL Stadt**
Distanz zwischen Abgängen [m] (Mittelwerte)	10	15	9
Gesamtlänge* [m]	390 (*bei 39 Lasten)	600 (*bei 40 Lasten)	360 (*bei 39 Lasten)

In Abbildung 21 ist die Netztopologie Stadt für das Smart Grid Lab dargestellt. Die Verschaltungen der Netzabschnitte weisen, im Vergleich zu den anderen Netztopologien, die meisten Verzweigungen auf und kürzesten Distanzen zwischen den Verbrauchern.

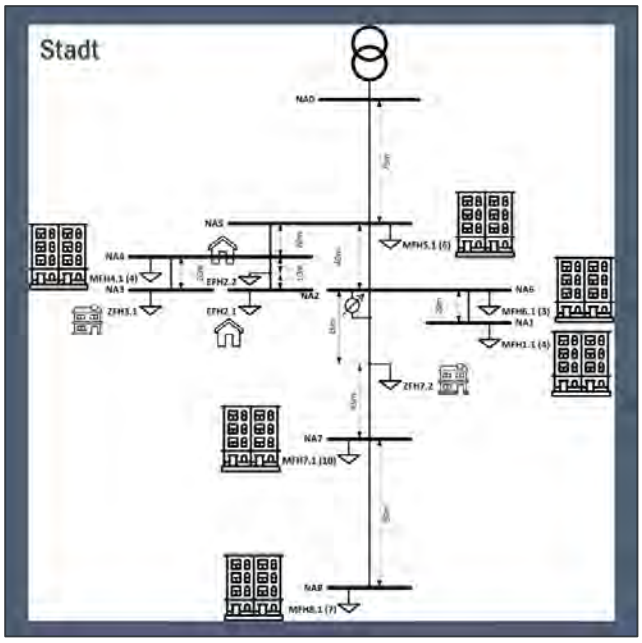


Abbildung 21: Netztopologie Stadt.

Gesamtes Netz

Für jede Kategorie wurde mindestens ein Strangtyp entwickelt. Um eine höhere Varianz zu erzeugen, wurde von dem ursprünglichen Plan vier Kabelabschnitte und fünf Lastrennschaltern abgewichen. Da acht Wechselrichterpaare in der Beschaffung waren und ein Laborwechselrichter schon zur Diskussion stand, sollten acht Abschnitt mit je einem Wechselrichterpaar und ein Abschnitt für den Laborwechselrichter vorgesehen werden. (Im Folgenden Text werden diese auch Netzabschnitte bzw. n Kurzform NA genannt.)

Als Ausgangsabschnitt sollte dieser, an dem dann der Laborwechselrichter angeschlossen werden soll, dienen. Die Einspeisung wurde so ebenfalls an diesem Netzabschnitt platziert.

Um die Verschaltung zwischen den Netzabschnitten zu erzeugen, wurden die einzelnen Strangtypen in einer Matrix erfasst, um die unterschiedlichsten Längen zu gruppieren und die Verschaltung zu erzeugen. Als Ergebnis wurde das Labornetz (Abbildung 22) und mit den sieben Topologien festgehalten: „Land 1“, „Land 2“, „Dorf 1“, „Dorf 2“, „Vorstadt 1“, „Vorstadt 2“ und „Stadt“. (Abbildung 12, Abbildung 15, Abbildung 18 und Abbildung 21). Das Ingenieurbüro Pfeffer hat sich bereiterklärt, Teile seiner Infrastruktur für Testzwecke zur Verfügung zu stellen. Dazu gehören eine 60 kVA CCS Ladesäule und ein Batteriespeicher mit 68 kWh Kapazität und 60 kVA Lade- und Entladeleistung. Die Einbindung dieser beiden Komponenten können über den Netzabschnitt ByPass eingebunden werden.

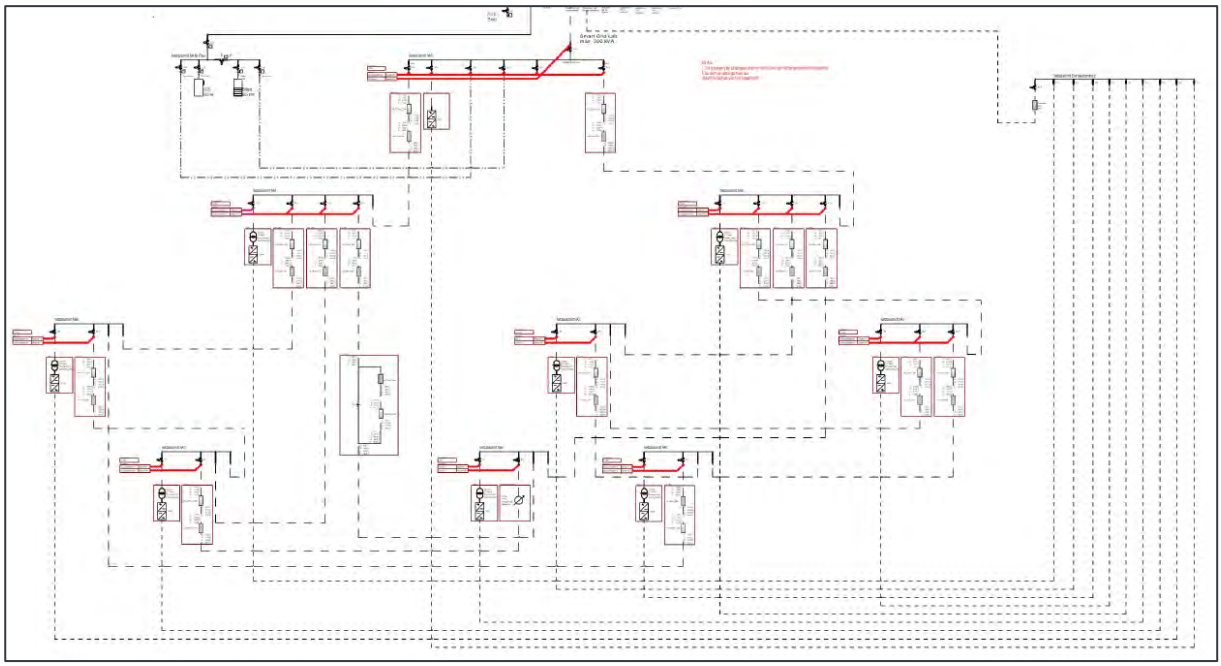


Abbildung 22: Single Line Plan des Labornetzes.

2.1.2. Hauptkomponenten

Wechselrichter

Die Wechselrichter sollen im Niederspannungsnetz 400V verkettet und mit 50 Hz arbeiten. Es werden je zwei Wechselrichter Back-to-Back angeordnet und bilden zusammen einen Strang bzw. ein Wechselrichterpärchen. Mit der Wechselstromkreisseite sollen sie an das Niederspannungsnetz angeschlossen werden. Es soll die VDE-AR-N 4105 eingehalten werden. Die Wechselrichter werden parallel verschaltet und sollen zu den anderen Wechselrichtern mit unterschiedlichen Lastgangkurven betreiben werden.

Im Labor wurden acht Stränge mit Wechselrichtern der Firma Siemens angeschafft. Diese können Einspeisungen sowie Lasten mit 16 kVA simulieren. In Abbildung 23 ist der Aufbau der Wechselrichter zusehen. Die Wechselrichter werden über eine Speicherprogrammierbaresteuerung (SPS / bei Siemens S7) angesteuert. In der SPS können Lastpunkte vorgeben werden, welche die Wechselrichter dann imitieren. Auf beiden Seiten des Stranges ist ein Filter vorgeschaltet. Der Filter dient zu Filterung von Störsignalen für einen sauberen Sinus. Der rechte Wechselrichter ist an den Teststromkreis angeschlossen und hat weitere Bauteile vorgeschaltet. Das Modul VSM misst die Spannung und dient in Verbindung mit dem zweiten Modul VSM nach dem Trenntransformator zur Messung der Regelparameter für den Controller.

Der Trenntransformator hat einen induktiven Anteil, welcher für eine Phasenverschiebung verantwortlich ist. Um dieser Verschiebung entgegen zu wirken, wird vor und hinter dem Transformator gemessen und. Die Differenz der Parameter ist die zu regelnde Größe, welche der Controller kontinuierlich nachjustiert, um die eingestellten Werte aus der S7 einzuhalten. Jedes Wechselrichterpaar hat einen Trenntransformator verbaut, um eine galvanische Trennung zu realisieren.

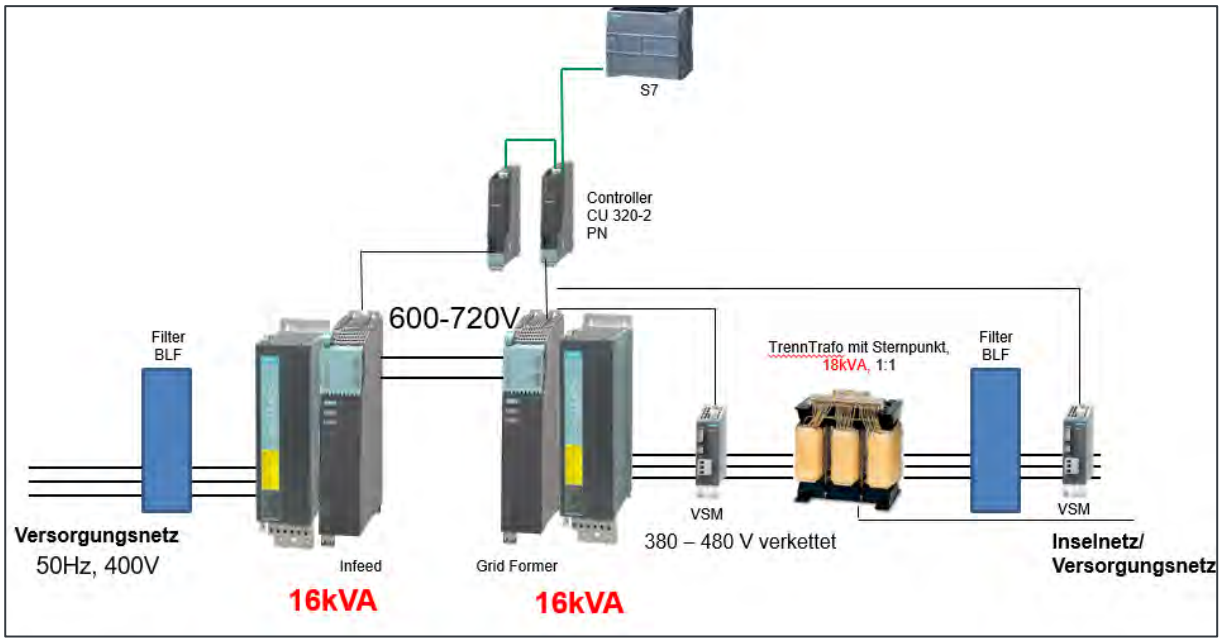


Abbildung 23: Aufbau eines Wechselrichterstranges mit Steuerung.

Längsspanungsregler

Ein Lösungsansatz zur Einhaltung des Spannungsbandes nach der Norm DIN EN 50160 ist der Einsatz von Spannungsreglern im Netz. Spannungsregler stellen im Smart Grid LAB dynamische Betriebsmittel zur Spannungseinhaltung dar.

Die Norm DIN EN 50160 definiert die Merkmale der Spannung in öffentlichen elektrischen Versorgungsnetzen. Sie spezifiziert die Merkmale am Netzanschlusspunkt unter normalen betrieblichen Bedingungen. In der Norm sind Merkmale zur Netzfrequenz, zur Höhe der Versorgungspannung, Spannungsänderungen, Spannungseinbrüche, Überspannung, Flicker und Oberschwingungen definiert. Die Norm unterscheidet bei der Frequenzangabe zwischen Netzen im Verbundnetz und Inselnetzen. In Verbundnetzen soll die Netzfrequenz 50 Hz±1% betragen. Die Norm wird immer noch eingehalten, wenn in 0,5% der Zeit des Jahres eine Abweichung von 4% nach unten oder von bis zu 6% nach oben eintritt. Bei Inselnetzen soll die Netzfrequenz 50 Hz±2% einhalten. In 5% der Zeit einer jeden Woche darf die Frequenz um bis zu 15% von der Nennfrequenz abweichen. Somit ist die Toleranz der Frequenzabweichung bei Inselnetzen wesentlich höher. [18]

Im Smart Grid LAB ist ein 70 kVA Längsregler (LVRSys der Firma Aeberle) verbaut. In Abbildung 24 ist das technische Prinzip dieses Spannungsreglers dargestellt. Über zwei Transformatoren, welche über Thyristoren angesteuert werden, kann die Spannung angehoben oder gesenkt werden. In dem Beispiel von Abbildung 10 sind die Transformatoren so eingestellt, dass der erste Transformator die Spannung um 4,5% anheben oder senken kann und der zweite um 1,5%. Es können sowohl beide Transformatoren gleichzeitig angesteuert werden, sodass die Ausgangsspannung zwischen 1,5%-6% geregelt werden kann.

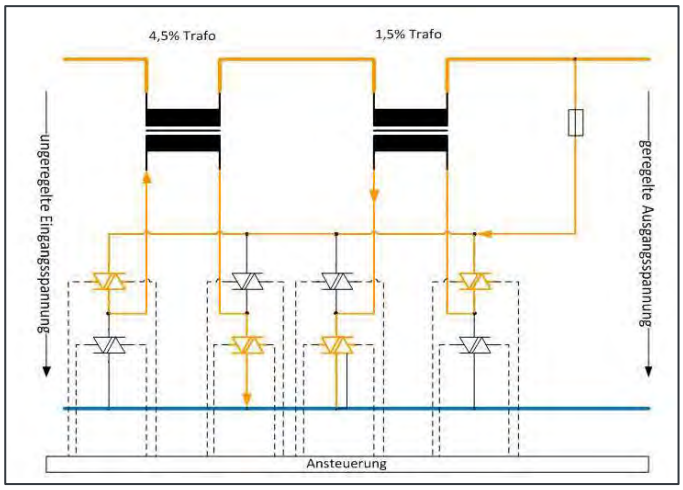


Abbildung 24: Technisches Prinzip eines Spannungsreglers [19].

2.1.3. Zusammenstellung und Platzierung

Eine technische Anforderung, welche stets eine Wichtigkeit hatte, war der benötigte Platzbedarf. Letzt endlich ist es gelungen, das gesamte Labor in dem vom Ingenieurbüro Pfeffer zur Verfügung gestelltem Bereich zu errichten. Zwei Ausnahmen wurden jedoch gemacht. Der Längsspannungsregler und der Laborwechselrichter konnten nicht in dem Bereich platziert werden, jedoch in unmittelbarer Nähe vor dem vorgesehenen Laborbereich. (Abbildung 25 und Abbildung 26)

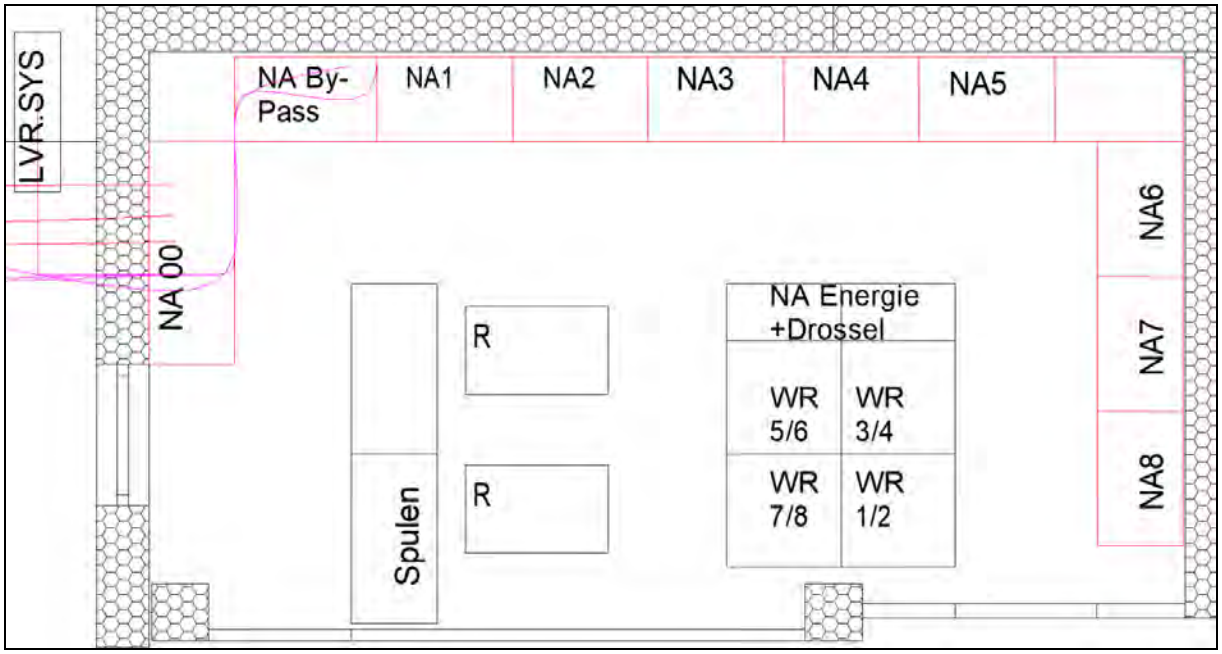


Abbildung 25: Raumplan des Labors.

Abbildung 26: fertiges Smart Grid LAB Hessen.

2.1.4. Berechnung des minimalen Kurzschlussstromes

Beschreibung der Kurzschlussart

Um die Leistungsschalter richtig zu parametrieren, war der minimale Kurzschlussstrom zu berechnen. Dieser legt die Grenze fest, an der die Geräte immer noch sicher auslösen müssen und bestimmt damit die Wirksamkeit von Schutzeinrichtungen. Die Berechnung des Kurzschlussstromes erfolgt nach DIN EN 60909-0 VDE 0102 und die Norm VDE 0100-410 regelt die Schutzmaßnahmen für den Schutz gegen elektrischen Schlag. [20]

Das Labor ist direkt an dem Ortsnetztransformator des Ingenieurbüro Pfeffer angeschlossen. Der dort bereits installierte Transformator, ist auf der Niederspannungsseite sternförmig geschaltet und aus dem geerdeten Sternpunkt der Neutralleiter herausgeführt. Dadurch wird ein TN-System im elektrischen Netz des Gebäudes realisiert. Sowohl für den Teststromkreis als auch für den Energiestromkreis ist jeweils ein Abgang an der Hauptverteilung vorgesehen. Beide sind über die Wechselrichterpaare mit ihren vorgeschalteten Trenntransformatoren miteinander verbunden. Durch eine geschickte Stellung der Gleichspannungen im Zwischenkreis der Wechselrichterpaare kann ein Stromfluss erzeugt werden. Dadurch wird die vorgegebene Leistung auf dem Teststromkreis aus dem Netz bezogen und anschließend über den Energiestromkreis wieder zurück gespeist. Werden Netzeinspeisungen simuliert, so erfolgt der Stromfluss in entgegengesetzter Richtung. Da der Widerstand der Leitungen proportional zu ihrer Länge ist, wurde für die Berechnung des minimalen Kurzschlussstromes die Netztopologie mit den längsten Leitungslängen ermittelt. Dies ist in der Topologie Dorf 1 mit „465 m“ der Fall (Abbildung 15).

Mit Hilfe der Elektroplanungssoftware Elaplan von der Firma ElektroSoft, wurde das Netz simuliert und anschließend der minimale Kurzschlussstrom an allen Knotenpunkten berechnet. Um den minimalen

Kurzschlussstrom zu ermitteln, wurden alle Wechselrichter als Lasten betrachtet, wodurch das Labornetz nur noch von der Netzeinspeisung versorgt wird. Der Netzplan von Dorf 1 wurde in Elaplan eingegeben und die Elemente anschließend parametriert. Das vollständige Ergebnis der Berechnungen ist im Anhang zu finden.

Im Labor ist auf der Teststromkreisseite von einem generatorfernen Kurzschluss auszugehen, bei dem der Fehler zwischen einem der drei spannungsführenden Außenleiter und dem potentialfreien N-Leiter auftritt, der mit dem geerdeten Sternpunkt des Trenntransformators verbunden ist. Da dessen Sekundärseite nach VDE 0100 Teil 410 nicht geerdet sein darf, kann dort dieser Fehler nicht auftreten. Aus diesem Grund ist der zweipolige Kurzschluss zwischen dem Wechselrichterpaar und dem Trenntransformator als minimal anzunehmen.

Da bei einem ein- bzw. zweipoligen Kurzschluss die Symmetrie des Netzes gestört wird, muss das Verfahren der symmetrischen Komponenten angewendet werden, in die die Impedanzwerte des Betriebsmittels zu transformieren sind.

$$\left[\underline{Z}_{012}\right] = \begin{bmatrix} \underline{Z} + 3\underline{Z}_E & 0 & 0 \\ 0 & \underline{Z} & 0 \\ 0 & 0 & \underline{Z} \end{bmatrix}$$

Beim Transformator handelt es sich um ein Betriebsmittel ohne rotierende Teile, weshalb im Ersatzschaltbild für das Mit- und Gegensystem die gleichen Impedanzen einzusetzen sind, wie für den symmetrischen Betrieb. Durch die Herausführung des Sternpunkts auf der Niederspannungsseite können sich dort Nullströme ausbilden, deren Größe meist messtechnisch ermittelt wird. Rechnerisch können sie in Elaplan näherungsweise bestimmt werden. [21]

Im Inselnetzbetrieb wird die Netzeinspeisung vom Laboraufbau getrennt und die Energiezufuhr nur noch über eine Hälfte der Wechselrichterpaare realisiert. Sie weisen ein technisches Einspeisemaximum von 16 kVA bzw. 50 kVA auf. Hinzu kommt, dass im Fehlerfall aufgrund der Gleichzeitigkeitsfaktoren nicht alle Wechselrichter mit der vollen Leistung einspeisen werden, was die Kurzschlussleistung weiter reduziert. Somit liegt die maximal technisch mögliche Einspeiseleistung um etwa den Faktor 2000 unter der Leistung bei Netzeinspeisung. Daraus ergeben sich minimale Kurzschlussströme, die unter möglichen Betriebsströmen liegen können. Ein Schutzkonzept, das starr auf die Parametrierung der Leistungsschalter ausgelegt ist, wäre also nicht zielführend. Aus diesem Grund wird zusätzlich eine Unterspannungserkennung installiert, die das gesamte Netz im Fehlerfall abschaltet. Sie erkennt Spannungseinbrüche, die durch fehlerhafte niederohmige Verbindungen im Netz auftreten.

Berechnungsergebnisse

Nachdem die Betriebsmittel in Elaplan vollständig parametriert wurden, konnte der minimale Kurzschlussstrom berechnet werden. Der erwartungsgemäß kleinste Fehlerstrom wird durch einen zweipoligen Kurzschluss zwischen dem Trenntransformator TR3 und dem Wechselrichterpaar WR3 im Netzabschnitt NA3 hervorgerufen. Dieser Kurzschlussort weist die längste Distanz zur Einspeisequelle, und somit die höchste Kurzschlussimpedanz auf. Er liegt aber noch vor dem Wechselrichterpaar, welches die beiden Stromkreise Teststromkreis und Energiestromkreis voneinander trennt. Das Ergebnis der einpoligen Kurzschlussstromberechnung bei wanderndem Kurzschlussort liefert erwartungsgemäß nur ein Ergebnis für die Primärseite des Trenntransformators. (Abbildung 27)

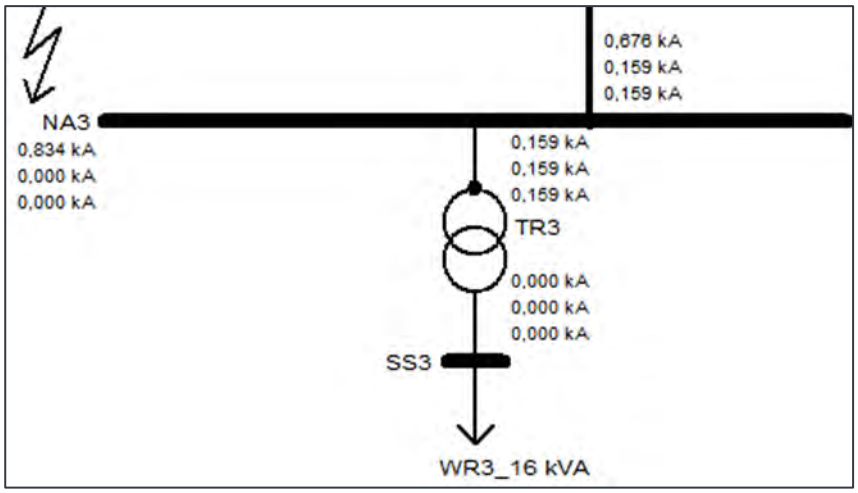


Abbildung 27: IK1min am Knoten NA3.

Durch die Dreiecksschaltung auf der Sekundärseite, kann dort nur ein zweipoliger Kurzschluss auftreten. Der dabei entstehende Kurzschlussstrom liegt deutlich unter dem einpoligen Kurzschlussstrom an der Sammelschiene NA3 und bestätigt somit die Annahme des Ortes für den minimalen Kurzschlussstrom. (Abbildung 28)

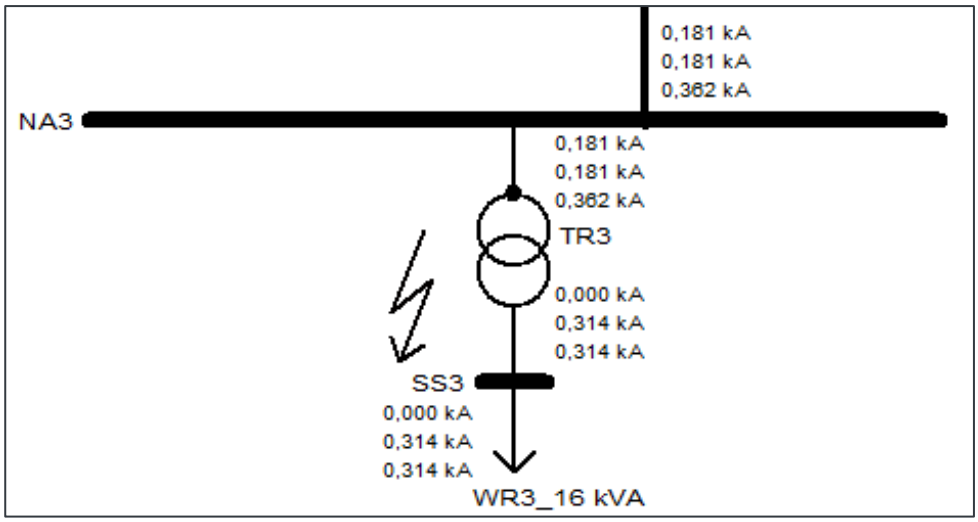


Abbildung 28 Ik2min hinter dem Trenntransformator.

2.1.5. Validierung der Topologien

Mit Hilfe von PowerFactory-Modellen sollen die erstellen Topologien überprüft und validiert werden. Dazu galt es die die Topologien in dem Simulationsprogramm abzubilden und durchlaufen zu lassen. Dazu wurden die hinterlegten Lastprofile aus dem Programm verwendet. Ein Auszug für Dorf 1 wird mit den folgenden Abbildungen gezeigt. (weitere Abbildungen sind im Anhang)

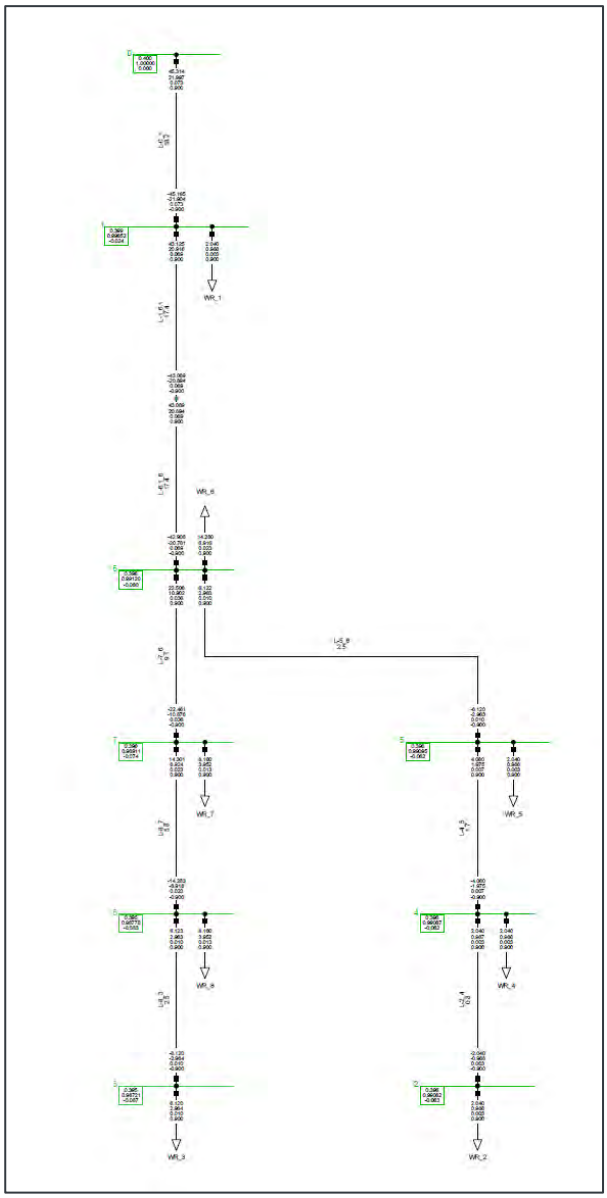


Abbildung 29: Dorf 1 in PowerFactory.

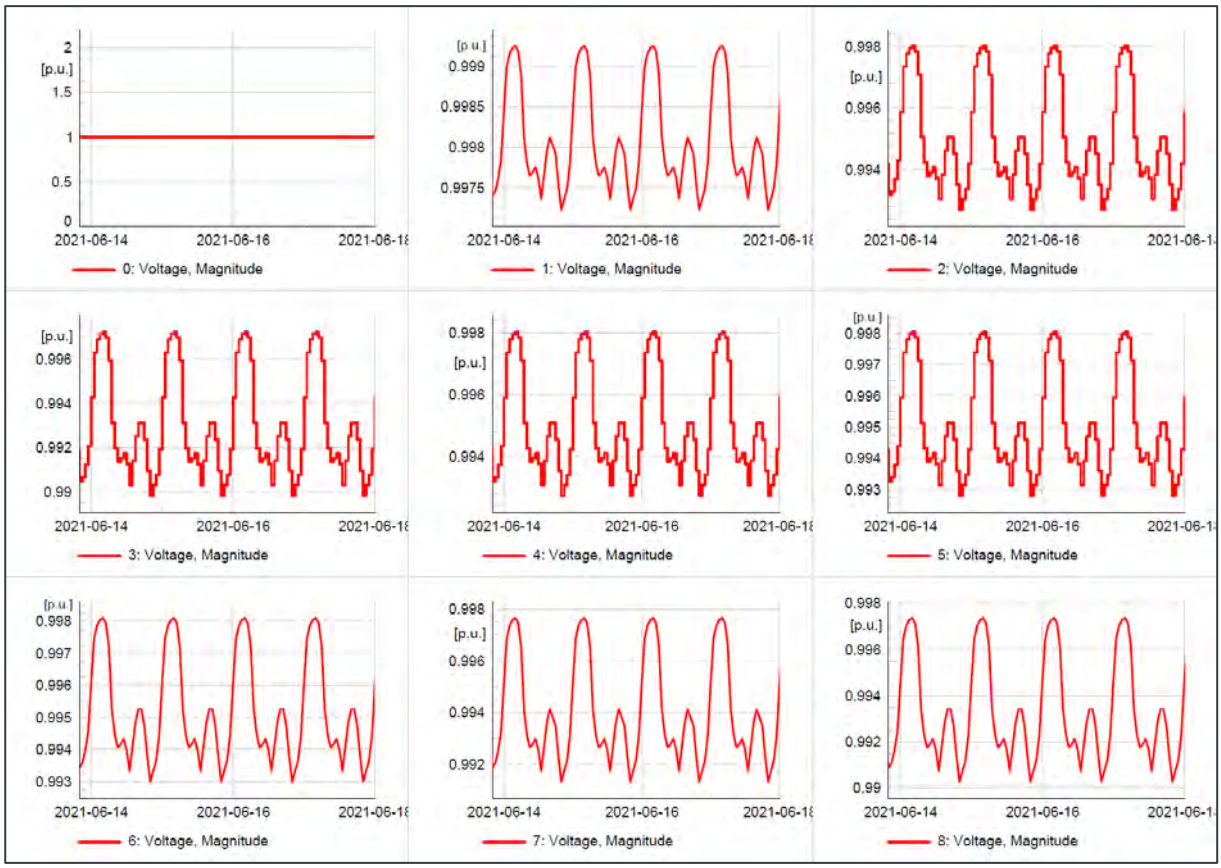


Abbildung 30: Spannungsverläufe der einzelnen Netzabschnitte von Dorf 1 in PowerFactory.

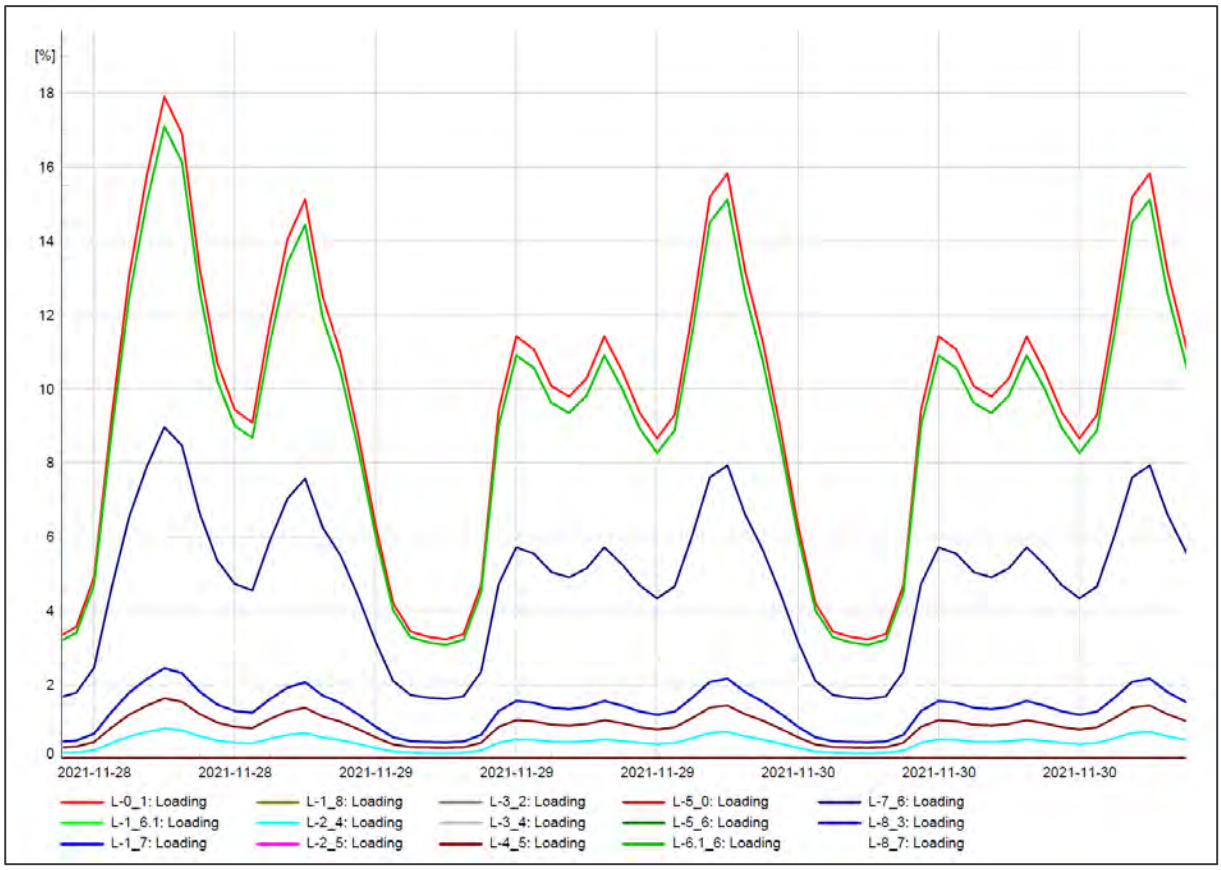


Abbildung 31: Kabelauslastungen der einzelnen Strecken von Dorf 1 in PowerFactory.

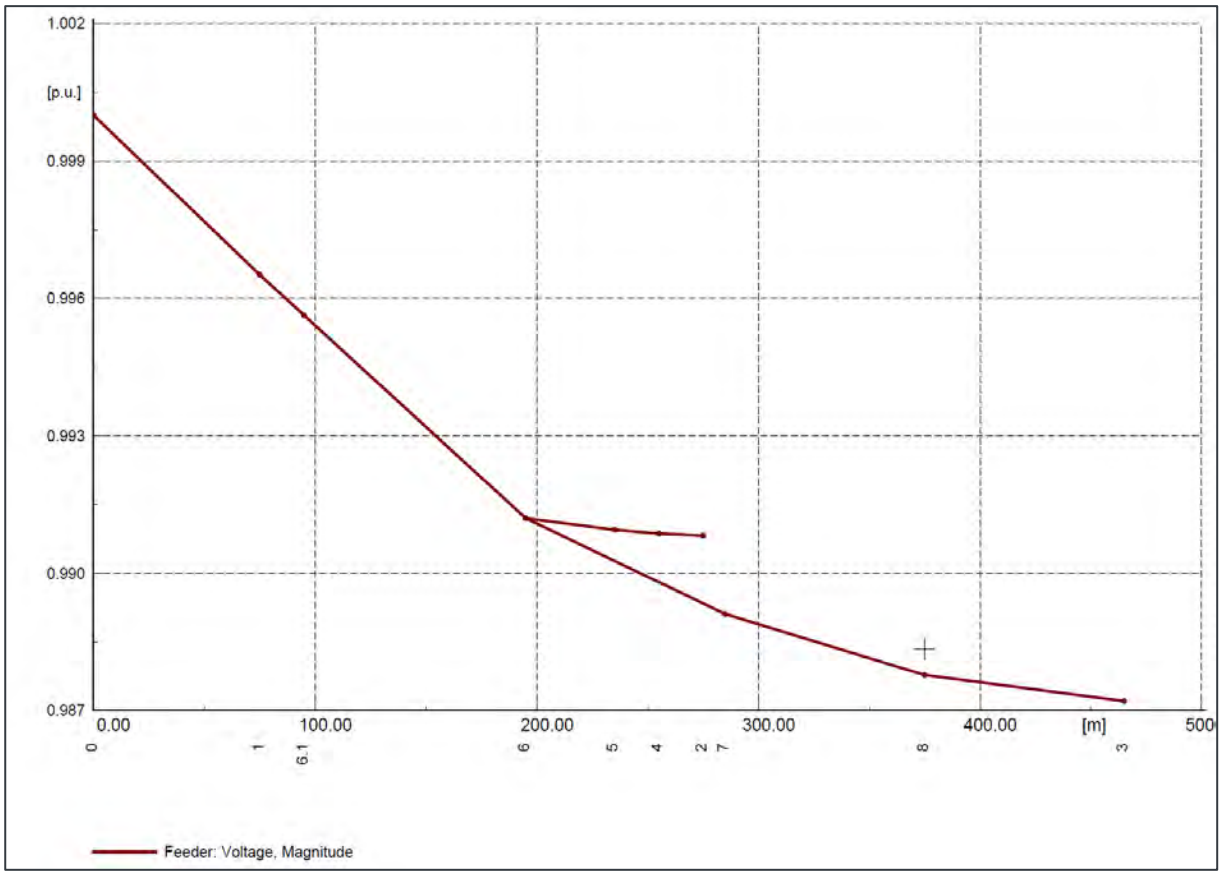


Abbildung 32: Zeitpunkt des maximalen Spannungsabfalls über die Strecke in der Simulation von Dorf 1 in PowerFactory.

Als Erkenntnis kann festgehalten werden, dass mit den entwickelten Topologien mit den Standardlastprofielen nur kleine und unkritische Spannungsänderungen sowie niedrige Auslastungen auftreten. Früher wäre dies für einen Netzbetreiber eine deutliche Überdimensionierung.

Ziel ist es mit dem Labor auf dem aktuellen Standard der Verteilnetzbetreiber zu arbeiten und diese rüsten sich für die weitere Entwicklung (Ausbau von Photovoltaik-Anlagen, E-Mobilät und Wärmepumpen). Diese war in den Simulationen nicht mit abgebildet. Es lässt schlussfolgern, dass die Topologien einen sehr guten Netzausbauzustand abbilden. Ein Ableiten auf nicht zu gut ausgebaute netze ist möglich. Ein Transfer und die Bewertung ist für Bestandsnetze und zukünftige Netze gegeben. Das Labor bildet eine Plattform um „Straße der Zukunft“ zu testen.

2.1.6. Basis für Lastprofile

Paragraf 17 des Energiewirtschaftsgesetzes (EnGW) regelt den Netzanschluss und verpflichtet die Netzbetreiber dazu Verbraucher und Erzeuger diskriminierungsfrei an ihr Energieversorgungsnetz anzuschließen. Um ein stabiles Netz zu gewährleisten, müssen sich die Erzeugung und der Verbrauch jederzeit möglichst exakt decken. Dafür werden im Voraus Netzlasten aufgestellt, damit der Netzbetreiber sein Netzmanagement auf den zu erwartenden Lastfluss einstellen kann. Um diese Prognosen zu ermöglichen, existieren Standardlastprofile (SLP), die auf Erfahrungswerten und Kenntnissen der Kundengruppen beruhen und eine Vorschau des zu erwartenden Abnahmeverhaltens für einen Tag erstellen. Der Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW, früher VDEW) stellt normierte repräsentative Lastprofile zur Verfügung, die für die unterschiedlichen Kundengruppen (Haushalt, Landwirtschaft und Gewerbe) angewendet werden können, bei denen jeweils ein ähnliches Abnahmeverhalten anzunehmen ist. Sie ersetzen die unbekannte Lastganglinie

von Letztverbrauchern durch eine errechnete, hinreichend genaue Prognose der Leistungsabnahme im Viertelstundentakt. Die Standardlastprofile sind normiert auf einen Jahresverbrauch von 1000 kWh/a und müssen an den tatsächlichen Verbrauch angepasst werden, der sich unter anderem nach der Anzahl der im Haushalt lebenden Personen richtet. [22] Ein Beispiel ist in Abbildung 33 zu sehen.

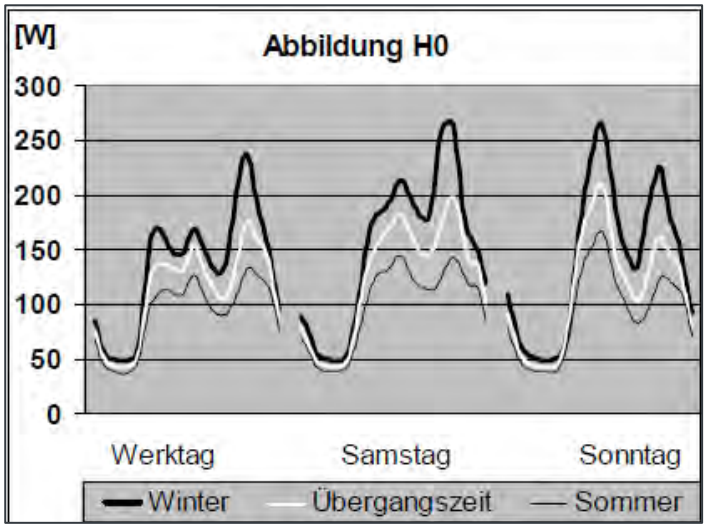


Abbildung 33: VDEW SLP für die Kundengruppe H0 [22].

Allerdings ergeben sich zwei wesentliche Problempunkte für die Anwendung solcher Standardprofile im Laborbetrieb. Zum einen existieren nur Leistungswerte im viertelstündigen Takt. Im Smart Grid Labor sollen aber gerade herausfordernde Netzsituationen abgebildet werden, in denen das Netz kurzfristig an der technischen Grenze betrieben wird. Dafür müssen die Zeitreihen wesentlich feiner gestaltet werden, bei einer Abtastrate von mindestens 60 Sekunden. Außerdem stellen die SLP nur einheitlich normierte Profile dar, die sich aus Mittelwerten einer Vielzahl von untersuchten Messdaten unterschiedlicher Haushaltstypen und -größen zusammensetzen. Kurzfristig hohe Leistungsspitzen treten durch diese Vergleichmäßigung nicht mehr in Erscheinung. Eine Messung aus einem Privathaushalt verdeutlicht diesen Punkt (siehe Abbildung 34).

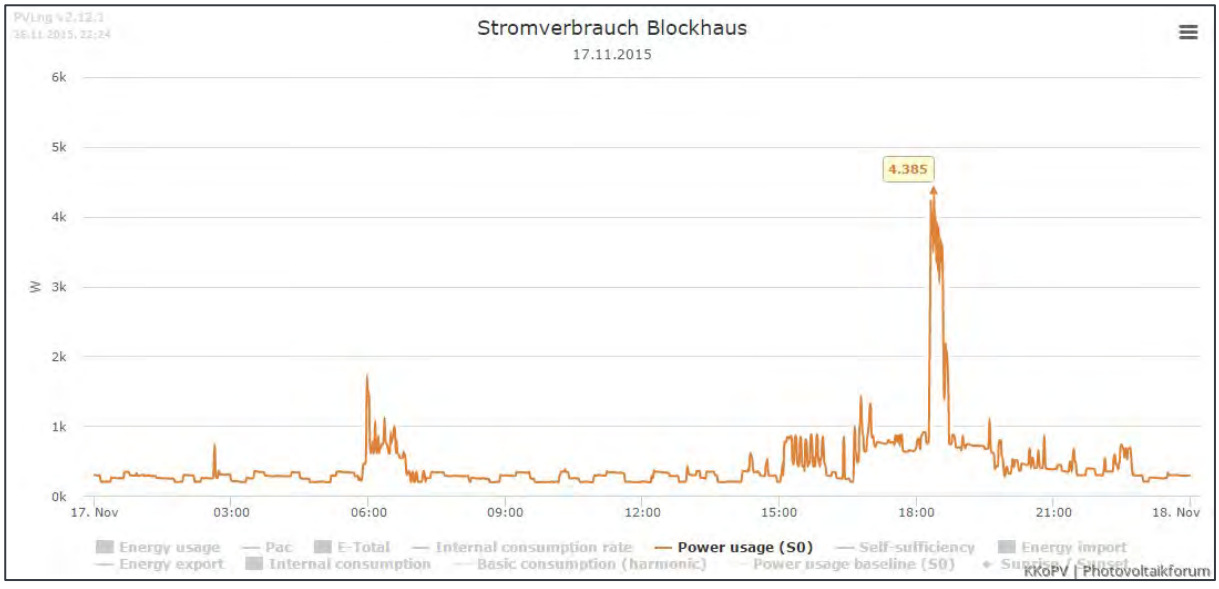


Abbildung 34: Lastprofil eines privaten Haushalts [23].

Hier sorgt eine Kaffeemaschine in den Morgenstunden und ein Herd abends für Spitzenwerte, während der Verbrauch im Rest des Tages deutlich geringer und relativ kontinuierlicher verläuft. Für den Netzbetreiber sind solche kurzfristigen Schwankungen einzelner Abnehmer nicht relevant, da er nur die Summe aller Kunden beliefert, bei der sich die einzelnen Peaks wieder annähernd im Standardlastgang aufaddieren. Das Smart Grid Labor betrachtet aber Netzabschnitte mit einer geringen Anzahl von ein bis maximal zwölf Netzanschlusspunkten. Dort spielen die einzelnen Last- oder Erzeugungsspitzen dann wieder eine Rolle. Aus den Standardlastprofilen und dessen Herleitung lassen sich allerdings wichtige Kriterien und Gliederungsmerkmale ableiten, die auch für die Erstellung der Laborkurven anwendbar sind und in den folgenden Abschnitten aufgeführt werden.

In Standardlastprofilen werden Verbraucher in unterschiedliche Kundengruppen eingeteilt. Während beispielsweise in der Gastronomie der Elektrizitätsbedarf vor allem in die Abendstunden und auf das Wochenende fällt, weisen andere Gewerbeeirichtungen wie Handwerksbetriebe und Bürogebäude an Wochentagen während der Arbeitszeit einen Bedarf auf, der Betragsmäßig höher ausfällt als bei einem Arbeitnehmerhaushalt, der hauptsächlich morgens und abends elektrische Energie benötigt und sich dessen Bezugsspitzen deshalb dort konzentrieren. Sowohl der Gesamtverbrauch als auch das Zeitverhalten sind somit unterschiedlich weshalb Netzauslastungen in den unterschiedlichen Topologien des Smart Grid LAB zu anderen Zeiten, an anderen Orten, in anderen Beträgen anzunehmen sind. Das Verbraucherverhalten ist außerdem in den VDEW-Kurven in die charakteristischen Tage, Werktag, Samstag und Feiertag eingeteilt und es werden die unterschiedlichen charakteristischen Jahreszeiten Winter-, Sommer- und Übergangszeit dokumentiert. Auch das sollte langfristig in den Daten für das Labor berücksichtigt werden. Die folgenden Abschnitte verdeutlichen diesen Punkt, da durch die neuen Komponenten, Wärmepumpe, Elektromobile und Photovoltaikanlagen die Art und Weise des elektrischen Energiebedarfs wandelt. Das Hessische Statistische Landesamt gibt außerdem eine Übersicht über die Bevölkerung in Privathaushalten aus der hervorgeht, dass es im Jahr 2019 rund 500.000 Privathaushalte gab, von denen die meisten Ein- und Zweipersonenhaushalte sind. Die durchschnittliche Anzahl an Personen je Haushalt betrug 2,31 [24] bei einem jährlichen Stromverbrauch von rund 2.500 kWh im Jahr. [25]

Es wird speziell auf einen Haushalt in Hessen eingegangen, wobei vor allem die Anzahl und das Alter der Personen den Elektrizitätsbedarf und dessen Zeitverhalten bestimmen. Das statistische Bundesamt hat die elektrischen Verbraucher der Haushalte in Deutschland analysiert und in einer Tabelle zusammengefasst. Dabei wurden auch die Wahrscheinlichkeiten des Vorkommens berücksichtigt. Die Tabelle gilt als Grundlage für den konventionellen Grundverbrauch eines Haushaltes und wurde durch die elektrischen Durchschnittsleistungen der einzelnen Komponenten erweitert. Ein Auszug aus der Tabelle soll das Vorgehen verdeutlichen.

Tabelle 6: Auszug aus der erweiterten Tabelle des statistischen Bundesamtes [24].

Haushalts- und sonstige Geräte in Deutschland	2019	2020	2021	Erweiterungen	
Haushalte insgesamt (in 1000)	**37 869**	**37 993**	**37 993**		
Anteil der Haushalte in % (Ausstattungsgrad)				**P el [kW]**	**Peak/konst**
Kühlschrank, Kühl- und Gefrierkombination	**99.9**	**99.8**	**99.9**	**0,15**	**k**
Gefrierschrank, Gefriertruhe	**48.0**	**48.0**	**49.0**	**0,12**	**k**

Geschirrspülmaschine	**71.7**	**72.3**	**73.1**	**2**	**P**
Mikrowellengerät	**73.2**	**73.8**	**73.8**	**0,800…1,5**	**P**

Bei den Verbrauchern wurden unterschiedliche Zeitverhalten bestimmt. Kühl- und Gefrierschränke weisen einen relativ kontinuierlichen Verbrauch auf, während Großverbraucher wie der Herd oder Ofen nur kurzfristig Leistungsbedarfsspitzen erzeugen. Es musste also herausgearbeitet werden, was die konstante Grundlast beansprucht und wodurch Peaks entstehen, die wiederum konkreten Zeitbereichen zugeordnet werden können. Für die erstellten Kurven wurde angenommen, das vor allem Kühlgeräte, Interneteinrichtungen und sonstige Elektronik im Standbybetrieb eine kontinuierliche Grundlast von 0,3 bis 0,6 kW beanspruchen, die in den Morgen- und Abendstunden durch Beleuchtungsanlagen heraufgesetzt wird. Der durchschnittliche Stromverbrauch dafür beträgt pro Haushalt jährlich rund 400 kWh, was einem Leistungsbedarf von rund 45 Watt pro Stunde entspricht. [26] Es wird angenommen, dass sich der Beleuchtungsbedarf vor allem auf die Morgen- und Abendstunden konzentriert.

Die Leistungsspitzenwerte werden kurzzeitig vor allem durch Großverbraucher wie Staubsauger, Föhn, Wasserkocher, Elektroherde oder Mikrowellen hervorgerufen und liegen zwischen 2 bis 15 kW. [27, 28] Die Hochschule für Technik und Wirtschaft (HTW) Berlin hat Datensatz mit Grundlastkurven erstellt. Dieser besteht aus 74 Lastprofile über ein ganzes Jahr. Es gilt das Kalenderjahr von 2010 für Werk- Sonn- und Feiertage. Die Schrittweite dabei ist eine Sekunde. [29] Weil sich die Zusammenstellung der Grundlastprofile als sehr aufwendig erweist, wird auf diesen Datensatz zurückgegriffen. In Abbildung 35 sind Beispiele für Grundlastverbräche zu sehen.

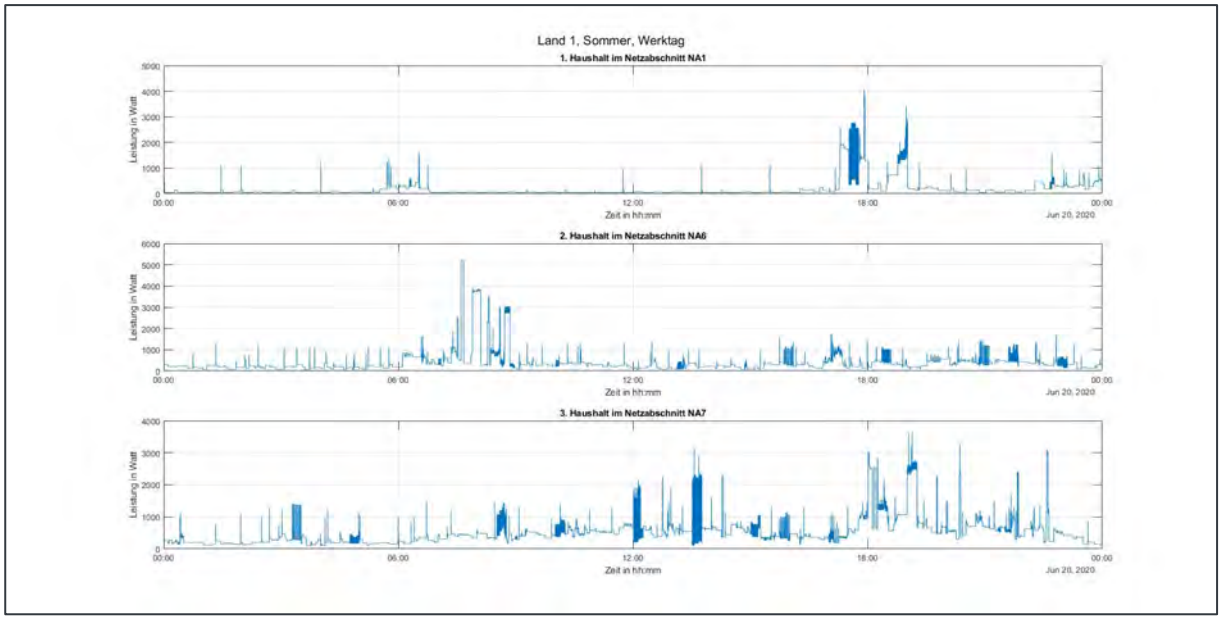


Abbildung 35: Drei Beispiel für Grundlastverbräuche aus dem HTW Datensatz.

2.2 Sekundärtechnik

Das Smart Grid LAB Hessen bezieht sich hauptsächlich auf die Untersuchung von Stromnetzen in Deutschland und setzt seinen Fokus auf die Verteilnetzbetreiber in Hessen. Im Folgenden werden die Anforderungen für Messgeräte für zukünftige Netze erörtert und es werden Messgeräte für Mittel- und

Niederspannung und Fernwirkgeräte gegenübergestellt. Grundlage zur Auswahl dieser Messgeräte ist eine Zusammenstellung von verwendeten Messgeräten der jeweiligen Verteilnetzbetreiber, welche auf Basis von aktuellen Transformatorenstation-Projekten des Ingenieurbüro Pfeffer zusammengestellt sind. In ganz Deutschland gibt es insgesamt 874 [30] Verteilnetzbetreiber, von den 50 [31] Verteilnetzbetreiber aus Hessen sind. In der folgenden Untersuchung sind 32 Verteilnetzbetreiber aus Hessen berücksichtigt, was 64 % der Verteilnetzbetreiber in Hessen entspricht. Die Untersuchung soll eine Tendenz der verwendeten Messegräte im hessischen Verteilnetz aufzeigen.

2.2.1. Messtechnik Erd- und Kurzschlussanzeiger

Das Niederspannungsnetz des Smart Grid LAB ist an eine intelligente Ortsnetzstation an das Mittelspannungsnetz angeschlossen. In der Mittelspannungsschaltanlage werden Erd- und Kurzschlussanzeiger eingesetzt, um Erd- und Kurzschlüsse im Netz zu detektieren. Im Folgenden werden die Anforderungen der Erd- und Kurzschlussanzeiger für zukünftige Netze aufgezeigt. Bei der Analyse der aktuellen Transformatorenstationen-Projekten wird ersichtlich, welche Erd- und Kurzschlussanzeiger hauptsächlich eingesetzt werden. Im Folgenden werden die Erd- und Kurzschlussanzeiger hinsichtlich ihrer Funktionen erläutert und verglichen. In Abbildung 36 ist der prozentuale Anteil der Erd- und Kurzschlussanzeiger, welche in aktuellen Projekten von den Verteilnetzbetreibern verwendet werden, dargestellt. Ersichtlich wird, dass die meist verwendeten Erd- und Kurzschlussanzeiger der Sigma D+/D++, Alpha E oder der Compass B 2.0 sind.

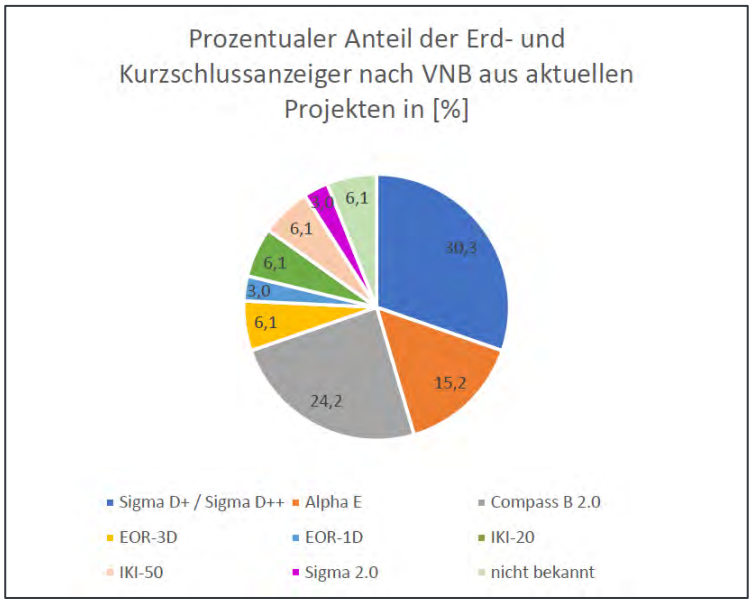


Abbildung 36: Diagramm zu Erd- und Kurzschlussanzeigern nach VNB aus Hessen.

Anforderungen an einen Erd- und Kurzschlussanzeiger für zukünftige Netze

Die Anforderungen an Erd- und Kurzschlussanzeiger verändern sich aufgrund der Veränderungen von zukünftigen Netzstrukturen. Der Lastfluss ist nicht mehr unidirektional von konventionellen Energieerzeugern hin zu den Verbrauchern, sondern bidirektional. Die Zunahme von erneuerbaren Energien führt zu dezentralen Einspeisungen im Netz. Eine Anforderung des Erd- und Kurzschlussanzeigers für die zukünftigen Netze ist, dass dieser die Richtung des Fehlers anzeigen muss. Wurde früher nur von einer Seite des Netzes eingespeist, so konnte der Fehler identifiziert werden. Der Fehler liegt bei dieser Vorgehensweise und Netzstruktur zwischen der Station die einen Kurzschluss anzeigt und der nächsten Station, welche keinen Kurzschluss anzeigt. Für die heutigen Netzstrukturen

mit dezentralen Einspeisungen funktioniert diese Vorgehensweise nicht mehr, da der Kurzschlussstrom aufgrund des bidirektionalen Lastflusses von beiden Richtungen fließen kann und somit keine Fehlerortung möglich ist. Für die zukünftigen Netze ist es sinnvoll, gerichtete Erd- und Kurzschlussanzeiger zur Fehlerortung einzusetzen. Eine weitere Anforderung ist die Einbindung in das Leitsystem des Verteilnetzbetreibers. Im Leitsystem wird die Meldung des Erd- oder Kurzschlusses angezeigt und der Verteilnetzbetreiber ist in der Lage sofort zu reagieren und den Fehler so schnell wie möglich zu beheben, um weitere Fehlerfolgen oder Ausfälle zu verhindern.

Hierzu sollte der Erd- und Kurzschlussanzeiger über verschiedene Schnittstellen zur Kommunikation an eine Fernwirkeinheit bereitstellen. Kommunikationsprotokolle wie Modbus RTU oder IEC 60870-5-104 sollten von Erd- und Kurzschlussanzeiger zur Fernwirkeinheit möglich sein. Für die zukünftigen Umsetzungen von Kommunikationswegen innerhalb der Ortsnetzstation sollte auch drahtlose Kommunikation zwischen den Geräten möglich gemacht werden. Die Kommunikation über LoraWan ist an dieser Stelle eine Möglichkeit, welche aufwendige Verdrahtungen und damit verbundene mögliche Fehlerquellen umgeht.

Das Messen von wattmetrischen Daten in der Mittelspannung stellt eine weitere Anforderung dar. Über Stromwandler und Spannungssensoren werden Strom- und Spannungswerte erfasst, um gerichtete Erd- und Kurzschlüsse zu detektieren. Strom- und Spannungswerte sind demnach bereits vorhanden. Aus diesen können dann restliche wattmetrische Daten errechnet werden. Zu klären ist, welche Daten wirklich für den Verteilnetzbetreiber in der Mittelspannung von Relevanz sind. Das Messen von Stromwerten kann Überlastungen frühzeitig erkennen und dient der Betriebsmittelüberwachung. Die Überprüfung der Spannungswert ist sinnvoll, um Abweichungen außerhalb des Spannungsbandes nach DIN EN 50160 frühzeitig zu erkennen und diese zu verhindern. Leistungswerte können aus den gemessenen Werten errechnet werden und machen das Netz hinsichtlich ihrer Lastflüsse transparent. Der Verteilnetzbetreiber kann somit einsehen, ob in das Mittelspannungsnetz zurückgespeist wird.

2.2.2. Messtechnik Niederspannungs-Einspeisung

In der Niederspannungseinspeisung wird vor den Niederspannungsabgängen gemessen. Aus den Ergebnissen wird ersichtlich, welche Messegräte in der Niederspannungseinspeisung am häufigsten verwendet werden. In Abbildung 37 ist der prozentuale Anteil der verschiedenen Messgeräte dargestellt. Das PL-Multi 2 und das UMG 96-S2 sind nach dieser Auswertung am häufigsten im Verteilnetz vertreten.

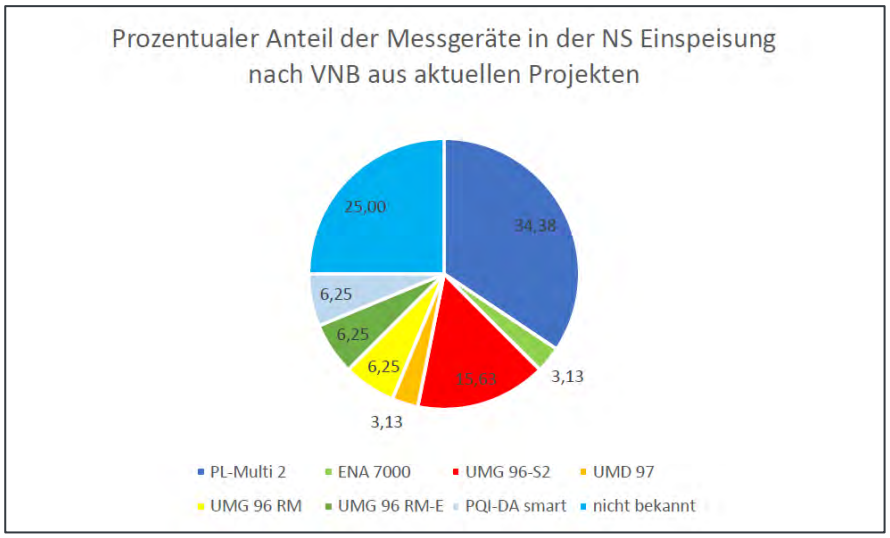


Abbildung 37: Diagramm zum prozentualen Anteil von Messgeräten in der NS-Einspeisung nach VNB aus Hessen.

Anforderungen an Messgeräte in der Niederspannungseinspeisung

In der Niederspannungseinspeisung sollten wattmetrischen Daten erfasst werden, um die Auslastung des Niederspannungsnetzes überwachen zu können. Die Veränderung im Niederspannungsnetz, durch dezentrale Einspeiser und Lasten durch E-Mobilität und elektrische Wärmepumpen, bedingt eine veränderte Auslastung im Niederspannungsnetz. Diese Veränderung sollte mit Messgeräten erfasst werden, um die Betriebsmittel vor möglichen Überlastungen zu schützen. Die gemessenen Daten können zur besseren Planung von Netzausbaumaßnahmen für zukünftige Netze dienlich sein.

Eine weitere Funktion und Anforderung an das Messgerät in der Niederspannung ist es, die Leistungswerte zu erfassen, um die Höhe der Rückspeisungen zu kennen. Die Zunahme von regenerativen dezentralen Einspeisern bedingt eine Erhöhung der zurückgespeisten Energie und eine Bereitstellung von noch mehr Anschlusspunkten und Aufnahme der Energie seitens des Verteilnetzbetreibers.

Nach dem EEG 2021 §8 müssen Anlagen, welche der Erzeugung von regenerativer Energie dienen, an eine geeignete Spannungsebene und an eine Stelle mit der kürzesten Entfernung der Erzeugung angeschlossen werden. Laut EEG 2021 §11 sind Netzbetreiber dazu verpflichtet die Energie aus erneuerbaren Energien abzunehmen, zu übertragen und zu verteilen. Nach dem EEG 2021 §12 muss der Netzbetreiber sein Netz ausbauen und auf den Stand der Technik bringen, um die Abnahme und Verteilung der Energie, aus erneuerbaren Energien, sicherzustellen. [32] Mit den Messdaten aus der Niederspannungseinspeisung können Anschlüsse von erneuerbaren Energien geplant und die Netzauslastung mit den Echtzeitmessdaten berechnet werden. Durch eine genaue Berechnung der Netzauslastung können neue Netzanschlusspunkte und die daraus resultierenden Netzausbaumaßnahmen besser und genauer bestimmt werden.

Das Messgerät sollte die Spannungsqualität nach der DIN EN 50160 messen, um Qualitätsvereinbarungen zwischen Energieversorger und Kunde im Fall eines Fehlers nachweisen zu können. Nach dem Produkthaftungsgesetz gemäß ProdHaftG §2 ist Elektrizität ein Produkt. Kommt es zu einer Sachbeschädigung z.B. aufgrund einer Überhöhung der Spannung, so haftet der Hersteller, in dem Fall der Verteilnetzbetreiber, und muss den Schaden ersetzen. Der Verteilnetzbetreiber wird als Hersteller definiert, da dieser die Energie auf eine andere Spannungsebene transformiert und somit die Eigenschaften des Stromes verändert. Ein Urteil vom 25.02.2014 (VI ZR 144/13) zeigt, dass im Fall eines

Fehlers des Produktes Elektrizität der Verteilnetzbetreiber als Hersteller haftet und den Schaden ersetzen muss. In diesem Fall wurden aufgrund von Spannungsüberhöhungen Haushaltsgeräte beschädigt und mussten ersetzt werden. [33]

2.2.3. Messtechnik Niederspannungsabgänge

In der Niederspannungsschaltanlage können die einzelnen Abgänge über Stromwandler und Spannungssensoren mit einem Messgerät gemessen werden. Die untersuchten Verteilnetzbetreiber verwenden zu 84 % keine Messgeräte in den Niederspannungsabgängen. 2 von 32 Verteilnetzbetreibern verwenden das PL Plano von Jean Müller und jeweils ein Verteilnetzbetreiber die Modulkarten von SAE bzw. VIVAVIS oder die Dreiphasenmessklemme von Wago (siehe Abbildung 38). Insgesamt ist zu erkennen, dass die meisten Verteilnetzbetreiber keine Messung in den Niederspannungsabgängen einsetzen. Durch die Veränderung der Netze insbesondere der Niederspannungsnetze ist zu erwarten, dass Verteilnetzbetreiber mehr Messungen in den Niederspannungsabgängen einsetzen, um die Netzveränderungen zu erkennen und Maßnahmen abzuleiten.

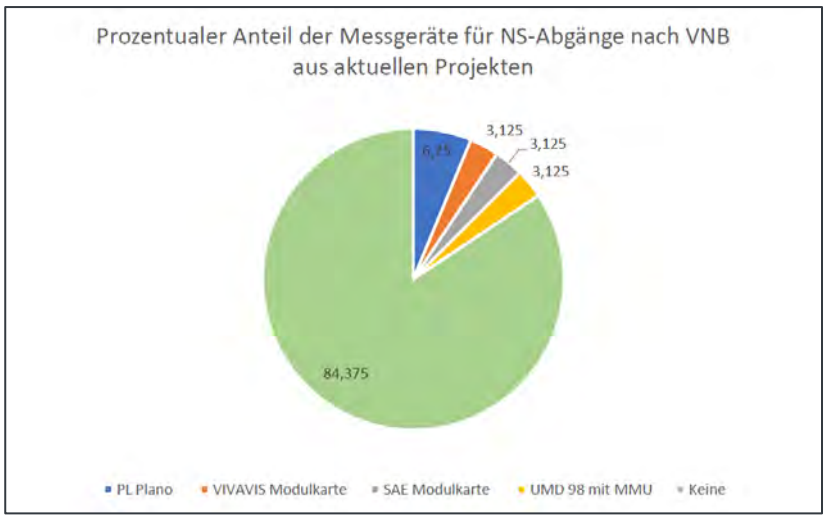


Abbildung 38: Diagramm zum prozentualen Anteil von Messgeräten in den NS-Abgängen nach VNB aus Hessen.

Anforderungen an Messgeräte in den Niederspannungsabgängen

An den einzelnen Niederspannungsabgängen sind mehrere Verbraucher angeschlossen. Bei einer Messung eines einzelnen Niederspannungsabgangs erhöht sich die Granularität der Lastflüsse. Im Vergleich bei der Messung der Niederspannungseinspeisung in Kapitel 2.2.2 wird der gesamte Lastfluss aus allen Abgängen erfasst. Somit wird erkannt, welcher Bezug bzw. Einspeisung insgesamt im angeschlossenen Niederspannungsnetz anliegt. Durch die Erfassung der Messwerte der einzelnen Abgänge wird die Granularität erhöht und es können die einzelnen Lastflüsse von Industrie oder Straßenzügen erkannt werden. Durch die Erhöhung der dezentralen Einspeisung durch Photovoltaikanlagen und durch die Nutzung von Ladesäulen und Wallboxen besonders im privaten Bereich wird die Kenntnis der Lastflüsse aus dem Niederspannungsnetz und deren Veränderung immer wichtiger, um Überlastungen und Netzengpässe frühzeitig zu erkennen. Eine Herausforderung der Verteilnetzbetreiber wird die Umsetzung des Redispatch 2.0 sein. Ab Oktober 2021 wird der Redispatch 2.0 umgesetzt. Mit dem Redispatch 2.0 werden die Vorgaben des Netzausbaubeschleunigungsgesetz zum Management von Netzengpässen angepasst. Die Maßnahmen zum Redispatch 1.0 betrifft insbesondere Höchst- und Hochspannungsnetze.

Übertragungsnetzbetreiber sind verantwortlich die Netze stabil zu halten und Netzengpässe sowieso Überlastungen zu vermeiden. Der Redispatch 1.0 wird mit Maßnahmen zur Lastverlagerungen umgesetzt. Hier müssen beispielsweise Kraftwerksbetreiber mit Leistungen über 10MW ihre Last bei prognostizierten Netzengpässen verlagern. Mit dem Netzausbaubeschleunigungsgesetz wurde der Redispatch 1.0 erweitert zum Redispatch 2.0. Beim Redispatch 2.0 sind alle Spannungseben betroffen. Die Redispatch Maßnahmen betreffen nun auch Verteilnetzbetreiber, welche für das Mittelspannungs- und Niederspannungsnetz verantwortlich sind. Betroffen von der Abregelung sind konventionelle Kraftwerke ab 100 kW, erneuerbare Energien und KWK-Anlagen und auch Erzeugungsanlagen und Speicher mit Leistungen unter 100 kW, wenn der Netzbetreiber diese Anlagen aus der Ferne ansteuern kann. [34] Eine Umsetzung des Redispatch 2.0 ist nur möglich, wenn der Netzbetreiber Kenntnis über die Lastflüsse im Niederspannungsnetz hat. Die Messung in den einzelnen Abgängen kann einen Hinweis darauf geben, dass abgeregelt werden muss, wenn Netzengpässe erkannt werden. Die tatsächliche Abregelung der Anlagen kann jedoch nur dezentral mit Kommunikationseinheiten an der zu abregelnden Anlage realisiert werden. Die Überwachung der Auslastung an den einzelnen Abgängen gibt dem Verteilnetzbetreiber Aufschlüsse darauf, inwiefern sein Netz ausgelastet ist und ob der Zubau von weiteren Verbrauchern und Einspeisern möglich ist. Im Niederspannungsnetz sollte vor allem der Leistungswert zur Überwachung der Lastflüsse, die Spannung zur Einhaltung der Spannungsqualität und der Strom zur Überwachung der Auslastung ermittelt werden.

2.3 Monitoring

Das Monitoring stellt im Laboraufbau eine zentrale Überwachungs- und Steuerungseinheit dar, in die alle gemessenen Daten aus dem Versuchsaufbau zusammenfließen, gespeichert und ausgewertet werden können. Zum einen wird sie als Datenbank und Visualisierungsmöglichkeit verwendet und zum anderen werden die Leistungsschalter angesteuert.

2.3.1. Leitwarte

Das Leitsystem bildet das gesamte Verteilnetz ab und findet Anwendung bei Versorgungsunternehmen und Verteilnetzbetreibern um die Mittelspannungsebene und aufwärts abzubilden. Diese können mit dem Leitsystem Veränderungen im Netz sehen und aktiv darauf eingehen, indem sie das Netz regeln, steuern und schalten.

Die Leitwarte bzw. der Leitrechner verwendet die Software HIGH-LEIT von der Firma VIVAVIS. An dieses System lassen sich verschiedene Fernwirksysteme koppeln, wie auch der Fernwirkkopf ACOS 750.

In der Leitwarte dieses Projektes wurde von der Ortsnetzstation des Ingenieurbüro Pfeffer bis ins Labor rein alles erfasst und ist in Abbildung 39 zu sehen.

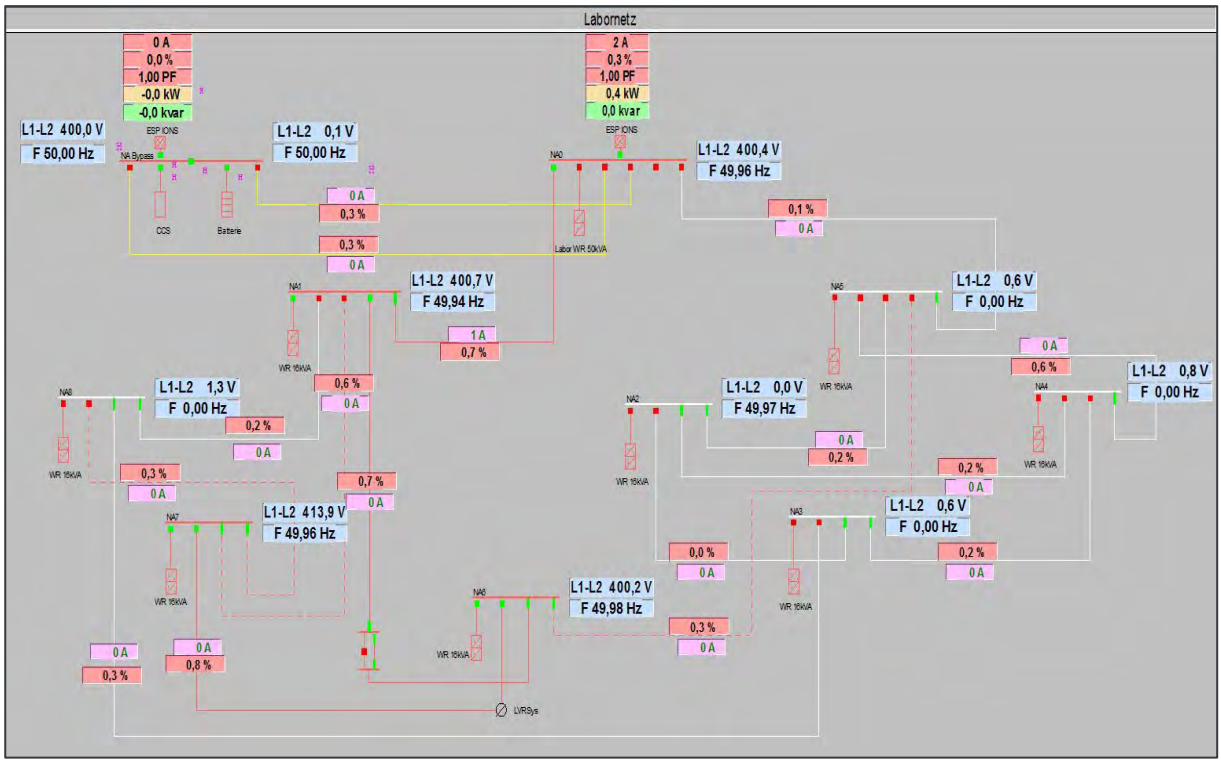


Abbildung 39: Leitwarte vom Smart Grid LAB Hessen.

Im Labor dient die Leitwarte nicht nur zur Visualisierung und Steuerung der Leistungsschalter, sondern auch als Daten Logger für die Messwerte. Es wird jeder Messwert abgespeichert, die Versuche im Nachgang auch nochmal auswerten zu können.

2.3.2. Weitere Möglichkeiten

Grundsätzlich kann bei den weiteren Möglichkeiten zur Visualisierung, Datenerfassung und Steuerung von zwei verschiedenen Ansatz gesprochen werden. Die zentrale Lösung und die dezentrale Lösung.

Cloud-Lösungen

Die zentrale Lösung sind Clouds. Die Prinzipielle Funktionsweise dabei ist immer gleich. Die Fernwirkeinheit (im SGL PFC200 / A8000) soll Daten über das MQTT-Protokoll an die Cloud senden. Das MQTT-Protokoll basiert auf dem Publisher-Subscriber Modell. Sender und Empfänger sind komplett voneinander entkoppelt und kommunizieren über einen zentralen Nachrichtenvermittler, der sich Broker nennt (siehe Abbildung 40). Der Empfänger muss den Hostname oder die IPAdresse des Senders wissen. Die Verbindung ist über die Transport Layer Security (TLS) zum Broker verschlüsselt.

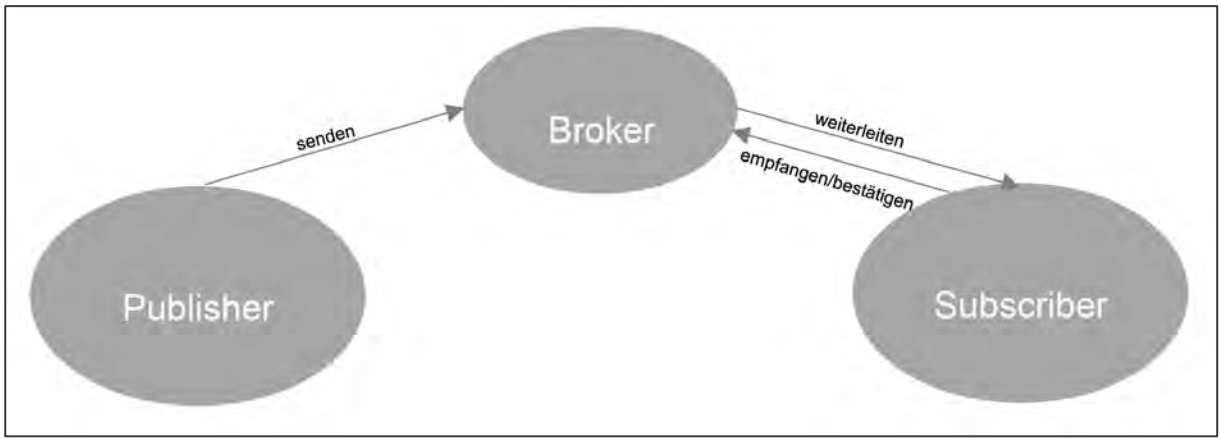


Abbildung 40: MQTT-Protokoll Modell.

Wegen der Datensicherheit ist bei den Verteilnetzbetreibern häufig die Frage, wer ist der Broker und wo werden die Daten gespeichert. Als Beispiel wird der Broker von Amazon genutzt. Es wird also eine weitere Partei involviert. Und aus Sicherheitsgründen sollen es, wenn deutsche Unternehmen und Speicherorte in Deutschland sein.

Um einen Einblick in die verschiedenen Cloudlösungen zu geben, werden im Folgenden für die im Labor implementieren Lösungen beispielhaft Abbildungen gezeigt.

Mindsphere

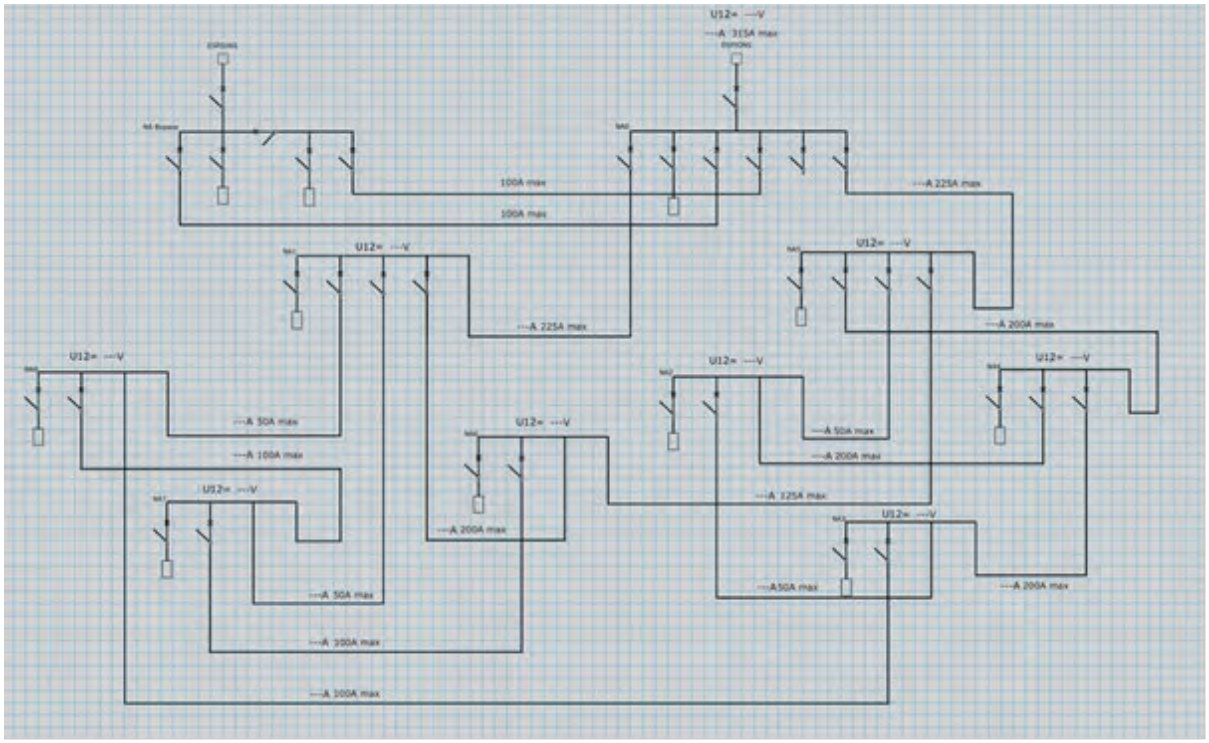


Abbildung 41: Übersicht des Labornetzes in der Mindsphere.

WAGO Cloud

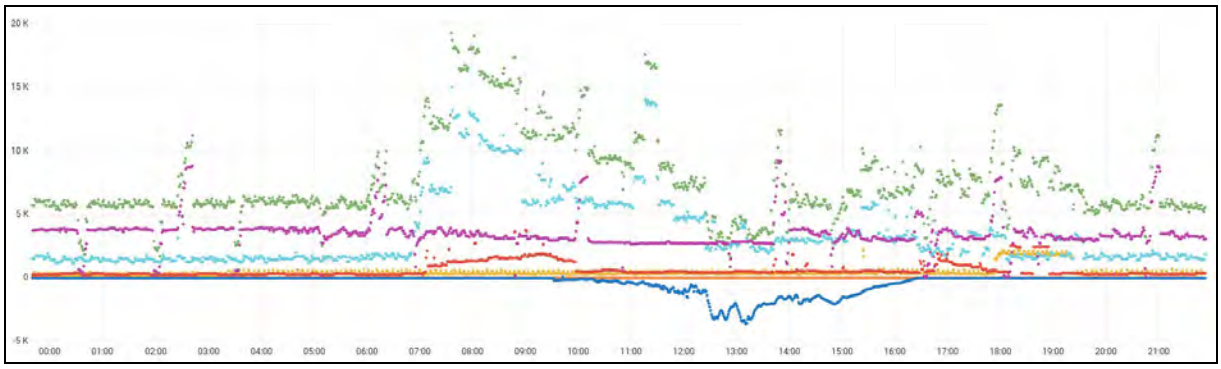


Abbildung 42: Ein Tagesverlauf in der Wago-Cloud.

Bentonet

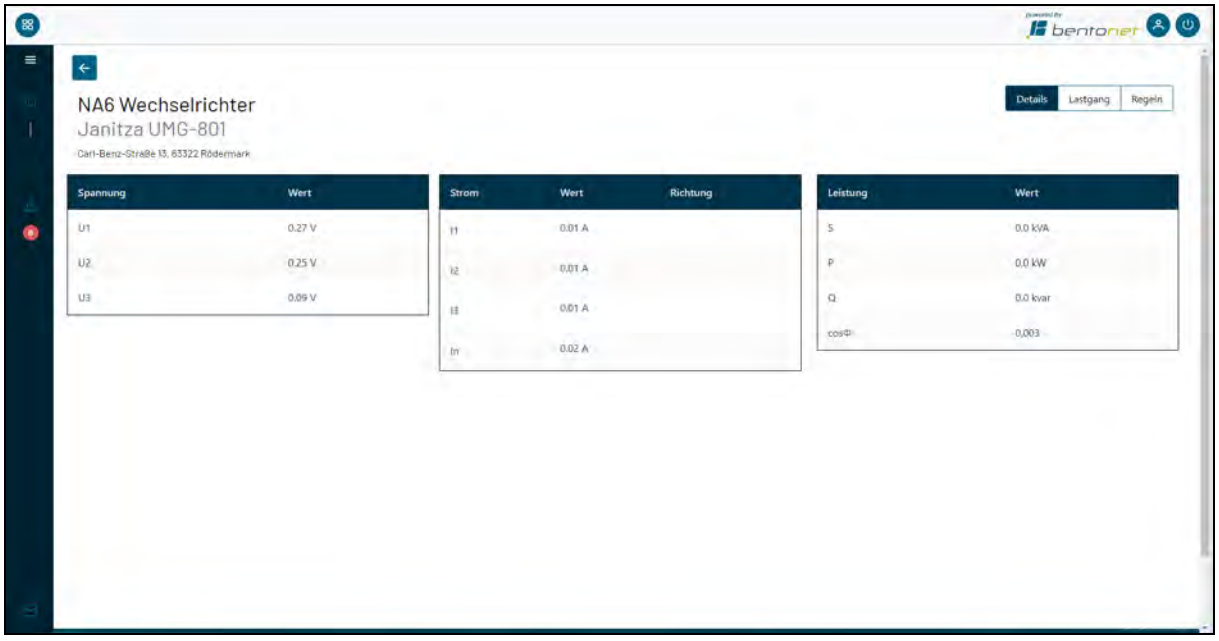


Abbildung 43: Darstellung der Momentanwerte in der Bentonet-Cloud.

Dezentrale Lösung

GridCal ist eine dezentrale Lösung. Es ist eine Software die auf den PFC 200 von Wago läuft. Es werden die Messwerte auf diesem lokal gespeichert und sind über ein Gatway von außen aufrufbar. Dies bedeutet auch, dass die Visualisierung direkt auf dem Controller stattfindet. Beispiele dazu sind in den folgenden Abbildungen zu sehen.

Abbildung 44: Topologie Dorf 1 in GridCal.

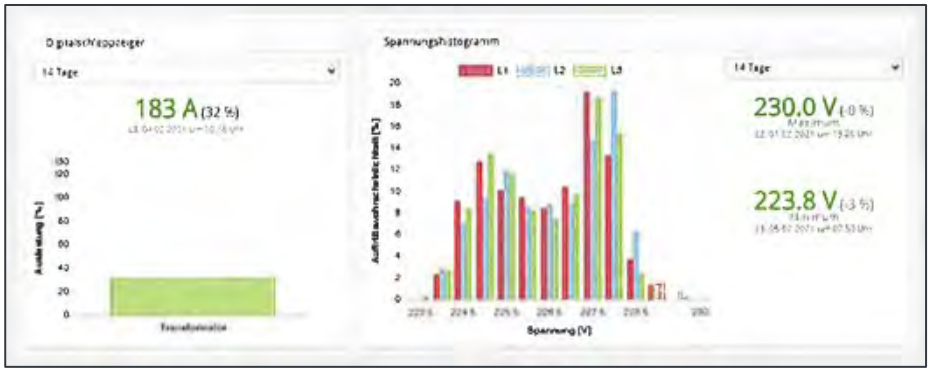


Abbildung 45: Beispielhafte Visulisierung in GridCal.

2.3.3. Aufbau im Smart Grid LAB Hessen

Im Smart Grid LAB Hessen wurde jeder Netzabschnitt in der Sekundärtechnik mit Fernwirk- und Messgeräten ausgestattet als sei jeder eine eigene Ortsnetzstation.

Es werden unterschiedlichen Kommunikationsprotokolle und Anbindungen an Software- oder Cloudlösungen installiert, um die Kommunikationswege auf IT-Sicherheit zu prüfen. Im Folgenden wird ein Beispiel dargestellt, wie eine Kombination von Fernwirkeinheiten und Software- bzw. Cloudlösungen aussehen könnte. In Abbildung 46 sind Möglichkeiten der Kommunikation mit dem Wago Controller und der Fernwirktechnik von Siemens dargestellt. Über die 3-Phasenleistungsmessklemme am Wago Controller PFC 200 werden Strom- und Spannungswerte dreiphasig aus der Niederspannung erfasst. Diese werden über einen internen Bus an den Controller gesendet, welcher über ein Gateway und das MQTT-Protokoll in die Azure Cloud gelangen. In der Azure Cloud können die Daten gespeichert und visualisiert werden. Über Modbus TCP IEC 60870-5-104 kann der Wago Controller an die Fernwirkeinheit SICAM A8000 von Siemens angebunden werden. Über die A8000 können Daten über ein Gateway über das IoT-Protocol MQTT in das cloudbasierte System MindSphere gesendet und ausgewertet werden. Über IEC 60870-5-104 können parallel zur Cloud die Daten in die Leitwarte übertragen werden. Statt über die A8000 könnte auch über den PFC 200 Daten

in die Leitwarte gesendet werden. Die Übertragung in die MindSphere ist jedoch auf die SICAM A8000 angewiesen.

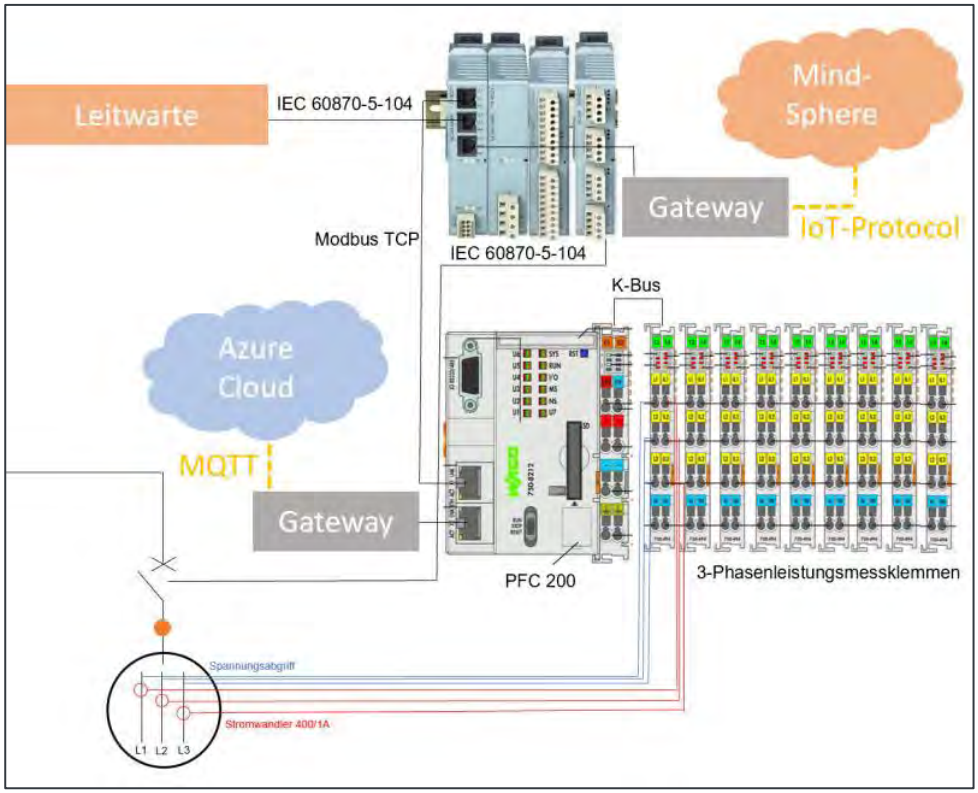


Abbildung 46: Beispiel für Kommunikationsmöglichkeiten.

Dies bedeutet im Labor werden alle Daten von der SICAM A8000 eingesammelt und dann in die Cloud Mindsphere gesendet. Für die WAGO Cloud sendet jeder PFC 200 seine Daten direkt in diese WAGO Cloud. Als kleines AddOn ist die Bentonet Cloud zu betrachten. Es wird der LTE Router direkt an das Messgerät UMG 801 von Janitza angeschlossen und dieser sendet die Daten in die Cloud.

Die gesamte Kommunikationsübersicht des Smart Grid LAB Hessens ist Abbildung 47. Mit eingebunden in diese Übersicht ist der Analyser der QGroup, näheres im Kapitel 5, sowie die Leitwarte. Die Fernwirkeinheit Acos750 dient dabei als Empfänger und gibt die Daten weiter.

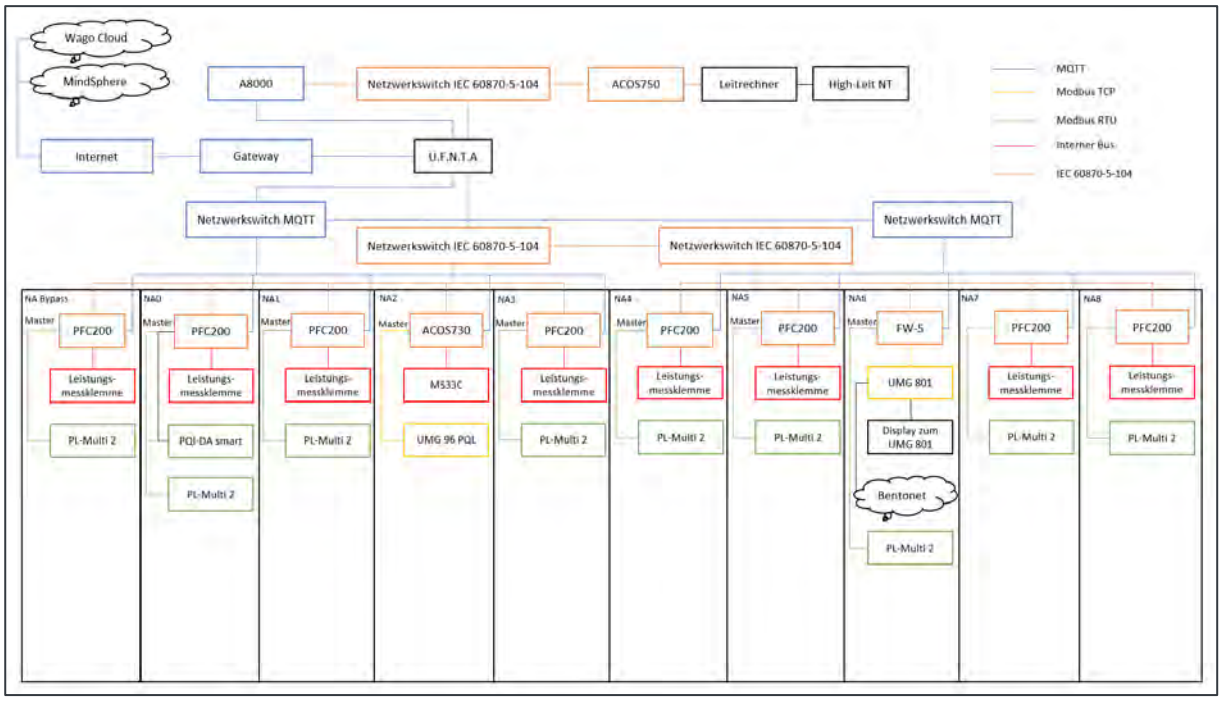


Abbildung 47: Kommunikationsübersicht des Smart Grid LAB Hessen.

2.4 Bestellungen

Wie im Änderungsantrag vom 22. Februar 2022 angezeigt kam es zu deutlichen Verzögerungen bei den Bestellungen und den Lieferzeiten, gegenüber den geplanten Zeiten.

In dem Projekt wurde zwar kommerzielle Technik eingesetzt, jedoch ist diese für unseren Anwendungsbereich und damit in der Auslegung des Labors nicht üblich und neuartig. Dies hat die Folge, dass das Feinkonzept in Teilen nicht nach Standards bzw. Referenzen vollzogen werden kann. Es muss mit möglichen Lieferanten die Einsatzfähigkeit und die Verfügbarkeit in weit größerem Maße als sonst üblichen Projekten validiert werden. Die Validierung mit den Lieferanten während der Covid-19 Pandemie hat nicht so gut, wie ursprünglich ohne Covid-19 geplant, funktioniert. Der Personalaufwand hat sich dadurch deutlich erhöht als angedacht und der Prozess bis zur Bestellung hat sich somit in die Länge gezogen. Und als dann bestellt wurde (Oktober 2021), kam es zu dramatischen Verlängerungen der Lieferzeiten von entscheidenden Komponenten, wie zum Beispiel Komponenten für die Wechselrichter. Bis dahin wurde von einer Inbetriebnahme im Oktober 2021 ausgegangen.

Bis zur Fertigstellung des Labors ist dann fast noch ein Jahr vergangen. Erst im September 2022 wurde der Aufbau soweit abgeschlossen, dass angefangen werden konnte, den Betrieb des Labors zu starten. Es fehlten noch Kleinigkeiten die dem Betrieb nicht geschadet haben, jedoch mussten so immer wieder noch Provisorien ausgebessert werden. So kann davon gesprochen werden, dass der finale Stand erst um die Jahreswende erreicht wurde.

Im Änderungsantrag wurde die Inbetriebnahme des Labors noch für Mitte Juli 2022 geplant (Abbildung 48), weil die Lieferung der Speicherprogrammierbarensteuerung sich weiter verzögert hatte. Anfang September wurde deshalb uns von der Siemens AG kostenneutral ein Leihgerät bis zur finalen Auslieferung (März 2023) zur Verfügung gestellt. Die finale Inbetriebnahme konnte so im September starten.

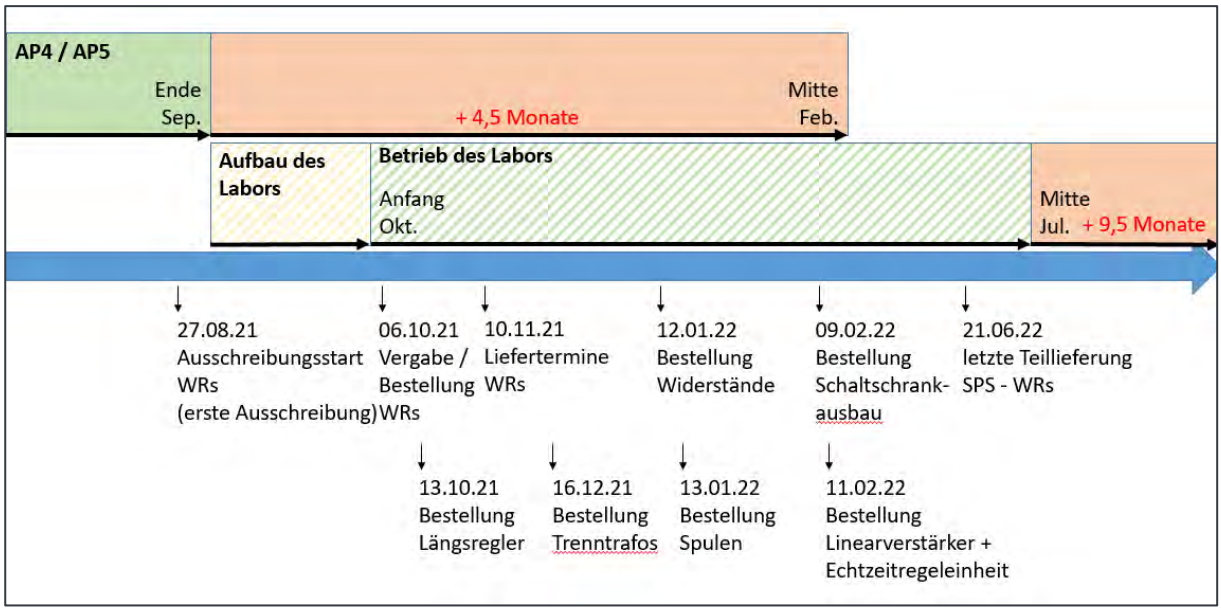


Abbildung 48: Prozessablauf bis in die Inbetriebnahme [35].

3. Szenarien

Die Szenarien definieren die Lastkurven der Prosumer in den Topologien. Eine Lastkurve kann sich aus einer Haushaltlastkurve (Grundlast), einer PV-Anlage mit und ohne Batteriespeicher, einer Wärmepumpe und einer Ladestation für Elektroautos zusammensetzen. Dabei ist die Auflösung 1 s.

Die „neuen Smart Grid Komponenten“ wie PV-Anlage, Batterie, Wärmepumpe und Ladestation werden berechnet und der Grundlastkurve hinzugefügt. Für die Szenarien werden 24 h Fenster aus den vier Jahreszeiten betrachtet. Die betrachteten Zeitfenster lassen sich jedoch auch variabel verändern.

3.5 Hauptbestandteile der Szenarien

3.5.1. Photovoltaik Anlagen

Photovoltaikanlagen mit kleineren Leistungen, welche üblicherweise bei Prosumern zu finden sind, werden am Niederspannungsnetz angeschlossen. Eine durchschnittliche Photovoltaikgröße eines Einfamilienhauses liegt bei 4-10 KWp. Besonders in Haushalten mit Photovoltaikanlagen wird die erzeugte Energie nicht lokal verbraucht, da der Bezug tagsüber zu gering ist. Der Verbrauch und die Erzeugung finden jeweils in einem anderen Zeitfenster statt und gleichen sich nicht lokal aus. Aus diesem Grund entstehen Erzeugungsspitzen, welche in das Niederspannungsnetz zurückgespeist werden und so zur Entstehung von Netzengpässen beitragen. Zur Verschiebung dieser Erzeugungsspitzen zur Eigenverbrauchsoptimierung können Hausbatteriespeicher eingesetzt werden.

Regulatorische Rahmenbedingungen

Die Einspeisevergütung richtet sich nach dem Errichtungsjahr, der Vergütungsart und dem EEG-Gesetz aus dem Errichtungsjahr. Für die Vergütungsart ist entscheidend, wie hoch die installierte Leistung der Photovoltaikanlage ist. Bei einer Photovoltaikanlage, welche eine installierte Leistung kleiner 100 kW besitzt, gilt die feste Einspeisevergütung. Bei Photovoltaikanlagen, welche eine installierte Leistung bis 750 kW besitzen, gilt das Marktprämienmodell. Nach EEG 2021 §61a entfällt die EEG-Umlage, wenn sich der Stromerzeuger selbst mit der Energie versorgt, keine Vergütung in Anspruch nimmt und nicht unmittelbar noch mittelbar am Netz angeschlossen ist. [32] Die erzeugte Energie wird mit der Einspeisevergütung vergütet. Nach 20 Jahre läuft diese Vergütung aus und der Betreiber kann die erzeugte Energie selbst verbrauchen oder direkt vermarkten.

Aktueller Status

Die Stromerzeugung aus Photovoltaikanlagen deckt 2020 9,2% des Bruttostromverbrauchs mit insgesamt 50,6 TWh. Die 2 Millionen installierten Photovoltaikmodule in Deutschland kommen auf eine Nennleistung von insgesamt 54 GW. Zeitweise kann zwei Drittel des Stromverbrauchs aus Photovoltaikstrom bezogen werden.

Die Einspeisevergütung für eingespeiste Energie aus Photovoltaikanlagen liegt aktuell bei 7,58 ct/kWh (Juni 2021). Im Vergleich dazu lag die Einspeisevergütung im Jahr 2004 bei 57,4 ct/kWh. Die Vergütung ist seit 2004 um 87% gesunken. Eine ähnliche Degression ist auch für die Photovoltaikmodule zu erkennen. Pro kWp Leistung kostete eine Photovoltaikanlage noch 6.500 € und liegt 2018 bei 1.200 €/kWh. [36]

Die Einspeisevergütung für die eingespeiste Energie aus Photovoltaikanlagen entfällt nach 20 Jahren. Prosumer, welche weiterhin ins Netz zurückspeisen, werden mit dem Jahresmarktwert Solar vergütet.

Dieser wird nicht aus dem durchschnittlichen Strompreis ermittelt, sondern hängt zusätzlich von der erzeugten Strommenge in jeder einzelnen Stunde ab. Die Einspeisevergütung liegt dann bei ca. 3 - 4 ct/kWh. [37]

Bei einem üblichen Lastgang eines Haushalts lässt sich mit einer 5 kWp Photovoltaikanlage 30% des Stromverbrauchs abdecken. Der Eigenverbrauchsanteil kann mit einem Batteriespeicher mit einer Kapazität von 6 kWh auf 60% angehoben werden. Bei einem Batteriespeicher mit 10 kWh und eine Photovoltaikanlage mit 10 kWp lässt sich der Eigenverbrauchsanteil auf 80% erhöhen. Eine weitere Erhöhung der Photovoltaikleistung oder Kapazität des Batteriespeichers bewirken nur minimale Verbesserungen des Autarkiegrades. [38]

3.5.2. Batteriespeicher

Das zunehmende volatile Stromnetz durch regenerative Energien führt zu Zeiten des Energieüberflusses und des Energiedefizites und muss bilanziert werden. Batteriespeicher können eine Flexibilitätsoption im Stromnetz darstellen und netzdienlich eingesetzt werden, um das Stromnetz stabil zu halten. Sie können Primärleistung bereitstellen, Erzeugungsspitzen zwischenspeichern und Lastspitzen glätten. Durch den Einsatz von Batteriespeicher kann das Netz ständig verbessert werden und gewinnt an Flexibilität. Es können Netzengpässe und Abschaltungen von regenerativen Energien verhindert werden. Batteriespeicher können im Stromnetz zur Spannungshaltung beitragen, indem sie Blindleistung bereitstellen, Kurzschlussleistung bereitstellen, Ein- und Ausspeichern von Wirkleistung und fluktuierende Einspeisung ausgleichen. Bisher wurde die Kurzschlussleistung von den konventionellen Stromerzeugern, durch die rotierenden Massen, und die elektromagnetische Energie der Generatoren bereitgestellt. Da die rotierenden Massen immer weniger werden und Wind- und Photovoltaikanlagen im Fehlerfall vom Netz gehen, fehlt die Bereitstellung von Kurzschlussleistung. Batteriespeicher können unter anderem mit der Bereitstellung von Kurzschlussleistung dem Netz dienlich sein. Um das Angebot und die Nachfrage an Energie immer abzugleichen und dabei die Frequenz zu halten, kann der Batteriespeicher zur Bereitstellung von Regel- und Reserveleistung dienen. [39] Außerdem können Batteriespeicher zur unterbrechungsfreien Stromversorgung beitragen und sind schwarzstartfähig.

Regulatorische Rahmenbedingung

Nach dem FNN-Hinweis sind Netz- und Systemdienlichkeit für das Stromnetz zum Teil umgesetzt. Der FNN-Hinweis beinhaltet unteranderem, dass der Batteriespeicher sich durch die Einhaltung von VDE-AR-N 4105 an der dynamischen Netzstützung beteiligen muss. Beim Ladevorgang ist ein cos φ=0,95 bis 1 vorgeschrieben. Nach VDE-AR-N 4100 muss eine Wirkleistungsbegrenzung des Batteriespeichers am Netzanschlusspunkt umgesetzt werden. Nach der VDE-AR-N 4100 muss der Batteriespeicher bei Über- und Unterfrequenz sein Wirkleistungsverhalten anpassen. Dabei muss er sich ständig auf der Frequenz-Kennlinie nach VDE-AR-N 4105 bewegen. [40]

Nach dem EEG 2021 §3 sind Batteriespeicher, welche aus erneuerbaren Energien Energie zwischenspeichern, als EEG-Anlage definiert. Der Betreiber von einem Batteriespeicher, welcher aus erneuerbaren Energien, Energie zwischenspeichert hat Anspruch auf eine EEG-Vergütung (EEG 2021 §19).

Nach dem EnWG §118 Abs. 6 sind Anlagen zur Speicherung von elektrischer Energie, welche ab dem 04.08.2011 innerhalb von 15 Jahren in Betrieb genommen werden, keine Netzentgelte für 20 Jahre ab dem Zeitpunkt der Inbetriebnahme zu zahlen. Nach EEG 2021 §61a entfällt die EEG-Umlage für den Batteriespeicher, wenn sich der Stromerzeuger selbst mit der Energie versorgt, keine Vergütung in

Anspruch nimmt und nicht unmittelbar noch mittelbar am Netz angeschlossen ist. [32] Nach StromStG §5 Abs. 4 sind stationäre Batteriespeicher, welche Energie vorübergehend speichern und dann wieder ins Versorgungsnetz einspeisen, Teil des Versorgungsnetzes und sind von der Stromsteuer befreit.

Aktueller Status

Batteriespeicher lassen sich in drei Größen kategorisieren: Heimspeicher (bis 30 kWh, Industriespeicher 30-1.000 kWh, Großspeicher ab 1.000 kWh). [41] In Abbildung 49 ist zu erkennen, dass die kumulierte Kapazität der Batteriespeicher in Deutschland stetig wächst. 2019 lag sie bei einer kumulierten Kapazität von über 2.000 kWh. Die meist eingesetzte Technologie sind Lithium-Ionen-Akkus mit insgesamt 87% Marktanteil.

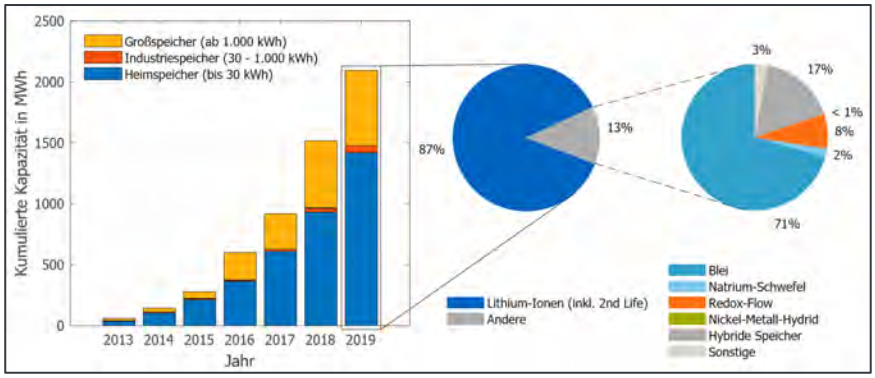


Abbildung 49: Kumulierte Kapazität und prozentuale Batterietechnologie von Batteriespeichern in Deutschland [41].

Die Kosten der Lithium-Ionen-Akkus zeigen eine deutliche Degression. In Abbildung 50 ist die Preisentwicklung zu sehen. 2010 lag der Preis pro kWh noch bei 600€, 10 Jahre später lag er bereits bei 111€/kWh. Bis 2025 ist nach dieser Statistik mit weiteren Preissenkungen zu rechnen. [42]

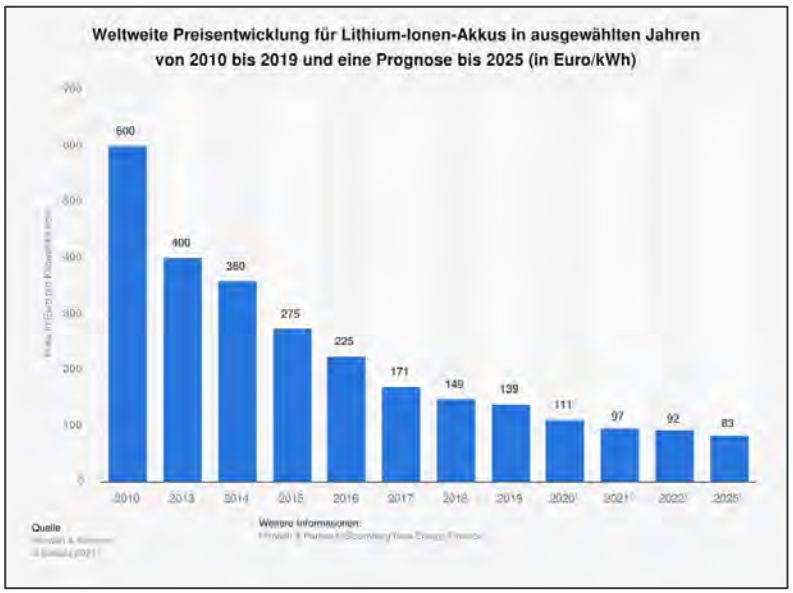


Abbildung 50: Preisentwicklung von Lithium-Ionen-Akkus [42].

Heimspeicher zu Speicherung der Energie aus der eigenen Photovoltaikanlage werden immer häufiger für die Eigenverbrauchsoptimierung verwendet. Grund hierfür ist unteranderem das Auslaufen der Einspeisevergütung. Der Bestand der Heimspeicher in Deutschland beläuft sich auf 272.000 Stück. Seit 2017 steigt der Zubau von Batteriespeicher für Solaranlagen stetig an.

Durch die enorme Preissenkung der Lithium-Ionen-Batterien ist davon auszugehen, dass immer mehr in Batteriespeicher investiert wird und sowohl im Heimnetz als auch im Versorgungsnetz Batteriespeicher eingesetzt werden. Im Heimnetz wird es immer wichtiger werden, Batteriespeicher für die erzeugte Energie der Photovoltaikanlage zu benutzen, da die Förderungen des Stroms aus erneuerbaren Energien auslaufen wird und der Zeitpunkt von Erzeugung und Verbrauch nicht übereinstimmen. Die aktuellen Zahlen der Entwicklung des Zubaus von Heimspeichern und der stetig ansteigenden kumulierten Leistung bestätigen das.

3.5.3. Elektrische Wärmepumpen

Elektrische Wärmepumpen beziehen ihre Energie aus der Umwelt und sind im Vergleich zu konventionellen Heizsystemen umweltfreundlich. Bei elektrischen Wärmepumpen wird zwischen Luft-, Erd- und Wasserwärmepumpen unterschieden. Wärmepumpen benötigen für den Antrieb und für die Pumpe Strom. [43] Durch die Nutzung von elektrischen Wärmepumpen wird der Bezug im Niederspannungsnetz erhöht. Der Stromverbrauch für ein Einfamilienhaus mit zwei Personen beträgt 7.500 kWh - 10.000 kWh pro Jahr. [44] Im Vergleich zum durchschnittlichen Stromverbrauch eines Einfamilienhauses pro Jahr, welcher zwischen 2.000 kWh – 4.000 kWh [45] liegt, stellt die Wärmepumpe eine erhebliche Erhöhung der Gesamtlast dar. Wärmepumpen belasten das Niederspannungsnetz mit der Erhöhung der Gesamtlast, aber auch mit auftretenden Lastspitzen.

Regulatorische Rahmenbedingung

Das Gebäudeenergiegesetz (GEG) wurde 2020 verkündet und führt das alte Energieeinsparungsgesetz, die Energieeinsparverordnung und das Erneuerbare-Energien-Wärmegesetz zusammen. In dem Gesetz werden energetische Anforderungen an Neubauten, an Bestandsgebäude und die Verwendung von erneuerbaren Energien für Wärme- und Kälteversorgung definiert. [46] Das GEG fordert bei allen Gebäuden eine Nutzung von erneuerbaren Energien, wie zum Beispiel durch Solaranlagen, Brennstoffzellenheizung, Geothermie, Umweltwärme und Strom aus erneuerbaren Energien.

Nach GEG §37 werden die Anforderungen an die elektrische Wärmepumpe erfüllt, wenn der Wärme- und Kältebedarf zu 50 % aus der elektrischen Wärmepumpe gedeckt wird. [32]

Aktueller Status

Laut einer Absatzstatistik des Bundesverbandes Wärmepumpe, welche in Abbildung 51 zu sehen ist, sind 2020 insgesamt 120.000 elektrische Wärmepumpen abgesetzt worden. 2019 lag der Absatz noch bei ca. 85.000, was im Vergleich zu 2020 ein Wachstum von 41 % ausmacht. Ein Viertel der in 2020 installierten Wärmepumpen ersetzen alte Ölheizungen. [43] Aus der Statistik wird ersichtlich, dass insbesondere Luft- und Wasserwärmepumpen installiert werden und die Absatzzahlen zur Wärmepumpe tendenziell stiegen.

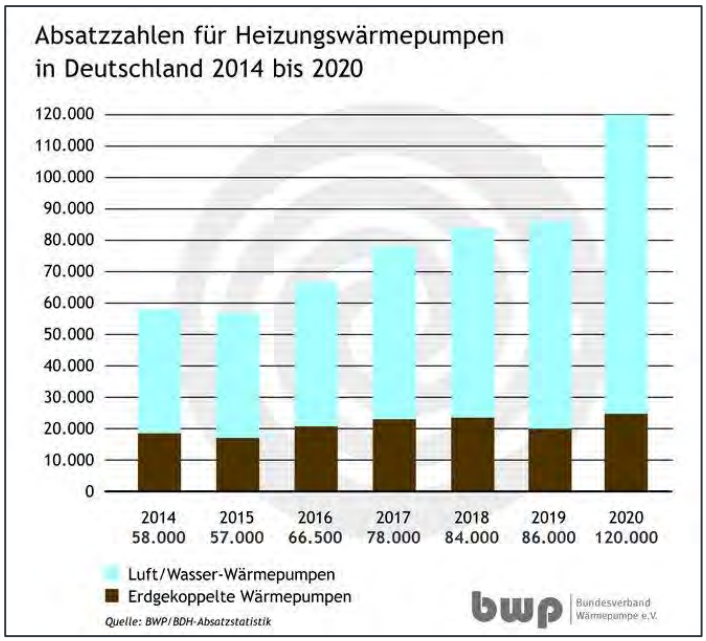


Abbildung 51: Absatzentwicklung von elektrischen Wärmepumpen in Deutschland [43].

Nach der BDEW-Studie zum Heizungsmarkt beträgt der Anteil von elektrischen Wärmepumpen bei Wohngebäuden in Deutschland 3,4 % und bei Wohnungen 2,2 %. Die am meiste verwendete Heizungsart in Deutschland ist die Erdgas Heizung gefolgt von der Öl-Heizung. [47] Da diese Kennzahlen aus dem Jahr 2019 sind und in 2020 nach der Absatzstatistik des Bundesverbandes Wärmepumpe die Absatzzahlen um 40 % gestiegen sind, sind auch die prozentualen Anteile der elektrischen Wärmepumpe in Deutschland gestiegen und zeigen somit nicht den ganz aktuellen Stand. Die Kennzahlen aus 2019 zeigen trotzdem eine Tendenz, dass der Anteil der elektrischen Wärmepumpe als Heizsystem in Deutschland noch sehr gering ist. Die Umstellung von konventionellen Heizsystemen auf elektrische Wärmepumpen wird etwas länger andauern, da Heizungen eine lange Lebensdauer aufweisen und davon auszugehen ist, dass Verbraucher erst ihr Heizsystem erneuern, wenn die alte Heizung kaputt ist. Im Neubau beträgt der Anteil von elektrischen Wärmepumpen 43 % und bei neuen Heizungen in Bestandsgebäuden 6 %. [48]

3.5.4. Elektromobilität

Der Verkehrssektor in Deutschland ist mit 19% am CO2 beteiligt. 96% des CO2-Ausstoßes wird von PKWs und LKWs verursacht. Bis 2030 sollen mindestens 40-42% weniger CO2 ausgestoßen werden zum Vergleichsjahr 1990. [49] Von der Politik getrieben, wird der Ausbau der Ladeinfrastruktur und die Zunahme von Elektrofahrzeugen voranschreiten. Dazu sind regulatorische Rahmenbedingungen verfasst, es gibt verschiedene Förderungsprogramme und Forschungsprojekte zum Thema Ladeinfrastruktur, Elektromobilität und Lademanagement. Im Folgenden soll eine Übersicht zur Entwicklung und regulatorischen Rahmenbedingungen von Elektromobilität und Ladeinfrastruktur gegeben werden. Das soll die Grundlage zur Erstellung der Szenarien bezüglich Ladesäulen und Elektrofahrzeuge im Smart Grid Lab sein.

Regulatorische Rahmenbedingungen

Elektrofahrzeuge zählen laut EnWG §14a zu steuerbaren Verbrauchseinrichtungen. Wird mit dem Endkunden die netzdienliche Steuerung von Verbrauchseinrichtungen vereinbart, so reduziert sich das Netzentgelt für den Verbraucher. [32] Demnach gibt dieses Gesetz dem Verteilnetzbetreiber die

Möglichkeit, beispielsweise bei einem Netzengpass, die Ladeleistung eines Elektromobils abregeln und diese netzdienlich für sein Netz einzusetzen. Das Gesetz EnWG §14a ist eine Novelle zum EnWG §14 und erweitert sich insbesondere durch den marktorientieren Ansatz. Die Förderung zur Flexibilität des Marktes und die Möglichkeiten für neue Geschäftsmodelle werden hier gesetzlich verankert.

Aktueller Status

Die Anzahl der Zulassungen von Fahrzeugen mit reinem Elektroantrieb haben im Jahr 2020 im Vergleich zum Vorjahr um 206% zugenommen. In Deutschland haben insgesamt 13,5% aller neu zugelassenen Fahrzeuge einen elektrischen Antrieb. [50] Aus der aktuellen Statistik der Neuzulassungen ist davon auszugehen, dass die Anzahl der Elektroautos stetig zunimmt. Zum 1. Januar 2021 betrug die Anzahl der zugelassenen Elektrofahrzeuge 309.100. [42] Der Marktanteil von Elektrofahrzeugen am Bestand von Personenkraftwagen beträgt 1,22 %. [42] In Abbildung 52 ist die Entwicklung des Marktanteils von Elektrofahrzeugen in Deutschland von 2011 bis 2021 dargestellt. Mit insgesamt 1,22% Marktanteil von rein elektrischen Fahrzeugen und Hybriden fällt der Marktanteil von Elektromobilen sehr gering aus. Aus der Statistik ist jedoch zu entnehmen, dass der Anteil innerhalb der letzten 4 Jahre stetig wächst und es eine signifikante Erhöhung des Marktanteils von 2020 bis 2021 gibt, wobei die Statistik mit den Werten des ersten Quartal 2021 endet. Daraus ist zu schließen, dass es in 2021 voraussichtlich zu einer weiteren Erhöhung in den nächsten drei Quartalen kommt und der Marktanteil von Elektrofahrzeugen in der Zukunft erheblich steigt. Der erhöhte Anstieg in den letzten vier Jahren ist, im Vergleich zu den geringen Erhöhungen vor 2017, damit zu begründen, dass zum einen die Technik von Elektrofahrzeugen weiter ist und zum anderen die Ladeinfrastruktur ausgebaut wurde. In den Jahren zuvor gab es wenige Anreize ein Elektrofahrzeug anzuschaffen. Mit den Förderungen und dem Ausbau von Ladeinfrastruktur hat sich das für die Zukunft geändert.

Abbildung 52: Statistik zur Entwicklung des Marktanteils von Elektrofahrzeugen am Bestand von PKWs [42].

Das Ziel der Bundesregierung ist es, bis 2030 7-10 Millionen Elektrofahrzeuge zuzulassen und eine Millionen Ladepunkte zu Verfügung zu stellen. [49] Im Quartal 2 2021 sind es in Deutschland insgesamt 23.081 Ladepunkte. Innerhalb eines Jahres von Quartal 2 2020 bis Quartal 2 2021 wurden 3.720 neue Ladepunkte installiert. [42] Die Ziele der Bundesregierung bis 2030 eine Millionen Ladepunkte zur Verfügung zu stellen scheint unrealistisch bei einem Zuwachs von Ladepunkten pro Jahr um 3.720 Stück.

Im Forschungsprojekt „E-Mobility-Carré“ wird die Integration von Elektromobilität in die bestehende Netzinfrastruktur erprobt. Es zeigt sich, dass ein intelligentes Lademanagement die Anschlussleistung der Ladepunkte absenkt und Lastspitzen reduziert werden. In diesem Projekt wird ein Mehrfamilienhaus mit insgesamt 58 Ladepunkten untersucht. Es kam maximal zu einer Gleichzeitigkeit von 13 parallelen Ladevorgängen von Elektromobilen. [51] In Bezug auf dieses Projekt ist mit einem Gleichzeitigkeitsfaktor in Wohngebieten insbesondere in Mehrfamilienhäusern von 22% auszugehen.

Ladesäulen-Stationen mit mehreren Schnellademöglichkeiten können auch so umgesetzt werden, dass sie nicht das Stromnetz belasten. Das zeigt das Vorhaben eines Pilotprojekts von Audi. Es sollen Charging Hubs aufgebaut werden, in dem der Kunde sein Elektrofahrzeug laden und in der Zeit in einer Lounge warten kann. Das Stromnetz wird dabei nicht belastet, da die gesamte Energie aus Speichern entnommen wird. Diese Speicher bestehen aus gebrauchten Lithium-Ionen-Akkus. Ein Charging Hub besteht aus drei Speichereinheiten, welche insgesamt eine Kapazität von 2,45 MWh aufweisen. An sechs Schnellladepunkten kann mit bis zu 300 kW geladen werden. Der Stromspeicher wird aus dem Stromnetz mit 11 kW geladen und hat zusätzlich eine Photovoltaikanlage als Erzeugungseinheit auf dem Dach. [52] Das vorgestellte Vorhaben zeigt, dass durch Integration von Photovoltaikanlage, Batteriespeicher und Ladeinfrastruktur das Stromnetz nicht belastet werden muss und gleichzeitiges Schnellladen gewährleistet werden kann. An Ladepunkten, welche in Bereichen des längeren Aufenthalts liegen und an denen es zum Gleichzeitigen Laden kommt, beispielsweise Kaufhäuser, könnte es eine Lösung für die Umsetzung von Ladeinfrastruktur sein, um Netzengpässe und die damit verbundenen Netzausbaumaßnahmen zu verhindern.

In der Studie „Ladeinfrastruktur nach 2025/2030“ der Nationalen Leitstelle Ladeinfrastruktur wird der Bedarf an Ladeinfrastruktur innerhalb von sechs Entwicklungsszenarien bestimmt. Für das Jahr 2030 wird prognostiziert, dass 61% der privaten Stellplätze über einen Ladepunkt verfügen. Bei einer ins gesamten Lademenge im Jahr 2030 von 30.000 GWh werden 41% dieser Energiemenge an privaten Ladepunkten verladen. 32% der Energiemenge wird im öffentlichen Bereich geladen und 27% im gewerblichen Bereich. Der Anteil der privaten Ladevorgänge wird mit 76-88% angenommen und im öffentlichen Bereich 12-24%. Das Verhältnis Elektrofahrzeug zu öffentlichen Ladeinfrastruktur wird mit 20:1 angegeben. Im urbanen Raum liegt das Verhältnis bei 14:1 und im suburbanen Raum bei 23:1. [53]

3.6 Feineinstellungen

Das Niederspannungsnetz des Labors lässt sich in vier Netztypen Land, Dorf, Vorstadt und Stadt verschalten. In diesen wurden Prosumer in verschiedenen Ausbau-Szenarien und deren Auswirkung auf den Netzbetrieb untersucht, um die zentralen Fragestellungen des Forschungsprojekts zu erörtern.

Die hessischen Gemeinden können eindeutig nach ihren Gemeindeschlüsseln identifiziert werden. Um das Bundesland aussagekräftig darzustellen, wurden mit Hilfe der Hessischen Gemeindestatistik 2021 [54] die einzelnen Gemeinden anhand ihrer Einwohner-Arbeitsplatzdichte gewichtet und einem Verdichtungsraum zugeordnet. Dadurch lassen sich Datensätze aus Hessen in die Labortopologien Land, Dorf, Vorstadt und Stadt klar einteilen. Der Schwerpunkt bei der Erstellung der Energie-Szenarien lag auf der technischen Umsetzung der Energiepolitischen Ziele auf Verteilnetzebene. In den Szenarien sind keine demographischen Strukturen, wie Wandel oder Bevölkerungswanderungen, berücksichtigt. Daher ändert sich die Anzahl der Gebäude in den Labor-Szenarien über die Jahre nicht.

Den aktuellen Stand beschreibt das Szenario-Jahr 2020. Hierfür wurden die Einträge des Marktstammdatenregisters für Hessen hinsichtlich PV-Anlagen mit und ohne Batteriespeicher

analysiert [55]. Es ließen sich dort auch die aktuellen Trends im Ausbau herausarbeiten. Gebäudebestände und Einwohnerzahlen lieferte die Hessische Gemeindestatistik 2021 [54]. Die Datengrundlage für den Kraftfahrzeug- und Ladesäulenbestand lieferte das Bundeskraftfahramt [56].

Als Grundlage der Zukunfts-Szenarien dient das Osterpaket 2022 der Bundesregierung und die daraus entstandenen Gesetzesentwürfe [57] [58]. Hier werden konkrete Ausbauziele der Erneuerbaren Energien festgelegt. Die von der Bundesregierung definierten Energiepolitischen Ziele sind gestaffelt und betreffen den gesamten Energiesektor. Die Untersuchungen im Labor fokussieren sich auf die Szenario-Jahre 2020, 2030 und 2045. In den Szenarien werden verschiedene Prosumer-Strukturen im Sektor der privaten Haushalte in Hessen abgebildet. Zusätzlich wird ein viertes Szenario Vollausbau entwickelt. Dieses beschreibt den maximalen Prosumer-Ausbau, bei dem alle Gebäude über eine PV-Anlage, einen Batteriespeicher, eine elektrische Wärmepumpe und eine private Ladestation für Elektroautos verfügen.

3.6.1. Energierahmen

Der Energierahmen zeigt den übergeordneten Ausbau-Stand und die energiepolitischen Ziele. Auf Grundlage der aktuellen Verhältnisse können die Ziele für die gesamte Bundesrepublik zunächst auf Hessen und anschließend auf die für das Labor relevanten privaten Haushalte des Bundeslandes Hessen heruntergerechnet werden. Als tragende Säulen der Energiewende werden, nach den energiepolitischen Zielen Windkraft- und Solaranlagen gesehen. Gemäß dem aktuellen technischen Stand ist der Ausbau zu einem Prosumer nur mit Photovoltaik-Aufdachanlagen wirtschaftlich realisierbar.

Die aktuellen installierten Leistungen für Wind- und Solarenergie für Deutschland liefert das Bundesministerium für Wirtschaft und Klimaschutz [59]. Die derzeitig installierte Gesamtleistung für Hessen wurde dem Energiemonitoringbericht 2021 für Hessen entnommen und die installierte PV-Leistung auf und an Wohngebäuden konnte aus dem Marktstammdatenregister ermittelt werden [60] [55]. Zukünftige Ausbauziele enthält der Gesetzesentwurf zum EEG 2023 [59]. Um den hessischen Anteil daraus zu ermitteln, wurde der Mittelwert aus dem aktuellen Anteil an der installierten PV-Leistung und dem Gesamtflächenanteil gebildet. Die installierte Leistung für den Sektor der privaten Haushalte wurde anhand des aktuellen Anteils fortgeführt.

Die aktuellen PKW-Bestände lieferte das Kraftfahrbundesamt, wobei die Anzahl der privaten und öffentlichen Ladestationen dem Energiemonitoringbericht Hessen 2021 entnommen wurde [56] [60]. Die prozentualen zukünftigen Anteile der Batterieelektrischen- und Hybridfahrzeuge wurden in der Verteilnetzstudie Hessen abgeschätzt [61]. Ausbauziele für öffentliche Ladestationen sind im ersten Masterplan Ladeinfrastruktur der Bundesregierung für das Jahr 2030 festgehalten [62]. Die dena-Studie „Privates Ladeinfrastrukturpotential in Deutschland“ führt auf, dass Automobile verstärkt auf privaten Stellplätzen geparkt werden, weshalb privaten Lademöglichkeiten ein großes Potential zugeschrieben wird [63]. Diese These unterstützen auch die in der Studie aufgeführten Zahlen aus Norwegen und den Niederlanden, in den vier- bis fünfmal mehr private Ladestationen installiert sind als öffentliche. Für Hessen gibt das Hessische Ministerium für Wirtschaft, Energie, Verkehr und Landesentwicklung ähnliche Erkenntnisse an und den Zahlen aus dem Energiemonitoringbericht nach, übertrifft bereits heute in Hessen die Anzahl der privaten Ladestationen die der öffentlichen um das Vierfache [60]. Aus diesem Grund wurden die Ziele für den öffentlichen Ausbau in den Jahren 2030 und 2045 mit dem Faktor 4,5 multipliziert, um die Anzahl der privaten Lademöglichkeiten abzuschätzen.

Eine Studie des BDEW zum Heizungsmarkt stellt die deutschen und hessischen Heizungssysteme gegenüber [47]. In Hessen wurden 2019 rund 4,7 % aller Wohngebäude mit Elektro-Wärmepumpen beheizt, was knapp über dem Wert für ganz Deutschland liegt. Die Ziele in der zukünftigen Wärmeversorgung sind noch recht breit gesteckt. Bis zum Jahr 2045 wird die vollständige Klimaneutralität von Gebäuden angestrebt, bei einem deutlich reduzierten Energiebedarf. Ab dem Jahr 2025 muss jede neu eingebaute Heizung auf der Basis von mindestens 65 % Erneuerbarer Energien betrieben werden und bis 2030 soll 50 % der gesamten Wärme klimaneutral erzeugt werden. Der Energiemonitoringbericht zeigt, dass in den vergangenen Jahren vermehrt elektrische Wärmepumpen zur Beheizung von Neubauten eingesetzt wurden [60]. Diese haben derzeit die höchsten Fördersätze der KfW, gelten aber allgemein noch als recht kostspielig. Vor allem die Sanierung von Heizsystemen in Bestandsgebäuden ist hochpreisig. Aus diesem Grund wurde angenommen, dass in Zukunft ein Mix aus verschiedenen Technologien im Gebäudebestand eingesetzt wird.

Tabelle 7: Rahmendaten für die Szenarien [54] [55] [56] [57] [58] [29] [59] [60] [61] [62] [63] [47] [64] [65] [66] [67] [68] [69] [70] [71] [72] [73].

	2020		2030		2045	
	Deutschland	Hessen	Deutschland	Hessen	Deutschland	Hessen
PV gesamt [GW]	53,72	2,41	215,00	10,75	400,00	20,00
PV auf HH [GW]	9,75	0,67	53,75	3,23	100,00	6,00
Batteriespeicher [GW]		0,05				
Wind onshore [GW]	55,63	2,26	115,00	5,75	160,00	9,60
Wind offshore [GW]	7,79	-	30,00	-	70,00	-
Biomasse [MW]	9.293,00	303,60	8.400,00			
Biomasse [TWh]	45,03	1,37				
Pkw-Bestand	48.248.584	3.772.207	50.000.000	4.100.000	55.000.000	4.300.000
Elektroautos PHEV+BEV	588.944	113.914	9.000.000	738.000	44.000.000	3.440.000
Anteil E-Autos	1,22%	3,02%	18%	18%	80%	80%
Ladestationen privat	300.000	12.212	4.500.000	318.446	10.350.000	724.500
Ladestationen öffentlich	39.440	2.791	1.000.000	70.766	2.300.000	161.000
Wärmepumpen	915.200	133.896	4.075.600	288.464	10.395.000	800.000
Einwohner*Innen	83.161.000	6.293.154	84.700.000	6.370.000	85.100.000	6.400.000
Wohngebäude	19.300.000	1.405.221	20.378.000	1.442.319	20.790.000	1.600.000
Wohnungen / Haushalte	41.600.000	2.975.475	44.300.000	3.135.475	46.200.000	3.415.475

3.6.2. Durchdringungen

Über die Gesamtgebäudezahl in Hessen konnten in Bezug auf die Daten aus dem Energie-Rahmenbedingungen die Durchdringungen der jeweiligen untersuchten Prosumer-Technologien in Prozent ermittelt werden. Photovoltaik-Aufdachanlagen stellen aktuell noch die älteste laborrelevante Technologie im Vergleich zu den anderen Technologien (Wärmepumpe, Batteriespeicher, etc.) dar und sind deshalb auch stärker im derzeitigen Gebäudebestand vertreten. Batteriespeicher werden erst seit ein paar Jahren verstärkt eingesetzt, um solare Strahlungsenergie privat nutzbar zu machen. Aus diesem Grund sind diese im Gesamtbestand für das Szenario-Jahr 2020 noch kaum vertreten. Ebenso verhalten sich private Ladestationen, die erst seit 2020 vermehrt nachgefragt werden und deshalb im Gesamtbestand der Wohngebäude noch eine verschwindend geringe Durchdringung aufweisen. Für Wärmepumpen liegen keine aussagekräftigen Datensätze vor, weshalb, in Anlehnung an die oben aufgeführte BDEW-Studie zum Heizungsmarkt in Hessen, eine durchschnittliche Durchdringung von fünf Prozent für alle Topologien angenommen wird.

Das Osterpaket sieht vor, die Rahmenbedingungen für den Ausbau privater Photovoltaik-Dachanlagen zukünftig zu verbessern und Studien, wie die hessische Verteilnetzstudie, sehen ein großes, derzeit noch ungenutztes, Potential auf Hausdächern. Ein deutlicher Zuwachs wird deshalb für das Szenario-Jahr 2030 in allen Topologien angenommen. Auch wenn die jüngsten Zubau-Zahlen im Marktstammdatenregister einen stärkeren Zuwachs in den städtischen Topologien erkennen lassen, wurde für die ländlichen Gebiete im Gesamtbestand weiterhin eine höhere Durchdringung angenommen. Während dort der Ausbau einfacher umsetzbar ist, begründet durch klare Eigentumsverhältnisse bei Ein- und Zweifamilienhäusern und leichter nutzbare Flächen, bremsen Mietverhältnisse, Verschattungen und eine stärkere Flächenkonkurrenz den Ausbau in der Stadt Topologie [64]. Die Kombination einer PV-Anlage und einem Batteriespeicher kommt in allen Topologien stärker zum Einsatz. Die bereits aufgeführte dena-Studie gibt einen Zusammenhang zwischen der Kaufkraft in Landkreisen und der Entwicklung der Elektromobilität an. Kurzfristig wird deshalb ein Zuwachs der Elektromobilität vor allem in den finanziell stärker aufgestellten städtischen Gemeinden angenommen. In der Stadttopologie wird der Ausbau an privaten Ladestationen allerdings stark eingeschränkt, aufgrund der mangelnden privaten Stellplätze.

Im Jahr der Klimaneutralität 2045 wurde angenommen, dass die Durchdringung von PV-Dachanlagen in den Dorf- und Vorstadt-Topologien am höchsten ist. Dort ist der Anteil an Ein- und Zweifamilienhäusern sehr hoch, da aufgrund der geringen Verschattungen und Dachflächen PV-Anlagen optimal zur Stromerzeugung genutzt werden können. Die einkommensschwächeren Landkreise, die der Topologie Land zugeordnet wurden, fallen etwas zurück. Die Stadt-Topologie weist die geringste Durchdringung auf, begründet durch Mehrparteienhäuser, Verschattungen durch dichtere Bebauung und Flächenkonkurrenz. Jede zweite PV-Dachanlage wird in diesem Szenario in Kombination mit einem Batteriespeicher betrieben. Der Durchdringungstrend für private Ladestationen aus dem oben beschriebenen Szenario-Jahr 2030 wurde auch für das Jahr 2045 fortgesetzt und elektrische Wärmepumpen kommen im Gesamtbestand der Wohngebäude vermehrt zum Einsatz.

Um die Auswirkungen zu analysieren, die ein Vollausbau der Prosumer in allen Topologien nach sich ziehen könnte, wurde abschließend das Neubau-Szenario erstellt. Hier verfügt jedes der simulierten Labor-Gebäude über alle untersuchten Technologien.

Land

Tabelle 8: Durchdringungen in den Topologien Land.

Technologie	2020	2030	2045	Vollausbau
PV	10,00%	32,00%	40,00%	100%
Batteriespeicher	1,00%	10,70%	20,00%	100%
Wärmepumpe	5,00%	10,00%	40,00%	100%
Ladestation	0,90%	14,00%	28,00%	100%

Dorf

Tabelle 9: Durchdringungen in den Topologien Dorf.

Technologie	2020	2030	2045	Vollausbau
PV	8,40%	28,00%	50,00%	100%
Batteriespeicher	1,00%	9,30%	25,00%	100%
Wärmepumpe	5,00%	10,00%	40,00%	100%
Ladestation	1,30%	24,00%	55,00%	100%

Vorstadt

Tabelle 10: Durchdringungen in den Topologien Vorstadt.

Technologie	2020	2030	2045	Vollausbau
PV	6,70%	24,00%	45,00%	100%
Batteriespeicher	0,90%	8,00%	22,50%	100%
Wärmepumpe	5,00%	10,00%	40,00%	100%
Ladestation	1,20%	26,00%	60,00%	100%

Stadt

Tabelle 11: Durchdringungen in den Topologien Stadt.

Technologie	2020	2030	2045	Vollausbau
PV	3,80%	21,00%	33,00%	100%
Batteriespeicher	0,60%	7,00%	16,50%	100%
Wärmepumpe	5,00%	10,00%	40,00%	100%
Ladestation	0,40%	12,00%	30,00%	100%

3.6.3. Leistungen

Die durchschnittlichen Leistungen der PV-Anlagen und die der Batteriespeicher, sowie deren Kapazität, wurden durch die Einträge im Marktstammdatenregister ermittelt. Während die Größen der Batteriespeicher relativ unabhängig von der jeweiligen Topologie sind, ist zu erkennen, dass in den Leistungsklassen der PV-Anlagen in ländlichen Gebieten größer dimensioniert werden. Dort werden aufgrund größerer Dachflächen, weniger Verschattungen und weniger Flächenkonkurrenz größere Module eingesetzt, als in den städtischen Gebieten. Außerdem ist die noch bis 2021 geltende EEG-Umlagenpflicht für Anlagen über 10 kWp deutlich als Leistungsgrenze in den installierten Leistungen pro Modul zu erkennen. Als Leistungen für private Ladestationen wurden die derzeit für Wallboxen üblichen 11 kW angenommen. Private Ladestationen fassen installierte Wallboxen und E-Fahrzeuge zusammen. Dies liegt daran, dass ein E-Fahrzeug auch ohne Wallbox geladen werden kann. Des

Weiteren sind E-Fahrzeuge nicht ausschließlich an einen Anschluss gebunden. Für das Erstellen der Szenarien sind jedoch die Leistungsflüsse an den einzelnen Punkten interessant. Für den ersten Aufschlag wird angenommen, dass nur ein Ladepunkt pro Gebäude existiert. An diesem können mehrere Ladevorgänge nacheinander stattfinden.

Durch den Abbau regulatorischer Hürden in der jüngsten EEG-Novelle für Dachanlagen bis 30 kW, lässt sich eine Verschiebung der Leistungen pro installierte Anlage deutlich über die 10 kWp Grenze erkennen. Dadurch könnten auch zukünftig Dachflächen vollständiger ausgenutzt werden, was sich positiv auf die durchschnittlich installierten Leistungen pro Anlage auswirkt. Allerdings setzen die kleineren Bestandsanlagen den Durchschnittswert herab. Leistungssteigerungen durch neuartige Technologien wurden in den Szenarien nicht berücksichtigt. Durch die Vergrößerung der Quelle wurden in diesem Zusammenhang auch die Speicher in allen Topologien größer dimensioniert. Größere Speicher sind jedoch nicht zwingend sinnvoll, wenn der Verbrauch zu niedrig ist. Die Wirtschaftlichkeit des Speichers nimmt mit einer Überdimensionierung ab. Für die Ladestationen wurden weiterhin 11 kW angenommen.

Vor allem die Kombination der neuen Verbraucher, wie der elektrischen Wärmepumpe und der privaten Ladestation für Elektroautos und einer eigenen PV-Dachanlage wurde bei der Erstellung der Szenarien als vorteilhaft angesehen. Die Stromgestehungskosten von Photovoltaikanlagen liegen deutlich unter den Preisen der Stromtarife für Privatkunden [65], weshalb bei einem erhöhten Bedarf an elektrischer Energie PV-Anlagen die Kosten senken. Gleichzeitig profitieren Betreiberinnen und Betreiber dieser Anlagen durch den Eigenverbrauch. Deshalb steigen in allen Szenarien die durchschnittlichen Leistungen der PV-Dachanlagen und in diesem Zusammenhang auch die Speichergrößen.

Land

Tabelle 12: Leistungswerte für Land Topologien.

Technologie	2020	2030	2045	Vollausbau
PV [kW]	8,1	8,6	9,5	9,5
Batterie				
Leistung [kW]	4,4	5,3	7	7
Energie [kWh]	7	7	7,2	8
Heizlast				
EFH [kW]	12	12	12	12
ZFH [kW]	20	20	20	20
MFH [kW/HH]	10	10	10	10
Ladestation [kW]	11	11	11	11

Dorf

Tabelle 13: Leistungswerte für Land Topologien.

Technologie	2020	2030	2045	Vollausbau
PV [kW]	7,5	8,4	9,2	9,2
Batterie				
Leistung [kW]	4,4	5,3	7,2	7,2
Energie [kWh]	7	7,2	7,5	8,5

Heizlast				
EFH [kW]	12	12	12	12
ZFH [kW]	20	20	20	20
MFH [kW/HH]	10	10	10	10
Ladestation [kW]	11	11	11	11

Vorstadt

Tabelle 14: Leistungswerte für Land Topologien.

Technologie	2020	2030	2045	Vollausbau
PV [kW]	7	7,9	8,5	8,5
Batterie				
Leistung [kW]	4,3	5,1	7,5	7,5
Energie [kWh]	7	7,5	8,7	9
Heizlast				
EFH [kW]	12	12	12	12
ZFH [kW]	20	20	20	20
MFH [kW/HH]	10	10	10	10
Ladestation [kW]	11	11	11	11

Stadt

Tabelle 15: Leistungswerte für Land Topologien.

Technologie	2020	2030	2045	Vollausbau
PV [kW]	6,8	7,3	8	8
Batterie				
Leistung [kW]	4,3	5	7	7
Energie [kWh]	7	7,5	9	9
Heizlast				
EFH [kW]	12	12	12	12
ZFH [kW]	20	20	20	20
MFH [kW/HH]	10	10	10	10
Ladestation [kW]	11	11	11	11

3.6.4. Technologien in den Topologien

Aus den Energierahmendaten konnten die Durchdringungen ermittelt werden, die sich schließlich bis auf den simulierten Hausanschluss der einzelnen Gebäude herunterrechnen lässt. Die Anteile der EFH, ZFH und MFH Gebäude pro Topologie wurden aus der Hessischen Gemeindestatistik 2021 ermittelt und bleiben für die Szenario-Jahre unverändert. Anhand der Durchdringungen können die einzelnen Technologien anteilig für die einzelnen Topologien und Jahre berechnet werden, wobei ganzzahlig gerundet wurde. Niedrige Durchdringungen machen sich bei einer kleinen Gebäudeanzahl wie bei den Land-Topologien anfangs noch kaum bemerkbar.

Land 1

Tabelle 16: Anschlussverteilung von Land 1.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
Anschlüsse	3	1					1	1	
Gebäude	3	1					1	1	
EFH	3	1					1	1	
ZFH									
MFH									

2020

Tabelle 17: Komponentenverteilung von 2020 – Land 1.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module									
Batteriespeicher									
Wärmepumpen									
Ladestationen									

2030

Tabelle 18: Komponentenverteilung von 2030 – Land 1.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	1							1	
Batteriespeicher									
Wärmepumpen									
Ladestationen									

2045

Tabelle 19: Komponentenverteilung von 2045 – Land 1.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	1							1	
Batteriespeicher	1							1	
Wärmepumpen	1						1		
Ladestationen	1	1							

Vollausbau

Tabelle 20: Komponentenverteilung von Vollausbau – Land 1.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	3	1					1	1	
Batteriespeicher	3	1					1	1	
Wärmepumpen	3	1					1	1	
Ladestationen	3	1					1	1	

Land 2

Tabelle 21: Anschlussverteilung von Land 2.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
Anschlüsse	4					1	1	1	1
Gebäude	4					1	1	1	1
EFH	4					1	1	1	1
ZFH									
MFH									

2020

Tabelle 22: Komponentenverteilung von 2020 – Land 2.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module									
Batteriespeicher									
Wärmepumpen									
Ladestationen									

2030

Tabelle 23: Komponentenverteilung von 2030 – Land 2.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	1					1			
Batteriespeicher									
Wärmepumpen									
Ladestationen	1					1			

2045

Tabelle 24: Komponentenverteilung von 2045 – Land 2.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	2					1	1		
Batteriespeicher	1						1		
Wärmepumpen	2					1	1		
Ladestationen	1						1		

Vollausbau

Tabelle 25: Komponentenverteilung von Vollausbau – Land 2.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	4					1	1	1	1
Batteriespeicher	4					1	1	1	1
Wärmepumpen	4					1	1	1	1
Ladestationen	4					1	1	1	1

Dorf 1

Tabelle 26: Anschlussverteilung von Dorf 1.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
Anschlüsse	22	1	1	3	1	1	7	4	4
Gebäude	18	1	1	2	1	1	5	4	3
EFH	15	1	1	1	1	1	4	4	2
ZFH	2			1					1
MFH	1						1		

2020

Tabelle 27: Komponentenverteilung von 2020 – Dorf 1.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	2						1		1
Batteriespeicher									
Wärmepumpen	1						1		
Ladestationen									

2030

Tabelle 28: Komponentenverteilung von 2030 – Dorf 1.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	5	1		1		1	1		1
Batteriespeicher	2	1				1			
Wärmepumpen	2	1		1			1		
Ladestationen	4	1				1	1		1

2045

Tabelle 29: Komponentenverteilung von 2045 – Dorf 1.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	9	1		2	1	1	1	2	1
Batteriespeicher	5	1		1	1	1		1	
Wärmepumpen	7	1	1	1	1	1	1	1	
Ladestationen	10	1	1	1		1	2	2	2

Vollausbau

Tabelle 30: Komponentenverteilung von Vollausbau – Dorf 1.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	18	1	1	2	1	1	5	4	3
Batteriespeicher	18	1	1	2	1	1	5	4	3
Wärmepumpen	18	1	1	2	1	1	5	4	3
Ladestationen	18	1	1	2	1	1	5	4	3

Dorf 2

Tabelle 31: Anschlussverteilung von Dorf 2.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
Anschlüsse	22	1	2			1	7	7	4
Gebäude	17	1	2			1	3	6	4
EFH	14	1	2			1	1	5	4
ZFH	2						1	1	

2020

Tabelle 32: Komponentenverteilung von 2020 – Dorf 2.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	1		1						
Batteriespeicher									
Wärmepumpen	1		1						
Ladestationen									

2030

Tabelle 33: Komponentenverteilung von 2030 – Dorf 2.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	4	1	1			1	1		
Batteriespeicher	1	1							
Wärmepumpen	2		1			1			
Ladestationen	4	1	1			1	1		

2045

Tabelle 34: Komponentenverteilung von 2045 – Dorf 2.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	8	1	1			1	2	2	1
Batteriespeicher	4	1					1	1	1
Wärmepumpen	6		1			1	2	1	1
Ladestationen	9	1	1			1	2	2	2

Vollausbau

Tabelle 35: Komponentenverteilung von Vollausbau – Dorf 2.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	17	1	2			1	3	6	4
Batteriespeicher	17	1	2			1	3	6	4
Wärmepumpen	17	1	2			1	3	6	4
Ladestationen	17	1	2			1	3	6	4

Vorstadt 1

Tabelle 36: Anschlussverteilung von Vorstadt 1.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
Anschlüsse	25	3	2			3	6	5	6
Gebäude	19	2	2			2	2	5	6
EFH	15	1	2			1		5	6
ZFH	3	1				1	1		
MFH	1						1		

2020

Tabelle 37: Komponentenverteilung von 2020 – Vorstadt 1.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	1		1						
Batteriespeicher									
Wärmepumpen	1		1						
Ladestationen									

2030

Tabelle 38: Komponentenverteilung von 2030 – Vorstadt 1.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	5		2			1	1		1
Batteriespeicher	2		1				1		
Wärmepumpen	2		1				1		
Ladestationen	5		2			1	1		1

2045

Tabelle 39: Komponentenverteilung von 2045 – Vorstadt 1.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	9	1	2			1	1	2	2
Batteriespeicher	4		1			1	1	1	
Wärmepumpen	8	1	2			1	1	2	1
Ladestationen	11	2	2			1	1	2	3

Vollausbau

Tabelle 40: Komponentenverteilung von Vollausbau – Vorstadt 1.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	19	2	2			2	2	5	6
Batteriespeicher	19	2	2			2	2	5	6
Wärmepumpen	19	2	2			2	2	5	6
Ladestationen	19	2	2			2	2	5	6

Vorstadt 2

Tabelle 41: Anschlussverteilung von Vorstadt 2.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
Anschlüsse	25	6	2	2	2	2	2	4	5
Gebäude	19	5	2	2	2	2	2	3	1
EFH	16	4	2	2	2	2	2	2	
ZFH	2	1						1	
MFH	1								1

2020

Tabelle 42: Komponentenverteilung von 2020 – Vorstadt 2.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	1			1					
Batteriespeicher									
Wärmepumpen	1			1					
Ladestationen									

2030

Tabelle 43: Komponentenverteilung von 2030 – Vorstadt 2.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	5	1	1	1		1		1	
Batteriespeicher	2	1						1	
Wärmepumpen	2	1		1					
Ladestationen	5	1	1	1		1		1	

2045

Tabelle 44: Komponentenverteilung von 2045 – Vorstadt 2.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	9	2	1	1	1	1	1	2	
Batteriespeicher	4	1	1		1			1	
Wärmepumpen	8	1	1	1	1	1	1	1	1
Ladestationen	11	2	1	1	2	1	1	2	1

Vollausbau

Tabelle 45: Komponentenverteilung von Vollausbau – Vorstadt 2.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	19	5	2	2	2	2	2	3	1
Batteriespeicher	19	5	2	2	2	2	2	3	1
Wärmepumpen	19	5	2	2	2	2	2	3	1
Ladestationen	19	5	2	2	2	2	2	3	1

Stadt

Tabelle 46: Anschlussverteilung von Stadt.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
Anschlüsse	40	4	2	2	4	6	3	12	7
Gebäude	10	1	2	1	1	1	1	2	1
EFH	2		2						
ZFH	2			1				1	
MFH	6	1			1	1	1	1	1

2020

Tabelle 47: Komponentenverteilung von 2020 – Stadt.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	1				1				
Batteriespeicher									
Wärmepumpen	1				1				
Ladestationen									

2030

Tabelle 48: Komponentenverteilung von 2030 – Stadt.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	3			1	1			1	
Batteriespeicher	1			1					
Wärmepumpen	1				1				
Ladestationen	2			1				1	

2045

Tabelle 49: Komponentenverteilung von 2045 – Stadt.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	4		1	1	1			1	
Batteriespeicher	2		1	1					
Wärmepumpen	5		1	1	2			1	
Ladestationen	4		1	1	1			1	

Vollausbau

Tabelle 50: Komponentenverteilung von Vollausbau – Stadt.

Einheit	Anzahl	NA 1	NA 2	NA 3	NA 4	NA 5	NA 6	NA 7	NA 8
PV-Module	13	1	2	1	4	1	1	2	1
Batteriespeicher	13	1	2	1	4	1	1	2	1
Wärmepumpen	13	1	2	1	4	1	1	2	1
Ladestationen	13	1	2	1	4	1	1	2	1

3.6.5. Einstellungen für das Labor

Abschließend wurden alle vorangegangenen Schritte zusammengefasst, um die Einstellungen für das Labor festzulegen. Die folgenden Tabellen enthalten alle simulierten Gebäude mitsamt den Prosumer-Komponenten. Zwei- und Mehrfamilienhäuser werden durch eine Zusammenfassung mehrerer Anschlüsse dargestellt. Die eingestellten Leistungen für PV-Anlagen und Batterien wurden normalverteilt, zufällig um die jeweiligen Durchschnittswerte erstellt. Als durchschnittliche Heizlast für Einfamilienhäuser wurden 12 kW angenommen, wobei auch hier die eingestellten Werte zufällig normalverteilt um den Mittelwert liegen. Für Zwei- und Mehrfamilienhäuser wurde pro Haushalt eine durchschnittliche Heizlast von 10 kW angenommen. In den Simulationen werden hauptsächlich elektrische Luftwärmepumpen berücksichtigt, die eine Jahresarbeitszahl im Durchschnitt von drei charakterisiert. Die elektrische Last berechnet sich schließlich aus der Heizlast geteilt durch die Jahresarbeitszahl.

Die Tabellen mit den genauen Einstellungen sind dem Anhang zu entnehmen, als Beispiel ist folgend Dorf 1 2045.

Tabelle 51: finale Parameter für Lastkurven zu 2045 - Dorf 1.

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	1	EFH1.1	6	1,4	8,2	5,6	7	13	3,1	11
NA 1 - gesamt		1								
NA 2	1	EFH2.1	2	4,5	9,1	7	7,6	11	3,5	11
NA 2 - gesamt	1	1								
NA 3	1	EFH3.1	61	4,57						
NA 3	2	ZFH3.2.1	8	5,18	8,4	7	7,8	18	3	11
NA 3		ZFH3.2.2	5	3,2						
NA 3 - gesamt	3	2								
NA 4	1	EFH4.1	66	3,62						
NA 4 - gesamt	1	1								
NA 5	1	EFH5.1	22	4,04	8,3	7	7,5	14	3,3	11
NA 5 - gesamt	1	1								
NA 6	1	EFH6.2	16	3,2						
NA 6	1	EFH6.3	73	4,34	6,9			12	3	11
NA 6	1	EFH6.4	39	5,17						

NA 6	1	EFH6.5	55	4,78	8,8					11
NA 6	3	MFH6.1.1	1	3,24						
NA 6		MFH6.1.2	23	7,5						
NA 6		MFH6.1.3	32	5,32						
NA 6 - gesamt	7	5								
NA 7	1	EFH7.1	74	4,27						11
NA 7	1	EFH7.2	22	4,04						
NA 7	1	EFH7.3	7	2,94						
NA 7	1	EFH7.4	31	5,01	9,2	7,2	7,7	13	3,5	11
NA 7 - gesamt	4	4								
NA 8	1	EFH8.1	3	6,62	9,3					
NA 8	1	EFH8.2	19	5,49	7,5			12,8	3	11
NA 8	2	ZFH8.3.1	71	4,32						11
NA 8		ZFH8.3.2	41	5,52						
NA 8 - gesamt	4	3								

4. Ergebnisse des Labors

Die Interpretation der Messwerte ist hauptsächlich von zwei Größen abhängig, der Spannung und des Stromes.

Die Grenzwerte für Spannung werden durch die DIN EN 50160 mit der langsamen Spannungsänderung 230 V ± 10 % definiert. Da das Toleranzband jedoch nicht nur für die Niederspannung gilt, sondern schon in der Mittelspannung anfängt (siehe Abbildung 53), wurden die Ober- und Untergrenze verringert. Diese liegen dann bei -5 % und +3 %.

Der Strom wird durch die Stromtragfähigkeit des Kabels vorgegeben. Das Labor ist auf Grundlage von Kabeln des Typs NAYY 240 mm² aufgebaut, weshalb der dafür übliche Grenzwert (364 A) genutzt wird.

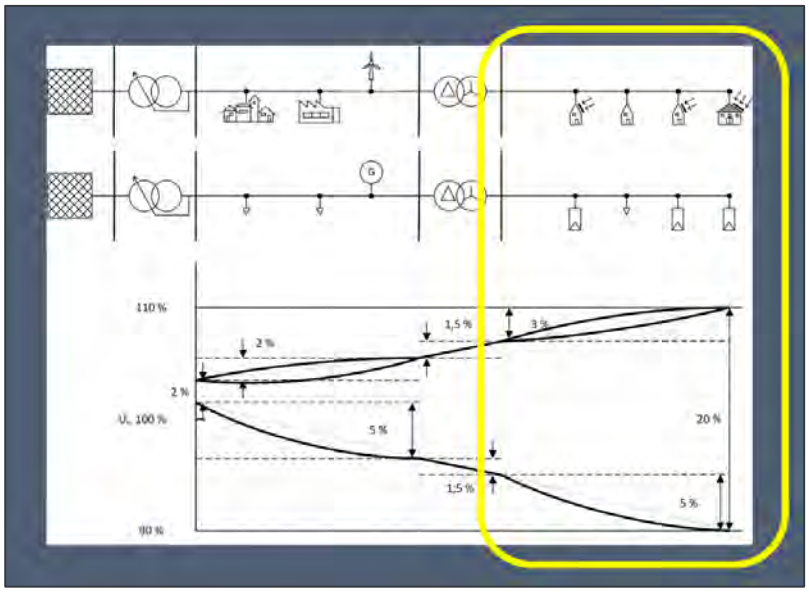


Abbildung 53: zu betrachtendes Spannungsband im Niederspannungsnetz nach [74].

4.1 Beispiel

Die folgenden Abbildungen wurden aus den Messwerten eines Versuches erstellt. Die farblich markierten Bereiche signalisieren die Grenzwerte.

Die gezeigte Messreihe beschreibt den Versuch Vollausbau mit einer Gleichzeitigkeit der ladenden E-Fahrzeuge von 1 über 4 h in der Topologie Dorf 1 an einem Wintertag (22. Dezember -> Wochentag). Dies entspricht einer Ladeenergie von 44 kWh, was wiederum für eine ungefähre Fahrleistung von fast 250 km bei einem Verbrauch von 18 kWh/100 km. In der Auswertung wird als Kabel das NAYY 240 mm² genommen.

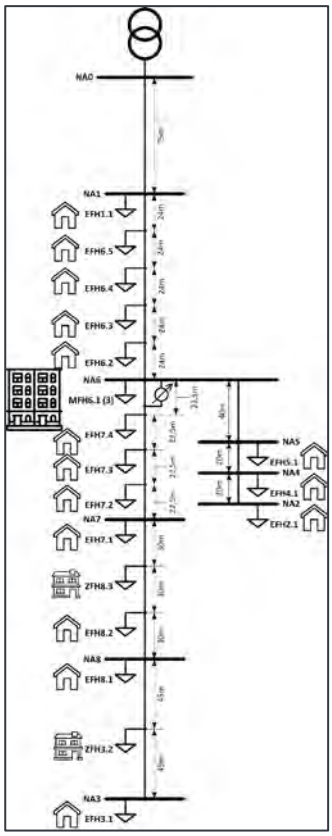


Abbildung 54: Topologie Dorf 1.

Spannungen

In diesem Szenario kommt es zu keiner Spannungsbandverletzung. Über die meiste Zeit ist der maximale Spannungsabfall nicht höher als 2 %. Erst wenn um 18 Uhr alle Ladesäulen in Betrieb gehen, steigt der Spannungsabfall auf etwa 4,5 % an. Dieser liegt knapp unter der Grenze von 5 % und ist als kritisch zu betrachten, ohne dass es zu einer Verletzung kommt.

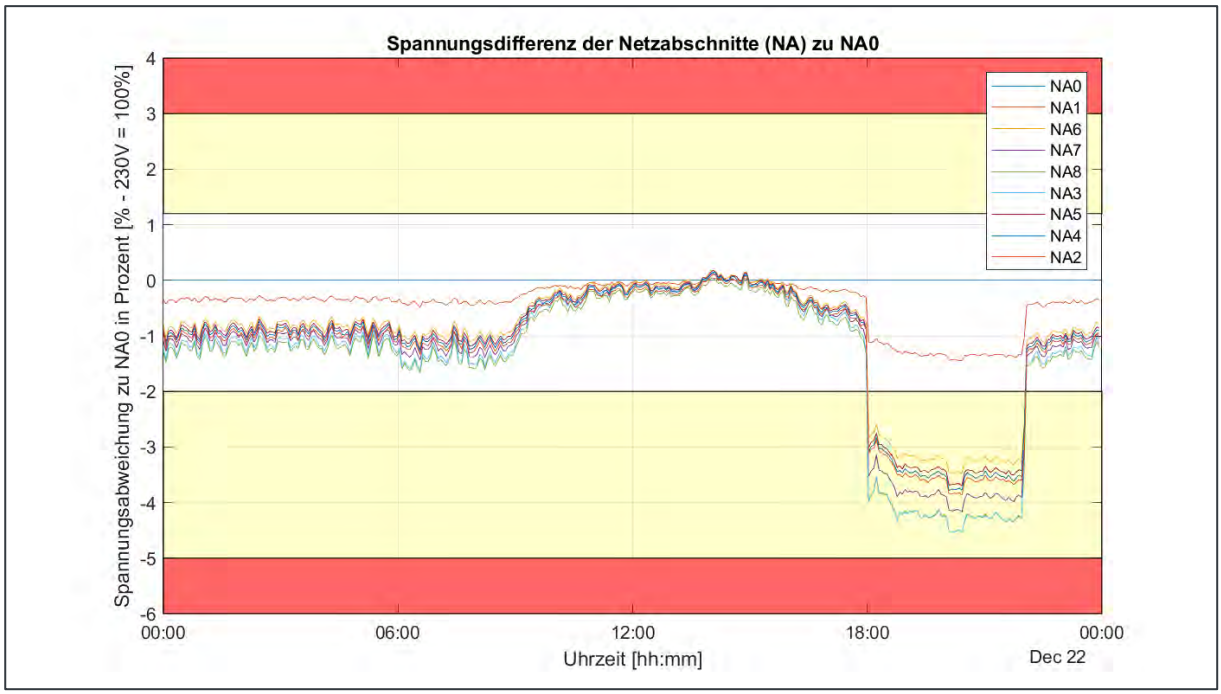


Abbildung 55: Auswertung des Beispiels - Spannungsdifferenzverlauf zu NA0.

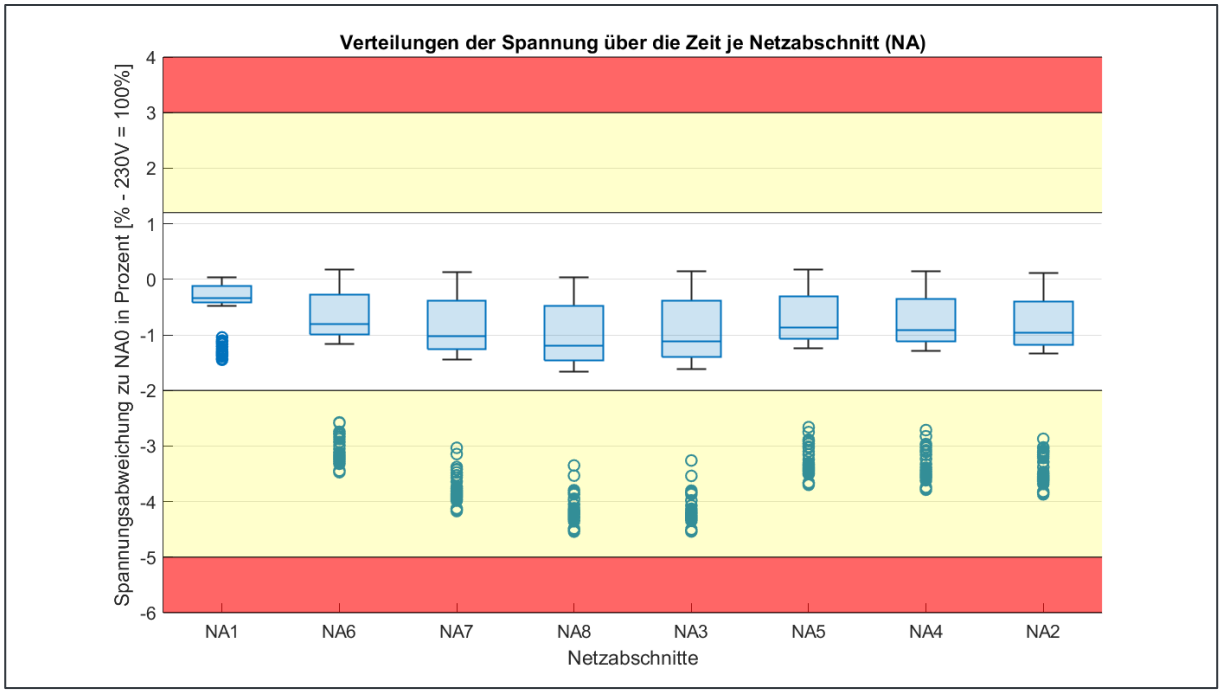


Abbildung 56: Auswertung des Beispiels - Verteilungen der Spannung über die Zeit je Netzabschnitt.

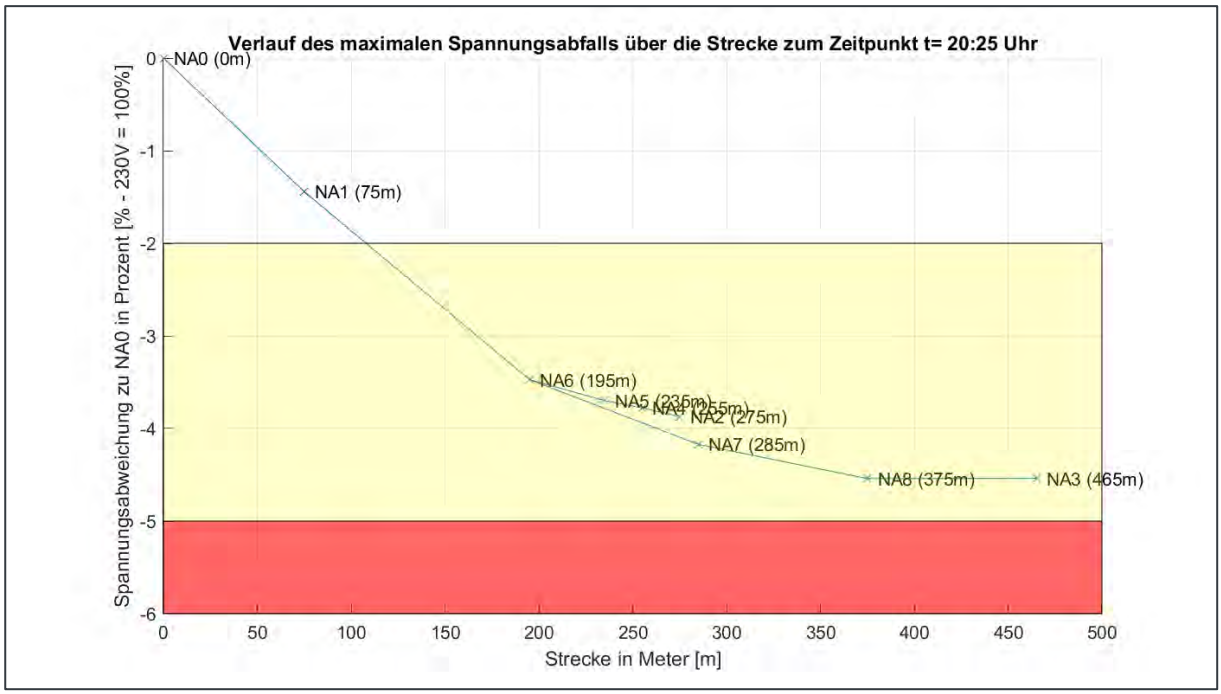


Abbildung 57: Auswertung des Beispiels - Verlauf des maximalen Spannungsabfalls über die Strecke.

Ströme

Bei den Strömen kommt es jedoch zu einer Überschreitung der Grenzwerte, wenn die Fahrzeuge laden. In der Realität müsste die Sicherung in der Ortsnetzstation einschreiten.

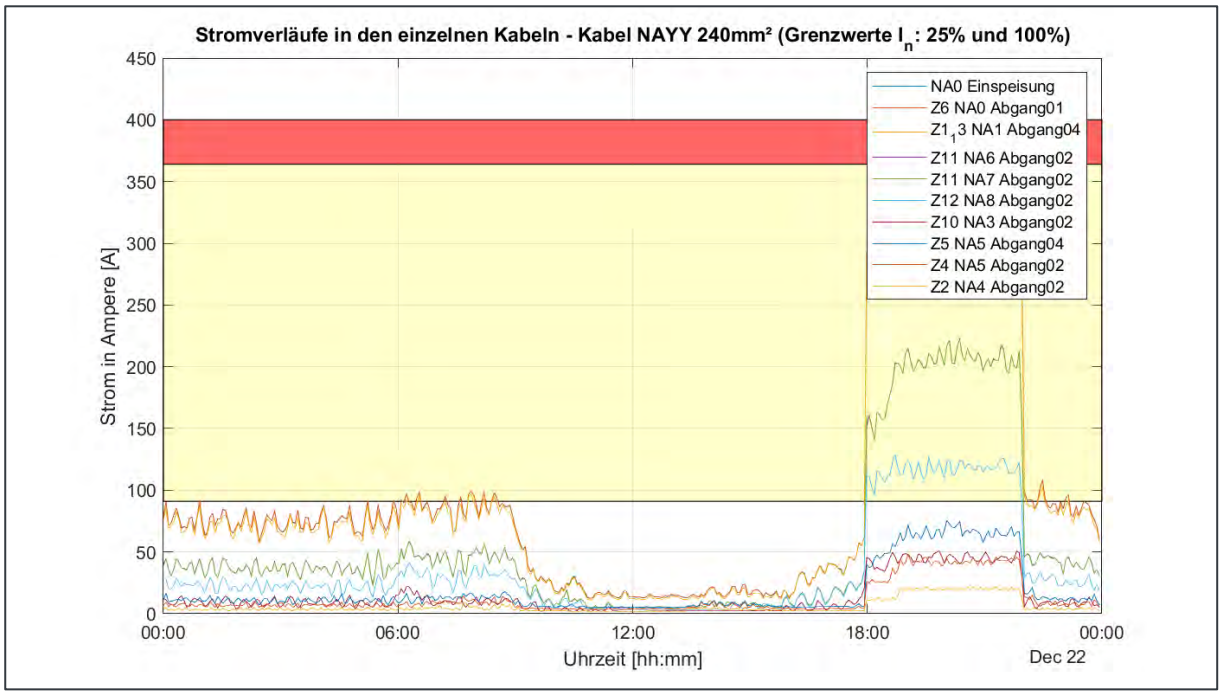


Abbildung 58: Auswertung des Beispiels - Stromverläufe in den einzelnen Kabeln.

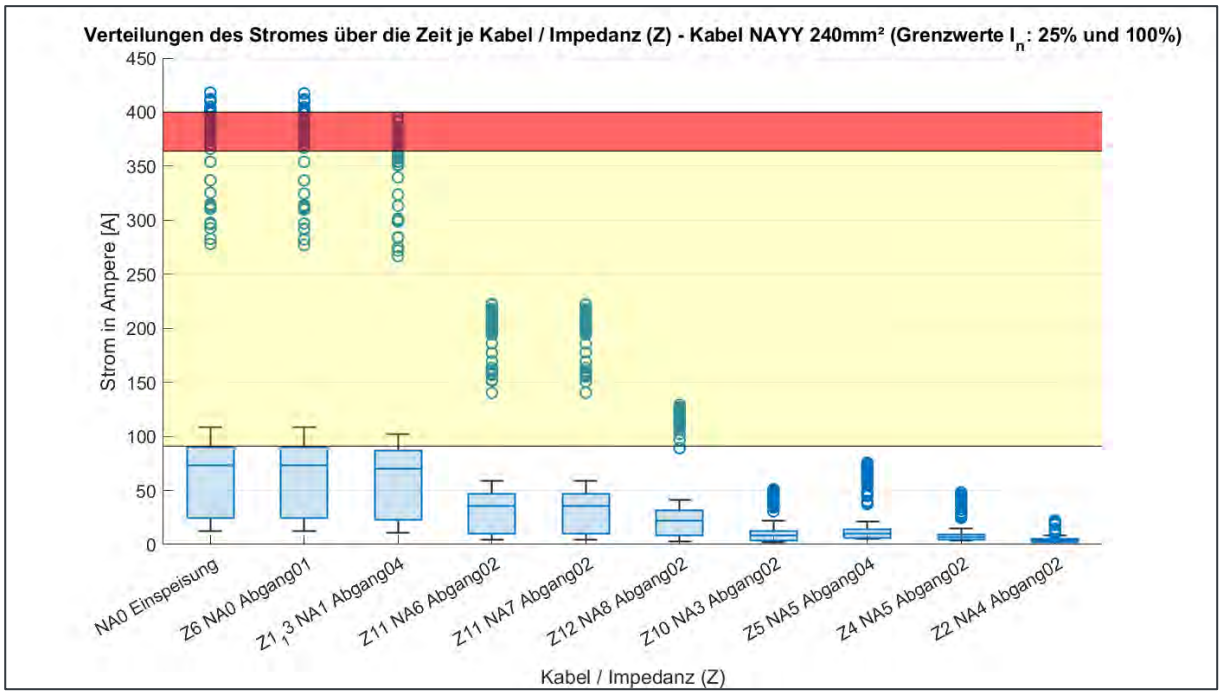


Abbildung 59: Auswertung des Beispiels - Verteilungen des Stromes über die Zeit je Kabel.

4.1.1. Lösungsansatz

Ein Lösungsansatz ist, die E-Ladesäulen abzuregeln. Die beiden folgenden Abbildungen zeigen die gleiche Ausgangssituation wie im Beispiel, jedoch wurden die Ladesäulen auf 50 % abgeregelt, was wiederum zu einer doppelt so langen Ladezeit führt. Der maximale Spannungsabfall sinkt um ca. 1 % und der Strom bleibt auch deutlich unterhalb des Grenzwertes.

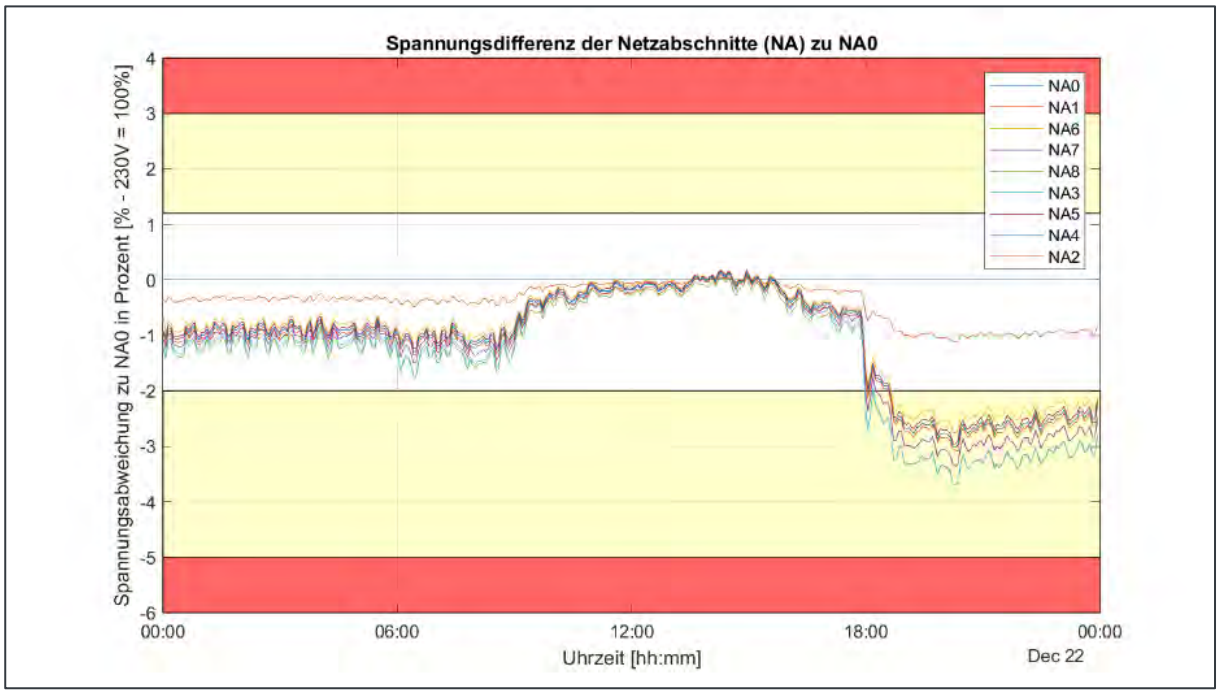


Abbildung 60: Auswertung des Lösungsansatzes - Spannungsdifferenzverlauf zu NA0.

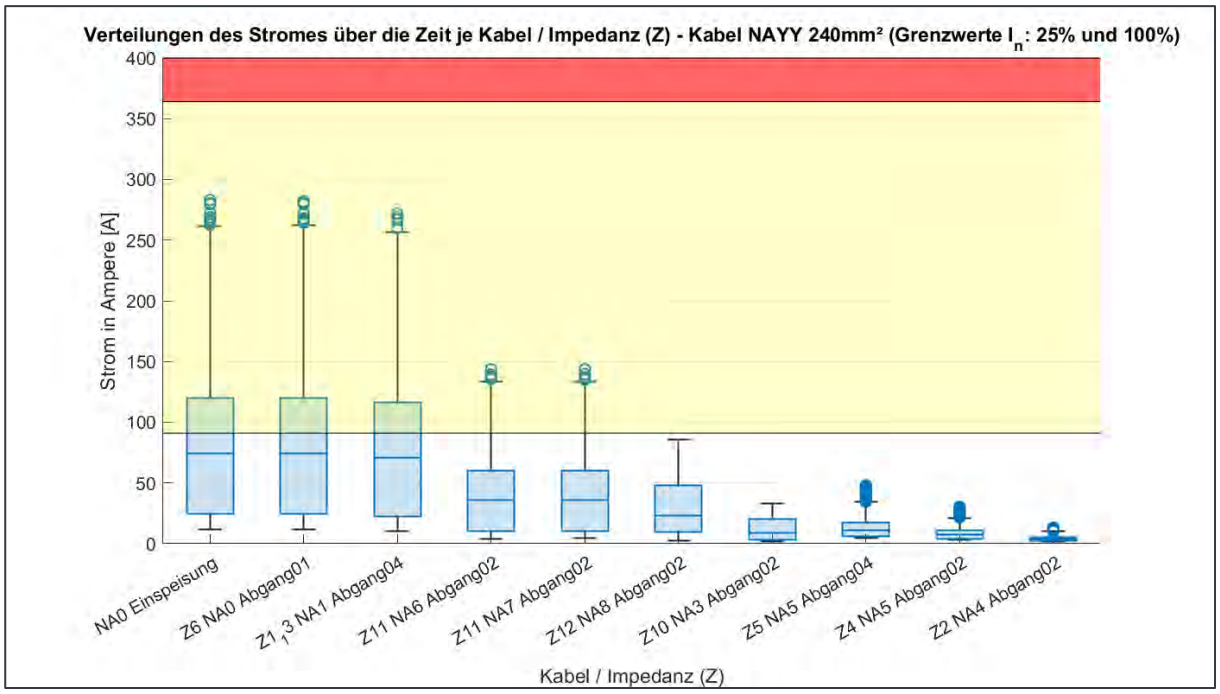


Abbildung 61: Auswertung des Lösungsansatzes - Verteilungen des Stromes über die Zeit je Kabel.

4.2 Schlussfolgerung

Die Lastkurven je Haushalt werden durch die neuen Technologien maßgeblich verändert. Durch die Entwicklung und den Ausbau von Prosumern wird eindeutig, dass die Standardlastkurven der Vergangenheit angehören. Prosumer werden das Niederspannungsnetz massiv belasten. Wie in dem Beispiel gezeigt kommt es selbst mit einem sehr starken konventionellen Netzausbau zu Überlastungen der Kabelanlagen und weiteren Betriebsmitteln. Mit steigender Durchdringung der Sektorenkopplung, steigt in den Netzen auch die Anzahl der Netzengpässe. Dies betrifft nicht nur die Bestandsnetze, sondern in Extremfällen auch die konventionell ausgebauten Niederspannungsnetze.

Ein weiterer Betrachtungspunkt sind die Oberschwingungen. Im Labor wird größtenteils mit marktüblichen Wechselrichtern gearbeitet, weshalb die Zunahme der Oberschwingungen in den Szenarien nicht sinnvoll untersucht werden konnte. Beim zukünftigen Netzausbau sind diese Größen jedoch mit zu berücksichtigen. Bereits existierende Messgeräte können teilweise Oberschwingungsanteile messen und daraus könnten Ableitungen für die Netzführung erstellt werden.

5. Datensicherheit, Angriffsvektoren und Verteidigungsstrategie

Smart Grids, auch als intelligente Stromnetze bezeichnet, haben das Potenzial, die Energie-effizienz und -nachhaltigkeit erheblich zu verbessern, indem sie die Integration erneuerbarer Energiequellen und die Steuerung des Energieverbrauchs ermöglichen. Die Umsetzung von Smart Grids stellt jedoch auch große Herausforderungen dar, insbesondere im Bereich der Sicherheit. Smart Grids können Cyberangriffen mit physischen Konsequenzen ausgesetzt sein, was die an sie zu stellenden Sicherheitsanforderungen erhöht.

Die Sicherheitsanforderungen für Smart Grids sind ähnlich wie bei anderen Systemen, z. B. Vertraulichkeit, Integrität und Verfügbarkeit von Daten. Doch Cyberangriffe auf Smart Grids zielen hauptsächlich darauf ab, den Betrieb der physischen Stromerzeugungs-, Übertragungs- und Verteilungssysteme zu stören, indem sie den zugrunde liegenden Cyber-Layer ausnutzen. Dies führt zu einem komplexen Problem, da neben physischen auch dynamischen Bedrohungen existieren. Um die Sicherheit von komplexen Infrastrukturen wie Smart Grids zu gewähr-leisten, ist ein Ansatz erforderlich, der die Bereiche Cyber-Sicherheit und Systemtheorie kom-biniert. Denn Cyberangriffe können nicht nur die digitale Welt beeinflussen, sondern auch Auswirkungen auf die physische Welt haben. Daher müssen sowohl die Cyber- als auch die physischen Komponenten von Smart Grids angemessen geschützt werden.

Die Sicherheit von Smart Grids ist sehr wichtig, da diese Systeme die Energieversorgung in Städten und Gemeinden gewährleisten. Wenn es zu einer erfolgreichen Cyber-Attacke auf Smart Grids kommen würde, könnte dies schwerwiegende Auswirkungen auf die Energieversorgung und die öffentliche Sicherheit haben. Es ist daher unerlässlich, dass Smart Grids mit ausreichenden Sicherheitsmaßnahmen ausgestattet werden, um sowohl die Stromversorgung als auch die öffentliche Sicherheit zu gewährleisten.

Weiterführende Literatur:

- L. Kotut and L. A. Wahsheh, "Survey of Cyber Security Challenges and Solutions in Smart Grids", in 2016 Cybersecurity Symposium (CYBERSEC), pp. 32–37, Apr.2016.
- O. Otuoze, M. W. Mustafa, and R. M. Larik, "Smart grids security challenges: Classification by sources of threats"
- R. K. Pandey and M. Misra, "Cyber Security Threats- Smart Grid Infrastructure" in 2016 National Power Systems Conference (NPSC), pp. 1–6, Dec. 2016.

5.1 Standardisierung

Es ist wichtig, die Sicherheit des intelligenten Stromnetzes zu verbessern, indem man sich nicht nur auf IT-Systeme konzentriert, sondern auch auf die Integration von physischen Geräten und Ressourcen. Es muss ein Gleichgewicht zwischen Elektrizitäts- und Cyber-Systemtechnologien gefunden werden, um die Zuverlässigkeit und Sicherheit des intelligenten Stromnetzes und die Privatsphäre von Verbrauchern zu schützen. Es ist auch wichtig, dass Praktiken aus anderen Sektoren wie IT oder Kommunikation nur eingeschränkt auf den Elektrizitätssektor angewendet werden können, da sie die Zuverlässigkeit beeinträchtigen können. Der historische Fokus des Elektrizitätssektors lag auf der

Implementierung von Geräten, die die Zuverlässigkeit des Stromsystems verbessern können, aber die Kommunikations- und IT-Sektoren sind immer wichtiger geworden. Heute können Schwachstellen im System aufgrund von Fehlern in der Integration von IT- und Elektrizitätstechnologie auftreten.

Jeder der Sektoren, die am intelligenten Stromnetz beteiligt sind, hat eigene Sicherheitsstandards und Bewertungsprogramme, um bekannte Schwachstellen in ihren Systemen zu identifizieren und zu adressieren. Allerdings müssen diese Schwachstellen auch im Kontext der komplexen intelligenten Netzinfrastruktur bewertet werden, die viele Interessengruppen und hochsensible Betriebsanforderungen umfasst. Obwohl es viele Standards gibt, die über viele Monate entwickelt und alle fünf Jahre überprüft werden, um Aktualisierungen zu identifizieren, gibt es immer noch viele Standards, die keine Cybersicherheitsmaßnahmen enthalten oder auf aktuelle Sicherheitsstandards verweisen. Durch die fortlaufende Arbeit des Smart Grid Interoperability Panel (SGIP) und des Smart Grid Cyber Security Committee (SGCC) werden Smart Grid relevante Standards auf Cybersicherheit überprüft und Empfehlungen zur Einbeziehung von Cybersicherheit in zukünftige Überarbeitungen und Implementierungen der Standards gemacht.

Cyber Security muss in diesem Zusammenhang als Summe verschiedener Sicherheitstechno-logien, Lösungen und Verfahren betrachtet werden, die miteinander verwoben sind, um die Anforderungen von Richtlinien, Verfahrens- und technischen Standards zu erfüllen. Die Cyber Security jeder Komponente des Stapels ist wichtig, muss jedoch auch im Kontext der Implementierung einer Organisation betrachtet werden.

Weiterführende Literatur:

- H. Farhangi, "The path of the smart grid," in *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18-28, January-February 2010, doi: 10.1109/MPE.2009.934876.
- International Electrotechnical Commission (IEC): Smart Grid Standards, https://www.iec.ch/smartgrid/ M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A Survey on Smart Grid Cyber-Physical System Testbeds," IEEE Communications Surveys Tutorials, vol. 19, no. 1, pp. 446–464, 2017.

5.2 Cyber Physical Systems

Cyber Physical Systems (CPS) sind vernetzte Systeme aus Cyber- und physischen Elementen, die zusammen entworfen wurden, um adaptive und vorausschauende Systeme für verbesserte Leistung und Zuverlässigkeit zu schaffen. CPS werden in verschiedenen Bereichen wie intelligenten Stromnetzen, Fertigung, Verkehrssystemen und intelligenten Strukturen eingesetzt. Die Sicherheit von CPS, insbesondere im Zusammenhang mit intelligenten Stromnetzen, ist von großer Bedeutung, da sie viele einzigartige Merkmale aufweisen und eine Echtzeitreaktion erfordern, was Auswirkungen auf Entscheidungen zur Cyber-Sicherheit hat. Es ist wichtig, dass die Informationen und die unterstützenden Kommunikations- und Informationsinfrastrukturen von CPS angemessen geschützt sind, um ihre Zuverlässigkeit und Verfügbarkeit zu gewährleisten.

Da das Smart Grid sowohl physischen als auch dynamischen Bedrohungen ausgesetzt ist, müssen seine physischen und digitalen Komponenten entsprechend geschützt werden. Im Gegensatz zu herkömmlichen Netzwerkangriffen, die darauf abzielen, Schäden im Cyber-Layer zu verursachen, zielen Angriffe auf das Smart Grid darauf ab, den Betrieb der physischen Stromerzeugungs-, Übertragungs- und Verteilungssysteme zu stören.

Es kann verlockend sein anzunehmen, dass man bestehende Lösungen einfach auf neue Technologien anwenden kann. Aber oft gibt es bei neuen Technologien neue Herausforderungen, die neue Ansätze und Lösungen erfordern. Beim Smart Grid gibt es viele neue Sicherheitsprobleme, die neue Ansätze in der Cyber-Sicherheit erfordern. In diesem Forschungsprojekt untersuchen wir diese Herausforderungen genauer.

Das Smart Grid wird jedes Haus und Gebäude erreichen, was potenziellen Angreifern Zugang zu einigen Netzkomponenten bieten wird. Die Integration von Informationstechnologie, (IT)-Systemen und -Netzwerken macht das intelligente Netz anfällig für eine Vielzahl von Sicherheitsbedrohungen. Aufgrund seiner Größe und Komplexität ist es nahezu unmöglich, für jedes einzelne Subsystem Sicherheit zu garantieren. Das Smart Grid muss verschiedene Systeme und Netzwerke verbinden, darunter Erzeugungsanlagen, Verteilungseinrichtungen, intelligente Endpunkte und Kommunikationsnetzwerke, die möglicherweise dereguliert und von mehreren Einrichtungen besessen werden. Die Heterogenität, Vielfalt und Komplexität der Smart Grid-Komponenten können neben den bereits bekannten Schwachstellen auch neue Schwachstellen ermöglichen. Zudem können anspruchsvolle Steuerungs-, Schätzungs- und Preisalgorithmen, die in das Netz integriert sind, ebenfalls Schwachstellen generieren.

Im Jahr 2010 wurde eine neue Art von Malware namens Stuxnet entdeckt, die darauf abzielte, Steuerungssysteme von elektrischen Netzen zu sabotieren. Diese Art von Angriffen zielt darauf ab, die physische Integrität der Systeme zu stören. Zum Beispiel kann ein Angreifer die Integrität eines Zählers oder eines Sensors beeinträchtigen, nicht nur um die Geheimhaltung zu brechen, sondern auch um die Funktionalität des Netzes zu stören.

Um solche Angriffe zu verhindern, müssen neue Ansätze und Methoden entwickelt werden, die die Anforderungen von komplexen, groß angelegten und wachsenden Infrastrukturen wie dem Smart Grid bewältigen können. Eine Möglichkeit besteht darin, Cyber-Sicherheit und Systemtheorie zu kombinieren, um ein Konzept namens "Cyber-Physische Sicherheit" zu schaffen. Diese Modelle sollten in der Lage sein, dynamische Systeme und Bedrohungsmodelle in einem vereinheitlichten Rahmen zu integrieren und hybride Angriffe zu erkennen und zu bekämpfen.

Obwohl sowohl Cyber-Sicherheit als auch Systemtheorie wichtige Aspekte der Sicherheit von physischen und Cyber-Systemen behandeln, sind sie allein nicht ausreichend, um die Sicherheit des Smart Grids zu gewährleisten. Daher müssen CPS-Modelle entwickelt werden, die alle Aspekte in einem einzigen Rahmen integrieren können.

In einigen Forschungsartikeln wird argumentiert, dass Cyber-Physische Sicherheit neue und verbesserte Lösungen für die Erkennung, Reaktion, Rekonfiguration und Wiederherstellung von Systemfunktionalitäten bereitstellen kann, während das System weiterhin betrieben wird. Das QGroup Team geht davon aus, dass vorhandene Modellierungsformalismen wie Spieltheorie, vernetzte Steuerungssysteme und hybride dynamische Systeme genutzt werden können, um die Sicherheit von Cyber-Physischen Systemen systematisch zu behandeln. Es wird interessant sein zu sehen, wie Forschungsteams sich in der Zukunft mit diesen neuen Anforderungen auseinandersetzen werden.

Weiterführende Literatur:

- Guo, J., & Zhang, Y. (2015). Cyber security issues in smart grid: Threats and countermeasures. Proceedings of the IEEE, 103(5), 998-1017.

- Goodall, J. L., & Ma, Y. (2014). Cybersecurity considerations for the Smart Grid. IEEE Power and Energy Magazine, 12(4), 52-61.
- Bandyopadhyay, S., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. Wireless Personal Communications, 58(1), 49-69.
- Fu, K., Lu, R., & Liu, J. (2012). Security and privacy in smart grid: Challenges and opportunities. IEEE Network, 26(5), 34-41.

5.3 System-Modell

Smart Grids bestehen aus vier Komponenten: Erzeugung, Übertragung, Verteilung und Ver-brauch. In der Verbrauchskomponente nutzen Kunden elektrische Geräte (z. B. Smart Appliances, Elektrofahrzeuge), und ihr Stromverbrauch wird von einem erweiterten Messgerät, einem sogenannten Smart Meter, gemessen. Der Smart Meter ist eine der Kernkomponenten der Advanced Metering Infrastructure (AMI). Das Messgerät kann gemeinsam mit einem Gateway eines Home Area-Netzwerks (HAN) oder eines Business Area-Netzwerks (BAN) betrieben werden. Unterhalb einer Umspannstation wird ein Neighbour Area-Netzwerk (NAN) gebildet, in dem mehrere HANs gehostet werden. Schließlich kann ein Energieversorgungsunternehmen ein Wide Area-Netzwerk (WAN) nutzen, um verteilte NANs zu verbinden.

Standard Cyber-Sicherheit betrachtet das physische System nicht. Daher kann die Cyber-Sicherheit kaum gegen physische Angriffe verteidigen. Zum Beispiel schützt die Cyber-Sicherheit die Integrität von Messdaten durch den Einsatz von sicheren Geräten und Kommunikationsprotokollen. Die Integrität von Sensoren kann jedoch durch die lokale Modifikation des physischen Zustands des Systems gebrochen werden. Zum Beispiel können Shunt-Verbindungen parallel zu einem Messgerät platziert werden, um es mit dem Ziel des Energie-Diebstahls zu umgehen. In diesem Fall kann keine rein cyberbasierte Methode effektiv eingesetzt werden, um solche Angriffe zu erkennen und zu bekämpfen, da der Cyber-Teil des Systems gar nicht kompromittiert ist. Daher können selbst die Ziele der Cyber-Sicherheit in Cyber Physical-Systemen durch reine Cyber-Ansätze nicht erreicht werden.

Darüber hinaus ist die Cyber-Sicherheit nicht gut gerüstet, um die Auswirkungen von Cyber-Angriffen und Gegenmaßnahmen auf das physische System vorherzusagen. Zum Beispiel können DoS-Angriffe dazu führen, dass Messdaten und Steuerbefehle nicht kommuniziert werden, was zu Instabilität im Netz führen kann. Eine Gegenmaßnahme gegen DoS-Angriffe besteht darin, einige der kompromittierten Knoten aus dem Netzwerk zu isolieren, was jedoch zu noch schwerwiegenderen Stabilitätsproblemen führen kann. Daher ist ein Verständnis des physischen Systems auch für die Verteidigung gegen Cyber-Angriffe unerlässlich.

Weiterführende Literatur:

- J. Farquharson, A. Wang and J. Howard, "Smart Grid Cyber Security and substation Network Security," *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, Washington, DC, USA, 2012, pp. 1-5, doi: 10.1109/ISGT.2012.6175788.

5.4 Cyber Security-Anforderungen

Es müssen Sicherheitsmaßnahmen auf verschiedenen Ebenen implementiert werden, um eine umfassende Cyber-Sicherheitsstrategie zu gewährleisten. Dazu gehört die Implementierung von Schutzzonen, die den Zugriff auf kritische Systeme und Daten einschränken, sowie die Implementierung von Authentifizierungs- und Verschlüsselungstechnologien, um die Vertraulichkeit und Integrität von Daten zu gewährleisten. Daher ist es wichtig, dass die verschiedenen Schutzziele angemessen berücksichtigt werden, um eine effektive Cyber-Sicherheitsstrategie für Smart Grids zu entwickeln.

In diversen Forschungsprojekten wurde die Bedeutung des Schutzes der Kerninformationsarten im Hinblick auf die wichtigsten Sicherheitseigenschaften untersucht. Erwähnt werden sollte auch NISTIR 7628, ein Leitfaden des National Institute of Standards and Technology (NIST) für die Sicherheit von Cyber-Physischen Systemen (CPS). Dieser Leitfaden bietet einen Überblick über die Konzepte, Komponenten und Architekturen von CPS und diskutiert die Herausforderungen und Bedrohungen, die sie darstellen.

Die wichtigsten Anforderungen zum Schutz von Smart Grids sind im Folgenden zusammengefasst:

Die Vertraulichkeit von Messdaten ist wichtig, da Informationen über den Stromverbrauch Aufschluss über die Nutzungsmuster einzelner Geräte geben können und so persönliche Aktivitäten durch nicht intrusive Überwachung von Geräten offenbart werden können. Die Vertraulichkeit von Preisinformationen ist nicht wichtig, wenn sie öffentlich bekannt sind. Die Vertraulichkeit von Software sollte nicht kritisch sein, da die Sicherheit des Systems nicht auf der Geheimhaltung der Software, sondern nur auf der Geheimhaltung der Schlüssel basieren sollte.

Die Integrität der Preisinformationen ist allerdings sehr wichtig. Beispielsweise können negative Preise, die von einem Angreifer eingespeist werden, zu einem Stromverbrauchs-Spike führen, da zahlreiche Geräte gleichzeitig eingeschaltet werden, um den niedrigen Preis zu nutzen. Obwohl die Integrität der Messdaten und Befehle wichtig ist, ist ihre Auswirkung größtenteils auf den Umsatzverlust beschränkt. Auf der anderen Seite ist die Integrität der Software kritisch, da kompromittierte Software oder Malware jedes Gerät und jede Netzwerkkomponente kontrollieren kann.

Denial-of-Service (DoS)-Angriffe sind Angriffe, bei denen gefälschte Anfragen an Server oder ein Netzwerk mit dem Ziel gesendet werden, diese so stark auszulasten, dass sie reale Anfragen kaum noch oder sogar gar nicht mehr bearbeiten können, und verteilte DoS-Angriffe werden durch die Nutzung von verteilten Angriffsquellen wie beispielsweise kompromittierten Geräten durchgeführt. In Smart Grids ist die Verfügbarkeit von Informationen und Strom ein entscheidender Aspekt. Insbesondere die Verfügbarkeit von Preisinformationen ist aufgrund schwerwiegender finanzieller und möglicherweise rechtlicher Auswirkungen kritisch. Außerdem können veraltete Preisinformationen die Nachfrage negativ beeinflussen. Die Verfügbarkeit von Befehlen ist ebenfalls wichtig, insbesondere wenn ein Smart Meter nach Abschluss der Zahlung einer Stromrechnung wieder eingeschaltet wird. Auf der anderen Seite ist die Verfügbarkeit von Smart Meter-Daten (z. B. Stromverbrauch) möglicherweise nicht so kritisch, da die Daten in der Regel zu einem späteren Zeitpunkt abgerufen werden können.

Weiterführende Literatur:

- Farhangi, H. (2010). The path of the smart grid. IEEE Power and Energy Magazine, 8(1), 18-28. DOI: 10.1109/MPE.2009.934876

- J. Liu, Y. Xiao, S. Li, W. Liang and C. L. P. Chen, "Cyber Security and Privacy Issues in Smart Grids," in *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 981-997, Fourth Quarter 2012, doi: 10.1109/SURV.2011.122111.00145.
- M. K. Kuyucu, Ş. Bahtiyar and G. İnce, "Security and Privacy in the Smart Home: A Survey of Issues and Mitigation Strategies," *2019 4th International Conference on Computer Science and Engineering (UBMK)*, Samsun, Turkey, 2019, pp. 113-118, doi: 10.1109/UBMK.2019.8907037.

5.5 Klassifizierung von Angreifern

Da es möglich ist, dass Angreifer oder Benutzer bewusst oder unbewusst Schwachstellen in Smart Grid-Netzwerken ausnutzen und Schäden auf verschiedenen Ebenen des Systems für verschiedene Zwecke verursachen, haben Forscher die unterschiedlichen Angreifer-Typen klassifiziert.

Die Klassifizierung der Angreifer erfolgt auf Basis der Ziele und Motivationen, die sie verfolgen. Cyber-Angriffe auf Smart Grid-Netzwerke können durch verschiedene Faktoren wie Cyberkrieg, Terrorismus, Wirtschaftsspionage, Aktivismus, wirtschaftliche Gründe, unzufriedene Mitarbeiter und sogar Scherze motiviert sein.

Angreifer können sehr unterschiedlich qualifiziert und kategorisierbar sein - Amateure oder Profis, Terroristen, Mitarbeiter, Konkurrenten und sogar Kunden selbst. Nicht bösartige Angreifer sind diejenigen, die neugierig auf das System sind und deren primäres Ziel nicht darin besteht, Schaden anzurichten. Sie gehen Fragestellungen der Systemsicherheit und des Systembetriebs an, als ob es ein Rätsel wäre, das gelöst werden müsste. Diese Angreifer handeln aus einem Gefühl der intellektuellen Neugier und Herausforderung. Script Kiddies und Hobbyisten werden im Allgemeinen als harmlose Angreifer in Smart Grid-Kommunikationsnetzen angesehen.

Diese Endbenutzer können ihre Smart Meter oder Datenübertragungsleitungen so nutzen, dass es für sie von Vorteil ist. Kunden könnten ihre Stromrechnungen senken, indem sie sich mit dem nächstgelegenen Advanced Metering Infrastructure-System verbinden und die Daten manipulieren.

Wenn Terroristen Angriffe auf elektrische Stromnetze starten, hoffen sie, den Betrieb kritischer Infrastrukturen zu stören, die Wirksamkeit ihrer terroristischen Handlungen zu erhöhen und eine weitreichende Störung der öffentlichen Ordnung zu verursachen.

Darüber hinaus kann ein unzufriedener Mitarbeiter, dem der Zugang zu Systemkomponenten gewährt wurde, die Einstellungen von Software-Algorithmen oder die Konfiguration von Geräten so ändern, dass sie seinen eigenen Interessen und Nutzen entsprechen. Der Begriff „interne Angreifer“ wird häufig verwendet, um dieses unzufriedene Personal zu beschreiben.

Konkurrenten können auch aus finanziellen Gründen Krieg gegeneinander führen. Solche Angriffe können beispielsweise darauf abzielen, sensible Unternehmens- oder Verbraucherdaten aus einer Datenbank zu stehlen, um sich einen Wettbewerbsvorteil zu verschaffen.

Weiter gehören auch staatlich unterstützte Hacker, organisierte kriminelle Angreifer und Hacktivisten zu den Angreifern. Es ist daher wichtig, eine Vielzahl von Sicherheitsmaßnahmen zu ergreifen, um viele Arten von Angriffen abzudecken.

Weiterführende Literatur:

- M. Z. Gunduz and R. Das, "A comparison of cyber-security-oriented testbeds for IoT-based smart grids" in 2018 6th International Symposium on Digital Forensic and Security (ISDFS), pp. 1–6, Mar. 2018, .
- C. P. Vineetha and C. A. Babu, "Smart grid challenges, issues and solutions" in 2014 International Conference on Intelligent Green Building and Smart Grid (IGBSG), pp. 1–4, Apr. 2014.
- V. Delgado-Gomes, J. F. Martins, C. Lima, and P. N. Borza, "Smart grid security issues" in 2015 9th International Conference on Compatibility and Power Electronics (CPE), pp. 534–538, June 2015. 10.1109/CPE.2015.7231132
- Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications", IEEE Communications Surveys Tutorials, vol. 14, no. 4, pp. 998–1010, 2012.

5.6 Schwachstellen

Im Folgenden werden einige der ungewöhnlicheren Schwachstellen des Smart Grids untersucht, die in klassischer Cyber Security meist anders gesehen werden. Das Smart Grid ist, wie oben schon erwähnt, ein Konzept, bei dem Komponenten von traditionellen Stromnetzen mit Informationstechnologie und Kommunikationstechnologie digitalisiert und vernetzt werden, um die Effizienz und Verfügbarkeit des Stromsystems zu verbessern. Allerdings birgt diese Integration auch Gefahren. Schwachstellen können beispielsweise durch Cyberangriffe ausgenutzt werden, die auf die Kontrollsysteme des Stromnetzes abzielen. Dadurch kann die Versorgung beeinträchtigt oder sogar lahmgelegt werden. Es ist wichtig zu erkennen, dass auch physische Angriffe wie Sabotage oder Vandalismus an den Komponenten des Smart Grids zu Störungen führen können. Es ist daher wichtig, diese Schwachstellen zu erkennen und geeignete Maßnahmen zu ergreifen.

Weiterführende Literatur:

- Clements S and Kirkham H. Cyber-security considerations for the smart grid. In: *Proc of the IEEE Power and Energy Society General Meeting*, 2010:1-5.
- Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2013). Smart grid technologies: Communication technologies and standards. IEEE Transactions on Industrial Informatics, 9(1), 28-42.
- Aloul, F., Zualkernan, I. A., & Al-Muhtadi, J. (2013). Smart grid security: Threats, vulnerabilities and solutions. Journal of Smart Grid and Clean Energy, 2(1), 1-15.

5.6.1. Personenbezogene Daten

Smart Meter sammeln autonom massive Datenmengen und transportieren sie an das Versorgungsunternehmen, den Verbraucher und Dienstleister. Diese Daten enthalten private Verbraucherinformationen, die dazu verwendet werden könnten, Verbraucheraktivitäten, verwendete Geräte und Zeiten, in denen das Haus leer steht, abzuleiten.

Um die Sicherheit von Kundeninformationen im Smart Grid zu gewährleisten, müssen Basis-Anforderungen erfüllt werden. Dazu gehört die Verwendung von robusten Verschlüsselungstechnologien, um sicherzustellen, dass die Daten während der Übertragung und Speicherung nicht kompromittiert werden. Der Zugriff auf die Daten muss auf autorisierte Personen beschränkt sein und es müssen Maßnahmen zum Schutz vor Datenverlust oder Diebstahl ergriffen

werden. Darüber hinaus sollten die Kunden über die Verwendung ihrer Daten informiert werden und die Möglichkeit haben, der Nutzung ihrer Daten zu widersprechen. Was allein schon von der Datenschutz-Grundverordnung (DSGVO) zwingend vorgeschrieben wird.

Weiterführende Literatur:

- Cardenas, Alvaro & Safavi-Naini, Reihaneh. (2012). Security and Privacy in the Smart Grid. 10.1016/B978-0-12-415815-3.00025-X.
- C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," *2010 First IEEE International Conference on Smart Grid Communications*, Gaithersburg, MD, USA, 2010, pp. 238-243, doi: 10.1109/SMARTGRID.2010.5622050.

5.6.2. Geräteanzahl

Das Smart Grid ist ein komplexes Netzwerk von Geräten und Systemen, dass die Stromerzeugung, Stromversorgung und Nachfrage steuern. Es besteht aus einer Vielzahl von intelligenten Geräten, wie z. B. Smart Meter, Smart Appliances und Elektrofahrzeugen. Diese Geräte können somit nicht nur den Stromverbrauch messen, sondern auch Informationen über das Netzwerk übertragen und Signale zur Steuerung der Stromversorgung empfangen. Durch die Integration von vielen verschiedenen Geräten und Systemen wird die Angriffsfläche deutlich erhöht und potenzielle Schwachstellen im Netzwerk werden schwerer zu identifizieren und zu beheben.

Die Größe des Smart Grid-Netzwerks macht es auch schwierig, das Netzwerk zu überwachen und zu verwalten. Zudem erfordern die Koordination und Integration dieser vielen Geräte komplexe Systeme, die ebenfalls anfällig für Angriffe sein können. Es ist daher von entscheidender Bedeutung, dass die Cyber-Sicherheit im Smart Grid auch für sehr große Gerätezahlen effektiv gemanagt werden kann.

Weiterführende Literatur:

- Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, 2015. doi: 10.1109/COMST.2015.2444095.
- S. N. Islam, Z. Baig and S. Zeadally, "Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures," in *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6522-6530, Dec. 2019, doi: 10.1109/TII.2019.2931436.

5.6.3. Physische Gewalt

Sicherheit bezieht sich auch auf Maßnahmen, die ergriffen werden, um physische Bedrohungen gegen das Smart Grid-System zu verhindern oder zu minimieren. Dies ist ein entscheidender Faktor für die Gesamtsicherheit des Smart Grids, da viele Komponenten des Systems an unsicheren physischen Standorten installiert sind, was sie anfällig für physischen Zugriff macht. Physische Bedrohungen können in Form von Sabotage, Vandalismus, Diebstahl oder anderen Angriffen auf die Infrastruktur auftreten.

Um diese Bedrohungen zu minimieren, werden physische Barrieren wie Zäune, Mauern oder Tore verwendet, um unautorisierten Zugang zu verhindern. Zusätzlich können Überwachungssysteme wie Kameras oder Bewegungssensoren installiert werden, um Bedrohungen zu erkennen und schnell darauf reagieren zu können. Es ist jedoch auch wichtig, dass das Versorgungsunternehmen seine

Mitarbeiter schult, um potenzielle Bedrohungen zu erkennen und geeignete Maßnahmen zu ergreifen, um das System zu schützen.

5.6.4. Alter der Geräte

Die Kompatibilität von älteren Geräten mit neueren Smart Grid-Systemen stellt eine weitere Herausforderung dar, da sie möglicherweise nicht über die notwendigen Kommunikations-protokolle verfügen. Auch die Installation von Sicherheitsupdates auf veralteten Geräten kann problematisch sein, da die Hersteller möglicherweise keinen Support mehr für ältere Geräte anbieten. Darüber hinaus gibt es auch Sicherheitsrisiken im Zusammenhang mit der Implementierung neuer Technologien im Smart Grid. Zum Beispiel können intelligente Messgeräte (Smart Meter) anfällig für Angriffe sein, da sie möglicherweise nicht über ausreichende Sicherheitsfunktionen verfügen. Angreifer können diese Schwachstellen ausnutzen, um Zugriff auf das Gesamtsystem zu erhalten.

Es ist daher wichtig, dass Unternehmen, die Smart Grid-Systeme implementieren, die neuesten Sicherheitstechnologien und Protokolle verwenden, um potenzielle Sicherheitsbedrohungen zu minimieren. Außerdem müssen sie regelmäßig ihre Systeme überwachen und Aktualisierungen durchführen, um sicherzustellen, dass sie vor aktuellen und aufkommenden Bedrohungen geschützt sind.

Weiterführende Literatur:

- Muhammed Zekeriya Gunduz and Resul Das. 2020. Cyber-security on smart grid: Threats and potential solutions. Comput. Netw. 169, C (Mar 2020). https://doi.org/10.1016/j.comnet.2019.107094

5.6.5. Klassische Power Devices

Klassische Stromgeräte wie Generatoren, Transformatoren und Schaltanlagen sind ebenfalls anfällig für Sicherheitsbedrohungen. Da diese Geräte oft über Jahrzehnte hinweg verwendet werden, können sie Schwachstellen aufweisen, die es Angreifern ermöglichen, in das System einzudringen und es zu beeinträchtigen. Ein Beispiel hierfür ist der Zugriff auf Steuerungssysteme über unsichere Netzwerkverbindungen, mit denen Stromversorgungen manipuliert oder sogar ganz abgeschaltet werden können. Um solche Angriffe zu verhindern, müssen auch in klassische Strom-Infrastrukturen Sicherheitsvorkehrungen wie Firewalls, Zugriffsbeschränkungen und Intrusion Detection-Systeme eingerichtet werden.

Darüber hinaus erfordert die Integration von Smart Grid-Technologien in vorhandene Strom-netze eine erhöhte Aufmerksamkeit für die Sicherheit. Da Smart Grid-Geräte und -Systeme in der Regel auf offenen Standards und Protokollen basieren, können sie leichter von Angreifern ausgenutzt werden, die sich auf die Ausnutzung bekannter Sicherheitslücken konzentrieren. Um diese Bedrohungen zu minimieren, müssen spezifische Sicherheitsmaßnahmen für Authentifizierung, Verschlüsselung und zudem regelmäßige Sicherheitsupdates geplant werden.

Weiterführende Literatur:

- X. Chu, M. Tang, H. Huang and L. Zhang, "A security assessment scheme for interdependent cyber-physical power systems," *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, Beijing, China, 2017, pp. 816-819, doi: 10.1109/ICSESS.2017.8343036.

- Y. Liu, Y. Peng, B. Wang, S. Yao and Z. Liu, "Review on cyber-physical systems," in *IEEE/CAA Journal of Automatica Sinica*, vol. 4, no. 1, pp. 27-40, Jan. 2017, doi: 10.1109/JAS.2017.7510349.

5.6.6. Organisation

Eine mangelhafte Zusammenarbeit zwischen den Infrastrukturteams kann zu Kommunikationsproblemen und Konflikten führen, die die Umsetzung von Sicherheitsrichtlinien und -maßnahmen behindern. IT- und OT-Teams haben oft unterschiedliche Ziele und Arbeitsweisen, was die Zusammenarbeit erschweren kann. Die OT-Teams (Operational Technology) konzentrieren sich auf die Stromerzeugung, -übertragung und -verteilung, während IT-Teams sich auf Netzwerk- und Informationssicherheit konzentrieren. Daher können diese Teams unterschiedliche Prioritäten und Perspektiven haben, wenn es um die Sicherheit des Smart Grids geht.

Es ist wichtig, dass eine klare Rollen- und Verantwortungszuweisung innerhalb aller Teams etabliert wird, um eine effektive Zusammenarbeit zu gewährleisten. Um eine effektive Zusammenarbeit zu erreichen, sollten klare Kommunikationswege zwischen den Teams festgelegt werden. Regelmäßige Treffen und Schulungen können dazu beitragen, dass die Teams auf dem neuesten Stand bleiben und dass potenzielle Sicherheitsbedrohungen frühzeitig erkannt werden. Die Zusammenarbeit zwischen den Teams sollte auch in der Planung und Umsetzung von Sicherheitsmaßnahmen berücksichtigt werden, um sicherzustellen, dass alle Aspekte der Sicherheit des Smart Grids abgebildet sind.

5.6.7. Protokolle

IT- und OT-Standard-Protokolle werden in Smart Grids eingesetzt, um Kompatibilität zwischen den verschiedenen Komponenten zu gewährleisten. IP-basierte Netzwerkangriffe sind zum Beispiel IP-Spoofing, Tear Drop und Denial-of-Service-Angriffe. IP-Spoofing bezieht sich auf die Fälschung von IP-Adressen, um auf Netzwerke zuzugreifen oder Angriffe zu verschleiern. Tear Drop-Angriffe verwenden manipulierte Pakete, die nicht in der Lage sind, von den Geräten verarbeitet zu werden, was zu Systemabstürzen führt. Denial-of-Service-Angriffe sind darauf ausgelegt, Ressourcen in einem Netzwerk zu überlasten, indem sie mehr Datenverkehr generieren, als das Netzwerk verarbeiten kann.

Um diese Angriffe zu vermeiden, müssen geeignete Sicherheitsmaßnahmen implementiert werden, die die IP-basierte Kommunikation in Smart Grids schützen. Hierbei können z. B. verschlüsselte Übertragungsprotokolle, Authentifizierung und Autorisierung von Geräten, Zugriffsbeschränkungen für sensible Daten und Network Intrusion Detection Systeme (NIDS) eingesetzt werden. Darüber hinaus sollten die Geräte regelmäßig aktualisiert und gewartet werden, um Schwachstellen zu minimieren und die Sicherheit des Netzwerks zu gewährleisten.

OT-Protokolle (Operational Technology-Protokolle) sind spezielle Kommunikationsprotokolle, die für die Steuerung von industriellen Prozessen und Systemen eingesetzt werden. Sie stellen eine wichtige Verbindung zwischen den physischen Systemen und den Steuerungs- und Überwachungseinrichtungen dar. Schwachstellen in OT-Protokollen können dazu führen, dass Angreifer auf industrielle Kontrollsysteme zugreifen und diese beeinträchtigen können. Da viele industrielle Systeme über Jahrzehnte im Einsatz sind und möglicherweise nicht auf die neuesten Standards aktualisiert werden können, ist es besonders wichtig, geeignete Sicherheitsmaßnahmen und Schutzvorkehrungen zu

implementieren, um Schwachstellen in OT-Protokollen zu minimieren und Industrieanlagen vor möglichen Cyberangriffen zu schützen.

SCADA (Supervisory Control and Data Acquisition) ist eine Technologie, die in Smart Grid-Systemen verwendet wird, um Stromversorgungsanlagen und -netze aus der Ferne zu überwachen und zu steuern. Das System sammelt und analysiert Daten über Stromerzeugung, -verteilung und -verbrauch und aktiviert automatische Steuerungsfunktionen, um die Stromversorgung in Echtzeit zu optimieren und zu verwalten. Es ermöglicht Energieversorgungsunternehmen, den Zustand von Geräten in Echtzeit zu überwachen, Energieverbrauchsmuster zu analysieren und Energieeffizienzprogramme durchzuführen. SCADA ist ein wichtiger Bestandteil des Smart Grid-Systems, da es die Effizienz und Zuverlässigkeit der Stromversorgung verbessert und eine schnellere Reaktion auf Ausfälle und Störungen ermöglicht. Es gibt eine Vielzahl von SCADA-Protokollen, einschließlich Modbus, DNP3, IEC 60870-5 und PROFIBUS, die je nach Anwendung und Hersteller verwendet werden.

Das bekannte Modbus-Protokoll wurde ursprünglich für die serielle Kommunikation mit geringer Geschwindigkeit in Prozesssteuerungsnetzwerken entwickelt und ist daher nicht für hochsicherheitskritische Umgebungen konzipiert. Aus diesem Grund gibt es verschiedene Schwachstellen im Modbus-Protokoll, die es einem Angreifer ermöglichen, das System zu beeinträchtigen. Ein Beispiel dafür ist die Möglichkeit, mit einem Protokollanalyse-Tool den Netzwerkverkehr zu sniffen, SCADA Distributed Network Protocol 3.0 (DNP3) Frames abzufangen und unverschlüsselte Klartext-Frames zu sammeln, die wertvolle Informationen wie Quell- und Zieladressen liefern. Diese abgefangenen Daten, die Steuerungs- und Einstellungsinformationen enthalten, könnten dann zu einem späteren Zeitpunkt auf einem anderen SCADA-System oder Intelligent Equipment Device (IED) verwendet werden, um im schlimmsten Fall Dienste herunterzufahren oder zumindest Serviceunterbrechungen zu verursachen.

Eine weitere Schwachstelle ist die Möglichkeit, gefälschte Befehle an ein Gerät oder eine Gruppe von Geräten in einer Zielregion zu senden, was zu Stromausfällen führen kann. Zum Beispiel kann das Senden von Trennungsanweisungen an Smart Meter in einer Region zur Unterbrechung der Stromversorgung in dieser Region führen. Auch ungültiges Schalten elektrischer Geräte kann unsichere Verbindungen verursachen, die zu Bränden führen können. Daher kann auch unsichere Kommunikation in Smart Grids menschliches Leben bedrohen.

Weiterführende Literatur:

- G. Rajendran, H. V. Sathyabalu, M. Sachi and V. Devarajan, "Cyber Security in Smart Grid: Challenges and Solutions," *2019 2nd International Conference on Power and Embedded Drive Control (ICPEDC)*, Chennai, India, 2019, pp. 546-551, doi: 10.1109/ICPEDC47771.2019.9036484.
- X. Li, X. Liang, R. Lu, X. Shen, X. Lin and H. Zhu, "Securing smart grid: cyber-attacks, countermeasures, and challenges," in *IEEE Communications Magazine*, vol. 50, no. 8, pp. 38-45, August 2012, doi: 10.1109/MCOM.2012.6257525.

5.6.8. Insider

Insider-Angriffe stellen eine ernsthafte Bedrohung für die Sicherheit von Smart Grids dar, da sie von Personen ausgeführt werden, die bereits Zugang zu vertraulichen Informationen und Kontrollfunktionen haben. Dies kann von Mitarbeitern von Energieversorgern bis hin zu externen Dienstleistern reichen. Insider-Angriffe können auf verschiedene Weise durchgeführt werden, wie z. B.

durch das Einfügen von Malware in das System, durch physische Manipulation von Geräten oder durch den Diebstahl von Zugangsdaten. Um solche Angriffe zu verhindern, gibt es verschiedene Sicherheitskontrollen wie die Implementierung von Zugangskontrollen, Überwachung und Protokollierung von Benutzeraktivitäten, Schulung und Sensibilisierung von Benutzern für Sicherheitsfragen sowie regelmäßige Sicherheitsaudits und Schwachstellenbewertungen. Wichtig ist auch, dass Energieversorgungsunternehmen und andere Stakeholder klare Richtlinien und Verfahren für den Umgang mit vertraulichen Informationen und kritischer Infrastruktur haben und diese regelmäßig überprüft und aktualisiert werden, um den ständig wechselnden Bedrohungen gerecht zu werden.

Weiterführende Literatur:

- H. Bao, R. Lu, B. Li and R. Deng, "BLITHE: Behavior Rule-Based Insider Threat Detection for Smart Grid," in *IEEE Internet of Things Journal*, vol. 3, no. 2, pp. 190-205, April 2016, doi: 10.1109/JIOT.2015.2459049.

5.7 Angriffstypen

Im Folgenden wollen wir die Hauptarten von Bedrohungen beschreiben. Es gibt zwei Arten von Sicherheitsangriffen, die zur Kompromittierung der Sicherheit von Smart Grid-Netzwerken verwendet werden können: passiv und aktiv.

Passiv bedeutet, dass der Angreifer versucht, Informationen aus dem Netzwerk zu stehlen, ohne dessen Funktionsweise zu beeinträchtigen. Aktiv bedeutet, dass der Angreifer versucht, das Netzwerk durch Einfügen von gefälschten Daten oder Ändern der bereits vorhandenen Daten zu beeinträchtigen.

Weiterführende Literatur:

- *Pandey, R.K., & Misra, M. (2016). Cyber security threats — Smart grid infrastructure. 2016 National Power Systems Conference (NPSC), 1-6.*
- A. Procopiou and N. Komninos, "Current and future threats framework in smart grid domain," *2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, Shenyang, China, 2015, pp. 1852-1857, doi: 10.1109/CYBER.2015.7288228.
- Wenye Wang and Zhuo Lu. 2013. Survey Cyber security in the Smart Grid: Survey and challenges. Comput. Netw. 57, 5 (April, 2013), 1344–1371.

5.7.1. Passive Angriffe

Passive Angriffe zielen darauf ab, Informationen aus dem Netzwerk zu stehlen, ohne seine Funktionsweise zu beeinträchtigen. Die häufigsten Beispiele für passive Angriffe sind Abhören und Traffic-Analyse. Beim Abhören lauscht der Angreifer die übertragenen Daten ab, um Informationen zu sammeln, ohne das System zu stören. Traffic-Analyse ist ein passiver Angriff, der darauf abzielt, Muster im Netzwerkverkehr zu erkennen, um Informationen über das System zu erhalten. Indem der Angreifer das Verhalten des Netzwerks beobachtet, kann er Rückschlüsse auf die Architektur und den Betrieb des Netzwerks ziehen. Auch der physische Zugriff auf Netzwerkkabel oder Komponenten des Smart Grids kann ein Sicherheitsrisiko darstellen.

Es ist wichtig, Maßnahmen zu ergreifen, um diese Angriffsvektoren zu minimieren und damit die Sicherheit des Smart Grids zu gewährleisten. Um solche Angriffe zu verhindern, sollten

Sicherheitskontrollen wie Verschlüsselung, Authentifizierung und Zugangskontrollen implementiert werden. Darüber hinaus können Netzwerküberwachungstools und regelmäßige Sicherheitsaudits dazu beitragen, Abhörangriffe zu erkennen und zu verhindern.

5.7.2. Aktive Angriffe

Aktive Angriffe unterscheiden sich von passiven Angriffen dadurch, dass sie darauf abzielen, das System zu beeinträchtigen, indem sie die übertragenen Daten verändern oder gefälschte Daten in das System einspeisen. Es gibt neben den Geräten selbst drei Hauptkategorien von aktiven Angriffen: komponenten-, protokoll- und topologiebasierte.

Komponentenbasierte Angriffe können auch auf andere Komponenten abzielen, wie beispielsweise auf Smart Meter oder Sensoren, die zur Datenerfassung und -übertragung verwendet werden. Ein Angreifer kann die Firmware eines Smart Meter manipulieren, um den Stromverbrauch zu reduzieren oder zu erhöhen, was zu ungenauen Abrechnungen führt oder den Energiebedarf des Netzes überlastet. Ebenso können Angriffe auf Sensoren das System stören und zu Fehlfunktionen bei der Datenerfassung führen, was wiederum zu Fehlern bei der Entscheidungsfindung führen kann.

Protokollbasierte Angriffe auf Smart Grid-Systeme können auf verschiedene Arten erfolgen. Einer der gängigsten Ansätze ist der Reverse Engineering-Angriff, bei dem der Angreifer versucht, das Protokoll zu verstehen, um Schwachstellen zu identifizieren und auszunutzen. Reverse Engineering bezieht sich auf den Prozess, bei dem der Angreifer die Funktionen und das Verhalten des Protokolls durch die Analyse des Datenverkehrs und anderer Informationen, die von den Komponenten des Smart Grid-Systems gesendet und empfangen werden, untersucht. Ein weiterer Ansatz bei protokollbasierten Angriffen ist die Injektion von falschen Daten. Der Angreifer kann gefälschte Daten in den Datenstrom einschleusen, um die Funktionen des Systems zu beeinträchtigen oder die Daten selbst zu manipulieren. Dies kann zu Problemen wie falschen Messungen, fehlerhaften Steuerungsbefehlen und Sicherheitsverletzungen führen. Netzwerksegmentierung und Netzwerkzugangskontrollen können dazu beitragen, das Risiko von protokollbasierten Angriffen zu minimieren.

Topologiebasierte Angriffe zielen darauf ab, die physische oder logische Netzwerkstruktur eines Systems zu beeinträchtigen. Ein Beispiel für einen topologiebasierten Angriff ist der Denial-of-Service (DoS)-Angriff, bei dem ein Angreifer das Netzwerk mit einer hohen Anzahl von Anfragen überflutet und dadurch das System überlastet und träge macht. Eine andere Art von topologiebasiertem Angriff ist das Routing Protokoll Spoofing, bei dem ein Angreifer falsche Routing-Informationen an das Netzwerk sendet, um den Datenfluss zu beeinträchtigen. Derartige Angriffe können zur Beeinträchtigung der Verfügbarkeit des Systems und damit zu unangemessenen Entscheidungen der Betreiber führen.

Smart Meter-Geräte, die für die Überwachung und Messung des Energieverbrauchs in Haushalten und Unternehmen verwendet werden, können anfällig für Angriffe sein, die auf ihre Firmware abzielen. Firmware ist die eingebettete Software in der Hardware des Geräts und kann Schwachstellen aufweisen, die von Angreifern ausgenutzt werden können, um Malware einzuschleusen und die Kontrolle über das Gerät zu übernehmen. Sobald die Firmware kompromittiert ist, kann der Angreifer die Messwerte manipulieren oder sogar die Kommunikation zwischen dem Smart Meter-Gerät und dem Smart Grid-Netzwerk stören.

Die Problematik besteht darin, dass Angriffe auf Smart Grid-Geräte oft auf gemeinsame Schwachstellen abzielen und daher schwer zu erkennen sein können. Eine Lieferkette kann ebenfalls für Angriffe genutzt werden, indem bösartiger Code in ein Gerät vor dem Versand an einen Zielort installiert wird, um die Kontrolle über das Gerät zu übernehmen oder sensible Daten zu stehlen. Daher müssen

Sicherheitsvorkehrungen im Entwicklungs- und Herstellungsprozess von Software, Firmware und Ausrüstung gewährleistet werden, um solche Angriffe zu verhindern.

5.8 Physische Bedrohungen

Physische Angriffe auf das Stromnetz können schwerwiegende Auswirkungen haben, da sie direkt auf die physischen Komponenten des Netzes abzielen. Ein erfolgreicher Angriff kann erhebliche Schäden an der Infrastruktur verursachen und möglicherweise zu einem landesweiten Stromausfall führen.

Ein Beispiel für einen physischen Angriff auf das Stromnetz ist ein Scharfschützenangriff auf eine Umspannstation in Kalifornien im Jahr 2013. Bei diesem Angriff wurde ein Teil des Stromnetzes für mehrere Wochen lahmgelegt. Der Täter hat mit einem Gewehr gezielt auf die Kühlsysteme der Umspannstation geschossen, wodurch sie beschädigt wurden und ausfielen. (Pagliery, 2014)

Ein weiteres Beispiel für einen physischen Angriff auf das Stromnetz ist das Aufbrechen von Smart Meter, um sie zu manipulieren oder zu deaktivieren. Dies kann zum Zweck von Energie-Diebstahl erfolgen, denn der Smart Meter ist möglicherweise nicht mehr in der Lage, den Energieverbrauch korrekt zu messen. In einem Bericht des US-Energieministeriums wurde festgestellt, dass Smart Meter bei physischen Angriffen zerstört oder beschädigt werden können, was zu erhöhten Kosten für die Reparatur oder den Austausch führen kann. (Department of Energy, 2010)

Um physische Angriffe auf das Stromnetz zu verhindern, sind verschiedene Maßnahmen erforderlich. Dazu gehört zum Beispiel die Verbesserung der physischen Sicherheit von Umspannstationen und anderen kritischen Infrastrukturen durch Zäune, Überwachungssysteme und andere Sicherheitsmaßnahmen. Es ist auch wichtig, Smart Meter und andere physische Komponenten des Stromnetzes vor physischen Angriffen zu schützen, indem sie in sicheren Gehäusen installiert werden oder durch andere physische Barrieren geschützt werden.

Weiterführende Literatur:

- Pagliery, J. (2014). Sniper attack on california power grid may have been an insider, dhs says. CNN.com. Abgerufen von
- Department of Energy. (2010). Smart Grid Cyber Security Strategy and Requirements.

5.9 Dynamische Systemangriffe

Ein dynamischer Systemangriff (DSA) ist ein Angriff auf ein physisch-dynamisches System, d. h. auf Systeme, die sich im Laufe der Zeit ändern und sich an ihre Umgebung anpassen können. Im Fall des Smart Grids kann ein DSA durch verschiedene Angriffsvektoren durchgeführt werden, wie z. B. das Einfügen von Malware in das System, den physischen Zugriff auf das System oder das Abhören von Netzwerkverkehr. Der Replay-Angriff (RA) ist eine spezielle Art von DSA, bei dem ein Angreifer das System mit gefälschten Eingabedaten füttert, ohne dass das System diese als gefälscht erkennen kann. Dies kann zu Fehlfunktionen oder sogar zum Ausfall des gesamten Systems führen. Um solche Angriffe zu verhindern, müssen Sicherheitskontrollen wie die Überwachung und Protokollierung von Benutzeraktivitäten und Zugangskontrollen implementiert werden.

Eine weitere Art von DSAs ist der dynamische Dateninjektionsangriff (D-DIA), bei dem der Angreifer das Wissen über das dynamische Modell des Netzwerks nutzt, um Daten einzuschleusen, die zu einem

blinden Fleck bezüglich instabiler Pole führen. Dies bedeutet, dass der Netzwerkbetreiber Instabilitäten möglicherweise nicht erkennt, was wiederum zu einem Systemausfall führen kann.

Ein verdeckter Angriff ist eine weitere Art von DSAs, bei der der Angreifer Eingabedaten in das System einspeist, ohne Änderungen an den messbaren Ausgaben zu verursachen. Der Angreifer erreicht dies, indem er Sensoren kompromittiert und ihre Ausgänge überwacht, um sie zu wiederholen. Diese Art von Angriffen kann die Stabilität des gesamten Smart Grids gefährden und erfordert dringend Sicherheitsmaßnahmen.

Insgesamt sind diese Arten von Angriffen besonders gefährlich, da sie die Stabilität des gesamten Smart Grids gefährden können. In den folgenden Abschnitten werden einige besonders gefährliche Angriffe genauer beschrieben.

5.9.1. Koordinierte Angriffe

Das Stromsystem ist in der Regel mit Maßnahmen zur Robustheit ausgestattet, um potenzielle Ausfälle zu überstehen. Unter normalen Bedingungen können eine oder wenige Komponenten ausfallen, ohne dass dies signifikante Auswirkungen auf den Betrieb des Stromnetzes hat, da das System auf Redundanzen im Design setzt, um den normalen Betrieb aufrechtzuerhalten, selbst wenn eine Komponente ausfällt. Dies wird durch das "N-1"-Sicherheitskriterium gewährleistet. Jedoch können Angreifer, die über ausreichende Ressourcen verfügen, koordinierte Angriffe (CAs) durchführen, indem sie die dichten Verbindungen zwischen den Stromnetzkomponenten ausnutzen, um gleichzeitig mehrere Angriffe auf verschiedene Komponenten zu starten.

Ein Beispiel für einen koordinierten Angriff auf das Stromnetz ist der Angriff auf das Stromversorgungsunternehmen Ukrenergo in der Ukraine im Jahr 2016. Die Angreifer waren in der Lage, sich Zugang zum Netzwerk von Ukrenergo zu verschaffen und manipulierten dann das SCADA-System, um den Stromfluss zu unterbrechen. Dies führte zu einem Stromausfall, der etwa eine Stunde dauerte und Zehntausende von Menschen betraf.

Ein weiterer bekannter Angriff war der „BlackEnergy“-Angriff im Jahr 2015, der ebenfalls in der Ukraine stattfand. Die Angreifer infizierten die Computersysteme des Stromversorgungsunternehmens und manipulierten das SCADA-System. Um den Stromfluss zu unterbrechen, trennten sie gleichzeitig etwa 27 Umspannstationen vom Netz, was dann als Folge einen Stromausfall verursachte.

CAs gelten als die schwierigsten Arten von Angriffen, da sie traditionelle Zuverlässigkeits- und Robustheitsdesignlösungen überwinden können und einen mehrschichtigen Sicherheitsansatz erfordern.

Weiterführende Literatur:

- I. Kawoosa and D. Prashar, "A Review of Cyber Securities in Smart Grid Technology," *2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM)*, Dubai, United Arab Emirates, 2021, pp. 151-156, doi: 10.1109/ICCAKM50778.2021.9357698.

5.9.2. Data Injection Attack (DIA)

Dynamic Data Injection Attacks (DIAs) beziehen sich auf Angriffe, bei denen ein Angreifer manipulierte Daten wie Sensorwerte, Feedback-Control-Signale und Strompreissignale in der Übertragung austauscht. Diese Art von Angriffen kann auf verschiedene Arten durchgeführt werden, wie zum

Beispiel durch Kompromittierung von Hardware-Komponenten oder durch Abfangen von Kommunikationsverbindungen.

Ein typisches Ziel von DIAs sind die Zustandsschätzer-Systeme im Stromnetz. Die Zustände des Stromsystems bestehen aus den Spannungsmagnituden und Phasenwinkeln an jedem Knotenpunkt. Die Schätzung dieser Zustände ermöglicht eine vollständige Überwachung des Strom- und Stromflusses im gesamten Netz. Um diese Zustände zu schätzen, werden Messungen aus dem gesamten Netz gesammelt und einem Zustandsschätzer zugeführt. Eine Manipulation dieser gesammelten Messungen kann zu einer falschen Schätzung des Betriebszustands des Systems führen, was wiederum zu falschen Betriebsmaßnahmen und möglicherweise zur Destabilisierung des Stromsystems führen kann.

Eine besondere Herausforderung bei DIAs besteht darin, dass herkömmliche Mechanismen zur Erkennung fehlerhafter Daten (Bad Data Detection, BDD) nicht in der Lage sind, manipulierte Daten zu erkennen, die geschickt in das System injiziert wurden. Diese Art von Angriffen ist als Stealthy Data Injection Attack Model bekannt und kann die Ergebnisse der Zustandsschätzung manipulieren, ohne dass dies erkannt wird.

Die Auswirkungen von DIAs können je nach Ziel des Angreifers sehr unterschiedlich sein und reichen von falschen Preisen bis hin zur Destabilisierung des gesamten Stromsystems. Manche DIAs haben in erster Linie das Ziel, das System zu beschädigen und sind rein destruktiver Natur, wie es bei terroristischen Angriffen der Fall ist. Zum Beispiel kann ein Angreifer Systemmessungen manipulieren, sodass eine bereits überlastete Übertragungsleitung falsch dargestellt und ihre thermische Übertragungsgrenze als noch nicht erreicht angezeigt wird. Basierend auf diesen falschen Schätzungen würde der Systembetreiber mehr Energie über die Leitung leiten, was zu Überhitzung und Durchhang führt. Dieser Durchhang verringert den Abstand zwischen der Leitung und dem Boden (oder anderen Objekten dazwischen), was zu einem Kurzschluss führen kann. Unter Belastungsbedingungen kann ein solcher Kurzschluss zu großen Schwankungen in den Systemdynamiken führen, die zum Abschalten weiterer Leitungen, zur Trennung von Generatoren, zur Lastabschaltung oder sogar zu einem System-Blackout führen können.

Im Strommarkt können die Marktteilnehmer den Strom zu variablen Preisen kaufen und verkaufen. Um dies zu ermöglichen, wird der Zustand des Stromsystems in Echtzeit geschätzt. Ein erfolgreicher DIA-Angriff kann jedoch diese Schätzung manipulieren und somit die Strompreise beeinflussen. Dadurch kann der Angreifer profitieren, indem er zum Beispiel den Strom teurer einspeisen kann. Dies hat ernsthafte Auswirkungen auf die Integrität des Strommarktes und erfordert eine umfassende Sicherheitsstrategie, um solche Angriffe zu verhindern.

Weiterführende Literatur:

- E. -N. S. Youssef and F. Labeau, "False Data Injection Attacks Against State Estimation in Smart Grids: Challenges and Opportunities," *2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE)*, Quebec, QC, Canada, 2018, pp. 1-5, doi: 10.1109/CCECE.2018.8447683.
- He, H. and Yan, J. (2016), Cyber-physical attacks and defences in the smart grid: a survey. IET Cyber-Physical Systems: Theory & Applications, 1: 13-27. https://doi.org/10.1049/iet-cps.2016.0019

5.9.3. Zeitsynchronisation

Phasoren-Messdaten sind Messwerte, die im Smart Grid verwendet werden, um den Zustand des Stromnetzes in Echtzeit zu überwachen. Es sind numerische Werte, die den Betrag und die Phase des

Stroms oder der Spannung an einem bestimmten Punkt im Netzwerk angeben und in der Regel mit hoher Frequenz erfasst werden. Diese Daten werden verwendet, um den Stromfluss und die Netzwerkstabilität zu überwachen und um automatische Steuerungsfunktionen auszulösen, um das Netzwerk in Echtzeit zu optimieren und zu verwalten.

Phasor Measurement Units (PMUs) sind hochpräzise Messgeräte, die dazu verwendet werden, das Stromnetz in Echtzeit zu überwachen. Diese Geräte sind typischerweise in der Lage, die Phasoren von Spannung und Strom sowie lokale Frequenzen mit hoher Abtastrate zu messen. Da die PMUs über das gesamte Netzwerk verteilt sind, können die gesammelten Messdaten an zentralen Standorten gesammelt und analysiert werden. Um sicherzustellen, dass die Daten korrekt ausgerichtet sind, werden alle PMU-Daten basierend auf einer von einem GPS-Signal bereitgestellten Zeitreferenz synchronisiert.

Ein Angreifer kann jedoch das GPS-Signal fälschen und so die Zeitreferenz der PMUs manipulieren, um falsche Systembedingungen vorzutäuschen und ungenaue Schutz- und Steuerungsmaßnahmen auszulösen. Solche Angriffe werden als Time Synchronization Attacks (TSAs) bezeichnet. Bei TSAs werden die PMUs dazu gezwungen, Proben zu einem falschen Zeitpunkt zu nehmen, was zu Messungen mit falschen Zeitstempeln führt. Diese falschen Messungen können dazu führen, dass das System falsche Entscheidungen trifft und letztendlich zu Fehlfunktionen führt.

Ein Beispiel für die Auswirkungen von TSAs auf das Stromnetz ist der nordamerikanische Nord-ost-Blackout im Jahr 1965. Eine falsche Trennung von Übertragungsleitungen aufgrund falscher Messungen war einer der Hauptauslöser für diesen Blackout. Neuere Untersuchungen haben gezeigt, dass TSAs erhebliche Abweichungen bei der Fehlerlokalisierung verursachen können, die bis zu 180 km für eine Leitungslänge von 400 km betragen können und sogar einen falschen Alarm auslösen können. Ein solcher falscher Alarm kann zur Unterbrechung einer Übertragungsleitung führen, die dann eine Kettenreaktion von Ausfällen im Netz auslösen kann.

Um solche Angriffe zu verhindern, müssen Schutzmechanismen implementiert werden, die sicherstellen, dass die GPS-Signale authentisch sind und nicht gefälscht werden können. Zusätzlich können Technologien wie Blockchain eingesetzt werden, um die Integrität der gesammelten Daten sicherzustellen.

Weiterführende Literatur:

- J. S. Thorp, G. B. Sheble, "Computer applications in power systems", McGraw-Hill, New York, 1996.
- Bin, Q., Ziwen, C., Yong, X., Liang, H. and Sheng, S. (2020), GPS spoofing-based time synchronisation attack in advanced metering infrastructure and its protection. J. Eng., 2020: 809-815.

5.9.4. Beispiele weiterer Angriffsmethoden

Im Folgenden sollen einige weitere Angriffsmethoden diskutiert werden.

Die Verwendung von Malware ist eine Möglichkeit für einen Angreifer, Smart Meter und Server im Smart Grid-Umfeld zu infizieren. Hierbei wird eine Schadsoftware erstellt, die das Verhalten der Geräte oder Systeme beeinflussen kann, indem sie neue Funktionen hinzufügt, sensible Informationen stiehlt oder den Betrieb des Geräts stört oder verändert.

Ein Datenbankangriff ist eine Art von Angriff, bei dem ein Angreifer versucht, auf eine Datenbank zuzugreifen, um Daten abzurufen oder zu manipulieren. Im Kontext von Control-Systemen wird die

Aktivität des Systems in Datenbanken im Control-System-Netzwerk aufgezeichnet und diese Protokolle werden normalerweise in das Business-Netzwerk gespiegelt. Wenn ein Angreifer in der Lage ist, Zugang zu einer unzureichend gesicherten Datenbank im Business-Netzwerk zu erlangen, kann er diese als Sprungbrett nutzen, um auf das Control-System-Netzwerk zuzugreifen. In einem solchen Szenario kann der Angreifer eine Schwachstelle in der Datenbank ausnutzen, um Zugang zu vertraulichen Informationen wie Benutzernamen und Passwörtern zu erhalten. Mit diesen Anmeldedaten kann der Angreifer dann Zugriff auf die Control-Systeme im Netzwerk erhalten und sie entweder stören oder manipulieren, was zu einem Systemausfall oder einer Verletzung der Verfügbarkeit, Integrität oder Vertraulichkeit des Systems führen kann.

Ein Angreifer kann die Kommunikationsausrüstung, wie Multiplexer, Router oder Switches kompromittieren, um direkten Schaden zu verursachen oder sie als Hintertür nutzen, um zukünftige Angriffe zu starten. Kommunikationsausrüstungen wie Multiplexer dienen dazu, die Datenkommunikation zwischen verschiedenen Komponenten des Smart Grids zu ermöglichen. Wenn ein Angreifer Zugriff auf die Kommunikationsausrüstung hat, kann er in der Lage sein, direkt Schaden zu verursachen, indem er beispielsweise wichtige Daten löscht oder die Datenübertragung zwischen wichtigen Komponenten blockiert. Darüber hinaus kann die Kompromittierung der Kommunikationsausrüstung auch als Hintertür genutzt werden, um zukünftige Angriffe auf das Smart Grid durchzuführen. Ein Angreifer kann die Kompromittierung der Kommunikationsausrüstung nutzen, um sich in das Netzwerk zu integrieren und Zugriff auf weitere Systeme und Komponenten zu erlangen. Dies kann es dem Angreifer ermöglichen, vertrauliche Informationen zu stehlen, sensible Daten zu manipulieren oder das System vollständig zu übernehmen.

Ein Beispiel für eine solche Attacke fand 2015 in der Ukraine statt, als ein Hackerangriff auf das Stromnetz des Landes durchgeführt wurde. Die Angreifer schickten gefälschte Befehle an die Stromnetzsteuerung und lösten so einen Stromausfall aus, der Zehntausende von Menschen betraf. Dieser Vorfall zeigte die Verwundbarkeit von Stromnetzen auf der ganzen Welt und die potenziell schwerwiegenden Folgen von Angriffen auf die Strominfrastruktur.

Ein weiteres Beispiel ist die „Hannibal"-Attacke, die im Jahr 2013 gegen die Israel Electric Corporation durchgeführt wurde. Die Angreifer injizierten gefälschte Daten in das SCADA-System des Unternehmens, was zu Überlastungen und anderen Problemen führte. Dieser Vorfall verdeutlichte, wie Angriffe auf die Strominfrastruktur nicht nur finanzielle Auswirkungen, sondern auch Auswirkungen auf die Sicherheit und Stabilität der Stromversorgung haben können.

Die bekanntesten Angriffe auf Geräte selbst ist „Stuxnet". Im Jahr 2011 bestätigte die iranische Regierung, dass das Atomkraftwerk Bushehr angegriffen worden war. Dieser komplexe Angriff wird als Stuxnet bezeichnet und gilt als erste Malware, die kritische Infrastrukturen direkt manipuliert hat. Stuxnet wurde über einen USB-Stick verteilt und infizierte alle Windows-Maschinen im System. Die Angriffsvektoren von Stuxnet betrafen unterschiedliche Teile des Systems. Es wurde speziell für SCADA-Systeme entwickelt, wobei es mindestens vier Schwachstellen des Betriebssystems ausnutzte. Der Angriff führte zur Zerstörung von über tausend iranischen Nuklearzentrifugen. Der Angriff demonstrierte erneut die Bedeutung von Cybersicherheit und wird als das zerstörerische Beispiel einer Cyberwaffe angesehen.

Weiterführende Literatur:

- T. M. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," in *Computer*, vol. 44, no. 4, pp. 91-93, April 2011, doi: 10.1109/MC.2011.115.

- X. Wang and P. Yi, "Security Framework for Wireless Communications in Smart Distribution Grid," in *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 809-818, Dec. 2011, doi: 10.1109/TSG.2011.2167354.
- V. Dhanesh Menon, J. Trilok Kumar, M. Sabhanayagan, A. Ramkumar and K. Rajesh, "Cyber Security for Smart Meters," *2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*, Tamilnadu, India, 2019, pp. 1-5, doi: 10.1109/INCOS45849.2019.8951407.

5.10 Einschränkungen und neue Ansätze

Im Bereich der Cybersicherheit sind Intrusion Detection und Kryptographie wichtige Sicherheitslösungen, die auch im Smart Grid eingesetzt werden können. Allerdings ist das Smart Grid ein komplexes, dezentralisiertes System, das maßgeschneiderte Sicherheitslösungen erfordert. Ein wichtiges Anliegen im Smart Grid ist die Integrität von Datenströmen in Echtzeit, was die Anwendung einiger Kryptographielösungen, die bei der Speicherung oder Übertragung von Daten verwendet werden, einschränken kann. Ein weiteres Problem ist, dass einige klassische Sicherheitslösungen zu viel Overhead hinzufügen können, was zu Latenzproblemen führen kann mit der Gefahr, die Betriebsfähigkeit des Smart Grids zu beeinträchtigen. Deshalb ist es wichtig, Sicherheitslösungen zu entwickeln, die speziell auf die Bedürfnisse des Smart Grids zugeschnitten sind und die Integrität und Betriebsfähigkeit des Systems nicht beeinträchtigen.

Weiterführende Literatur:

- V. Delgado-Gomes, J. F. Martins, C. Lima and P. N. Borza, "Smart grid security issues," *2015 9th International Conference on Compatibility and Power Electronics (CPE)*, Costa da Caparica, Portugal, 2015, pp. 534-538, doi: 10.1109/CPE.2015.7231132.
- P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," in *IEEE Security & Privacy*, vol. 7, no. 3, pp. 75-77, May-June 2009, doi: 10.1109/MSP.2009.76

5.10.1. Physikalische Systeme

Um das Smart Grid effektiv zu schützen, müssen Sicherheitslösungen entwickelt werden, die sowohl die Cyber- als auch die physischen Aspekte des Systems berücksichtigen. Diese Sicherheitslösung integriert Cyber-Sicherheitsmaßnahmen mit physischen Sicherheitsmaßnahmen, um das Smart Grid vor Angriffen zu schützen. Ein wichtiger Aspekt der Smart Grid-Sicherheit ist die Erkennung von Anomalien. Eine erfolgreiche Erkennung von Anomalien erfordert jedoch eine genaue Kenntnis des normalen Betriebs des Systems und eine kontinuierliche Überwachung. Ein Beispiel für eine solche Überwachungslösung ist, wie schon oben beschrieben, die Verwendung von Phasor Measurement Units (PMUs), die hochpräzise Messungen des Zustands des Stromsystems liefern und somit Anomalien schnell erkennen können.

5.10.2. Risk Management durch Simulation

In einem physischen System wie dem Smart Grid ist die Analyse der Ausbreitung von Angriffen komplexer als in einem reinen Cyber-System. Im Gegensatz zu einem Cyber-System besteht das Smart Grid aus physischen Komponenten wie Generatoren, Übertragungsleitungen, Umspannstationen, Schaltern und Verteilernetzen, die miteinander interagieren und von verschiedenen Faktoren beeinflusst werden. Wenn ein Angriff auf eine Komponente stattfindet, kann er sich auf andere

Komponenten ausbreiten und das gesamte System destabilisieren. Die Ausbreitung von Fehlern und Störungen im System hängt von verschiedenen Faktoren wie Laständerungen, Wetterbedingungen und anderen dynamischen Faktoren ab und kann sich auf unvorhersehbare Weise verstärken.

Die Analyse der Ausbreitung von Angriffen erfordert daher eine umfassende Modellierung und Simulation der physikalischen Komponenten des Smart Grids und deren Interaktionen, um die möglichen Auswirkungen auf das System zu verstehen. Die Modellierung und Simulation sollten auch mögliche Ausweichszenarien und alternative Reaktionspläne des Systems berücksichtigen. Solche Analysen können dazu beitragen, Schwachstellen im System zu identifizieren und mögliche Gegenmaßnahmen zu entwickeln, um Angriffe zu verhindern oder abzuschwächen.

Weiterführende Literatur:

- J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen, and Y. Xiang, “Deep learning based attack detection for cyber-physical system cybersecurity: a survey,” IEEE/CAA J. Autom. Sinica, vol. 9, no. 3, pp. 377–391, Mar. 2022. doi: 10.1109/JAS.2021.1004261
- Q. Liu, V. Hagenmeyer and H. B. Keller, "A Review of Rule Learning-Based Intrusion Detection Systems and Their Prospects in Smart Grids," in *IEEE Access*, vol. 9, pp. 57542-57564, 2021, doi: 10.1109/ACCESS.2021.3071263.

5.10.3. Zuverlässigkeit

Durch die zunehmende Vernetzung von sehr vielen Komponenten im Smart Grid und den Einsatz von vielen verschiedenen IT-Systemen und -Technologien wird das Netzwerk anfälliger für Cyberangriffe. Ein koordinierter Angriff (CA) kann dabei verschiedene Komponenten und Systeme im Smart Grid gleichzeitig angreifen und so zu einem flächendeckenden Ausfall führen. Das CA-Szenario wird oft bei der Entwicklung von Sicherheitsstrategien für das Smart Grid vernachlässigt, da es als sehr unwahrscheinlich gilt. Jedoch können Cyberangriffe von gut finanzierten, staatlichen oder nichtstaatlichen Akteuren durchgeführt werden, die über Ressourcen und Kenntnisse verfügen, um einen solchen koordinierten Angriff durchzuführen.

Daher ist es wichtig, bei der Entwicklung von Zuverlässigkeitsdesigns für das Smart Grid auch das CA-Szenario zu berücksichtigen und entsprechende Maßnahmen zur Minimierung des Risikos eines solchen Angriffs zu ergreifen.

Weiterführende Literatur:

- W. Zhaoyang, L. Caihua, X. Zuibing and J. Mengqiang, "Reliability evaluation of cyber-physical system considering integration of power and communication risk," 2021 International Conference on Power System Technology (POWERCON), Haikou, China, 2021, pp. 1883-1888, doi: 10.1109/POWERCON53785.2021.9697864.
- S. Chren, "Towards Multi-layered Reliability Analysis in Smart Grids," *2017 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, Toulouse, France, 2017, pp. 116-119, doi: 10.1109/ISSREW.2017.67.

5.10.4. Modellbasierte Lösungen

Konventionelle Sicherheitsanalysen der Regelungstechnik beschäftigen sich hauptsächlich mit der Gestaltung robuster Regelungen, die operative Anforderungen auch bei exogenen Störungen

aufrechterhalten können. Solche Analysen berücksichtigen jedoch nicht explizit die Cyber-Sicherheit und alle damit verbundenen Bedrohungen, die ein CPS wie das Smart Grid beeinträchtigen können.

Es ist daher notwendig, spezielle Analysemethoden zu entwickeln, die die Wechselwirkungen zwischen den beiden Layern des cyber-physikalischen Systems berücksichtigen und somit eine umfassende Sicherheitsanalyse ermöglichen.

Eine solche Analyse erfordert eine ganzheitliche Betrachtung von Sicherheitsaspekten sowohl auf der Cyber- als auch auf der physischen Ebene. Die Entwicklung solcher Methoden erfordert eine tiefgreifende Kenntnis der komplexen Wechselwirkungen zwischen den verschiedenen Komponenten des Smart Grids sowie der damit verbundenen Risiken und Bedrohungen. Ein Ansatz, der in der Literatur vorgeschlagen wird, ist die Verwendung von Modellen, die die Interaktionen zwischen den verschiedenen Komponenten des Smart Grids sowie die Auswirkungen von Angriffen auf diese Komponenten modellieren. Solche Modelle ermöglichen es, potenzielle Schwachstellen im System zu identifizieren und geeignete Gegenmaßnahmen zu entwickeln.

Um die Wirksamkeit von Sicherheitsmaßnahmen zu evaluieren, müssen verschiedene Szenarien von Angriffen und Störungen modelliert werden. Dazu gehören nicht nur Cyber-Angriffe, sondern auch Naturkatastrophen und andere unvorhergesehene Ereignisse. Eine solche Simulation erfordert auch die Entwicklung von Werkzeugen und Methoden zur Überwachung des Systems in Echtzeit, um schnell auf Angriffe oder Störungen reagieren zu können.

Die Entwicklung von robusten und sicheren Regelungssystemen für das Smart Grid erfordert auch die Zusammenarbeit von Experten aus verschiedenen Bereichen, einschließlich Ingenieuren, Informatikern und Sicherheitsexperten. Eine solche Zusammenarbeit ist notwendig, um sicherzustellen, dass alle Aspekte der Sicherheit und Zuverlässigkeit des Smart Grids berücksichtigt werden und dass geeignete Gegenmaßnahmen entwickelt werden können, um Angriffe und Störungen zu verhindern oder abzuschwächen.

Weiterführende Literatur:

- U. Khare, A. Malviya, S. Kumar Gawre and A. Arya, "Cyber Physical Security of a Smart Grid: A Review," *2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, Bhopal, India, 2023, pp. 1-6, doi: 10.1109/SCEECS57921.2023.10062966.
- Q. Li *et al*., "A Risk Assessment Method of Smart Grid in Cloud Computing Environment Based on Game Theory," *2020 IEEE 5th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA)*, Chengdu, China, 2020, pp. 67-72, doi: 10.1109/ICCCBDA49378.2020.9095625.
- O. Ur-Rehman and N. Zivic, "Secure Design Patterns for Security in Smart Metering Systems," *2015 IEEE European Modelling Symposium (EMS)*, Madrid, Spain, 2015, pp. 278-283, doi: 10.1109/EMS.2015.49.

5.10.5. Performance Tradeoff

Das Smart Grid ist ein CPS, das aus einer Vielzahl von physikalischen Komponenten besteht, die miteinander interagieren und von verschiedenen Faktoren wie Laständerungen und Wetterbedingungen beeinflusst werden. Daher ist es für das Smart Grid entscheidend, dass jede Sicherheitslösung nahtlos in das Netz integriert werden kann, ohne die Betriebs- und Leistungsfähigkeit zu beeinträchtigen.

Die Integration von Sicherheitslösungen in das Smart Grid erfordert daher ein tiefes Verständnis der Architektur des Netzes und seiner betrieblichen Anforderungen, sowie der eingesetzten Technologien und Protokolle. Es müssen Lösungen entwickelt werden, die die Sicherheitsanforderungen des Netzes erfüllen und gleichzeitig die Leistung des Netzes nicht beeinträchtigen.

Die Kompromisse zwischen Sicherheit und Leistung im Smart Grid sind in der Tat ausgeprägter als in anderen Netzwerken. Die vollständige Eliminierung von Wireless- und Internetverbindungen würde das Smart Grid zwar sicherer machen, aber auch alle wirtschaftlichen und operativen Vorteile nehmen, die eine moderne Cyber-Infrastruktur bietet. Daher müssen Sicherheitsstrategien so entwickelt werden, dass sie sowohl den Schutz des Netzes als auch seine betriebliche Effizienz berücksichtigen. Dies erfordert die Entwicklung von maßgeschneiderten Sicherheitslösungen, die die spezifischen Anforderungen des Smart Grid erfüllen und gleichzeitig die Leistung des Netzes nicht beeinträchtigen.

5.10.6. Alterung von Komponenten

Die Tatsache, dass die meisten Komponenten des Smart Grids vor der Integration des Cyber-Layer entworfen wurden, führt zu mehreren Herausforderungen in Bezug auf die Sicherheit. Zum Beispiel wurden viele der älteren Komponenten ohne Berücksichtigung der Notwendigkeit von Software-Updates und -Patches entwickelt. Diese älteren Systeme verwenden möglicherweise veraltete oder unsichere Protokolle und Betriebssysteme, die anfällig für bekannte Schwachstellen und Exploits sind. Es kann schwierig sein, solche Systeme zu patchen oder zu aktualisieren, da viele von ihnen kritische Funktionen im Stromnetz übernehmen und eine unvorhergesehene Downtime verursachen können. Darüber hinaus können Patches und Updates zu Kompatibilitätsproblemen führen, wenn sie nicht sorgfältig getestet und validiert werden. In einigen Fällen können Patches sogar zu neuen Sicherheitsbedrohungen führen, wenn sie nicht vollständig implementiert oder konfiguriert werden.

Daher erfordert die Sicherung des Smart Grids eine gründliche Prüfung und Bewertung aller Komponenten und deren Interaktionen, um potenzielle Schwachstellen zu identifizieren und Sicherheitslücken zu schließen, ohne die Leistung des Systems zu beeinträchtigen. Die Sicherheitslösungen sollten auch mit älteren Systemen kompatibel sein und eine nahtlose Integration in das vorhandene System ermöglichen.

Weiterführende Literatur:

- H. J. Dcruz and B. Kaliaperumal, "Analysis of Cyber-Physical Security in Electric Smart Grid: Survey and challenges," *2018 6th International Renewable and Sustainable Energy Conference (IRSEC)*, Rabat, Morocco, 2018, pp. 1-6, doi: 10.1109/IRSEC.2018.8702957.

5.11 Sicherheitslösungen

Nachdem verschiedene Bedrohungen und Herausforderungen des Stromnetzsystems identifiziert wurden, soll nun ein Ansatz für die operationale Sicherheit bereitgestellt werden.

Sicherheitslösungen, die für herkömmliche IT-Netzwerke entwickelt wurden, sind in Smart Grid-Netzwerken aufgrund der großen Unterschiede zwischen beiden Infrastrukturen nicht effektiv. Ihre Sicherheitsziele unterscheiden sich dahingehend, dass die Sicherheit in IT-Netzwerken darauf abzielt, die drei Sicherheitsprinzipien (Vertraulichkeit, Integrität und Verfügbarkeit) durchzusetzen, während die Sicherheit in Automatisierungsnetzwerken (Smart-Grid) zusätzlich darauf abzielt, menschliche Sicherheit, Schutz von Ausrüstung und Stromleitungen sowie Systembetrieb zu gewährleisten. Somit

unterscheidet sich die Sicherheitsarchitektur von IT-Netzwerken von der des Smart Grid-Netzwerks erheblich.

Auch ihre zugrunde liegende Topologie ist unterschiedlich, da IT-Netzwerke eine eingeschränkte Menge von Betriebssystemen (OS) und Protokollen verwenden, während Automatisierungsnetzwerke proprietäre OS und Protokolle spezifischer Anbieter verwenden. Schließlich unterscheiden sich ihre Quality of Service (QoS)-Metriken dahingehend, dass es in IT-Netzwerken akzeptabel ist, Geräte im Falle von Fehlern oder Upgrades neu zu starten, während dies in Automatisierungsnetzwerken nicht akzeptabel ist, da die Dienste jederzeit verfügbar sein müssen.

Aufgrund der erheblichen Unterschiede zwischen den IT- und den Netzwerksicherheitszielen müssen angepasste Sicherheitslösungen speziell für das Smart Grid-Netzwerk entwickelt werden.

Weiterführende Literatur:

- Wei, D., Lu, Y., Jafari, M., Skare, P. M., & Rohde, K. (2011). Protecting smart grid automation systems against cyberattacks. *IEEE-Transactions on Smart Grid*, *2*(4), 782-795. [6003813]. https://doi.org/10.1109/TSG.2011.2159999

5.11.1. Cyber Physische Systeme

Sicherheitslösungen für Cyber-Physische Systeme (CPS) sind durch ihre physische Komponente im Vergleich zu herkömmlichen Cyber-Infrastrukturen erheblich komplexer. Das erhöht nicht nur den Aufwand für potenzielle Angreifer, sondern stellt auch eine Herausforderung für die Verteidigung dar. Die physische Komponente von CPS bringt zusätzliche Sicherheitsanforderungen mit sich, die von reinen Cyber-Infrastrukturen nicht erfasst werden, wie beispielsweise die Kontinuität der Stromversorgung und die Genauigkeit der dynamischen Preisgestaltung. Diese Anforderungen sind eng mit den Modellen und Zuständen des physischen Systems verknüpft und können allein durch Informationssicherheit schwer zu bewältigen sein.

Um CPS effektiv zu schützen, müssen Sicherheitslösungen sowohl die physische als auch die cybertechnische Ebene berücksichtigen. Techniken wie Schlüsselverwaltung, sichere Kommunikation und Intrusion Detection Systems, die auch in herkömmlichen Cyber-Infrastrukturen eingesetzt werden, sind auch für CPS relevant. Allerdings müssen sie um spezifische Aspekte von CPS erweitert werden, um die physischen Komponenten und deren Interaktionen zu berücksichtigen.

Ein Beispiel für die Herausforderungen, die sich aus der Kombination von physischen und cybertechnischen Komponenten ergeben, ist die Notwendigkeit, die Kontinuität der Stromversorgung sicherzustellen. Dazu müssen sowohl die elektrischen als auch die IT-Komponenten des Systems synchronisiert werden, um sicherzustellen, dass das System auch bei Störungen weiterhin stabil läuft. Das erfordert eine umfassende Modellierung und Simulation, um das Verhalten des physischen Systems zu verstehen und geeignete Sicherheitsmaßnahmen zu ergreifen.

Insgesamt erfordert die Sicherheit von CPS eine holistische Betrachtung der physischen und cybertechnischen Aspekte des Systems sowie die Integration von Sicherheitsmaßnahmen, die spezifisch für CPS sind.

Weiterführende Literatur:

- Sadeghi, A.-R., Wachsmann, C., & Waidner, M. (2015). *Security and privacy challenges in industrial internet of things. Proceedings of the 52nd Annual Design Automation Conference on - DAC '15.* doi:10.1145/2744769.2747942

- H. Abbas, "Keynote Speaker 5: Cyber Security Threat Landscape in the Context of Industry 4.0," *2022 15th International Conference on Security of Information and Networks (SIN)*, Sousse, Tunisia, 2022, pp. 1-1, doi: 10.1109/SIN56466.2022.9970503.

5.11.2. Basis von Smart Grid Security

Eine Smart Grid Security-Lösung besteht aus einer Kombination von IT- und OT-Sicherheitslösungen, um sowohl Benutzer- als auch Betriebsdaten zu schützen. Die Sicherheitsziele für Benutzerdaten betreffen die Vertraulichkeit und Integrität der Daten, um eine Verletzung der Privatsphäre zu vermeiden. Hierfür werden Verschlüsselungstechnologien, Authentifizierung und Zugriffskontrolle eingesetzt, um sicherzustellen, dass nur autorisierte Benutzer auf die Daten zugreifen können. Betriebs- und Wartungsdaten hingegen müssen auf höchstem Sicherheitsniveau geschützt werden, da Angriffe auf diese Daten zu Stromausfällen und anderen Schäden führen können.

Um Betriebsdaten zu schützen, sind Technologien wie Intrusion Detection und Präventionssysteme, Firewall-Systeme und Anomalieerkennung erforderlich, um verdächtige Aktivitäten zu erkennen und zu verhindern. Um eine integrierte OT-Sicherheitslösung zu schaffen, muss eine sichere Kommunikationsarchitektur bereitgestellt werden, die den sicheren Austausch von Daten zwischen Geräten ermöglicht.

Eine erfolgreiche Smart Grid Security-Lösung erfordert daher eine Integration von IT- und OT-Sicherheitslösungen sowie eine ganzheitliche Risikobewertung, die die physischen und logischen Komponenten des Smart Grid-Systems berücksichtigt. Das Ziel ist es, die gesamte Smart Grid-Infrastruktur zu schützen, indem sowohl IT- als auch OT-Sicherheitslösungen integriert und verwaltet werden.

Weiterführende Literatur:

- Farhangi, H. (2010). *The path of the smart grid. IEEE Power and Energy Magazine, 8(1), 18–28.* doi:10.1109/mpe.2009.934876
- A. -R. Sadeghi, C. Wachsmann and M. Waidner, "Security and privacy challenges in industrial Internet of Things," *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, San Francisco, CA, USA, 2015, pp. 1-6, doi: 10.1145/2744769.2747942.

CIA - Security-Prinzipien
Die drei primären Sicherheitsziele aller Kommunikationsnetzwerke sind Vertraulichkeit, Integrität und Verfügbarkeit von Daten. Vertraulichkeit bedeutet den Schutz personenbezogener Daten vor unbefugtem Zugriff. Die Integrität von Daten stellt sicher, dass sie korrekt sind. Die Verfügbarkeit von Diensten stellt sicher, dass die Dienste zugänglich sein werden.

In herkömmlichen Kommunikationsnetzwerken ist die Bedeutung der Sicherheitsanforderungen in der Reihenfolge von CIA (Vertraulichkeit, Integrität und Verfügbarkeit), während in Smart Grid-Netzwerken die Bedeutung der Anforderungen in der Reihenfolge von AIC (Verfügbarkeit, Integrität und Vertraulichkeit) liegt. Um die CIA-Triade im Smart Grid zu schützen, gibt es verschiedene Lösungsansätze. Eine Möglichkeit besteht darin, eine mehrschichtige Sicherheitsarchitektur mit sicheren Kommunikationskanälen bereitzustellen.

Weiterführende Literatur:

- M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A Survey on Smart Grid Cyber-Physical System Testbeds

- M. Z. Gunduz and R. Das, "A comparison of cyber-security-oriented testbeds for IoT-based smart grids," *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, Antalya, Turkey, 2018, pp. 1-6, doi: 10.1109/ISDFS.2018.8355329.
- P. Haji Mirzaee, M. Shojafar, H. Cruickshank and R. Tafazolli, "Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and Countermeasures)," in *IEEE Access*, vol. 10, pp. 52922-52954, 2022, doi: 10.1109/ACCESS.2022.3174259.

Verfügbarkeit (Availability)

Die Verfügbarkeit ist eine entscheidende Anforderung für die Sicherheit in Smart Grids. Verfügbarkeit in Smart Grids kann in verschiedene Aspekte aufgeteilt werden, insbesondere die Verfügbarkeit von Preisinformationen, Befehlen und Steuerungsnachrichten. Der Verlust von Steuerungsnachrichten oder der Zugänglichkeit des Datenstroms kann sich auf die Wirkungsweise der Stromverteilung und des Systems auswirken. Die Generatoren im Smart Grid sind mit lokalen und globalen Kontrollsystemen ausgestattet, die ein dreischichtiges Design verwenden, um eine konstante Winkelgeschwindigkeit zu gewährleisten. Das Smart Grid besteht aus einer Verbindung vieler Stromsysteme, die über Leitungsschaltungen verbunden sind, und die dynamische Stabilität des Netzes hängt wesentlich von der Verfügbarkeit der Sensor-Messungen und Kontrollsignale ab. DoS-Angriffe können das primäre Kontrollsignal blockieren, was zur Abschaltung des Generators durch ein Überspannungsrelais führen kann. Lösungsansätze zur Gewährleistung der Verfügbarkeit von Smart Grids bei DoS/DDoS-Angriffen und anderen Bedrohungen der Cyber Security wurden in verschiedenen Studien untersucht. Es sind spezielle Schutzmaßnahmen erforderlich, um die Verfügbarkeit von Smart Grids zu gewährleisten und den Betrieb stabil zu halten.

Weiterführende Literatur:

- Wang, W., & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. *Computer networks*, *57*(5), 1344-1371. DOI:
- More, S., Hajari, S., Majeed, M.A., Singh, N.K., Mahajan, V. (2022). Cyber Security for Smart Grid: Vulnerabilities, Attacks, and Solution. In: Mahajan, V., Chowdhury, A., Padhy, N.P., Lezama, F. (eds) Sustainable Technology and Advanced Computing in Electrical Engineering. Lecture Notes in Electrical Engineering, vol 939. Springer, Singapore. https://doi.org/10.1007/978-981-19-4364-5_60

Integrität (Integrity)

Die Integrität von Daten im Smart Grid ist von zentraler Bedeutung, da sie die Grundlage für effiziente und sichere Energieversorgung bildet. Insbesondere bei Preisinformationen ist die Integrität von größter Bedeutung. Wenn beispielsweise ein Angreifer negative Preise in das System einspeist, könnten zahlreiche Geräte gleichzeitig eingeschaltet werden, um von dem niedrigen Preis zu profitieren. Dies würde zu einem plötzlichen Anstieg des Stromverbrauchs führen, der zu Netzwerküberlastungen führen kann. Um dieses Problem zu lösen, müssen Mechanismen implementiert werden, um die Integrität der Preisinformationen zu schützen.

Eine Möglichkeit, die Integrität von Preisinformationen zu schützen, besteht darin, digitale Signaturen zu verwenden, um die Authentizität und Unveränderbarkeit von Daten zu gewährleisten. Dieser Ansatz kann dazu beitragen, die Datenintegrität zu schützen, indem sie sicherstellen, dass die Daten von einer vertrauenswürdigen Quelle stammen und dass sie seit der Erstellung nicht manipuliert wurden. Zertifikate und öffentliche Schlüssel können ebenfalls verwendet werden, um die Authentizität von

Daten und Geräten zu überprüfen und sicherzustellen, dass nur autorisierte Benutzer auf das System zugreifen.

Ein weiterer Lösungsansatz zur Sicherung der Integrität von Daten im Smart Grid ist die Implementierung von Anomalie-Erkennungssystemen, die verdächtige Aktivitäten in Echtzeit erkennen und darauf reagieren können, bevor sie zu größeren Problemen führen.

Weiterführende Literatur:

- J. Wei, "A data-driven cyber-physical detection and defense strategy against data integrity attacks in smart grid systems," *2015 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Orlando, FL, USA, 2015, pp. 667-671, doi: 10.1109/GlobalSIP.2015.7418280.
- S. Kher, V. Nutt, D. Dasgupta, H. Ali and P. Mixon, "A detection model for anomalies in smart grid with sensor network," *2012 Future of Instrumentation International Workshop (FIIW) Proceedings*, Gatlinburg, TN, USA, 2012, pp. 1-4, doi: 10.1109/FIIW.2012.6378345.

Vertraulichkeit (Confidentiality)
Vertraulichkeit stellt sicher, dass die gespeicherten und übertragenen Daten nur von den relevanten Empfängern abgerufen werden können. Vertraulichkeit verhindert auch, dass unbefugte Benutzer auf Daten zugreifen, um die persönliche Privatsphäre und Sicherheit zu schützen. Smart Grids übertragen Daten, von Verbrauchsdaten bis hin zu kundenspezifischen Daten, mit unterschiedlichen Sensitivitäts- und Datenschutzniveaus. Verbrauchsdaten eines Endbenutzers sollten nur dem Endbenutzer und dem Energieversorger bekannt sein. Das Erfassen von Steuerbefehlen oder Datenströmen durch Angreifer kann das System gefährden. Vertraulichkeit bezieht sich daher auf die Offenlegung sensitiver Daten für unbefugte Benutzer.

Aus der Perspektive eines Smart Grids bezieht sich dies auf den Datenschutz von Kundendaten, Strommarktdaten und kritischen Unternehmensdaten. Eine Verletzung der Vertraulichkeit führt eventuell zur Offenlegung von privaten Daten und damit einer Verletzung der DSGVO. Mit der zunehmenden Zugänglichkeit von Kundendaten im Internet wird Vertraulichkeit daher immer wichtiger. Die Vertraulichkeit von Messdaten ist wichtig, da Verbrauchsdaten Informationen über das Nutzungsverhalten einzelner Geräte liefern können, was durch nicht invasive Überwachung der Geräteaktivitäten Rückschlüsse auf persönliche Aktivitäten zulässt. Die Vertraulichkeit von Preisinformationen und Steuerbefehlen ist nicht wichtig, wenn sie bereits öffentlich bekannt sind.

Lösungsansätze zur Wahrung der Vertraulichkeit können Verschlüsselungs- und Zugangskontrollmechanismen beinhalten. Durch die Verschlüsselung von Daten kann verhindert werden, dass unbefugte Benutzer darauf zugreifen und sensible Informationen abfangen. Zugangskontrollmechanismen können sicherstellen, dass nur autorisierte Benutzer auf die Daten zugreifen können. Außerdem kann die Anonymisierung von Daten die Privatsphäre schützen, indem sie die Identität von Endbenutzern verschleiert.

Weiterführende Literatur:

- Yang, Y., McLaughlin, K., Littler, T., Sezer, S., Gyu Im, E., Pranggono, B., & Wang, H. (2012). Man-in-the-Middle Attack Test-bed Investigating Cyber-security Vulnerabilities in Smart Grid SCADA Systems. In *Proceedings of the International Conference on Sustainable Power Generation (SUPERGEN 2012)* (611 CP ed., Vol. 2012)

- N. Komninos, E. Philippou and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933-1954, Fourthquarter 2014, doi: 10.1109/COMST.2014.2320093.

Weitere Security-Herausforderungen
Smart Grids sind anfällig für weitere Sicherheitsbedrohungen und Herausforderungen wie Diebstahl, Terrorismus und Naturkatastrophen. Diese Bedrohungen können zu Stromausfällen, IT-Infrastrukturausfällen, beschädigten Verbrauchergeräten, Energiemarktchaos und gefährdeter menschlicher Sicherheit führen.

Einige wichtige Sicherheitsziele für Smart Grids umfassen Authentifizierung, Autorisierung, nicht Abstreitbarkeit, Zugangskontrolle, Auditing, Zuverlässigkeit/Konsistenz und Rechenschaftspflicht. Lösungsansätze zur Verbesserung der Sicherheit und Widerstandsfähigkeit von Smart Grids umfassen verschiedene Techniken und Aspekte, wie z. B. die Verwendung von kryptografischen Technologien, die Implementierung von Zugangskontrollen, die Schulung von Benutzern und Administratoren sowie die Überwachung und Auswertung von Sicherheitsereignissen.

Authentifizierung ist der Prozess der Überprüfung der Identität eines Benutzers oder Geräts, um unbefugten Zugriff zu verhindern. Autorisierung stellt sicher, dass ein authentifiziertes Objekt oder eine Person vorbestimmte Rechte hat, um bestimmte Operationen auf bestimmten Ressourcen durchzuführen. Die nicht Abstreitbarkeit gewährleistet, dass eine bestimmte Aktion, die von einem System oder Benutzer durchgeführt wurde, später nicht bestritten werden kann.

Die Auditierung bezieht sich auf die systematische Bewertung der Sicherheit eines Informations-systems durch die Messung, wie gut es zu einem Satz etablierter Kriterien passt. Zuverlässigkeit/Konsistenz und Rechenschaftspflicht gewährleisten, dass das System zuverlässig und konsistent arbeitet und dass die Benutzer für ihre Handlungen zur Rechenschaft gezogen werden können.

Weiterführende Literatur:

- H. Farhangi, "The path of the smart grid," in *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18-28, January-February 2010, doi: 10.1109/MPE.2009.934876.
- Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. F. Wang, "Impact of cyber-security issues on Smart Grid," *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, Manchester, UK, 2011, pp. 1-7, doi: 10.1109/ISGTEurope.2011.6162722.

5.11.3. Sicherheitsarchitektur

Eine effektive Sicherheitsarchitektur für Smart Grids muss Schlüsseleigenschaften umfassen, die insbesondere in Bezug auf die Widerstandsfähigkeit gegen Störungen, Angriffe und Naturkatastrophen von Bedeutung sind. Die wichtigste Eigenschaft für die Sicherheit von Smart Grids ist laut US-Energieministerium (DoE) die Fähigkeit, während solcher Ereignisse weiterhin zuverlässig zu arbeiten.

Die Konstruktion einer hoch widerstandsfähigen Kommunikationsarchitektur ist hierbei von entscheidender Bedeutung, um Angriffe zu minimieren und eine hohe Verfügbarkeit zu er-reichen. Dies erfordert die Entwicklung von Mechanismen zur Sicherstellung der Zuverlässigkeit und Resilienz von intelligenten Netzen, um Bedrohungen durch Cyber-Sicherheitsrisiken abzuwehren. Um diese Maßnahmen umzusetzen, bedarf es einer umfassenden und integrierten Herangehensweise, bei der Experten aus verschiedenen Bereichen zusammenarbeiten müssen. Eine mögliche Lösung ist die

Integration von Sicherheitsmaßnahmen in die Netzwerkinfrastruktur selbst. Dazu können intelligente Sensoren eingesetzt werden, die Anomalien erkennen und Alarme auslösen, sowie Algorithmen zur Verarbeitung großer Datenmengen in Echtzeit. Eine solche Architektur würde es ermöglichen, Bedrohungen und Anomalien schnell zu erkennen und darauf zu reagieren, bevor sie das System beeinträchtigen können.

Insgesamt muss eine Smart Grid Security Architecture die Resilienz und Zuverlässigkeit der Systeme in Echtzeit sicherstellen, um Bedrohungen und Angriffe auf intelligente Netze abzuwehren und gleichzeitig die Stabilität des Netzes und die Versorgungssicherheit zu gewährleisten.

Weiterführende Literatur:

- *Smart Grid System Report 2018 Report to Congress*. (2018).
- Buchholz, B., Styczynski, Z. (2020). Modern Technologies and the Smart Grid Challenges in Transmission Networks. In: Smart Grids. Springer, Berlin, Heidelberg.

Sichere Kommunikation
Eine sichere Kommunikationsarchitektur für Smart Grids ist wichtig, um das System widerstandsfähig gegen Angriffe und Störungen zu machen. Die Netzwerktopologie muss hochresilient sein, um sicherzustellen, dass das Netzwerk Angriffen standhalten kann. Routing-Protokolle müssen gesichert werden, da ein einzelner kompromittierter Router die gesamte Netzwerkkommunikation beeinträchtigen kann. Daten müssen vertraulich und authentisch sein, um sicherzustellen, dass nur autorisierte Personen Zugriff darauf haben und unerlaubte Änderungen verhindert werden. Einfache, reduzierte Protokolle können erforderlich sein, um eine effiziente Kryptographie für Low-Power-Geräte zu ermöglichen. Sicheres Broadcasting ist wichtig, um die Authentizität von übertragenen Informationen sicherzustellen und Manipulationen von Preisen und Spitzen im Stromverbrauch zu verhindern. Abwehrmaßnahmen gegen Denial-of-Service-Attacken und Jamming sind ebenfalls notwendig, um eine ununterbrochene Kommunikation zu gewährleisten.

Jamming bezieht sich auf eine Art von Cyber-Angriff, bei dem ein Angreifer eine Funkfrequenz stört oder blockiert, um die drahtlose Kommunikation zu unterbrechen oder zu verhindern. Dies kann durch das Senden von störenden Signalen auf der gleichen Frequenz geschehen, auf der die drahtlose Kommunikation stattfindet, was zu einer Überlastung des Kommunikationskanals führt und die Übertragung von Daten unmöglich macht. Jamming kann auf verschiedenen Frequenzbändern durchgeführt werden, einschließlich des WLAN-Bands oder des Mobilfunkbands.

Insgesamt erfordert die Entwicklung einer sicheren Kommunikationsarchitektur für Smart Grids ein umfassendes Konzept, das den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Daten sowie die Widerstandsfähigkeit des Systems gegen Angriffe und Störungen sicherstellt.

Weiterführende Literatur:

- Liu, Y., Chen, H. H., & Wang, L. (2017). Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges. *IEEE Communications Surveys and Tutorials*, *19*(1), 347–376.

- Z. Pourmirza and A. Srivastava, "Cybersecurity Analysis for the Communication Protocol in Smart Grids," *2020 IEEE 8th International Conference on Smart Energy Grid Engineering (SEGE)*, Oshawa, ON, Canada, 2020, pp. 58-63, doi: 10.1109/SEGE49949.2020.9182015.

Software Defined Networking

SDN steht für Software Defined Networking und bezeichnet eine Netzwerkarchitektur, bei der die Steuerungslogik des Netzwerks von der physischen Netzwerkhardware getrennt ist. In herkömmlichen Netzwerken ist die Steuerungslogik in der Netzwerkhardware eingebettet, was zu einer begrenzten Flexibilität bei der Konfiguration und Verwaltung des Netzwerks führt. SDN bietet dagegen eine zentralisierte Steuerung des Netzwerks über eine Software-Schnittstelle, die als SDN-Controller bezeichnet wird.

Durch die Trennung von Steuerungslogik und physischer Netzwerkhardware kann die Netzwerk-konfiguration und -verwaltung flexibler gestaltet werden. Änderungen an der Netzwerkkonfiguration können zentral vom SDN-Controller gesteuert werden, ohne dass Eingriffe in die physische Hardware notwendig sind. Dadurch können Netzwerke schneller und effizienter an neue Anforderungen angepasst werden.

Ein weiterer Vorteil von SDN ist die Möglichkeit, die Datenverkehrssteuerung in Echtzeit zu opti-mieren. Der SDN-Controller kann den Netzwerkverkehr basierend auf verschiedenen Parametern, wie z. B. Datenmenge, Zieladresse oder Priorität, steuern und optimieren. Dadurch können Netzwerkprobleme schneller erkannt und behoben werden, was zu einer verbesserten Leistung und Zuverlässigkeit des Netzwerks führt. SDN wird in verschiedenen Anwendungen eingesetzt, wie beispielsweise Netzwerkmanagement, Optimierung der Dienstqualität (QoS) und Verbesserung der Systemsicherheit.

In Smart Grids kann SDN eingesetzt werden, um die Kommunikation zwischen verschiedenen Komponenten des Netzes, wie beispielsweise Smart Meter, Übertragungsleitungen und Verteilungsnetzen, zu verbessern und zu optimieren. Eine Studie von S. Yang et al. untersuchte die Vorteile von SDN für Smart Grids und zeigte, dass SDN eine flexible Netzwerkkonfiguration ermöglicht, die sich schnell an neue Anforderungen und Änderungen im Netzwerk anpassen kann. SDN könnte auch dazu beitragen, die Widerstandsfähigkeit des Netzwerks zu verbessern, indem es die Implementierung von Sicherheitsrichtlinien vereinfacht und die schnelle Erkennung und Reaktion auf Angriffe ermöglicht. Eine weitere Studie von A. Wu et al. zeigte, dass SDN-basierte Lösungen auch dazu beitragen können, das Risiko von Denial-of-Service-Angriffen auf Smart Grids zu verringern, indem sie eine bessere Überwachung und Reaktion auf solche Angriffe ermöglichen.

Die Verwendung von SDN in Smart Grids bietet zudem eine Möglichkeit zur Optimierung des Energieverbrauchs. Eine Studie von Y. Liu et al. schlug vor, dass die Anwendung von SDN-basierten Verfahren zur Steuerung von Lasten und Netzwerkelementen dazu beitragen kann, den Energieverbrauch in Smart Grids zu reduzieren, indem sie die Verwendung erneuerbarer Energiequellen wie Solar- und Windenergie optimieren.

Eine Herausforderung bei der Implementierung von SDN in Smart Grids besteht jedoch darin, sicherzustellen, dass das Netzwerk gegen böswillige Angriffe geschützt ist.

Eine Studie von J. Jin et al. zeigte, dass SDN-basierte Smart Grids anfälliger für bestimmte Arten von Angriffen sind, wie beispielsweise Distributed-Denial-of-Service-Angriffe, bei denen große Mengen von Datenverkehr das Netzwerk überfluten und zu Ausfällen führen.

Es ist daher wichtig, Mechanismen zu entwickeln, um solche Angriffe zu erkennen und zu verhindern, um die Widerstandsfähigkeit des Netzwerks zu gewährleisten. Insgesamt bietet die Verwendung von SDN in Smart Grids eine vielversprechende Möglichkeit, die Flexibilität und Widerstandsfähigkeit von Smart Grids zu verbessern. Aber es ist wichtig, die Risiken und Herausforderungen zu verstehen und geeignete Mechanismen zur Absicherung des Netzwerks zu implementieren.

Weiterführende Literatur:

- Dong, X., Lin, H., Tan, R., Iyer, R. K., & Kalbarczyk, Z. (2015). Software-defined networking for smart grid resilience: Opportunities and challenges. In *CPSS 2015 - Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, Part of ASIACCS 2015* (pp. 61-68). (CPSS 2015 - Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, Part of ASIACCS 2015). Association for Computing Machinery. DOI: 10.1145/2732198.2732203
- Demirci, S., & Sagiroglu, S. (n.d.). *Software-Defined Networking for Improving Security in Smart Grid Systems*.

5.12 Gerätesicherheit

Die Sicherheit von Smart Grids hängt stark von der Sicherheit der darin verwendeten Geräte und ihrer Firmware ab. Firmware-Angriffe können durch Ausnutzen von Schwachstellen in den eingebetteten Systemen, die das Netzwerk und die Stromversorgung unterstützen, verheerende Folgen haben.

Firmware-Angriffe auf Smart Grid-Komponenten wie Stromzählern, intelligenten Leistungsschaltern und Überwachungssystemen können es Angreifern ermöglichen, das System zu beschädigen. Um solche Angriffe zu verhindern, sind sichere Firmware-Updates und Authentifizierungsmechanismen erforderlich, um die Integrität und Authentizität der Firmware zu gewährleisten. Hersteller von Smart Grid-Komponenten müssen sichere Firmware-Entwicklung und -Validierung durchführen, um Schwachstellen zu minimieren. Regelmäßige Sicherheitsüberprüfungen und Penetrationstests sind erforderlich, um potenzielle Schwachstellen zu identifizieren und zu beheben. In diesem Zusammenhang wurden mehrere Techniken vorgeschlagen, um Präventions- und Erkennungsmechanismen gegen Malware bereitzustellen, wie die Erhöhung der Diversität der eingebetteten Firmware und die sichere Speicherung von Schlüsselmaterial zur Validierung der Software.

Ein bekanntes Beispiel für einen Firmware-Angriff auf Smart Grid-Komponenten ist der Stuxnet-Wurm, der 2010 entdeckt wurde. Der Wurm wurde speziell entwickelt, um das iranische Atom-programm zu sabotieren und zielte auf die Siemens-Industriesteuerungen ab, die in Atomkraftwerken eingesetzt wurden. Der Wurm nutzte eine Schwachstelle in der Firmware der Steuerungs-komponenten, um sie zu infizieren und dann ihre Kontrolle zu übernehmen.

Ein weiteres Beispiel für einen Firmware-Angriff ist der Dragonfly 2.0-Angriff auf die US-Stromversorgung im Jahr 2017. Die Angreifer infiltrierten das Netzwerk der Energieversorgungsunternehmen und installierten bösartige Firmware auf den Steuerungssystemen, um eine Hintertür zu schaffen und Zugriff auf das Netzwerk zu erhalten.

Im Zusammenhang mit Smart Grids haben Forscher mehrere Techniken beschrieben, um Präventions- und Erkennungsmechanismen gegen Malware bereitzustellen. Die Autoren McLaughlin et al. haben vorgeschlagen, die Diversität der eingebetteten Firmware zu erhöhen, um ein apokalyptisches Szenario zu vermeiden, bei dem eine Malware die meisten Geräte im Smart Grid kompromittiert. Sie argumentieren, dass die Verwendung unterschiedlicher Firmware-Versionen auf verschiedenen Geräten es schwieriger macht, Schwachstellen in der Firmware auszunutzen, da jeder Angriff speziell auf eine bestimmte Firmware-Version zugeschnitten sein müsste. Auf diese Weise können gemeinsame Schwachstellen vermieden werden und die Wahrscheinlichkeit verringert werden, dass Malware mehrere Geräte im Smart Grid gleichzeitig beeinträchtigt.

Um Malware-Angriffe auf eingebettete Systeme zu verhindern, ist eine sichere Speicherung mit Schlüsselmaterial zur Validierung der Software erforderlich. Diese Maßnahme hilft dabei, die Integrität der Software zu gewährleisten und zu verhindern, dass bösartiger Code in das System eingeschleust wird. Eine vielversprechende neue Methode zur Remote Code-Verifizierung ist die Attestation. Mit Hilfe dieser Technologie kann die auf einem System ausgeführte Software von einer externen Einheit auf eine Weise überprüft werden, die das Verstecken von Malware erschwert. Das bedeutet, dass Attestation es ermöglicht, eine digitale Signatur der ausführenden Software zu erstellen, wodurch selbst unbekannte Malware erkannt werden kann.

Für Standard IT-Systeme sind aktuelle und häufig aktualisierte Endpunkt-Sicherheitslösungen (EDR) sowie hostbasierte Eindringungserkennung erforderlich, um die Geräte vor verschiedenen Arten von Angriffen zu schützen.

Weiterführende Literatur:

- P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong and A. Martin, "Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2886-2927, thirdquarter 2019, doi: 10.1109/COMST.2019.2899354.
- O. Duman, M. Ghafouri, M. Kassouf, R. Atallah, L. Wang and M. Debbabi, "Modeling Supply Chain Attacks in IEC 61850 Substations," *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Beijing, China, 2019, pp. 1-6, doi: 10.1109/SmartGridComm.2019.8909818.

5.13 Technische Aspekte von Sicherheitslösungen

Dieser Abschnitt beschreibt den technischen Aspekt der Sicherheit von Smart Grids. Die Literatur identifiziert drei zentrale Bedrohungsbereiche: die Sicherheit der Infrastruktur, die technische Betriebssicherheit und die Sicherheit des Datenmanagements. Die Arbeiten geben einen Überblick über die technischen Herausforderungen und Bedrohungen für Smart Grids, wie z. B. Netzwerkangriffe, Stromausfälle und die Manipulation von Daten. Darüber hinaus werden mögliche Lösungsansätze und Technologien zur Verbesserung der technischen Sicherheit in Smart Grids diskutiert, wie z. B. sichere Netzwerkarchitekturen, robuste Stromversorgungssysteme und intelligente Überwachungs- und Analysetools. Die wissenschaftlichen Arbeiten betonen die Bedeutung einer umfassenden Sicherheitsstrategie, die alle Aspekte des Smart Grid-Systems berücksichtigt, um die Widerstandsfähigkeit und Integrität der Infrastruktur zu gewährleisten.

Weiterführende Literatur:

- Abdulrahaman Okino Otuoze a,b,∗, Mohd Wazir Mustafa a, Raja Masood Larik R, A Department of Power Engineering, Faculty of Electrical Engineering, Universiti Teknologi, Malaysia, Johor Bahru, Malaysia Department of Electrical and Electronics Engineering, Faculty of Engineering and Technology, University of Ilorin, Ilorin, Nigeria Received 24 December 2016; received in revised form 14 August 2017; accepted 5 January 2018
- Otuoze, A. O., Mustafa, M. W., & Larik, R. M. (2018). Technical Aspects of Threats to Smart Grid Infrastructure: A Review. International Journal of Engineering and Technology (IJET), 9(1), 20-24.

5.13.1. Infrastrukturelle Security

Die Infrastruktur von Smart Grids ist, wie schon gezeigt, ein komplexes System, das viele verschiedene Komponenten wie Benutzer, Kraftwerke, Übertragungs- und Verteilungsnetze, Umspannwerke, Transformatoren und Kommunikationssysteme miteinander verbindet. Die Sicherheit der Infrastruktur ist daher von entscheidender Bedeutung, da Angriffe auf das System zu schwerwiegenden Infrastrukturausfällen führen können. In Goel und Hong (2015) wurden einige Angriffe auf das Stromnetz, die zu Infrastrukturausfällen führten, wie z. B. Cyber-Sicherheitsverletzungen, Kaskadenfehler, Stromausfälle usw. beschrieben. Die Advanced Metering Infrastructure (AMI) ist aufgrund ihrer zentralen Rolle in der Smart Grid-Operation besonders anfällig für Angriffe. Die AMI-Architektur besteht aus einem Netzwerk von Sensoren, Zählern, Geräten und Computern zur Datenaufzeichnung und -analyse. Die Sicherheit von Smart Grid darf sich daher nicht allein auf die Advanced Metering Infrastructure (AMI) beschränken, sondern muss auch die Bereiche weitflächige Situationswahrnehmung, IT-Netzwerkintegration, Interoperabilität, Nachfragesteuerung, Kundendatenschutz und Effizienz berücksichtigen.

Einen guten Überblick gibt die Sicherheitsinitiative der NIST, die als Best Practices-Handbuch für die Sicherheit von Smart Grid-Systemen dient.

Weiterführende Literatur:

- Srivastava, M. (2021). An Overview of Cyber-Security Issues in Smart Grid. In: Pandian, A., Fernando, X., Islam, S.M.S. (eds) Computer Networks, Big Data and IoT. Lecture Notes on Data Engineering and Communications Technologies, vol 66. Springer, Singapore.

- Barrett, M. (2018), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework, [online], https://doi.org/10.6028/NIST.CSWP.04162018, https://www.nist.gov/cyberframework (Accessed June 13, 2023)

5.13.2. Cyber Security

Cyber-Angriffe sind aufgrund der Anfälligkeit der Infrastruktur für digitale Angriffe zweifellos die am meisten diskutierten Angriffe auf intelligente Stromnetze. Wenn sie nicht angemessen abgewehrt werden, sind sie in der Lage, das System vollständig zum Zusammenbruch zu bringen. Bereits bei Dennis und Keogh (2009) wurden eine Reihe bedeutender Schwachstellen des intelligenten Stromnetzes identifiziert und diese sind bis heute weiter vorhanden. Jeder Angriff kann die Versorgungsunternehmen dazu bringen, falsche Entscheidungen bezüglich des Verbrauchs und der Kapazität zu treffen und sie möglicherweise vor bevorstehenden Problemen oder laufenden Angriffen blind machen. Die Vertraulichkeit, Authentifizierung und der Datenschutz von Daten, die für die Zuverlässigkeit und Effizienz des Netzes von Bedeutung sind, müssen garantiert sein, um unbefugte Änderungen über die Infrastruktur zu verhindern.

Beispiele von bekannten Cyber-Angriffen sind Angriffe auf das konventionelle Stromnetz in den USA, als es angeblich von Spionen infiltriert wurde. Auch Estland, Georgien, Litauen, Kirgisistan, Ukraine, Kasachstan und das Vereinigte Königreich wurden Berichten zufolge ins Visier genommen. In jüngerer Zeit häufen sich Berichte über Cyber-Angriffe auf verschiedene Bereiche der kritischen Infrastrukturen weltweit.

Cyber-Angriffe auf das intelligente Stromnetz können zu verheerenden Auswirkungen führen, die zu kaskadierenden Ausfällen der kritischen Infrastruktur und Störungen in der Wirtschaft führen können, da kritische Infrastrukturen auf eine gesicherte und zuverlässige Stromversorgung angewiesen sind.

In etlichen Forschungsprojekten konzentriert man sich darauf, wie diese Angriffe abgemildert werden können, indem Meter-Bots, breit gestreute DoS-Angriffe, Verbrauchsprotokolle, SM-Rootkits und meterbasierte Antivirenprogramme für eine verbesserte Sicherheit bereitgestellt werden, und es werden in der Literatur etliche weitere Ansätze entwickelt.

Weiterführende Literatur:

- C. Konstantinou and S. P. Mohanty, "Cybersecurity for the Smart Grid," in *Computer*, vol. 53, no. 5, pp. 10-12, May 2020, doi: 10.1109/MC.2020.2975901.

5.13.3. Betriebssicherheit

Angesichts der hohen Komplexität des Stromnetzes ist es unerlässlich, dass sichere Betriebs-systeme eingesetzt werden, da Ausfälle schwerwiegende Folgen haben können und kritische Infrastrukturen von einer gesicherten und zuverlässigen Stromversorgung und -steuerung abhängig sind. Während einige Funktionen der Betriebsführung des Stromnetzes durch automatisierte Systeme koordiniert werden, ist für einen Teil der Betriebsführung die Aufmerksamkeit der Operator im Kontrollzentrum erforderlich, insbesondere in kritischen Situationen.

Die technische Betriebssicherheit umfasst daher verschiedene Aspekte, darunter die Sicherheit der Infrastrukturanlagen und Betriebsverfahren, die Steuerung von Regelsystemen auf Basis des Systemstatus, die Zuverlässigkeit und Widerstandsfähigkeit des Betriebs, den Intelligenzgrad des Systems, die Sicherheit der Systemdaten und Analyse, die Qualifikation und technischen Fähigkeiten des Personals sowie regelmäßige Kontrollen und Wartungspläne.

Um ein widerstandsfähiges Stromnetz zu schaffen, sind rechtzeitige Erkennung und Diagnose von Problemzuständen entscheidend, um die Ausbreitung von Störungen zu verhindern. Hierbei kommen moderne Ansätze, Analysewerkzeuge und Technologien zum Einsatz, die auf Fortschritten in den Bereichen Berechnung, Steuerung und Kommunikation basieren, um Lösungen für Stromnetze und andere Infrastrukturen bereitzustellen, die sich lokal selbst regulieren und bei Ausfällen, Bedrohungen oder Störungen automatisch neu konfigurieren.

Die Bedeutung der Widerstandsfähigkeit des Stromnetzes wurde auch von Amin und Wollenberg (2005) hervorgehoben. Sie betonen, dass widerstandsfähige Systeme für unterbrechungsfreie Betriebsabläufe sorgen und dass moderne Technologien einen wichtigen Beitrag leisten können, um dies zu erreichen.

Weiterführende Literatur:

- S. Massoud Amin and B. F. Wollenberg, "Toward a smart grid: power delivery for the 21st century," in *IEEE Power and Energy Magazine*, vol. 3, no. 5, pp. 34-41, Sept.-Oct. 2005, doi: 10.1109/MPAE.2005.1507024.
- W. H. Sanders, "Building resilient infrastructures for smart energy systems (abstract)," *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, Washington, DC, USA, 2012, pp. 1-1, doi: 10.1109/ISGT.2012.6175572.

5.13.4. Data Management Security

Die Sicherheit der Daten im Bereich der Energieversorgung ist ein bekanntes Thema, da die erhobenen Daten für die Zuverlässigkeit und Wartbarkeit des Systems von entscheidender Be-deutung sind. Um sicherzustellen, dass die Daten sicher und vor unbefugtem Zugriff geschützt sind, werden Echtzeit-Aufzeichnung, Überwachung und Speicherung von Daten und Informationen durchgeführt. Es werden Regeln und Vorschriften aufgestellt, um sicherzustellen, dass die Datenrichtlinien eingehalten werden und die Privatsphäre der Kunden geschützt wird.

Die Einführung von intelligenten Zählern (Smart Meter) hat neue Herausforderungen im Bereich der Datensicherheit geschaffen. Es gibt Bedenken bezüglich Datenschutzverletzungen durch Versorgungsunternehmen im Zusammenhang mit der Offenlegung von Kundendaten. Eine Kompromittierung des Smart Meter kann zu einem weitreichenden Angriff auf das Hauptnetz führen, indem subtile Veränderungen im Kundenverbrauch vorgenommen werden, um beispielsweise falsche Verbrauchswerte anzuzeigen.

Um diese Bedrohungen zu minimieren, ist es notwendig, dass eine umfassende Analyse der Sicherheitsbedrohungen und -schwachstellen durch den Energieversorger durchgeführt wird. Der Schutz der Daten und der Privatsphäre der Kunden ist von entscheidender Bedeutung für die Kundenzufriedenheit und das Vertrauen in die Energieversorger. Es müssen angemessene Sicherheitsvorkehrungen getroffen werden, um sicherzustellen, dass die Daten sicher und zuverlässig gespeichert und übertragen werden.

5.14 Nicht technische Aspekte von Sicherheitslösungen

Die Implementierung eines Smart Grids wird nicht nur von technischen Faktoren beeinflusst, sondern auch von nicht technischen Faktoren wie natürlichen und vom Menschen verursachten Umweltrisiken sowie staatliche Regulierungen, Planung und Umsetzung von Marktoperationen und der Mobilisierung des privaten Sektors. Obwohl einige dieser Faktoren als nicht technisch betrachtet werden können, kann es erforderlich sein, auch technische Ansätze zur Bewältigung dieser Faktoren zu entwickeln. Eine umfassende Analyse aller möglichen Quellen von Smart Grid-Bedrohungen ist unerlässlich, um eine robuste und widerstandsfähige Smart Grid-Infrastruktur aufzubauen, die in der Lage ist, auch unvorhergesehene Ereignisse zu bewältigen.

5.14.1. Umweltsicherheit

Die Sicherstellung von Umweltsicherheit ist ein wichtiger Aspekt bei der Implementierung von Smart Grids, da dies potenziell katastrophale Auswirkungen auf die Infrastrukturen aufgrund von natürlichen oder künstlichen Umweltrisiken wie Überschwemmungen, Erdbeben, Erdrutschen, Baumstürzen, Verbrennungen von Pflanzen usw. vermeiden kann. Ein intelligentes Reaktionsmanagement basierend auf Umweltaspekten wird im Wesentlichen durch die Bereitstellung geeigneter Bedrohungswarnungen auf der Grundlage empfangener Daten und alternativen Zuleitungen für kritische Infrastrukturen in solchen Notfällen erreicht. Obwohl dieser Aspekt der Smart Grid-Sicherheit in dieser Studie als nicht technisch eingestuft ist, hat er sowohl technische als auch nicht technische Auswirkungen. Die Fähigkeit des Systems, schnell auf Fehler zu reagieren und den Dienst wiederherzustellen, hat höchste Priorität in Smart Grids und wird im Wesentlichen durch automatisches Schalten zur Wiederherstellung des Dienstes im Fall von Stromausfällen erreicht. Naturkatastrophen, extreme Temperaturen, die Erschöpfung fossiler Brennstoffe, Volatilität der globalen Energiemärkte, Terrorismus, Sabotage und

Vandalismus sind Faktoren, die gegen die Widerstandsfähigkeit von Smart Grids sprechen. Auf geografischen Informationssystemen (GIS) basierende Instant-Daten sind bei dieser Analyse besonders wichtig, insbesondere im Zusammenhang mit Vorhersagen und Analysen von Naturkatastrophen, die zur Bestimmung von Bedrohungswarnungen verwendet werden. Naturkatastrophen können zudem die Aufmerksamkeit von der Cybersicherheit ablenken und zu Angriffen unter Ausnutzung der Situation einladen.

Weiterführende Literatur:

- H. Sharifi and Y. Yamagata, "Resilience-based optimal design of urban energy systems", Energy Procedia, vol. 88, pp. 401-406, 2016.

5.14.2. Regulatorische Anforderungen

Regulatorische Vorschriften sind ein weiterer wichtiger Aspekt. Sie bieten klare Richtlinien und Standards für die Hersteller von Smart Grid-Komponenten und für die Betreiber von Smart Grids. Dadurch wird sichergestellt, dass alle Beteiligten sich an bestimmte Sicherheits- und Datenschutzstandards halten, um mögliche Bedrohungen und Risiken für die Systeme zu minimieren. Regulatorische Vorschriften können auch die Interoperabilität von Smart Grid-Komponenten fördern und damit die Integration von erneuerbaren Energiequellen und dezentralen Energieerzeugern erleichtern. Darüber hinaus können sie den Verbraucherschutz stärken, indem sie sicherstellen, dass Verbraucher eine transparente Rechnungsstellung erhalten und dass ihre Privatsphäre geschützt wird. Insgesamt sind regulatorische Vorschriften ein wichtiger Bestandteil der Infrastruktur für Smart Grids, um sicherzustellen, dass sie sicher und zuverlässig betrieben werden können.

In Deutschland gibt es eine Vielzahl von regulatorischen Vorschriften für Smart Grids, die von verschiedenen staatlichen Stellen ausgehen. Die wichtigsten Regelungen betreffen den Bereich der Stromversorgung und beziehen sich auf die Verwendung von Smart Meter, die Netzstabilität und die Integration erneuerbarer Energien.

Eine wichtige Rolle spielen hierbei die sogenannten "Smart Meter-Gateway-Regulierung" und die "Marktregeln für den Messstellenbetrieb". Diese Regulierungen legen fest, wie Smart Meter installiert und betrieben werden sollen, um den Schutz der Privatsphäre der Verbraucher zu gewährleisten und die Sicherheit des Smart Grids zu gewährleisten.

Die Bundesnetzagentur (BNetzA) ist in Deutschland für die Regulierung des Strommarkts und damit auch für Smart Grids zuständig. Sie legt unter anderem die Rahmenbedingungen für den Netzzugang und die Netzentgelte fest und überwacht die Einhaltung der regulatorischen Vorgaben durch die Netzbetreiber. Darüber hinaus gibt es auch auf europäischer Ebene Vorschriften für Smart Grids, wie etwa die "Richtlinie über Maßnahmen zur Gewährleistung der Sicherheit der Stromversorgung und der Netzstabilität", die den Aufbau von Smart Grids in Europa fördern und unterstützen soll.

NIS 2 (Network and Information Systems Directive 2) ist eine Richtlinie der Europäischen Union, die dazu dient, die Sicherheit von Netzwerk- und Informationssystemen in der EU zu erhöhen. Es gibt spezifische Anforderungen für bestimmte Branchen, einschließlich der Energiebranche und Smart Grids. Für Smart Grids gilt die NIS 2 als wichtigste regulatorische Vorschrift, die die Betreiber von Smart Grids verpflichtet, Maßnahmen zu ergreifen, um die Sicherheit von Netzwerken und Informationssystemen zu gewährleisten. Die NIS 2 legt auch fest, dass Betreiber von Smart Grids verpflichtet sind, Sicherheitsvorfälle zu melden und eine kontinuierliche Überwachung der Systeme durchzuführen.

In Deutschland muss NIS 2 bis 2024 in nationales Recht umgesetzt werden. Der IT-Sicherheitskatalog, der von der Bundesnetzagentur veröffentlicht wurde, stellt sicher, dass Betreiber von Smart Grids in Deutschland die Anforderungen der NIS 2 erfüllen. Dazu gehören unter anderem die Durchführung von Risikobewertungen und die Einrichtung von Maßnahmen zur Erkennung, Vermeidung und Meldung von Sicherheitsvorfällen. Insgesamt hat die NIS 2 somit einen erheblichen Einfluss auf die Nutzung von Smart Grids in Deutschland.

Weiterführende Literatur:

- Z. Hu and T. Cui, "Market Analysis of Auxiliary Regulation to Promote the Consumption of Clean Energy," *2021 5th International Conference on Smart Grid and Smart Cities (ICSGSC)*, Tokyo, Japan, 2021, pp. 130-133, doi: 10.1109/ICSGSC52434.2021.9490488.

5.14.3. Analytische und modellbasierte Maßnahmen

Die Implementierung effektiver Smart Grid-Sicherheitslösungen erfordert analytische Rahmenbedingungen, die die Modellierung des Cyber- und physischen Systems des Netzes und ihrer engen Verknüpfung, die Interdependenz zwischen verschiedenen Netzkomponenten und die Entscheidungsprozesse des Betreibers und Angreifers ermöglichen. Zusätzlich zur Verwendung von Lösungen aus der Informationssicherheit, der Schutztechnik des Stromsystems, der Kontrolltheorie und der Zuverlässigkeitsbewertung sind zusätzliche analytische und theoretische Ansätze sehr nützlich bei der Modellierung und Untersuchung von Smart Grid-Sicherheitsproblemen.

Eine grundlegende Komponente der Implementierung eines Smart Grids ist die Verwundbarkeitsbewertung und das Risikomanagement, die die Identifizierung von Netzkomponenten beinhalten, die anfällig für verschiedene Bedrohungen sind. Diese Komponenten können mithilfe von vergangenen Daten oder analytischen und experimentellen Methoden ermittelt werden. Die Verwundbarkeitsbewertung umfasst die Bestimmung, welche Netzkomponenten anfällig für welche Arten von Bedrohungen sind. Anhand vergangener Daten kann der Smart Grid-Betreiber identifizieren, welche Komponenten in der Vergangenheit welchen Angriffen ausgesetzt waren. Beispielsweise sind Phishing-Angriffe auf GPS-Signale üblich, daher sind PMUs anfällig für Spoofing und TSAs. Darüber hinaus können die Verwundbarkeit einiger Komponenten auch analytisch und experimentell analysiert werden. Beispielsweise sind unverschlüsselte Sensordaten anfällig für Replay-Angriffe, da der Angreifer leicht eine Folge von zuvor generierten Daten erlernen und wiederholen kann. Ebenso ist ein ungeschützter Zähler, der mit dem Internet verbunden ist, anfällig für Dateninjektionsangriffe.

Das Risikomanagement verwendet die Ergebnisse der Verwundbarkeitsbewertung und kombiniert sie mit einer Einschätzung der Auswirkungen, die eine Verwundbarkeit auf das Smart Grid haben kann. Das Risikomanagement für Smart Grid umfasst dabei zwei Schlüsselaufgaben:

a) Kontingenzanalyse: Bewertung der Auswirkungen des Ausfalls einer Komponente wie einer Übertragungsleitung, eines Generators, eines Transformators oder eines Sensors auf die dynamische Stabilität und den Betriebszustand des Netzes.

b) Kaskadenfehleranalyse: Analyse der Ausbreitung von Fehlern im Netz.

Letzteres erfordert ein Verständnis für die Wechselbeziehungen zwischen den verschiedenen Netzkomponenten, um die Kaskadenkette von Ereignissen vorherzusagen, die auftreten können, wenn einige Komponenten ausfallen. Beispielsweise kann der Verlust einer Übertragungsleitung unter

schweren Lastbedingungen zu Kaskadenfehlern führen, die zu einem Blackout führen, während der Verlust einer anderen Leitung kaum Auswirkungen hat. Die Verwundbarkeits-bewertung und das Risikomanagement sind kontinuierlich sich entwickelnde Prozesse, bei denen der Betreiber kontinuierlich über potenzielle Bedrohungen und Schwachstellen lernt, um den Schutz des Systems zu verbessern.

Sicherheitsverstärkung: Sobald Bedrohungen und ihre Auswirkungen charakterisiert sind, müssen Maßnahmen zur Verstärkung der Netzwerksicherheit abgeleitet werden. Solche Verstärkungsverfahren unterliegen jedoch in der Regel Budget- und Investitionsbeschränkungen. Die Ergebnisse des Verwundbarkeits- und Risikomanagements können daher verwendet werden, um eine Rangliste der wichtigsten zuerst zu schützenden Komponenten zu erstellen. Die Sicherheit kann verbessert werden, indem man die Verschlüsselung von Sensor-Daten verbessert, ältere Zähler durch modernere und bessere Modelle ersetzt, kabelgebundene Kommunikation anstelle von drahtloser nutzt oder robustere Methoden implementiert. Die Verwundbarkeitsbewertung und das Risikomanagement sind kontinuierlich sich entwickelnde Prozesse, bei denen der Betreiber kontinuierlich über potenzielle Bedrohungen und Schwach-stellen lernt, um den Schutz des Systems zu verbessern.

Weiterführende Literatur:

- Sanjab, A., Saad, W., Guvenc, I., Sarwat, A., & Biswas, S. (2018). Smart Grid Security: Threats, Challenges, and Solutions. IEEE Communications Surveys & Tutorials, 20(1), 36-79.
- Subramanian, V., & Zonouz, S. A. (2016). Towards a cyber-resilient and secure Smart Grid: developments, challenges and future directions. Journal of Cybersecurity, 2(1), 53-67

5.15 Praktische Untersuchungen im Smart Grid Lab

Im Rahmen der Untersuchungen von QGroup im Smart Grid Lab wurden verschiedene Methoden und Werkzeuge eingesetzt, um potenzielle Schwachstellen und Bedrohungen im Smart Grid zu identifizieren. Dabei war es jedoch nicht möglich, alle theoretisch möglichen Angriffsszenarien zu testen und alle potenziellen Schwachstellen zu untersuchen. Stattdessen wurde eine Auswahl von Angriffsvektoren und Schwachstellen identifiziert, die als am relevantesten für das Smart Grid angesehen wurden.

Ein Grund dafür, dass nicht alle möglichen Schwachstellen untersucht wurden, war die Tatsache, dass das Smart Grid Lab ein aktives Forschungsumfeld ist und andere Forschungsgruppen im Labor arbeiteten. Es war daher wichtig, die Untersuchungen so durchzuführen, dass die anderen Forschungsaktivitäten im Labor nicht gestört wurden. Dies bedeutete auch, dass destruktive Tests vermieden wurden, um sicherzustellen, dass die Infrastruktur des Smart Grid Lab nicht beschädigt wurde.

Dennoch war es wichtig, eine angemessene Auswahl von Tests durchzuführen, um potenzielle Schwachstellen zu identifizieren und Schutzmaßnahmen zu entwickeln. Hierbei wurden Werkzeuge und Methoden eingesetzt, die als relevant für das Smart Grid angesehen wurden. Dazu gehörten Netzwerk-Forensik-Tools wie Fidelis und Tenable OT sowie ICS-Simulatoren und Penetration Testing Tools wie Metasploit. Die Ergebnisse der Tests wurden analysiert und dokumentiert, um potenzielle Schwachstellen und Angriffsvektoren zu identifizieren und geeignete Schutzmaßnahmen zu empfehlen.

Es ist wichtig zu betonen, dass die Untersuchungen im Smart Grid Lab als eine Momentaufnahme betrachtet werden sollten und nicht als endgültiges Urteil darüber, ob das Smart Grid sicher und widerstandsfähig gegenüber Angriffen ist. Vielmehr sollten die Ergebnisse der Untersuchungen als Grundlage zur weiteren Forschung und Entwicklung von Schutzmaßnahmen dienen.

Zusammenfassend lässt sich sagen, dass das Smart Grid eine komplexe und vielschichtige Technologie ist, die eine umfassende technische Analyse erfordert, um sicherzustellen, dass es sicher und widerstandsfähig gegenüber Angriffen ist. Obwohl es nicht möglich war, alle potenziellen Schwachstellen und Bedrohungen zu untersuchen, wurden dennoch relevante Tests durchgeführt und Schutzmaßnahmen empfohlen. Es bleibt jedoch eine kontinuierliche Herausforderung für Forscher und Praktiker, das Smart Grid fortlaufend zu analysieren und Schutzmaßnahmen zu verbessern, um die Sicherheit und Widerstandsfähigkeit des Systems zu gewährleisten.

5.15.1. Netzwerk Design im Smart Grid Lab

Bei unseren Untersuchungen haben wir festgestellt, dass das Smart Grid Lab vornehmlich aus einem Netzwerk besteht, das ausschließlich über das IEC 60870-5-104-Protokoll kommuniziert. Dieses Netzwerk ist Teil des Class-C-Netzwerks mit der IP-Adresse 192.168.200.0/24. Das Netz-werk ist in Abbildung 1 schematisch dargestellt, wobei das IEC 60870-5-104-Netzwerk in orange eingezeichnet ist.

Das IEC 60870-5-104-Protokoll ist ein Kommunikationsstandard, der speziell für die Steuerung von Stromnetzen entwickelt wurde. Es ermöglicht den Austausch von Daten zwischen verschiedenen Stromnetzkomponenten wie Schaltanlagen, Leitstellen und Stromzählern. Das Protokoll wird typischerweise über TCP/IP übertragen und bietet Funktionen wie Datenübertragung, Überwachung und Steuerung von Stromnetzkomponenten.

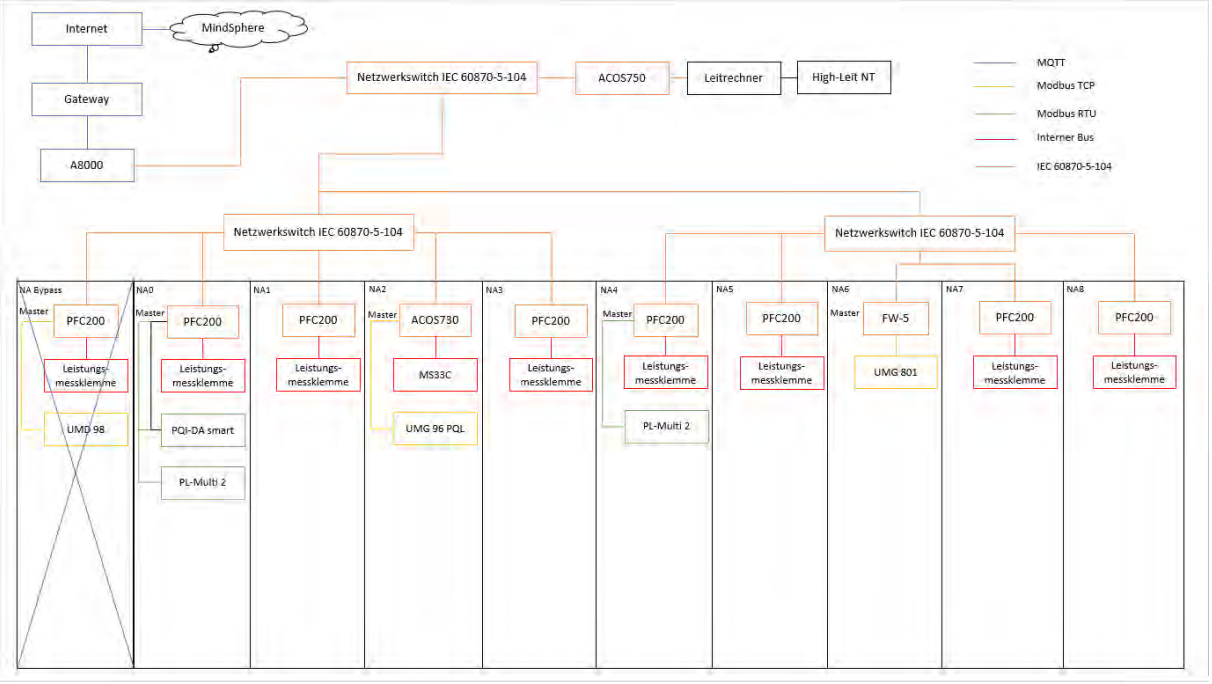


Abbildung 62: Smart Grid Netzwerk

In diesem Netzwerk installierte die QGroup einen U.F.N.T.A.-Server (Universal Forensics Network Traffic Analyzer). Bei diesem handelt es sich um ein System auf Basis von ESXi, auf welchem die QGroup mehrere virtuelle Maschinen betrieb wie u. a. virtuelle Maschinen für Fidelis Network (Netzwerk-

Forensik-Tool), Tenable Nessus Professional (Schwachstellenscanner) sowie eine QTrust Firewall und eine Ubuntu VM für manuelle Tests. Dieses System wurde über einen Switch der QGroup an einen der beiden NetGear Switches angeschlossen. Das direkte Anschließen des Servers war nicht möglich, da die NetGear Switche nicht konfigurierbar sind. Diese Verbindung wurde genutzt, um mit dem Netzwerk kommunizieren zu können (Injection Interface). Zudem wurde die Netzwerkverbindung zwischen dem Switch im Lab und dem Switch vor dem Fernwirkkopf unterbrochen, um diese ebenfalls durch den QGroup-Switch zu leiten (Mirror Interface). Dies ermöglichte es, jeglichen Verkehr zwischen den Netzabschnitten (NA) und dem Fernwirkkopf mitzulesen.

Der U.F.N.T.A.-Server wurde zusätzlich mit dem Standard IT-Netzwerk der FritzBox verbunden. Die Verbindung zwischen Server und FritzBox wurde ebenfalls mit einem Netzwerkkabel direkt hergestellt (Injection Interface), die Zuleitung von der FritzBox zum NetGear Switch wurde unterbrochen und durch den Switch der QGroup geleitet, um auch in diesem Netzwerk jeglichen Verkehr zwischen dem IEC 60870-5-104 und dem Internet mitprotokollieren zu können.

Weiterführende Literatur zu den verwendeten Werkzeugen:

- Agent Requirements on Windows, https://support.sentinelone.com/hc/en-us/articles/4410565200151-Agent-Requirements-on-Windows, Zugegriffen am 3. März 2023
- Agent Requirements on Linux, https://support.sentinelone.com/hc/en-us/articles/4410580891543-Agent-Requirements-on-Linux, Zugegriffen am 3. März 2023
- CrowdStrike Capabilities https://www.crowdstrike.com/products/faq/, Zugegriffen am 6. März 2023
- Metasploit IEC104 Client Utility https://www.infosecmatter.com/metasploit-module-library/?mm=auxiliary/client/iec104/iec104, Zugegriffen am 9. März 2023

5.15.2. Analyse mit klassischen IT-Tools

In der IT-Sicherheitsbranche haben sich Analysetools bewährt, die zum Schutz von Kommunikationsteilnehmern eingesetzt werden. Diese sogenannten Anti-Malware-Programme dienen der Identifizierung und Abwehr von bösartiger Software wie Viren, Trojanern und Ransomware. Darüber hinaus gibt es Monitoring Tools, die Geräte aus der Ferne scannen, um Schwachstellen zu identifizieren und gegebenenfalls zu patchen. Diese klassischen Schwachstellenscanner werden in der Regel von IT-Administratoren eingesetzt, um die Sicherheit ihrer Netzwerke zu gewährleisten. Ein weiteres wichtiges Tool in der IT-Sicherheitsbranche ist die Netzwerk-Forensik. Netzwerk-Forensik-Tools überwachen den Netzwerkverkehr zwischen einzelnen Kommunikationsteilnehmern, um Angriffe und Datenlecks aufzudecken und zu verhindern. Diese Tools können in einem Smart Grid-Netzwerk eingesetzt werden, um potenzielle Angriffe aufzudecken und zu verhindern.

Schutz der Kommunikationsteilnehmer
Klassische Anti-Malware-Programme und Next-Generation Endpoint Detection and Response-Systeme (EDR) sind Analysetools, die zum Schutz der Kommunikationsteilnehmer in klassischen IT-Umgebungen eingesetzt werden. Diese Programme werden auf den zu über-wachenden Systemen installiert und bieten einen Malwareschutz. Jedoch unterstützen sie lediglich die gängigen IT-Betriebssysteme wie Linux, Windows und macOS und häufig nur aktuelle Versionen davon. Ältere Systeme, die in Smart Grid-Umgebungen noch häufig anzutreffen sind, werden oft nicht unterstützt.

In Smart Grid-Netzen ist es dennoch unumgänglich, Malwareschutz auf den Steuerungsrechnern zu installieren, um Angriffe über diese auszuschließen. Dies ist besonders wichtig, wenn

Steuerungsrechner mit öffentlichen Netzen kommunizieren können. Die meisten Anti-Malware-Programme und EDR-Tools unterstützen, mit Ausnahme der Steuerungsrechner, alle anderen Kommunikationsteilnehmer im Smart Grid-Umfeld nicht oder nur sehr spärlich. Es besteht die Notwendigkeit, spezielle Analysetools zu verwenden, die auch das Smart Grid-Umfeld unter-stützen und in der Lage sind, den Netzwerkverkehr zu überwachen.

Monitoring Tools
Monitoring Tools werden in Smart Grid-Infrastrukturen genutzt, um eine umfassende Überwachung des Netzwerks durchzuführen und sicherzustellen, dass alle Systeme ordnungsgemäß funktionieren. Mit diesen Tools können Administratoren den Netzwerkverkehr zwischen den verschiedenen Komponenten überwachen, und dies nicht nur, um Probleme wie Engpässe, Überlastungen und mögliche Angriffe zu identifizieren, sondern besonders auch um sie möglichst direkt der Behebung zuzuleiten. Zudem können Schwachstellen und Sicherheitslücken in der Netzwerkinfrastruktur durch Schwachstellenscanner entdeckt werden. Durch die Überwachung des Netzwerkverkehrs können Administratoren auch die Leistung des Netzwerks optimieren, indem sie die Bandbreitenverteilung auf die verschiedenen Systeme anpassen und so sicherstellen, dass das Netzwerk reibungslos funktioniert und dass es nicht zu Ausfällen oder Unterbrechungen kommt. Darüber hinaus kann die Netzwerk-Forensik dazu genutzt werden, um bei Bedarf eine umfassende Analyse von Sicherheitsvorfällen durchzuführen und um mögliche Schwachstellen und Angriffsmuster zu identifizieren, die in Zukunft verhindert werden müssen. Insgesamt können Monitoring Tools somit dazu beitragen, die Sicherheit, Verfügbarkeit und Integrität von Smart Grid-Netzwerken zu erhöhen.

Schwachstellenscanner
Schwachstellenscanner wie Nessus Professional wurden im Smart Grid-Netzwerk genutzt, um Schwachstellen in den Geräten zu identifizieren. Allerdings haben diese Scanner in der Regel keine Policies für die Protokolle, die in Smart Grid-Netzwerken eingesetzt werden, wie zum Beispiel das IEC 60870-5-104-Protokoll. Dadurch konnten keine Schwachstellen des eingesetzten Protokolls erkannt werden. Auch reine Clients ohne exponierte Ports werden von Schwachstellenscannern nicht erkannt.

In den durchgeführten Schwachstellenscans im Smart Grid Lab wurden lediglich Probleme mit den SSL-Zertifikaten der webbasierten Verwaltung einiger Wago Gateways und die Etherleak-Schwachstelle bei einem Command-Prozessor erkannt.

Diese Schwachstelle tritt auf, wenn ein Gerät Datenpakete an einen anderen Host im Netzwerk sendet, ohne dass diese Daten verschlüsselt werden. Ein Angreifer, der Zugriff auf das Netzwerk hat, kann dann diese unverschlüsselten Daten abfangen und möglicherweise schädliche Aktionen ausführen oder vertrauliche Informationen stehlen. In diesem Zusammenhang hat der Nessus Professional Scanner die Etherleak-Schwachstelle bei einem Command-Prozessor im Smart Grid Lab entdeckt und darauf hingewiesen, dass die Datenübertragung zwischen den Geräten nicht ausreichend geschützt ist.

Die Alarme zeigten, dass selbstsignierte Zertifikate für die Verwaltung eingesetzt wurden und keine Zertifikate, die zumindest von einer eigenen PKI ausgestellt wurden. Dadurch waren die Verwaltungs-Frontends anfällig für Man-in-the-Middle-Angriffe, um auf diesem Weg Zugriff auf die Smart Grid-Systeme zu erhalten oder diese zu manipulieren. Es wurden keine spezifischen Schwachstellen des eingesetzten IEC 60870-5-104-Protokolls entdeckt, da der Scanner dafür nicht ausgelegt war.

Sev	Score	Name	Family	Count
MEDIUM	6.4	SSL Certificate Cannot Be Trusted	General	7
MEDIUM	6.4	SSL Self-Signed Certificate	General	7
MEDIUM	5.0	SSL Certificate Expiry	General	7
LOW	3.3	Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)	Misc.	1

Abbildung 63: Ergebnisse des Nessus Professional Scanners

ARP-Scanner

ARP (Address Resolution Protocol) ist ein Netzwerkprotokoll, das dafür sorgt, dass Geräte im Netzwerk miteinander kommunizieren können. Das Tool **arpwatch**, das auf der Ubuntu VM im Smart Grid Lab installiert wurde, nutzt ARP, um alle Zuordnungen von MAC-Adressen zu IP-Adressen im Netzwerk zu protokollieren. Arpwatch aktiviert auf dem Interface den Promicious Mode, um sämtlichen Traffic mitzuprotokollieren. Es analysiert das ARP-Protokoll und führt eine Logdatei (/var/log/syslog), in welche es alle Zuordnungen von MAC-Adressen zu IP-Adressen protokolliert. Dadurch können neue Geräte im Netzwerk und Änderungen an bestehenden Geräten erkannt werden.

Optional kann konfiguriert werden, dass auch Benachrichtigungen ausgelöst werden, wie beispielsweise der Versand einer E-Mail. Dies ermöglichte es, im Netzwerk sowohl neue Geräte zu erkennen als auch einen Teilnehmer, welcher seine MAC-Adresse änderte (siehe Abbildung 64 und Abbildung 65).

```
root@ubuntu:/tmp# macchanger -r ens224
Current MAC:   52:25:d9:8a:a2:71 (unknown)
Permanent MAC: 00:0c:29:0b:cb:2d (VMware, Inc.)
New MAC:       1a:03:07:56:c0:12 (unknown)
```

Abbildung 64: Änderung der MAC-Adresse mittels macchanger

```
Mar  7 11:00:03 ubuntu2 systemd[1]: Starting arpwatch service...
Mar  7 11:00:03 ubuntu2 systemd[1]: Finished arpwatch service.
Mar  7 11:00:06 ubuntu2 kernel: [1906425.996942] device ens192 entered promiscuous mode
Mar  7 11:00:06 ubuntu2 arpwatch: listening on ens192
Mar  7 11:00:07 ubuntu2 arpwatch: new station 192.168.200.150 00:0c:29:d9:4d:4b ens192
Mar  7 11:00:17 ubuntu2 arpwatch: new station 192.168.200.100 00:12:ad:01:32:68 ens192
Mar  7 11:00:29 ubuntu2 arpwatch: new station 192.168.200.104 00:e0:a8:fd:31:67 ens192
Mar  7 11:00:43 ubuntu2 arpwatch: new station 192.168.200.120 00:0c:29:88:b6:01 ens192
Mar  7 11:00:46 ubuntu2 arpwatch: new station 192.168.200.14 00:30:de:4f:02:ed ens192
Mar  7 11:05:41 ubuntu2 arpwatch: new station 192.168.200.18 00:30:de:4f:02:c8 ens192
Mar  7 11:06:00 ubuntu2 arpwatch: bogon 192.168.178.251 00:0c:29:88:b6:01 ens192
Mar  7 11:10:57 ubuntu2 arpwatch: new station 192.168.200.151 00:0c:29:0b:cb:2d ens192
Mar  7 11:55:38 ubuntu2 arpwatch: changed ethernet address 192.168.200.151 52:25:d9:8a:a2:71 (00:0c:29:0b:cb:2d) ens192
Mar  7 11:56:34 ubuntu2 arpwatch: changed ethernet address 192.168.200.151 1a:03:07:56:c0:12 (52:25:d9:8a:a2:71) ens192
```

Abbildung 65: Ergebnisse von arpwatch nach Änderung der MAC-Adresse

Zusätzlich scannte die QGroup das IEC 60870-5-104-Netzwerk mit dem Tool arp-scan, welches alle Hosts im Netzwerk aktiv zu erreichen versucht und dabei gleichzeitig versucht, anhand der jeweiligen MAC-Adresse den Hersteller des Gerätes zu ermitteln. Durch diesen Scan konnten alle Geräte im Smart Grid Lab erfolgreich erkannt werden. (siehe Abbildung 66).

```
root@ubuntu2:/home/qadmin/arp-scan# arp-scan -I ens192 192.168.200.0/24
Interface: ens192, type: EN10MB, MAC: 00:0c:29:73:92:39, IPv4: 192.168.200.130
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.200.8   ec:fc:55:01:34:8e       A. Eberle GmbH & Co. KG
192.168.200.10  00:30:de:4f:02:e1       WAGO Kontakttechnik GmbH
192.168.200.11  00:30:de:4f:02:ce       WAGO Kontakttechnik GmbH
192.168.200.12  00:12:ad:01:8a:b1       IDS GmbH
192.168.200.13  00:30:de:4f:02:8b       WAGO Kontakttechnik GmbH
192.168.200.14  00:30:de:4f:02:ed       WAGO Kontakttechnik GmbH
192.168.200.15  00:30:de:4f:03:a3       WAGO Kontakttechnik GmbH
192.168.200.16  70:e2:4c:15:39:7c       SAE IT-systems GmbH & Co. KG
192.168.200.17  00:30:de:4f:02:65       WAGO Kontakttechnik GmbH
192.168.200.18  00:30:de:4f:02:c8       WAGO Kontakttechnik GmbH
192.168.200.100 00:12:ad:01:32:68       IDS GmbH
192.168.200.104 00:e0:a8:fd:31:67       SAT GmbH & Co.
192.168.200.120 00:0c:29:88:b6:01       VMware, Inc.
192.168.200.150 00:0c:29:d9:4d:4b       VMware, Inc.
192.168.200.151 1a:03:07:56:c0:12       (Unknown: locally administered)

15 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.944 seconds (131.69 hosts/sec). 15 responded
```

Abbildung 66: Ergebnisse von arp-scan

Bei den letzten drei Geräten in Abbildung 66 handelt es sich um die Ubuntu Analyse VM sowie um eine weitere VM, die für Tests benutzt wurde. Der letzte Eintrag, das unbekannte Interface, ist das zweite Interface der Test-VM, dessen MAC-Adresse für die oben erwähnten arpwatch-Tests mit-hilfe des Tools macchanger geändert wurde (siehe Abbildung 64).

Die Ergebnisse des ARP-Scanners und von arpwatch haben gezeigt, dass es im Smart Grid Lab keine unbekannten Geräte gab und dass Änderungen an MAC-Adressen aufgezeichnet werden konnten. Dies ermöglicht eine bessere Kontrolle über die Geräte im Netzwerk und erhöht die Sicherheit gegenüber unbefugtem Zugriff.

Netzwerk-Forensik-Tools

Tools wie das oben erwähnte arpwatch gehen allerdings nicht so weit wie Netzwerk-Forensik-Tools, wie beispielsweise Fidelis Network, welches die QGroup im Smart Grid Lab betrieben hat. Netzwerk-Forensik-Tools sind sinnvoll, weil sie eine umfassende Überwachung des Netzwerkverkehrs ermöglichen und so Anomalien oder Angriffe auf das Netzwerk schnell erkennen können. Mit diesen Tools können Netzwerkadministratoren eine tiefgehende Analyse des Netzwerkverkehrs durchführen und verdächtige Aktivitäten aufspüren. Darüber hinaus ermöglichen Netzwerk-Forensik-Tools eine schnelle Reaktion auf Angriffe, da sie in Echtzeit auf Bedrohungen reagieren können. So können beispielsweise Bedrohungen automatisch blockiert oder isoliert werden.

Fidelis Network erhielt über einen Mirrorport sämtlichen Traffic der beiden im Smart Grid Lab vorhandenen Netzwerke und generierte anhand seiner Policies Alarme. Die Fidelis-Policies umfassen unter anderem bekannte Angriffsszenarien wie beispielsweise Log4J, Bash-Shellshock, Directory Traversal, SQL-Injection sowie Malware, geblacklistete DNS-Domänen und bekannte Command & Control-Server.

Im Smart Grid Lab löste das Tool lediglich Alarme aus, weil der oben erwähnte Tenable Nessus Scanner auf der Webschnittstelle des Servers 192.168.200.104 versuchte, die Log4J-Schwachstelle auszunutzen (siehe Abbildung 67 und Abbildung 68).

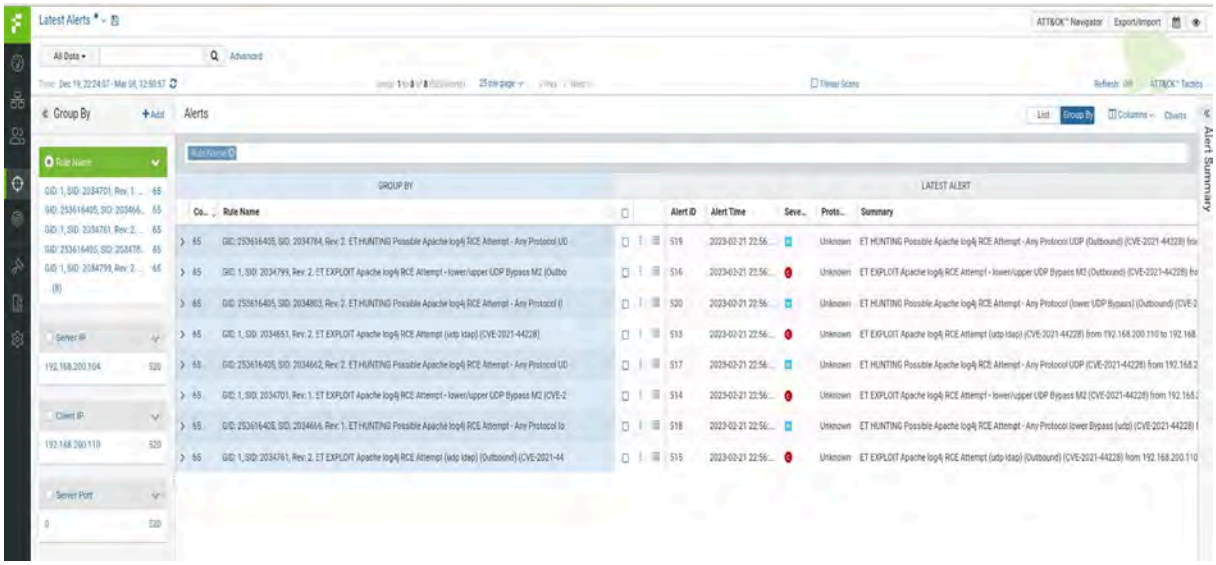


Abbildung 67: Von Fidelis Network geloggte Alarme

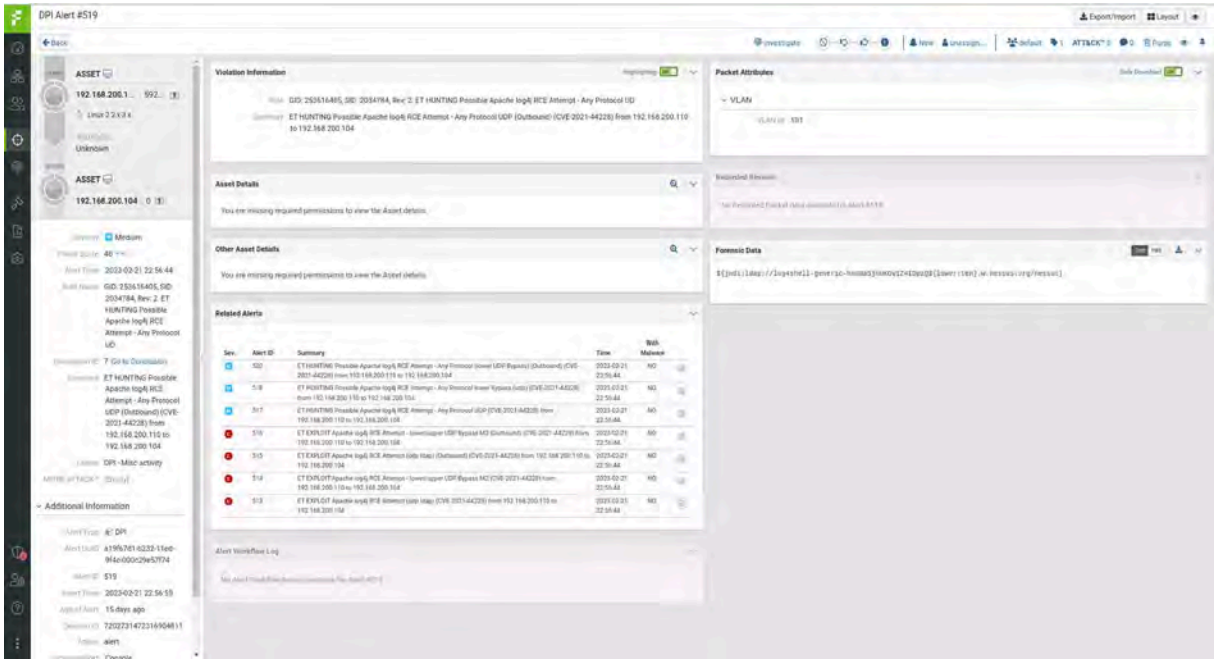


Abbildung 68: Details zu einem Log4j-Alarm in Fidelis

Da jedoch von der IP 192.168.200.104 keine durch die Log4j-Schwachstelle getriggerten ausgehenden Anfragen durch Fidelis beobachtet wurden, handelt es sich hierbei höchstwahrscheinlich um ein False Positive.

Dies zeigt zwar, dass Angriffsversuche mit herkömmlichen Mechanismen erkannt werden, Policies für spezifische Angriffe für OT/IoT-Netzwerke sind im Standardumfang der Lösung jedoch nicht enthalten. Auch werden die kommunizierten Protokolle nur unzureichend in den Metadaten aufgeführt (siehe Abbildung 69).

Die mangelnde Unterstützung spezifischer Protokolle ist ein typisches Problem bei herkömmlichen IT-Sicherheitslösungen, da diese hauptsächlich auf die Absicherung von Standard-IT-Netzwerken

ausgelegt sind. In OT- und IoT-Netzwerken kommen jedoch oft proprietäre Protokolle zum Einsatz, die von herkömmlichen IT-Sicherheitslösungen nicht oder nur unzureichend unterstützt werden. Dadurch können Schwachstellen und Angriffe auf diese Protokolle nicht erkannt und abgewehrt werden, was ein erhebliches Sicherheitsrisiko darstellt. Netzwerk-Forensik-Tools sind daher nur dann sinnvoll, wenn sie speziell für die Analyse von Netzwerkverkehr in OT- und IoT-Netzwerken entwickelt wurden und somit auch proprietäre Protokolle unterstützen können. Dadurch können Schwachstellen und Angriffe auf diese Protokolle erkannt und abgewehrt werden, was zu einer verbesserten Sicherheit im Netzwerk führt.

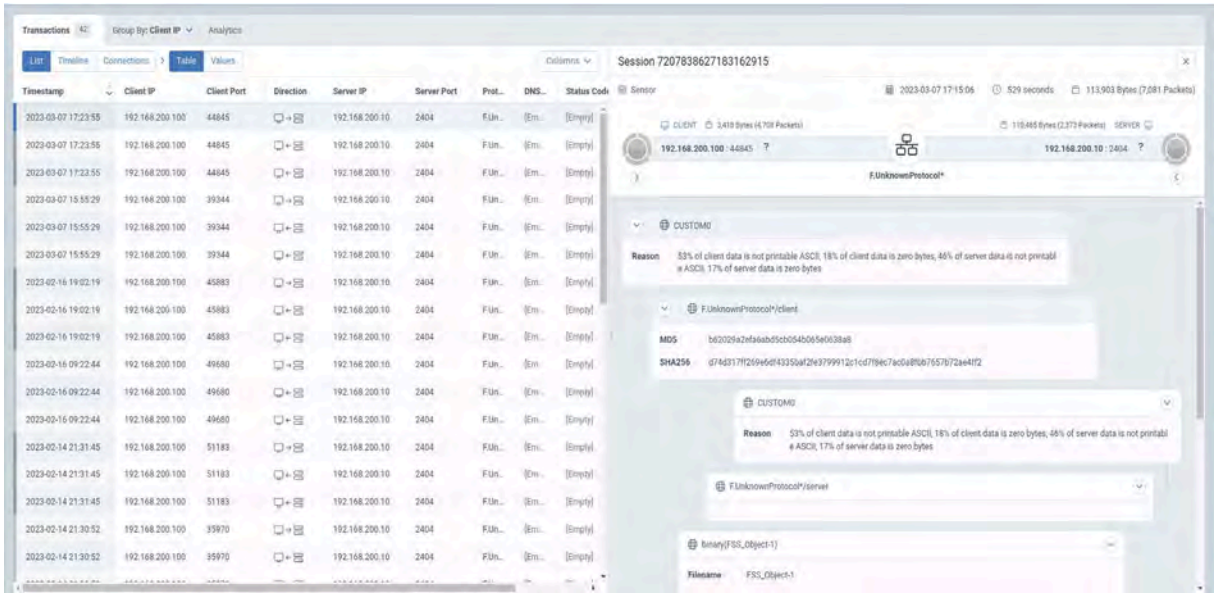


Abbildung 69: Metadaten von Fidelis

5.15.3. Firmware-Analyse

Eine Schwachstelle in der Firmware eines Smart Grid-Geräts kann schwerwiegende Folgen haben. Denn dadurch können Angreifer auf das Gerät zugreifen, ohne dass dies von Sicherheitsmaßnahmen wie Firewalls und Anti-Malware-Programmen erkannt wird. In der Firmware können auch Hintertüren oder unentdeckte Schwachstellen vorhanden sein, die es Angreifern ermöglichen, das Gerät zu übernehmen oder zu manipulieren. Wenn diese Schwachstellen nicht entdeckt und behoben werden, können sie dazu führen, dass ein Angreifer das Gerät in einem Smart Grid-Netzwerk kontrollieren oder stören kann, was zu Ausfällen oder sogar zu schwerwiegenden Sicherheitsverletzungen führen kann. Daher ist es wichtig, die Firmware von Smart Grid-Geräten auf Schwachstellen zu untersuchen und sicherzustellen, dass alle bekannten Schwachstellen durch Updates oder Patches behoben werden.

Das Tool OneKey wird eingesetzt, um IoT-Geräte auf bekannte Schwachstellen und Sicherheitsrisiken zu untersuchen, indem es die Firmware der Geräte analysiert.

Dabei wurde speziell die Firmware-Version 1.0.1_8210 des Wago Application Grid Gateways und die Firmware-Version 1.0.0.r12145 des LTE Industry Routers TK800 untersucht. Nach dem Hochladen der Firmware-Dateien in OneKey konnte das Tool Schwachstellen wie Path Traversal-Angriffe erkennen. Path Traversal ist eine Angriffstechnik, bei der ein Angreifer versucht, unautorisierten Zugriff auf Dateien oder Verzeichnisse zu erlangen, die sich außerhalb des intendierten Pfades befinden. Dabei wird versucht, durch Manipulation von Datei- oder Verzeichnisnamen Zugriff auf andere Bereiche des Dateisystems zu erhalten. Path Traversal-Angriffe können zum Beispiel dazu führen, dass der Angreifer

vertrauliche Daten lesen, schreiben oder ausführen kann, auf die er normalerweise keinen Zugriff hätte. Es handelt sich um eine weit verbreitete Angriffstechnik und stellt somit eine wichtige Schwachstelle dar, die bei der Sicherheitsanalyse von IT-Systemen berücksichtigt werden muss.

Wir konnten auch eine Schwachstelle, welche das Ausführen von Programmcode auf dem System ermöglichen könnte, identifizieren. Zusätzlich wurden drei öffentliche SSH-Schlüssel gefunden, welche den Zugriff auf das Gerät ohne Eingabe eines Passworts ermöglichen und zwei in den Programmcode encodierte Passwort-Hashes.

Die kritischsten Schwachstellen des Wago Application Grid Gateways sind in *Abbildung 70: Mit OneKey gefundene Schwachstellen des Wago Application Grid Gateways* aufgelistet, während die gefundenen Passwort-Hashes in *Abbildung 71* dargestellt sind. Ein Beispiel für einen der gefundenen SSH-Schlüssel ist in *Abbildung 72* zu sehen. Durch die Untersuchung der Firmware von IoT-Geräten können potenzielle Schwachstellen aufgedeckt und behoben werden, um die Sicherheit der Smart Grid-Infrastruktur zu verbessern.

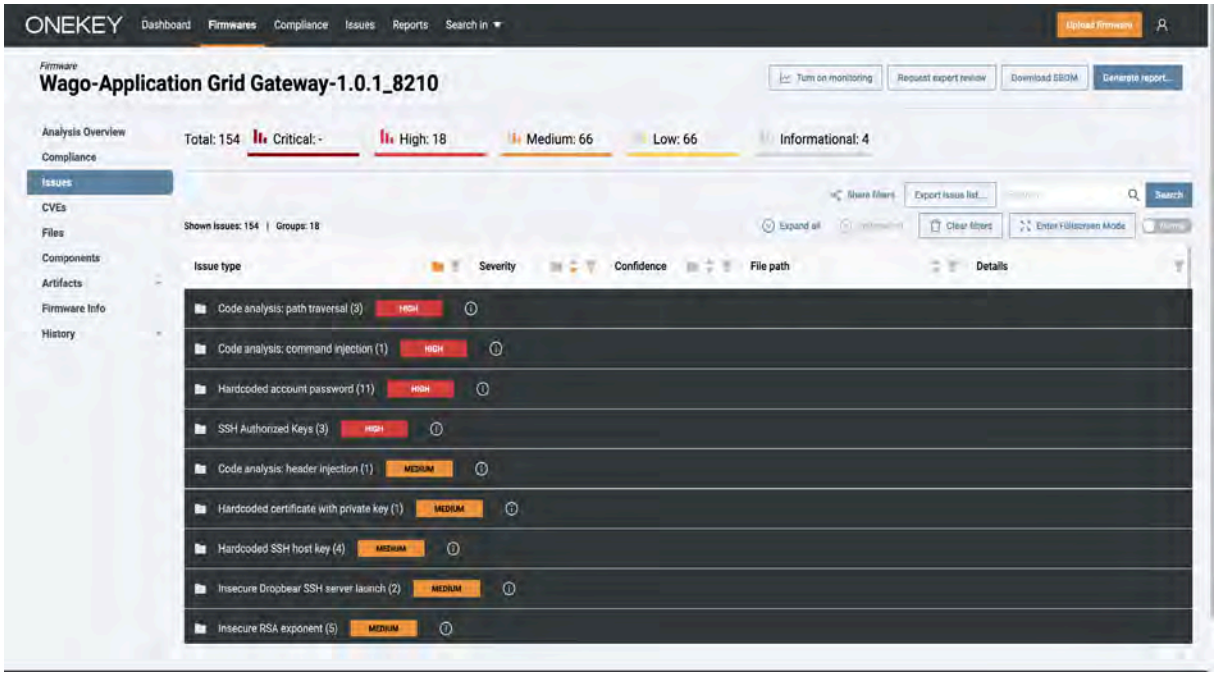


Abbildung 70: Mit OneKey gefundene Schwachstellen des Wago Application Grid Gateways

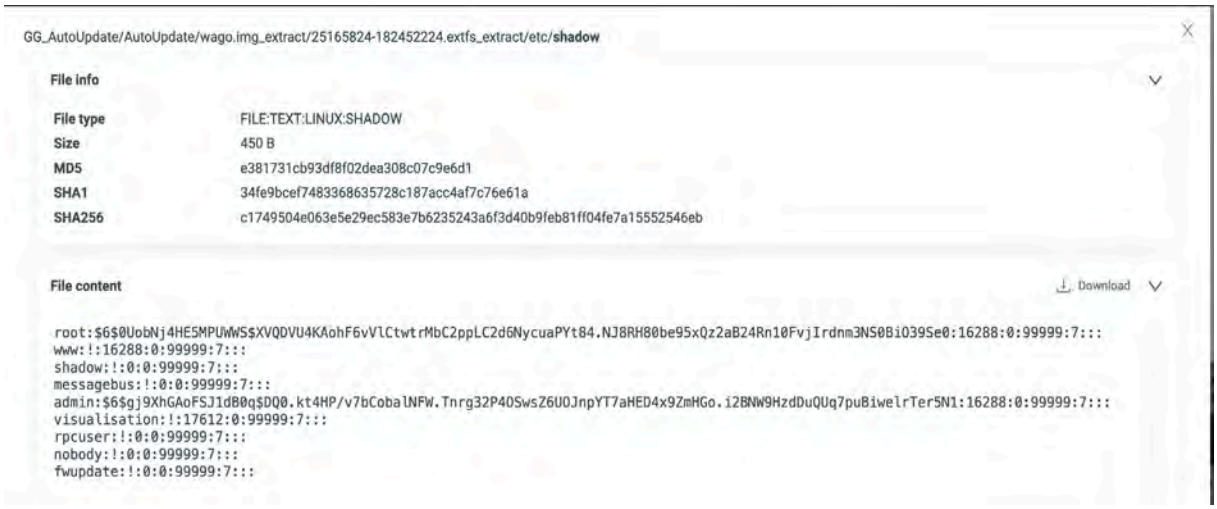


Abbildung 71: In der Wago-Firmware gefundene Passwort-Hashes

Abbildung 72: In der Firmware gefundener öffentlicher SSH-Schlüssel

Auch für den LTE Industry Router TK800 konnte OneKey Schwachstellen finden, allerdings nur mit mittlerem Risiko, wie beispielsweise ein privater Schlüssel (siehe Abbildung 73) sowie unverschlüsselte Kommunikation mittels curl (siehe Abbildung 74).

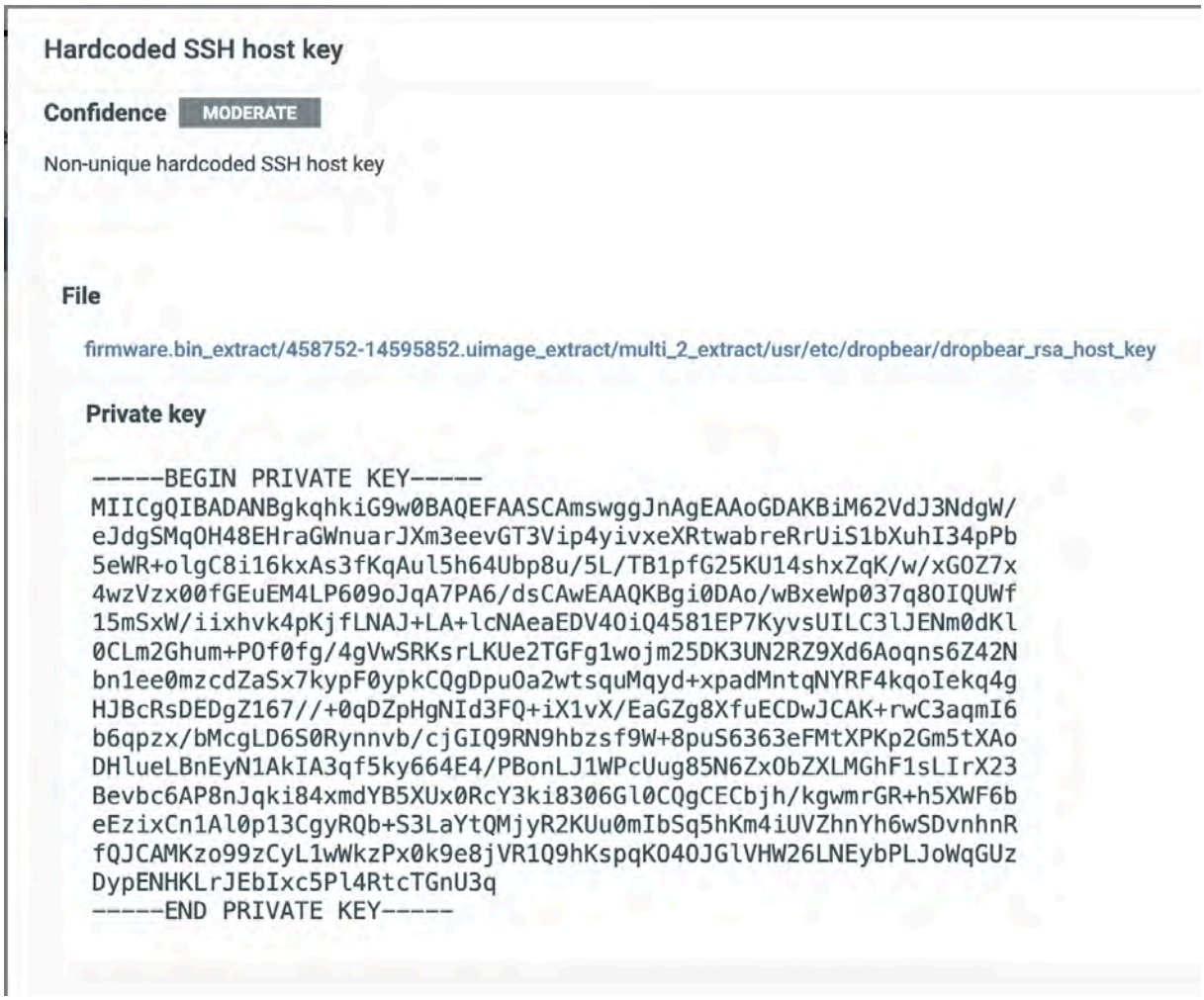


Abbildung 73: Privater Schlüssel in der Firmware des LTE Industry Routers TK800

Abbildung 74: Unverschlüsselte Kommunikation in der Firmware des LTE Industry Routers TK800

Außer den beiden erwähnten Firmware-Versionen versuchte die QGroup zusätzlich, die Firmware mehrerer im Smart Grid Lab verbauter Siemens-Geräte mit OneKey zu analysieren. Dies schlug jedoch fehl, da das Betriebssystem dieser Geräte zum Zeitpunkt der Testdurchführung nicht durch OneKey unterstützt wurde.

OneKey kann auch Stichproben der eingesetzten Geräte auf Lieferkettenangriffe untersuchen. Bei einem Lieferkettenangriff handelt es sich um eine Art von Cyberangriff, der darauf abzielt, die

Lieferkette zu kompromittieren, indem bösartige Komponenten oder Firmware in Hardwaregeräte eingeschleust werden. Eine kompromittierte Hardware in einer industriellen Steuerung kann einem Angreifer Fernzugriff und Kontrolle über das Gerät ermöglichen, was möglicherweise zu physischem Schaden oder Betriebsunterbrechungen führen kann.

Die häufigsten Arten von Supply Chain-Angriffen sind gefälschte Komponenten, schädliche Firmware, Hardware-Manipulation und Insider-Bedrohungen. Um solche Angriffe auf die Lieferkette zu verhindern, ist es wichtig, über eine sichere Lieferkette zu verfügen, die die Überprüfung der Authentizität aller Komponenten und die Überwachung der Lieferkette auf verdächtige Aktivitäten umfasst. Regelmäßige Sicherheitsaudits und Schwachstellen-bewertungen können auch dazu beitragen, Schwachstellen in industriellen Steuerungen zu erkennen und zu beheben.

Die Schwachstellen sind in späteren Versionen der Firmware behoben. Dies unterstreicht wiederum die Bedeutung der fortlaufenden Überwachung und Aktualisierung der Firmwarestände.

5.16 Analyse des OT-Netzwerkes

Es ist wichtig, das OT-Netzwerk auf Schwachstellen zu untersuchen, da diese Netzwerke normalerweise eine Vielzahl von Geräten und Systemen enthalten, die speziell für die Steuerung industrieller Prozesse und kritischer Infrastrukturen entwickelt wurden. Wenn diese Geräte Schwachstellen aufweisen, kann dies schwerwiegende Auswirkungen auf die Sicherheit und Zuverlässigkeit dieser Prozesse haben.

Darüber hinaus verwenden viele OT-Netzwerke veraltete Systeme und Protokolle, die nicht mehr aktualisiert oder unterstützt werden, was sie anfälliger für Angriffe macht. Die meisten herkömmlichen IT-Sicherheitswerkzeuge sind nicht in der Lage, diese veralteten Systeme und Protokolle zu erkennen oder zu überwachen, was die Notwendigkeit von spezialisierten OT-Sicherheitstools und -Technologien betont.

Eine regelmäßige Untersuchung auf Schwachstellen im OT-Netzwerk kann dazu beitragen, potenzielle Angriffsvektoren zu identifizieren und proaktiv Maßnahmen zu ergreifen, um Schwachstellen zu beheben und das Risiko von Cyberangriffen zu minimieren.

Tenable OT ist eine OT-Tool, welches ähnlich wie Fidelis den Traffic im Netzwerk beobachtet, jedoch im Gegensatz zu klassischen Schwachstellenscannern wie Nessus keine aktiven Scans durchführt.

Im Smart Grid Lab wurde Tenable OT mit demselben Mirror Port verbunden wie auch Fidelis und lieferte eine vollständige Inventarisierung des Netzwerks samt einer graphischen Darstellung der Kommunikationspartner (siehe Abbildung 75).

Wie auch arpwatch kann Tenable OT neue Kommunikationsteilnehmer im Netzwerk sowie Änderungen an der Paarung IP-Adresse zu MAC-Adresse bei bekannten Kommunikationspartnern bemerken.

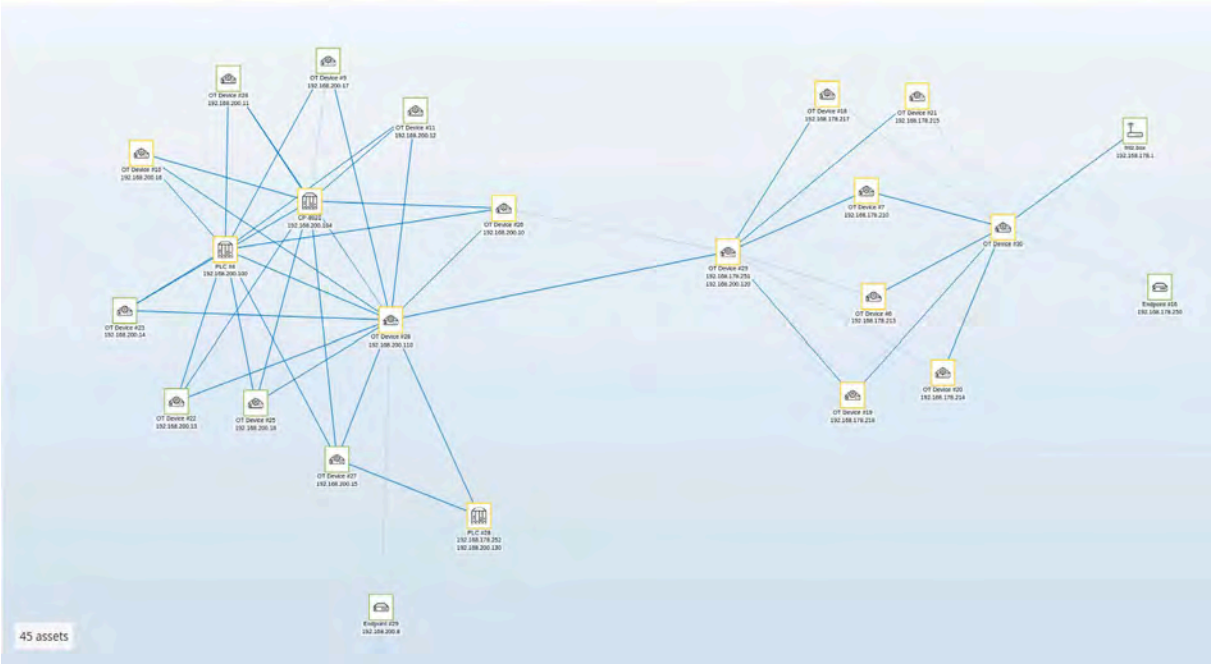


Abbildung 75: Graphische Darstellung des Smart Grid Lab in Tenable OT

Es werden alle Kommunikationen aufgelistet, die Tenable OT im Netzwerk beobachtet hat. Dazu gibt es sowohl eine graphische Übersicht (siehe Abbildung 76) als auch eine detaillierte tabellarische Darstellung (siehe Abbildung 77) und optional können Packet Captures erstellt werden.

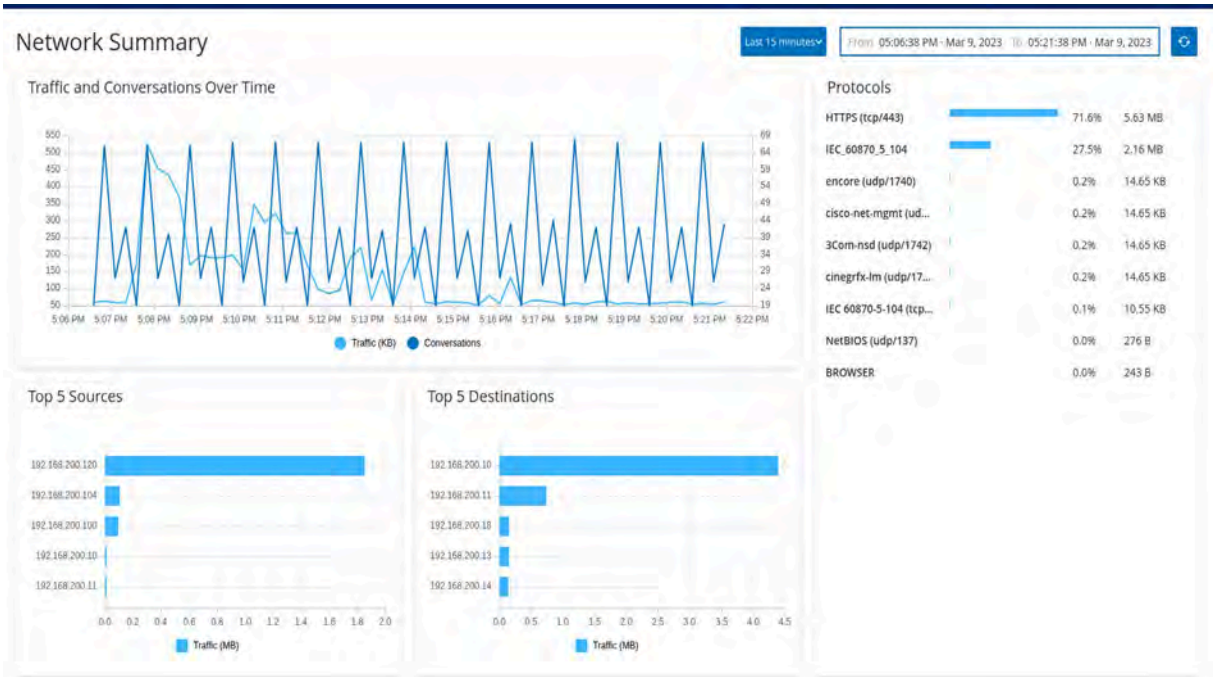


Abbildung 76: Graphische Übersicht der von Tenable OT beobachteten Kommunikationen im Smart Grid Lab

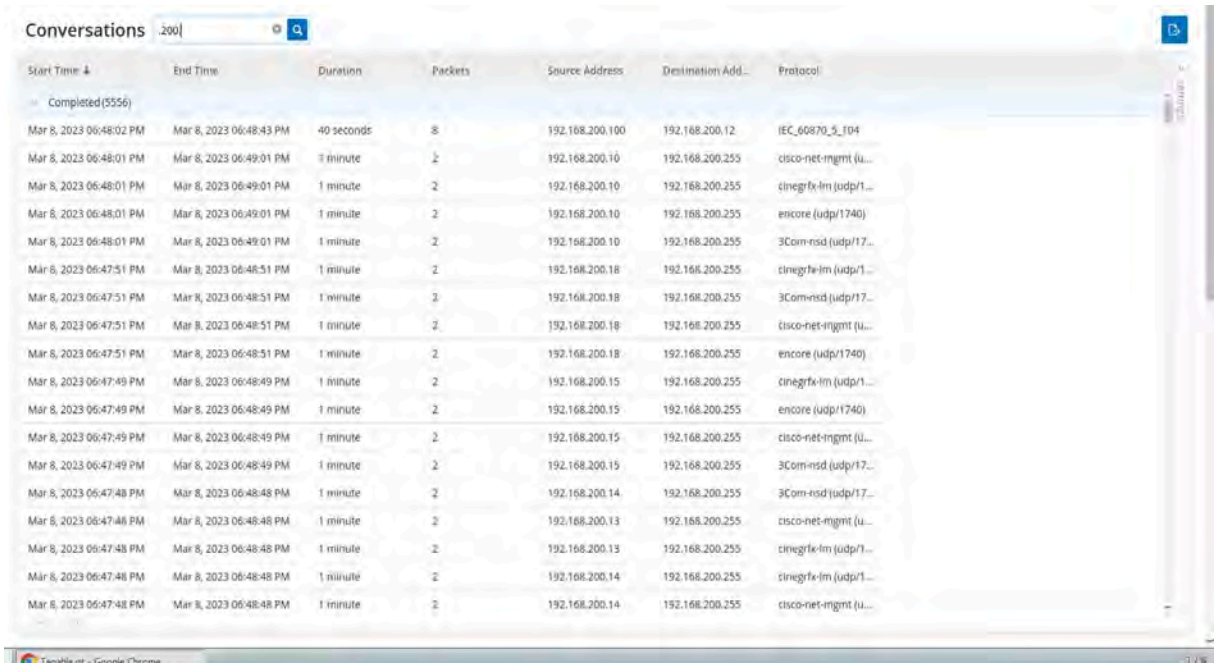


Abbildung 77: Von Tenable OT geloggte Kommunikationen

Alle erfassten Kommunikationsteilnehmer werden auf Schwachstellen hin überprüft. Diese Prüfung umfasst geöffnete Ports, beobachtete Kommunikationen sowie mögliche Angriffsvektoren.

Beispielhaft zeigt Abbildung 78 die von Tenable OT erkannten Schwachstellen der Siemens A8000 und in Abbildung 79 wird ein von Tenable OT generierter Angriffsvektor auf die Siemens A8000 dargestellt.

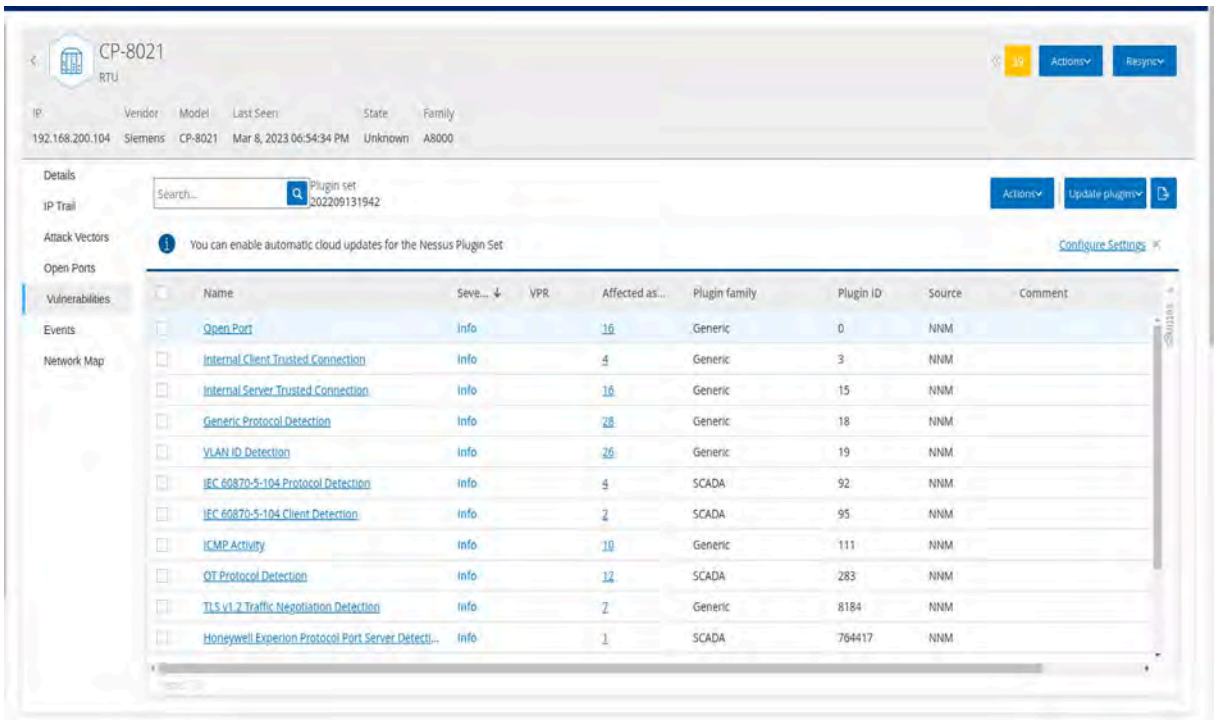


Abbildung 78: Von Tenable OT gefundene Schwachstellen der Siemens A8000

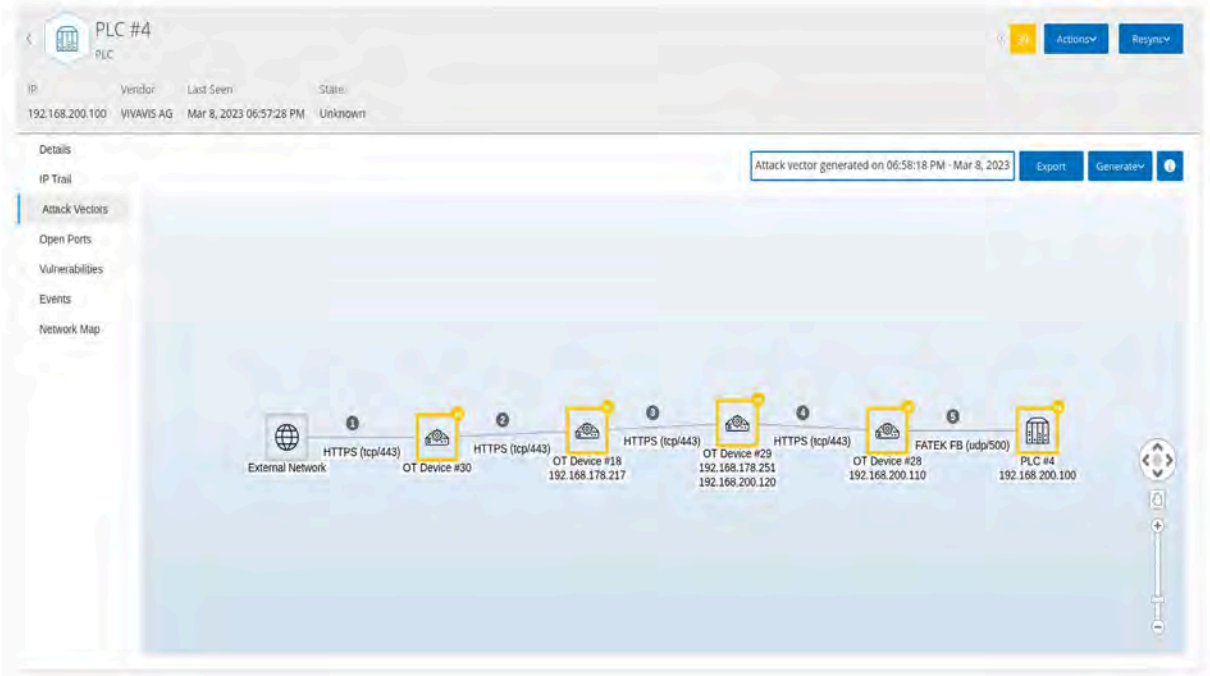


Abbildung 79: Von Tenable OT generierter Angriffsvektor

Eine weitere Besonderheit von Tenable OT besteht darin, dass es damit möglich ist, aus dem über eine längere Zeit, wie beispielsweise drei Wochen, beobachteten Netzwerkverkehr eine sogenannte Baseline zu erzeugen. Diese Baseline umfasst alle Kommunikationspartner im Netzwerk mit ihrer MAC- und IP-Adresse sowie alle Kommunikationswege, die seitens Tenable beobachtet wurden. Ändert sich daran nach Erstellung der Baseline etwas, kann Tenable OT entsprechende Alarme erzeugen wie beispielsweise eine Benachrichtigung per E-Mail (siehe Abbildung 80).

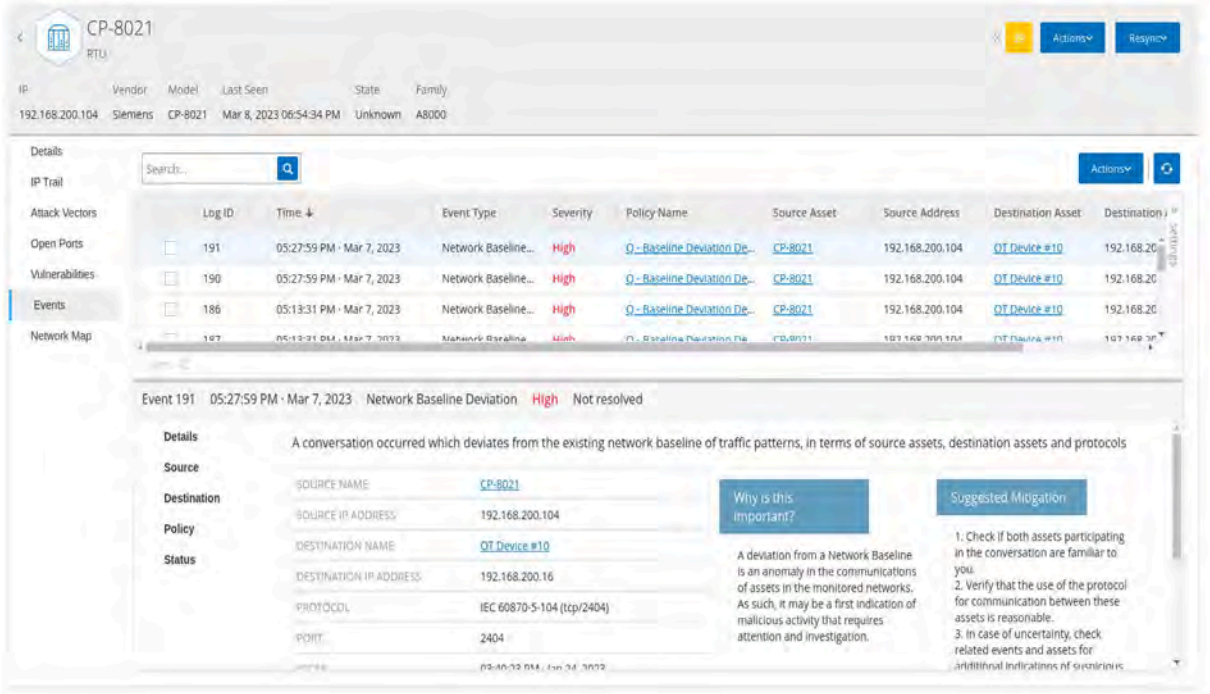


Abbildung 80: Von Tenable OT geloggte Abweichung von der Baseline

5.16.1. Angriffe auf das IEC 60870-5-104-Protokoll

IEC 60870-5-104 ist ein weit verbreitetes Protokoll, das in der Energieversorgungsbranche verwendet wird, um Daten zwischen Kontrollzentren und Schaltanlagen auszutauschen. Es ermöglicht eine sichere Übertragung von Steuerbefehlen, Statusmeldungen und anderen wichtigen Informationen in Echtzeit. In der heutigen vernetzten Welt, in der Cyberangriffe auf kritische Infrastrukturen zunehmen, ist es von entscheidender Bedeutung, dass das Protokoll und die damit verbundenen Systeme auf Schwachstellen und potenzielle Angriffsszenarien untersucht werden. Eine solche Untersuchung kann dazu beitragen, Schwachstellen aufzudecken, die von Angreifern ausgenutzt werden können, um das Protokoll zu manipulieren, zu unterbrechen oder um Schäden an kritischen Infrastrukturen zu verursachen. Daher ist es wichtig, dass Unternehmen und Organisationen, die das IEC 60870-5-104-Protokoll einsetzen, regelmäßige Sicherheitsüberprüfungen durchführen, um sicherzustellen, dass ihre Systeme und Daten vor potenziellen Angriffen geschützt sind.

Analyse
Das Vorgehen der QGroup zur Durchführung eines Angriffs auf das IEC 60870-5-104-Protokoll umfasst mehrere Schritte. Zunächst wurde der Netzwerkverkehr im IEC 60870-5-104-Netzwerk mit einem tcpdump aufgezeichnet. Dazu wurde eine Ubuntu VM genutzt, die mit dem Mirror Port verbunden war. Über mehrere Tage hinweg wurde der Verkehr aufgezeichnet und anschließend mit Hilfe von Wireshark (siehe Abbildung 81) genauer untersucht.

Bei der Analyse des Netzwerkverkehrs wurde festgestellt, dass sämtlicher Verkehr im IEC 60870-5-104-Netzwerk unverschlüsselt und ohne jegliche Authentifizierung erfolgt. Das bedeutet, dass alle übermittelten Messwerte und Steuerbefehle von jedem Kommunikationsteilnehmer mitgelesen und auch manipuliert werden könnten. Dies stellt ein erhebliches Sicherheitsrisiko dar.

Im Netzwerkverkehr konnten unter anderem die folgenden Nachrichtentypen beobachtet werden:

M_ME_TF_1
M_SP_TB_1
C_DC_TA_1

Dabei handelt es sich um Nachrichten zur Übertragung von Messwerten sowie zur Übermittlung von Befehlen. Durch die Analyse dieser Nachrichtentypen können Schwachstellen im Protokoll aufgedeckt werden, die für einen potenziellen Angreifer ausnutzbar wären.

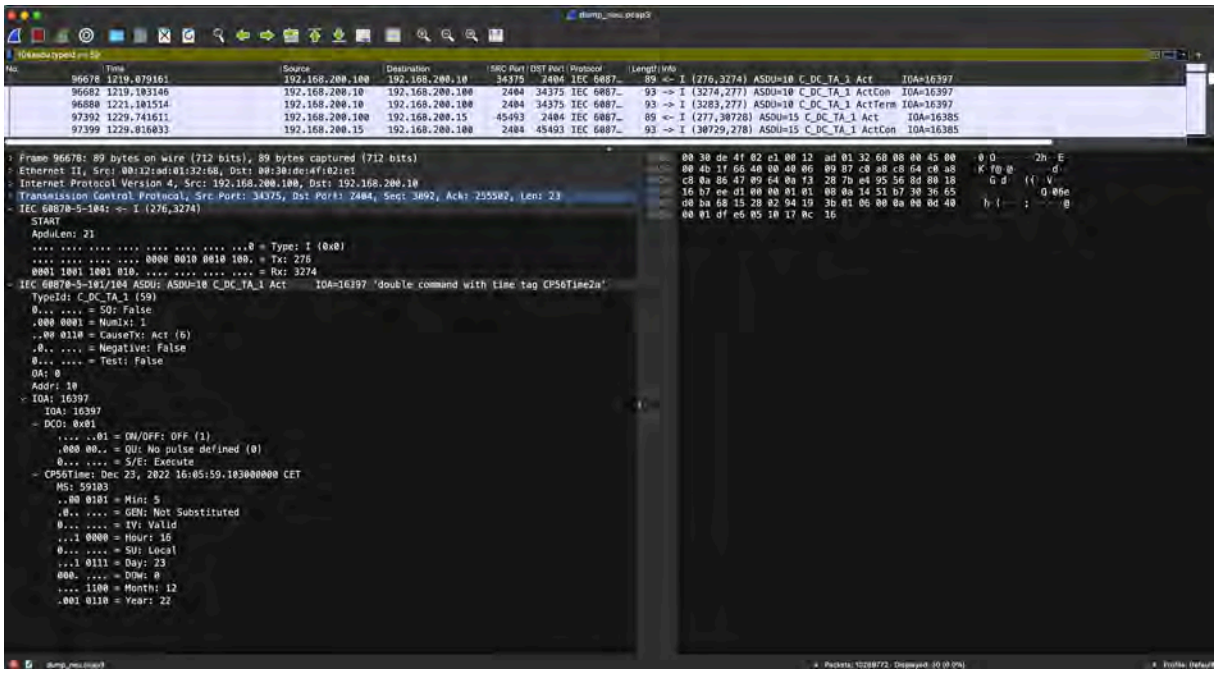


Abbildung 81: Analyse des Netzwerkverkehrs in Wireshark

Metasploit IEC104 Client Utility

Das Metasploit IEC104 Client Utility ist ein Werkzeug, das als Teil der Metasploit Framework-Suite bereitgestellt wird und speziell für Angriffe auf Systeme entwickelt wurde, die das IEC 60870-5-104-Protokoll verwenden. Es kann verwendet werden, um sich als Client in ein IEC 60870-5-104-Netzwerk einzuschleusen und Kommunikationsvorgänge mit anderen Geräten in diesem Netzwerk zu simulieren. Auf diese Weise können Sicherheitslücken und Schwachstellen im Netzwerk ausgenutzt werden, um unbefugten Zugriff zu erlangen, Informationen zu stehlen oder sogar Schaden anzurichten. Das Metasploit IEC104 Client Utility ist ein leistungsstarkes Werkzeug, das von Penetrationstestern und Ethical Hackern eingesetzt wird, um die Sicherheit von IEC 60870-5-104-Netzwerken zu testen und zu verbessern.

Die QGroup nutzte das Metasploit IEC104 Client Utility für weitere Untersuchungen. Dieses erwartet als Eingabe eine Liste von Zielen. Hier verwendete die QGroup das gesamte Class-C-Netz 192.168.200.0/24. Zusätzlich erwartet das Tool einen Nachrichtentyp. Hier verwendete die QGroup die Nachrichtentypen M_ME_TF_1 und C_DC_TA_1, die im Dump des Netzwerkverkehrs gefunden worden waren. Zusätzlich wurde auch der Nachrichtentyp C_DC_NA_1 verwendet.

Wie die Ausgabe in Abbildung 82 zeigt, war es so möglich, mit mehreren Komponenten im Smart Grid Lab zu kommunizieren. Folgende Geräte antworteten:

192.168.200.10

192.168.200.11

192.168.200.13

192.168.200.14

192.168.200.15

192.168.200.17

192.168.200.18

192.168.200.104 (Verbindung abgewiesen)

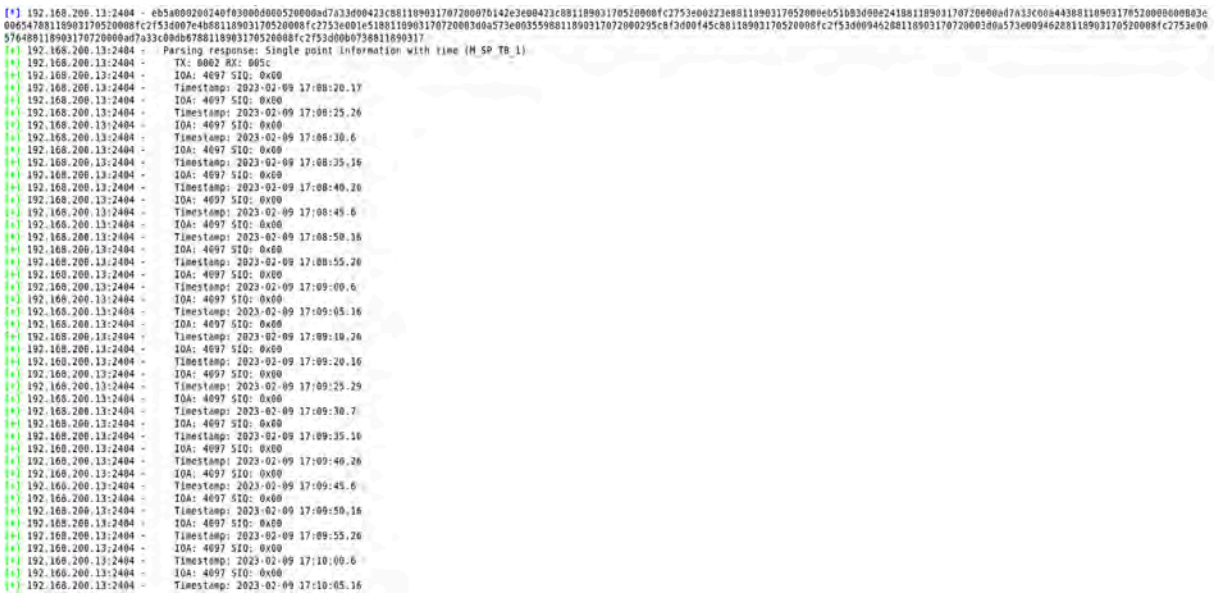


Abbildung 82: Kommunikation zwischen der QGroup Ubuntu VM und einem Gerät im Smart Grid Lab

Die erfolgreiche Kommunikation ist auch im tcpdump sichtbar, der in Abbildung 83 zu sehen ist.

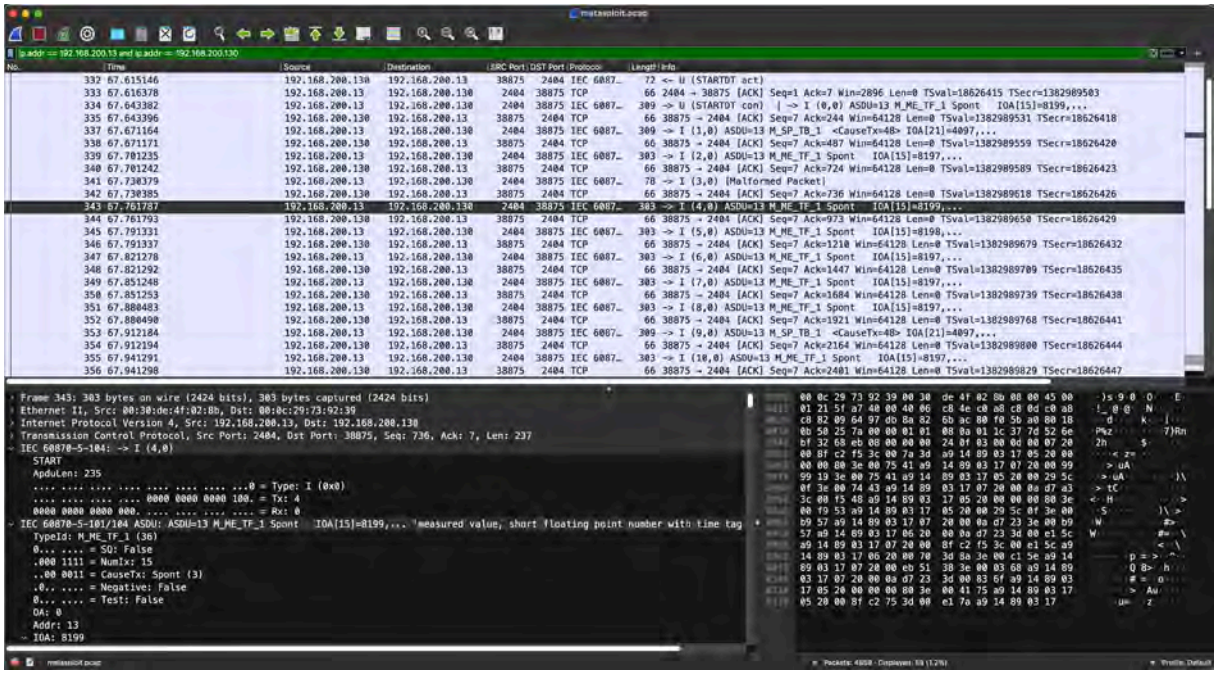


Abbildung 83: tcpdump der Kommunikation der Ubuntu VM mit dem Gerät 192.168.200.13

ARP-Poisoning

ARP-Poisoning ist eine Technik, bei der ein Angreifer das Address Resolution Protocol (ARP) ausnutzt, um die Kommunikation zwischen zwei Geräten in einem Netzwerk zu manipulieren. Das ARP-Protokoll

wird verwendet, um die MAC-Adresse eines Geräts in eine IP-Adresse aufzulösen, damit Geräte im Netzwerk miteinander kommunizieren können. Bei ARP-Poisoning sendet der Angreifer gefälschte ARP-Antworten aus, um die MAC-Adresse eines anderen Geräts in der Netzwerkumgebung zu verändern. Dadurch wird die Kommunikation zwischen dem betroffenen Gerät und anderen Geräten im Netzwerk über den Angreifer umgeleitet. Der Angreifer kann somit den Netzwerkverkehr abhören, manipulieren oder sogar blockieren, indem er die Pakete verwirft oder umleitet.

ARP-Poisoning kann auch verwendet werden, um eine Man-in-the-Middle (MitM)-Attacke durchzuführen, bei der der Angreifer sich als ein anderes Gerät im Netzwerk ausgibt und die Daten zwischen den betroffenen Geräten abfängt und manipuliert. Diese Technik kann verwendet werden, um vertrauliche Daten wie Passwörter oder Kreditkarteninformationen zu stehlen, oder um Malware zu verbreiten.

Es ist wichtig, Netzwerke gegen ARP-Poisoning-Angriffe zu schützen, indem z. B. ARP-Monitoring Tools verwendet werden, die den Netzwerkverkehr überwachen und verdächtige Aktivitäten erkennen können. Es sollten auch Sicherheitsmaßnahmen wie die Überwachung von Netzwerkverkehr, die Implementierung von Verschlüsselung und Authentifizierung sowie die Durchführung regelmäßiger Sicherheitsüberprüfungen und Audits ergriffen werden, um Netzwerkangriffe zu verhindern.

Die QGroup versuchte, von der Ubuntu VM aus mithilfe des Tools arpspoof den Verkehr zwischen den beiden Systemen 192.168.200.13 und 192.168.200.100 zu intercepten.

Dazu wurden an beide Systeme entsprechende gefälschte ARP-Replys geschickt wie in Abbildung 84 zu sehen ist. Allerdings schienen die beiden Geräte nicht auf diese Art von Angriff zu reagieren, wie Abbildung 85 zeigt.

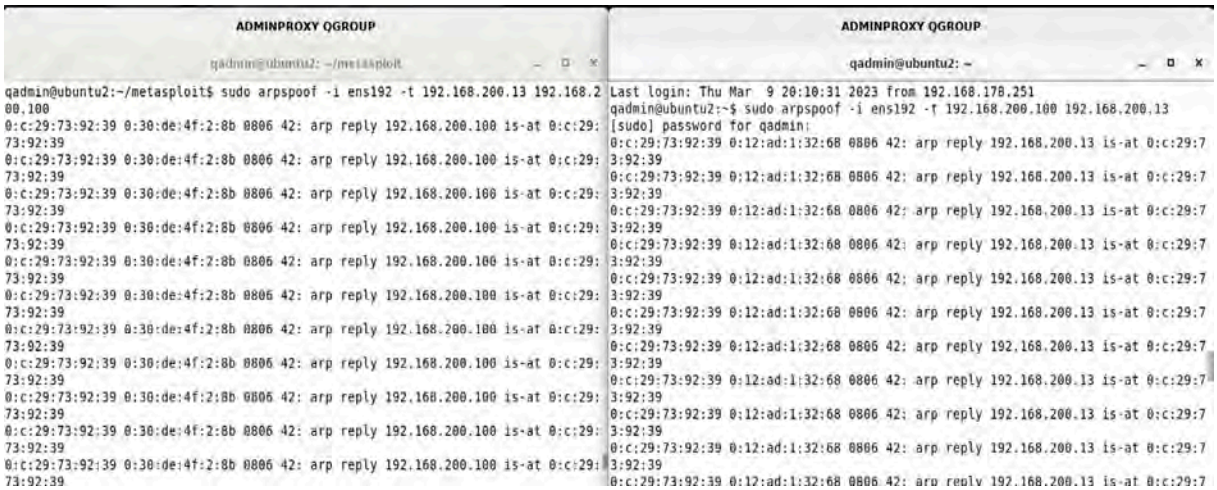


Abbildung 84: arpspoof-Attacke gegen die beiden Systeme 192.168.200.13 und 192.168.200.100

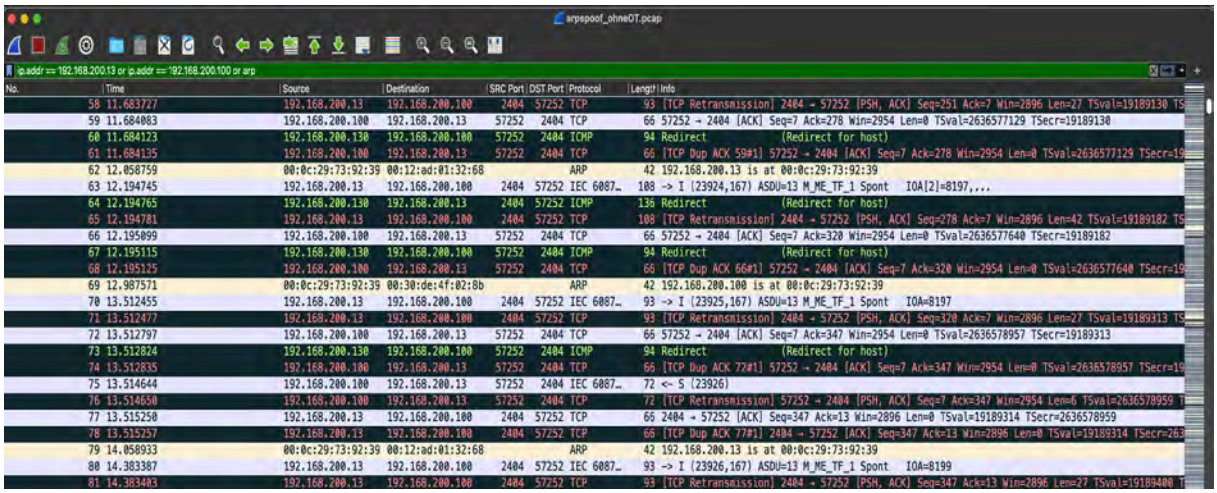


Abbildung 85: Kommunikation der beiden Geräte 192.168.200.13 und 192.168.200.100 trotz ARP-Poisoning

Vermutlich werden die ARP-Adressen im Smart Grid Lab einmal beim Start ausgetauscht oder sie sind sogar hart eingestellt. Gegen letztere These spricht jedoch der Umstand, dass der Fernwirkkopf 192.168.200.100 regelmäßig ARP-Anfragen für die nicht im Smart Grid Lab vorhandenen Geräte 192.168.200.9 und 192.168.200.20 stellte.

Die QGroup gab der Ubuntu VM der Reihe nach beide IP-Adressen und der Fernwirkkopf versuchte direkt, mit der Ubuntu VM im IEC 60870-5-104-Protokoll zu kommunizieren (siehe Abbildung 86).

Dies stellt somit einen interessanten Angriffsvektor dar: Ein Angreifer beobachtet die ARP-Pakete dahingehend, ob der Fernwirkkopf nach einem System sucht, das bei ihm als Kommunikationspartner eingestellt ist, jedoch nicht erreichbar ist. Er gibt sich dann die entsprechende IP-Adresse und kann im Netzwerk kommunizieren. Falls das Gerät nur temporär nicht erreichbar ist, der Fernwirkkopf also keine ARP-Anfragen für das Gerät stellt, könnten jedoch Pakete im IEC 60870-5-104-Protokoll, die ins Leere laufen, einem Angreifer helfen. Dieser würde sich dann die MAC-Adresse des fehlenden Geräts geben, um im Netzwerk kommunizieren zu können.

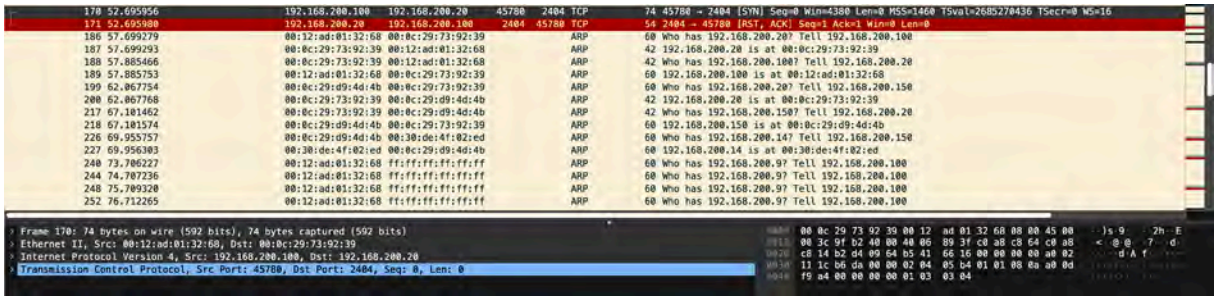


Abbildung 86: Kommunikation des Fernwirkkopfes mit der Ubuntu VM

5.17 QGroup-Praxisempfehlungen

Die QGroup-Untersuchungen des Smart Grid Lab haben gezeigt, dass Smart Grids zahlreiche Schwachstellen aufweisen können, die es Angreifern ermöglichen, auf sensible Daten und kritische Infrastruktur zuzugreifen. Es ist jedoch wichtig zu betonen, dass wir nicht alle theoretisch möglichen Schwachstellen untersucht haben, sondern uns auf eine Auswahl konzentriert haben. Es ist daher

ratsam, dass Betreiber von Smart Grids ihre Systeme regelmäßig auf Schwachstellen und Bedrohungen untersuchen und geeignete Schutzmaßnahmen ergreifen.

Als praktische Empfehlung schlägt die QGroup vor, alle Geräte im Smart Grid, soweit möglich, mit einer EDR-Lösung auszustatten. Mindestens die Steuerrechner sollten mit einem Betriebssystem ausgestattet sein, das von EDR-Lösungen unterstützt wird. Dadurch können Anomalien im Netzwerk erkannt werden und es können entsprechende SecOps-Prozesse etabliert werden, um darauf zu reagieren.

Eine weitere Empfehlung ist, das Netzwerk mindestens mit einem Tool wie arpwatch zu über-wachen, das neue Kommunikationspartner oder Änderungen an bekannten Kommunikations-partnern erkennt und entsprechende Alarmierungen versendet. Für eine umfassendere Lösung sollten Betreiber eine speziell an OT-Netzwerke angepasste Lösung wie Tenable OT einsetzen. Zudem sollten ausschließlich Switche verwendet werden, die gemanaged werden können, um neue Kommunikationspartner nicht nur schnell erkennen zu können, sondern auch von der Teilnahme an der Netzwerkkommunikation ausschließen zu können.

Eine weitere Empfehlung ist, Plausibilitätsprüfungen der Messwerte und Steuerungsbefehle durchzuführen, um sicherzustellen, dass nur legitime Befehle ausgeführt werden. Außerdem sollten Betreiber TLS-Verschlüsselung für die Kommunikation zwischen den Teilnehmern im IEC 60870-5-104-Netzwerk verwenden und für die TLS-Verschlüsselung im IEC 60870-5-104-Netzwerk wie auch für den Zugriff auf Web-Schnittstellen eine eigene vertrauenswürdige PKI anstelle von selbstsignierten Zertifikaten verwenden.

Ein weiterer wichtiger Punkt ist, regelmäßig die Firmware aller Komponenten auf neu erkannte Sicherheitslücken zu überprüfen und gegebenenfalls zu aktualisieren.

Es ist auch empfehlenswert, einen SecOps-Prozess zu etablieren, der beschreibt, wie mit den Alarmen der oben genannten Security Tools umgegangen werden soll, damit diese auch abgearbeitet werden.

Schließlich sollten Betreiber auf bestmögliche physische Sicherheit achten, um zu verhindern, dass Angreifer einfach an Netzwerkverteiler gelangen und dort eigene Geräte installieren können. Eine Anomalie-Erkennung für die physischen Bereiche ist ebenfalls empfehlenswert, um ungewöhnliche Aktivitäten zu erkennen und darauf zu reagieren.

Zusammenfassend ist es wichtig, dass Betreiber von Smart Grids geeignete IT- und OT-Schutzmaßnahmen ergreifen, um ihre Systeme vor Bedrohungen zu schützen.

5.18 QGroup-Zusammenfassung

Smart Grids sind eine Weiterentwicklung der traditionellen Stromnetze, die darauf abzielen, die Effizienz und Zuverlässigkeit der Energieversorgung zu verbessern. Die Notwendigkeit von Smart Grids ergibt sich aus den Herausforderungen, die traditionelle Stromnetze derzeit und in Zukunft zu bewältigen haben. Diese Herausforderungen umfassen unter anderem den Anstieg des Energiebedarfs aufgrund des Wachstums der Weltbevölkerung und der Urbanisierung, den Ausbau erneuerbarer Energien und die Notwendigkeit, die Energieeffizienz zu verbessern.

Smart Grids setzen auf innovative Technologien wie intelligente Sensoren, Netzwerkkommunikation und Automatisierung, um die Energieversorgung zu optimieren und die Effizienz zu steigern. Sie

ermöglichen es auch, erneuerbare Energiequellen wie Wind- und Solarenergie besser in das Stromnetz zu integrieren und den Energieverbrauch in Zeiten hoher Nachfrage zu steuern. Darüber hinaus bieten Smart Grids auch Vorteile für Verbraucher, indem sie ihnen bessere Kontrolle über ihren Energieverbrauch und ihre Energiekosten geben. Durch die Verwendung von Smart Meter-Technologie können Verbraucher ihren Energieverbrauch in Echtzeit überwachen und entsprechende Maßnahmen ergreifen, um den Verbrauch zu reduzieren und damit Kosten zu sparen. Insgesamt sind Smart Grids notwendig, um die Herausforderungen der modernen Energieversorgung zu bewältigen und die Effizienz und Zuverlässigkeit der Energieversorgung zu verbessern.

Die Sicherheit von Smart Grids ist von entscheidender Bedeutung, da es sich hierbei um eine kritische Infrastruktur handelt, die nicht nur das tägliche Leben der Menschen beeinflusst, sondern auch die Wirtschaft eines Landes und dessen Sicherheit. Smart Grids haben das Potenzial, die Effizienz und Zuverlässigkeit des Stromnetzes zu verbessern, indem sie die Integration von erneuerbaren Energiequellen und die Möglichkeit zur Echtzeit-Überwachung und -Steuerung des Stromnetzes ermöglichen. Gleichzeitig bringt die Technologie jedoch auch neue Sicherheitsrisiken mit sich, da das Stromnetz mit dem Internet verbunden ist und somit anfälliger für Cyberangriffe ist.

Die Sicherheit von Smart Grids ist jedoch auch komplex, da es sich um ein dezentrales Netzwerk handelt, das aus vielen verschiedenen Komponenten und Subsystemen besteht, die von verschiedenen Herstellern stammen und unterschiedliche Protokolle und Technologien verwenden. Zudem haben viele Komponenten im Smart Grid eine lange Lebensdauer und können nicht einfach durch neuere und sicherere Komponenten ersetzt werden. Dies bedeutet, dass Sicherheitslücken und Schwachstellen, die heute vorhanden sind, möglicherweise noch in vielen Jahren bestehen bleiben.

Die Sicherheit von Smart Grids erfordert daher eine umfassende, systemische Betrachtung, die sowohl die IT- als auch die OT-Komponenten umfasst. Eine Sicherheitsstrategie für Smart Grids sollte darauf abzielen, alle potenziellen Bedrohungen zu identifizieren und geeignete Maßnahmen zu ergreifen, um sie zu verhindern, zu erkennen und darauf zu reagieren. Hierbei spielen auch die Einhaltung von Sicherheitsstandards, die Schulung von Mitarbeitern sowie die regelmäßige Durchführung von Sicherheitsaudits eine wichtige Rolle.

Insgesamt ist es von großer Bedeutung, dass Sicherheitsaspekte von Anfang an in die Planung und Umsetzung von Smart Grids einbezogen werden, um ein höheres Maß an Sicherheit und Widerstandsfähigkeit zu gewährleisten.

Die QGroup hat im Rahmen ihrer Untersuchungen eine Vielzahl von Schwachstellen und Be-drohungen in Smart Grids identifiziert. Diese reichen von ungesicherten Protokollen bis hin zu schlecht konfigurierten Netzwerken. Es ist wichtig, dass die Betreiber von Smart Grids diese Schwachstellen identifizieren und geeignete Schutzmaßnahmen ergreifen, um ihre Systeme zu schützen. In diesem Kontext hat die QGroup im Smart Grid Lab verschiedene Untersuchungen durchgeführt, um Schwachstellen und Angriffsvektoren zu überprüfen und geeignete Schutzmaßnahmen zu entwickeln.

Die QGroup hat jedoch nur eine Auswahl dieser Bedrohungen untersucht, da sie nicht alle theoretischen Schwachstellen testen und andere Forschungsgruppen im Lab nicht stören wollte. Für die Untersuchung wurden verschiedene Tools und Methoden eingesetzt, darunter Netzwerk-Forensik-Tools wie Fidelis und OT-Tools wie Tenable OT, die speziell für OT-Netzwerke angepasste Policies und eine bessere Ergebnisqualität liefern. Die QGroup analysierte den Netzwerkverkehr über mehrere Tage mithilfe von tcpdump und wertete ihn mit Wireshark aus.

Diese Untersuchungen ergaben, dass das IEC 60870-5-104-Netzwerk unverschlüsselt und ohne jegliche Authentifizierung kommuniziert. Dies macht es möglich, dass alle übermittelten Messwerte und Steuerbefehle von jedem Kommunikationsteilnehmer mitgelesen und manipuliert werden können. Die QGroup empfiehlt daher die Verwendung von TLS-Verschlüsselung für die Kommunikation zwischen den Teilnehmern im IEC 60870-5-104-Netzwerk sowie die Überwachung des Netzwerks mit Tools wie arpwatch oder Tenable OT.

Um die Sicherheit von Smart Grids zu erhöhen, empfiehlt die QGroup die Verwendung von EDR-Lösungen, Plausibilitätsprüfungen der Messwerte und Steuerungsbefehle, regelmäßige Firmware-Updates und die Implementierung eines SecOps-Prozesses. Es ist auch wichtig, auf bestmögliche physische Sicherheit zu achten, damit Angreifer nicht einfach an Netzwerkverteiler gelangen können, um dort eigene Geräte zu installieren.

In Zukunft wird es entscheidend sein, dass Forscher und Praktiker ihre Bemühungen darauf konzentrieren, eine umfassende technische Analyse durchzuführen, um sicherzustellen, dass Smart Grids sicher und widerstandsfähig sind. Es wird auch wichtig sein, dass die Hersteller von Smart Grid-Komponenten angepasste Sicherheitsstandards implementieren und regelmäßig Updates bereitstellen, um die Sicherheit der Infrastruktur zu gewährleisten. Schließlich müssen auch die Betreiber von Smart Grids eng mit den Herstellern und Forschern zusammenarbeiten, um eine sichere und widerstandsfähige Infrastruktur zu gewährleisten.

Als Ausblick für die Sicherheit bei Smart Grids stellt die QGroup fest, dass es weiterhin ein wichtiges Thema bleiben wird, da die Technologie und die damit verbundenen Risiken ständig weiterentwickelt werden. Es ist daher wichtig, dass Forscher und Praktiker sich weiterhin auf die Identifizierung von Bedrohungen und Schwachstellen konzentrieren und sich bemühen, Lösungen und Schutzmaßnahmen zu entwickeln, um diese zu minimieren oder zu vermeiden.

Eine wichtige Herausforderung besteht darin, die Cyber Security und die physische Sicherheit im Smart Grid nahtlos zu integrieren. Es müssen Maßnahmen ergriffen werden, um die physische Infrastruktur vor Angriffen und Vandalismus zu schützen, während gleichzeitig die Cybersicherheit der Netzwerke und Systeme gewährleistet wird.

Ein weiteres Forschungsthema ist die Entwicklung von neuen, angepassten Sicherheitsstandards und Protokollen für Smart Grids, die eine einheitliche und umfassende Absicherung des Systems gewährleisten. Dazu gehört auch die Standardisierung von Protokollen und Schnittstellen, um eine Interoperabilität und einen nahtlosen Datenaustausch zwischen verschiedenen Systemen zu ermöglichen.

Es ist auch wichtig, dass Unternehmen und Regierungen stärker in die Sicherheit von Smart Grids investieren, indem sie Ressourcen bereitstellen und Forschung und Entwicklung in diesem Bereich unterstützen. Eine engere Zusammenarbeit zwischen Regierungen, Industrie und Forschungseinrichtungen ist notwendig, um effektive Lösungen zu entwickeln, umzusetzen und zu betreiben

Insgesamt bleibt die Sicherheit bei Smart Grids ein komplexes Thema, das eine ganzheitliche und durchgängige Herangehensweise erfordert und ein breites Spektrum an Technologien, Strategien und Maßnahmen umfasst. Es ist daher von entscheidender Bedeutung, dass die Forschung und Entwicklung in diesem Bereich fortgesetzt werden, um die Sicherheit der Stromnetze in der Zukunft zu gewährleisten.

6. Smart Grid in Entwicklungsländern

6.1 Einleitung

Um die "Übertragbarkeit der Ergebnisse auf Energieinfrastrukturprojekte" zu gewährleisten, müssen die technischen, regulatorischen und steuerlichen Bedingungen der Entwicklungs- und Schwellenländer verstanden und mit den in Deutschland geltenden Bedingungen verglichen werden.

In diesem Projekt wurde der Reifegrad des Netzes in Entwicklungsländern untersucht, um die besonderen Herausforderungen der Netzbetreiber in Entwicklungs- und Schwellenländern zu identifizieren und zu verstehen, und um Unterschiede zu denen den Netzbetreibern in Hessen festzustellen. Anschließend wurde ein Konzept für das "Netz der Zukunft" entwickelt, das Smart Grid zur Bewältigung dieser Herausforderungen beinhaltet.

Im Rahmen der Entwicklung der Szenarien für das Netz der Zukunft in Entwicklungsländern wurde eine Reihe von Stakeholder-Workshops mit Entwicklungsbanken, Verteilungsunternehmen und Geräteherstellern durchgeführt, um herauszufinden, wo sie die zukünftigen Herausforderungen sehen, und wie fortschrittliche Smart-Grid-Technologie helfen kann diese zu bewältigen.

Auf der Grundlage der dabei gewonnenen Informationen wurde eine Reihe von Szenarien für das "Netz der Zukunft" am Beispiel zweier Dörfer in Ostafrika entwickelt, in denen intelligente Netztechnologien und -komponenten simuliert wurden, um festzustellen, welche die Herausforderungen der Netze in der Zukunft am kosteneffizientesten angehen.

Die daraus gezogenen Resultate wurden dann in Leitlinien für die Implementierung intelligenter Netze in Entwicklungsländern zusammengefasst.

6.2 Warum Smart Grid in Entwicklungs- und Schwellenländern?

Die Einführung der Smart-Grid-Technologie kann die Netze zuverlässiger und stabiler machen und die Integration erneuerbarer Energien durch die Bereitstellung von Echtzeitinformationen über Energienutzung, -angebot und -nachfrage unterstützen. Die detaillierten Energiedaten können beispielsweise zur Verbesserung der Vorhersage der Erzeugung erneuerbarer Energien und des Energiebedarfs genutzt werden, um den Energiefluss besser zu steuern. Durch die Zwei-Wege-Kommunikation mit intelligenten Netzen können Maßnahmen zur Nachfragesteuerung ergriffen werden, wenn es Probleme mit der Energiebilanz gibt.

Zu den Bewertungskriterien für Investitionen in intelligente Netze, insbesondere in Entwicklungsländern, gehören die Verringerung von Verlusten, die Reduzierung von Ausfällen und Ausfallzeiten durch Fernüberwachung und Fehlerbehebung, die Senkung der Betriebskosten dank erhöhter Effizienz und die optimale Nutzung der Anlagen.

Die Smart-Grid-Technologie kann die Sicherheit und Zuverlässigkeit der Stromversorgung durch die Einführung automatisierter Technologien wie Fehlerortung, Isolierung und Systemwiederherstellung (FLISR), Automatisierung von Umspannwerken, fortschrittliche Verteilungsmanagementsysteme (ADMS), Zwei-Wege-Kommunikation zwischen den Geräten bei sich ändernden Bedingungen

verbessern und Selbstheilungsfunktionen ermöglichen, was wiederum die Betriebskosten senkt und die Effizienz erhöht. Durch diese zusätzliche Echtzeitbeobachtung und -steuerung können Erweiterungsinvestitionen vermieden oder hinausgezögert werden, was wiederum wirtschaftliche Vorteile mit sich bringt. Aus ökologischer Sicht können die Treibhausgasemissionen durch die Migration von zentraler zu variabler erneuerbarer Energie, die durch Smart Grid möglich wird, reduziert werden.

Die Hauptvorteile von Smart-Grid-Investitionen lassen sich im Allgemeinen in folgende Bereiche unterteilen:

- Verbesserung der Sicherheit und Zuverlässigkeit
- Verbesserung der Effizienz
- Schaffung von Umweltvorteilen
- Schaffung von wirtschaftlichen Vorteilen

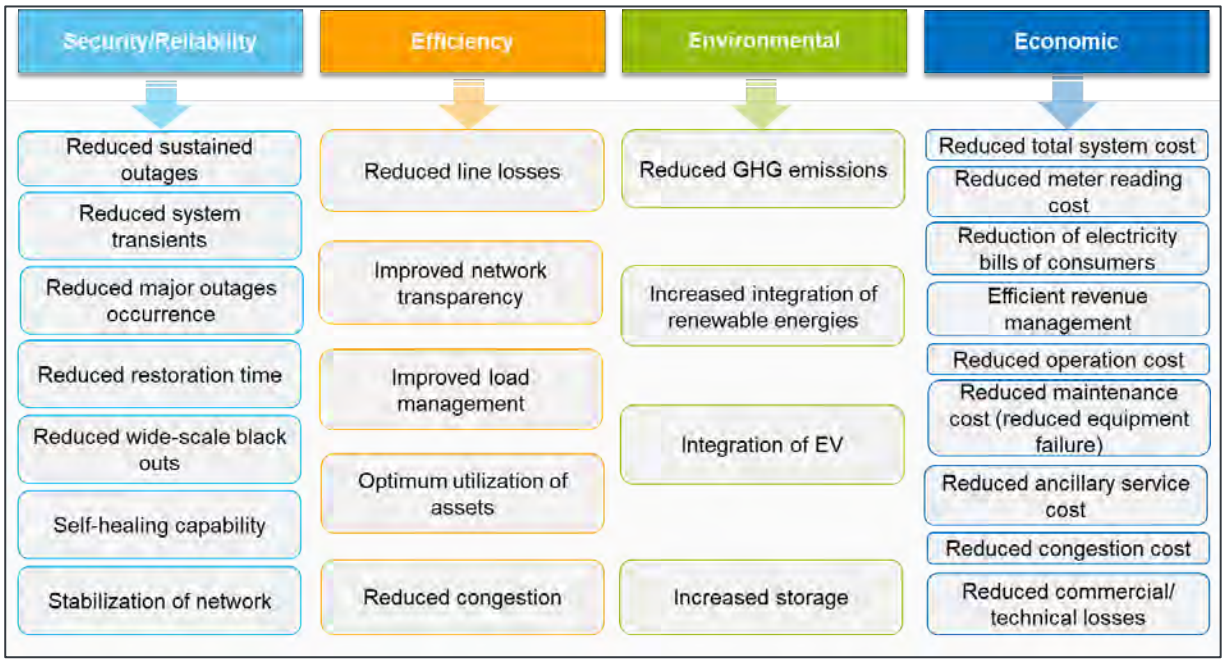


Abbildung 87: Hauptvorteile von Smart-Grid-Investitionen.

Ein einziger Technologietyp kann mehrere Vorteile oder Werttreiber haben. Es ist auch üblich, dass ein und dieselbe Ausrüstung mit unterschiedlichen Zielsetzungen implementiert wird. So kann ein Verteilungsnetzbetreiber (DNO) ein AMI-System einführen, um Verluste zu reduzieren, die Rechnungsstellung zu automatisieren und die Fehlerortung zu automatisieren, während ein anderer DNO ein AMI-System einführt, um Nutzungszeittarife oder Nachfragesteuerung zu ermöglichen.

Investitionsentscheidungen in Entwicklungsländern konzentrieren sich in der Regel eher auf Sicherheit/Zuverlässigkeit und wirtschaftliche Faktoren als auf Umwelt- oder Effizienzgründe.

6.3 Verständnis der Herausforderungen bei der Modernisierung von Verteilungsnetzen in Entwicklungsländern

In Deutschland werden die Investitionen in die Netzmodernisierung vom Netzbetreiber geplant, und nach der Genehmigung durch die Regulierungsbehörde wird eine bestimmte Rendite garantiert. Daher ist es für einen deutschen Verteilnetzbetreiber vergleichsweise einfach, eine Fremdfinanzierung für Investitionen zu erhalten, da das Risiko gering ist.

In Schwellen- und Entwicklungsländern ist die Situation ganz anders. Die Elektrizitätssysteme sind manchmal vertikal integriert, manchmal liberalisiert (getrennte Erzeugungs-, Übertragungs- und Verteilnetzbetreiber), aber fast immer mehrheitlich in staatlichem Besitz über eine Holdinggesellschaft. Die Stromtarife werden reguliert und in einer Höhe festgesetzt, die als politisch akzeptabel gilt, was oft zu weit weniger als kostendeckenden Tarifen führt, sodass den Versorgungsunternehmen die Mittel für grundlegende Instandhaltungs- oder Modernisierungsmaßnahmen fehlen.

Angesichts des Risikos dieser Investitionen sind Zuschüsse und konzessionäre Finanzierungen von internationalen Finanzinstitutionen (KfW, GIZ, World Bank, Asian Development Bank, usw.) oft die einzige externe Finanzierungsquelle für die Verteilnetzbetreiber. Diese Investitionsprogramme haben in der Regel eine Laufzeit von fünf Jahren und sind gemeinsame Vereinbarungen mit der Regierung, meist mit dem Energie- und dem Finanzministerium des jeweiligen Landes. Um für eine Finanzierung in Frage zu kommen, muss das Projekt bestimmte Ziele der bilateralen Zusammenarbeit erfüllen. Bei Verteilungsnetzen gehören dazu fast immer die Reduzierung von Treibhausgasemissionen, die Verbesserung der Effizienz des Systems und die Verringerung von Verlusten (was zu einer Verbesserung der finanziellen Ergebnisse führt).

Aufgrund des kurzen Planungshorizonts und der zahlreichen beteiligten Interessengruppen, die nicht dem Versorgungsunternehmen angehören, entsprechen die Investitionspläne nur selten den spezifischen Entwicklungsbedürfnissen des lokalen Versorgungsunternehmens und umfassen oft nur Teilprojekte, sodass das volle Nutzenpotential nicht ausgeschöpft wird.

6.4 Was sind die Herausforderungen bei der Einführung intelligenter Stromnetze in Entwicklungsländern?

Die Betreiber von Verteilungsnetzen in Entwicklungsländern sehen sich mit einer Reihe von einzigartigen Herausforderungen konfrontiert. Zusätzlich zu der Tatsache, dass es in vielen Ländern nicht genügend Erzeugungskapazitäten gibt, um die wachsende Last zu decken, sowie zu häufigen Fehlanpassungen zwischen Lastzentren und Erzeugungszentren, die die Übertragungsnetze belasten und zu häufigen Lastabwürfen führen, sind Verteilungsunternehmen oft unterfinanziert und haben weniger politischen Einfluss als die größeren Übertragungs- und Erzeugungsunternehmen bei den lokalen Ministerien.

Starke Nachfragesteigerung
Die jährliche Nachfragesteigerungen von 8-10 % aufgrund der zunehmenden Elektrifizierung und der steigenden Energieintensität, die durch den wachsenden Wohlstand (z. B. elektrisches Kochen,

Kühlschränke, Ventilatoren, Klimaanlagen) verursacht wird, stellen eine große Herausforderung dar. Ein Netzbetreiber sah sich beispielsweise mit einem Anstieg der Nachfrage von 19,7 auf 39 MWh im Sechsjahreszeitraum zwischen 2014 und 2020 konfrontiert, was einer Verdoppelung der Nachfrage innerhalb eines einzigen Planungs-/Investitionszyklus entspricht.

Veraltete Ausrüstung
Die vorhandene Ausrüstung ist oftmals stark veraltet, teilweise mehr als 50 Jahre, und da es keine kostendeckenden Tarife gibt, fehlen die Mittel für die grundlegende Wartung.

Kompatibilitätsprobleme erschweren sowohl die Implementierung als auch den Beschaffungsprozess. Dies ist insbesondere dann eine Herausforderung, wenn "Front-End"- und "Back-End"-Systeme getrennt ausgeschrieben werden, oder wenn intelligente Netztechnologie in Altsysteme implementiert werden soll.

Fehlende Kommunikationsnetze
Auch für unausgereifte Netze, die noch nicht die volle Funktionalität ausnutzen können, waren "Smart Grid" und "Smart Meter" in den letzten 10 Jahren sehr beliebte Investitionen. "Intelligente Zähler" gehören zu den ersten Investitionen, die durch IFI-Finanzierung umgesetzt werden, allerdings oft ohne die erforderliche Netzinfrastruktur, wie z. B. zuverlässige Kommunikationsnetze, sodass die Investitionen ihr Ziel nicht erreichen können.

Mangel an geschultem Personal
Die Installation und Wartung von Smart-Grid-Technologien erfordert spezielles technisches Fachwissen, das in Entwicklungsländern unter Umständen nicht vorhanden ist.

In vielen Schwellenländern ist der Personalbestand der Versorgungsunternehmen reguliert, und diese Vorschriften wurden manchmal seit Jahrzehnten nicht mehr aktualisiert. Dies kann zu Problemen bei der Einstellung der richtigen Personalressourcen für die Verwaltung der zunehmend digitalen Netze führen. So gibt es beispielsweise keine vorgeschriebene Stelle für einen IT-Experten, der für die Verwaltung und Wartung von SACDA- oder Serversystemen zuständig ist, so dass die für die Videoüberwachung zuständige Person auch die Verantwortung für SCADA übernimmt. Oft werden solche Probleme erst nach der Implementierung entdeckt, wenn sie auftreten.

Insbesondere bei der Automatisierung von SCADA/Unterstationen oder bei AMI/automatisierten Abrechnungsprojekten, die zu einem geringeren Personalbedarf führen, wird die Umsetzung des Projekts manchmal von Mitarbeitern der Versorgungsunternehmen sabotiert, die um ihren Arbeitsplatz oder den ihrer Kollegen fürchten.

Regulatorische Rahmenbedingungen
Vorschriften und Richtlinien können manchmal die Einführung von Smart-Grid-Technologien behindern, insbesondere in Entwicklungsländern, in denen die Vorschriften möglicherweise nicht so weit fortgeschritten sind oder gar nicht existieren.

6.5 Das Netz der Zukunft (Szenarien aus Perspektive der Entwicklungsländer)

Wichtige Erkenntnisse aus den Stakeholder-Workshops

Ein Aspekt der Durchführung dieser Arbeit ist die Entwicklung von Szenarien für das "Netz der Zukunft" (2030 und 2050) für verschiedene Netztypen. Für einige Netze, wie z. B. in Deutschland, wurde das

"Netz der Zukunft" bereits gründlich untersucht und die erwartete Entwicklung ist relativ gut bekannt. In Schwellen- und Entwicklungsländern ist dies jedoch nicht immer der Fall.

Um besser zu verstehen, wie sich das Netz der Zukunft entwickeln wird, wurde eine Reihe von Interviews mit Interessenvertretern durchgeführt, um ein tieferes Verständnis dafür zu gewinnen, wie das Netz der Zukunft aussehen könnte.

Die Workshops wurden durchgeführt mit:

- Verteilnetzbetreibern in Entwicklungsländern, um mehr über ihre wichtigsten Herausforderungen bei der Netzmodernisierung zu erfahren.
- Internationale Finanzinstitutionen (IFI), die eine wichtige und in einigen Fällen die einzige externe Quelle für Investitionsmittel für Netzmodernisierungsprojekte darstellen, mit dem Ziel zu verstehen, wie Investitionspakete für intelligente Netze in Entwicklungs- und Schwellenländern entwickelt und umgesetzt werden. Was sind die wichtigsten Überlegungen und Herausforderungen?
- Gerätehersteller, um ihre Ansichten darüber zu erfahren, wie sie die Entwicklung der Märkte angesichts des unterschiedlichen Reifegrads der Netze sehen. Zu den weiteren Themen gehören die Strategie zur Integration moderner Geräte in veraltete Systeme und die Frage, ob es einen Unterschied zwischen den in Deutschland und den in Entwicklungsländern verkauften Produkten gibt.

Aufbauend auf den in den Workshops gewonnenen Informationen haben wir zukünftige Netzszenarien definiert, in denen mögliche technische Lösungen im Smart Grid-LAB getestet und verifiziert werden.

Zentrale Erkenntnisse

Ein Hinweis auf die Definition von "Smart Grid" in Entwicklungsländern. Die Automatisierung von Umspannwerken (im Gegensatz zu ständig besetzten Umspannwerken, wie es üblich ist) und SCADA-Systeme werden als Smart-Grid-Investitionen betrachtet. Automatische Ablesesysteme oder vorausbezahlte Stromzähler mit automatisierten Abrechnungssystemen werden als intelligente Zähler/intelligentes Netz betrachtet, obwohl die Zähler nicht notwendigerweise Zähler sind, die eine Zweiwegekommunikation ermöglichen.

Im Folgenden werden die wichtigsten Erkenntnisse aus den Workshops zusammengefasst.

Smart-Grid-Investitionsumfeld Entwicklungsländer

- Der Zugang zu Energie steht im Vordergrund, Energieversorgung rund um die Uhr
- Bisher lag der Schwerpunkt der Investitionen vor allem auf der Elektrifizierung, der Sicherung der Energieerzeugung und der zuverlässigen Versorgung. Systemeffizienz und -optimierung hatten bisher nicht die höchste Priorität.
- Die meisten Geräte sind nicht kommunikationsfähig und benötigen daher eine RTU zur Integration von Altsystemen.
- Die Netze sind nicht in der Lage erneuerbare Energien im Versorgungsmaßstab zu integrieren, und neue Leitungen/Kupfer sind teuer.
- Abrechnungsproblem ->ERP-System - keine Unterscheidung zwischen Industrie- und Unternehmens-IT (kein Verständnis von IT vs. OT)

- Die Ziele der Smart Grid Implementierung werden von der Regierung von oben nach unten verordnet und stimmen daher nicht unbedingt mit den Notwendigkeiten der Versorgungsunternehmen überein.

Zu bewältigende Herausforderungen

- Für moderne intelligente Netze können keine alten Managementverfahren verwendet werden
- Die von den IFI als wichtig erachteten Investitionskomponenten sind in den Investitionspaketen enthalten. Aspekte, die von den IFI noch nicht gut verstanden werden, wie z. B. die IT/OT-Sicherheit, werden im Allgemeinen nicht berücksichtigt. Es werden nur ausgereifte Technologien für Investitionen ausgewählt.
- Die Finanzierung ist nur als Vorabinvestition vorgesehen. Es gibt keinen Mechanismus für die laufende Finanzierung, für die Wartung oder "as-a-service", zum Beispiel für die Überwachung und das Engpassmanagement. Wenn das eingeführte System nicht von den vorhandenen Mitarbeitern des Versorgungsunternehmens verwaltet und betrieben werden kann, wird es nicht eingeführt/genutzt. Der Bedarf an technischen Fähigkeiten zur Unterstützung wird nicht berücksichtigt. Es gibt keine verlässliche Finanzierungsquelle für die laufende technische Optimierung, die bei Investitionen in intelligente Netze erforderlich ist.
- Die Zeiten für die Genehmigung von Investitionen und die Durchführung von Projekten sind in der Regel deutlich länger als in Volkswirtschaften mit höheren Entwicklungsstand.
- Die Einführung von SCADA-Systemen bringt dem Versorgungsunternehmen klare finanzielle Vorteile. Die Vorteile intelligenter Netze verteilen sich jedoch auf die Akteure der Stromwertschöpfungskette (Erzeugung, Übertragung, Verteilung und Endverbraucher). Die daraus resultierenden finanziellen und wirtschaftlichen Vorteile für das Verteilungsunternehmen sind begrenzt und oft nicht hoch genug, um die finanziellen Investitionen zu rechtfertigen.
- Für fortgeschrittene Themen wie Sektorkopplung und E-Ladestation werden sowohl technische als auch finanzielle Partner benötigt. Die lokalen Versorgungsunternehmen haben keine Erfahrung in diesen Bereichen und die Finanzierungsinstitute brauchen Partner, um funktionierende Geschäftsmodelle unter den lokalen Bedingungen zu entwickeln.

6.6 Simulation von Netzen in Entwicklungsländern

Im Hinblick auf die Verpflichtung, den Anteil der erneuerbaren Energien zu erhöhen, um das globale 1,5 °C-Klimaziel zu erreichen und das Stromnetz zu dekarbonisieren, stehen Verteilernetzbetreiber vor großen Herausforderungen: die Spannungsstabilität, geringe Leistungsverluste, sowie ein sicheres und stabiles System aufrechtzuerhalten. Viele Regierungen auf der ganzen Welt beschließen jedoch Maßnahmen zur Integration dezentraler erneuerbarer Energiequellen (DRES) in Niederspannungsnetze [75], wie z. B. Photovoltaikanlagen auf Dächern und kleine Wind- und Biomasseanlagen. DRES sind wetterabhängig, und jede Wetteränderung wirkt sich auf die Erzeugung und damit auf die Stromqualität aus.

Das Spannungsniveau steigt, wenn die Einspeisung durch die Photovoltaik zunimmt und der Energieverbrauch niedrig ist. Anormaler Spannungsstress kann zu Schäden an der Isolierung von Energieanlagen und Haushaltsgeräten führen. Auch andere Probleme wie steigende Kurzschlussströme

und Probleme mit der Netzqualität können die Aufnahmekapazität (HC) der erneuerbaren Energien in Verteilernetzen einschränken [76].

6.6.1. Netz der Zukunft Fallstudie - Uganda

Die Republik Uganda ist ein Binnenstaat im Herzen des subsaharischen Afrikas. Es hat eine Fläche von 241.555 km2 mit einer Gesamtbevölkerung von über 34,6 Millionen Menschen [77]. Das Land liegt am Äquator und verfügt über eine hohe Sonneneinstrahlung, die über das ganze Jahr verteilt ist, mit einer durchschnittlichen Tageslichtdauer von etwa 12 Stunden pro Tag und etwa 4.380 Stunden pro Jahr [78]. Die Sonneneinstrahlung beträgt etwa 5-6 kWh/m2 pro Tag auf ebenen Flächen [79]. Die Wirtschaft Ugandas basiert auf der Landwirtschaft, und die Mehrheit der ugandischen Bevölkerung ist in der Land- und Forstwirtschaft sowie im Fischfang tätig [80]. Die Stromerzeugungskapazität des Landes wird hauptsächlich durch Wasserkraft bestimmt, unterstützt durch Schweröl- und Biomasse-Heizkraftwerke; dennoch ist die Elektrifizierungsrate eine der niedrigsten weltweit.

Etwa 80 % der ugandischen Bevölkerung leben in ländlichen Regionen und 20 % in städtischen Gebieten und Städten. Nach Angaben der Weltbank haben 60 % der Bevölkerung in ländlichen Regionen keinen Zugang zu Strom [81] (siehe Abbildung 88).

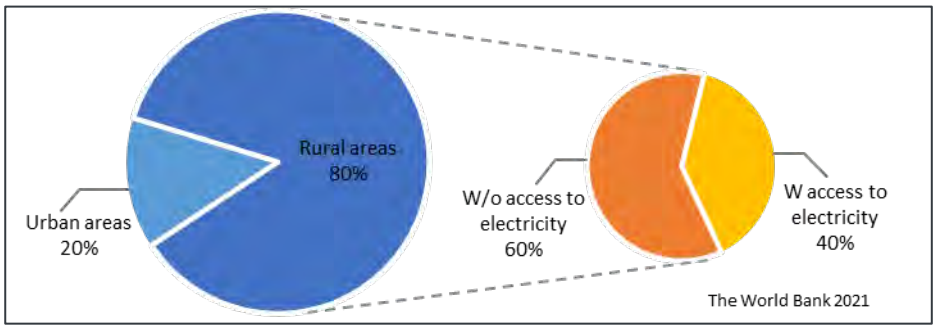


Abbildung 88: Zugang zu Elektrizität in Uganda.

Die Agentur für ländliche Elektrifizierung hat das Ziel, bis 2040 eine Elektrifizierungsrate von 100 % zu erreichen [82].

6.6.2. Überblick über das ugandische Energiesystem

Über 90 % der Stromerzeugung erfolgt durch Wasserkraftwerke. Obwohl Uganda eine sehr hohe Sonneneinstrahlung hat, macht die Stromerzeugung mit Photovoltaik (PV) nur 2 % der Gesamterzeugung aus. Andere Quellen wie Biomasse und Wärmekraftwerke machen etwa 6 % der Gesamtproduktion aus.

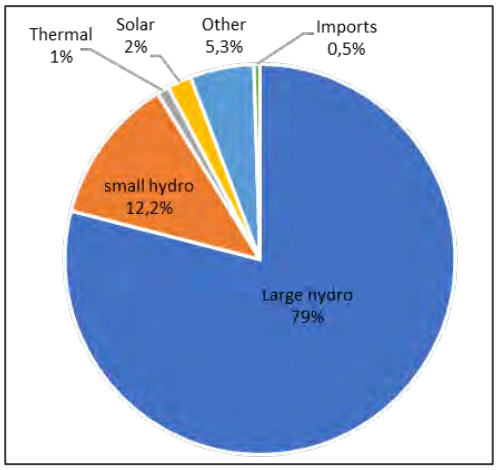


Abbildung 89: Stromerzeugung: Stromerzeugung in Uganda.

Herausforderungen im ugandischen Elektrizitätssektor

Wie in Abbildung 2 dargestellt, ist das Stromversorgungssystem in Uganda stark zentralisiert und wird von großen Wasserkraftwerken dominiert. Der Strom wird von den Erzeugungsanlagen über Übertragungsleitungen (220 kV, 132 kV und 66 kV) zu den Verteilerstationen und dann zu den Endverbrauchern übertragen [83]. Um die Haushalte zu erreichen, legt der Strom über die Verteilerleitungen weite Strecken zurück, was die Leistungsverluste und den Spannungsabfall erhöht. Nach Angaben des größten Verteilungsunternehmens in Uganda lagen die Stromverluste im Jahr 2021 bei 18 % [84]. Eine gängige Lösung zur Verringerung der Spannungs- und Stromverluste und zur Vermeidung von Überlastungen der Anlagen ist die traditionelle Netzverstärkung.

Das Erreichen einer Elektrifizierungsrate von 100 % bis 2040 [82] bedeutet einen dramatischen Anstieg des Strombedarfs in den nächsten Jahren. In [85] wurde eine Fallstudie durchgeführt, um die Auswirkungen der traditionellen Netzverstärkung in Abschnitt 3.3 und ihre wirtschaftliche Effizienz im Vergleich zu Flexibilitätsoptionen in Unterabschnitt 3.4 zu untersuchen. In der Fallstudie wurden drei Netzmodelle für die Jahre 2020, 2025 und 2030 vorgestellt, die den Anstieg der Stromnachfrage berücksichtigen. Es wird geschätzt, dass die Nachfrage im Jahr 2025 um den Faktor 1,37 und im Jahr 2035 um den Faktor 2 steigen wird.

Für die Fallstudie wurden zwei Dörfer in einem ländlichen Gebiet in Uganda ausgewählt. Die Netzdaten und der Standort beruhen auf realen Projektdaten, die von Tractebel Engineering bezogen wurden.

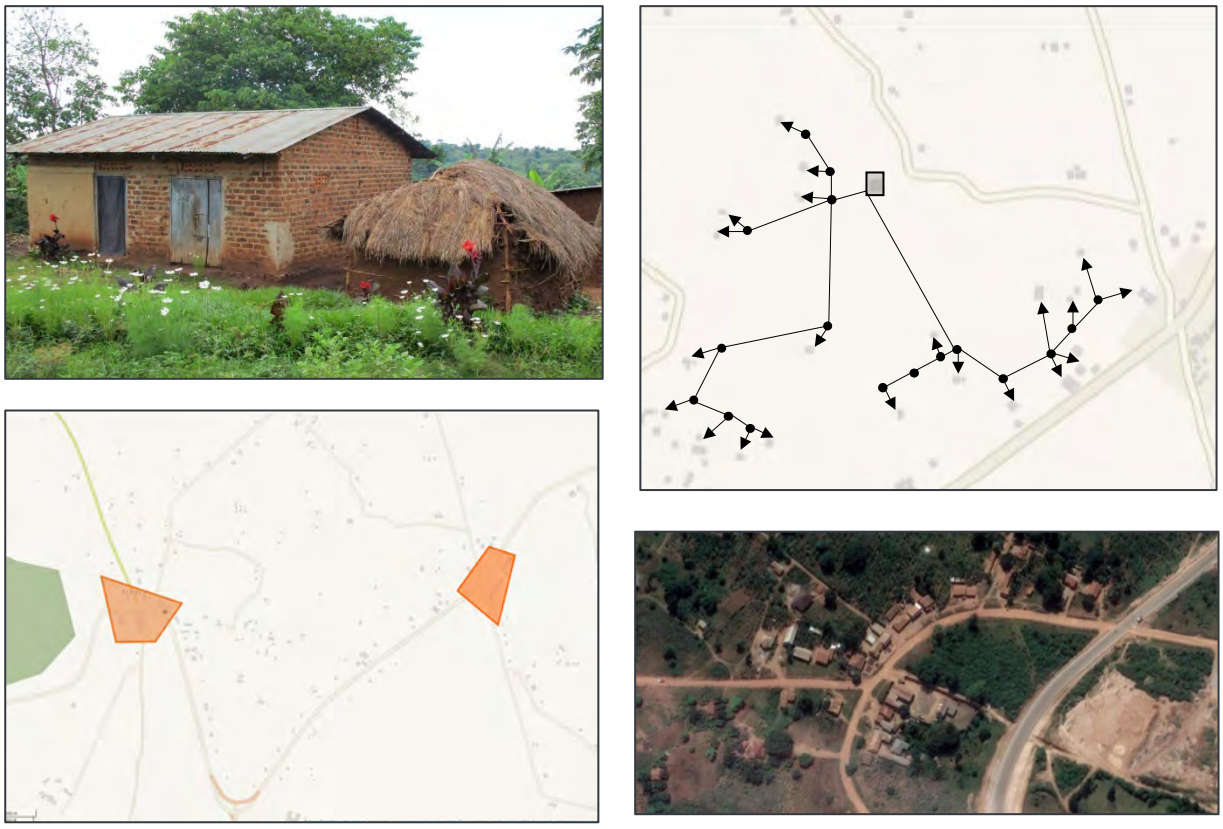


Abbildung 90: Modellierte Dörfer

Traditionelle Netzverstärkung

Das Netzmodell für die repräsentativen Dörfer ist in Abbildung 91 dargestellt. Das Netz enthält zwei Niederspannungseinspeisungen, die als Village 1 und Village 2 bezeichnet werden.

Jedes Dorf wird über einen 100 kVA MS/NS Transformator versorgt. Jeder Abzweig enthält zwei Hauptleitungen mit einer unterschiedlichen Anzahl von Haushalten.

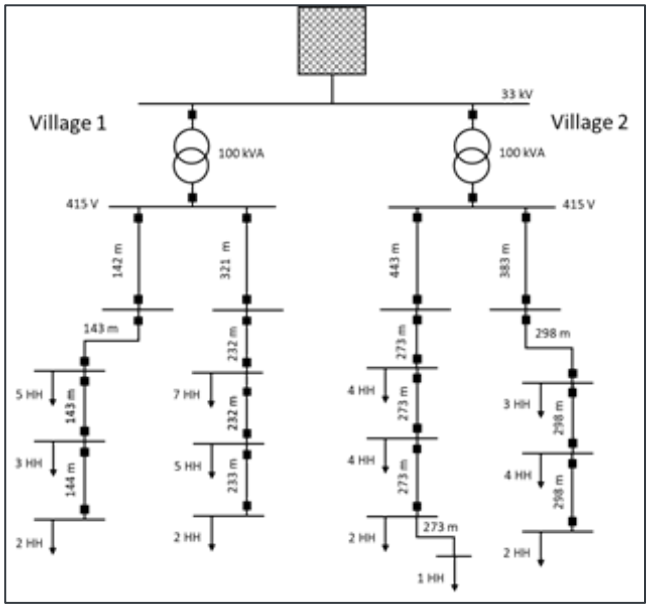


Abbildung 91: Netzwerkmodell der Fallstudie.

Es wurden eine Reihe von Simulationen mit den folgenden Netzverstärkungsmaßnahmen durchgeführt.

Ersatz von überlasteten Transformatoren durch Transformatoren mit höherer Leistung

Ein Transformator ist ein Gerät, das zwei Netze mit unterschiedlichen Spannungen miteinander verbindet. Verteiltransformatoren haben im Allgemeinen eine Nennspannung von 11 kV bis 110 V und eine Nennleistung von weniger als 200 MVA [85]. Verteiltransformatoren sind in der Regel so ausgelegt, dass sie mit 60 % bis 70 % ihrer Nennleistung betrieben werden können, da sie bei diesen Werten den maximalen Wirkungsgrad erreichen. Die Größe des Transformators richtet sich nach dem Versorgungsgebiet. Je höher die Last ist, desto stärker wird der Transformator belastet. Wenn die Belastung des Transformators 60 %-70 % übersteigt, wird er überlastet, und seine Innentemperatur steigt drastisch an, was zu Isolationsschäden führen kann.

Ersatz von überlasteten Kabeln durch Kabel mit größerem Querschnitt

Energiekabel werden nach Schlüsselparametern wie Netzspannung, Strombelastung (Strombelastbarkeit), Umgebungsbedingungen (z. B. Temperatur, Feuchtigkeit usw.) und zulässigem maximalen Spannungsabfall ausgewählt. In der Tat wird bei der Dimensionierung von Kabeln für Niederspannungsnetze manchmal der Spannungsabfall und nicht die Strombelastbarkeit berücksichtigt [86].

Folgende Gleichung zeigt die Beziehung zwischen dem Widerstand eines Kabels und seiner Querschnittsfläche. Diese sind umgekehrt proportional zueinander, so dass Kabel mit größeren Querschnittsflächen einen geringeren Widerstand, d. h. einen geringeren Spannungsabfall aufweisen.

$$R = \rho . \frac{l}{A}$$

R ist der Widerstand, ρ ist die Leitfähigkeit des Materials, l ist die Länge des Kabels und A ist der Querschnitt des Kabels

Platzierung von Blindleistungskompensationsanlagen

Blindleistungskompensationsanlagen (SCB) werden in der Regel zur Bereitstellung von kapazitiver Blindleistung für die Leistungsfaktorkorrektur eingesetzt. In der Industrie werden SCBs häufig installiert, um den Leistungsfaktor zu verbessern, da lokale Netze stark unter induktiven Lasten sowie Oberschwingungen leiden. SCBs können auch für andere Anwendungen wie Spannungsverbesserung und -regelung eingesetzt werden, wenn sie speziell für diesen Zweck ausgelegt sind. Sie sind kostengünstig, einfach und schnell zu installieren [87].

Tabelle 52 zeigt die Ergebnisse der Simulation mit traditionellen Netzverstärkungsmaßnahmen.

Tabelle 52: Traditionelle Netzverstärkung.

Szenario	Netzverstärkungsmaßnahme	Größe des Geräts	Auswirkungen auf das Modellnetz

1	Nur Austausch der Transformatoren	100 kVA 30 mm2	Das Netz weist Spannungsverletzungen auf, ohne dass der neue Transformator überlastet ist.
2	Austausch des Stromtransformators und der Kabel	100 kVA 50 mm2	Es wurden weder Spannungsverletzungen noch Überlastungen der Transformatoren festgestellt.
3	Austausch des Leistungstransformators und placement of shunt capacitor banks	100 kVA 50 mm2 5 kVAr	Die Simulationen ergaben einen Spannungsbereich zwischen 0,94 p.u. und 1,04 p.u., der innerhalb des zulässigen Bereichs (± 6%) liegt. Es wurde keine Überspannung beobachtet.

Die Ergebnisse zeigen, dass der Ersatz des Leistungstransformators durch einen Transformator mit höherer Kapazität das Problem der Spannungsverletzungen nicht lösen würde. Die Szenarien 2 und 3 zeigen eine vielversprechende Lösung für das Spannungsproblem. Durch die Einführung neuer Technologien und Strategien können die Investitions- und Betriebskosten gesenkt werden. Die Integration dezentraler erneuerbarer Energiequellen (DRES) in der Nähe des Verbrauchsortes kann die Stromverluste, die bei der Übertragung über große Entfernungen zu den Verteilungsleitungen entstehen, verringern und die Betriebskosten minimieren. Außerdem bieten DRES eine nachhaltige Energieversorgung und helfen den Versorgungsunternehmen bei der Dekarbonisierung ihres Systems.

Die Integration von DRES ist mit Netzrückwirkungen verbunden, die sich in Spannungsverletzungen, Überlastung von Stromversorgungsanlagen, zunehmenden Kurzschlussströmen und Problemen mit der Stromqualität äußern. Diese Probleme schränken die Netzaufnahmekapazität (HC) der DRES ein.

Simulationen aus der in [85] dargestellten Fallstudie haben gezeigt, dass die Netzbeschränkungen stark verletzt wurden, wenn die DRES zu einem geringen Prozentsatz installiert war. Die Ergebnisse zeigen, dass die Integration von 12 kWp in Dorf 1 und 10 kWp in Dorf 2 Spannungsabfälle von bis zu 0,85 p.u. verursachte. Außerdem verzeichneten die Leistungstransformatoren eine Überlastung von 100%.

Im nächsten Abschnitt werden neue Technologien und Ausrüstungen getestet, um ihre Auswirkungen auf den HC von DRES zu untersuchen.

6.6.3. Flexibilitätsoptionen bei der Erhöhung des HC von DRES

In einer in [88] durchgeführten Fallstudie werden verschiedene neue Technologien zur Verbesserung des HC von DRES vorgestellt. Dazu gehören die Neukonfiguration des Netzes, der Einsatz von Energiespeichersystemen und die Verwendung von Laststufenschaltern (On-Load Tap Changer, OLTC). In der Fallstudie wurde dieselbe Netzkonfiguration wie in Abbildung 91 verwendet.

Rekonfiguration des Netzes

Es gibt zwei Arten der Netzrekonfiguration, die statische und die dynamische. Während bei der dynamischen Rekonfiguration die Topologie mit Hilfe von ferngesteuerten Schaltern, IKT, verschiedenen Schutz- und Steuergeräten je nach Zustand des Netzes geändert werden kann, ist bei der statischen Rekonfiguration die Rekonfiguration nur einmal möglich. Eine Änderung der Topologie kann die Richtung des Leistungsflusses von überlasteten Einspeisungen zu weniger belasteten Einspeisungen ändern und somit den Leistungsfluss ausgleichen. Beide Methoden erfordern einen komplexen Planungs- und Ausführungsaufwand.

Blindleistungsregelung

Neue Generationen von DRES-Wechselrichtern können durch die Steuerung der Blindleistung eine begrenzte Spannungsregelung am Anschlussknoten bieten. Eine Studie in [89] zeigt, dass der Einsatz von Wechselrichtern mit Blindleistungsregelung den HC um etwa 20 % verbessern kann.

6.6.4. Laststufenschalter (OLTC) (Eine Fallstudie)

In [88] wurde eine Fallstudie durchgeführt, bei der OLTC, Phasor Measurement Units (PMU) und ein intelligenter Steuerungsalgorithmus eingesetzt wurden, um die Spannung optimal zu steuern und so die Leistung der verteilten erneuerbaren Energiequellen zu maximieren.

In dieser Studie wird das Potential der Photovoltaik (PV) analysiert, indem die Lastumschalter (NLTC) durch OLTC ersetzt werden. Das Netzmodell wurde mit der Simulationsumgebung Power Factory simuliert. Eine Monte-Carlo-Analyse (MC) wird verwendet, um die Zufälligkeit der Anzahl der PV-Installationen und der jeweiligen Standorte der Anschlusspunkte zu berücksichtigen. Bei jeder Iteration wurde eine zufällige Anzahl von PV-Anlagen an verschiedenen Standorten mit gleichmäßiger Wahrscheinlichkeit simuliert. Dann wird die Nennleistung der PV-Anlagen schrittweise erhöht, bis die Spannungs- und Belastungsgrenzwerte erreicht sind.

Die HC-Verbesserung durch OLTC-Transformatoren im Vergleich zu NLTC-Transformatoren ist in Abbildung 92 dargestellt. Das "Basis"-Szenario bezieht sich auf die herkömmlichen Transformatoren ohne OLTC. Der "verbesserte" Fall bezieht sich auf die mit OLTC ausgestatteten Transformatoren.

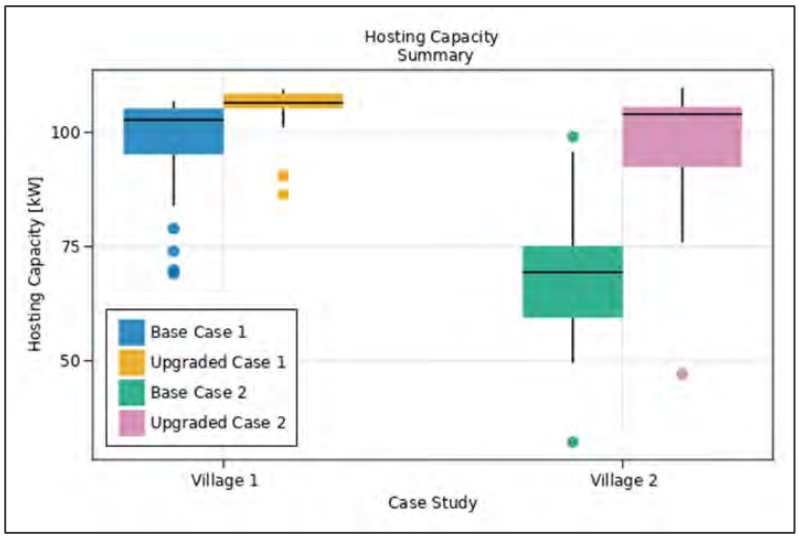


Abbildung 92: HC mit NLTC und OLTC.

Die Ergebnisse zeigen eine deutliche Verbesserung der PV-Hosting-Kapazität in Dorf 2 mit einem Anstieg von 68 kWp auf 97 kWp (ein Faktor von 1,42). In Dorf 1 ist eine leichte Verbesserung zu erkennen. Das Haupthindernis in Dorf 1 ist die Überlastung des Transformators. Eine höhere HC kann erreicht werden, wenn größere Transformatoren eingesetzt werden.

Abbildung 93 zeigt das Spannungsprofil (z-Achse) in Abhängigkeit von der von der PV-Anlage eingespeisten Gesamtleistung (y-Achse) und den Zeitschritten (x-Achse). Ein Zeitschritt entspricht 15 Minuten, d. h. 96 Viertelstunden pro Tag.

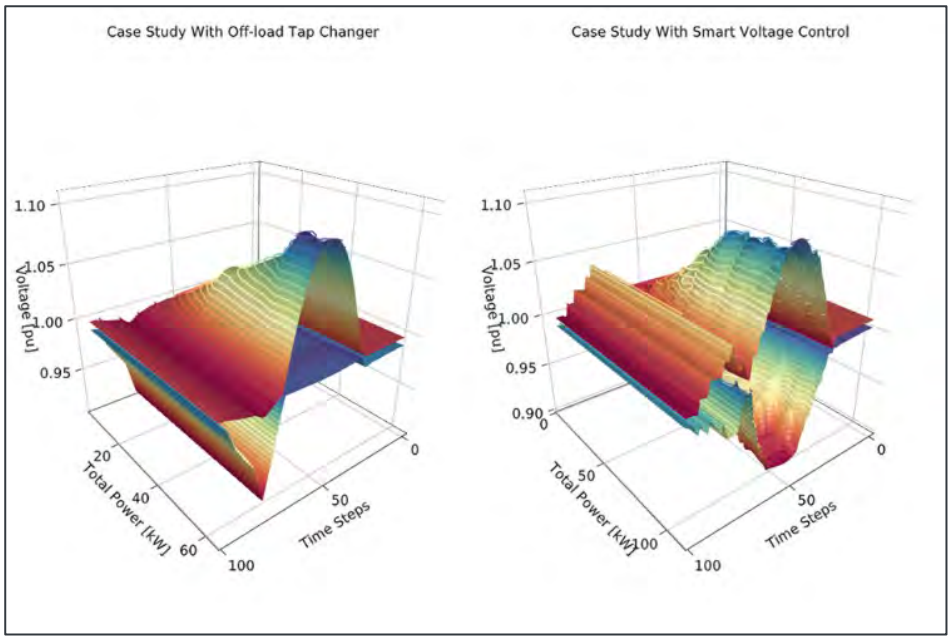


Abbildung 93: Spannungsprofil und Gesamtleistung in Abhängigkeit von den Zeitschritten.

Um die Rolle des OLTC bei der Verbesserung des HC zu verstehen, wird ein MC des Dorfes 2 analysiert. Die linke Grafik in Abbildung 93 zeigt, dass die Spannung den maximal zulässigen Schwellenwert von 1,10 p.u. bei einer maximalen Leistung von ca. 54 kWp der PV-Leistung erreicht. Da es keine Spannungsregelung an den Transformatorenklemmen gibt, ist die Form des Oberflächendiagramms nur das Ergebnis der PV-Einspeisung und des Lastprofils, und sie ist nicht symmetrisch. Im Gegenteil, die Teilgrafik auf der rechten Seite von Abbildung 93 zeigt dagegen ein symmetrisches Profil der maximalen und minimalen Spannung in der Einspeisung, das den maximalen Bereich der zulässigen Spannung ausnutzt und die Aufnahmekapazität maximiert.

Die gleichen Ergebnisse sind in Abbildung 94. Die verschiedenen Spannungsprofile entsprechen der eingespeisten PV-Leistung.

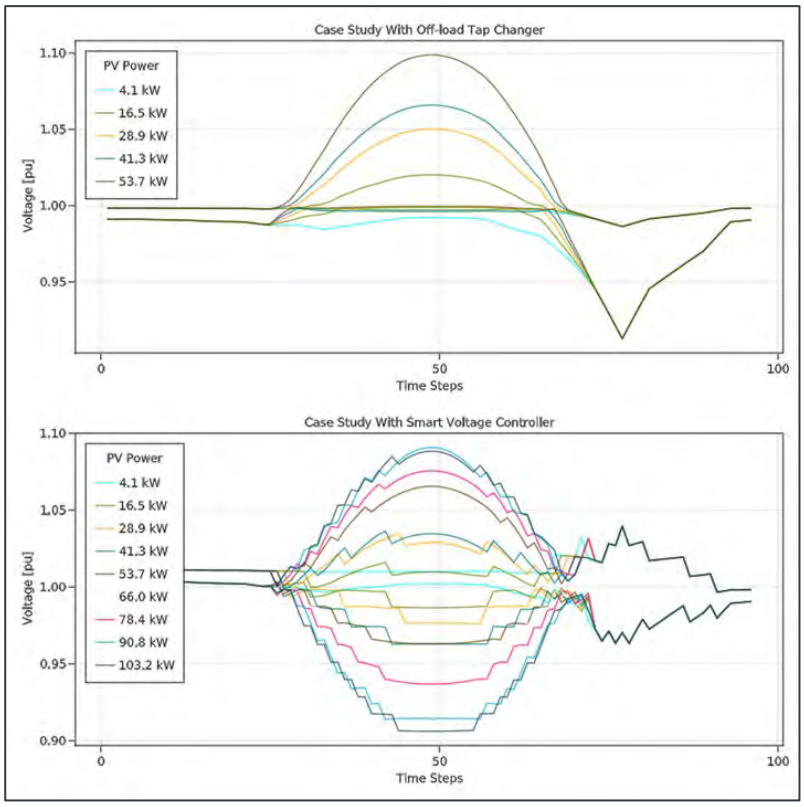


Abbildung 94: Spannungsprofil bei Verwendung von NLTC und OLTC.

Für diese spezielle MC-Iteration wird die Aufnahmekapazität durch den Einsatz von OLTC und intelligenten Reglern um den Faktor 1,92 verbessert (von 53,7 kW_p auf 103,2 kW_p). In dieser speziellen Iteration mit OLTC und intelligenten Reglern ist die Spannung keine Einschränkung mehr, und der begrenzende Faktor für die Aufnahmekapazität wird die Transformatorbelastung. Dies wird dadurch bestätigt, dass das entsprechende Diagramm in Abbildung 5 (unteres Teilbild) die Grenzen von 1,10 p.u. und 0,90 p.u. nicht erreicht.

Aus den Ergebnissen lässt sich schließen, dass in Netzen, in denen die Überlastung der Anlagen das Haupthindernis für eine Erhöhung der KW darstellt, zunächst die traditionelle Netzverstärkung untersucht werden sollte. Andererseits können in Netzen, in denen Spannungsengpässe das Haupthindernis darstellen, OLTC, PMUs und intelligente Steuerungen die HC von DRES um den Faktor 1,42 deutlich verbessern. In allen Fällen ist der Ersatz der Transformatoren durch leistungsstärkere Einheiten, die mit OLTC und intelligenten Steuerungen ausgestattet sind, eine vielversprechende Lösung zur Erhöhung der HC.

Die ausführliche Fallstudie [88] die im Rahmen des Smart Grid LAB Hessen durchgeführt wurde, finden Sie unter dem Titel "Auswirkung von Laststufenschaltern und Smart Controllern auf die dezentrale Erneuerbare-Energien-Aufnahmekapazität".

6.6.5. Intelligente Transformatoren (Eine Fallstudie)

Intelligente Transformatoren, auch Solid-State-Transformatoren genannt, sind Transformatoren auf Basis von Leistungselektronik. Intelligente Transformatoren werden als Flexibilitätsoption in Verteilungsnetzen eingesetzt, um die Spannung zu steuern und somit eine reibungslose Umwandlung von Wechselstrom in Gleichstrom und von Gleichstrom in Wechselstrom zu ermöglichen. [90]. Darüber hinaus können sie weitere Dienste wie Schnellladeanschlüsse für Elektrofahrzeuge bereitstellen.

In einer Fallstudie wurden die Auswirkungen intelligenter Transformatoren auf den HC von DRES in Verteilungsnetzen untersucht [91], unter Verwendung des gleichen Verteilungsnetzes in Abbildung 90. Die Fallstudie umfasste vier verschiedene Fälle, nämlich ***Fall (a)***, in dem herkömmliche Transformatoren mit NLTC und herkömmliche Wechselrichter verwendet werden, ***Fall (b)***, in dem herkömmliche Transformatoren mit NLTC und Wechselrichter mit Blindleistungsregelung verwendet werden, ***Fall (c)***, in dem ein intelligenter Transformator mit ungeregelten PV-Wechselrichtern verwendet wird, und schließlich ***Fall (d)***, in dem intelligente Transformatoren sowie PV-Wechselrichter mit Blindleistungsregelung verwendet werden.

Abbildung 95 zeigt das Spannungsprofil des Einspeisers in Dorf 2 bei Verwendung eines herkömmlichen Transformators und eines herkömmlichen Wechselrichters ohne Blindleistungsregelungsmöglichkeit. Die maximale Spannungsbegrenzung wird zum Zeitpunkt der maximalen PV-Leistungseinspeisung mit einer Gesamtleistung von 85,7 kW_p erreicht.

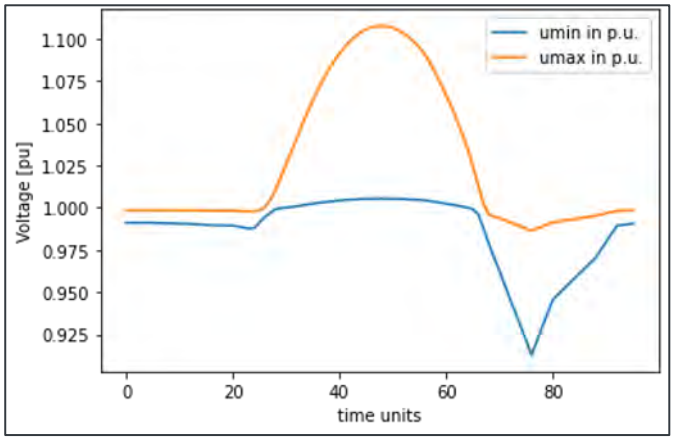


Abbildung 95: Maximale und minimale Spannung (p.u.) im Dorf 2, Fall (a).

Abbildung 96 zeigt die Simulationsergebnisse für den Fall (d), in dem der herkömmliche Transformator durch einen intelligenten Transformator mit derselben Leistung (100 kVA) und die herkömmlichen Wechselrichter durch Wechselrichter mit Blindleistungsregelung ersetzt wurden. Die Ergebnisse zeigen, dass mit dieser Lösung eine maximale HC von 172 kW_p erreicht werden kann.

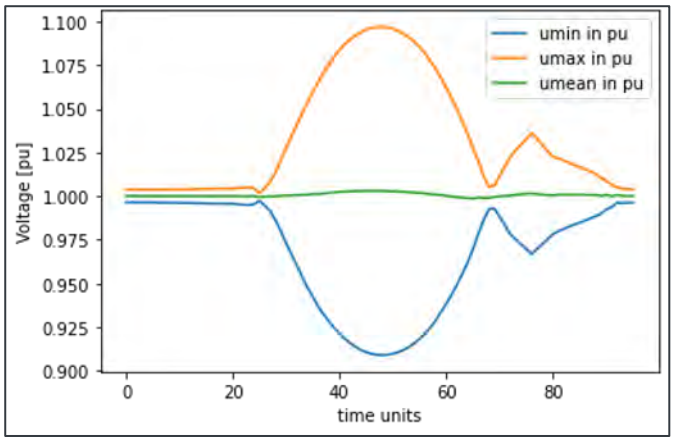


Abbildung 96: Maximale und minimale Spannung im Dorf 2, Fall (d).

Abbildung 97 zeigt einen Vergleich zwischen allen simulierten Lösungen, d. h. den Fällen (a), (b), (c) und (d). Die Abbildung zeigt eine signifikante Verbesserung der HC durch intelligente Transformatoren,

PMUs und intelligente Steuerungsalgorithmen in den Fällen (c) und (d). Die Verbesserung von Fall (a) zu Fall (d) beträgt etwa das Zweifache.

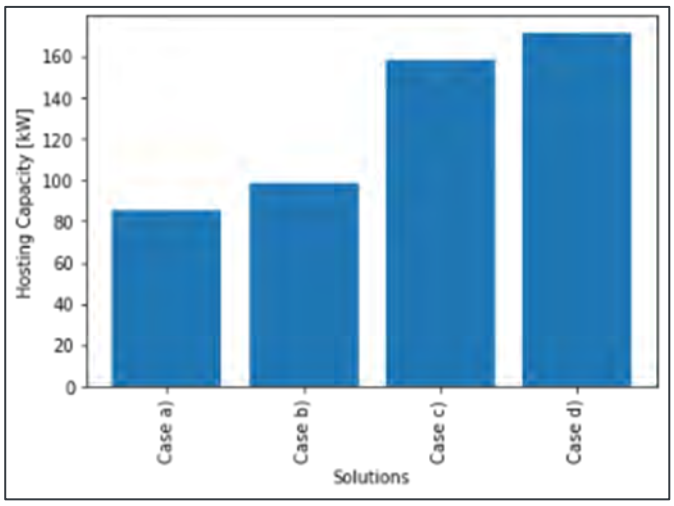


Abbildung 97: Verschiedene Lösungen zur Verbesserung des HC.

Eine detaillierte Fallstudie, die im Rahmen des Smart Grid LAB Hessen durchgeführt wurde, finden Sie unter dem Titel "Impact of Smart Grid Technologies on the Distribution Network in Uganda: Eine Fallstudie".

6.6.6. Schlussfolgerung

Eine Erhöhung der Elektrifizierungsrate bedeutet eine Erhöhung der Lastnachfrage. Die Stromerzeugung in Uganda hängt stark von der Wasserkraft ab und ist daher stark zentralisiert. Bei der Übertragung des Stroms von den Erzeugungsanlagen zu den Verbrauchern kommt es zu Stromverlusten und Problemen mit der Spannungsqualität. Um dieses Problem zu lösen, können DRES am Ort des Verbrauchs integriert werden, wo der Strom lokal verbraucht wird. Die traditionelle Netzverstärkung wurde untersucht.

Die Ergebnisse zeigen, dass die Integration von DRES in veraltete Netze zu Spannungsinstabilitäten sowie zur Belastung von Stromversorgungseinrichtungen wie Transformatoren und Kabeln führt. Als Lösung wurden neue Technologien wie OLTC und intelligente Transformatoren eingesetzt. Fallstudien haben gezeigt, dass der HC von DRES im Falle von intelligenten Transformatoren um den Faktor 2 und im Falle von OLTC-Transformatoren um den Faktor 1,42 erhöht werden kann.

6.7 Leitfaden für die Einführung intelligenter Netze in Entwicklungsländern

Sehr oft scheitert die Einführung intelligenter Netze in Entwicklungs- und Schwellenländern, bevor das erste Gerät überhaupt installiert ist. In Entwicklungs- und Schwellenländern ist der Planungsprozess entscheidend.

Vorab muss verstanden werden, was die Hauptprobleme des bestehenden Systems sind, was das Wertversprechen ist. Es sollte nicht davon ausgegangen werden, dass die Motivation für eine Investition darin besteht, die Nachfragesteuerung zu ermöglichen oder weitere Investitionen zu verschieben. Der zweite Aspekt ist die Kenntnis des aktuellen Zustands des Netzes und der damit

verbundenen Systeme. Back-End-Kommunikationssysteme sind sehr oft nicht vorhanden und müssen in das Investitionsprogramm aufgenommen werden. Es sollte auch bedacht werden, dass, selbst wenn die Kommunikationsausrüstung an bestimmten Punkten im Netz installiert ist, sie das Netz möglicherweise nicht vollständig abdeckt oder Schnittstellen zu Altsystemen aufweist, die die Kommunikationsgeschwindigkeit erheblich beeinträchtigen.

Das verfügbare Personal und der Ausbildungsstand müssen berücksichtigt werden. In der Planungsphase sollte ein Personal- und Einsatzplan erstellt werden.

Es kann schwierig sein, Ersatzteile an entlegene Orte zu liefern, wie sie in Entwicklungsländern zu finden sind. Diese Situation verschlimmert sich noch, wenn das Land Sanktionen jeglicher Art unterliegt; dies gilt auch für Ersatzbatterien für Messgeräte, die unter die Sanktionen fallen können.

7. Zusammenfassung und Handlungsempfehlungen

7.1 Zusammenfassung

Das Labor unterstützt eindeutig die These, dass es einen Handlungsbedarf in den Niederspannungsnetzen beim Thema Digitalisierung gibt. Dafür muss auch nicht auf ein proprietäres System zurückgegriffen werden. Bereits am Markt erhältliche Komponenten können herstellerunabhängig zu einer funktionierenden Gesamtlösung kombiniert werden. Dies ist im realnahen Labor Smart Grid LAB Hessen umgesetzt und die Funktionen sind dargestellt.

Die IT-Security ist mit dem aktuellen Stand beherrschbar und darf auf jeden Fall nicht vernachlässigt werden. Ein stetiges Aktualisieren ist auf jeden Fall notwendig. Jedoch sind die Angriffspunkte nicht immer eindeutig. Die einleitende Frage diesbezüglich ist, ob ein direkter Zugang zur Hardware existiert (Einbruch in die Ortsnetzstation). Des Weiteren besteht Bedarf für die OT und IoT Komponenten. Es müssen die gleichen Methoden und Architekturen verwendet werden, die bereits in der IT eingesetzt werden. Ein ganzheitliches Cyber-Security Konzept, einschließlich der physischen Sicherheit, ist notwendig und befindet sich erst in der Entstehung.

In den Industrieländern liegt, wie dieses Projekt zeigt, der Fokus auf Smart Grids zur Steuerung bidirektionaler Energieflüsse von Prosumern und zur Optimierung des Nachfragemanagements, um notwendige Netzinvestitionen zu reduzieren. Entwicklungsländer hingegen stehen aktuell noch vor ganz anderen Herausforderungen. Hier liegt der Fokus auf der Implementierung intelligenter Netzkomponenten, um eine flächendeckende Energieversorgung zu ermöglichen. Diese steht angesichts der oft schwachen Netzinfrastruktur nicht konstant zur Verfügung. Dabei ist das Hauptanliegen, mit dem stark wachsenden Strombedarf umgehen zu können und bisher unerschlossene Bereiche zu versorgen

In solchen Netzen liegt die Herausforderung eben nicht in den zahlreichen einzelnen Prosumern, sondern in der Stabilisierung des Netzes auf der Dorfebene. Obwohl die Herausforderungen unterschiedlich sind, helfen Smart-Grid-Komponenten, die z.B. eine automatisierte Überwachung, 2-Wege-Kommunikation und Steuerung ermöglichen, eine zuverlässige Netzstromversorgung mit minimalen Investitionen zu ermöglichen.

Um ein Smart Grid zu ermöglichen, ist es notwendig den Wandel vom Consumer zum Prosumer weiter voranzutreiben und noch einen Schritt weiter zum Flexsumer zu gehen. Mit dem Ansteuern der Komponenten im Smart Grid, wie zum Beispiel Ladesäulen und Batteriespeichern, wird es möglich, zeitnah eine Energiewende ohne Tolerierung von Engpässen zu ermöglichen. Der Prosumer muss definitiv flexibel steuerbar sein. Ohne die Nutzung der Regelbarkeit dieser Komponenten wird es ein netzengpassbedingtes Priorisieren geben bzw. wird es zu Abschaltungen von Verbrauchern kommen. Dabei lässt sich allgemein festhalten, dass in der Regulatorik eine Nachschärfung der Vorgaben hinsichtlich OPEX und der CAPEX notwendig ist, um weitere Anreize zu setzen.

7.2 Weiterer Forschungsbedarf

Ein finaler Aufbau eines Smart Grids konnte im Rahmen dieses Projekt also noch nicht geschaffen werden. Es wurde eine Grundlage aufgebaut, auf welcher die Entwicklung eines Smart Grids ganzheitlich weiter vorangetrieben werden kann, bzw. muss.

Um die feine Regelbarkeit der Pro-/Flexsumer mit aufzunehmen, gilt es das SmartMeter Gateway im Labor zu implementieren. Auch die Anreizregulierung durch den Strompreis muss ebenfalls noch betrachtet werden. Es bringt nichts, wenn die Komponenten zwar grundsätzlich regelbar sind, jedoch diese Möglichkeit nicht genutzt werden kann, weil der Zugang dazu fehlt.

Des Weiteren müssen Möglichkeiten für weitere Rollen der Batteriespeicher noch betrachtet werden. Genauso gilt es dabei Anreize zu schaffen, diese zur Verfügung zu stellen. Dies könnte benötigte Flexibilität bringen und den Nutzen von erneuerbaren Energien stärken. Dabei kann der Zellulare Ansatz an Bedeutung gewinnen. Kenntnis über den (Lade-)Zustand von regelbaren Batterien und über die Auslastung eines Stranges ermöglicht es, verbrauchsunabhängig Energie je nach Prognose aus dem Straßenzug zu entnehmen oder ihm zuzuführen.

Weiterführend gilt es Betrachtungen für primäre Technik und sekundäre Technik anzustellen. Für die Primärtechnik gilt es den Einfluss von Blindleistung im Niederspannungsnetz zu untersuchen und die möglichen Vorteile für ein Smart Grid zu gewinnen. In der Sekundärtechnik gilt es IT, OT und IoT in Zusammenarbeit mit der Energiewirtschaft weiterzuentwickeln, um auf beiden Seiten das Verständnis füreinander zu schärfen. Die Feldbus Norm IEC 61158 gilt es dabei zu überprüfen. Das Bussystem „eBus“, welches unter diese Norm fällt und vermehrt in Heizungs- und Smart Home Systemen zum Einsatz kommt, wird bisher noch nicht von den Komponentenherstellern in der Energiewirtschaft bedient.

Literaturverzeichnis

[1] Presse- und Informationsamt der Bundesregierung, „Wohlstand sichern – Klima schützen," 10 Mai 2022. [Online]. Available: https://www.bundesregierung.de/breg-de/themen/klimaschutz/wohlstand-und-klimaschutz-2018366. [Zugriff am 03 Juni 2022].

[2] B. Burger, „Energy-Charts," Fraunhofer ISE, 09 Januar 2022. [Online]. Available: https://www.energy-charts.de. [Zugriff am 31 Mai 2022].

[3] buzer.de Daniel Liebig, „Artikel 2 - Gesetz zu Sofortmaßnahmen für einen beschleunigten Ausbau der erneuerbaren Energien und weiteren Maßnahmen im Stromsektor," 08 Oktober 2022. [Online]. Available: https://www.buzer.de/2_EEGAusbGuEnFG.htm.

[4] Umweltbundesamt, „Was ist ein "Smart Grid"?," 03 August 2013. [Online]. Available: https://www.umweltbundesamt.de/service/uba-fragen/was-ist-ein-smart-grid.

[5] P. Bergmann, „Verteilnetzbetreiber 2030 - Aufgaben, Herausforderungen, Strategien," Becker Büttner Held, 2018.

[6] „IEEE," [Online]. Available: https://smartgrid.ieee.org/about-ieee-smart-grid. [Zugriff am 15 12 2022].

[7] I. E. A. (IEA), „Smart Grids," IEA, [Online]. Available: https://www.iea.org/reports/smart-grids. [Zugriff am 15 12 2022].

[8] I. E. C. (IEC), „Smart Grids," [Online]. Available: https://www.iec.ch/energies/smart-energy. [Zugriff am 15 12 2022].

[9] H. Abouelgheit, „Information and Communication Technologies in Modern Electrical Networks: A Brief Review," International Journal of Smart Grid, Bad Vilbel, 2022.

[10] O. o. e. d. a. e. reliability, „Distribution Automation: Results from the Smart Grid Investment Grant Program," U.S. Department of Energy, 2016.

[11] J. Ekanayake, K. Liyanage, J. W. A. Yokoyama und N. Jenkis, Smart Grid Technology and Applications, United Kingdom: John Wiley & Sons Ltd., 2012.

[12] U. Angela, B. C. Judith und D. T., „Data Privacy in the Smart Grid: A Decentralized Approach," in *52nd Hawaii International Conference on System Sciences*, Hawaii, 2019.

[13] I. Jeromin, „Smart Grid LAB Hessen - Projektskizze".

[14] C. Kittl, D. Sarajlić und C. Rehtanz, „k-means based identification of common supply tasks for low voltage grids," IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Sarajevo, Bosnia and Herzegovina, 2018.

[15] D. Sarajlic und C. Rehtanz, „Low Voltage Benchmark Distribution Network Models Based on Publicly Available Data," IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), 2019, pp. 1-5, doi: 10.1109/ISGTEurope.2019.8905726, Romania, Bucharest , 2019.

[16] J. Dickert, M. Domagk und P. Schegner, „Benchmark Low Voltage Distribution Networks Based on Cluster Analysis of Actual Grid Properties," IEEE Grenoble Conference, 2013, pp. 1-6, doi: 10.1109/PTC.2013.6652250, Grenoble, France, 2013.

[17] G. Kerber, „Aufnahmefähigkeit von Niederspannungsverteilnetzen," Technischen Universität München , München, 2010.

[18] Deutsches Institut für Normung, *DIN EN 50160:2020-11 Merkmale der Spannung in öffentlichen Elektrizitätsversorgungsnetzen,* 2020.

[19] a-eberle, *Auf die richtge Spannung kommt es an,* Nürnberg: a-eberle, 2021.

[20] T. SÜD, „tuvsud," Tüv Süd, 2021. [Online]. Available: https://www.tuvsud.com/de-de/industre/elektrotechnik-info/kurzschlussstromberechnung. [Zugriff am 15 Dezember 2021].

[21] L. Petry, Energieversorgung, Darmstadt: Hochschule Darmstadt, 2014.

[22] H. Dr.-Ing. Meier, C. Dipl. Ing. Fünfgeld, T. Dipl. Ing Adam und B. Prof. Dr. habil. Schieferdecker, Repräsentative VDEW-Lastprofile, Cottbus: VDEW Frankfurt am Main, 1999.

[23] KKoPV, „photovoltaikforum," 16 November 2015. [Online]. Available: https://www.photovoltaikforum.com/thread/ 110153-stromprofil-1-min%C3% BCtig-4-personen-haushalt/. [Zugriff am 28 Dezember 2021].

[24] „Statistik.Hessen," Hessisches Statistisches Landesamt, 2020. [Online]. Available: https://statistik.hessen.de/zahlen-fakten/ bevoelkerung-gebiet-haushalte-familien/ haushalte-familien/tabellen. [Zugriff am 28 Dezember 2021].

[25] „entega.de," ENTEGA Plus GmbH, 2021. [Online]. Available: https://www.entega.de/blog/stromverbrauch-2-personen-haushalt/. [Zugriff am 28 Dezember 2021].

[26] „entega.de," ENTEGA Plus GmbH, 2021. [Online]. Available: https://www.entega.de/blog/stromverbrauch-licht/. [Zugriff am 28 Dezember 2021].

[27] „123energie," Pfalzwerke Aktiengesellschaft, [Online]. Available: https://www.123energie.de/privatkunden/magazin/stromverbrauch_a201. [Zugriff am 28 Dezember 2021].

[28] J. Bauer, „Hausjounal," about:publishing GmbH, 2021. [Online]. Available: https://www.hausjournal.net/herd-leistung. [Zugriff am 28 Dezember 2021].

[29] T. Tjaden, J. Bergner, J. Weniger und V. Quaschning, „Repräsentative elektrische Lastprofile für Einfamilienhäuser in Deutschland auf 1-sekündiger Datenbasis," [Online]. [Zugriff am 15 Dezember 2021].

[30] „www.statista.com," 28 01 2021. [Online]. Available: https://de.statista.com/statistik/daten/studie/152937/umfrage/anzahl-der-stromnetzbetreiber-in-deutschland-seit-2006/. [Zugriff am 10 06 2021].

[31] „www.udo-leuschner.de," [Online]. Available: https://www.udo-leuschner.de/energie-chronik/160109d1.htm. [Zugriff am 10 06 2021].

[32] „www.gesetze-im-internet.de," 21 12 2020. [Online]. Available: https://www.gesetze-im-internet.de/eeg_2014/BJNR106610014.html#BJNR106610014BJNG000100000. [Zugriff am 31 05 2021].

[33] „juris.bundesgerichtshof.de," 25 02 2014. [Online]. Available: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&nr=66912&linked=pm. [Zugriff am 31 05 2021].

[34] „www.ewe-netz.de," [Online]. Available: https://www.ewe-netz.de/einspeiser/strom/redispatch. [Zugriff am 09 06 2021].

[35] I. Jeromin, „Begründung zur Anzeige Änderung zum Plan vom 3. Februar 2022," 2022.

[36] „www.zolar.de," 20 07 2018. [Online]. Available: https://www.zolar.de/blog/entwicklung-der-eeg-einspeiseverguetung. [Zugriff am 08 06 2021].

[37] „www.energie-experten.org," [Online]. Available: https://www.energie-experten.org/erneuerbare-energien/photovoltaik/direktvermarktung/marktwert-solar. [Zugriff am 08 06 2021].

[38] J. Weniger, T. Tjaden und V. Quaschning, „www.volker-quaschning.de," 2012. [Online]. Available: https://www.volker-quaschning.de/artikel/2012-10-solare-unabhaengigkeit/index.php. [Zugriff am 08 06 2021].

[39] M. Sterner, F. Eckert, M. Thema und F. Bauer, „www.bee-ev.de," 03 2015. [Online]. Available: https://www.bee-ev.de/fileadmin/Publikationen/Studien/BEE_HM_FENES_Kurzstudie_final.pdf. [Zugriff am 04 06 2021].

[40] VDE, „www.e-netzeallgaeu.de," 04 2019. [Online]. Available: https://www.e-netzeallgaeu.de/media/FNN_Hinweis_Anschluss_und_Betrieb_von_Speichern_am_Niederspa.pdf. [Zugriff am 04 06 2021].

[41] B. Tepe, N. Collath, H. Hesse, M. Rosenthal und U. Windelen, „Stationäre Batteriespeicher in Deutschland: Aktuelle Entwicklungen und Trends in 2021," *Energiewirtschaftliche Tagesfragen Heft 3,* 2021.

[42] „www.statista.de," 09 12 2020. [Online]. Available: https://de.statista.com/statistik/daten/studie/. [Zugriff am 04 06 2021].

[43] „www.waermepumpe.de," [Online]. Available: https://www.waermepumpe.de/. [Zugriff am 25 06 2021].

[44] „www.haus-xxl.de," [Online]. Available: https://www.haus-xxl.de/themen/wie-hoch-ist-der-stromverbrauch-fuer-ein-einfamilienhaus-479. [Zugriff am 23 06 2021].

[45] „www.energie.web.de," [Online]. Available: https://www.energie.web.de/ratgeber/verbrauch/stromverbrauch-einfamilienhaus/#:~:text=1%2DPersonen%2DHaushalt%3A%202.000,Haushalt%3A%203.800%20bis%204.200%20kWh. [Zugriff am 21 06 2021].

[46] „www.bmi.bund.de," [Online]. Available: https://www.bmi.bund.de/DE/themen/bauen-wohnen/bauen/energieeffizientes-bauen-sanieren/energieausweise/gebaeudeenergiegesetz-node.html. [Zugriff am 26 06 2021].

[47] Fachausschuss Marktforschung im BDEW, „Wie heizt Deutschland 2019?," BDEW Bundesverband der Energie- und Wasserwirtschaft e. V., Berlin, 2019.

[48] V. Breisig, J. Neuhaus, N. Deutsch, J. Homann und C. Linden, „Chancen und Risiken für deutsche Heizungsindustrie im globalen Wettbewerb," PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, 2020.

[49] „www.bundesregierung.de," [Online]. Available: https://www.bundesregierung.de/breg-de/themen/klimaschutz/. [Zugriff am 01 06 2021].

[50] „www.kba.de," 06 01 2021. [Online]. Available: https://www.kba.de/DE/Presse/Pressemitteilungen/2021/Allgemein/pm01_2021_E_Antrieb.html. [Zugriff am 09 05 2021].

[51] D. Schäfer, „Netzdienliches Laden im Untergrund," *50,2 Magazin für intelligente Stromnetze,* p. 42, 09 05 2021.

[52] „www.audi-mediacenter.com," 21 05 2021. [Online]. Available: https://www.audi-mediacenter.com/de/pressemitteilungen/audi-pilotiert-konzept-fuer-schnellladen-13977. [Zugriff am 02 06 2021].

[53] Reiner Lemoine Institut GmbH , „Ladeinfrastruktur nach 2025/2030: Szenarien für den Markthochlauf, Studie im Auftrag des BMVI," Nationale Leitstelle Ladeinfrastruktur, Berlin, 2020.

[54] Hessisches Statistisches Landesamt, „Hessische Gemeindestatistik," 2021. [Online]. Available: https://www.statistik.hessen.de. [Zugriff am 12 August 2022].

[55] Bundesnetzagentur, „Marktstammdatenregister," 2022. [Online]. Available: https://www.marktstammdatenregister.de/MaStR. [Zugriff am 12 August 2022].

[56] Karftfahrt-Bundeamt, „Bestand an Kraftfahrzeugen und Kraftfahrzeuganhängern nach Zulassungsbezirken," Kraftfahrt-Bundesamt, Flensburg, 2021.

[57] Bundesministerium für Wirtschaft und Klimaschutz (bmwk), „Habeck: „Das Osterpaket ist der Beschleuniger für die erneuerbaren Energien "," Bundesministerium für Wirtschaft und Klimaschutz (bmwk), 6 April 2022. [Online]. Available: https://www.bmwk.de/Redaktion/DE/Pressemitteilungen/2022/04/20220406-habeck-das-

osterpaket-ist-der-beschleuniger-fur-die-erneuerbaren-energien.html. [Zugriff am 12 August 2022].

[58] Bundesministerium für Wirtschaft und Klimaschutz (bmwk), „Entwurf eines Gesetzes zu Sofortmaßnahmen für einen beschleunigten Ausbau der erneuerbaren Energien und weiteren Maßnahmen im Stromsektor," Bundesministerium für Wirtschaft und Klimaschutz (bmwk), o.J..

[59] Bundesministerium für Wirtschaft und Klimaschutz (bmwk), „Erneuerbare Energien," Bundesministerium für Wirtschaft und Klimaschutz (bmwk), [Online]. Available: https://www.bmwk.de/Redaktion/DE/Dossier/erneuerbare-energien.html. [Zugriff am 12 August 2022].

[60] U. v. d. Busch, A. Gauler und H. Müller, „Energiewende in Hessen – Monitoringbericht 2021," Hessisches Ministerium für Wirtschaft, Energie, Verkehr und Wohnen, Wiesbaden, 2021.

[61] M. Braun, I. Krybus, H. Becker, R. Bolgaryn, J. Dasenbrock, P. Gauglitz, D. Horst, C. Pape, A. Scheidler und J. Ulffers, „VERTEILNETZSTUDIE HESSEN 2024 – 2034," Frankfurt / Kassel, 2018.

[62] Die Bundesregierung, „Masterplan Ladeinfrastruktur der Bundesregierung," Berlin, 2019.

[63] C. Bamberg, J. Lack, S. Siegemund und A. A. d. Maur, „dena, Prognos, 2020: "Privates Ladeinfrastrukturpotenzial in Deutschland"," Deutsche Energie-Agentur GmbH (dena), Berlin, 2020.

[64] J. Bergner, B. Siegel und V. Quaschning, „Hemmnisse und Hürden für die Photovoltaik," Hochschule für Technik und Wirtschaft Berlin, Berlin, 2020.

[65] C. Kost, S. Shammugam, V. Fluri, D. Peper, A. D. Memar und T. Schlegl, „Stromgestehungskosten Erneuerbare Energien," Fraunhofer ISE, Freiburg, 2021.

[66] Die Bundesregierung, „Mehr Windenergie auf See," 08 Juli 2022. [Online]. Available: https://www.bundesregierung.de/breg-de/themen/klimaschutz/windenergie-auf-see-gesetz-2022968. [Zugriff am 08 Juli 2022].

[67] E3/DC, „89 Prozent des Solarpotenzials auf deutschen Ein- und Zweifamilienhäusern sind noch ungenutzt," 07 April 2021. [Online]. Available: https://www.e3dc.com/89-prozent-des-solarpotenzials-auf-deutschen-ein-und-zweifamilienhaeusern-sind-noch-ungenutzt/. [Zugriff am 08 Juli 2022].

[68] J. Kirchner und M. Rodenfels, „Wohnungsbedarfsprognose für die hessischen," IWU - Institut Wohnen und Umwelt, Darmstadt, 2017.

[69] S. Koeller, „E.ON: 100% E-Autos im Jahr 2045 für Netze zu stemmen," 22 Mai 2019. [Online]. Available: https://www.electrive.net/2019/05/22/e-on-100-e-autos-im-jahr-2045-fuer-netze-zu-stemmen/. [Zugriff am 08 Juli 2022].

[70] S. Kohler, P. Haueisen, T. Koch und O. Ehrentraut, „Wohnen in Deutschland 2045 -," prognos Allianz, Stuttgart, 2016.

[71] M. Vaché und M. Rodenfels, „Wohnungsbedarfsprognose für die hessischen," IWU - Institut Wohnen und Umwelt, Darmstadt, 2020.

[72] Hessiches Statistisches Landesamt, „Hessen wächst und schrumpft — Modellrechnung zur Bevölkerungsentwicklung für die kreisfreien Städte und Landkreise in Hessen bis 2040 liegt vor," Statistik.Hessen, 2019.

[73] Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit (BMU), „Klimaschutzplan 2050," BMU, Arbeitsgruppe IK III 1, Berlin, 2019.

[74] Institut für Netz- und Anwendungstechnik GmbH, „RONT.info," [Online]. Available: https://ront.info/systemwirkung-ront/probleme-und-losungen/spannungsbandproblem/. [Zugriff am 28 Februar 2023].

[75] E. Martinot, „Global Status Report on Local Renewable Energy Policies," 2021.

[76] B. Azibek, A. Abukhan, H. Nunna, B. Mukatov, S. Kamalasadan und S. Doolla, „Hosting Capacity Enhancement in Low Voltage Distribution Networks: Challenges and Solutions," *IEEE International Conference on Power Electronics, Smart Grids and Renewable Energy (PESGE2020),* 2020.

[77] U. B. o. Statistics, „Uganda Profile," [Online]. Available: https://www.ubos.org/uganda-profile/. [Zugriff am 09 12 2022].

[78] „Worlddata.info," [Online]. Available: https://www.worlddata.info/africa/uganda/sunset.php. [Zugriff am 09 12 2022].

[79] F. Mwarania, O. Avellino, A. Al-Hassan und A. Kpatinde, „Uganda Solar Energy Utilization: Current Statuts and Future Trends," *International Journal of Scientific and Research Publications.*

[80] T. Tindimwebwa, S. Kigenyi, K. Fred und E. Khainza, „Understanding Economics in Uganda," Kawa Uganda, [Online]. Available: http://kawa.ac.ug/kawa_economics/agriculture.html. [Zugriff am 09 12 2022].

[81] „The World Bank," 2019. [Online]. Available: https://data.worldbank.org/indicator/EG.ELC.ACCS.UR.ZS?locations=UG. [Zugriff am 02 08 2022].

[82] K. Mokveld und S. v. Eije, „Final Report Uganda," Ministry of Foreign Affairs, 2018.

[83] E. R. Authority, „Transmission Network," [Online]. Available: https://www.era.go.ug/index.php/stats/transmission-stats/transmission-network-length. [Zugriff am 09 12 2022].

[84] „Umeme Limited," [Online]. Available: https://www.umeme.co.ug/umeme_api/wp-content/uploads/2022/08/Umeme_H1-2022-Results-Presentation_Final.pdf. [Zugriff am 09 12 2022].

[85] M. k. Saini, „tutorialspoint," 01 01 2022. [Online]. Available: https://www.tutorialspoint.com/difference-between-power-transformer-and-distribution-

transformer#:~:text=The%20usual%20voltage%20ratings%20of,%2C%20440%20kV%2C%20and%20above.. [Zugriff am 15 12 2022].

[86] „Cable Types and Selection Criteria," in *Technical Information Handbook Wire and Cable*, Anixter, p. 77.

[87] G. Brunello, B. Kasztenny und C. Wester, „Shunt Capacitor Bank Fundamentals and Protection," in *2003 Conference for Protective Relay Engineers*, Texas, 2003.

[88] H. Abouelgheit und L. Pizzimbone, „Impact of On-Load Tap Changers and Smart Controllers on the Distributed Renewable Energy Hosting Capacity," *International Journal of Smart Grid,* Bd. 6, Nr. 4, pp. 131-135, 2022.

[89] H. Abouelgheit, L. Pizzimbone und A. Danabal, „Impact of Smart Grid Technologies on the Distribution Network in Uganda: A Case Study," in *21st Wind & Solar Integration Workshop*, The Hague, The Netherlands, 2022.

[90] „Electrical India," 18 March 2018. [Online]. Available: https://www.electricalindia.in/smart-transformers-for-energy-sector/. [Zugriff am 15 12 2022].

[91] H. Abouelgheit, L. Pizzimbone und A. Danabal, „Impact of smart grid technologies on the distribution network in Uganda: A case study," in *21st Wind & Solar Integration Workshop (WIW 2022)*, 2022.

Abbildungsverzeichnis

Tabellenverzeichnis

Anhang

Anhang 1: Kurzschlussstromberechnung

Anhang 2: Simulationen PowerFactory

Anhang 3: Einstellungen für das Labor

Anhang 4: Lastkurven für die Haushalte des Beispiels

A1: Kurzschlussstromberechnung

Netze

Ergebnisdaten - Kurzschluss

Fester Kurzschlussort

I''k2-min Knotenorientiert

Datum	20.12.2021
Zeit	14:34:46
Revisionsnr.	

S. Pluetzer

Berechnung fester Kurzschlussort
I''k2-min Knotenorientiert

Kurzschlussort SS3

Knotennummer	Knotenname	Phase	U_n [kV]	U_k/ ((c*U_n)/1,73) [%]	|U_k| [kV]	I''k2 [kA]	S''k [MVA]	i_p [kA]
1	Labor Einspeisung	L1	0,400	100,89	0,221	0,000	0,000	0,000
		L2		100,48	0,220	0,000	0,000	0,000
		L3		102,71	0,225	0,000	0,000	0,000
		E		0,00	0,000	0,000	0,000	0,000
2	NA1	L1	0,400	100,35	0,220	0,000	0,000	0,000
		L2		104,55	0,229	0,000	0,000	0,000
		L3		109,51	0,240	0,000	0,000	0,000
		E		0,00	0,000	0,000	0,000	0,000
3	NA6	L1	0,400	99,86	0,219	0,000	0,000	0,000
		L2		111,22	0,244	0,000	0,000	0,000
		L3		121,09	0,266	0,000	0,000	0,000
		E		0,00	0,000	0,000	0,000	0,000
4	NA7	L1	0,400	99,80	0,219	0,000	0,000	0,000
		L2		115,50	0,253	0,000	0,000	0,000
		L3		128,74	0,282	0,000	0,000	0,000
		E		0,00	0,000	0,000	0,000	0,000
5	NA8	L1	0,400	99,94	0,219	0,000	0,000	0,000
		L2		119,80	0,263	0,000	0,000	0,000
		L3		136,56	0,300	0,000	0,000	0,000
		E		0,00	0,000	0,000	0,000	0,000
6	NA5	L1	0,400	99,87	0,219	0,000	0,000	0,000
		L2		111,22	0,244	0,000	0,000	0,000
		L3		121,09	0,266	0,000	0,000	0,000
		E		0,00	0,000	0,000	0,000	0,000
7	NA4	L1	0,400	99,87	0,219	0,000	0,000	0,000
		L2		111,22	0,244	0,000	0,000	0,000
		L3		121,09	0,266	0,000	0,000	0,000
		E		0,00	0,000	0,000	0,000	0,000
8	NA2	L1	0,400	99,87	0,219	0,000	0,000	0,000
		L2		111,22	0,244	0,000	0,000	0,000
		L3		121,09	0,266	0,000	0,000	0,000
		E		0,00	0,000	0,000	0,000	0,000
9	NA3	L1	0,400	100,28	0,220	0,000	0,000	0,000
		L2		124,11	0,272	0,000	0,000	0,000
		L3		144,52	0,317	0,000	0,000	0,000
		E		0,00	0,000	0,000	0,000	0,000
10	Vor Trafo	L1	20,000	99,89	10,957	0,000	0,000	0,000
		L2		100,00	10,970	0,000	0,000	0,000
		L3		99,85	10,954	0,000	0,000	0,000
		E		0,00	0,000	0,000	0,000	0,000
11	SS1	L1	0,400	99,99	0,219	0,000	0,000	0,000
		L2		92,33	0,203	0,000	0,000	0,000
		L3		91,96	0,202	0,000	0,000	0,000
		E		0,00	0,000	0,000	0,000	0,000
12	SS6	L1	0,400	99,97	0,219	0,000	0,000	0,000
		L2		81,35	0,178	0,000	0,000	0,000
		L3		83,29	0,183	0,000	0,000	0,000
		E		0,00	0,000	0,000	0,000	0,000
13	SS5	L1	0,400	99,96	0,219	0,000	0,000	0,000
		L2		81,35	0,178	0,000	0,000	0,000
		L3		83,29	0,183	0,000	0,000	0,000
		E		0,00	0,000	0,000	0,000	0,000
14	SS4	L1	0,400	99,96	0,219	0,000	0,000	0,000
		L2		81,35	0,178	0,000	0,000	0,000
		L3		83,29	0,183	0,000	0,000	0,000
		E		0,00	0,000	0,000	0,000	0,000

Berechnung fester Kurzschlussort
I''k2-min Knotenorientiert

Kurzschlussort SS3

Knotennummer	Knotenname	Phase	U_n [kV]	U_k/ ((c*U_n)/1,73) [%]	|U_k| [kV]	I''k2 [kA]	S''k [MVA]	i_p [kA]
15	SS8	L1	0,400	99,96	0,219	0,000	0,000	0,000
		L2		67,90	0,149	0,000	0,000	0,000
		L3		73,66	0,162	0,000	0,000	0,000
		E		0,00	0,000	0,000	0,000	0,000
16	SS3	L1	0,400	99,95	0,219	0,000	0,000	0,000
		L2		49,98	0,110	0,314	0,217	0,724
		L3		49,98	0,110	0,314	0,217	0,724
		E		0,00	0,000	0,000	0,000	0,000
17	SS2	L1	0,400	99,96	0,219	0,000	0,000	0,000
		L2		81,35	0,178	0,000	0,000	0,000
		L3		83,29	0,183	0,000	0,000	0,000
		E		0,00	0,000	0,000	0,000	0,000
18	SS7	L1	0,400	99,96	0,219	0,000	0,000	0,000
		L2		74,52	0,163	0,000	0,000	0,000
		L3		78,24	0,172	0,000	0,000	0,000
		E		0,00	0,000	0,000	0,000	0,000

Berechnung fester Kurzschlussort
I''k2-min Knotenorientiert

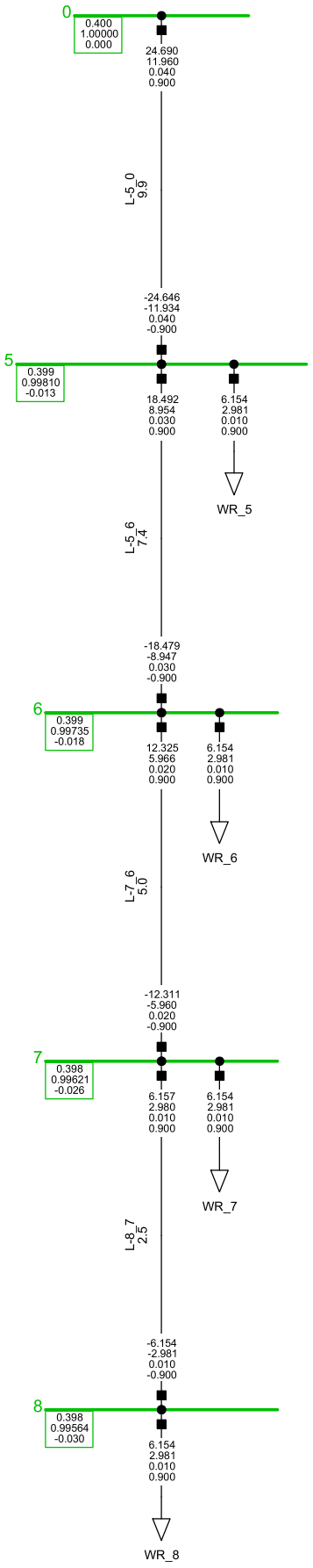
Kurzschlussort SS3

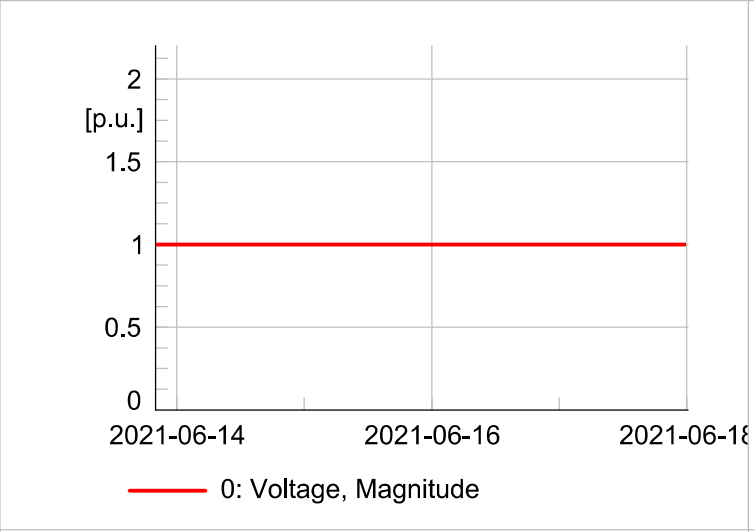
Daten des Kurzschlussortes

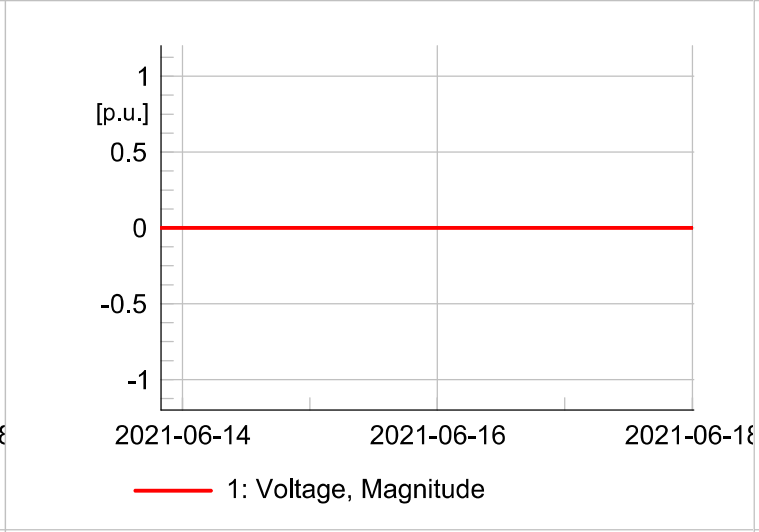
U_n [kV]	Faktor c	SF * Kappa	System	|U_k| [kV]	R [Ohm]	X [Ohm]	Phase	I''k2 [kA]	S''k [MVA]	i_p [kA]
0,400	0,95	1,63	0	0,000	*****	*****	L1	0,000	0,000	0,000
			1	0,110	0,487	0,361	L2	0,314	0,217	0,724
			2	0,110	0,487	0,360	L3	0,314	0,217	0,724

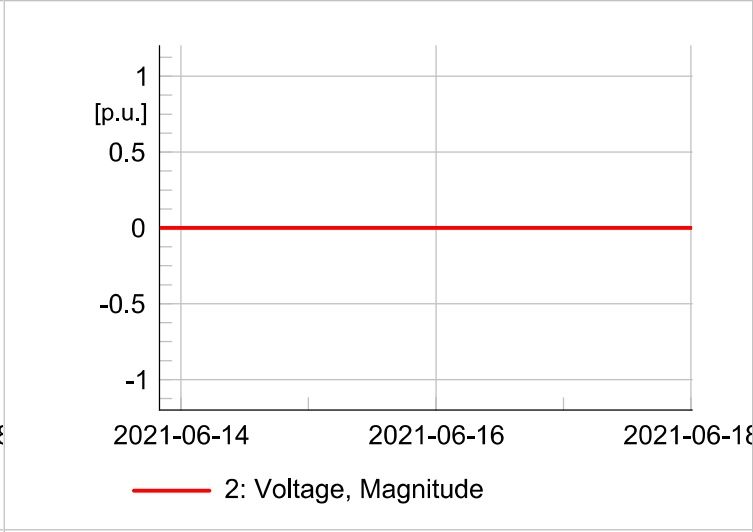
0 - Nullsystem
1 - Mitsystem
2 - Gegensystem

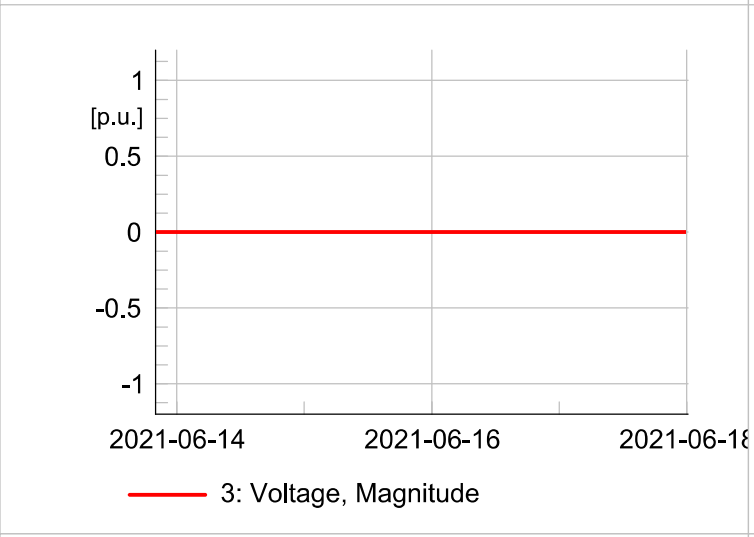
A2: Simulationen PowerFactory

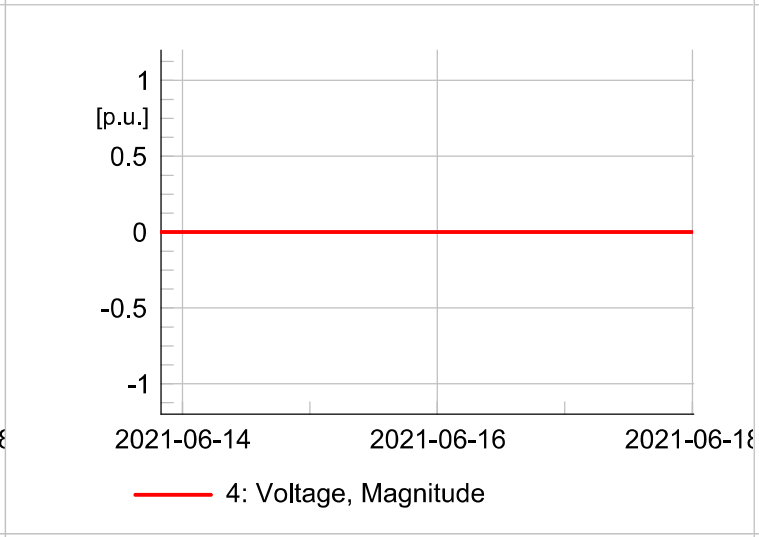

0
0.400
1.00000
0.000
24.690
11.960
0.040
0.900
L-5_0
9.9
-24.646
-11.934
0.040
-0.900
5
0.399
0.99810
-0.013
18.492
8.954
0.030
0.900
6.154
2.981
0.010
0.900
WR_5
L-5_6
7.4
-18.479
-8.947
0.030
-0.900
6
0.399
0.99735
-0.018
12.325
5.966
0.020
0.900
6.154
2.981
0.010
0.900
WR_6
L-7_6
5.0
-12.311
-5.960
0.020
-0.900
7
0.398
0.99621
-0.026
6.157
2.980
0.010
0.900
6.154
2.981
0.010
0.900
WR_7
L-8_7
2.5
-6.154
-2.981
0.010
-0.900
8
0.398
0.99564
-0.030
6.154
2.981
0.010
0.900
WR_8

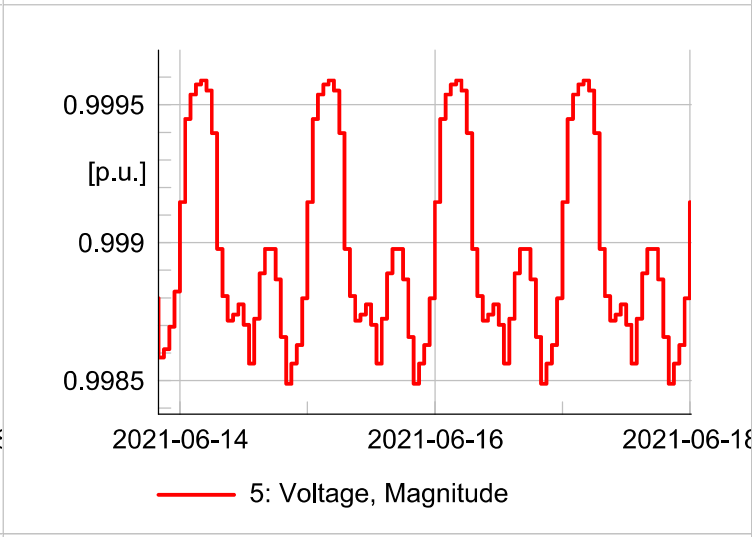

2
[p.u.]
1.5
1
0.5
0
2021-06-14
2021-06-16
2021-06-18
0: Voltage, Magnitude

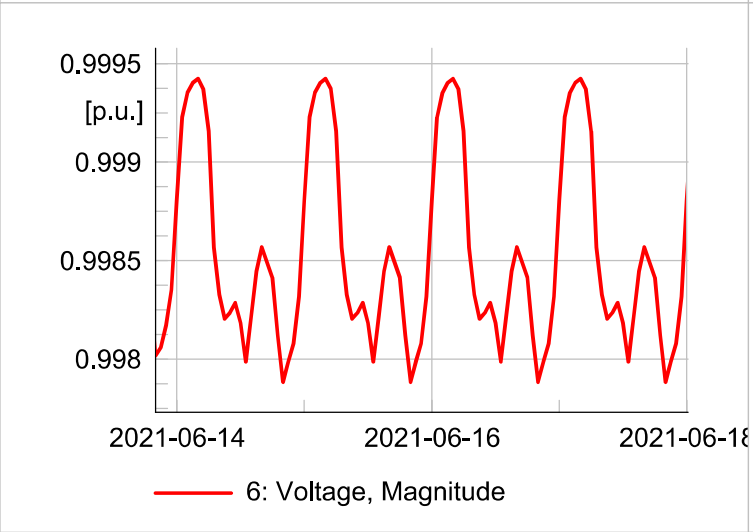

1
[p.u.]
0.5
0
-0.5
-1
2021-06-14
2021-06-16
2021-06-18
1: Voltage, Magnitude

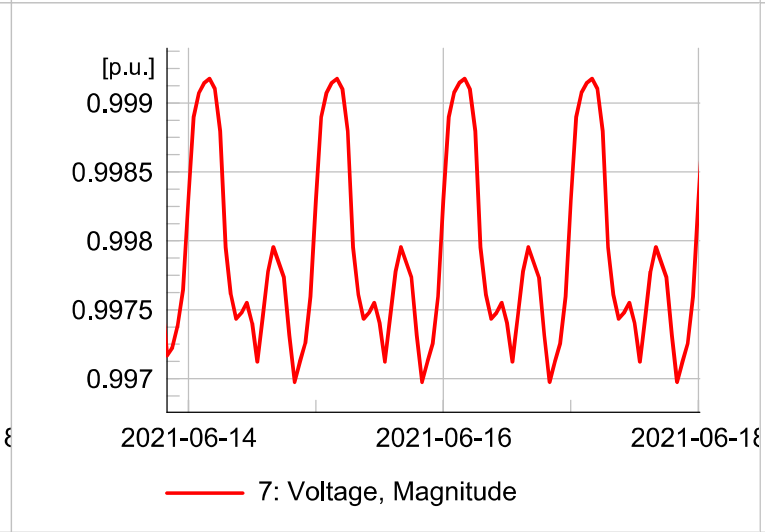

1
[p.u.]
0.5
0
-0.5
-1
2021-06-14
2021-06-16
2021-06-18
2: Voltage, Magnitude

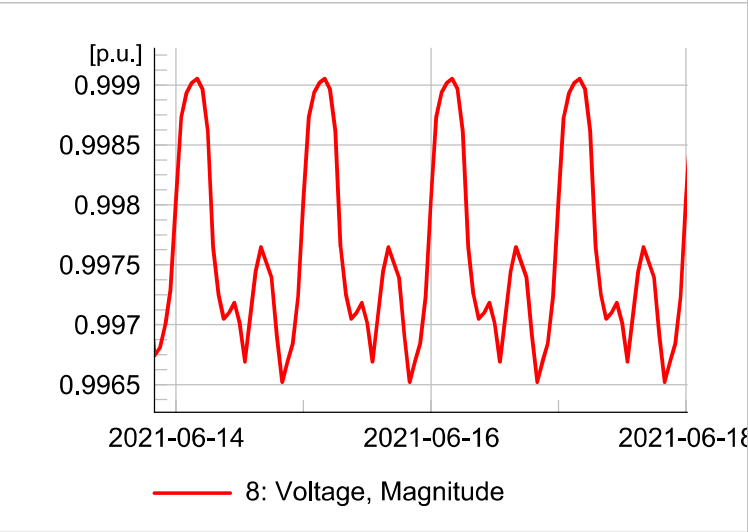

1
[p.u.]
0.5
0
-0.5
-1
2021-06-14
2021-06-16
2021-06-18
3: Voltage, Magnitude

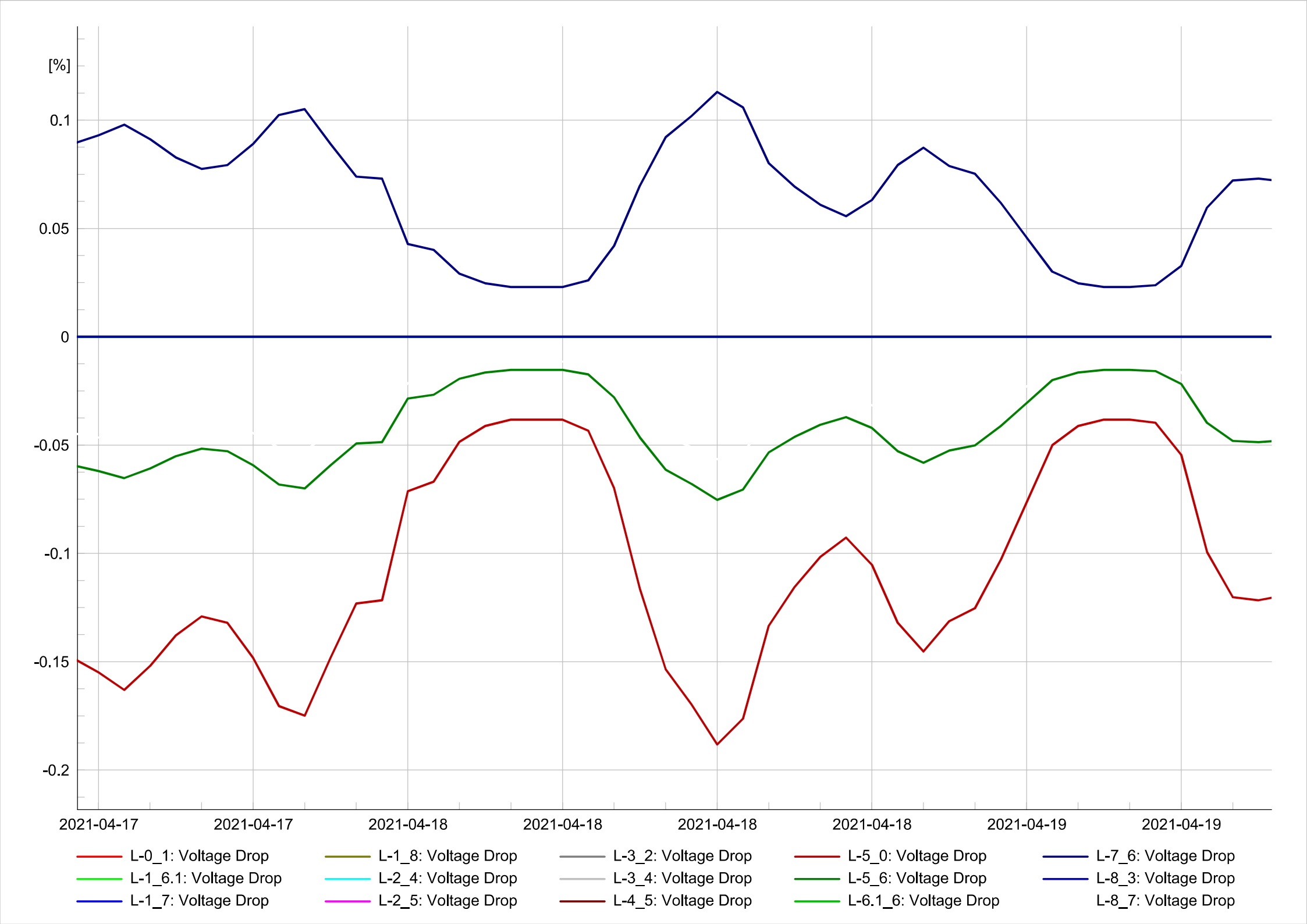

1
[p.u.]
0.5
0
-0.5
-1
2021-06-14
2021-06-16
2021-06-18
4: Voltage, Magnitude

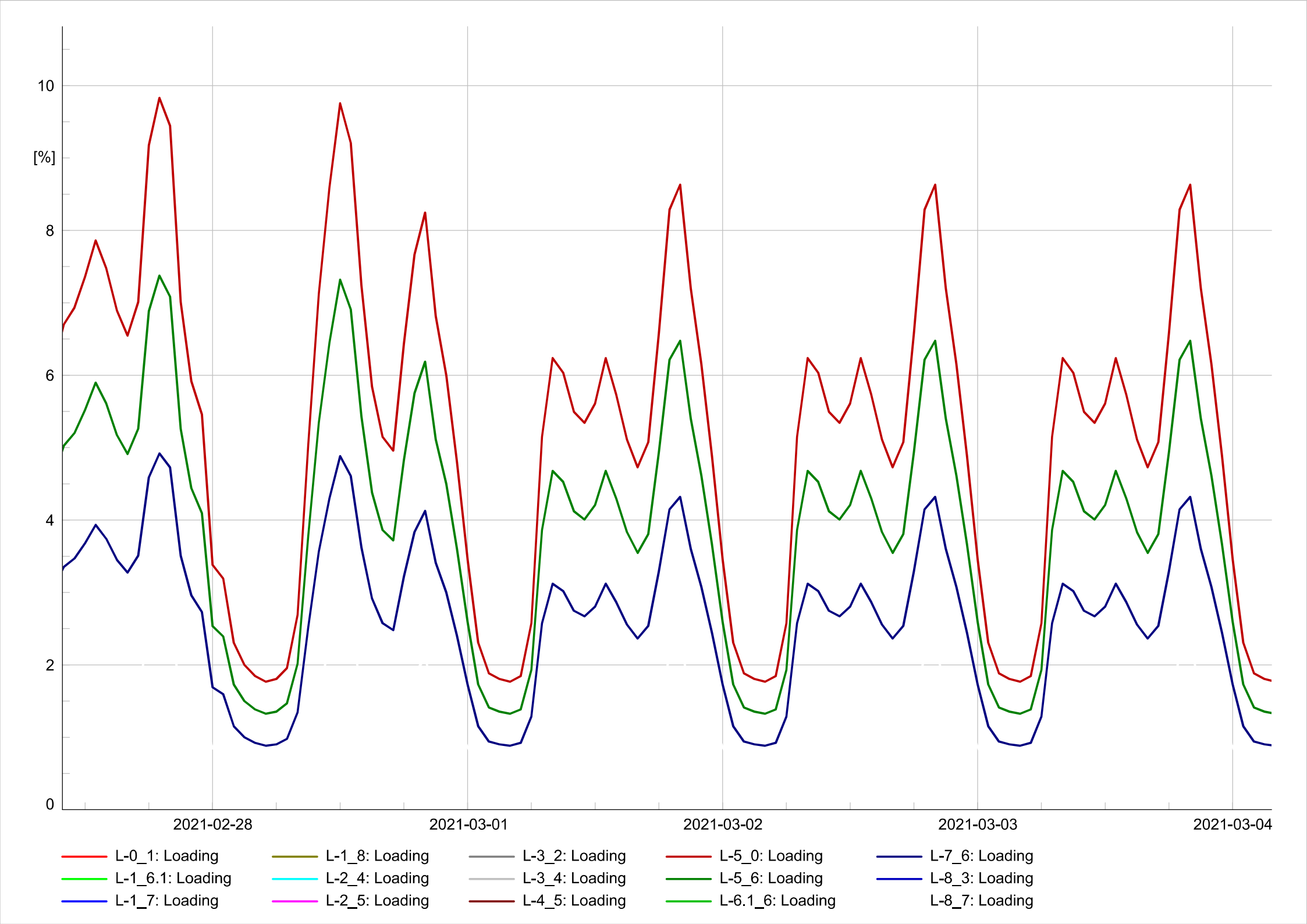

0.9995
[p.u.]
0.999
0.9985
2021-06-14
2021-06-16
2021-06-18
5: Voltage, Magnitude

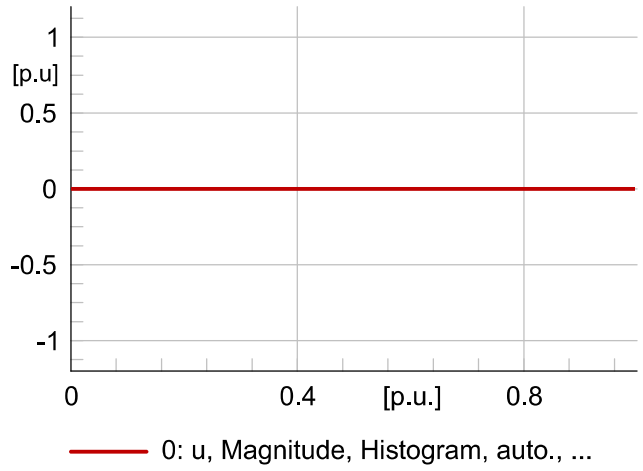

0.9995
[p.u.]
0.999
0.9985
0.998
2021-06-14
2021-06-16
2021-06-18
6: Voltage, Magnitude

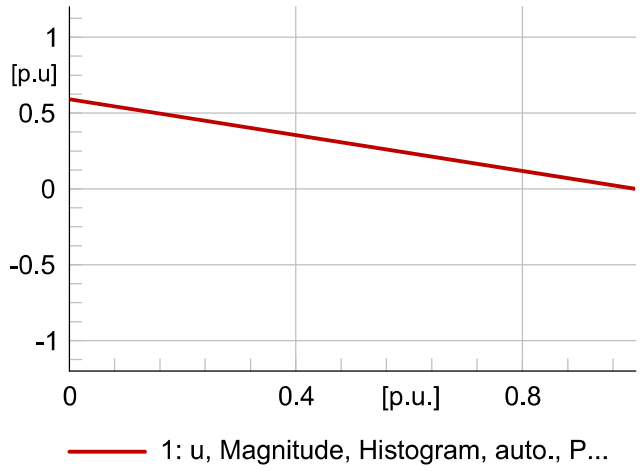

[p.u.]
0.999
0.9985
0.998
0.9975
0.997
2021-06-14
2021-06-16
2021-06-18
7: Voltage, Magnitude

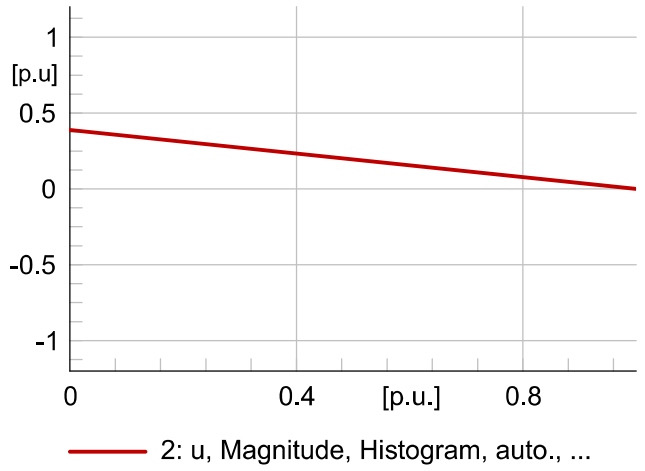

[p.u.]
0.999
0.9985
0.998
0.9975
0.997
0.9965
2021-06-14
2021-06-16
2021-06-18
8: Voltage, Magnitude

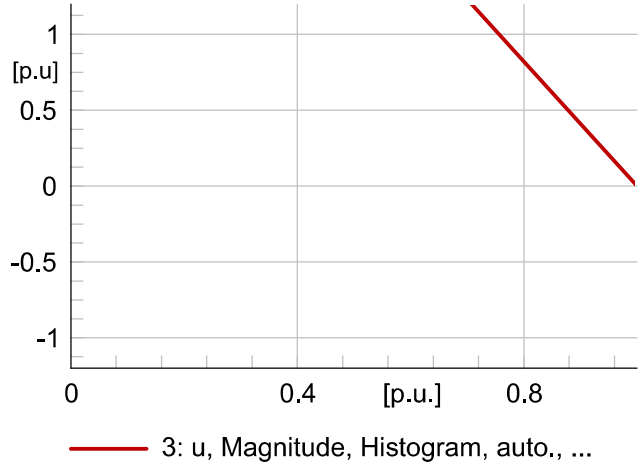

[%]
0.1
0.05
0
-0.05
-0.1
-0.15
-0.2
2021-04-17
2021-04-17
2021-04-18
2021-04-18
2021-04-18
2021-04-18
2021-04-19
2021-04-19
L-0_1: Voltage Drop
L-1_8: Voltage Drop
L-3_2: Voltage Drop
L-5_0: Voltage Drop
L-7_6: Voltage Drop
L-1_6.1: Voltage Drop
L-2_4: Voltage Drop
L-3_4: Voltage Drop
L-5_6: Voltage Drop
L-8_3: Voltage Drop
L-1_7: Voltage Drop
L-2_5: Voltage Drop
L-4_5: Voltage Drop
L-6.1_6: Voltage Drop
L-8_7: Voltage Drop

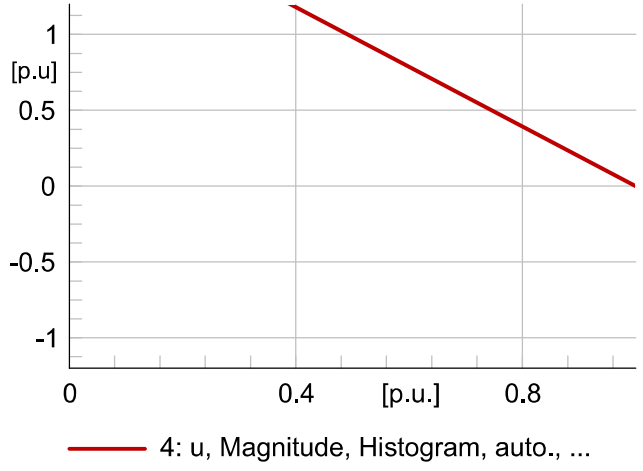

10
[%]
8
6
4
2
0
2021-02-28
2021-03-01
2021-03-02
2021-03-03
2021-03-04
L-0_1: Loading
L-1_6.1: Loading
L-1_7: Loading
L-1_8: Loading
L-2_4: Loading
L-2_5: Loading
L-3_2: Loading
L-3_4: Loading
L-4_5: Loading
L-5_0: Loading
L-5_6: Loading
L-6.1_6: Loading
L-7_6: Loading
L-8_3: Loading
L-8_7: Loading

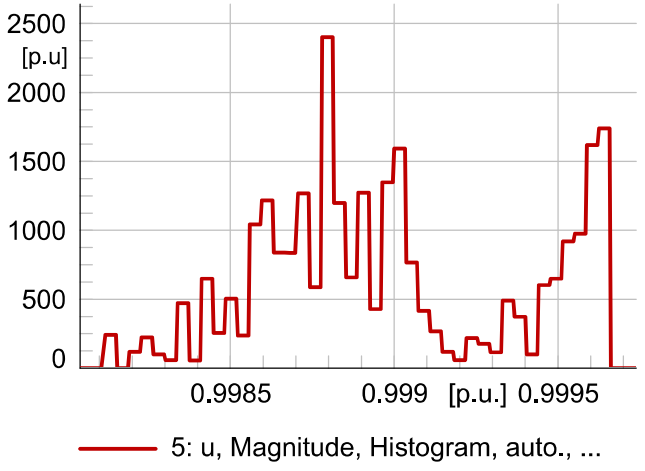

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
0: u, Magnitude, Histogram, auto., ...

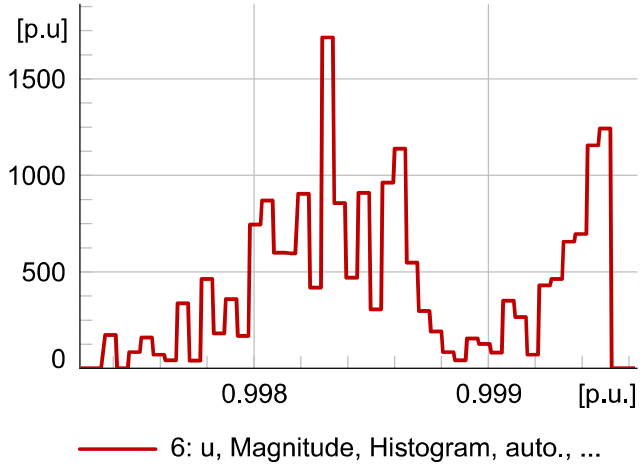

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
1: u, Magnitude, Histogram, auto., P...

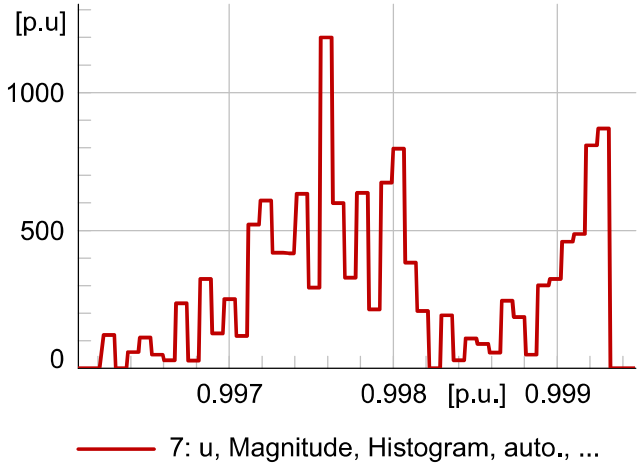

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
2: u, Magnitude, Histogram, auto., ...

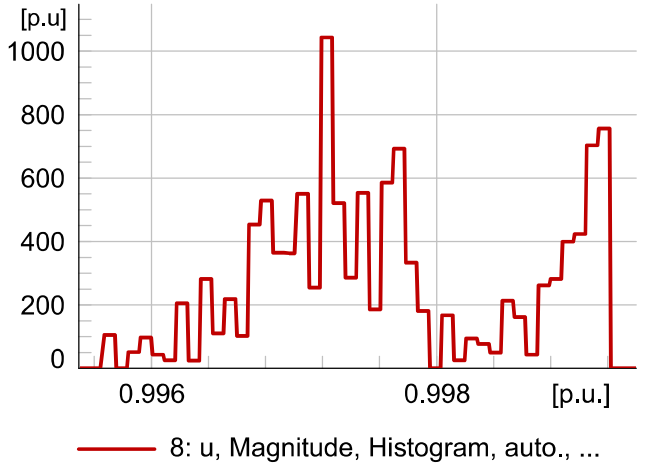

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
3: u, Magnitude, Histogram, auto., ...

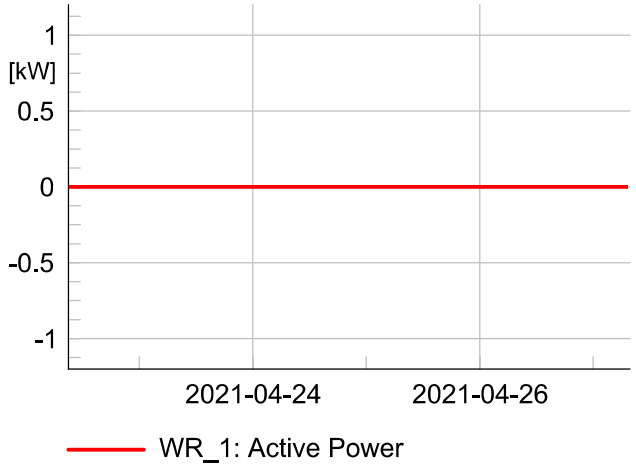

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
4: u, Magnitude, Histogram, auto., ...

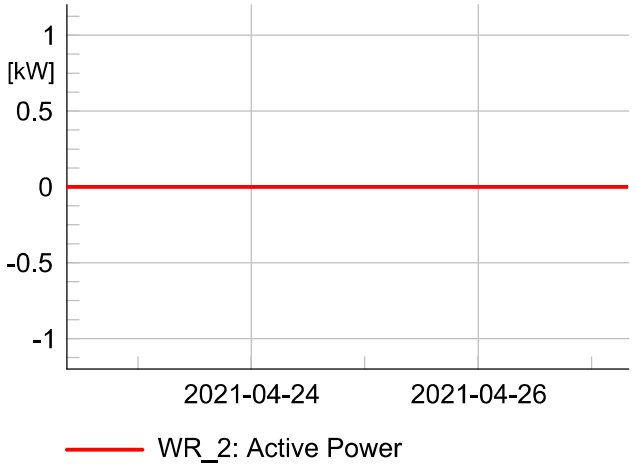

2500
[p.u]
2000
1500
1000
500
0
0.9985
0.999
[p.u.]
0.9995
5: u, Magnitude, Histogram, auto., ...

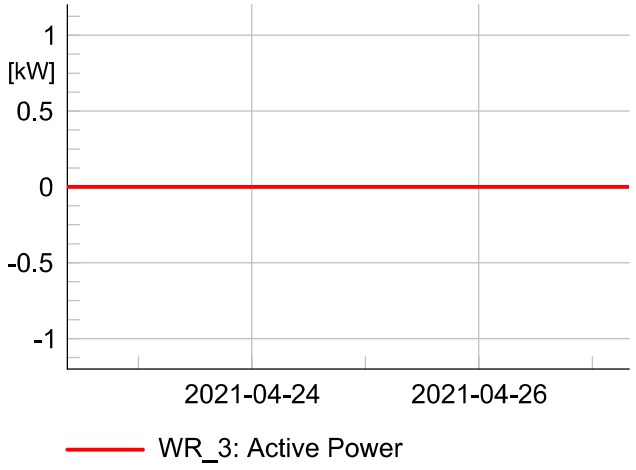

[p.u]
1500
1000
500
0
0.998
0.999
[p.u.]
6: u, Magnitude, Histogram, auto., ...

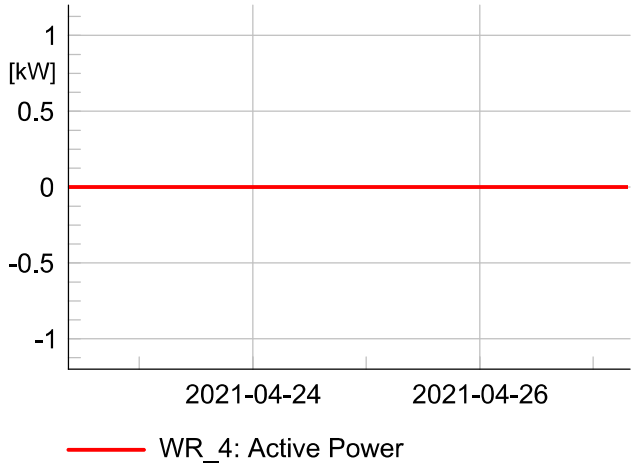

[p.u]
1000
500
0
0.997
0.998
[p.u.]
0.999
7: u, Magnitude, Histogram, auto., ...

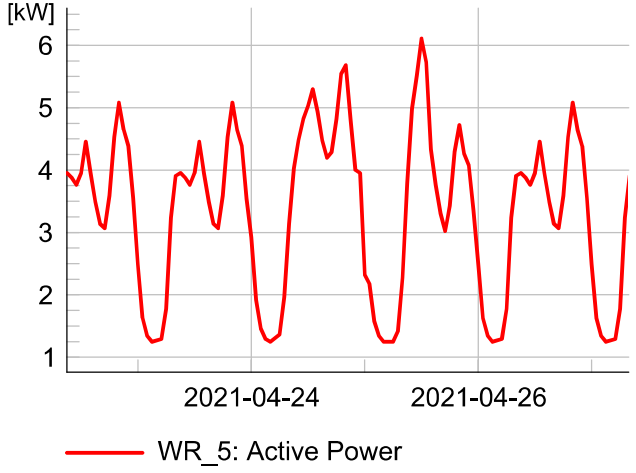

[p.u]
1000
800
600
400
200
0
0.996
0.998
[p.u.]
8: u, Magnitude, Histogram, auto., ...

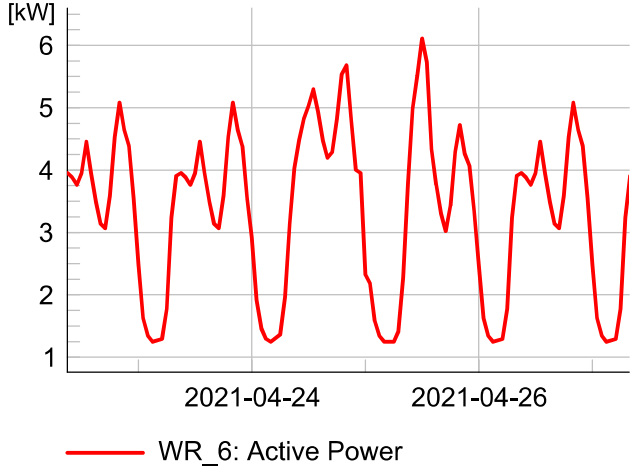

1
[kW]
0.5
0
-0.5
-1
2021-04-24
2021-04-26
WR_1: Active Power

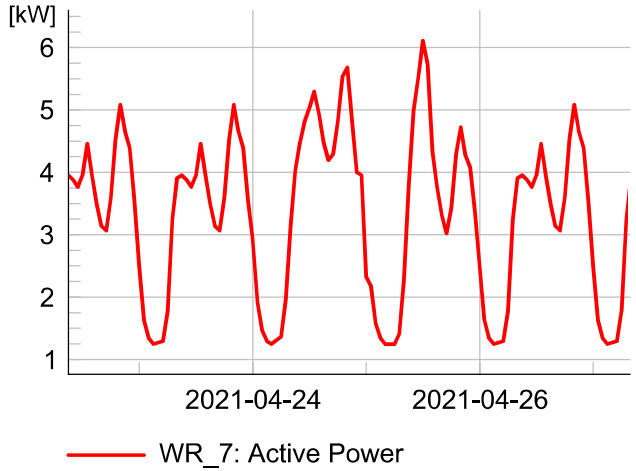

1
[kW]
0.5
0
-0.5
-1
2021-04-24
2021-04-26
WR_2: Active Power

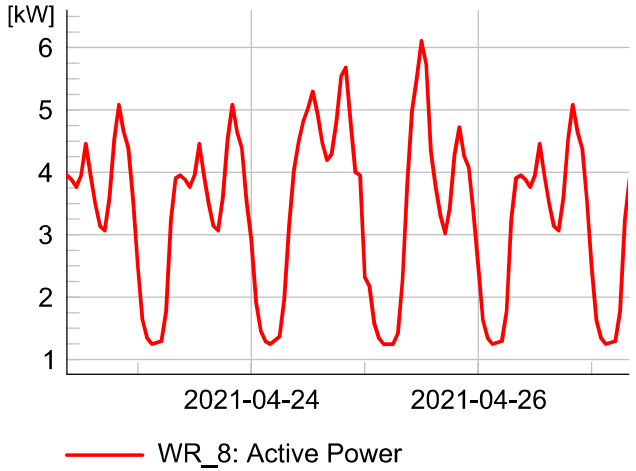

1
[kW]
0.5
0
-0.5
-1
2021-04-24
2021-04-26
WR_3: Active Power

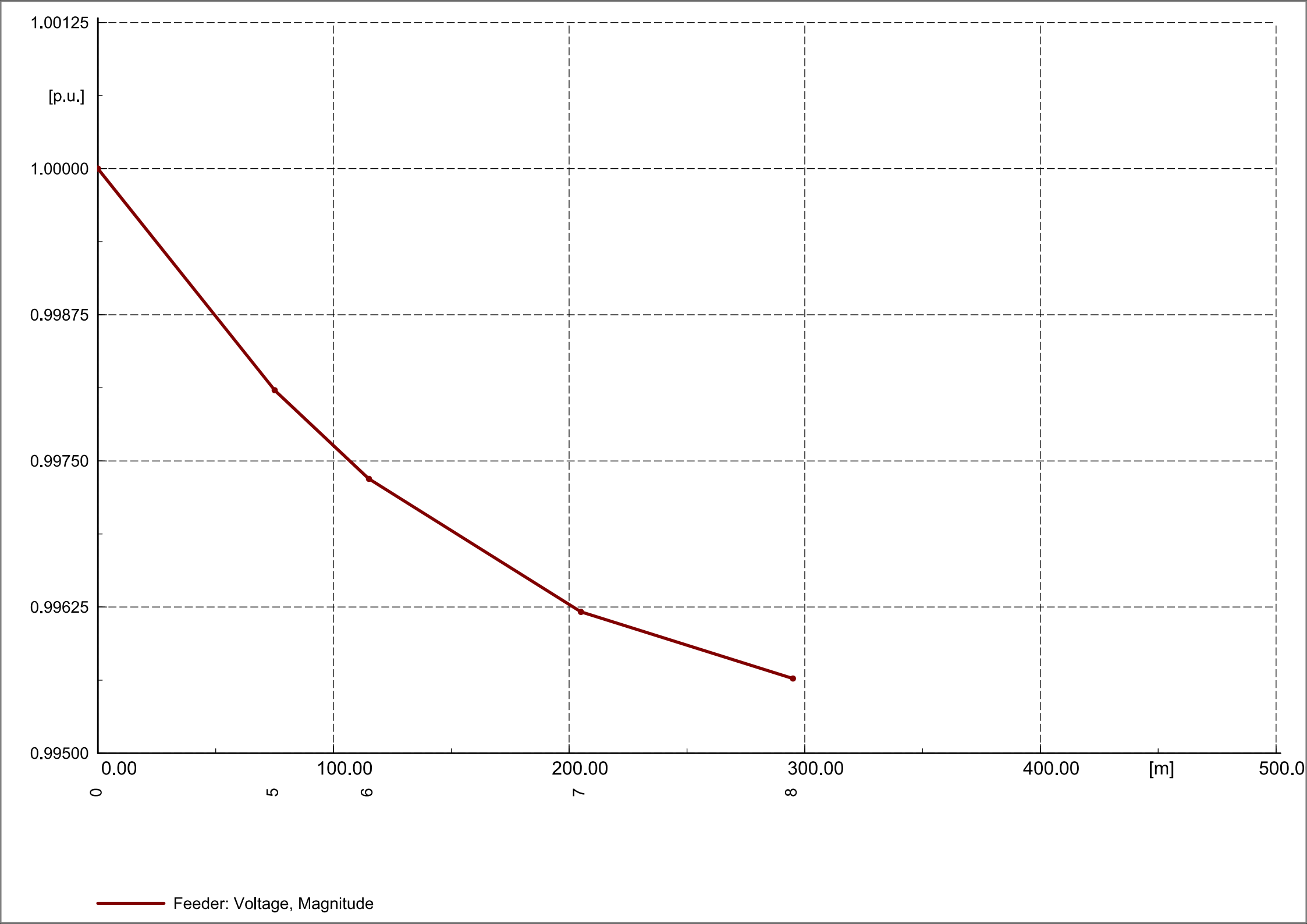

1
[kW]
0.5
0
-0.5
-1
2021-04-24
2021-04-26
WR_4: Active Power

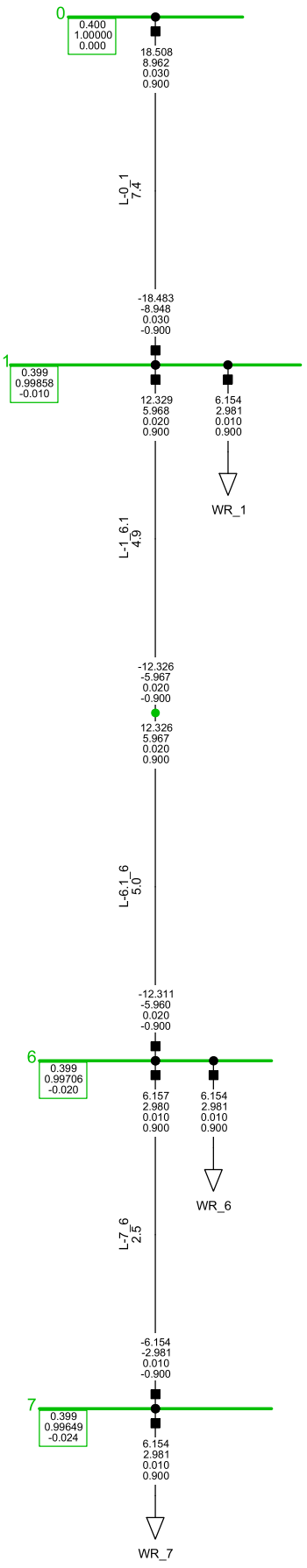

[kW]
6
5
4
3
2
1
2021-04-24
2021-04-26
WR_5: Active Power

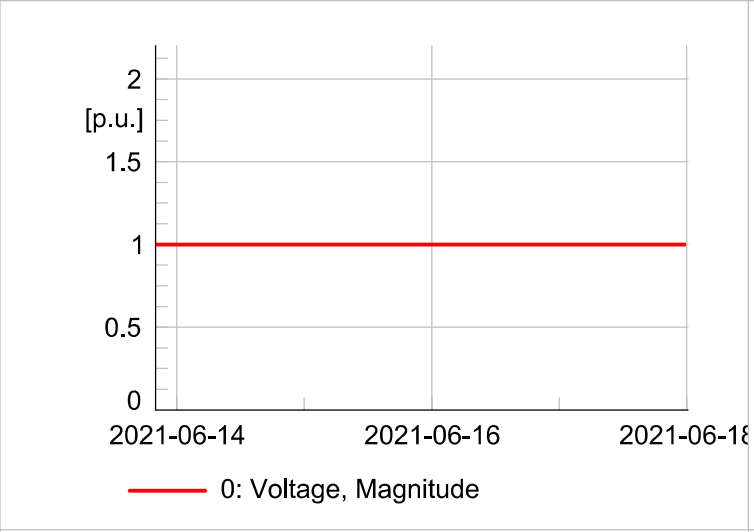

[kW]
6
5
4
3
2
1
2021-04-24
2021-04-26
WR_6: Active Power

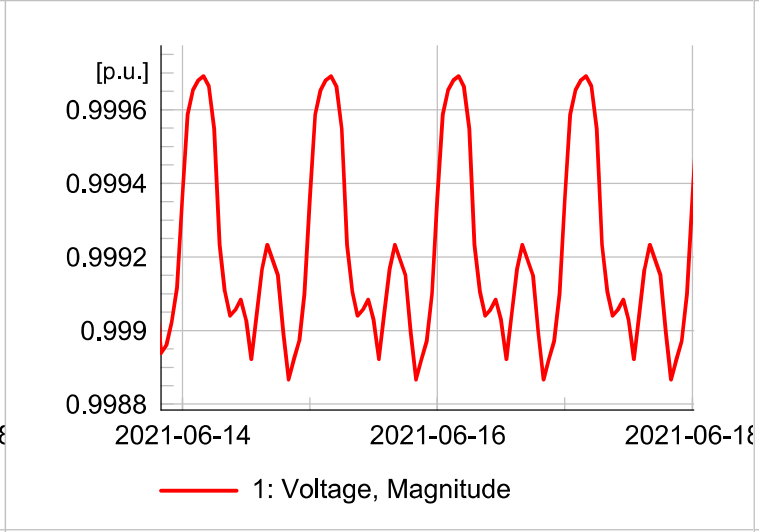

[kW]
6
5
4
3
2
1
2021-04-24
2021-04-26
WR_7: Active Power

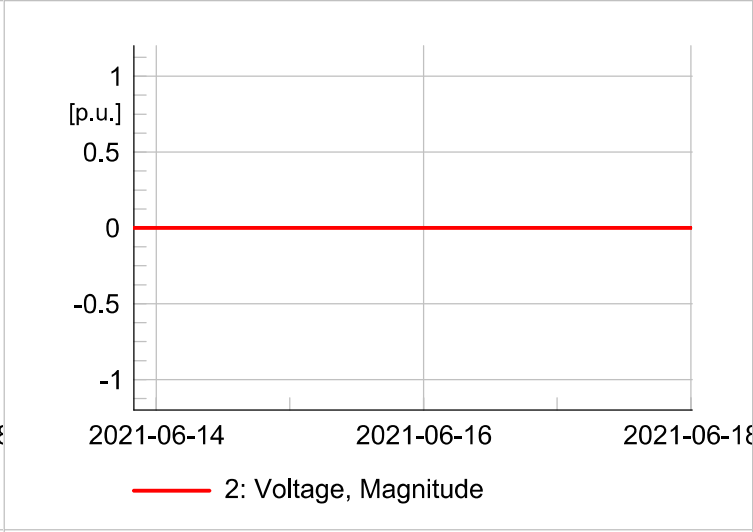

[kW]
6
5
4
3
2
1
2021-04-24
2021-04-26
WR_8: Active Power

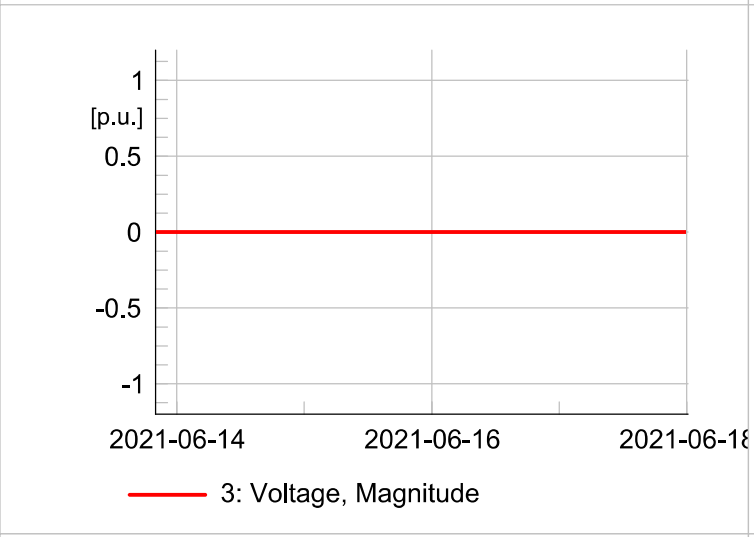

1.00125
[p.u.]
1.00000
0.99875
0.99750
0.99625
0.99500
0.00
100.00
200.00
300.00
400.00
[m]
500.0
0
5
6
7
8
Feeder: Voltage, Magnitude

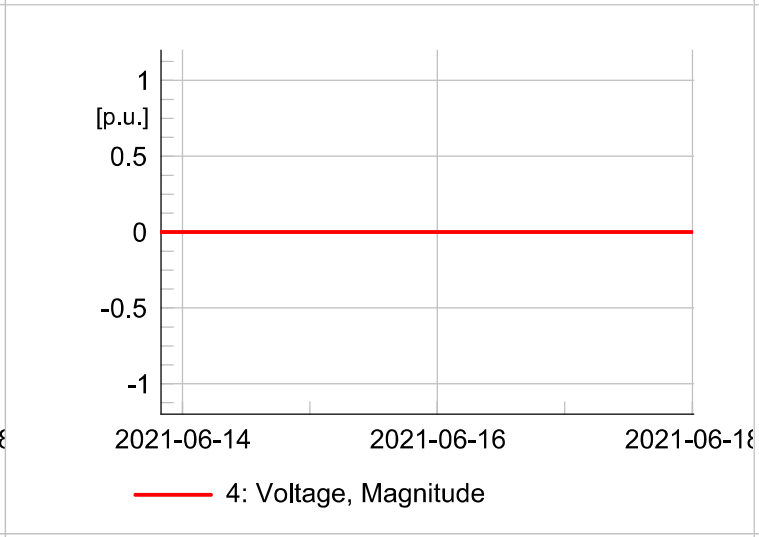

0
0.400
1.00000
0.000
18.508
8.962
0.030
0.900
L-0_1
7.4
-18.483
-8.948
0.030
-0.900
1
0.399
0.99858
-0.010
12.329
5.968
0.020
0.900
6.154
2.981
0.010
0.900
WR_1
L-1_6.1
4.9
-12.326
-5.967
0.020
-0.900
12.326
5.967
0.020
0.900
L-6.1_6
5.0
-12.311
-5.960
0.020
-0.900
6
0.399
0.99706
-0.020
6.157
2.980
0.010
0.900
6.154
2.981
0.010
0.900
WR_6
L-7_6
2.5
-6.154
-2.981
0.010
-0.900
7
0.399
0.99649
-0.024
6.154
2.981
0.010
0.900
WR_7

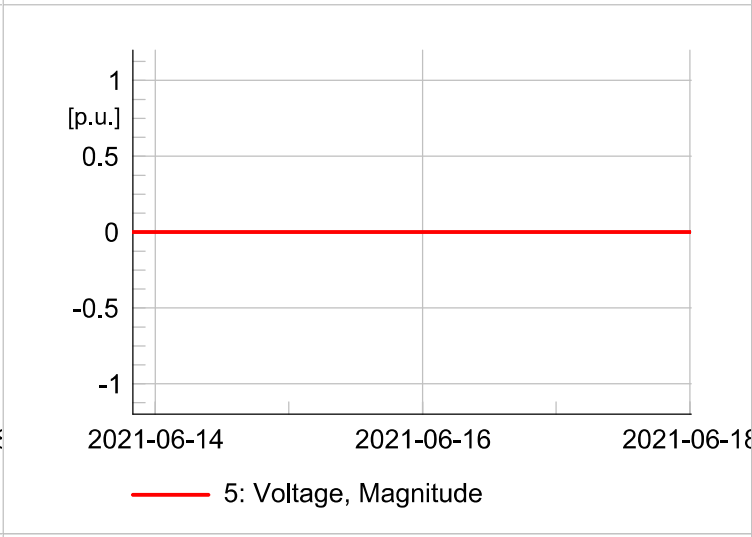

2
[p.u.]
1.5
1
0.5
0
2021-06-14
2021-06-16
2021-06-18
0: Voltage, Magnitude

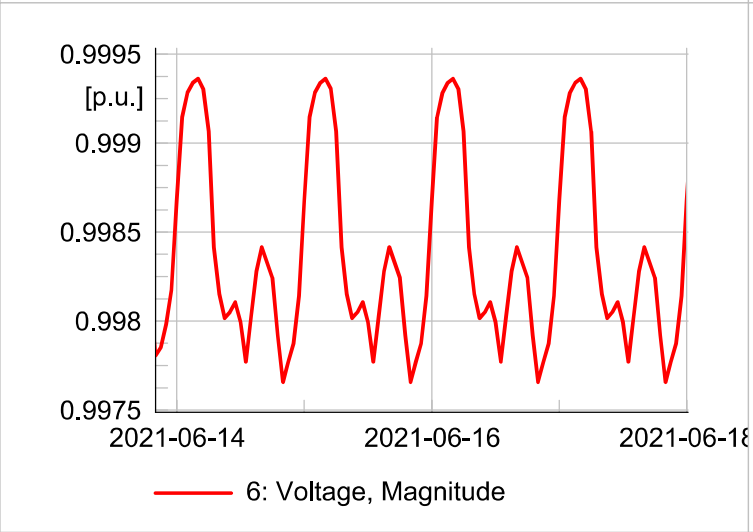

[p.u.]
0.9996
0.9994
0.9992
0.999
0.9988
2021-06-14
2021-06-16
2021-06-18
1: Voltage, Magnitude

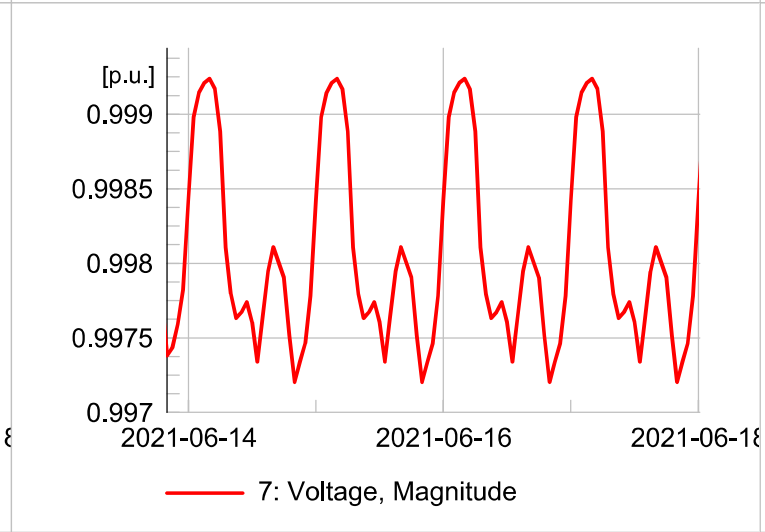

1
[p.u.]
0.5
0
-0.5
-1
2021-06-14
2021-06-16
2021-06-18
2: Voltage, Magnitude

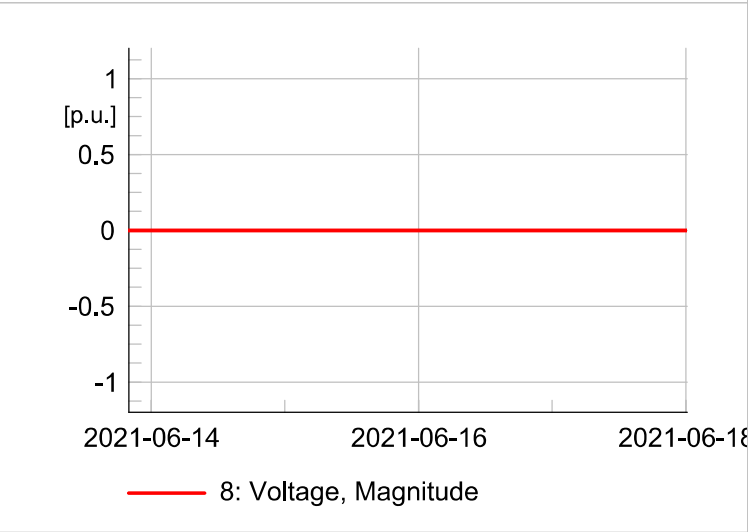

1
[p.u.]
0.5
0
-0.5
-1
2021-06-14
2021-06-16
2021-06-18
3: Voltage, Magnitude

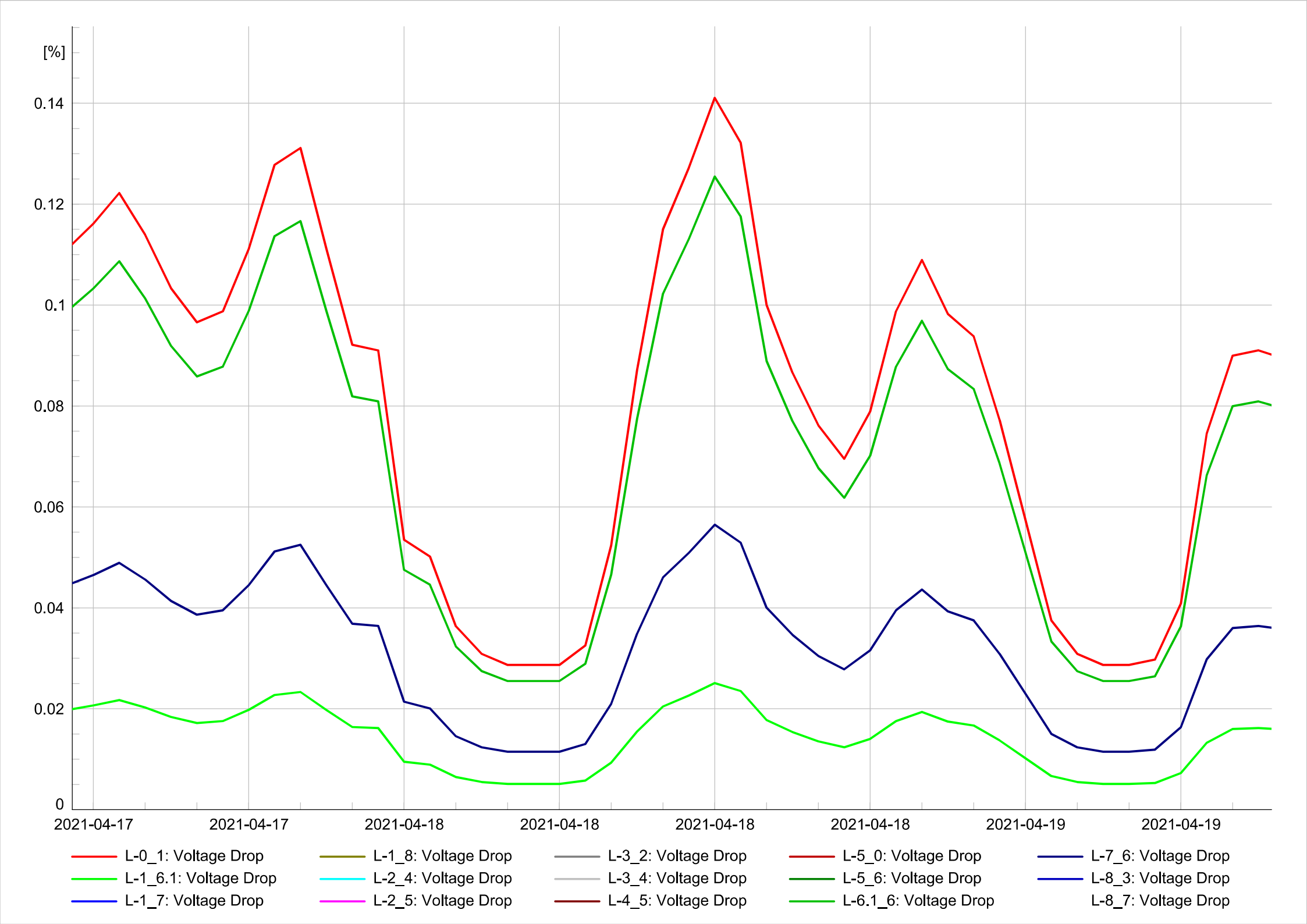

1
[p.u.]
0.5
0
-0.5
-1
2021-06-14
2021-06-16
2021-06-18
4: Voltage, Magnitude

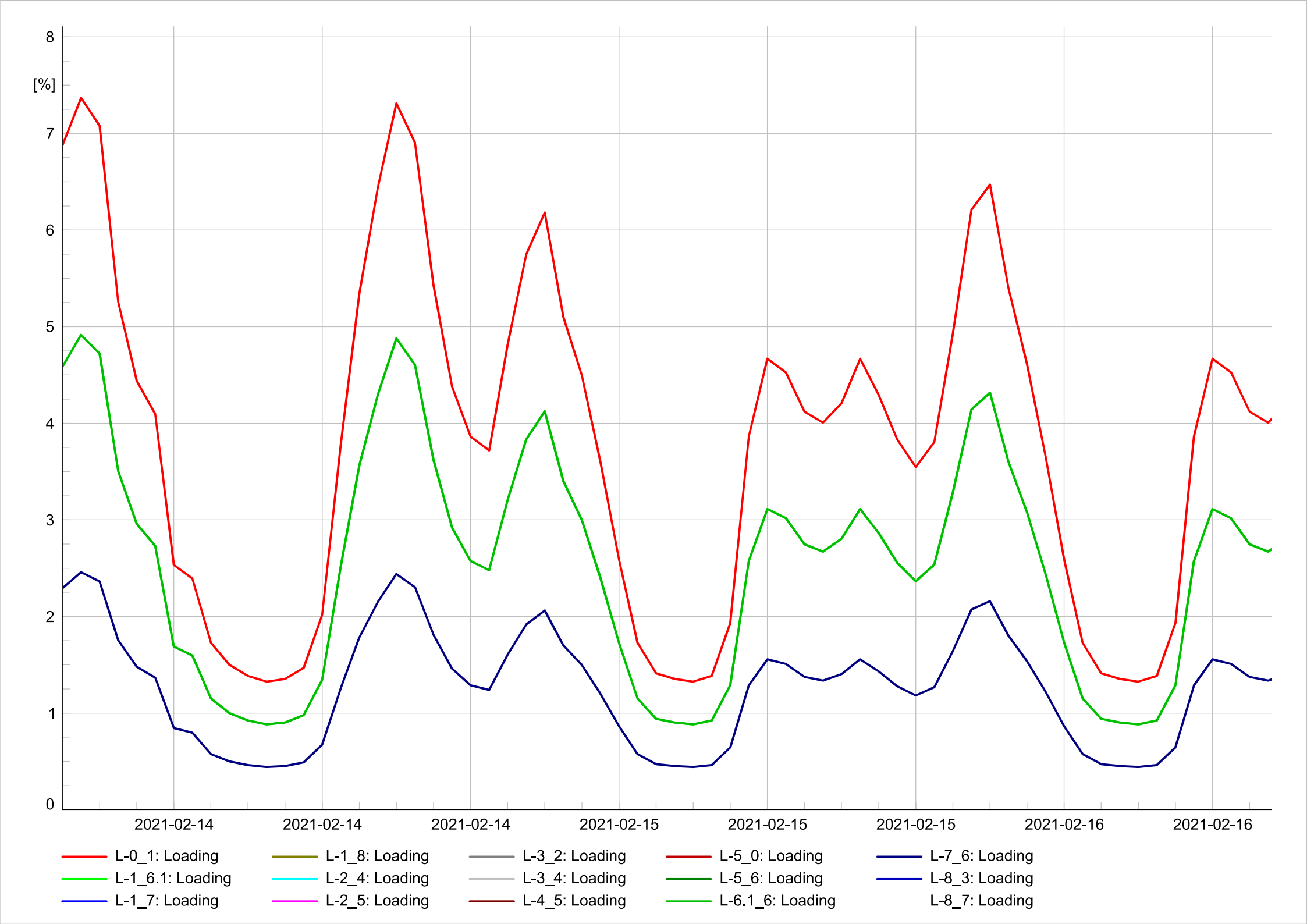

1
[p.u.]
0.5
0
-0.5
-1
2021-06-14
2021-06-16
2021-06-18
5: Voltage, Magnitude

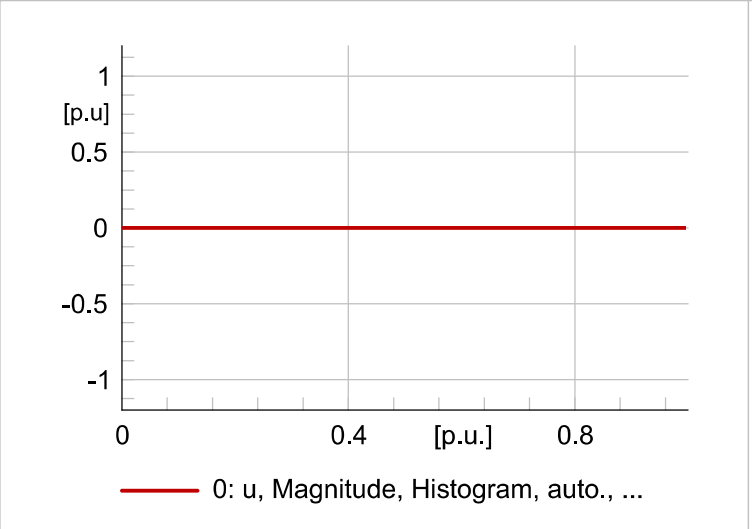

0.9995
[p.u.]
0.999
0.9985
0.998
0.9975
2021-06-14
2021-06-16
2021-06-18
6: Voltage, Magnitude

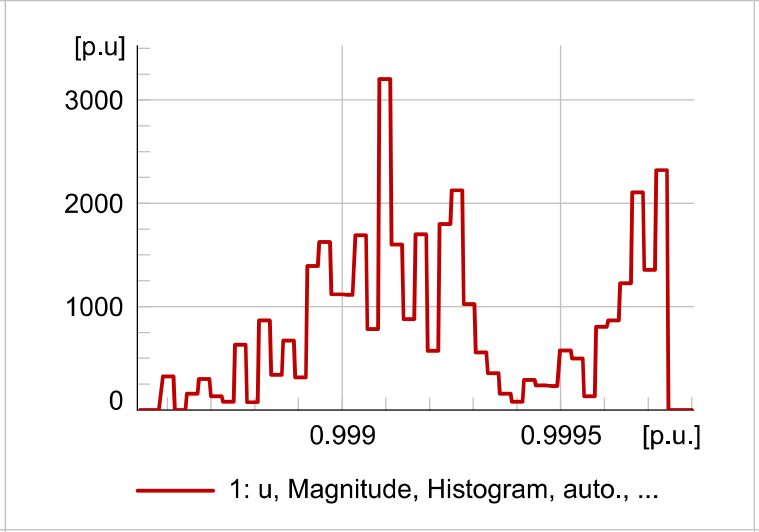

[p.u.]
0.999
0.9985
0.998
0.9975
0.997
2021-06-14
2021-06-16
2021-06-18
7: Voltage, Magnitude

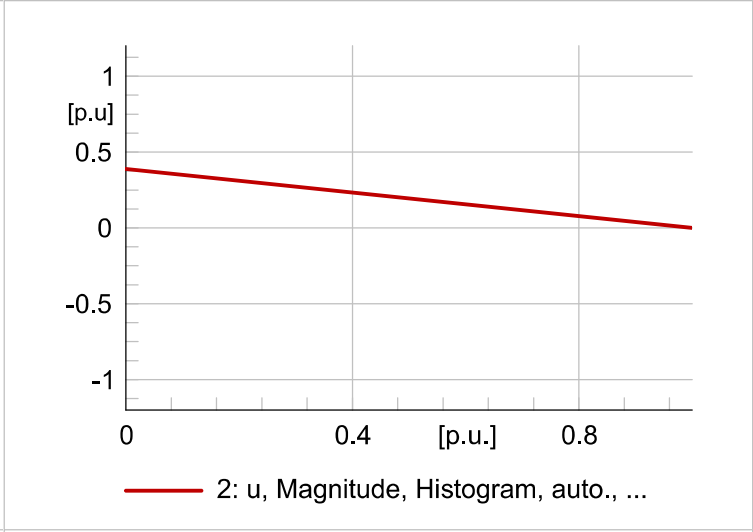

1
[p.u.]
0.5
0
-0.5
-1
2021-06-14
2021-06-16
2021-06-18
8: Voltage, Magnitude

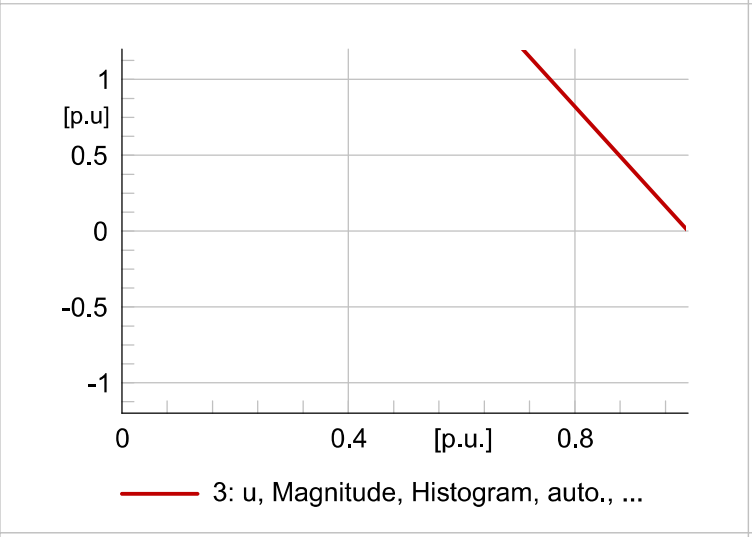

[%]
0.14
0.12
0.1
0.08
0.06
0.04
0.02
0
2021-04-17
2021-04-17
2021-04-18
2021-04-18
2021-04-18
2021-04-18
2021-04-19
2021-04-19
L-0_1: Voltage Drop
L-1_6.1: Voltage Drop
L-1_7: Voltage Drop
L-1_8: Voltage Drop
L-2_4: Voltage Drop
L-2_5: Voltage Drop
L-3_2: Voltage Drop
L-3_4: Voltage Drop
L-4_5: Voltage Drop
L-5_0: Voltage Drop
L-5_6: Voltage Drop
L-6.1_6: Voltage Drop
L-7_6: Voltage Drop
L-8_3: Voltage Drop
L-8_7: Voltage Drop

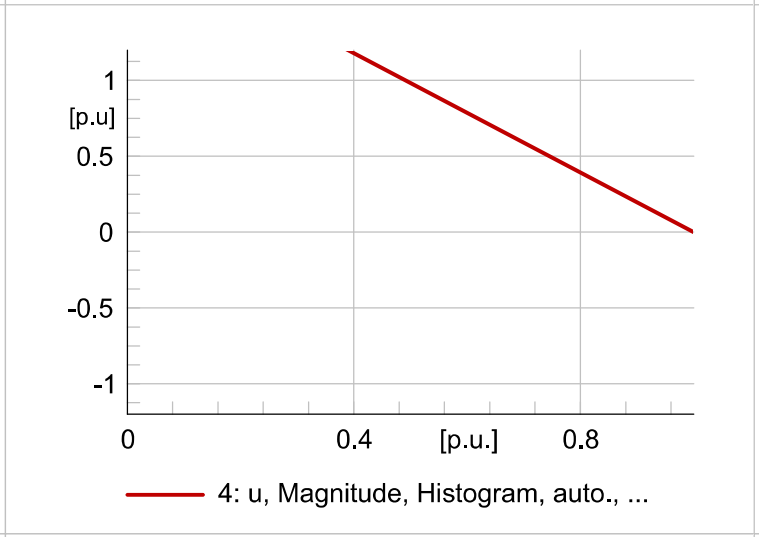

8
[%]
7
6
5
4
3
2
1
0
2021-02-14
2021-02-14
2021-02-14
2021-02-15
2021-02-15
2021-02-15
2021-02-16
2021-02-16
L-0_1: Loading
L-1_6.1: Loading
L-1_7: Loading
L-1_8: Loading
L-2_4: Loading
L-2_5: Loading
L-3_2: Loading
L-3_4: Loading
L-4_5: Loading
L-5_0: Loading
L-5_6: Loading
L-6.1_6: Loading
L-7_6: Loading
L-8_3: Loading
L-8_7: Loading

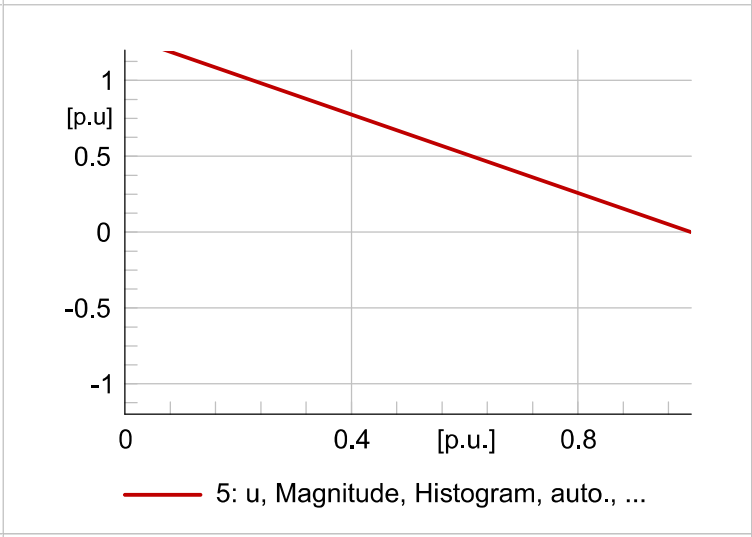

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
0: u, Magnitude, Histogram, auto., ...

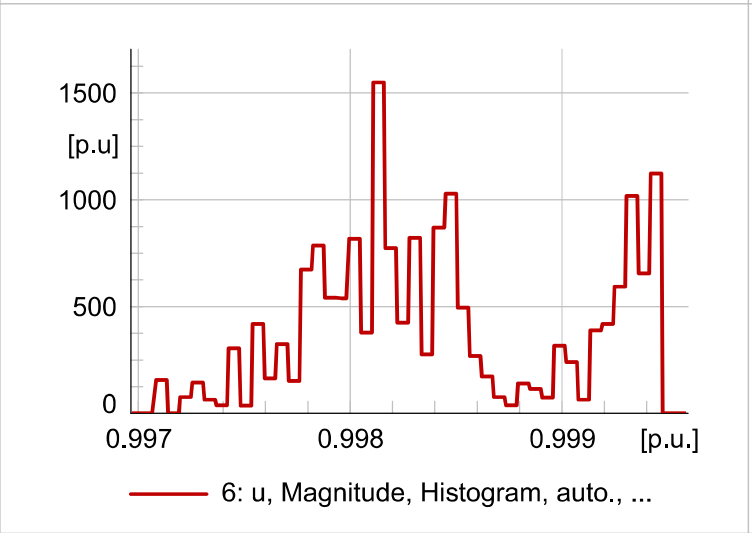

[p.u]
3000
2000
1000
0
0.999
0.9995
[p.u.]
1: u, Magnitude, Histogram, auto., ...

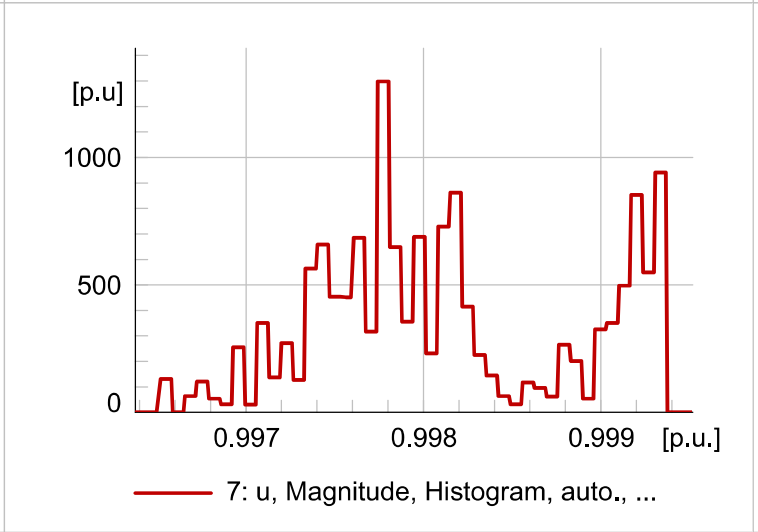

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
2: u, Magnitude, Histogram, auto., ...

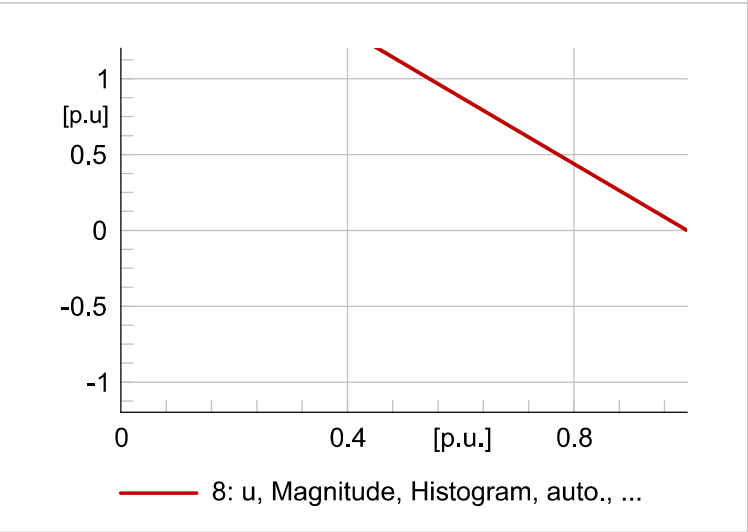

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
3: u, Magnitude, Histogram, auto., ...

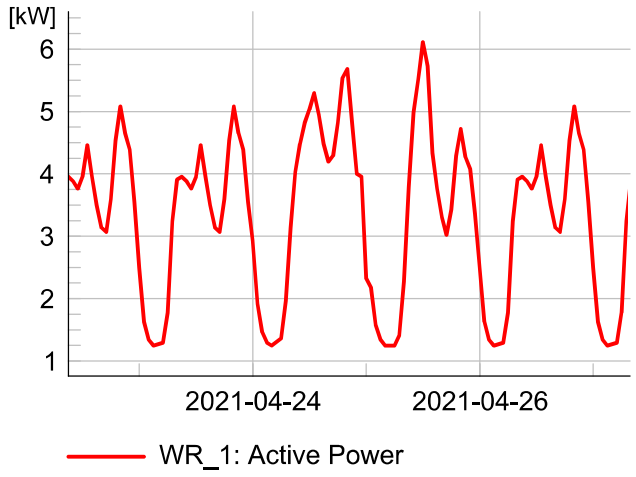

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
4: u, Magnitude, Histogram, auto., ...

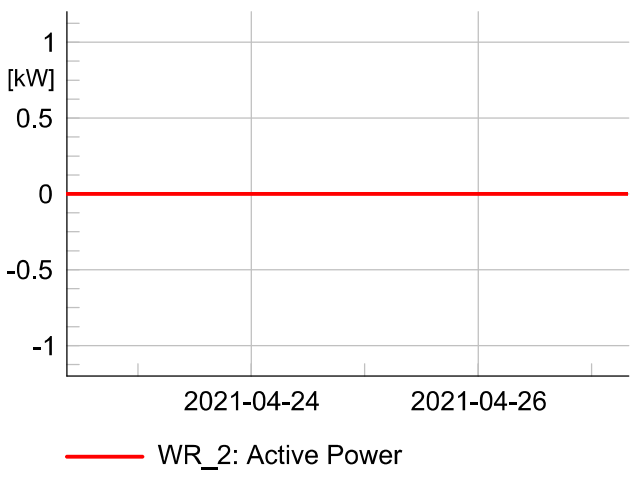

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
5: u, Magnitude, Histogram, auto., ...

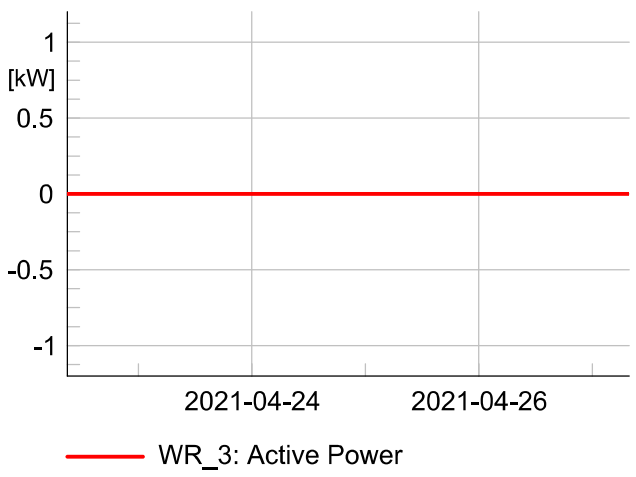

1500
[p.u]
1000
500
0
0.997
0.998
0.999
[p.u.]
6: u, Magnitude, Histogram, auto., ...

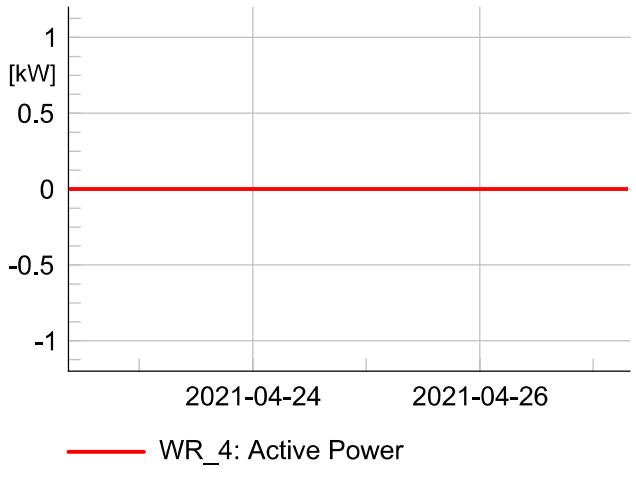

[p.u]
1000
500
0
0.997
0.998
0.999
[p.u.]
7: u, Magnitude, Histogram, auto., ...

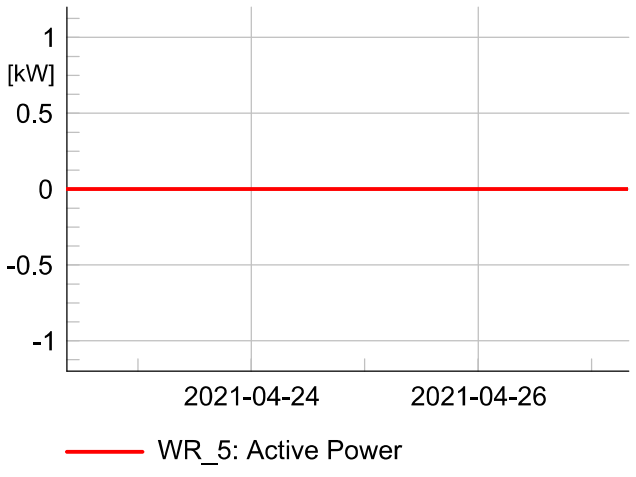

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
8: u, Magnitude, Histogram, auto., ...

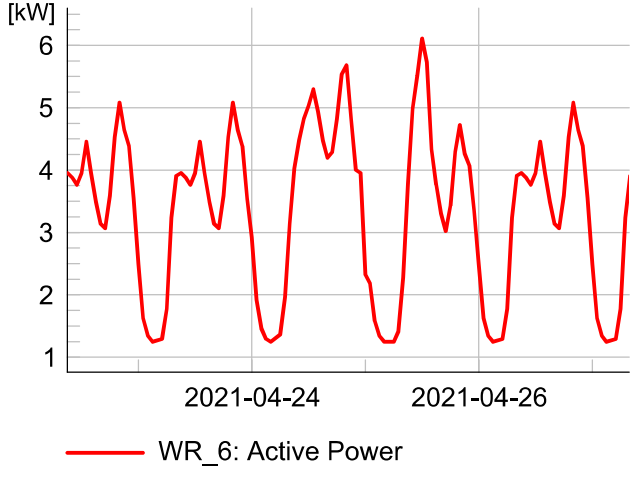

[kW]
6
5
4
3
2
1
2021-04-24
2021-04-26
WR_1: Active Power

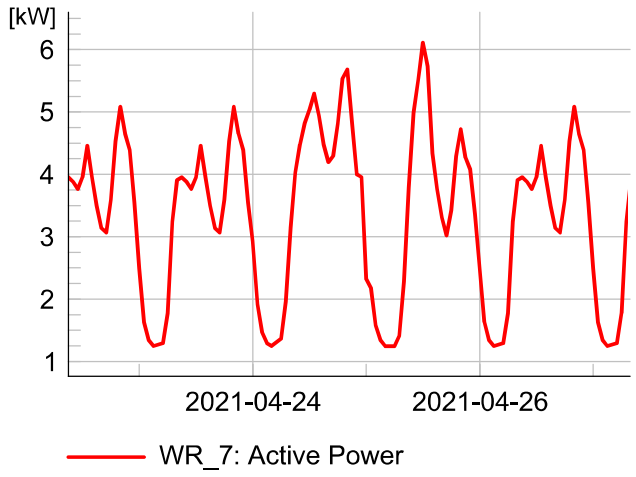

1
[kW]
0.5
0
-0.5
-1
2021-04-24
2021-04-26
WR_2: Active Power

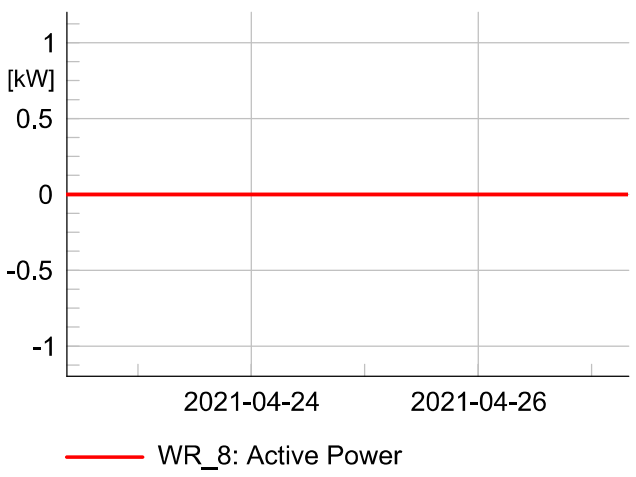

1
[kW]
0.5
0
-0.5
-1
2021-04-24
2021-04-26
WR_3: Active Power

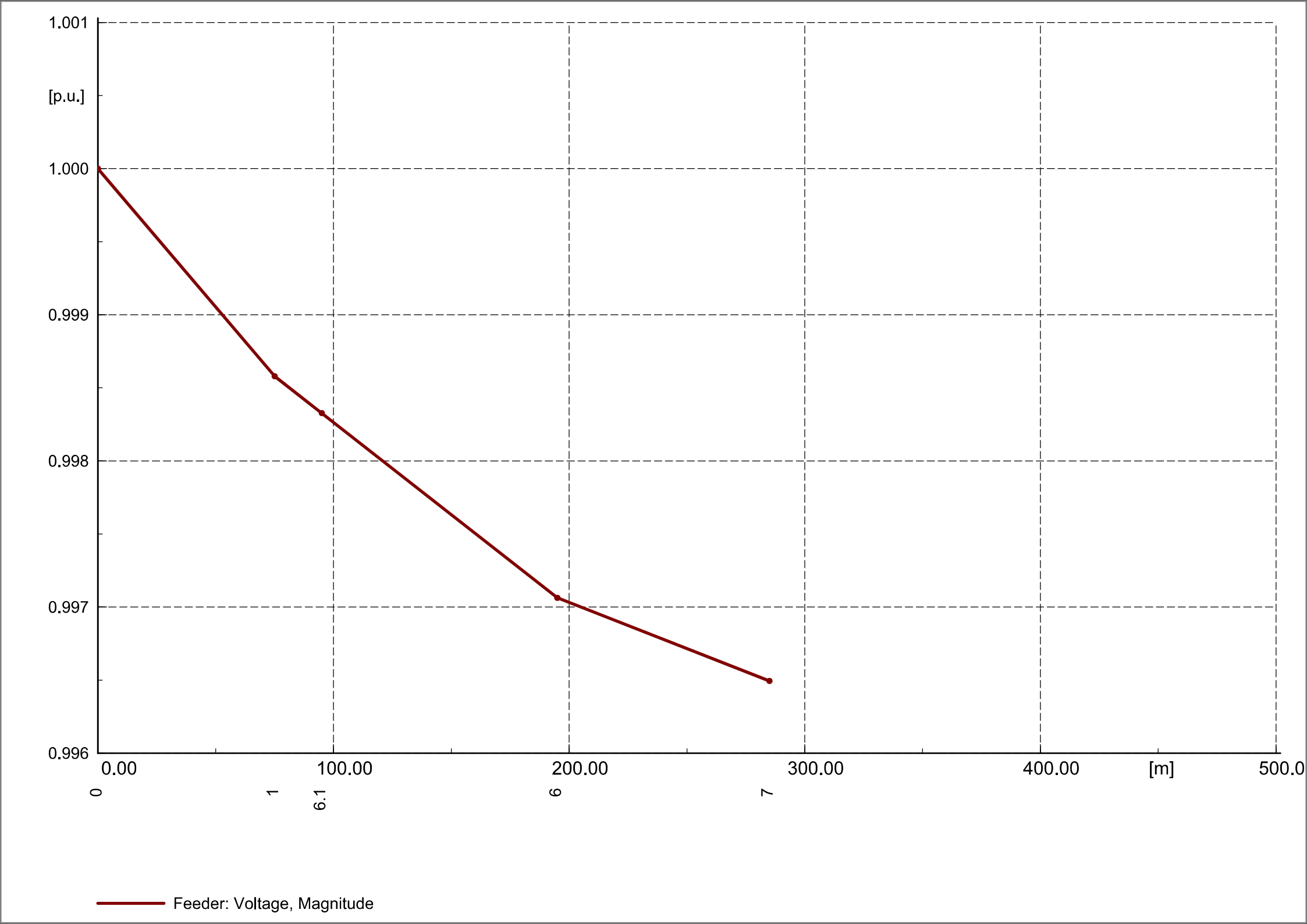

1
[kW]
0.5
0
-0.5
-1
2021-04-24
2021-04-26
WR_4: Active Power

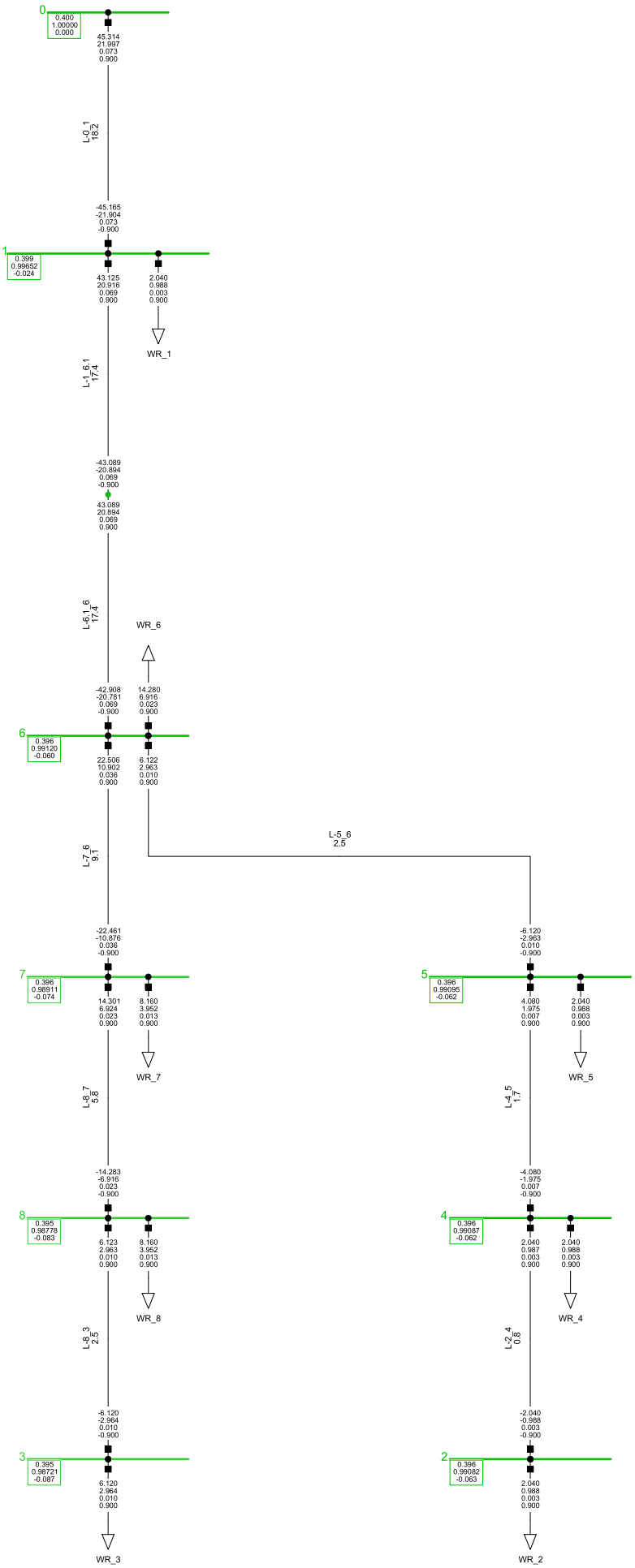

1
[kW]
0.5
0
-0.5
-1
2021-04-24
2021-04-26
WR_5: Active Power

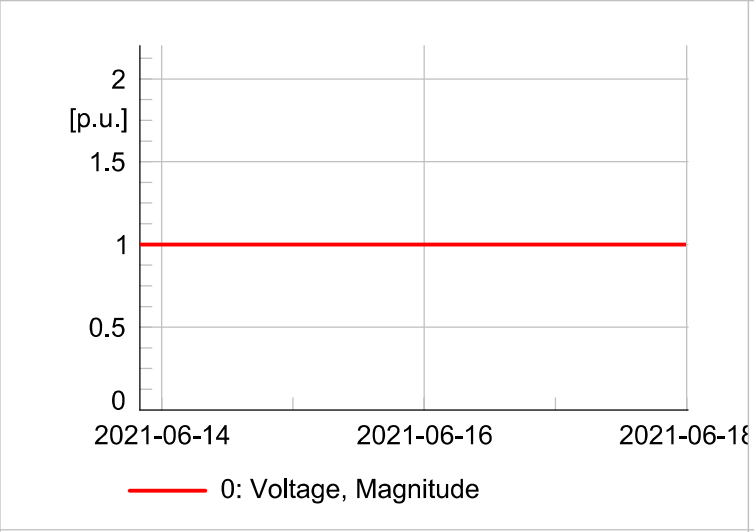

[kW]
6
5
4
3
2
1
2021-04-24
2021-04-26
WR_6: Active Power

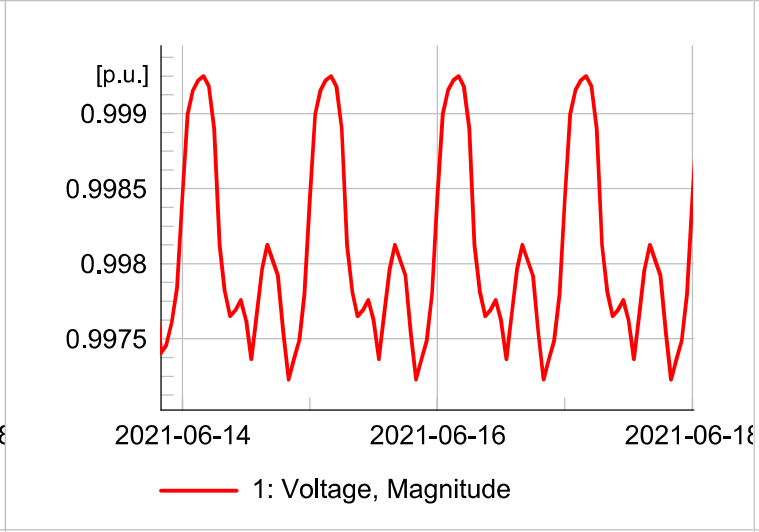

[kW]
6
5
4
3
2
1
2021-04-24
2021-04-26
WR_7: Active Power

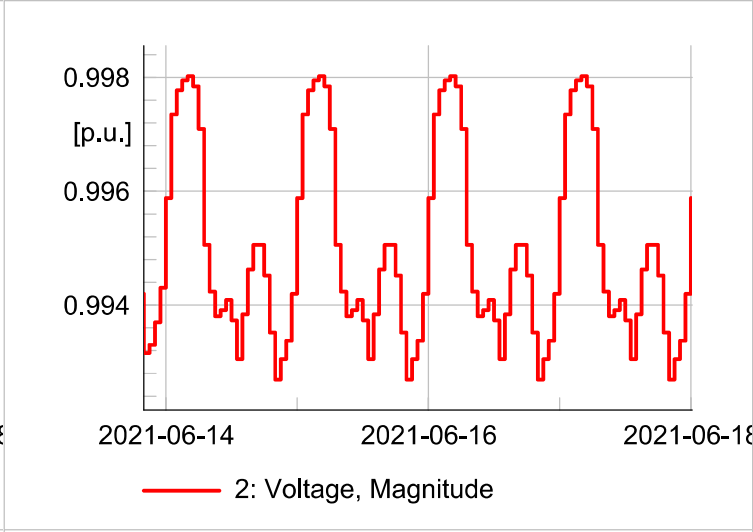

1
[kW]
0.5
0
-0.5
-1
2021-04-24
2021-04-26
WR_8: Active Power

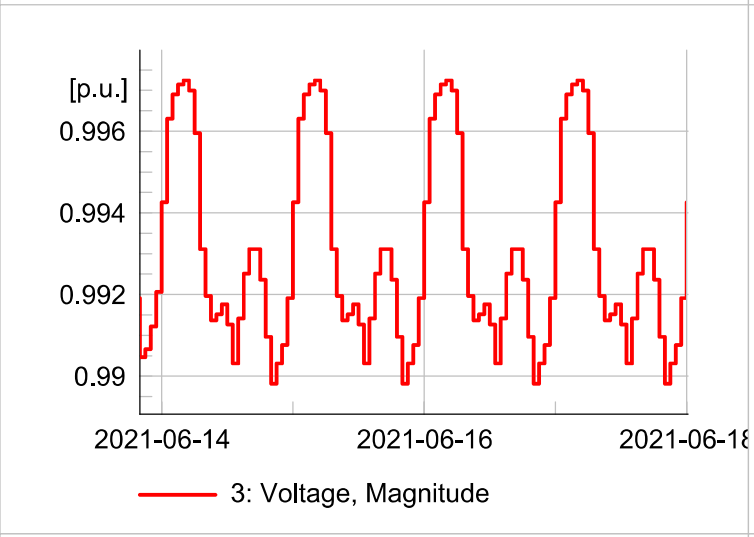

1.001
[p.u.]
1.000
0.999
0.998
0.997
0.996
0.00
100.00
200.00
300.00
400.00
[m]
500.0
0
1
6.1
6
7
Feeder: Voltage, Magnitude

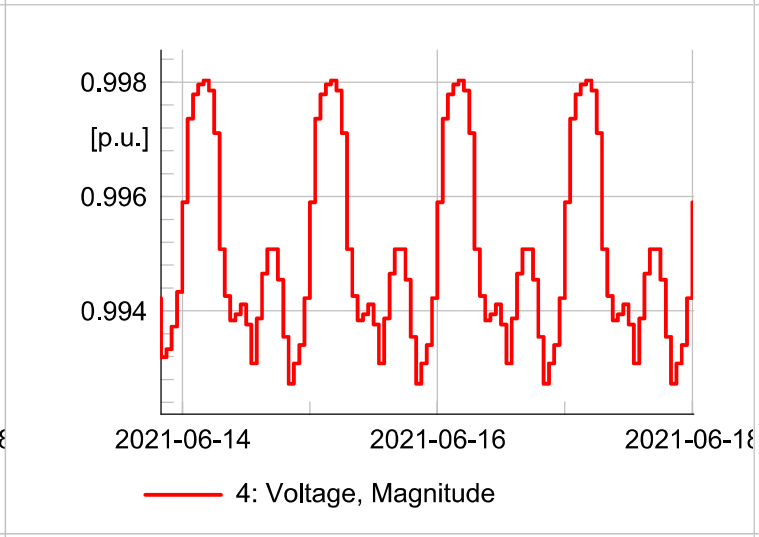

0
0.400
1.00000
0.000
45.314
21.997
0.073
0.900
L-0_1
18.2
-45.165
-21.904
0.073
-0.900
1
0.399
0.99652
-0.024
43.125
20.916
0.069
0.900
2.040
0.988
0.003
0.900
WR_1
L-1_6.1
17.4
-43.089
-20.894
0.069
-0.900
43.089
20.894
0.069
0.900
L-6.1_6
17.4
WR_6
-42.908
-20.781
0.069
-0.900
14.280
6.916
0.023
0.900
6
0.396
0.99120
-0.060
22.506
10.902
0.036
0.900
6.122
2.963
0.010
0.900
L-5_6
2.5
L-7_6
9.1
-22.461
-10.876
0.036
-0.900
-6.120
-2.963
0.010
-0.900
7
0.396
0.98911
-0.074
5
0.396
0.99095
-0.062
14.301
6.924
0.023
0.900
8.160
3.952
0.013
0.900
4.080
1.975
0.007
0.900
2.040
0.988
0.003
0.900
WR_7
WR_5
L-8_7
5.8
L-4_5
1.7
-14.283
-6.916
0.023
-0.900
-4.080
-1.975
0.007
-0.900
8
0.395
0.98778
-0.083
4
0.396
0.99087
-0.062
6.123
2.963
0.010
0.900
8.160
3.952
0.013
0.900
2.040
0.987
0.003
0.900
2.040
0.988
0.003
0.900
WR_8
WR_4
L-8_3
2.5
L-2_4
0.8
-6.120
-2.964
0.010
-0.900
-2.040
-0.988
0.003
-0.900
3
0.395
0.98721
-0.087
2
0.396
0.99082
-0.063
6.120
2.964
0.010
0.900
2.040
0.988
0.003
0.900
WR_3
WR_2

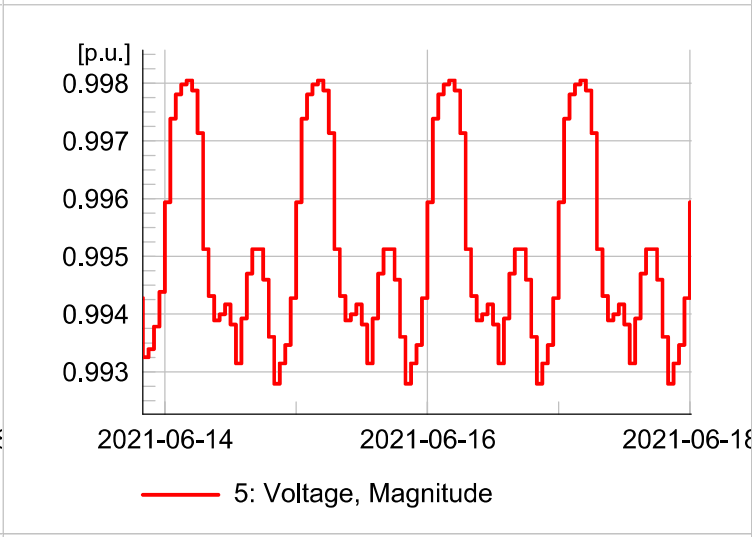

2
[p.u.]
1.5
1
0.5
0
2021-06-14
2021-06-16
2021-06-18
0: Voltage, Magnitude

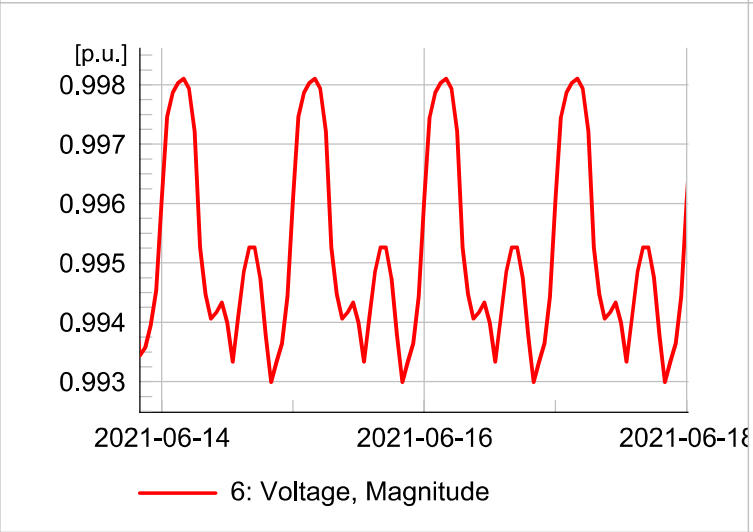

[p.u.]
0.999
0.9985
0.998
0.9975
2021-06-14
2021-06-16
2021-06-18
1: Voltage, Magnitude

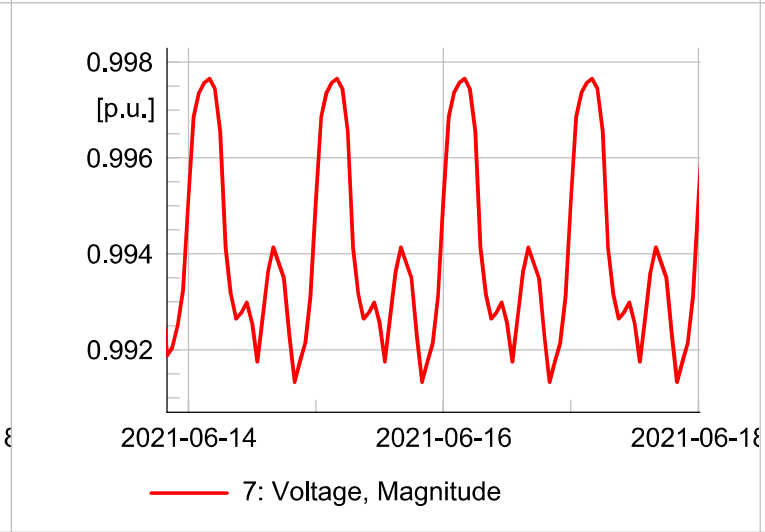

0.998
[p.u.]
0.996
0.994
2021-06-14
2021-06-16
2021-06-18
2: Voltage, Magnitude

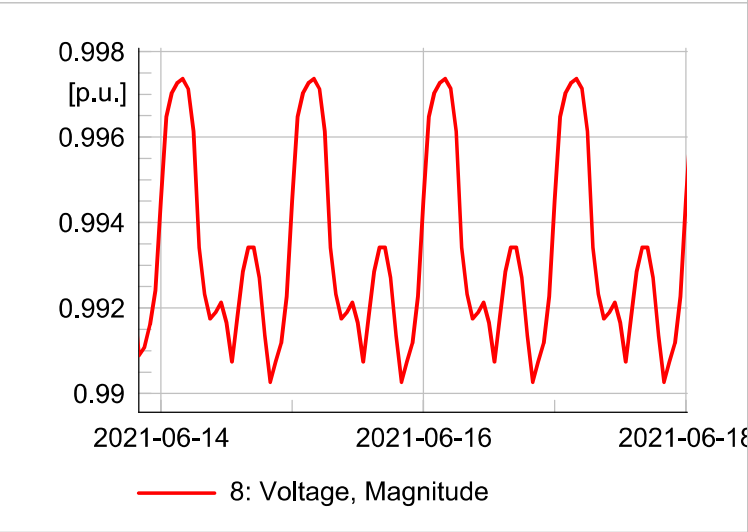

[p.u.]
0.996
0.994
0.992
0.99
2021-06-14
2021-06-16
2021-06-18
3: Voltage, Magnitude

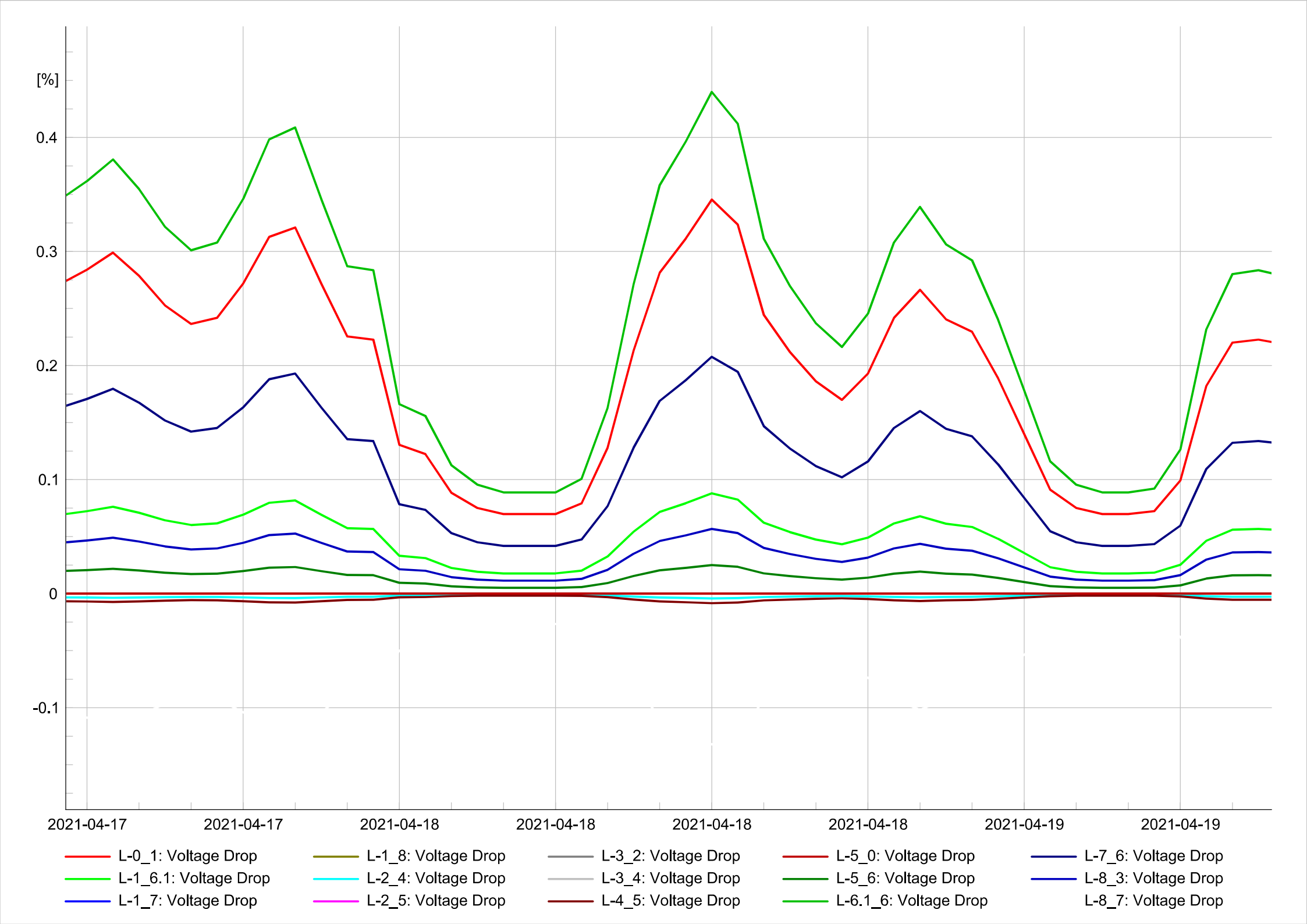

0.998
[p.u.]
0.996
0.994
2021-06-14
2021-06-16
2021-06-18
4: Voltage, Magnitude

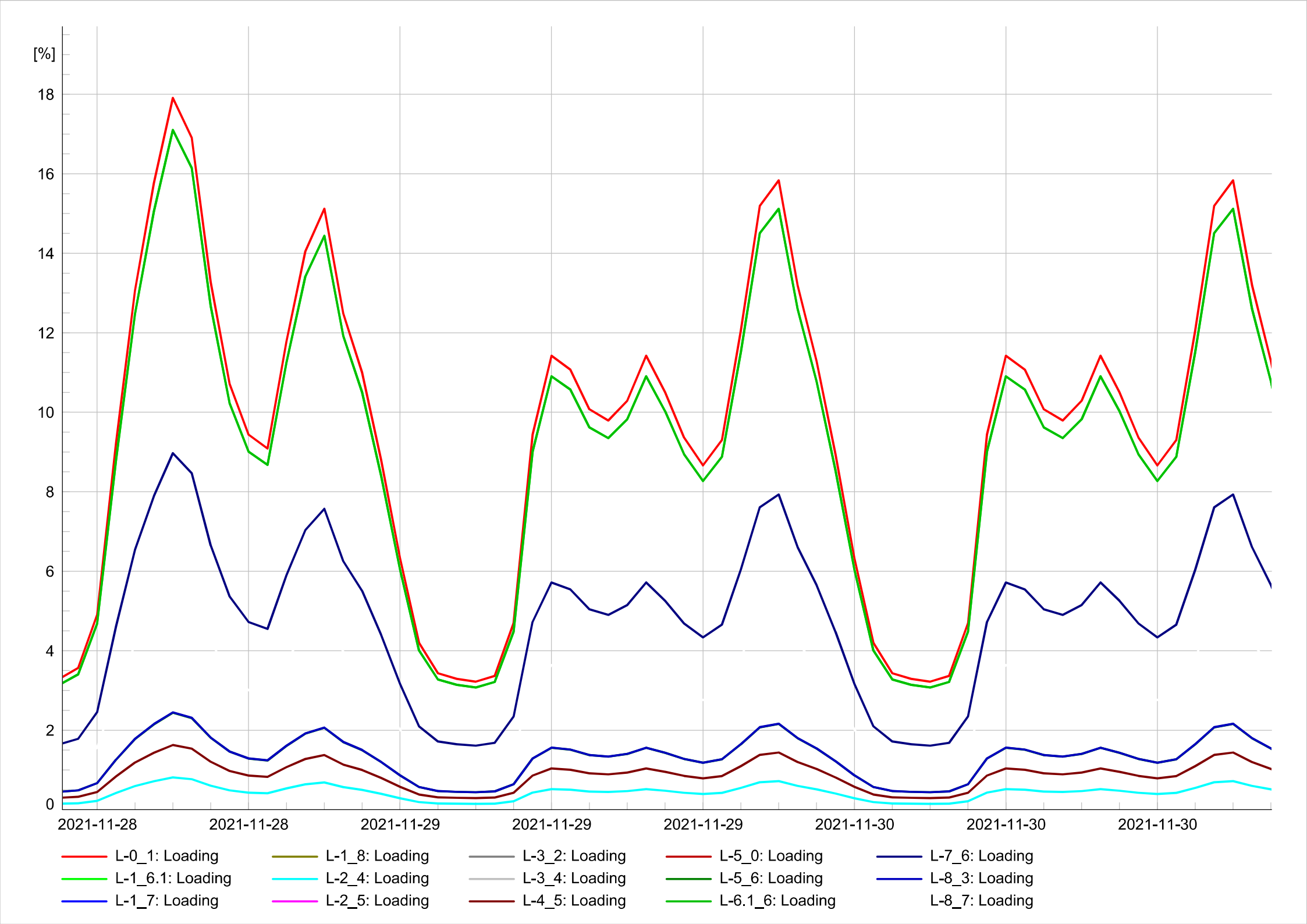

[p.u.]
0.998
0.997
0.996
0.995
0.994
0.993
2021-06-14
2021-06-16
2021-06-18
5: Voltage, Magnitude

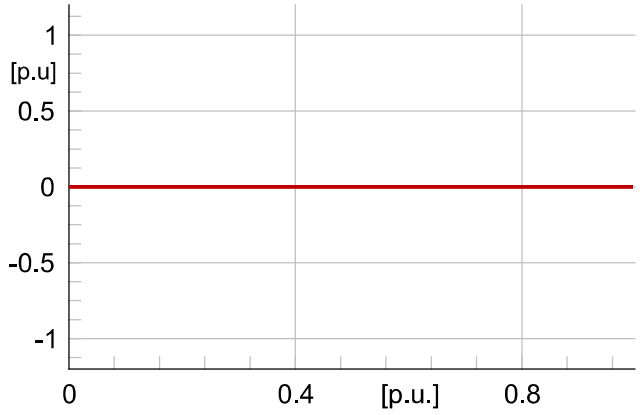

[p.u.]
0.998
0.997
0.996
0.995
0.994
0.993
2021-06-14
2021-06-16
2021-06-18
6: Voltage, Magnitude


0.998
[p.u.]
0.996
0.994
0.992
2021-06-14
2021-06-16
2021-06-18
7: Voltage, Magnitude

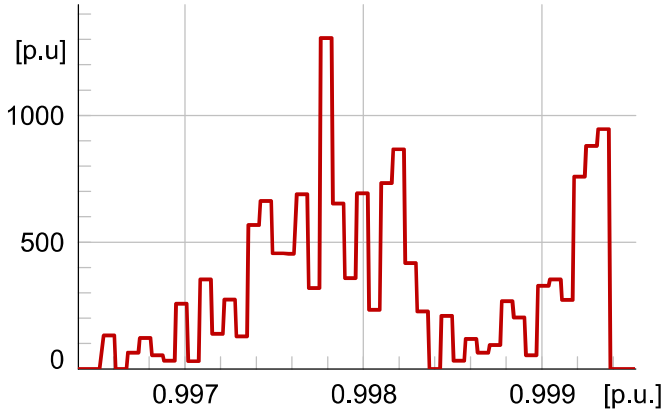

0.998
[p.u.]
0.996
0.994
0.992
0.99
2021-06-14
2021-06-16
2021-06-18
8: Voltage, Magnitude


[%]
0.4
0.3
0.2
0.1
0
-0.1
2021-04-17
2021-04-17
2021-04-18
2021-04-18
2021-04-18
2021-04-18
2021-04-19
2021-04-19
L-0_1: Voltage Drop
L-1_6.1: Voltage Drop
L-1_7: Voltage Drop
L-1_8: Voltage Drop
L-2_4: Voltage Drop
L-2_5: Voltage Drop
L-3_2: Voltage Drop
L-3_4: Voltage Drop
L-4_5: Voltage Drop
L-5_0: Voltage Drop
L-5_6: Voltage Drop
L-6.1_6: Voltage Drop
L-7_6: Voltage Drop
L-8_3: Voltage Drop
L-8_7: Voltage Drop

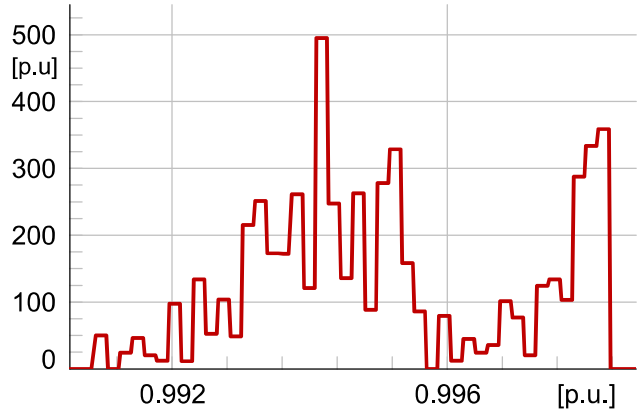

[%]
18
16
14
12
10
8
6
4
2
0
2021-11-28
2021-11-28
2021-11-29
2021-11-29
2021-11-29
2021-11-30
2021-11-30
2021-11-30
L-0_1: Loading
L-1_6.1: Loading
L-1_7: Loading
L-1_8: Loading
L-2_4: Loading
L-2_5: Loading
L-3_2: Loading
L-3_4: Loading
L-4_5: Loading
L-5_0: Loading
L-5_6: Loading
L-6.1_6: Loading
L-7_6: Loading
L-8_3: Loading
L-8_7: Loading



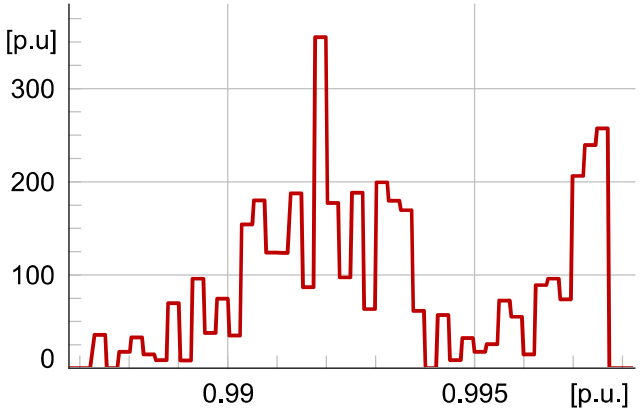
0: u, Magnitude, Histogram, auto., ...



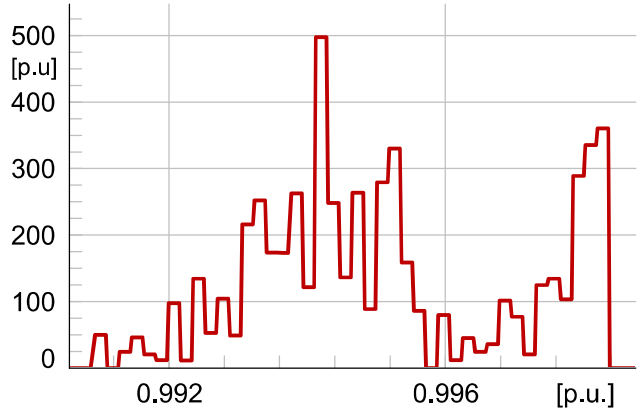
1: u, Magnitude, Histogram, auto., ...



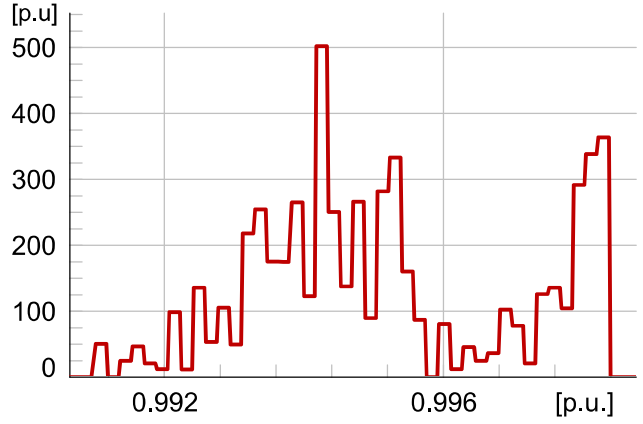
2: u, Magnitude, Histogram, auto., ...



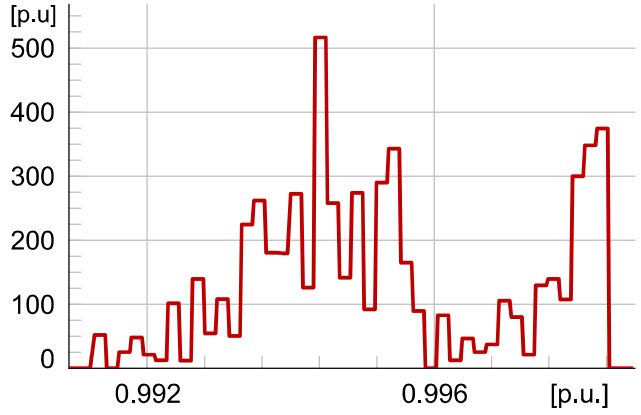
3: u, Magnitude, Histogram, auto., ...



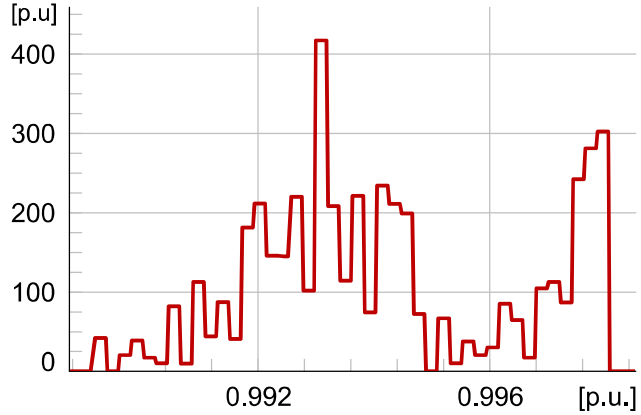
4: u, Magnitude, Histogram, auto., ...



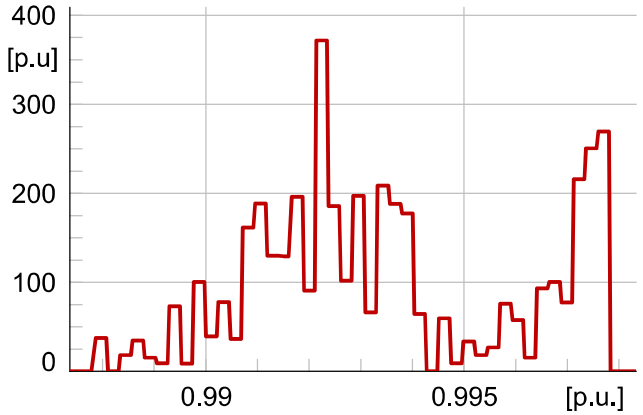
5: u, Magnitude, Histogram, auto., ...



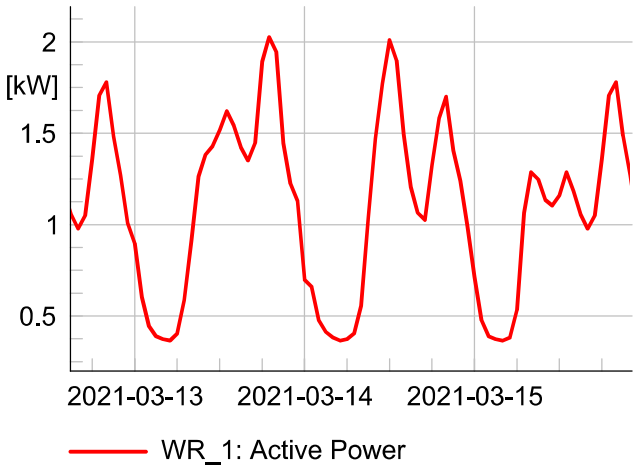
6: u, Magnitude, Histogram, auto., ...

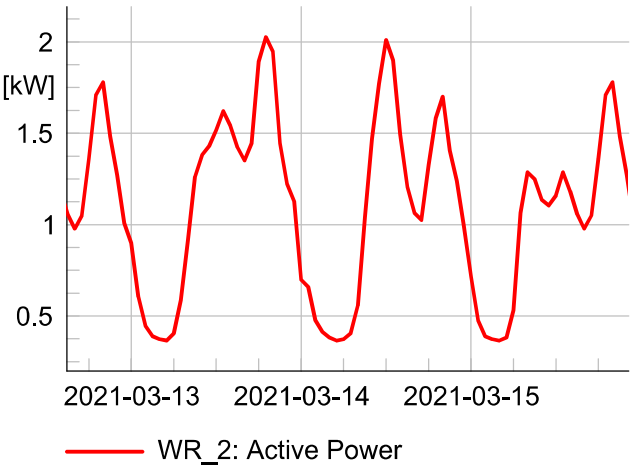


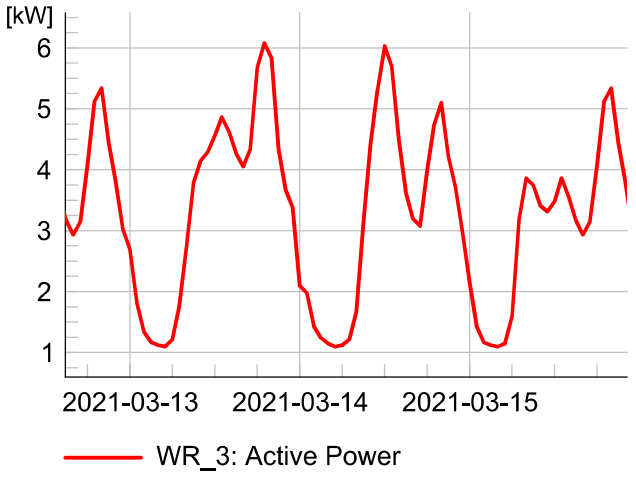
7: u, Magnitude, Histogram, auto., ...

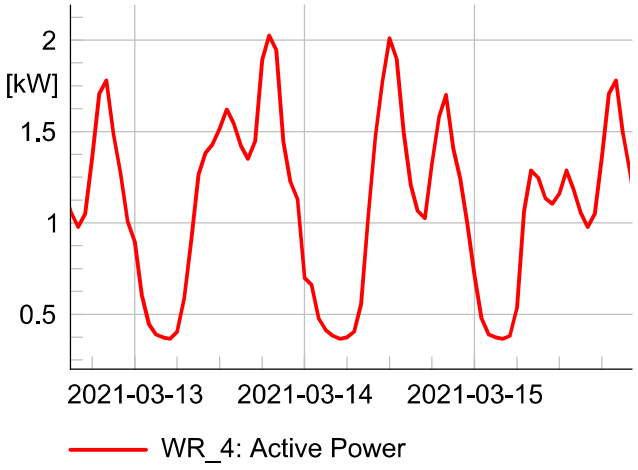


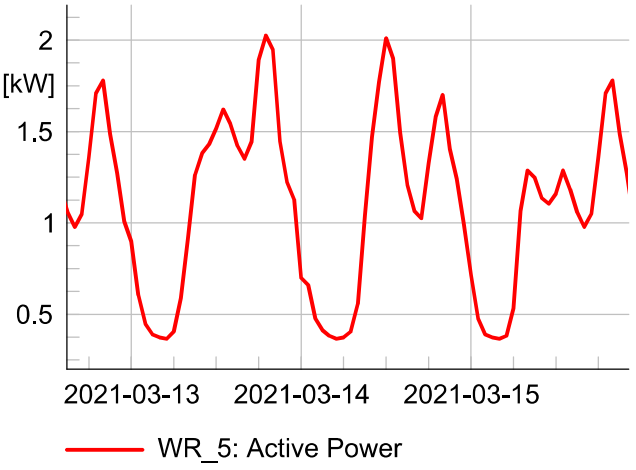
8: u, Magnitude, Histogram, auto., ...

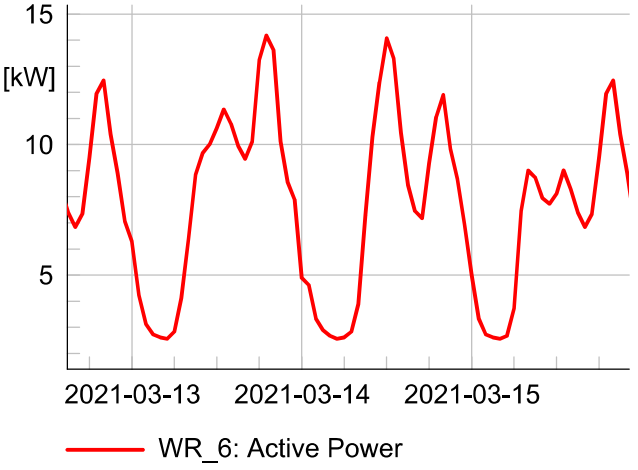

2
[kW]
1.5
1
0.5
2021-03-13
2021-03-14
2021-03-15
WR_1: Active Power

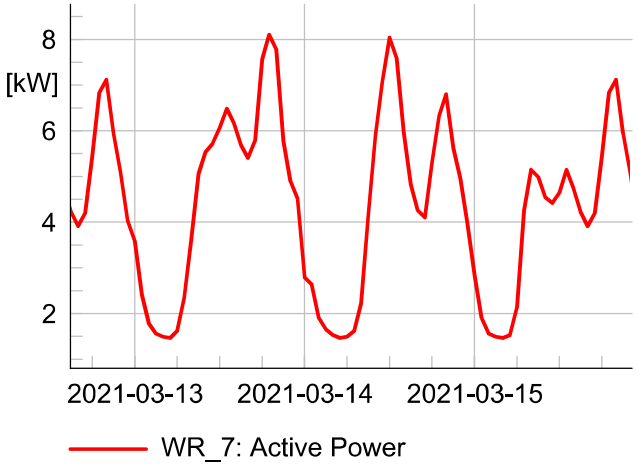

2
[kW]
1.5
1
0.5
2021-03-13
2021-03-14
2021-03-15
WR_2: Active Power

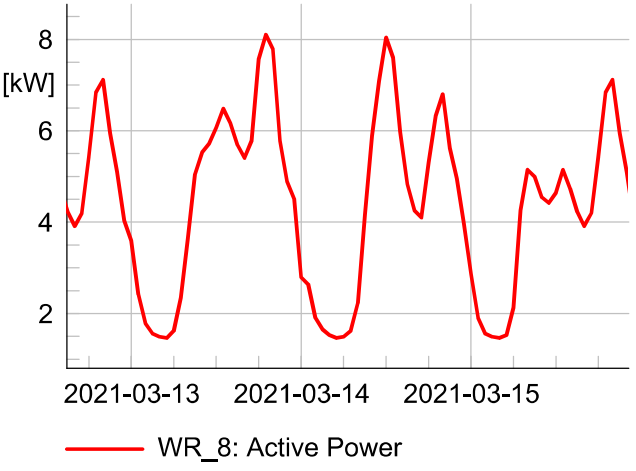

[kW]
6
5
4
3
2
1
2021-03-13
2021-03-14
2021-03-15
WR_3: Active Power

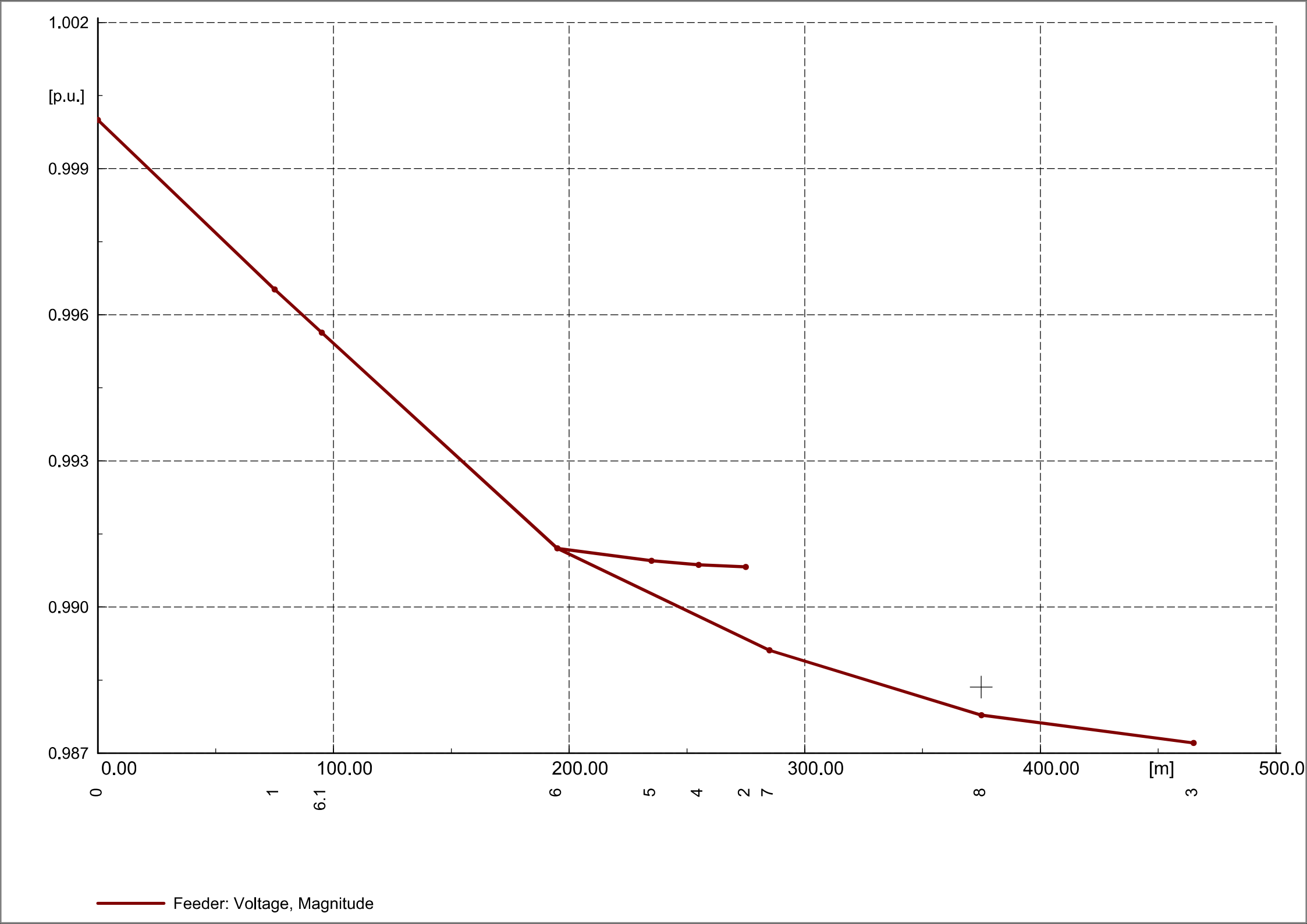

2
[kW]
1.5
1
0.5
2021-03-13
2021-03-14
2021-03-15
WR_4: Active Power

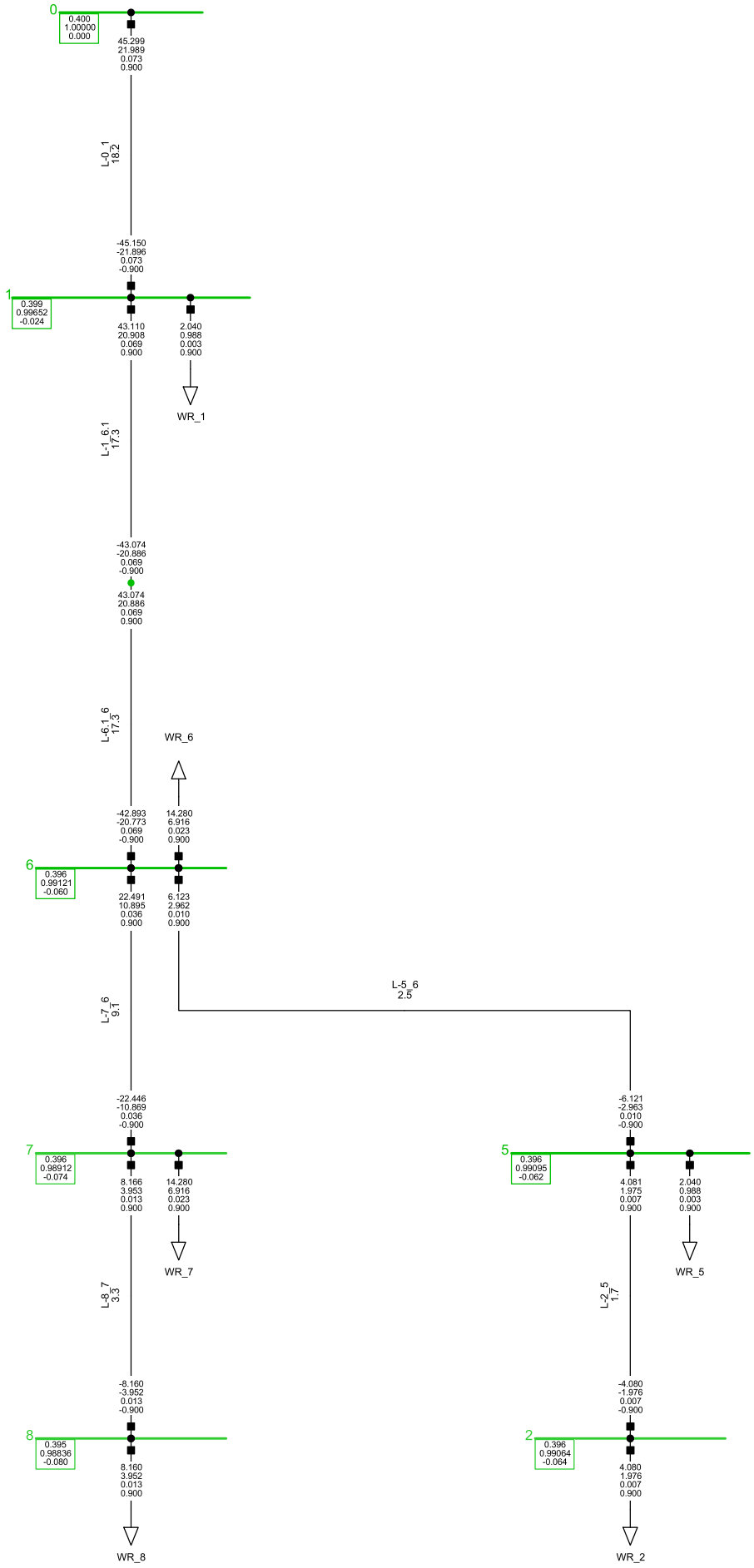

2
[kW]
1.5
1
0.5
2021-03-13
2021-03-14
2021-03-15
WR_5: Active Power

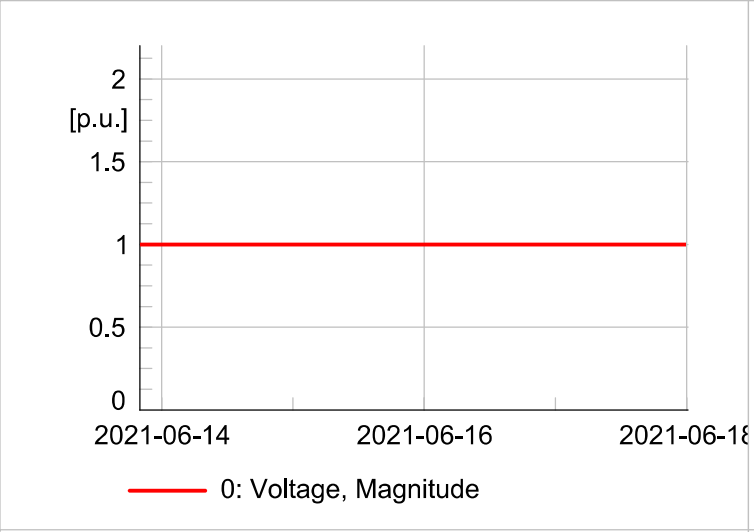

15
[kW]
10
5
2021-03-13
2021-03-14
2021-03-15
WR_6: Active Power

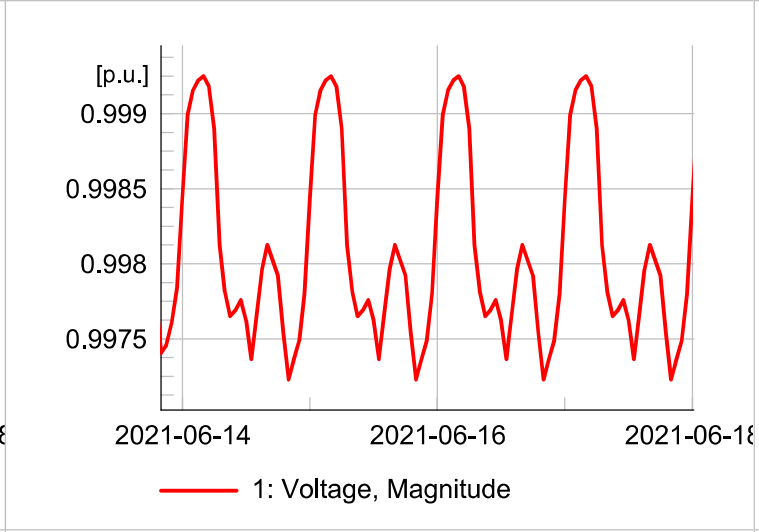

8
[kW]
6
4
2
2021-03-13
2021-03-14
2021-03-15
WR_7: Active Power

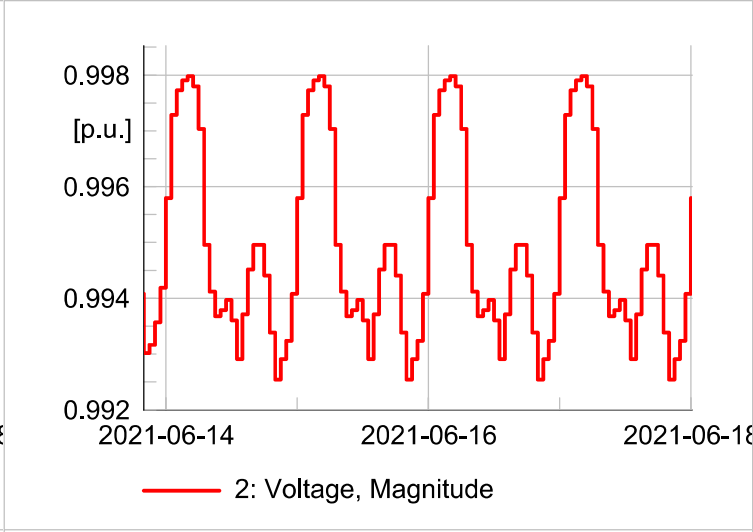

8
[kW]
6
4
2
2021-03-13
2021-03-14
2021-03-15
WR_8: Active Power

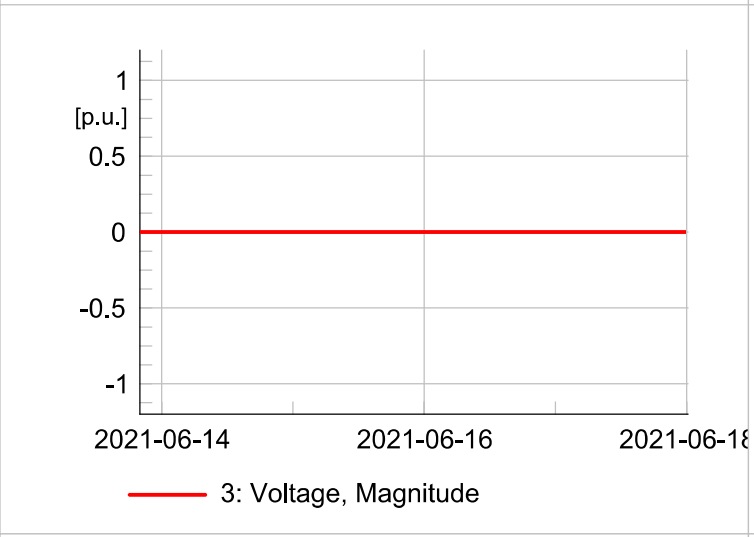

1.002
[p.u.]
0.999
0.996
0.993
0.990
0.987
0.00
100.00
200.00
300.00
400.00
[m]
500.0
0
1
6.1
6
5
4
2
7
8
3
Feeder: Voltage, Magnitude

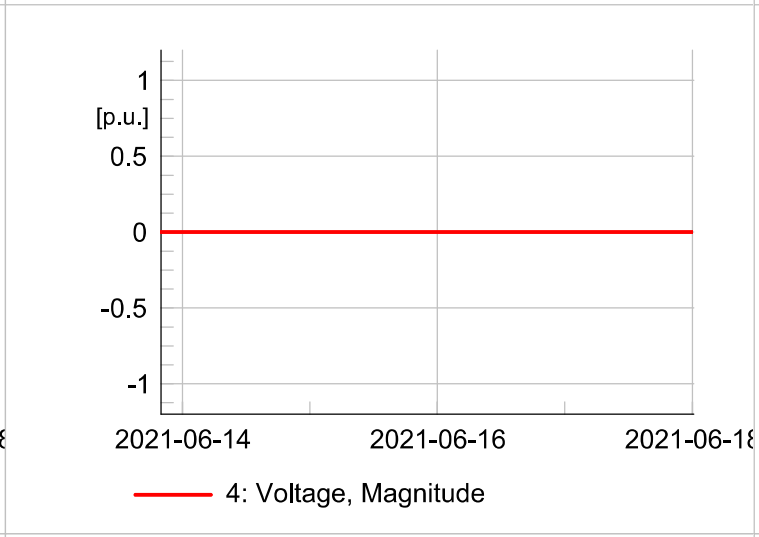

0
0.400
1.00000
0.000
45.299
21.989
0.073
0.900
L-0_1
18.2
-45.150
-21.896
0.073
-0.900
1
0.399
0.99652
-0.024
43.110
20.908
0.069
0.900
2.040
0.988
0.003
0.900
WR_1
L-1_6_1
17.3
-43.074
-20.886
0.069
-0.900
43.074
20.886
0.069
0.900
L-6_1_6
17.3
WR_6
-42.893
-20.773
0.069
-0.900
14.280
6.916
0.023
0.900
6
0.396
0.99121
-0.060
22.491
10.895
0.036
0.900
6.123
2.962
0.010
0.900
L-5_6
2.5
L-7_6
9.1
-22.446
-10.869
0.036
-0.900
-6.121
-2.963
0.010
-0.900
7
0.396
0.98912
-0.074
5
0.396
0.99095
-0.062
8.166
3.953
0.013
0.900
14.280
6.916
0.023
0.900
4.081
1.975
0.007
0.900
2.040
0.988
0.003
0.900
WR_7
WR_5
L-8_7
3.3
L-2_5
1.7
-8.160
-3.952
0.013
-0.900
-4.080
-1.976
0.007
-0.900
8
0.395
0.98836
-0.080
2
0.396
0.99064
-0.064
8.160
3.952
0.013
0.900
4.080
1.976
0.007
0.900
WR_8
WR_2

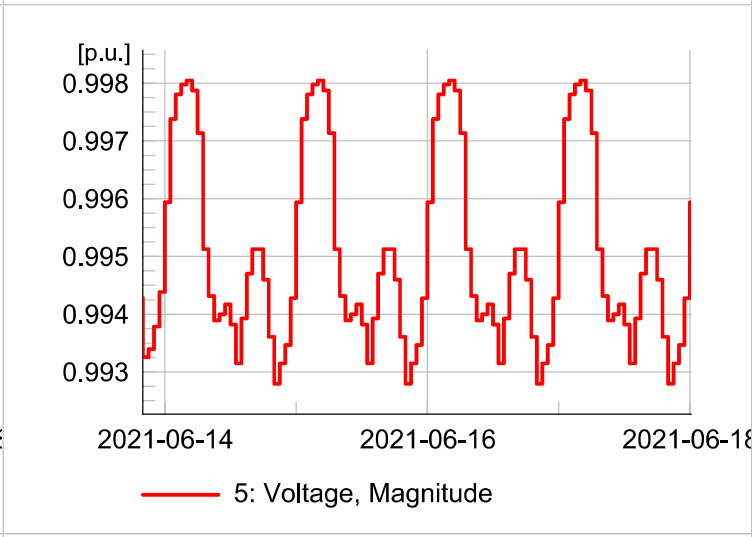

2
[p.u.]
1.5
1
0.5
0
2021-06-14
2021-06-16
2021-06-18
0: Voltage, Magnitude

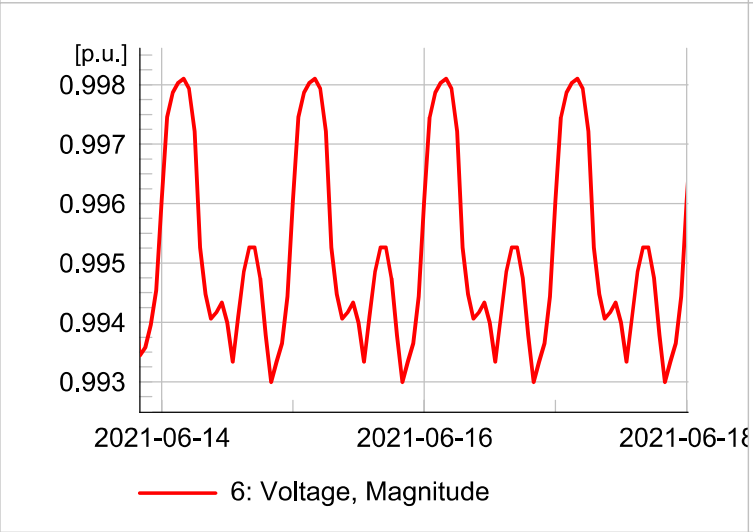

[p.u.]
0.999
0.9985
0.998
0.9975
2021-06-14
2021-06-16
2021-06-18
1: Voltage, Magnitude

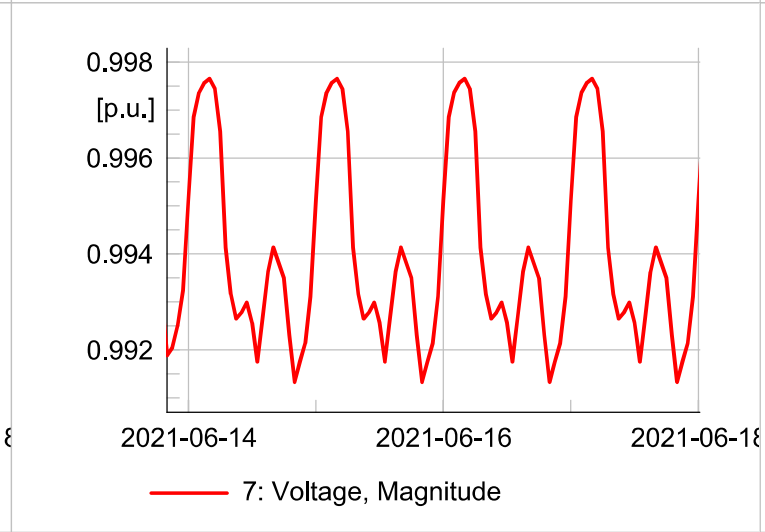

0.998
[p.u.]
0.996
0.994
0.992
2021-06-14
2021-06-16
2021-06-18
2: Voltage, Magnitude

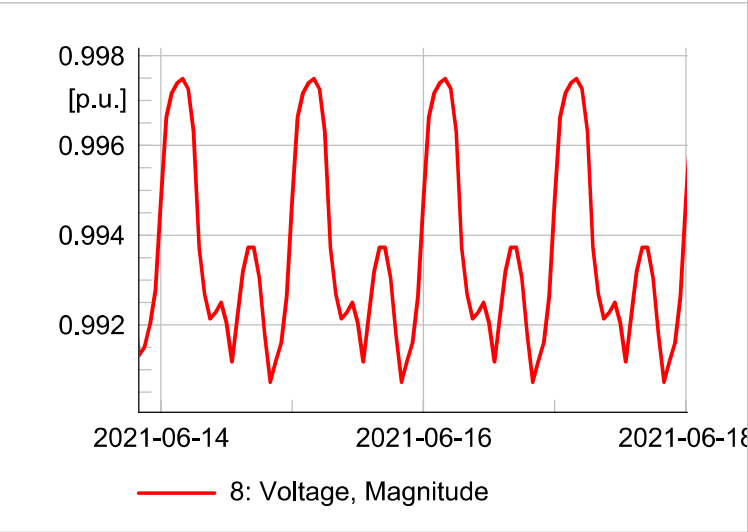

1
[p.u.]
0.5
0
-0.5
-1
2021-06-14
2021-06-16
2021-06-18
3: Voltage, Magnitude

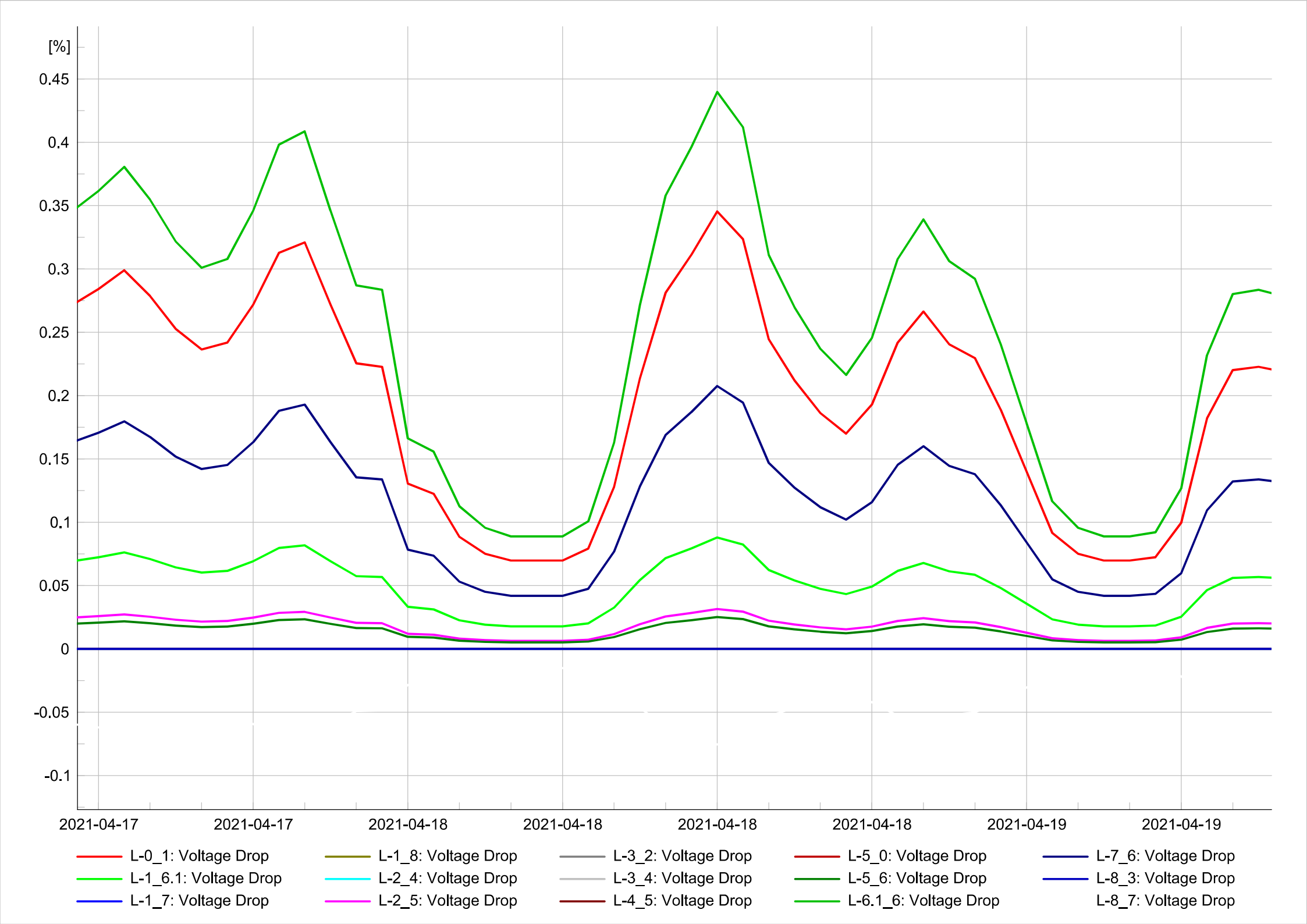

1
[p.u.]
0.5
0
-0.5
-1
2021-06-14
2021-06-16
2021-06-18
4: Voltage, Magnitude

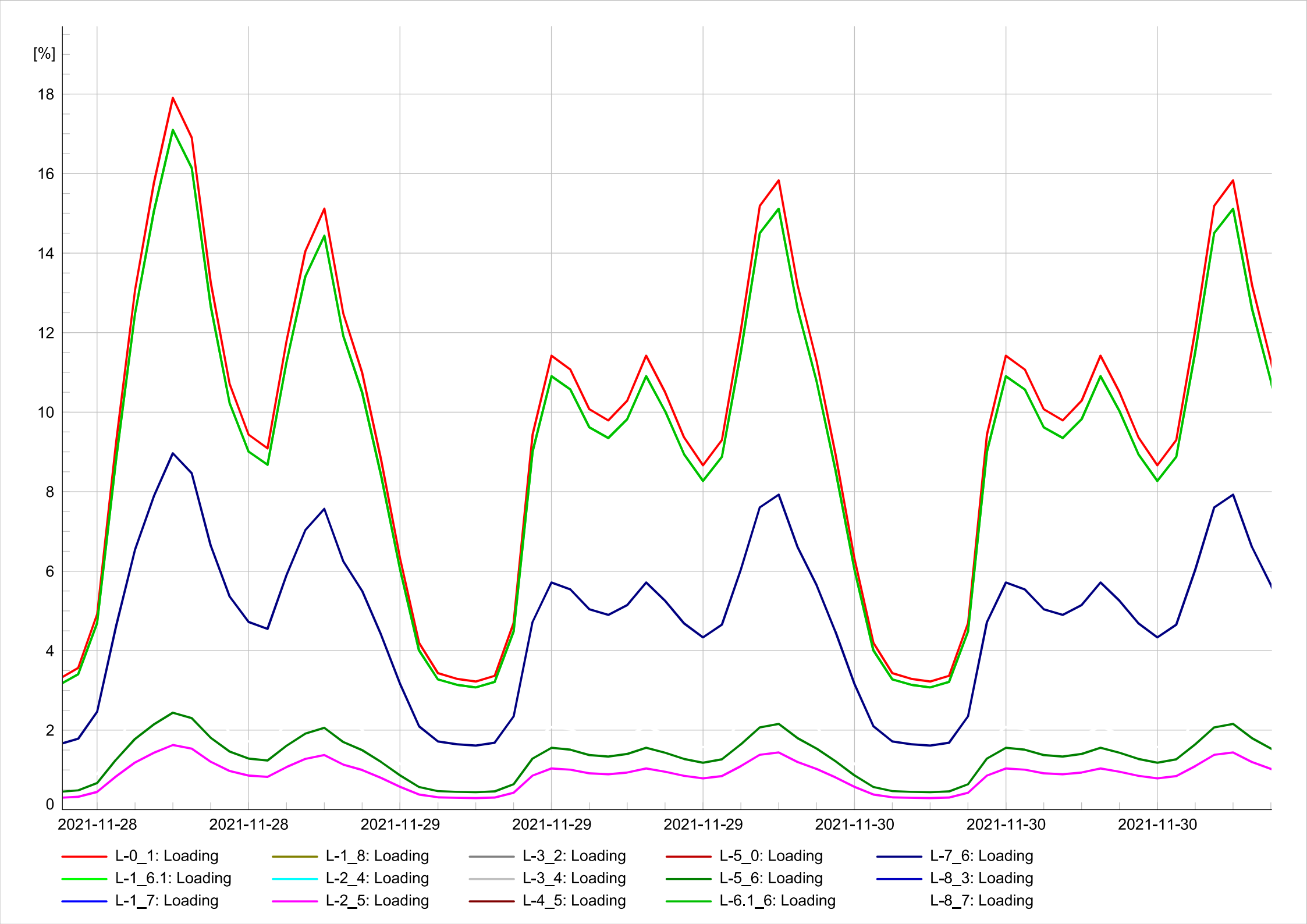

[p.u.]
0.998
0.997
0.996
0.995
0.994
0.993
2021-06-14
2021-06-16
2021-06-18
5: Voltage, Magnitude

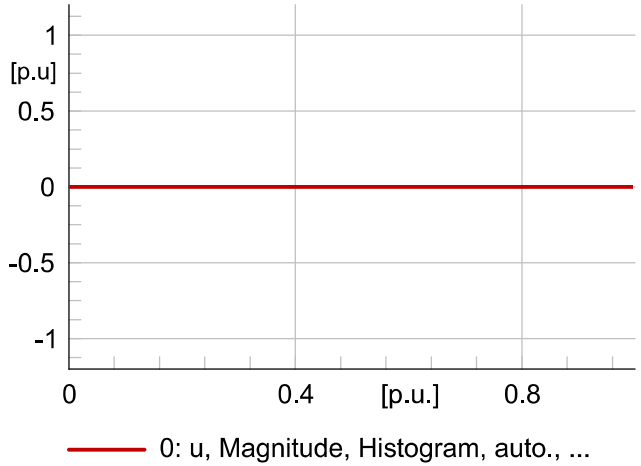

[p.u.]
0.998
0.997
0.996
0.995
0.994
0.993
2021-06-14
2021-06-16
2021-06-18
6: Voltage, Magnitude

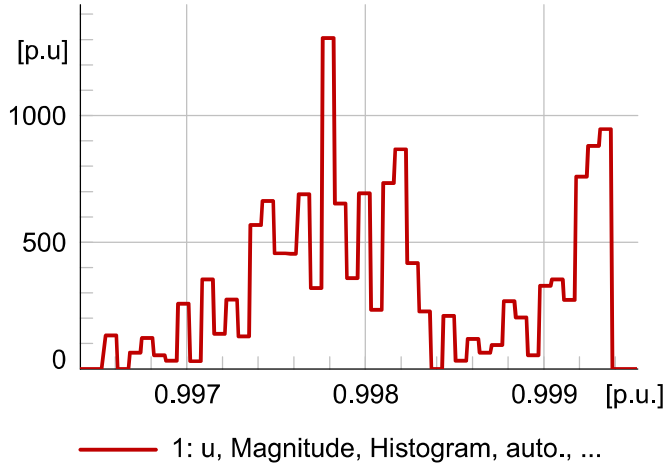

0.998
[p.u.]
0.996
0.994
0.992
2021-06-14
2021-06-16
2021-06-18
7: Voltage, Magnitude

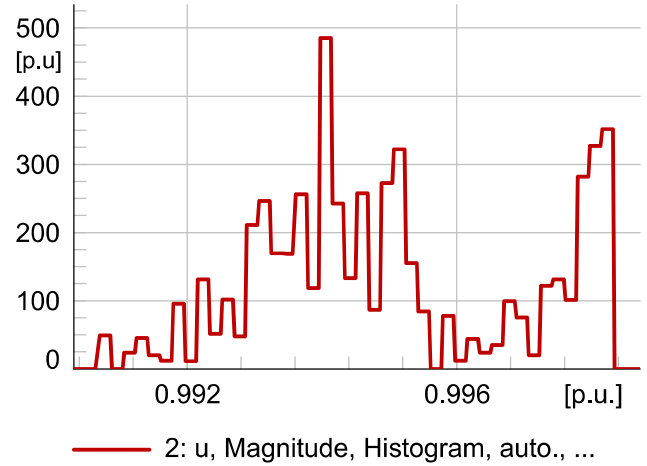

0.998
[p.u.]
0.996
0.994
0.992
2021-06-14
2021-06-16
2021-06-18
8: Voltage, Magnitude

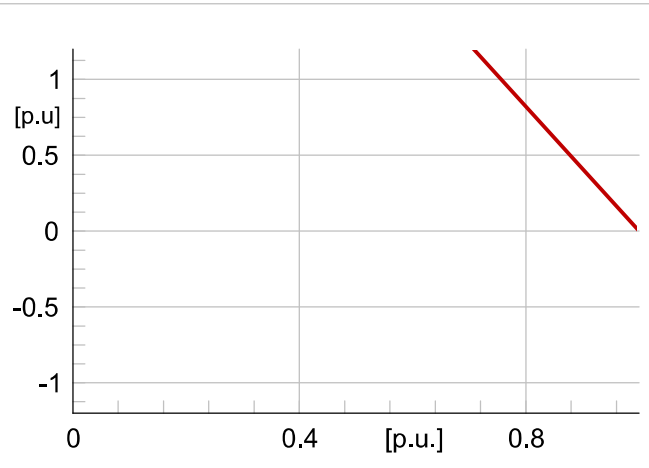

[%]
0.45
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
-0.05
-0.1
2021-04-17
2021-04-17
2021-04-18
2021-04-18
2021-04-18
2021-04-18
2021-04-19
2021-04-19
L-0_1: Voltage Drop
L-1_8: Voltage Drop
L-3_2: Voltage Drop
L-5_0: Voltage Drop
L-7_6: Voltage Drop
L-1_6.1: Voltage Drop
L-2_4: Voltage Drop
L-3_4: Voltage Drop
L-5_6: Voltage Drop
L-8_3: Voltage Drop
L-1_7: Voltage Drop
L-2_5: Voltage Drop
L-4_5: Voltage Drop
L-6.1_6: Voltage Drop
L-8_7: Voltage Drop

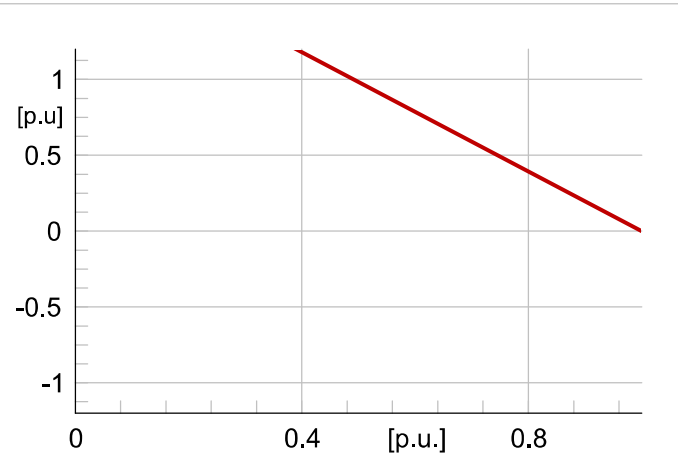

[%]
18
16
14
12
10
8
6
4
2
0
2021-11-28
2021-11-28
2021-11-29
2021-11-29
2021-11-29
2021-11-30
2021-11-30
2021-11-30
L-0_1: Loading
L-1_6.1: Loading
L-1_7: Loading
L-1_8: Loading
L-2_4: Loading
L-2_5: Loading
L-3_2: Loading
L-3_4: Loading
L-4_5: Loading
L-5_0: Loading
L-5_6: Loading
L-6.1_6: Loading
L-7_6: Loading
L-8_3: Loading
L-8_7: Loading

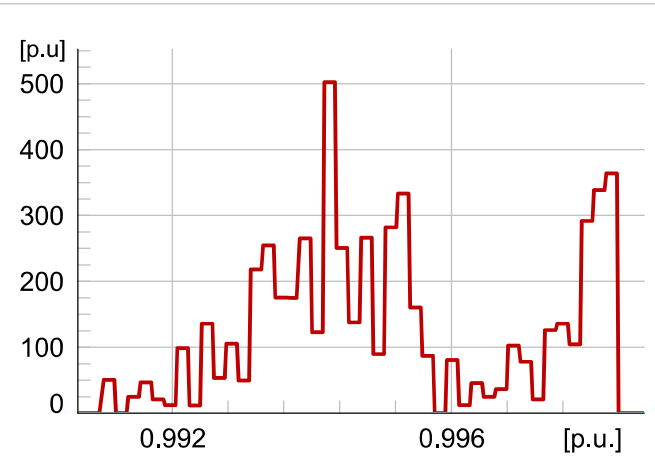

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
0: u, Magnitude, Histogram, auto., ...

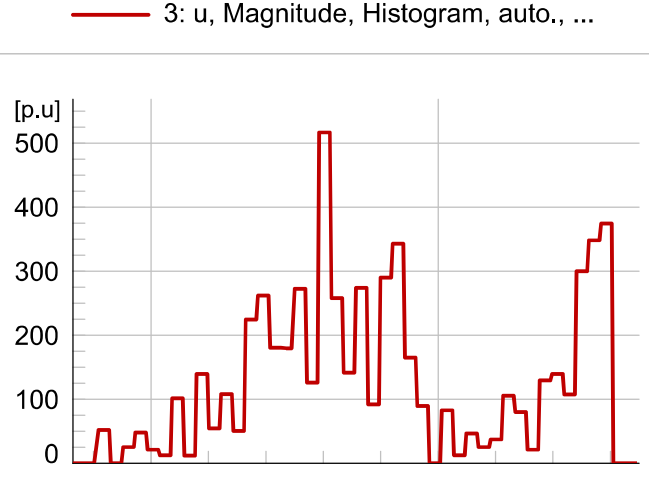

[p.u]
1000
500
0
0.997
0.998
0.999
[p.u.]
1: u, Magnitude, Histogram, auto., ...

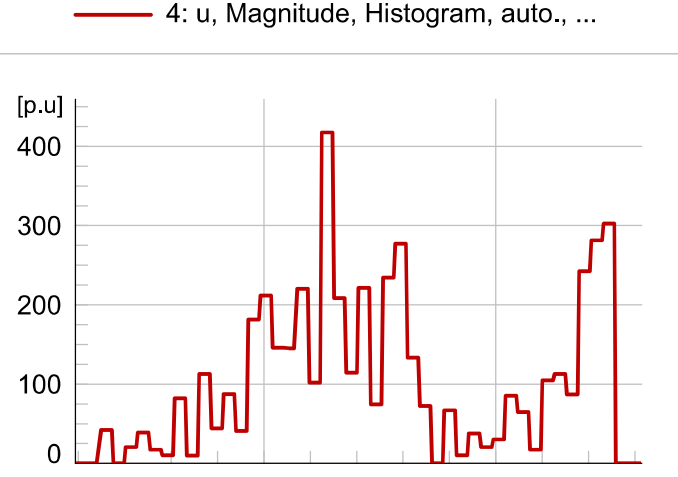

500
[p.u]
400
300
200
100
0
0.992
0.996
[p.u.]
2: u, Magnitude, Histogram, auto., ...

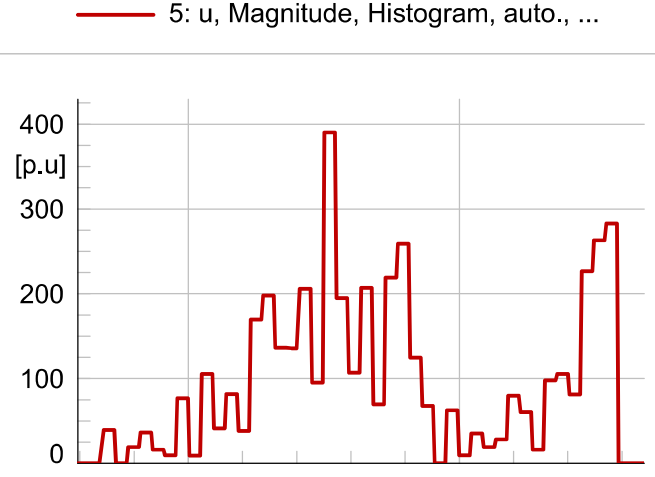

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
3: u, Magnitude, Histogram, auto., ...

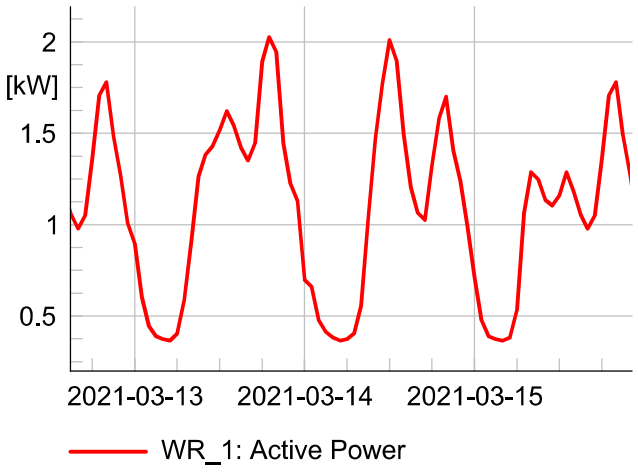

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
4: u, Magnitude, Histogram, auto., ...

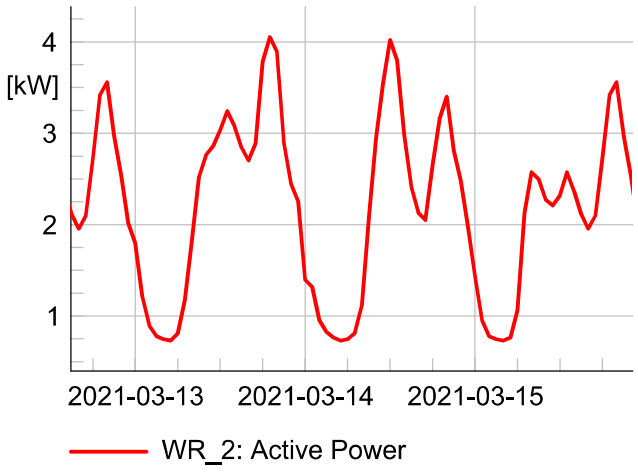

[p.u]
500
400
300
200
100
0
0.992
0.996
[p.u.]
5: u, Magnitude, Histogram, auto., ...

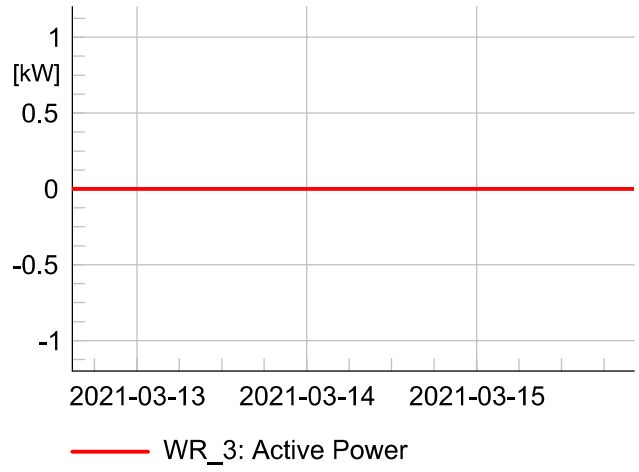

[p.u]
500
400
300
200
100
0
0.992
0.996
[p.u.]
6: u, Magnitude, Histogram, auto., ...

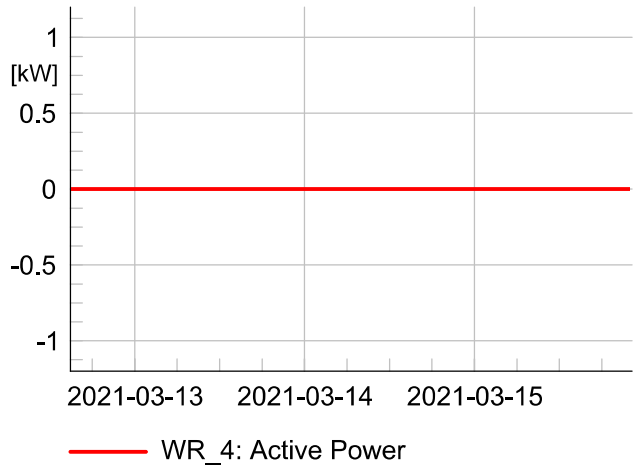

[p.u]
400
300
200
100
0
0.992
0.996
[p.u.]
7: u, Magnitude, Histogram, auto., ...

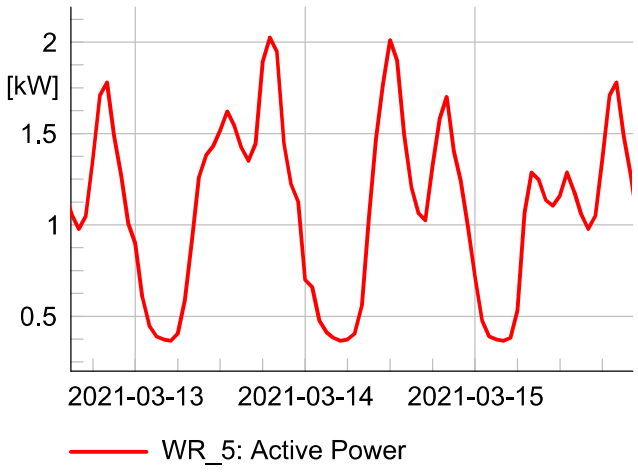

400
[p.u]
300
200
100
0
0.99
0.995
[p.u.]
8: u, Magnitude, Histogram, auto., ...

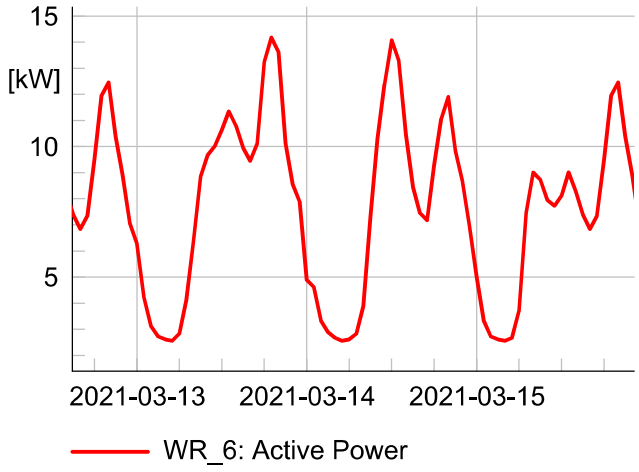

2
[kW]
1.5
1
0.5
2021-03-13
2021-03-14
2021-03-15
WR_1: Active Power

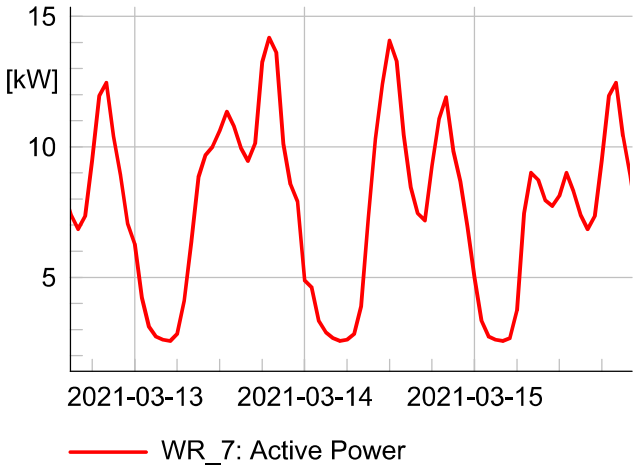

4
[kW]
3
2
1
2021-03-13
2021-03-14
2021-03-15
WR_2: Active Power

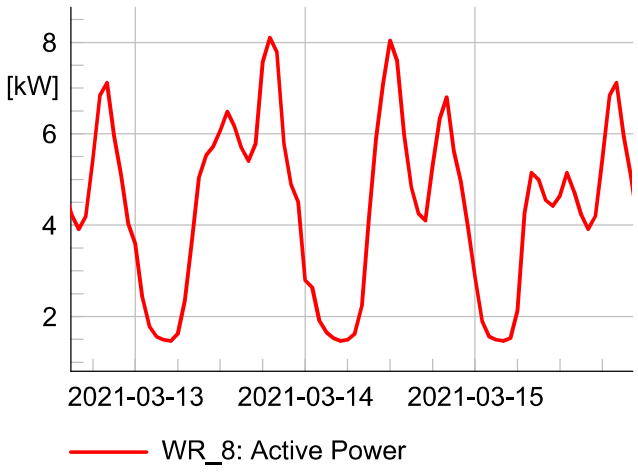

1
[kW]
0.5
0
-0.5
-1
2021-03-13
2021-03-14
2021-03-15
WR_3: Active Power

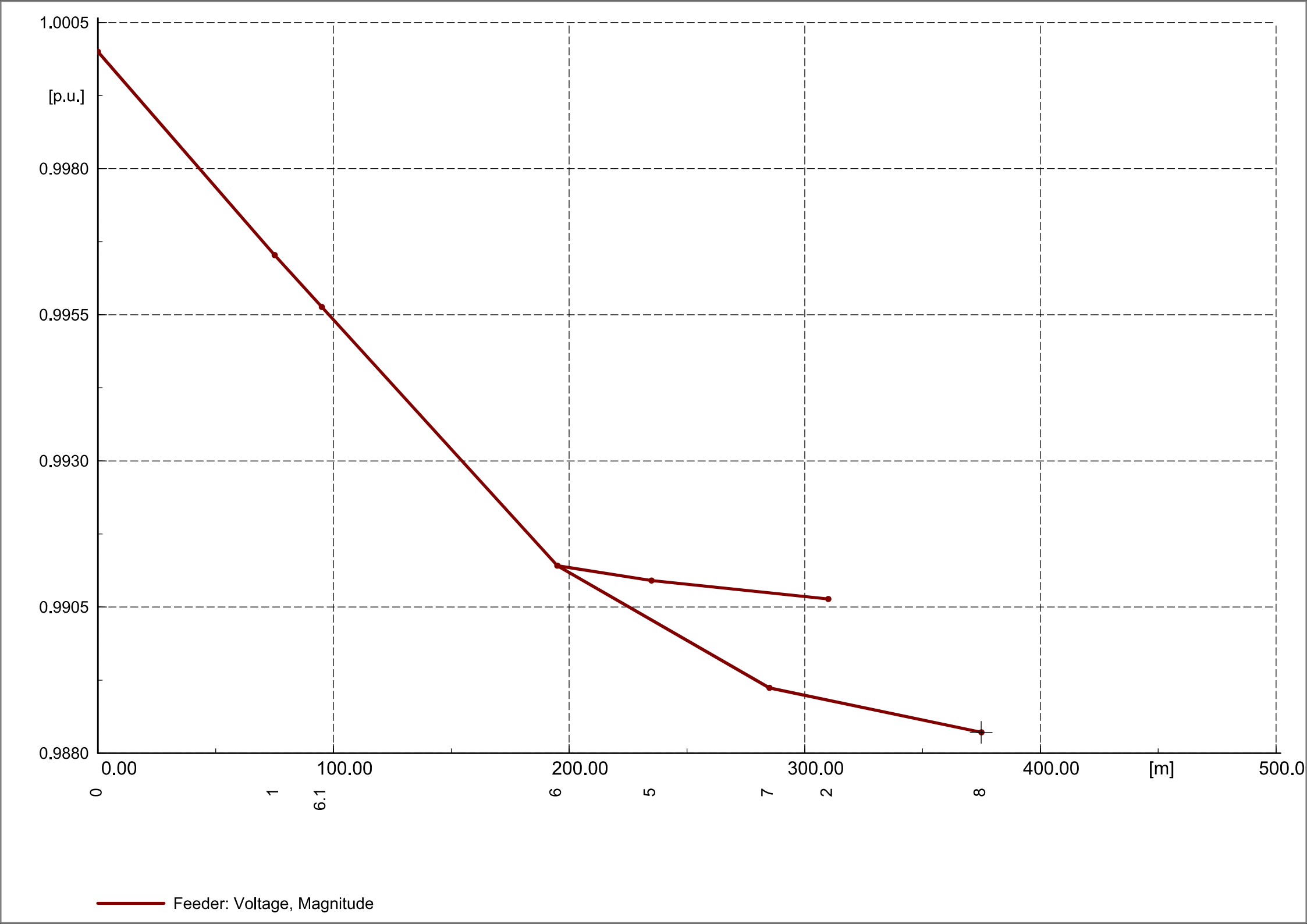

1
[kW]
0.5
0
-0.5
-1
2021-03-13
2021-03-14
2021-03-15
WR_4: Active Power

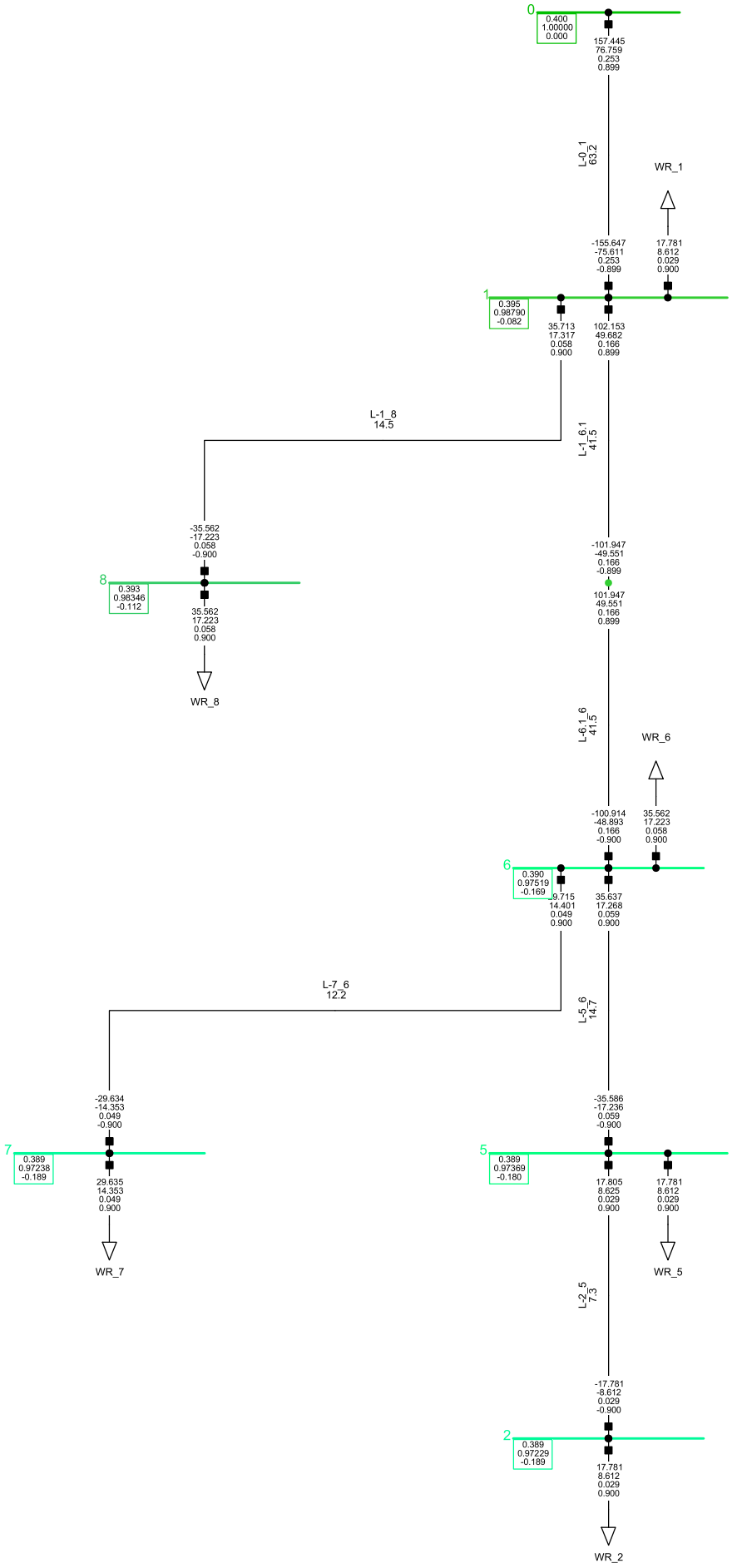

2
[kW]
1.5
1
0.5
2021-03-13
2021-03-14
2021-03-15
WR_5: Active Power

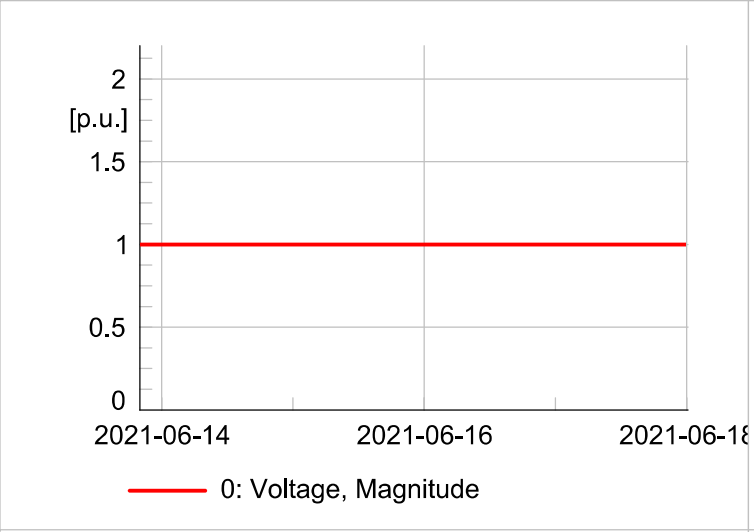

15
[kW]
10
5
2021-03-13
2021-03-14
2021-03-15
WR_6: Active Power

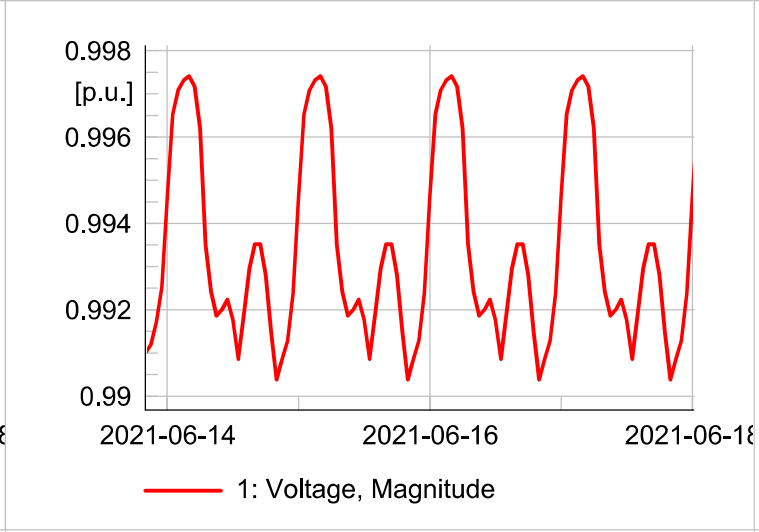

15
[kW]
10
5
2021-03-13
2021-03-14
2021-03-15
WR_7: Active Power

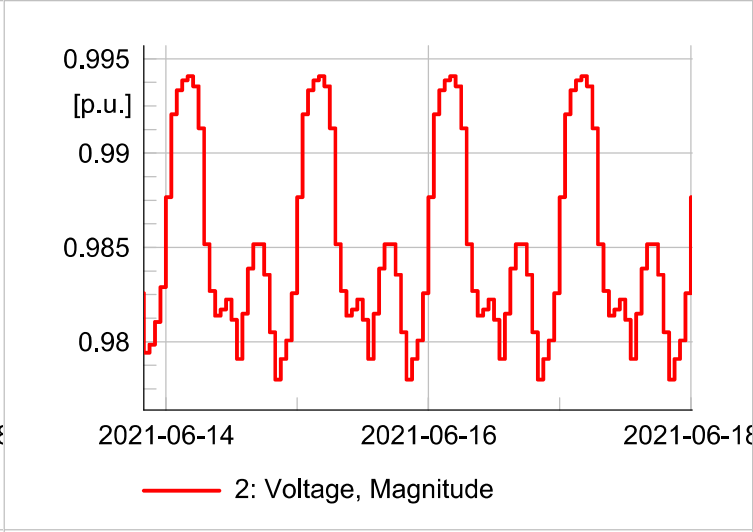

8
[kW]
6
4
2
2021-03-13
2021-03-14
2021-03-15
WR_8: Active Power

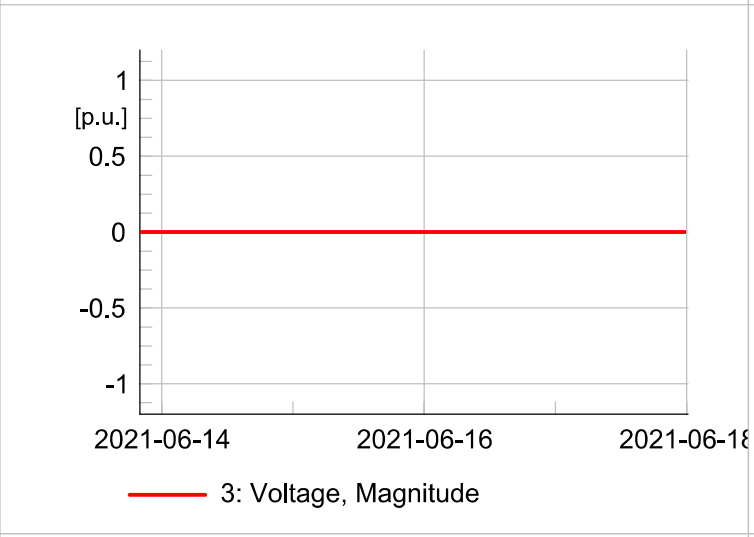

1.0005
[p.u.]
0.9980
0.9955
0.9930
0.9905
0.9880
0.00
100.00
200.00
300.00
400.00
[m]
500.0
0
1
6.1
6
5
7
2
8
Feeder: Voltage, Magnitude

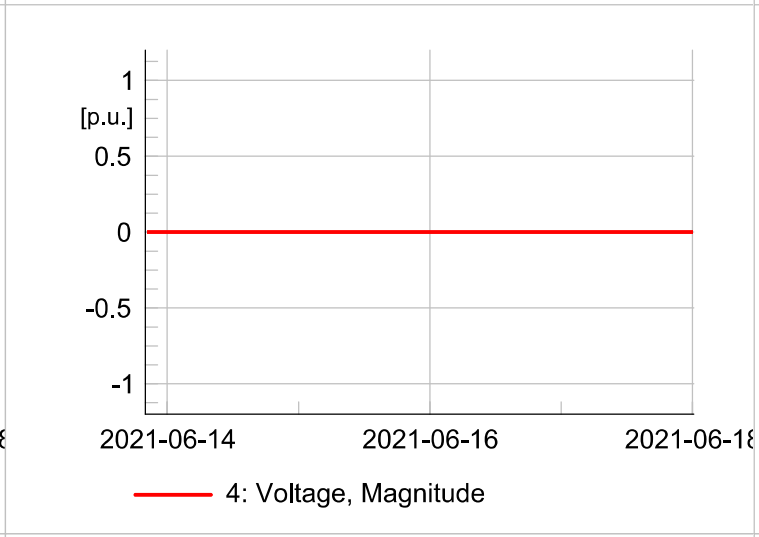

0
0.400
1.00000
0.000
157.445
76.759
0.253
0.899
L-0_1
63.2
WR_1
-155.647
-75.611
0.253
-0.899
17.781
8.612
0.029
0.900
1
0.395
0.98790
-0.082
35.713
17.317
0.058
0.900
102.153
49.682
0.166
0.899
L-1_8
14.5
L-1_6_1
41.5
-35.562
-17.223
0.058
-0.900
8
0.393
0.98346
-0.112
35.562
17.223
0.058
0.900
WR_8
-101.947
-49.551
0.166
-0.899
101.947
49.551
0.166
0.899
L-6_1_6
41.5
WR_6
-100.914
-48.893
0.166
-0.900
35.562
17.223
0.058
0.900
6
0.390
0.97519
-0.169
9.715
14.401
0.049
0.900
35.637
17.268
0.059
0.900
L-7_6
12.2
L-5_6
14.7
-29.634
-14.353
0.049
-0.900
7
0.389
0.97238
-0.189
29.635
14.353
0.049
0.900
WR_7
-35.586
-17.236
0.059
-0.900
5
0.389
0.97369
-0.180
17.805
8.625
0.029
0.900
17.781
8.612
0.029
0.900
WR_5
L-2_5
7.3
-17.781
-8.612
0.029
-0.900
2
0.389
0.97229
-0.189
17.781
8.612
0.029
0.900
WR_2

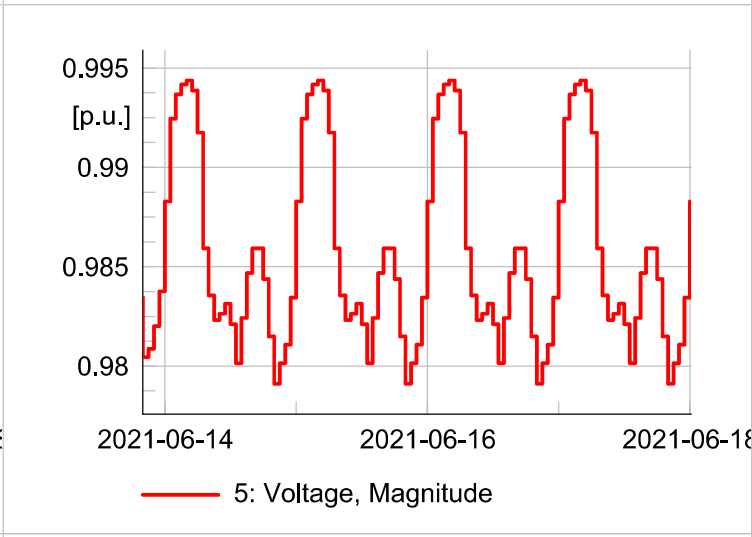

2
[p.u.]
1.5
1
0.5
0
2021-06-14
2021-06-16
2021-06-18
0: Voltage, Magnitude

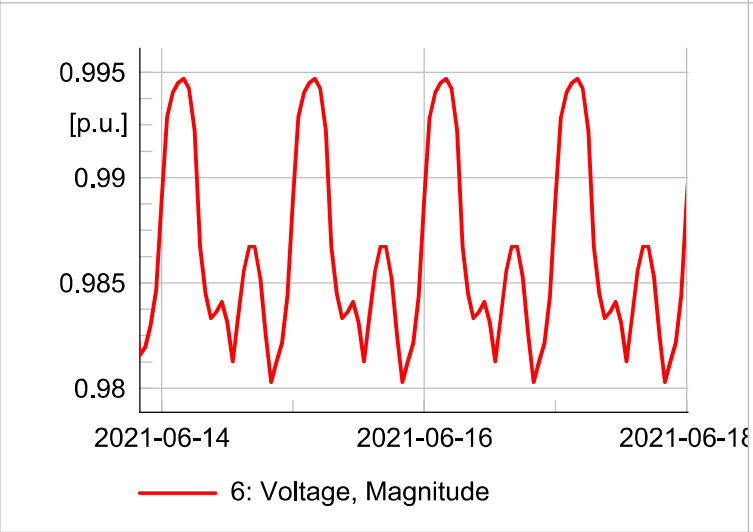

0.998
[p.u.]
0.996
0.994
0.992
0.99
2021-06-14
2021-06-16
2021-06-18
1: Voltage, Magnitude

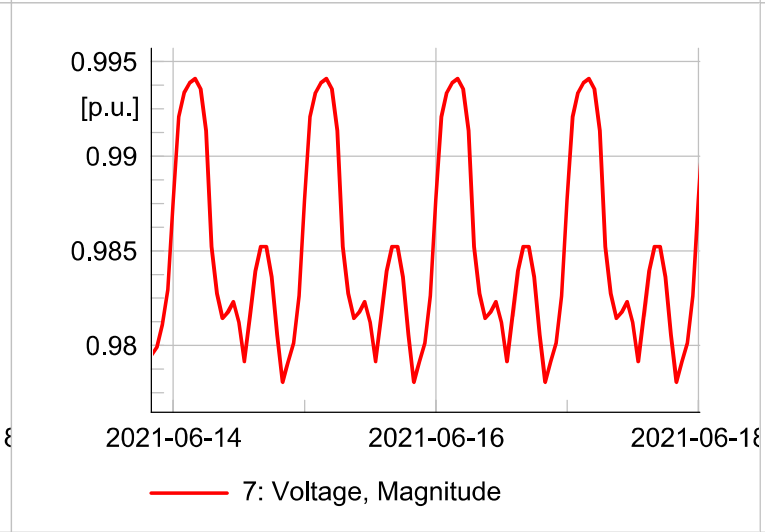

0.995
[p.u.]
0.99
0.985
0.98
2021-06-14
2021-06-16
2021-06-18
2: Voltage, Magnitude

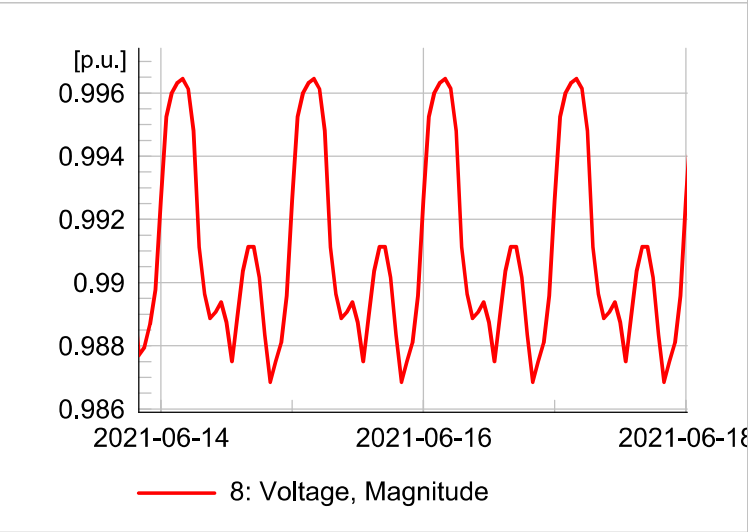

1
[p.u.]
0.5
0
-0.5
-1
2021-06-14
2021-06-16
2021-06-18
3: Voltage, Magnitude

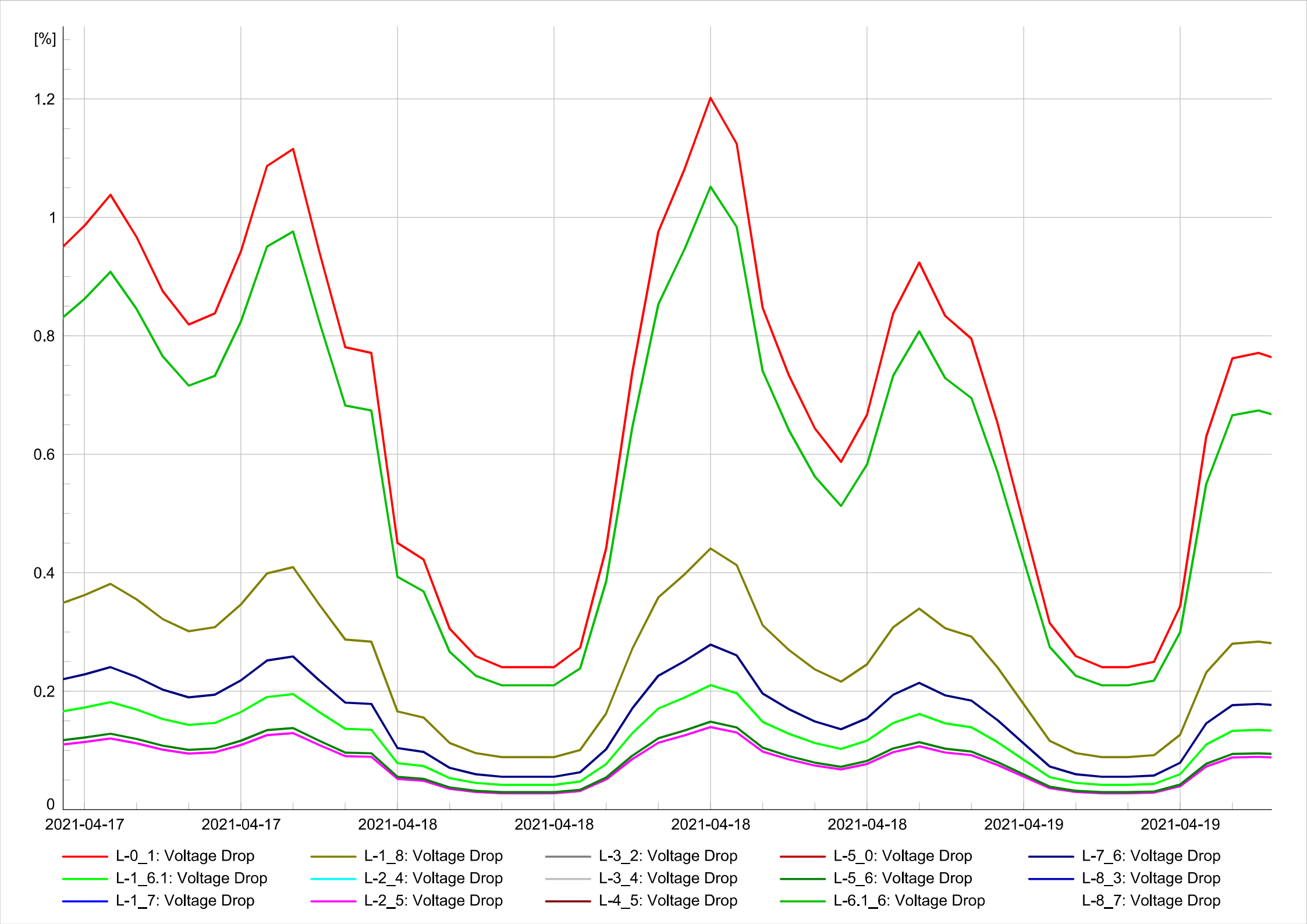

1
[p.u.]
0.5
0
-0.5
-1
2021-06-14
2021-06-16
2021-06-18
4: Voltage, Magnitude

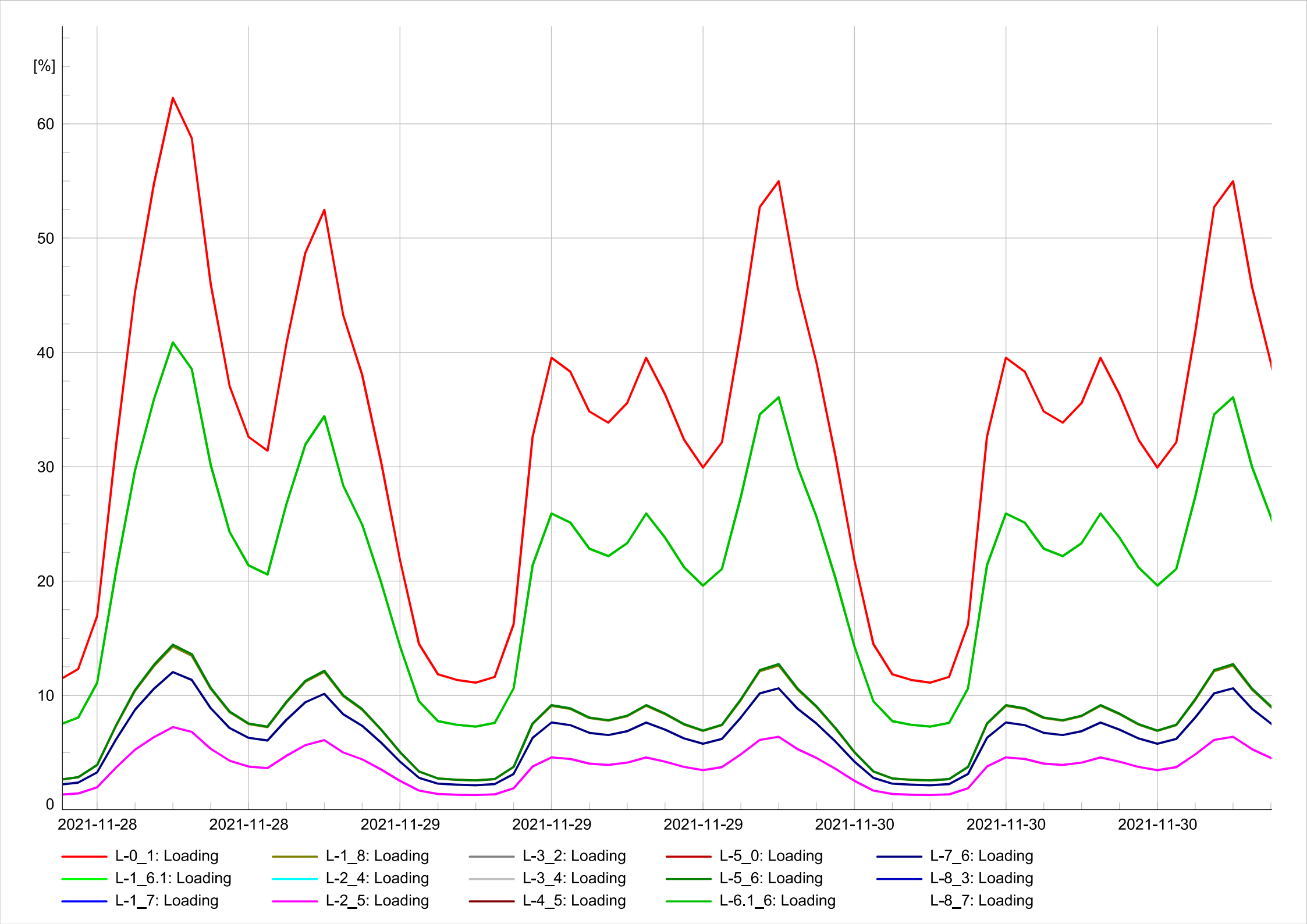

0.995
[p.u.]
0.99
0.985
0.98
2021-06-14
2021-06-16
2021-06-18
5: Voltage, Magnitude

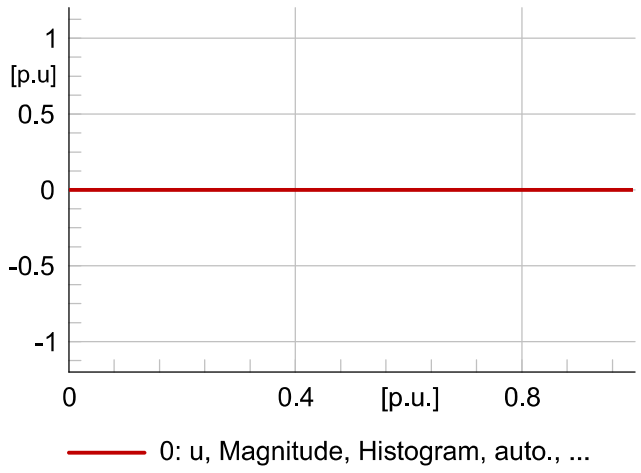

0.995
[p.u.]
0.99
0.985
0.98
2021-06-14
2021-06-16
2021-06-18
6: Voltage, Magnitude

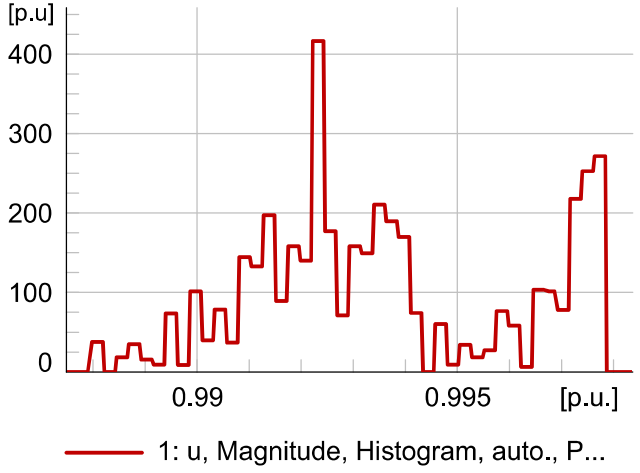

0.995
[p.u.]
0.99
0.985
0.98
2021-06-14
2021-06-16
2021-06-18
7: Voltage, Magnitude

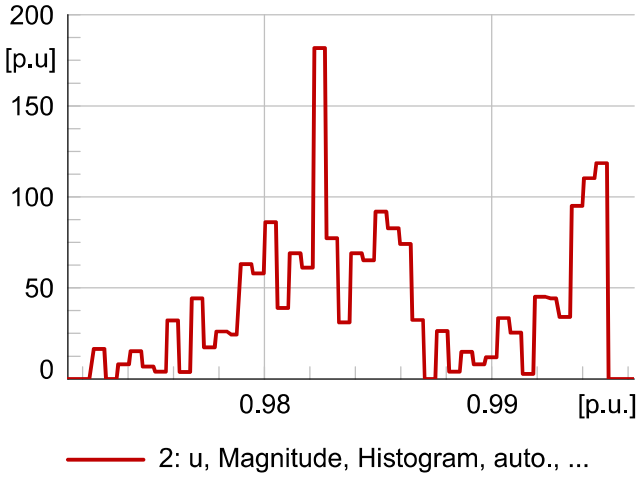

[p.u.]
0.996
0.994
0.992
0.99
0.988
0.986
2021-06-14
2021-06-16
2021-06-18
8: Voltage, Magnitude

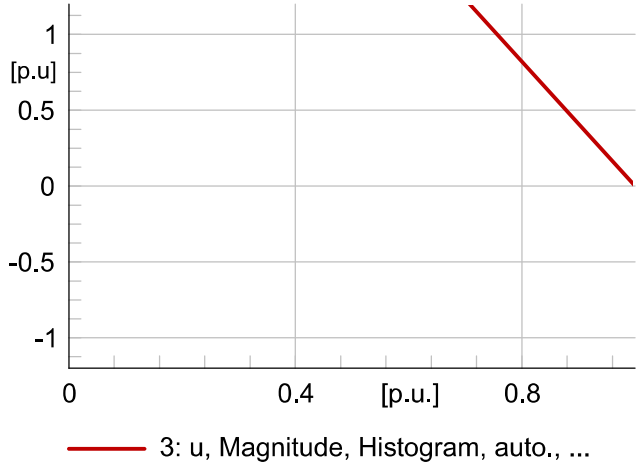

[%]
1.2
1
0.8
0.6
0.4
0.2
0
2021-04-17
2021-04-17
2021-04-18
2021-04-18
2021-04-18
2021-04-18
2021-04-19
2021-04-19
L-0_1: Voltage Drop
L-1_8: Voltage Drop
L-3_2: Voltage Drop
L-5_0: Voltage Drop
L-7_6: Voltage Drop
L-1_6.1: Voltage Drop
L-2_4: Voltage Drop
L-3_4: Voltage Drop
L-5_6: Voltage Drop
L-8_3: Voltage Drop
L-1_7: Voltage Drop
L-2_5: Voltage Drop
L-4_5: Voltage Drop
L-6.1_6: Voltage Drop
L-8_7: Voltage Drop

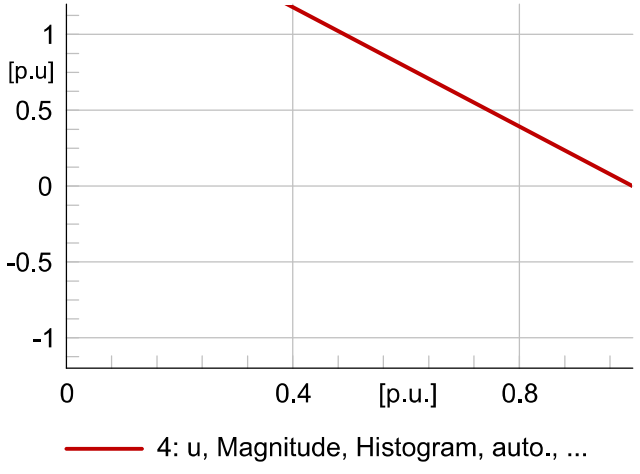

[%]
60
50
40
30
20
10
0
2021-11-28
2021-11-28
2021-11-29
2021-11-29
2021-11-29
2021-11-30
2021-11-30
2021-11-30
L-0_1: Loading
L-1_6.1: Loading
L-1_7: Loading
L-1_8: Loading
L-2_4: Loading
L-2_5: Loading
L-3_2: Loading
L-3_4: Loading
L-4_5: Loading
L-5_0: Loading
L-5_6: Loading
L-6.1_6: Loading
L-7_6: Loading
L-8_3: Loading
L-8_7: Loading

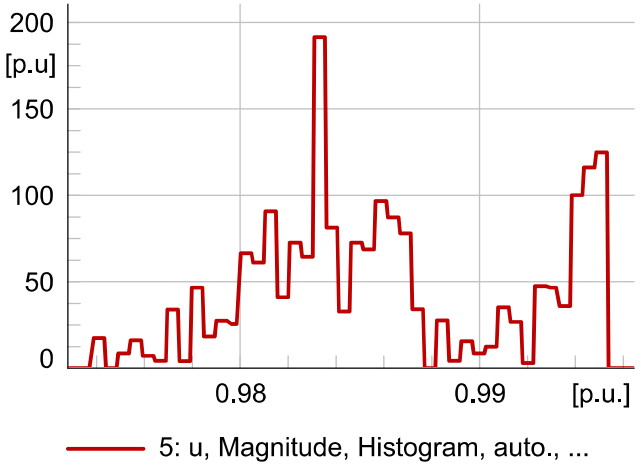

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
0: u, Magnitude, Histogram, auto., ...

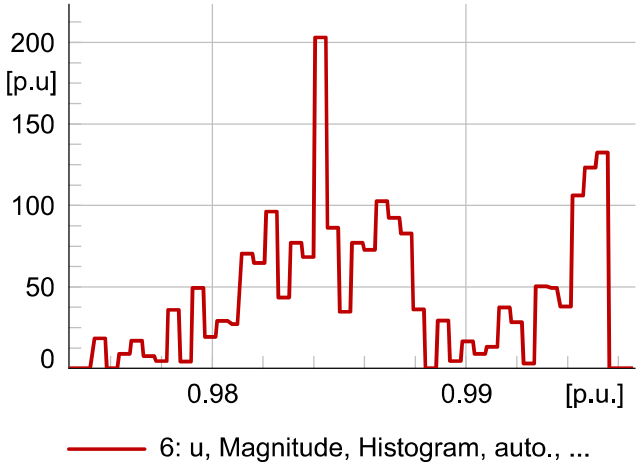

[p.u]
400
300
200
100
0
0.99
0.995
[p.u.]
1: u, Magnitude, Histogram, auto., P...

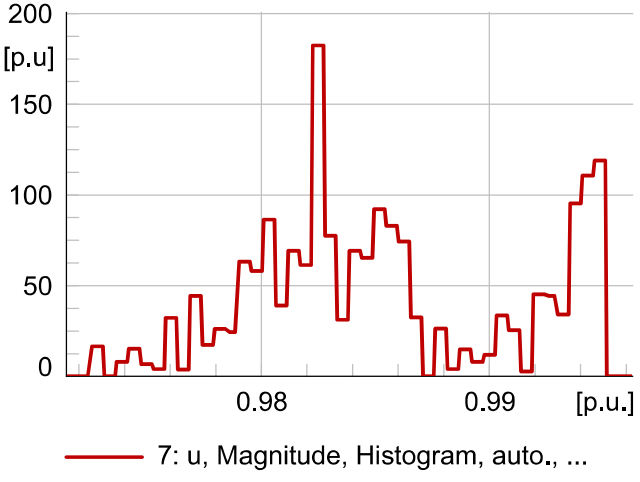

200
[p.u]
150
100
50
0
0.98
0.99
[p.u.]
2: u, Magnitude, Histogram, auto., ...

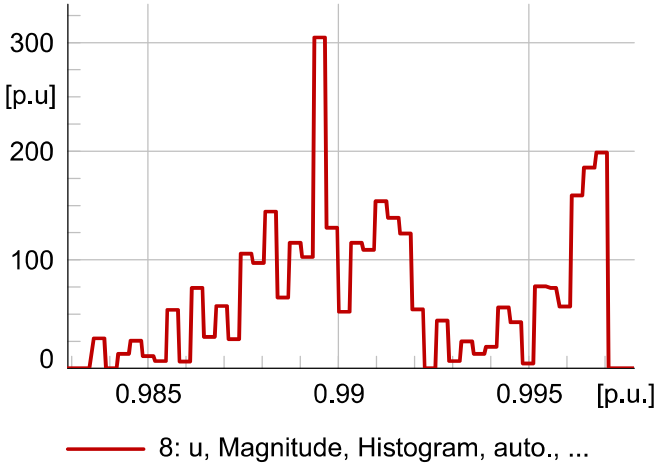

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
3: u, Magnitude, Histogram, auto., ...

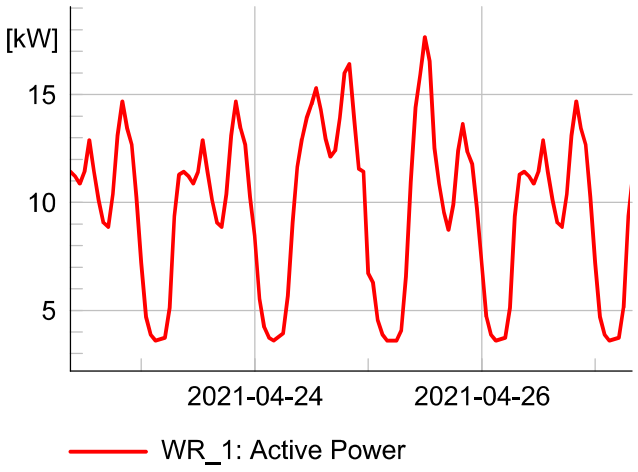

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
4: u, Magnitude, Histogram, auto., ...

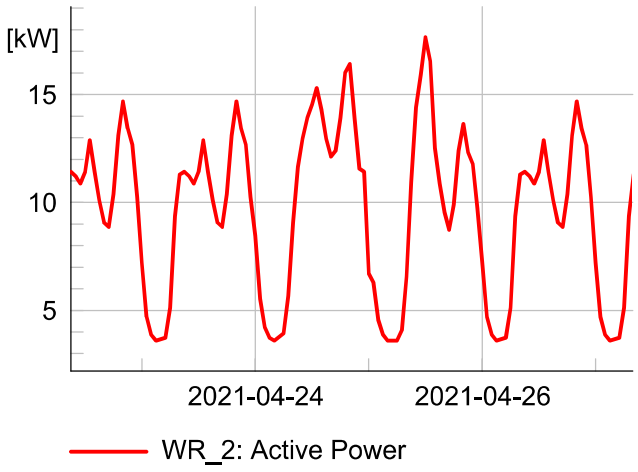

200
[p.u]
150
100
50
0
0.98
0.99
[p.u.]
5: u, Magnitude, Histogram, auto., ...

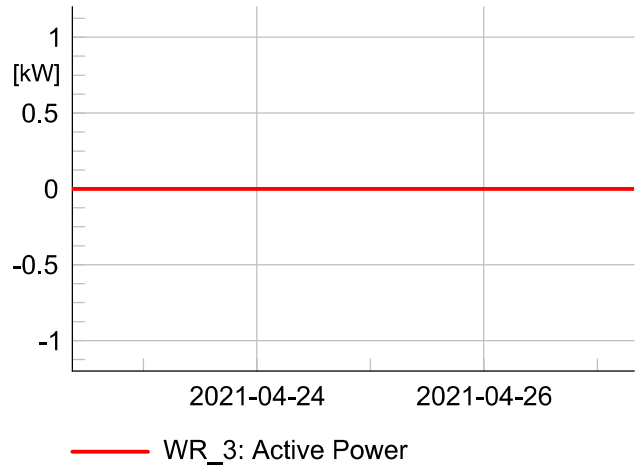

200
[p.u]
150
100
50
0
0.98
0.99
[p.u.]
6: u, Magnitude, Histogram, auto., ...

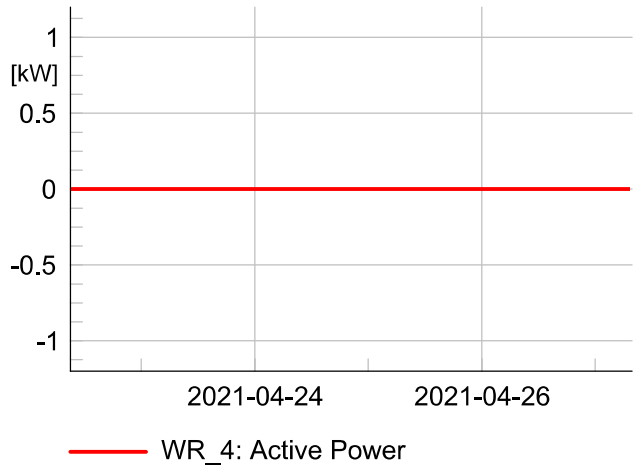

200
[p.u]
150
100
50
0
0.98
0.99
[p.u.]
7: u, Magnitude, Histogram, auto., ...

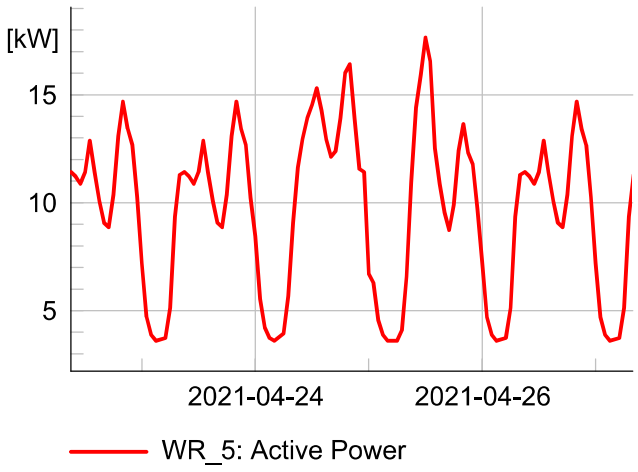

300
[p.u]
200
100
0
0.985
0.99
0.995
[p.u.]
8: u, Magnitude, Histogram, auto., ...

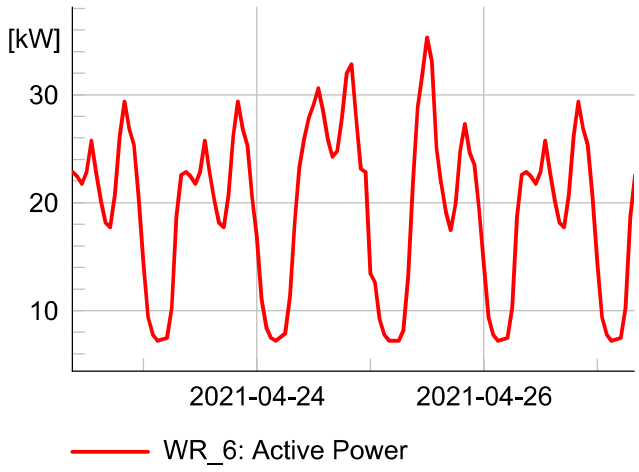

[kW]
15
10
5
2021-04-24
2021-04-26
WR_1: Active Power

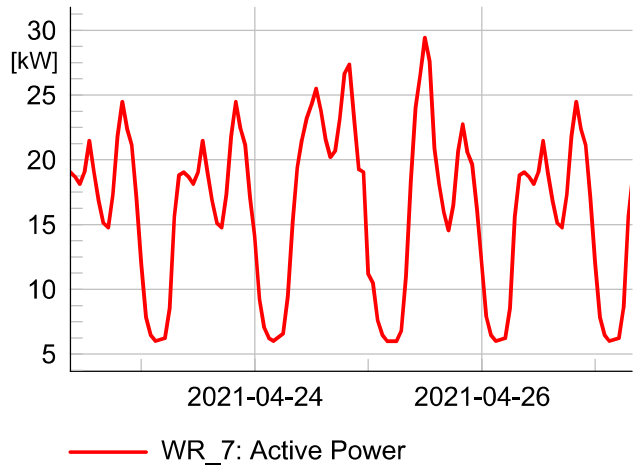

[kW]
15
10
5
2021-04-24
2021-04-26
WR_2: Active Power

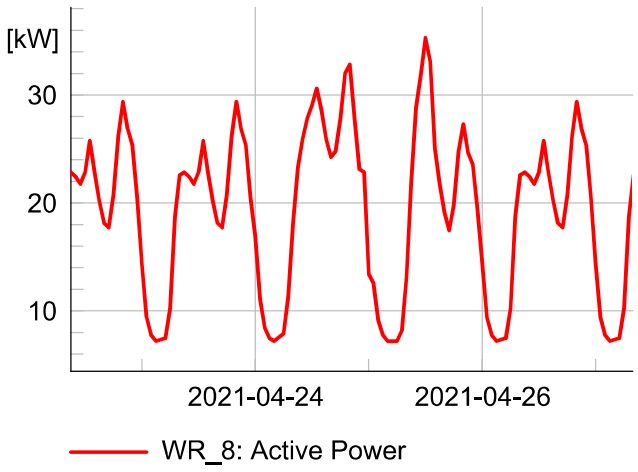

1
[kW]
0.5
0
-0.5
-1
2021-04-24
2021-04-26
WR_3: Active Power

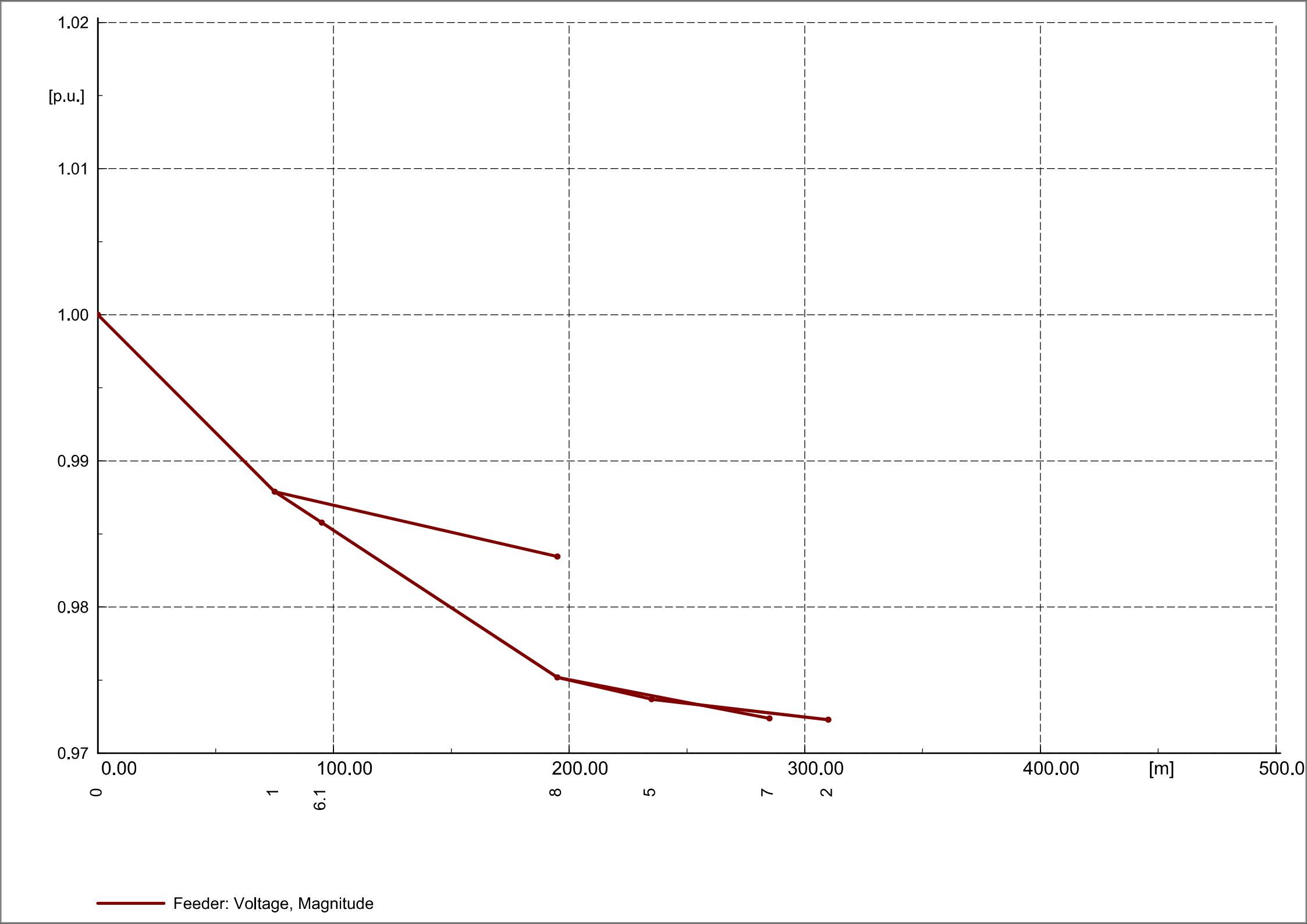

1
[kW]
0.5
0
-0.5
-1
2021-04-24
2021-04-26
WR_4: Active Power

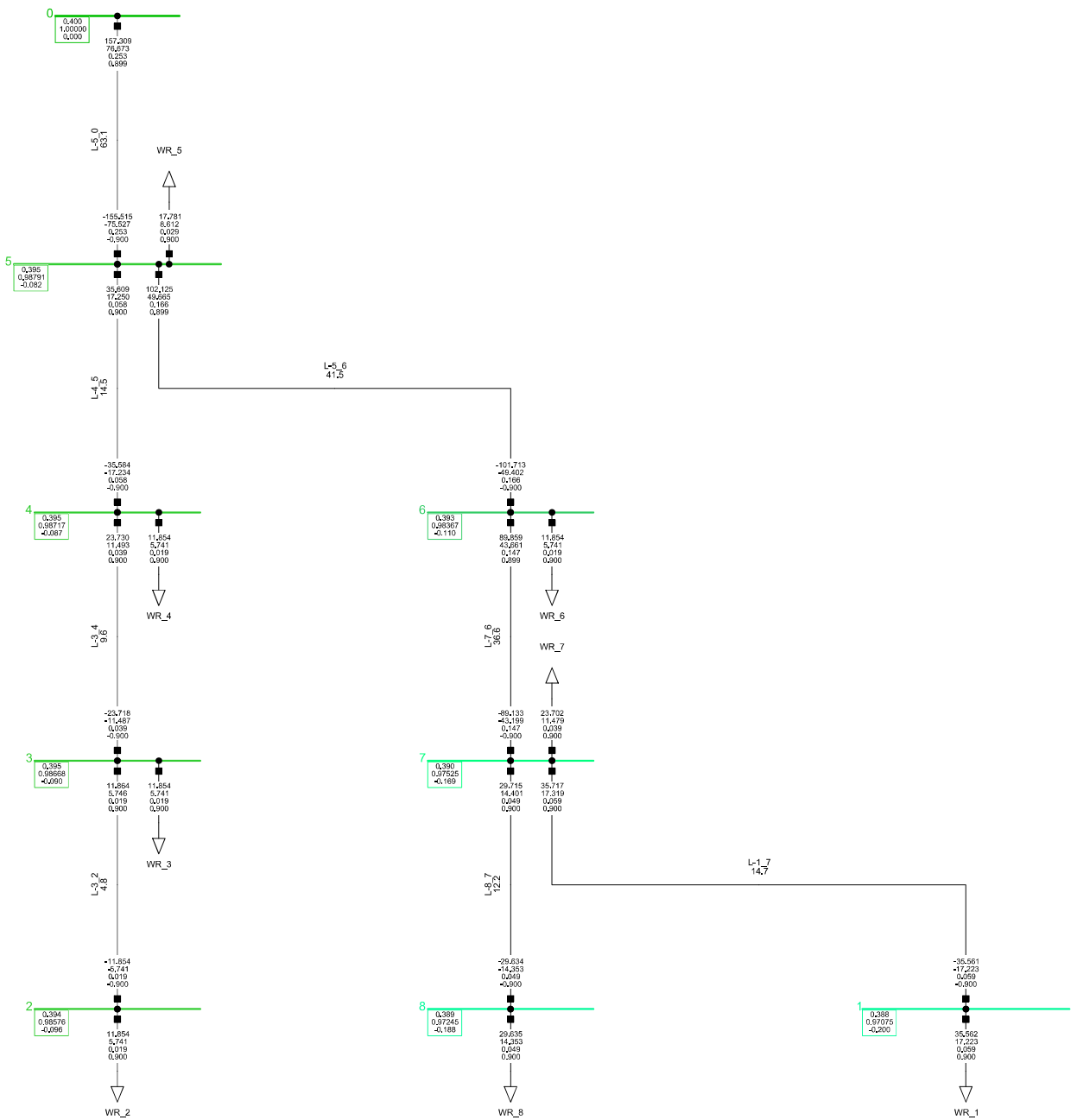

[kW]
15
10
5
2021-04-24
2021-04-26
WR_5: Active Power

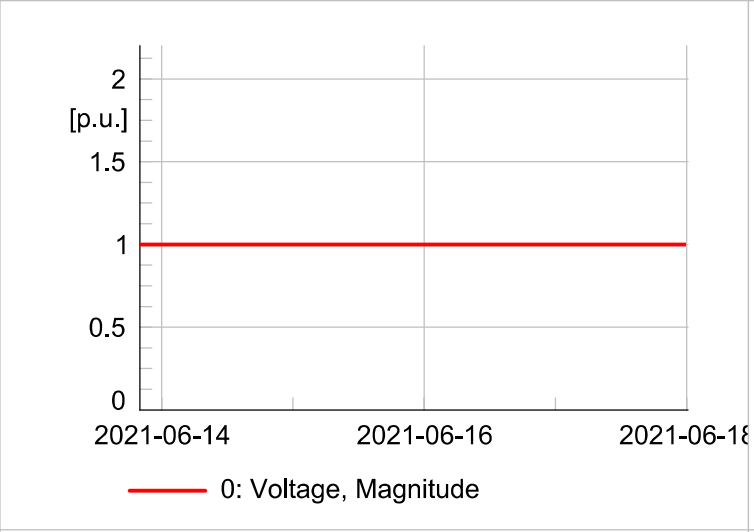

[kW]
30
20
10
2021-04-24
2021-04-26
WR_6: Active Power

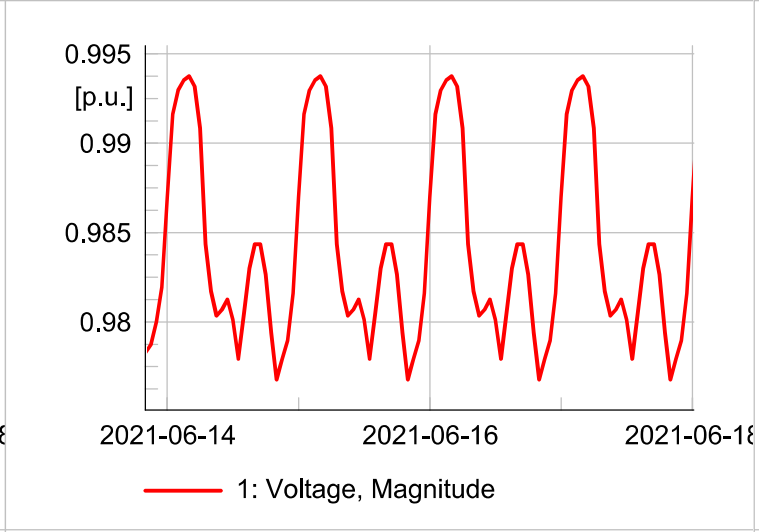

30
[kW]
25
20
15
10
5
2021-04-24
2021-04-26
WR_7: Active Power

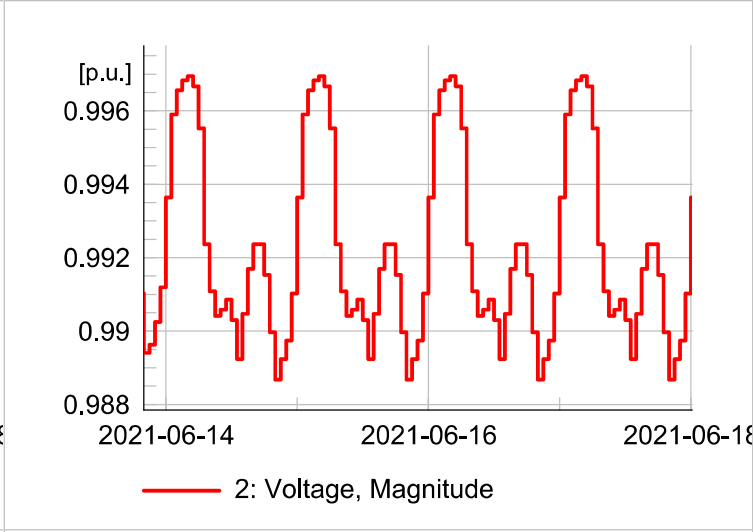

[kW]
30
20
10
2021-04-24
2021-04-26
WR_8: Active Power

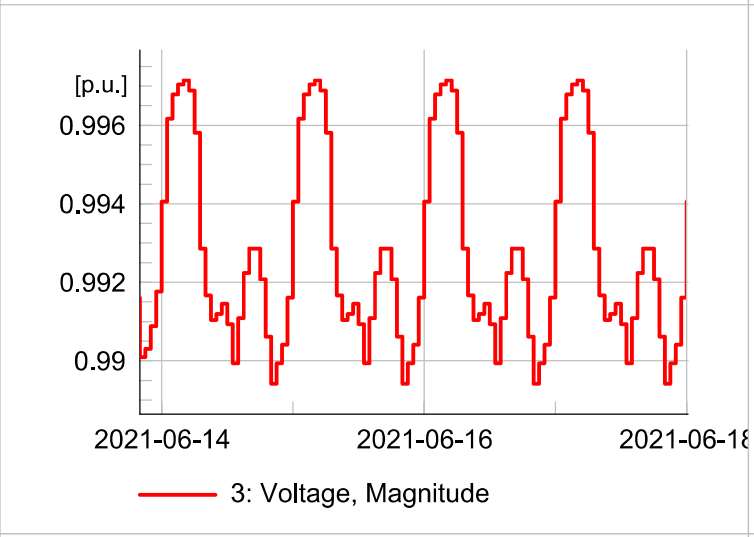

1.02
[p.u.]
1.01
1.00
0.99
0.98
0.97
0.00
100.00
200.00
300.00
400.00
[m]
500.0
0
1
6.1
8
5
7
2
Feeder: Voltage, Magnitude

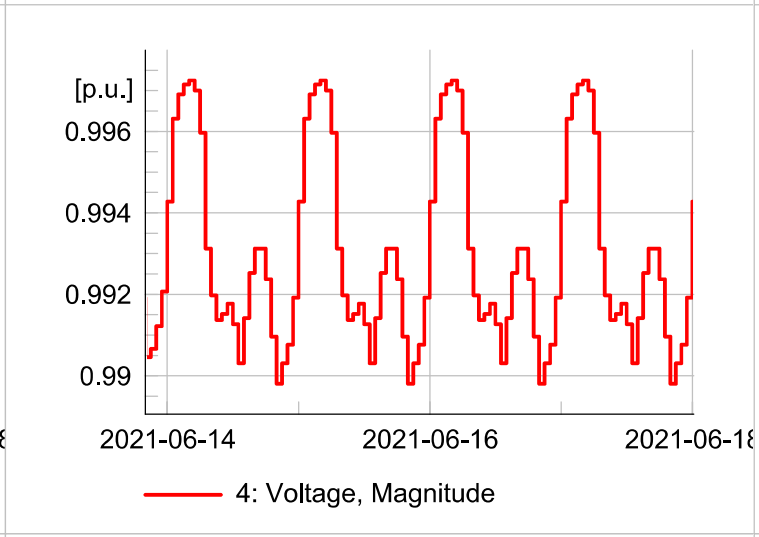

0
0.400
1.00000
0.000
157.209
76.673
0.253
0.899
L-5_0
63.1
WR_5
-155.515
-75.527
0.253
-0.900
17.781
8.612
0.029
0.900
5
0.395
0.98791
-0.082
35.609
17.250
0.058
0.900
102.125
49.565
0.166
0.899
L-5_6
41.5
L-4_5
14.5
-35.584
-17.234
0.058
-0.900
-101.713
-49.402
0.166
-0.900
4
0.395
0.98717
-0.087
23.730
11.493
0.039
0.900
11.854
5.741
0.019
0.900
6
0.393
0.98367
-0.110
89.859
43.661
0.147
0.899
11.854
5.741
0.019
0.900
WR_4
WR_6
L-3_4
9.6
L-7_6
36.6
WR_7
-23.718
-11.487
0.039
-0.900
-89.133
-43.199
0.147
-0.900
23.702
11.479
0.039
0.900
3
0.395
0.98668
-0.090
7
0.390
0.97525
-0.169
11.854
5.746
0.019
0.900
11.854
5.741
0.019
0.900
29.715
14.401
0.049
0.900
35.717
17.319
0.059
0.900
WR_3
L-1_7
14.7
L-3_2
4.8
L-8_7
12.2
-11.854
-5.741
0.019
-0.900
-29.634
-14.353
0.049
-0.900
-35.561
-17.223
0.059
-0.900
2
0.394
0.98576
-0.096
8
0.389
0.97245
-0.188
1
0.388
0.97075
-0.200
11.854
5.741
0.019
0.900
29.635
14.353
0.049
0.900
35.562
17.223
0.059
0.900
WR_2
WR_8
WR_1

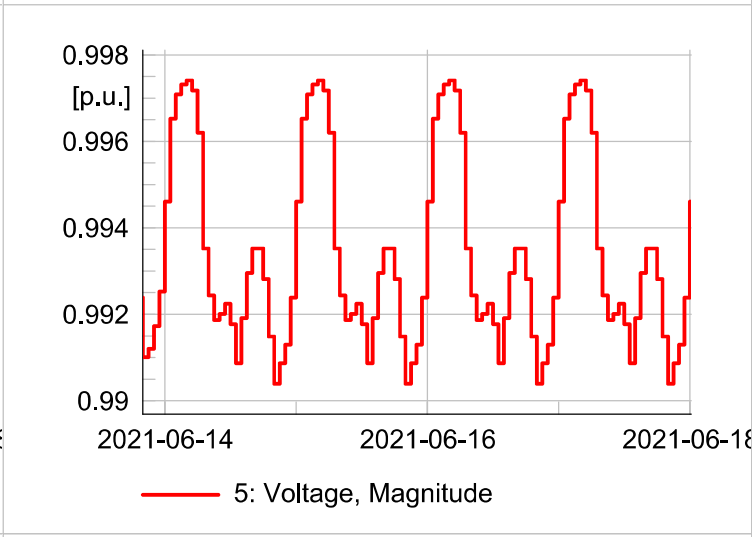

2
[p.u.]
1.5
1
0.5
0
2021-06-14
2021-06-16
2021-06-18
0: Voltage, Magnitude

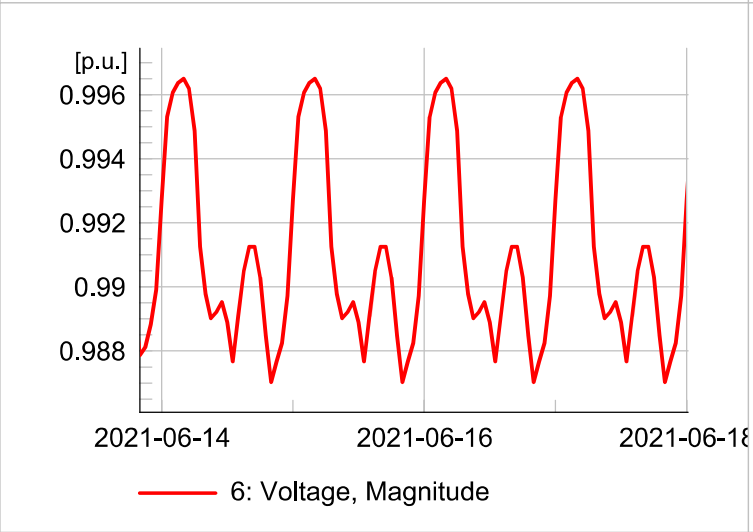

0.995
[p.u.]
0.99
0.985
0.98
2021-06-14
2021-06-16
2021-06-18
1: Voltage, Magnitude

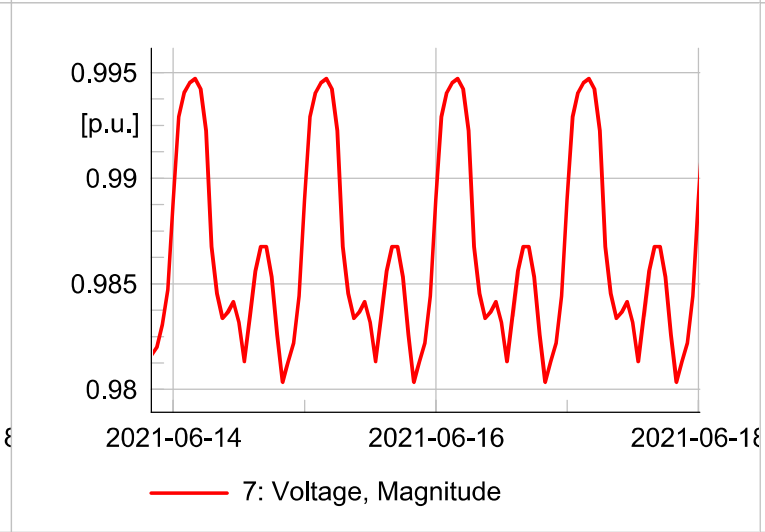

[p.u.]
0.996
0.994
0.992
0.99
0.988
2021-06-14
2021-06-16
2021-06-18
2: Voltage, Magnitude

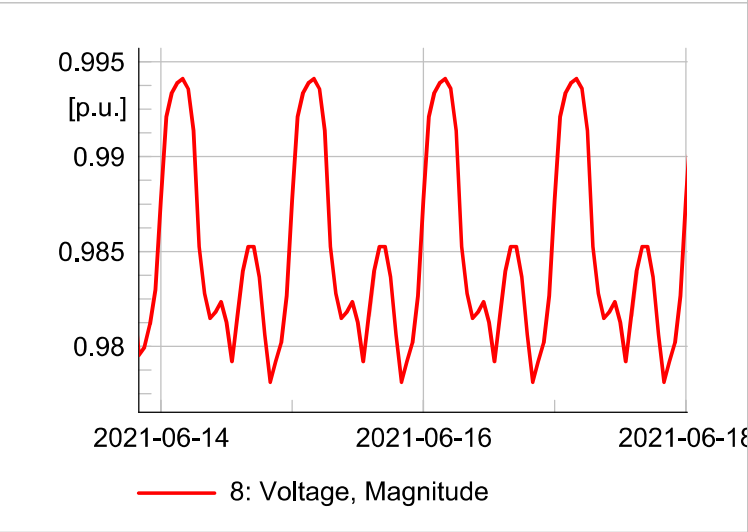

[p.u.]
0.996
0.994
0.992
0.99
2021-06-14
2021-06-16
2021-06-18
3: Voltage, Magnitude

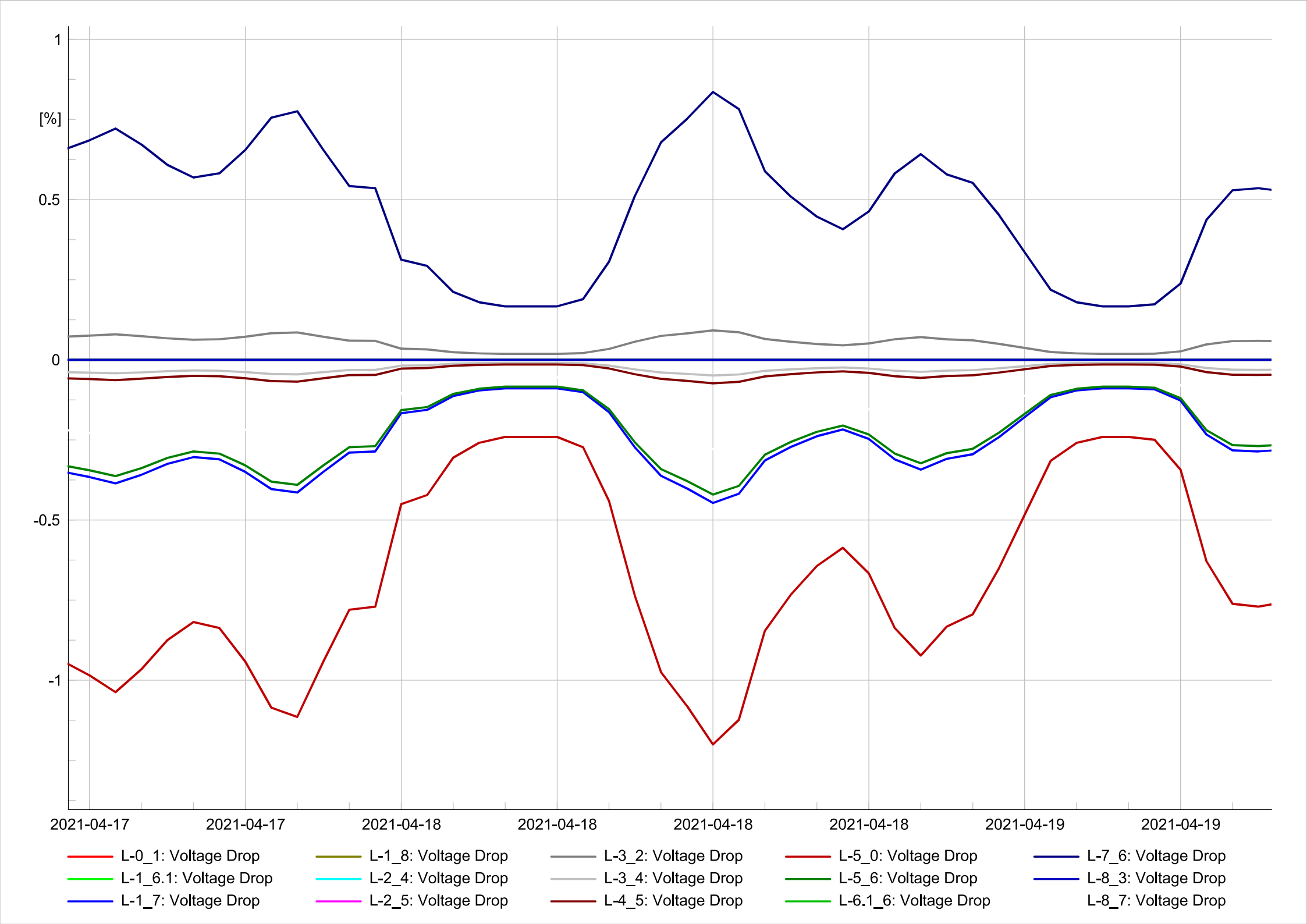

[p.u.]
0.996
0.994
0.992
0.99
2021-06-14
2021-06-16
2021-06-18
4: Voltage, Magnitude

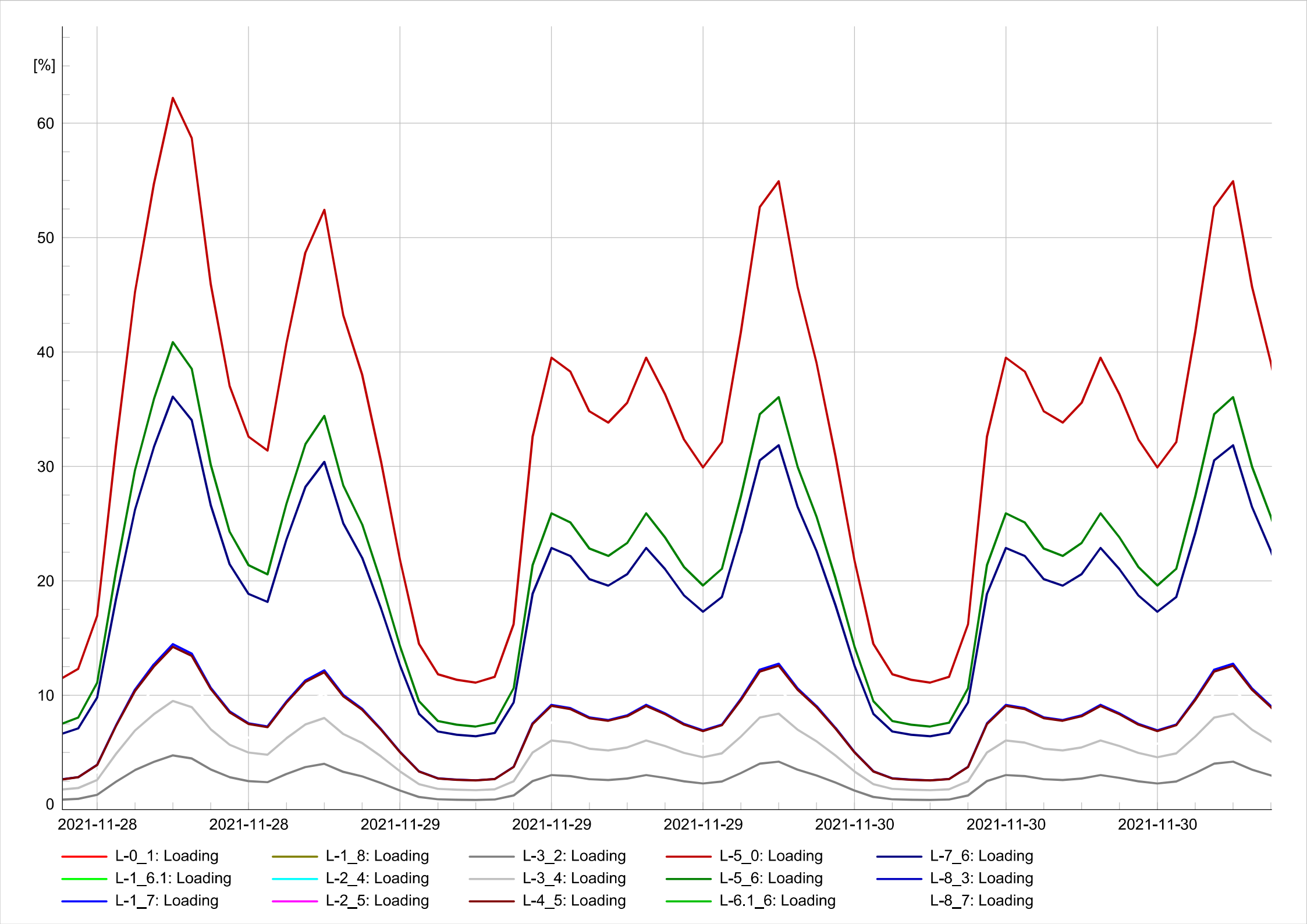

0.998
[p.u.]
0.996
0.994
0.992
0.99
2021-06-14
2021-06-16
2021-06-18
5: Voltage, Magnitude

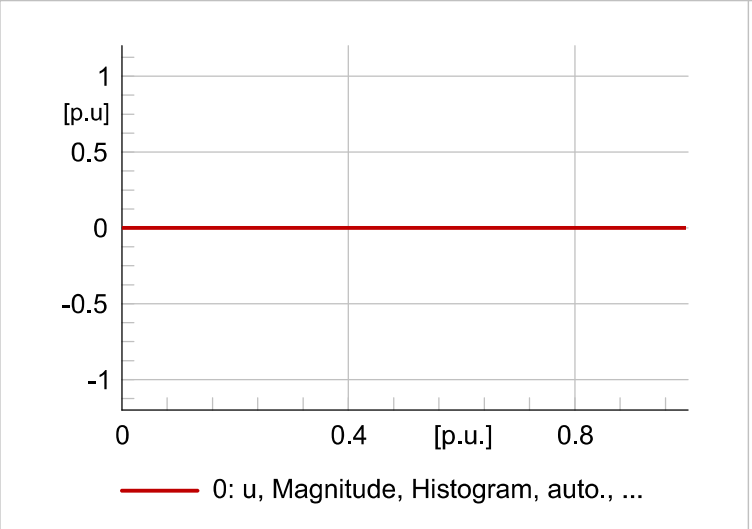

[p.u.]
0.996
0.994
0.992
0.99
0.988
2021-06-14
2021-06-16
2021-06-18
6: Voltage, Magnitude

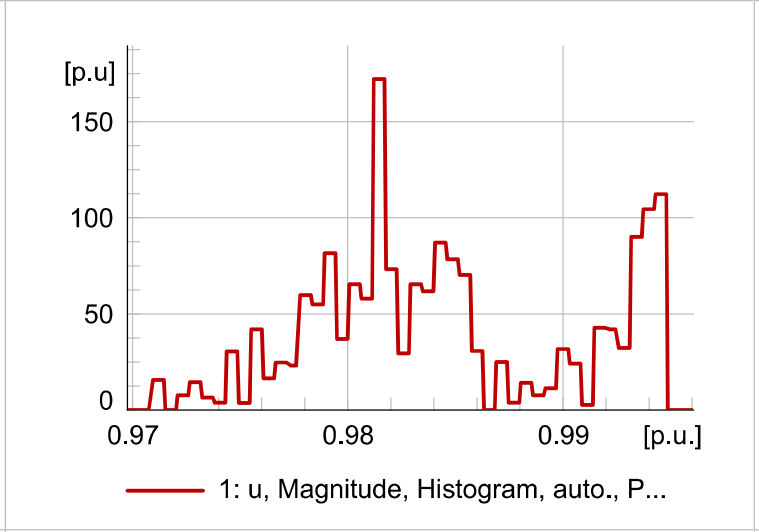

0.995
[p.u.]
0.99
0.985
0.98
2021-06-14
2021-06-16
2021-06-18
7: Voltage, Magnitude

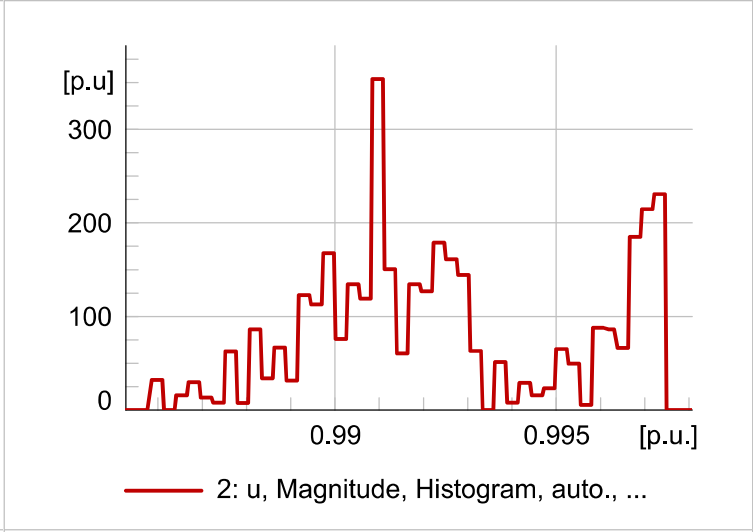

0.995
[p.u.]
0.99
0.985
0.98
2021-06-14
2021-06-16
2021-06-18
8: Voltage, Magnitude

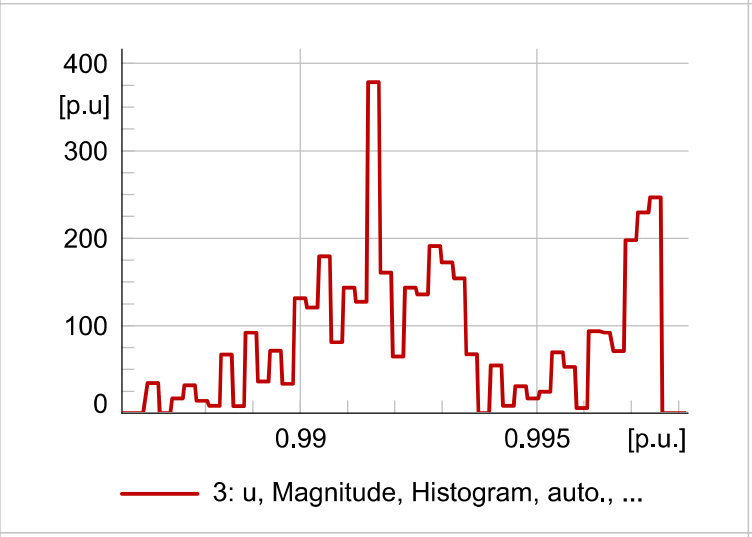

1
[%]
0.5
0
-0.5
-1
2021-04-17
2021-04-17
2021-04-18
2021-04-18
2021-04-18
2021-04-18
2021-04-19
2021-04-19
L-0_1: Voltage Drop
L-1_8: Voltage Drop
L-3_2: Voltage Drop
L-5_0: Voltage Drop
L-7_6: Voltage Drop
L-1_6.1: Voltage Drop
L-2_4: Voltage Drop
L-3_4: Voltage Drop
L-5_6: Voltage Drop
L-8_3: Voltage Drop
L-1_7: Voltage Drop
L-2_5: Voltage Drop
L-4_5: Voltage Drop
L-6.1_6: Voltage Drop
L-8_7: Voltage Drop

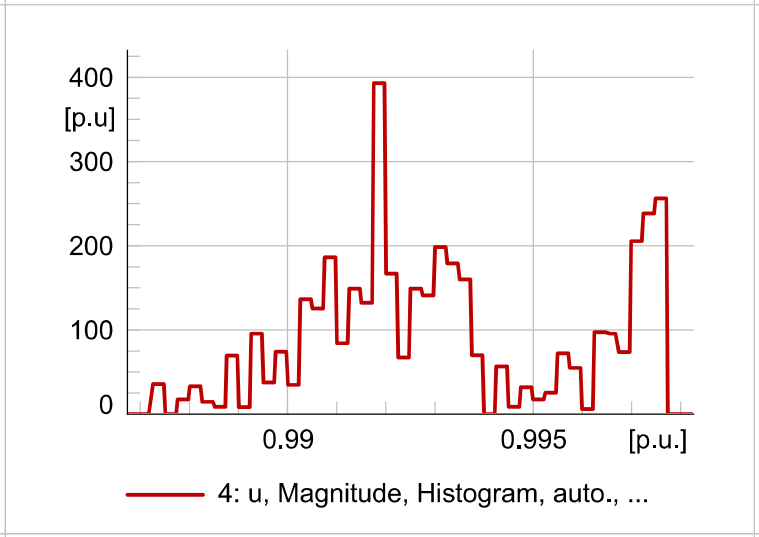

[%]
60
50
40
30
20
10
0
2021-11-28
2021-11-28
2021-11-29
2021-11-29
2021-11-29
2021-11-30
2021-11-30
2021-11-30
L-0_1: Loading
L-1_6.1: Loading
L-1_7: Loading
L-1_8: Loading
L-2_4: Loading
L-2_5: Loading
L-3_2: Loading
L-3_4: Loading
L-4_5: Loading
L-5_0: Loading
L-5_6: Loading
L-6.1_6: Loading
L-7_6: Loading
L-8_3: Loading
L-8_7: Loading

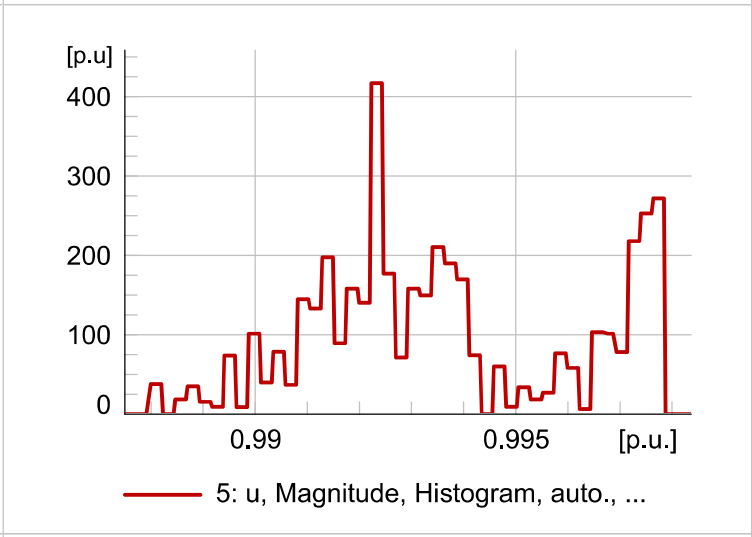

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
0: u, Magnitude, Histogram, auto., ...

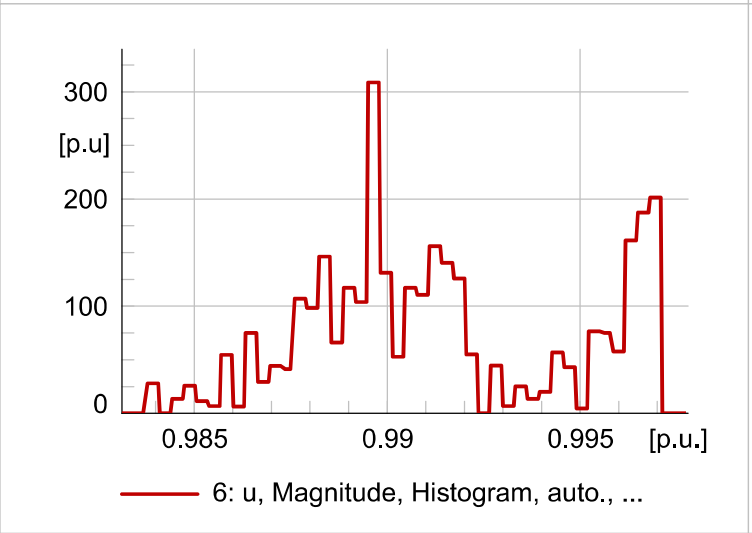

[p.u]
150
100
50
0
0.97
0.98
0.99
[p.u.]
1: u, Magnitude, Histogram, auto., P...

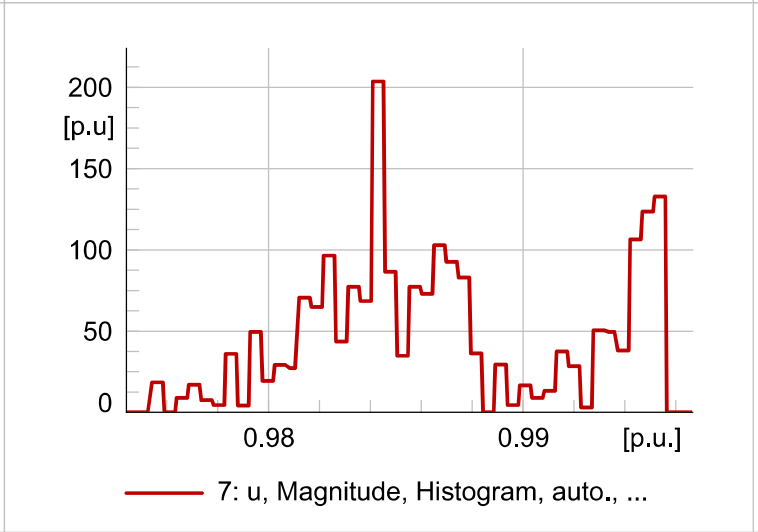

[p.u]
300
200
100
0
0.99
0.995
[p.u.]
2: u, Magnitude, Histogram, auto., ...

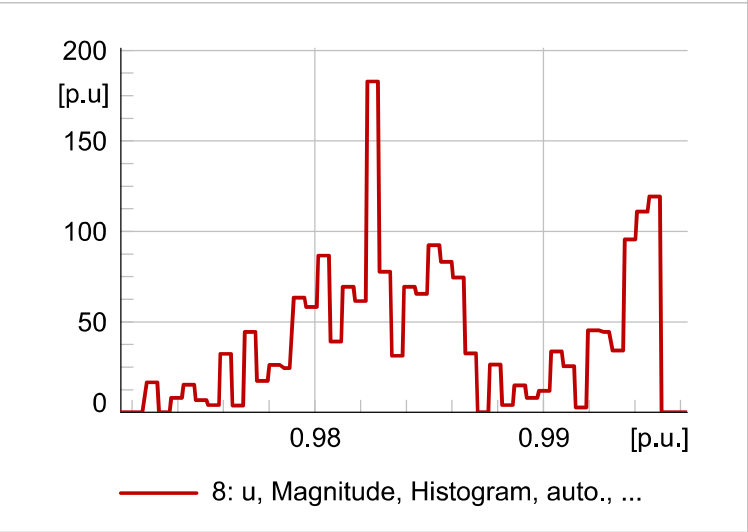

400
[p.u]
300
200
100
0
0.99
0.995
[p.u.]
3: u, Magnitude, Histogram, auto., ...

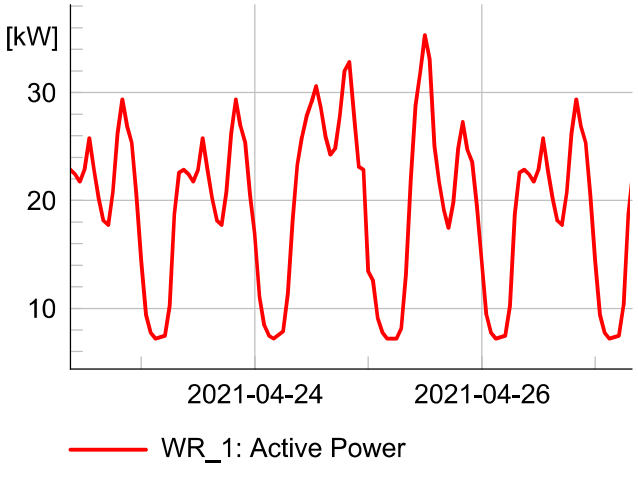

400
[p.u]
300
200
100
0
0.99
0.995
[p.u.]
4: u, Magnitude, Histogram, auto., ...

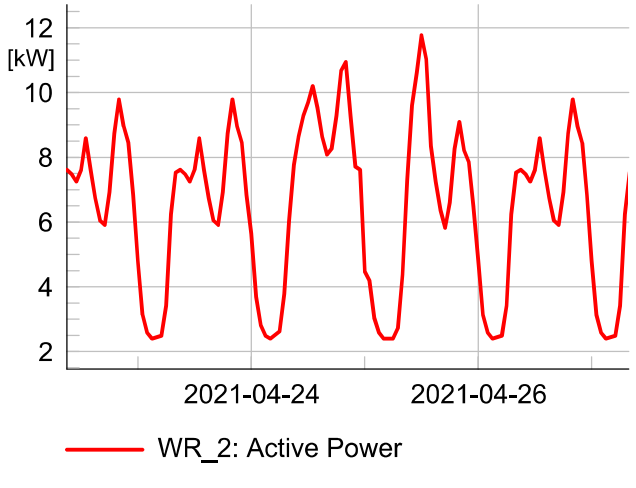

[p.u]
400
300
200
100
0
0.99
0.995
[p.u.]
5: u, Magnitude, Histogram, auto., ...

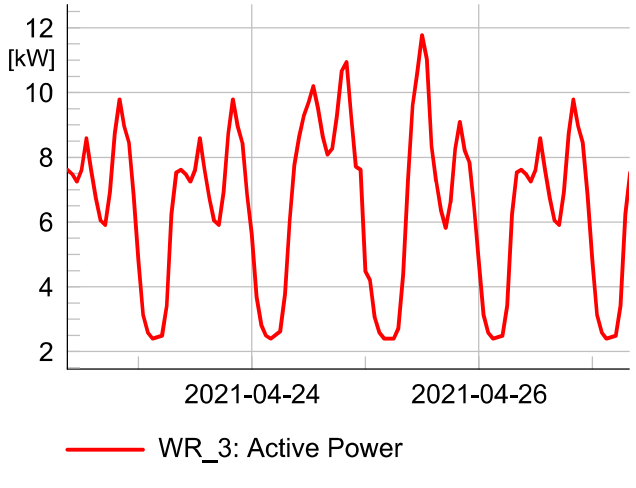

300
[p.u]
200
100
0
0.985
0.99
0.995
[p.u.]
6: u, Magnitude, Histogram, auto., ...

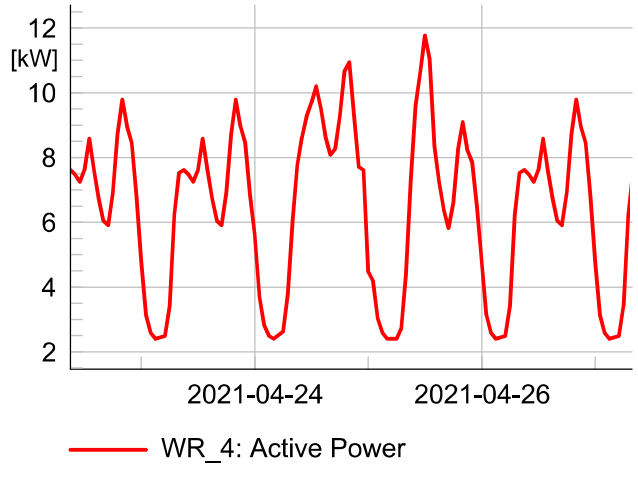

200
[p.u]
150
100
50
0
0.98
0.99
[p.u.]
7: u, Magnitude, Histogram, auto., ...

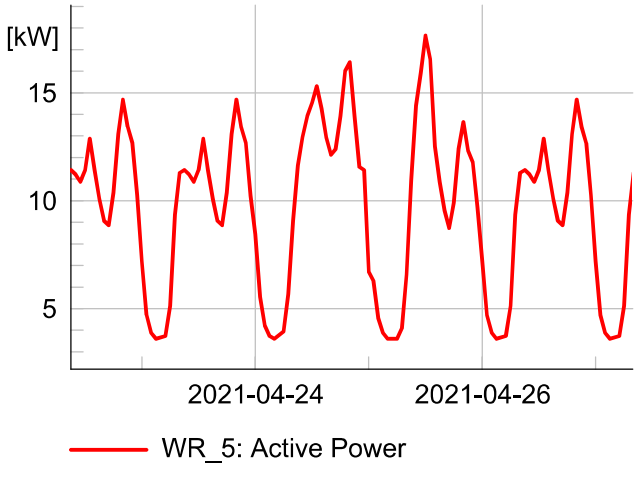

200
[p.u]
150
100
50
0
0.98
0.99
[p.u.]
8: u, Magnitude, Histogram, auto., ...

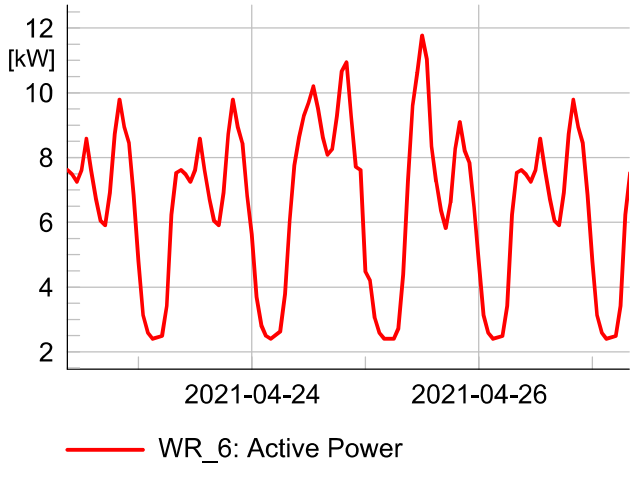

[kW]
30
20
10
2021-04-24
2021-04-26
WR_1: Active Power

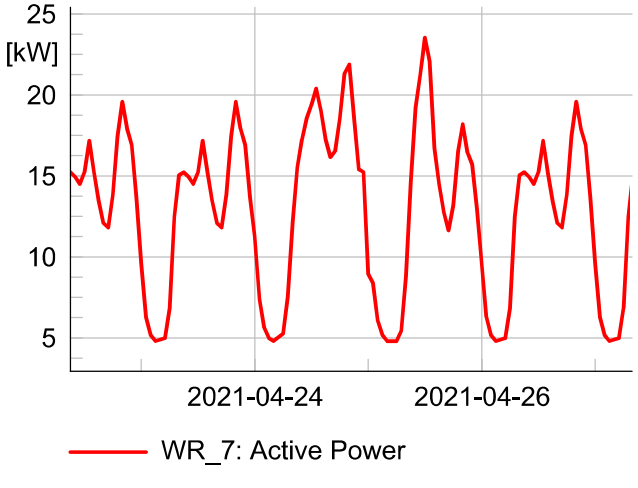

12
[kW]
10
8
6
4
2
2021-04-24
2021-04-26
WR_2: Active Power

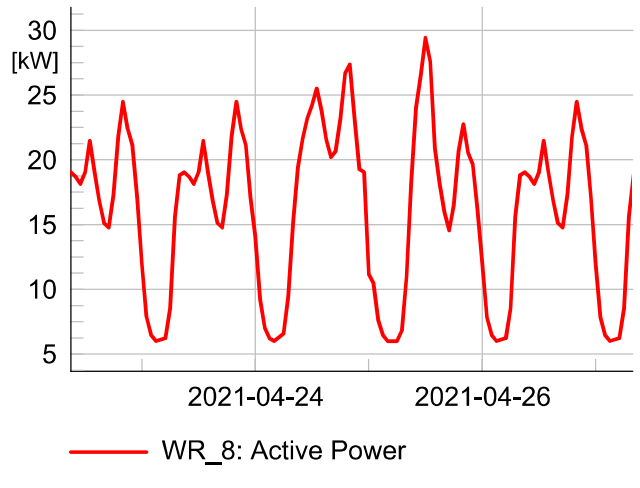

12
[kW]
10
8
6
4
2
2021-04-24
2021-04-26
WR_3: Active Power

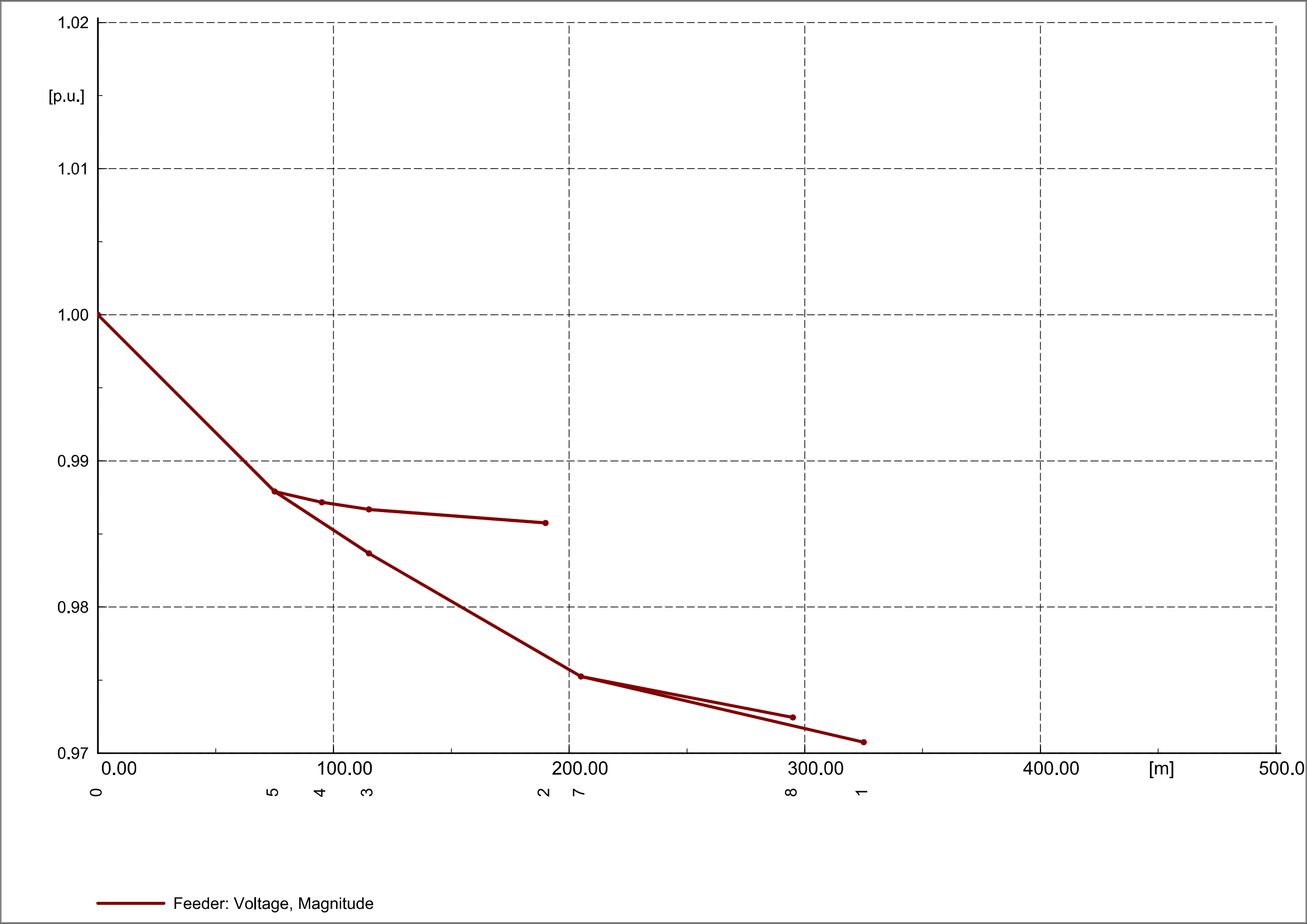

12
[kW]
10
8
6
4
2
2021-04-24
2021-04-26
WR_4: Active Power

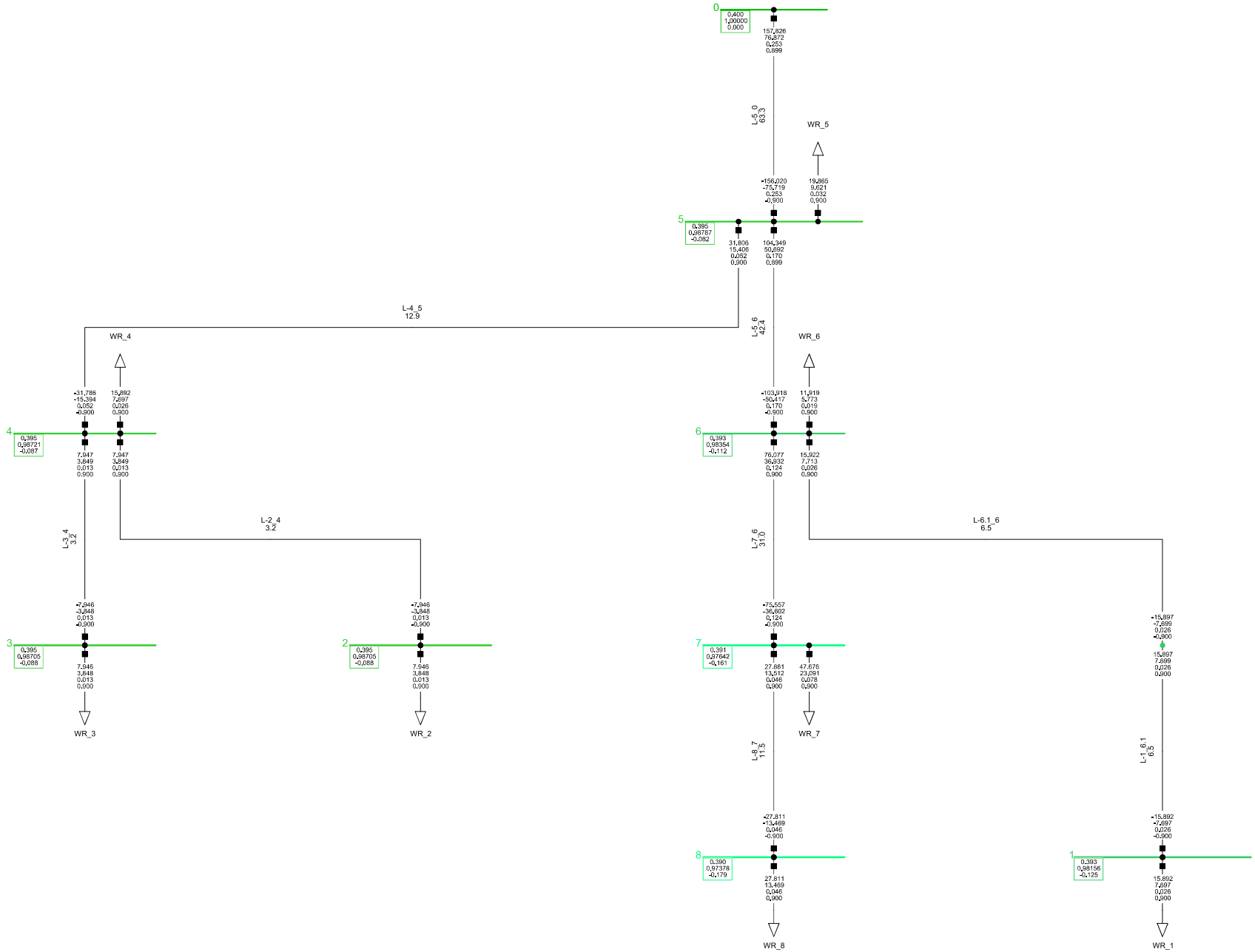

[kW]
15
10
5
2021-04-24
2021-04-26
WR_5: Active Power

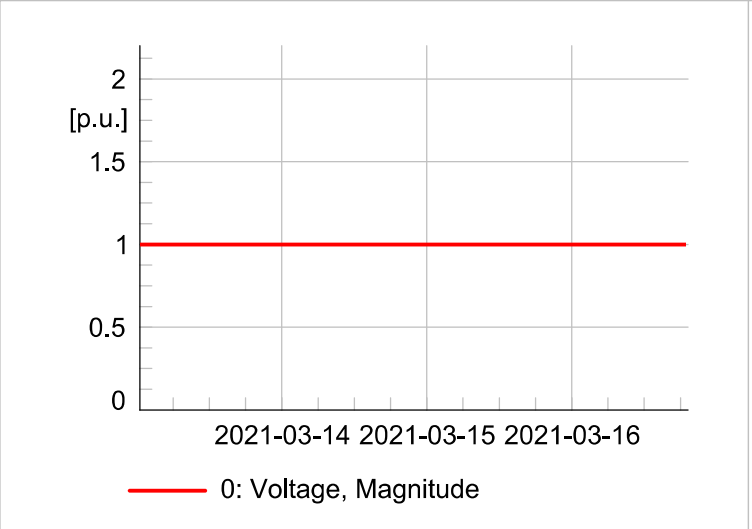

12
[kW]
10
8
6
4
2
2021-04-24
2021-04-26
WR_6: Active Power

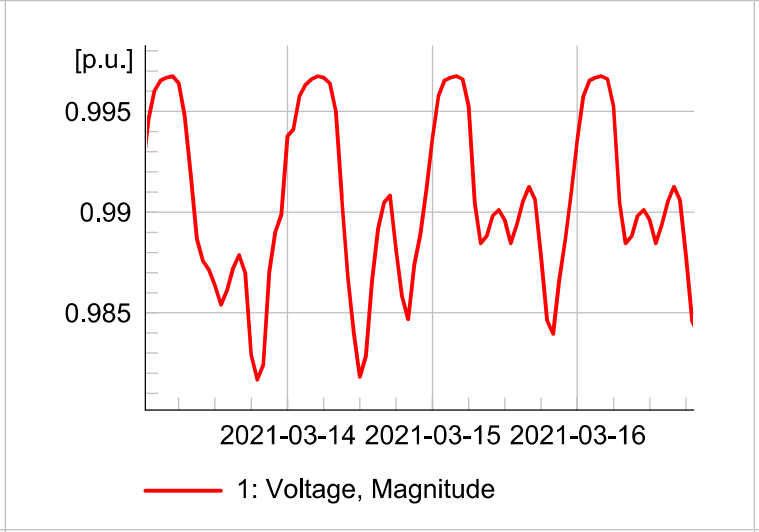

25
[kW]
20
15
10
5
2021-04-24
2021-04-26
WR_7: Active Power

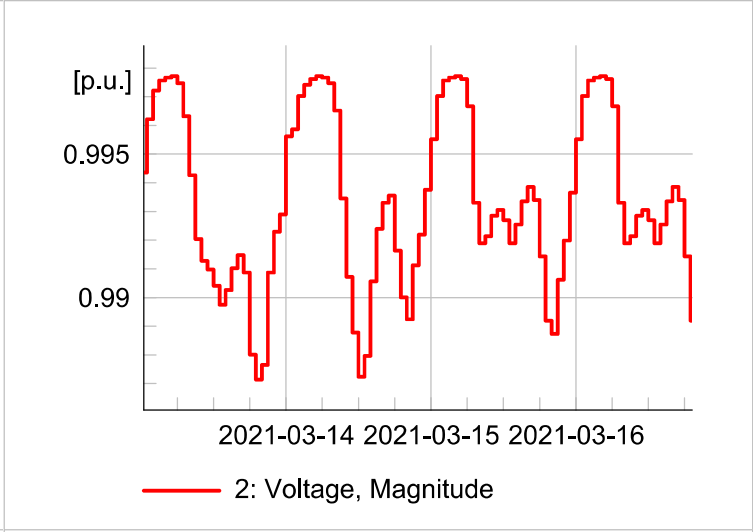

30
[kW]
25
20
15
10
5
2021-04-24
2021-04-26
WR_8: Active Power

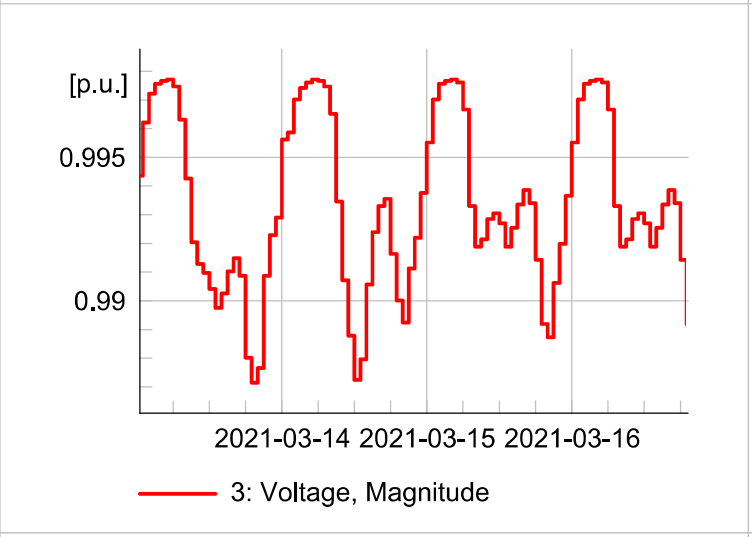

1.02
[p.u.]
1.01
1.00
0.99
0.98
0.97
0.00
100.00
200.00
300.00
400.00
[m]
500.0
0
5
4
3
2
7
8
1
Feeder: Voltage, Magnitude

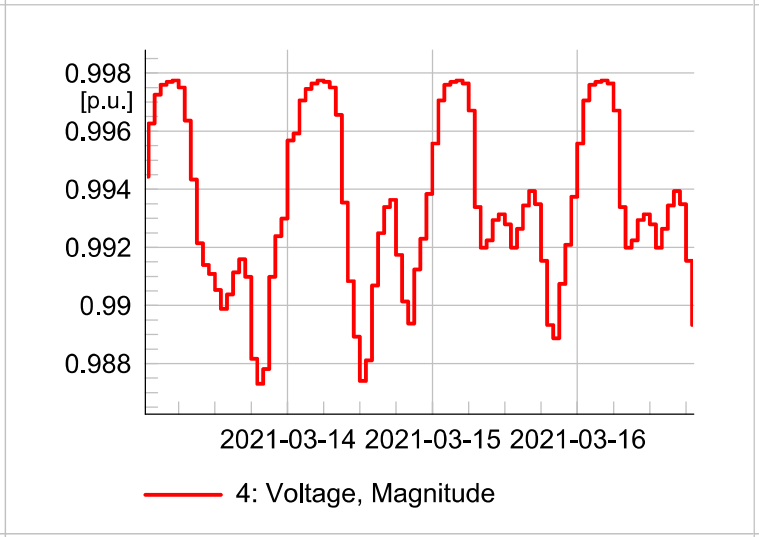

0
0,400
1,00000
0,000
157,826
76,872
0,253
0,899
L-5_0
63,3
WR_5
-156,020
-75,719
0,253
-0,900
19,365
9,621
0,032
0,900
5
0,395
0,28787
-0,082
31,806
15,406
0,052
0,900
104,349
50,892
0,170
0,899
L-4_5
12,9
L-5_6
42,4
WR_4
WR_6
-31,786
-15,394
0,052
-0,900
15,892
7,697
0,026
0,900
-103,918
-50,417
0,170
-0,900
11,919
5,773
0,019
0,900
4
0,395
0,98721
-0,087
6
0,393
0,98354
-0,112
7,947
3,849
0,013
0,900
7,947
3,849
0,013
0,900
76,077
36,932
0,124
0,900
15,922
7,713
0,026
0,900
L-3_4
3,2
L-2_4
3,2
L-7_6
31,0
L-6.1_6
6,5
-7,946
-3,848
0,013
-0,900
-7,946
-3,848
0,013
-0,900
-75,557
-36,602
0,124
-0,900
-15,897
-7,699
0,026
-0,900
3
0,395
0,98705
-0,088
2
0,395
0,98705
-0,088
7
0,391
0,97642
-0,161
7,946
3,848
0,013
0,900
7,946
3,848
0,013
0,900
27,881
13,512
0,046
0,900
47,676
23,091
0,078
0,900
15,897
7,699
0,026
0,900
WR_3
WR_2
WR_7
L-8_7
11,5
L-1_6.1
6,5
-27,811
-13,469
0,046
-0,900
8
0,390
0,97378
-0,179
1
0,393
0,98156
-0,125
-15,892
-7,697
0,026
-0,900
27,811
13,469
0,046
0,900
15,892
7,697
0,026
0,900
WR_8
WR_1

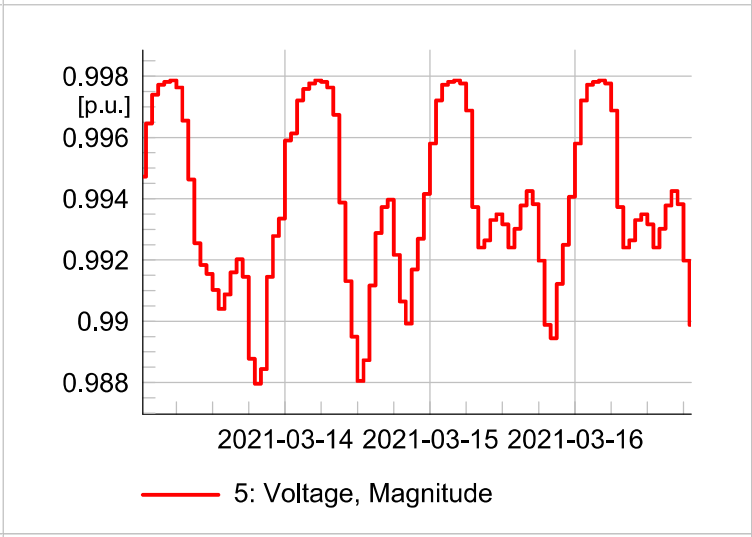

2
[p.u.]
1.5
1
0.5
0
2021-03-14 2021-03-15 2021-03-16
0: Voltage, Magnitude

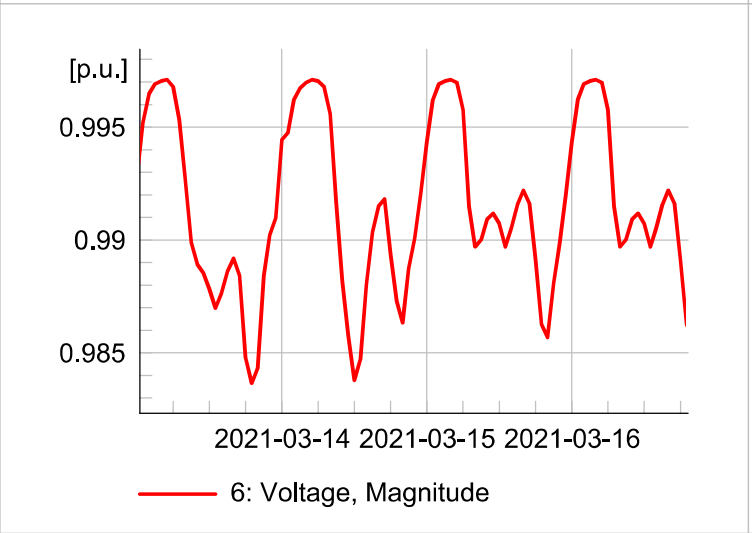

[p.u.]
0.995
0.99
0.985
2021-03-14 2021-03-15 2021-03-16
1: Voltage, Magnitude

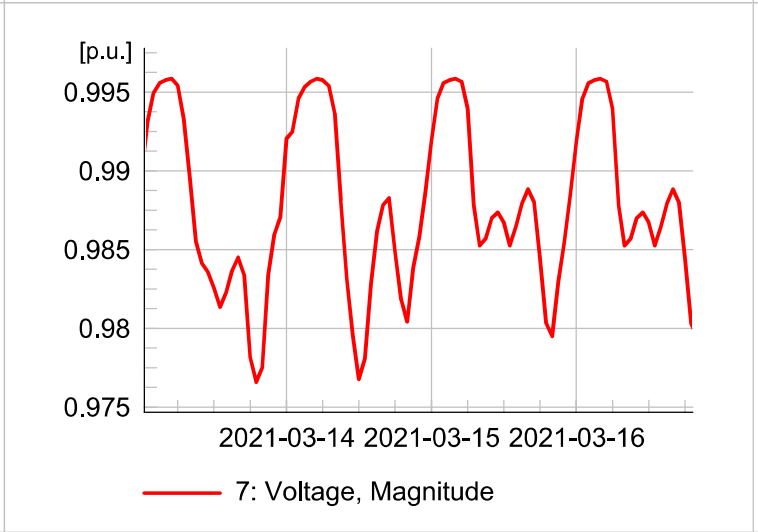

[p.u.]
0.995
0.99
2021-03-14 2021-03-15 2021-03-16
2: Voltage, Magnitude

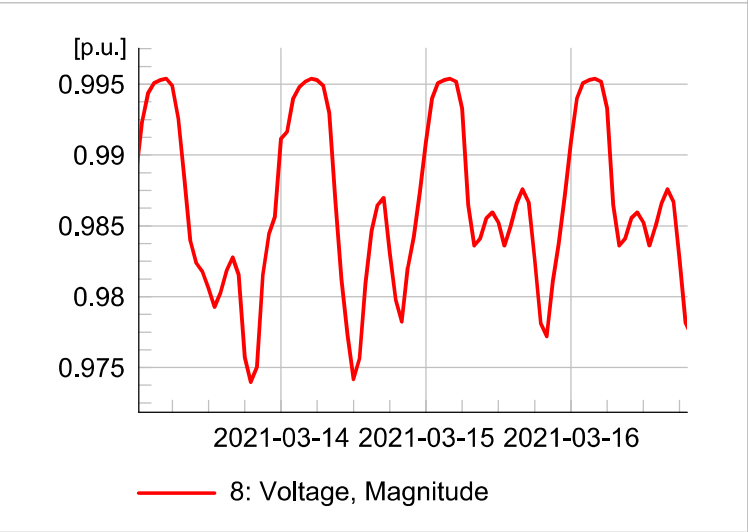

[p.u.]
0.995
0.99
2021-03-14 2021-03-15 2021-03-16
3: Voltage, Magnitude

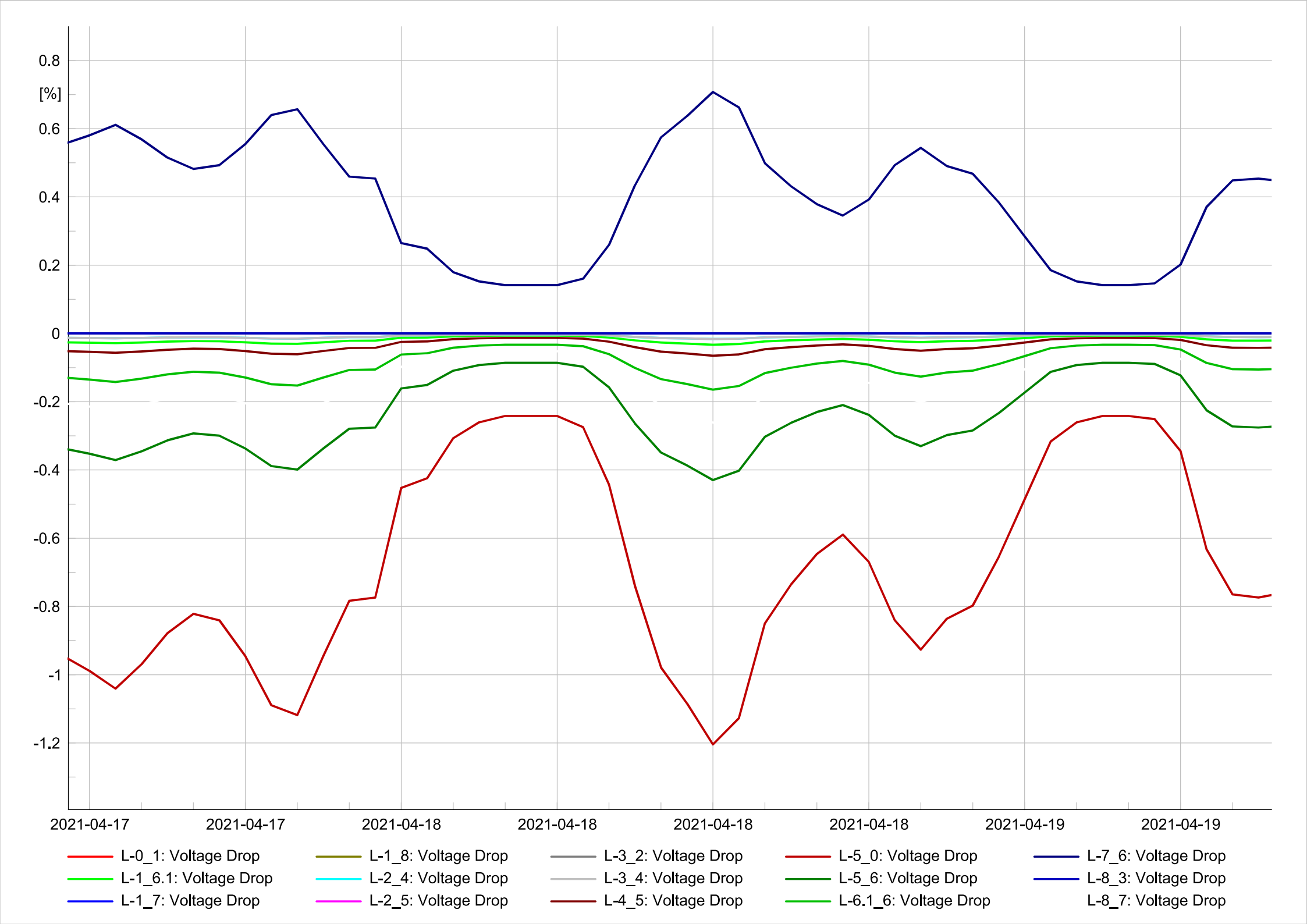

0.998
[p.u.]
0.996
0.994
0.992
0.99
0.988
2021-03-14 2021-03-15 2021-03-16
4: Voltage, Magnitude

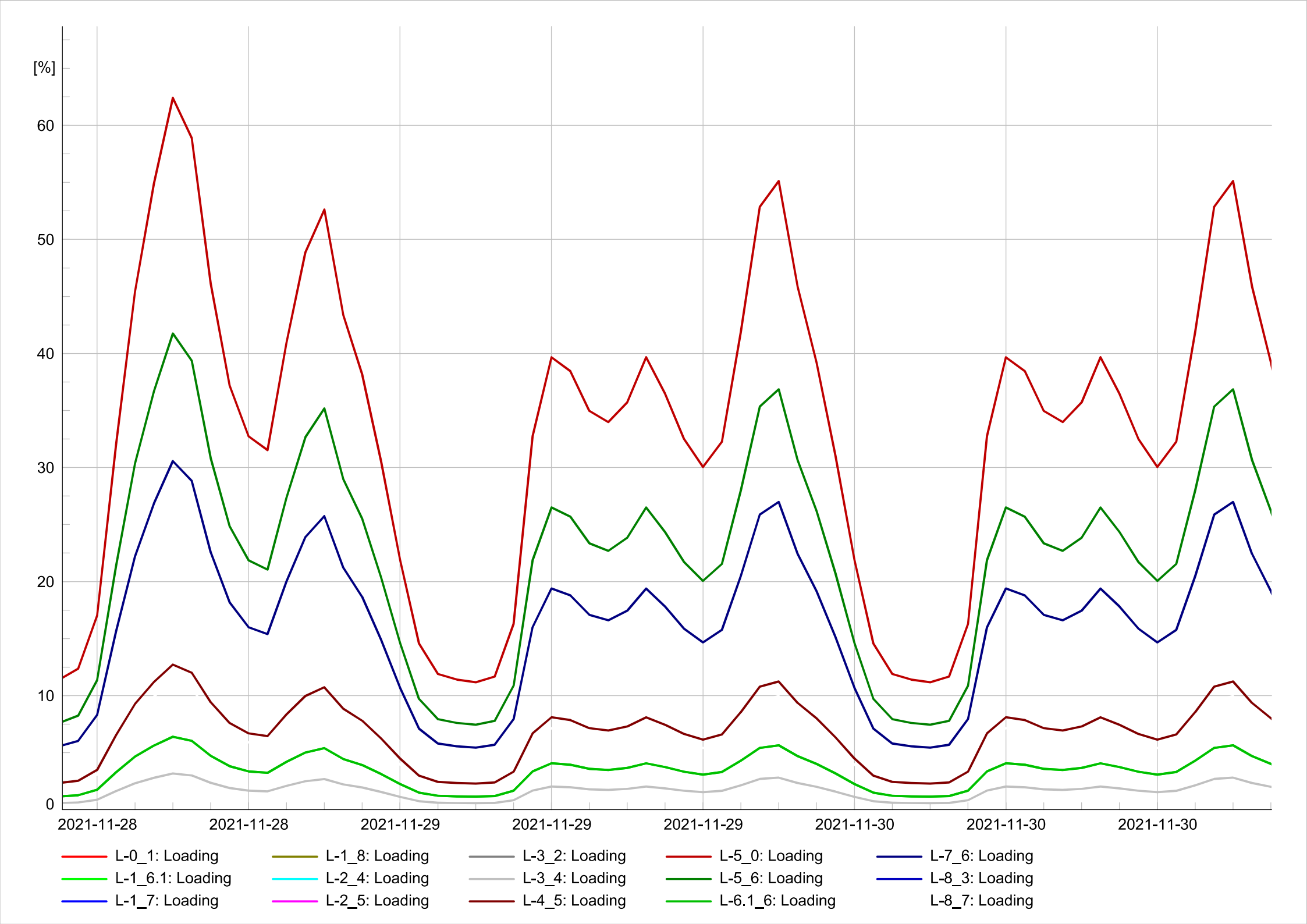

0.998
[p.u.]
0.996
0.994
0.992
0.99
0.988
2021-03-14 2021-03-15 2021-03-16
5: Voltage, Magnitude

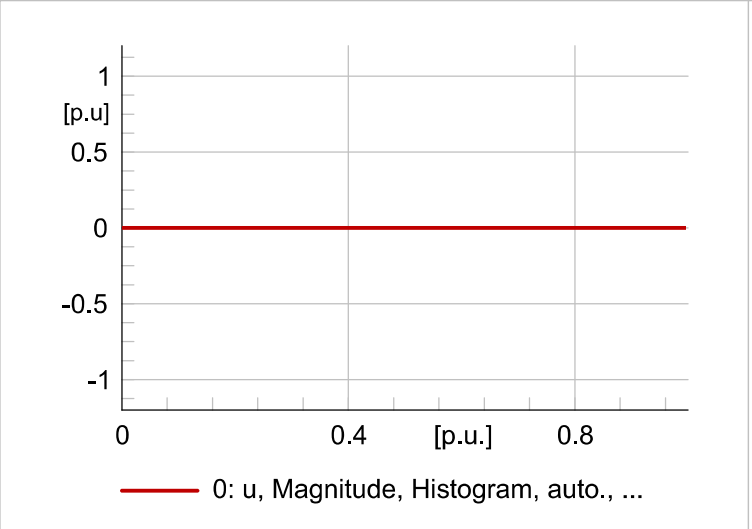

[p.u.]
0.995
0.99
0.985
2021-03-14 2021-03-15 2021-03-16
6: Voltage, Magnitude

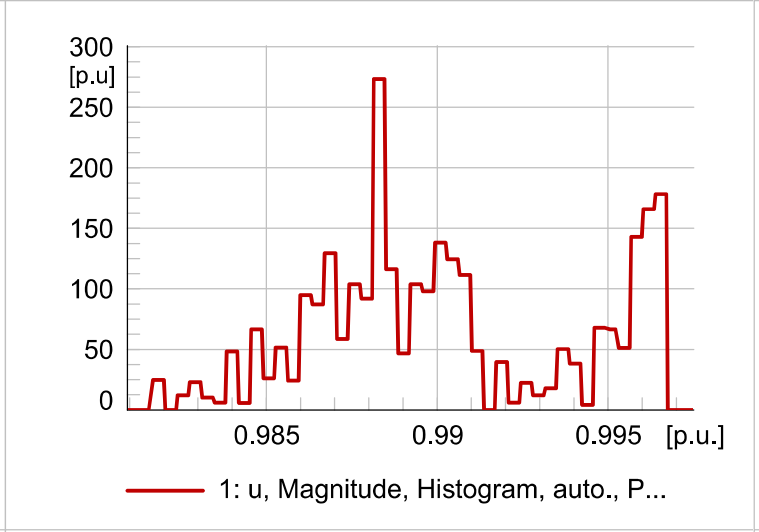

[p.u.]
0.995
0.99
0.985
0.98
0.975
2021-03-14 2021-03-15 2021-03-16
7: Voltage, Magnitude

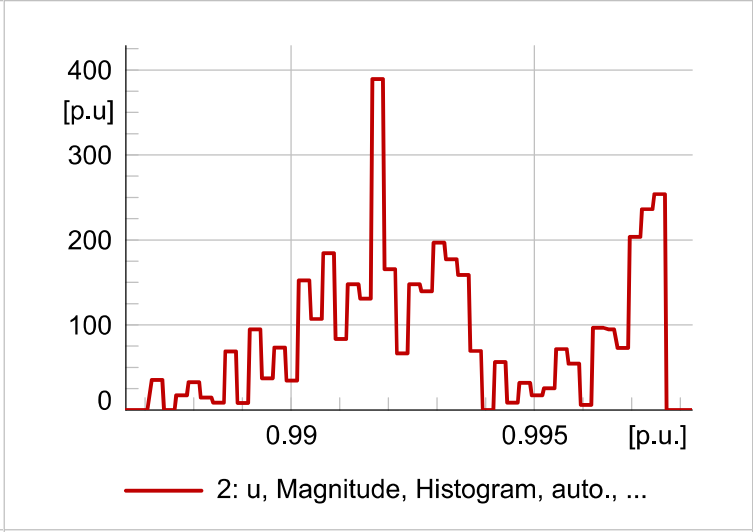

[p.u.]
0.995
0.99
0.985
0.98
0.975
2021-03-14 2021-03-15 2021-03-16
8: Voltage, Magnitude

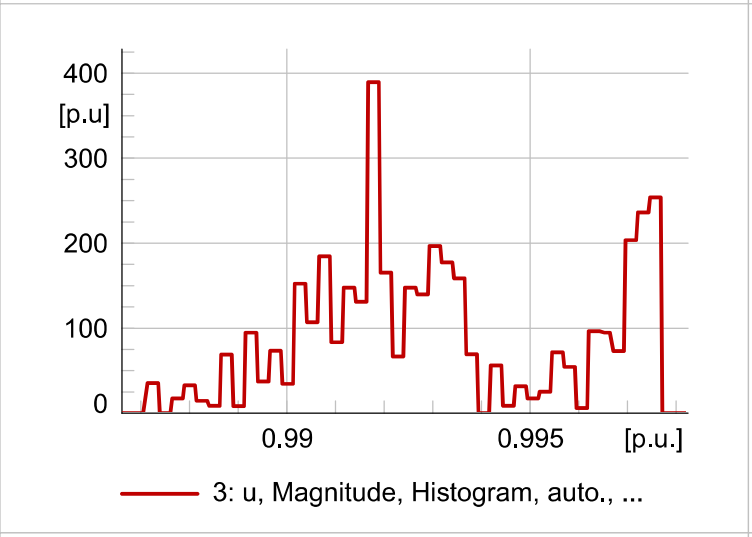

0.8
[%]
0.6
0.4
0.2
0
-0.2
-0.4
-0.6
-0.8
-1
-1.2
2021-04-17
2021-04-17
2021-04-18
2021-04-18
2021-04-18
2021-04-18
2021-04-19
2021-04-19
L-0_1: Voltage Drop
L-1_8: Voltage Drop
L-3_2: Voltage Drop
L-5_0: Voltage Drop
L-7_6: Voltage Drop
L-1_6.1: Voltage Drop
L-2_4: Voltage Drop
L-3_4: Voltage Drop
L-5_6: Voltage Drop
L-8_3: Voltage Drop
L-1_7: Voltage Drop
L-2_5: Voltage Drop
L-4_5: Voltage Drop
L-6.1_6: Voltage Drop
L-8_7: Voltage Drop

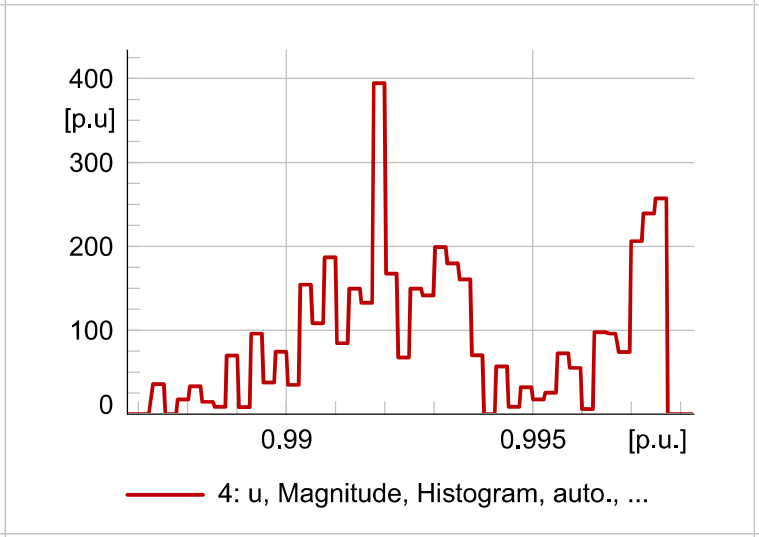

[%]
60
50
40
30
20
10
0
2021-11-28
2021-11-28
2021-11-29
2021-11-29
2021-11-29
2021-11-30
2021-11-30
2021-11-30
L-0_1: Loading
L-1_1: Loading
L-1_6.1: Loading
L-1_7: Loading
L-1_8: Loading
L-2_4: Loading
L-2_5: Loading
L-3_2: Loading
L-3_4: Loading
L-4_5: Loading
L-5_0: Loading
L-5_6: Loading
L-6.1_6: Loading
L-7_6: Loading
L-8_3: Loading
L-8_7: Loading

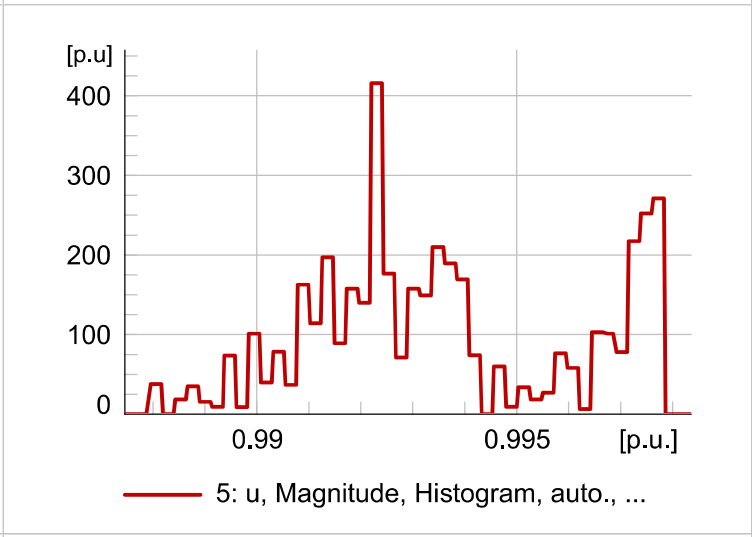

1
[p.u]
0.5
0
-0.5
-1
0
0.4
[p.u.]
0.8
0: u, Magnitude, Histogram, auto., ...

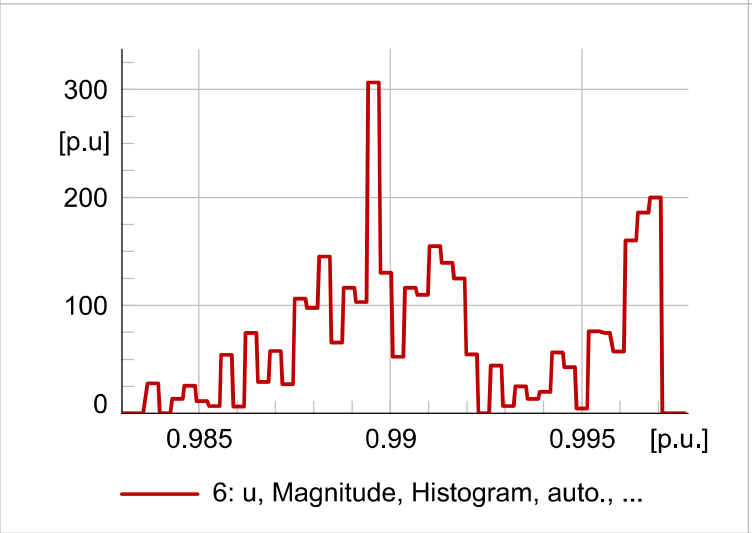

300
[p.u]
250
200
150
100
50
0
0.985
0.99
0.995
[p.u.]
1: u, Magnitude, Histogram, auto., P...

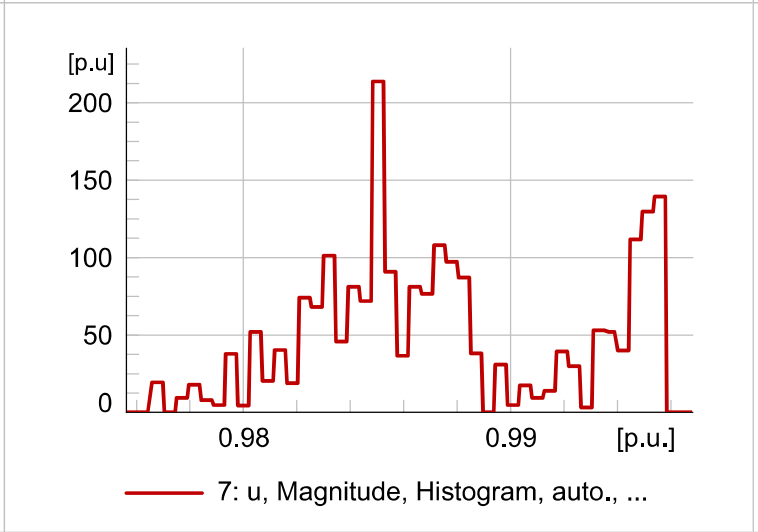

400
[p.u]
300
200
100
0
0.99
0.995
[p.u.]
2: u, Magnitude, Histogram, auto., ...

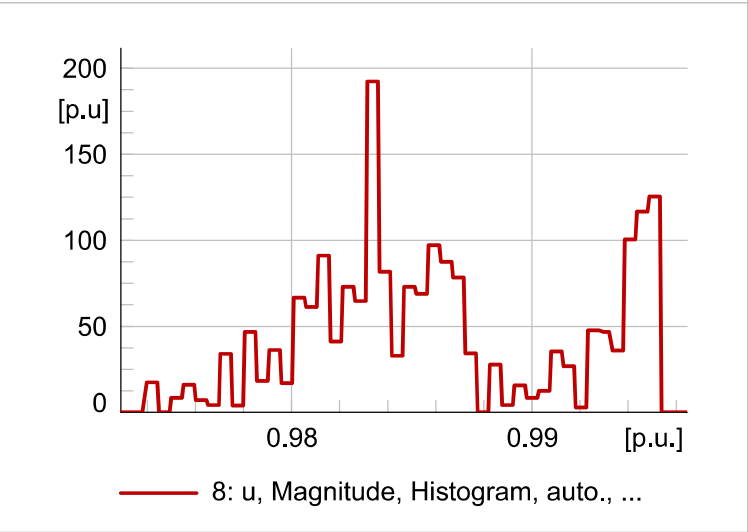

400
[p.u]
300
200
100
0
0.99
0.995
[p.u.]
3: u, Magnitude, Histogram, auto., ...

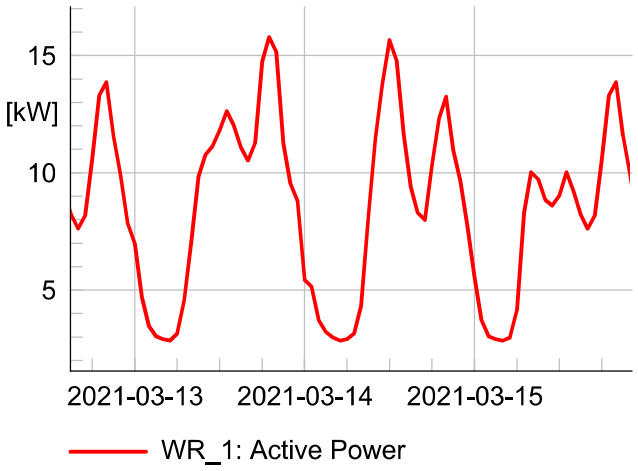

400
[p.u]
300
200
100
0
0.99
0.995
[p.u.]
4: u, Magnitude, Histogram, auto., ...

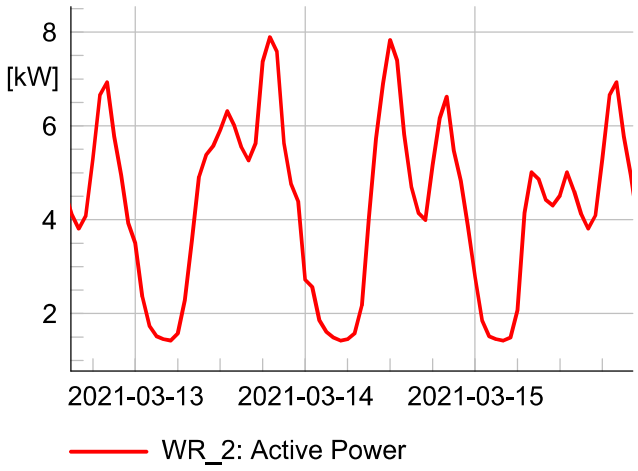

[p.u]
400
300
200
100
0
0.99
0.995
[p.u.]
5: u, Magnitude, Histogram, auto., ...

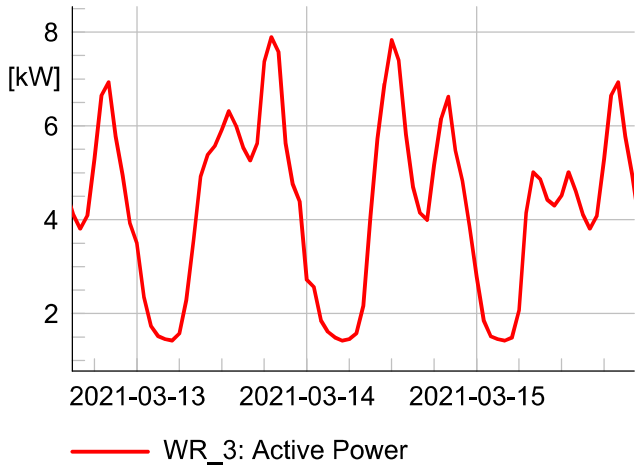

300
[p.u]
200
100
0
0.985
0.99
0.995
[p.u.]
6: u, Magnitude, Histogram, auto., ...

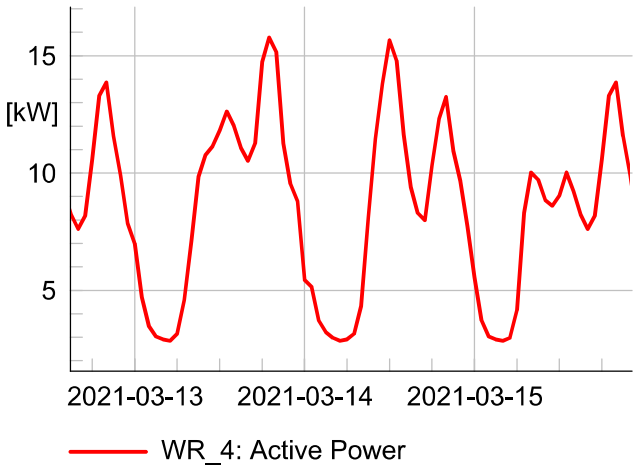

[p.u]
200
150
100
50
0
0.98
0.99
[p.u.]
7: u, Magnitude, Histogram, auto., ...

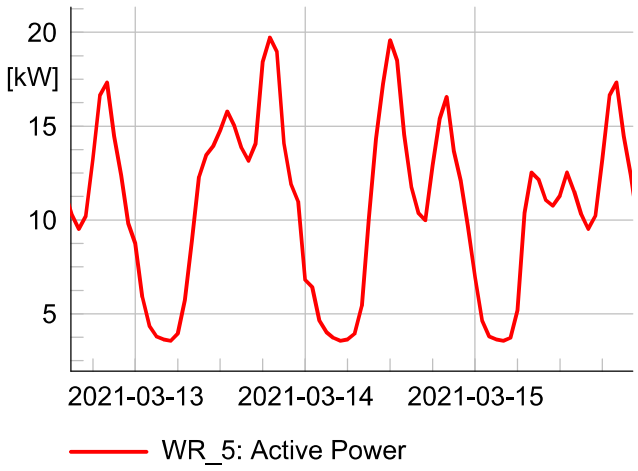

200
[p.u]
150
100
50
0
0.98
0.99
[p.u.]
8: u, Magnitude, Histogram, auto., ...

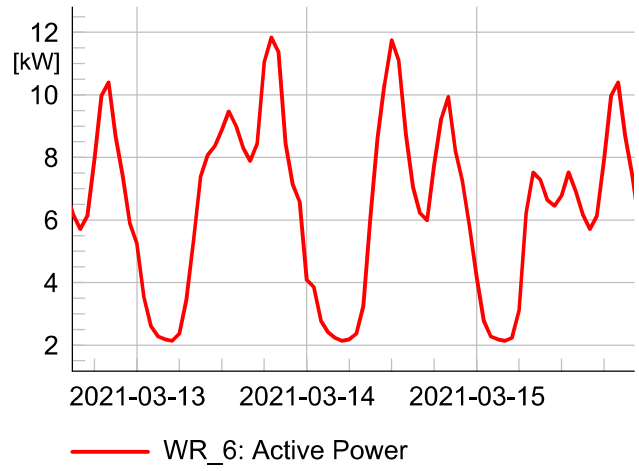

15
[kW]
10
5
2021-03-13
2021-03-14
2021-03-15
WR_1: Active Power

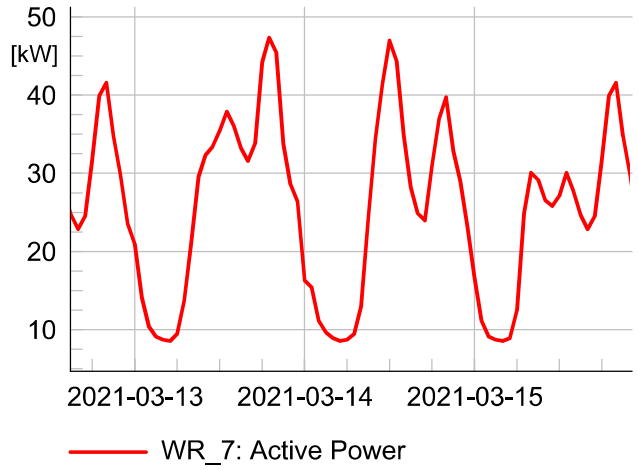

8
[kW]
6
4
2
2021-03-13
2021-03-14
2021-03-15
WR_2: Active Power

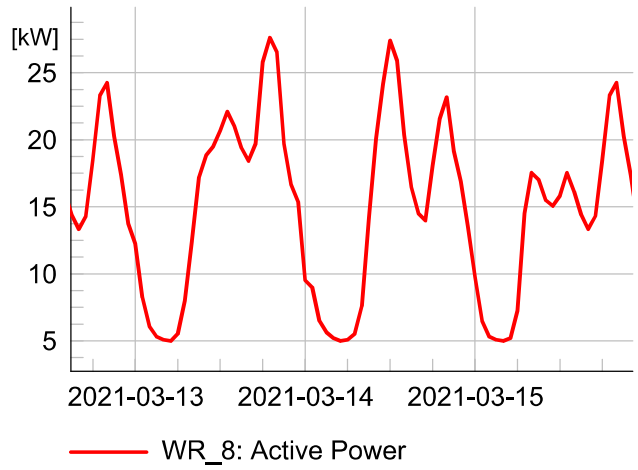

8
[kW]
6
4
2
2021-03-13
2021-03-14
2021-03-15
WR_3: Active Power

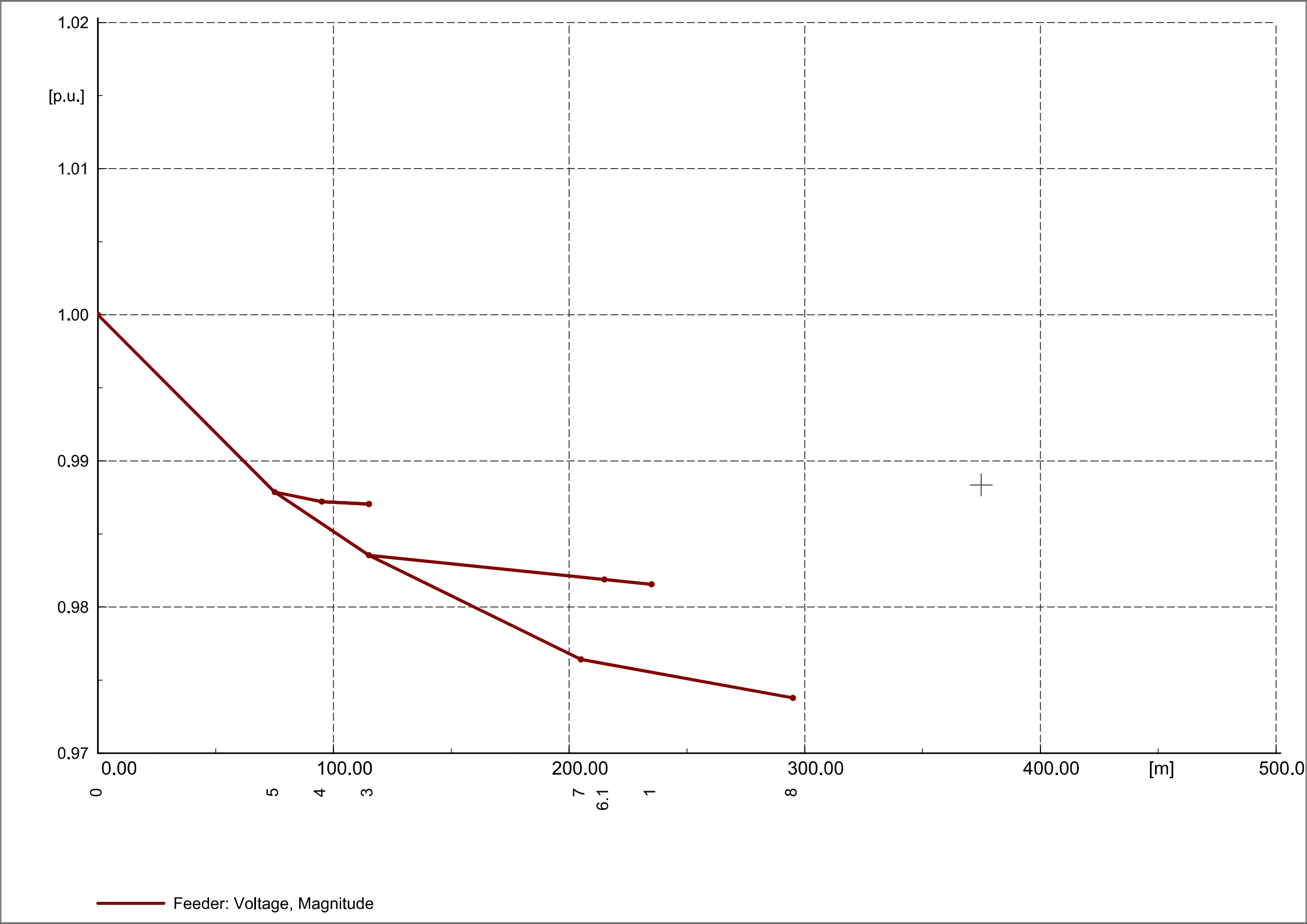

15
[kW]
10
5
2021-03-13
2021-03-14
2021-03-15
WR_4: Active Power


20
[kW]
15
10
5
2021-03-13
2021-03-14
2021-03-15
WR_5: Active Power


12
[kW]
10
8
6
4
2
2021-03-13
2021-03-14
2021-03-15
WR_6: Active Power


50
[kW]
40
30
20
10
2021-03-13
2021-03-14
2021-03-15
WR_7: Active Power


[kW]
25
20
15
10
5
2021-03-13
2021-03-14
2021-03-15
WR_8: Active Power


1.02
[p.u.]
1.01
1.00
0.99
0.98
0.97
0.00
100.00
200.00
300.00
400.00
[m]
500.0
0
5
4
3
7
6.1
1
8
Feeder: Voltage, Magnitude

A3: Einstellungen für das Labor

Auszug aus dem Szenarienkatalog (S.30 - S.57)

https://eit.h-da.de/smartgridlabhessen/nachrichten?tx_news_pi1%5Baction%5D=detail&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Bnews%5D=3182&cHash=dbba3b806a66ecbd03a428e5d196ea8a

6.1 Land 1

6.1.1 2020

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	1	EFH1.1	6	1,4						
NA 1 - gesamt	1	1								
NA 6	1	EFH6.1	1	3,24						
NA 6 - gesamt	1	1								
NA 7	1	EFH7.1	74	4,27						
NA 7 - gesamt	1	1								

Tabelle 45: finale Parameter für die Lastkurven zu 2020 – Land 1.

6.1.2 2030

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	1	EFH1.1	6	1,4						
NA 1 - gesamt	1	1								
NA 6	1	EFH6.1	1	3,24						
NA 6 - gesamt	1	1								
NA 7	1	EFH7.1	74	4,27	8,6					
NA 7 - gesamt	1	1								

Tabelle 46: finale Parameter für die Lastkurven zu 2030 – Land 1.

6.1.3 2045

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	1	EFH1.1	6	1,4						11
NA 1 - gesamt	1	1								
NA 6	1	EFH6.1	1	3,24				12,5	3	
NA 6 - gesamt	1	1								
NA 7	1	EFH7.1	74	4,27	8,6	7	7,2			
NA 7 - gesamt	1	1								

Tabelle 47: finale Parameter für die Lastkurven zu 2045 – Land 1.

6.1.4 Vollausbau

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	1	EFH1.1	6	1,4	9,5	5,9	7,8	11,5	3,2	11
NA 1 - gesamt	1	1								
NA 6	1	EFH6.1	1	3,24	9,0	6	8	12,5	3	11
NA 6 - gesamt	1	1								
NA 7	1	EFH7.1	74	4,27	8,6	6,2	8,2	13	3	11
NA 7 - gesamt	1	1								

Tabelle 48: finale Parameter für die Lastkurven zu Vollausbau – Land 1.

6.2 Land 2

6.2.1 2020

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 5	1	EFH5.1	4	2,66						
NA 5 - gesamt	1	1								
NA 6	1	EFH6.1	22	4,04						
NA 6 - gesamt	1	1								
NA 7	1	EFH7.1	72	4,84						
NA 7 - gesamt	1	1								
NA 8		EFH8.1	58	4,98						
NA 8 - gesamt	1	1								

Tabelle 49: finale Parameter für die Lastkurven zu 2020 – Land 2.

6.2.2 2030

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 5	1	EFH5.1	4	2,66	8,9					11
NA 5 - gesamt	1	1								
NA 6	1	EFH6.1	22	4,04						
NA 6 - gesamt	1	1								
NA 7	1	EFH7.1	72	4,84						
NA 7 - gesamt	1	1								
NA 8		EFH8.1	58	4,98						
NA 8 - gesamt	1	1								

Tabelle 50: finale Parameter für die Lastkurven zu 2030 – Land 2.

6.2.3 2045

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 5	1	EFH5.1	4	2,66	8,9			11	3	
NA 5 - gesamt	1	1								
NA 6	1	EFH6.1	22	4,04	9	6,7	7,5	12	3,2	11
NA 6 - gesamt	1	1								
NA 7	1	EFH7.1	72	4,84						
NA 7 - gesamt	1	1								
NA 8		EFH8.1	58	4,98						
NA 8 - gesamt	1	1								

Tabelle 51: finale Parameter für die Lastkurven zu 2045 – Land 2.

6.2.4 Vollausbau

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 5	1	EFH5.1	4	2,66	8,9	5,5	7,7	11	3	11
NA 5 - gesamt	1	1								
NA 6	1	EFH6.1	22	4,04	9	6	8	12	3,2	11
NA 6 - gesamt	1	1								
NA 7	1	EFH7.1	72	4,84	9,6	6,2	8,2	14	3,5	11
NA 7 - gesamt	1	1								
NA 8		EFH8.1	58	4,98	9,7	6,3	8,2	13,6	3,1	11
NA 8 - gesamt	1	1								

Tabelle 52: finale Parameter für die Lastkurven zu Vollausbau – Land 2.

6.3 Dorf 1

6.3.1 2020

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	1	EFH1.1	6	1,4						
NA 1 - gesamt		1								
NA 2	1	EFH2.1	2	4,5						
NA 2 - gesamt	1	1								
NA 3	1	EFH3.1	61	4,57						
NA 3	2	ZFH3.2.1	8	5,18						
NA 3		ZFH3.2.2	5	3,2						
NA 3 - gesamt	3	2								
NA 4	1	EFH4.1	66	3,62						
NA 4 - gesamt	1	1								
NA 5	1	EFH5.1	22	4,04						
NA 5 - gesamt	1	1								
NA 6	1	EFH6.2	16	3,2						
NA 6	1	EFH6.3	73	4,34	6,9			12	3	
NA 6	1	EFH6.4	39	5,17						
NA 6	1	EFH6.5	55	4,78						
NA 6	3	MFH6.1.1	1	3,24						
NA 6		MFH6.1.2	23	7,5						
NA 6		MFH6.1.3	32	5,32						
NA 6 - gesamt	7	5								
NA 7	1	EFH7.1	74	4,27						
NA 7	1	EFH7.2	22	4,04						
NA 7	1	EFH7.3	7	2,94						
NA 7	1	EFH7.4	31	5,01						
NA 7 - gesamt	4	4								
NA 8	1	EFH8.1	3	6,62						
NA 8	1	EFH8.2	19	5,49	7,5					
NA 8	2	ZFH8.3.1	71	4,32						
NA 8		ZFH8.3.2	41	5,52						
NA 8 - gesamt	4	3								

Tabelle 53: finale Parameter für die Lastkurven zu 2020 – Dorf 1.

6.3.2 2030

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	1	EFH1.1	6	1,4	8,2	5,3	7,2	13	3,1	11
NA 1 - gesamt		1								
NA 2	1	EFH2.1	2	4,5						
NA 2 - gesamt	1	1								
NA 3	1	EFH3.1	61	4,57						
NA 3	2	ZFH3.2.1	8	5,18	8,4			18	3	
NA 3		ZFH3.2.2	5	3,2						
NA 3 - gesamt	3	2								
NA 4	1	EFH4.1	66	3,62						
NA 4 - gesamt	1	1								
NA 5	1	EFH5.1	22	4,04	8,3	5,5	7,5			11
NA 5 - gesamt	1	1								
NA 6	1	EFH6.2	16	3,2						
NA 6	1	EFH6.3	73	4,34	6,9			12	3	11
NA 6	1	EFH6.4	39	5,17						
NA 6	1	EFH6.5	55	4,78						
NA 6	3	MFH6.1.1	1	3,24						
NA 6		MFH6.1.2	23	7,5						
NA 6		MFH6.1.3	32	5,32						
NA 6 - gesamt	7	5								
NA 7	1	EFH7.1	74	4,27						
NA 7	1	EFH7.2	22	4,04						
NA 7	1	EFH7.3	7	2,94						
NA 7	1	EFH7.4	31	5,01						
NA 7 - gesamt	4	4								
NA 8	1	EFH8.1	3	6,62						
NA 8	1	EFH8.2	19	5,49	7,5					11
NA 8	2	ZFH8.3.1	71	4,32						
NA 8		ZFH8.3.2	41	5,52						
NA 8 - gesamt	4	3								

Tabelle 54: finale Parameter für die Lastkurven zu 2030 – Dorf 1.

6.3.3 2045

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	1	EFH1.1	6	1,4	8,2	5,6	7	13	3,1	11
NA 1 - gesamt		1								
NA 2	1	EFH2.1	2	4,5	9,1	7	7,6	11	3,5	11
NA 2 - gesamt	1	1								
NA 3	1	EFH3.1	61	4,57						
NA 3	2	ZFH3.2.1	8	5,18	8,4	7	7,8	18	3	11
NA 3		ZFH3.2.2	5	3,2						
NA 3 - gesamt	3	2								
NA 4	1	EFH4.1	66	3,62						
NA 4 - gesamt	1	1								
NA 5	1	EFH5.1	22	4,04	8,3	7	7,5	14	3,3	11
NA 5 - gesamt	1	1								
NA 6	1	EFH6.2	16	3,2						
NA 6	1	EFH6.3	73	4,34	6,9			12	3	11
NA 6	1	EFH6.4	39	5,17						
NA 6	1	EFH6.5	55	4,78	8,8					11
NA 6	3	MFH6.1.1	1	3,24						
NA 6		MFH6.1.2	23	7,5						
NA 6		MFH6.1.3	32	5,32						
NA 6 - gesamt	7	5								
NA 7	1	EFH7.1	74	4,27						11
NA 7	1	EFH7.2	22	4,04						
NA 7	1	EFH7.3	7	2,94						
NA 7	1	EFH7.4	31	5,01	9,2	7,2	7,7	13	3,5	11
NA 7 - gesamt	4	4								
NA 8	1	EFH8.1	3	6,62	9,3					
NA 8	1	EFH8.2	19	5,49	7,5			12,8	3	11
NA 8	2	ZFH8.3.1	71	4,32						11
NA 8		ZFH8.3.2	41	5,52						
NA 8 - gesamt	4	3								

Tabelle 55: finale Parameter für die Lastkurven zu 2045 – Dorf 1.

6.3.4 Vollausbau

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	1	EFH1.1	6	1,4	8,2	5,3	7,5	13	3,1	11
NA 1 - gesamt		1								
NA 2	1	EFH2.1	2	4,5	9,1	6	8,2	11	3,5	11
NA 2 - gesamt	1	1								
NA 3	1	EFH3.1	61	4,57	9,2	6,3	8,5	13	3,3	11
NA 3	2	ZFH3.2.1	8	5,18	8,4	8	10	18	3	11
NA 3		ZFH3.2.2	5	3,2						
NA 3 - gesamt	3	2								
NA 4	1	EFH4.1	66	3,62	9,1	5,1	7,7	12,1	3,1	11
NA 4 - gesamt	1	1								
NA 5	1	EFH5.1	22	4,04	8,3	5,5	8	14	3,3	11
NA 5 - gesamt	1	1								
NA 6	1	EFH6.2	16	3,2	8,9	6	8	11,8	3	11
NA 6	1	EFH6.3	73	4,34	6,9	6,2	8,3	12	3	11
NA 6	1	EFH6.4	39	5,17	9	7	9	13,5	3,1	11
NA 6	1	EFH6.5	55	4,78	8,8	6,6	8,5	13	3,2	11
NA 6	3	MFH6.1.1	1	3,24	9,8	8,5	11	32	3,3	11
NA 6		MFH6.1.2	23	7,5						
NA 6		MFH6.1.3	32	5,32						
NA 6 - gesamt	7	5								
NA 7	1	EFH7.1	74	4,27	9,3	6,2	8,2	13,2	3	11
NA 7	1	EFH7.2	22	4,04	9,1	6	8	12,8	3,2	11
NA 7	1	EFH7.3	7	2,94	8,9	5,7	7,8	12	3,3	11
NA 7	1	EFH7.4	31	5,01	9,2	6,3	8,5	13	3,5	11
NA 7 - gesamt	4	4								
NA 8	1	EFH8.1	3	6,62	9,3	6,5	8,9	14	3,1	11
NA 8	1	EFH8.2	19	5,49	7,5	6,4	8,7	12,8	3	11
NA 8	2	ZFH8.3.1	71	4,32	9,3	6,3	8,5	18	3,2	11
NA 8		ZFH8.3.2	41	5,52						
NA 8 - gesamt	4	3								

Tabelle 56: finale Parameter für die Lastkurven zu Vollausbau – Dorf 1.

6.4 Dorf 2

6.4.1 2020

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	1	EFH1.1	1	3,24						
NA 1 - gesamt	1	1								
NA 2	1	EFH2.1	3	6,62	7			18	3,2	
NA 2	1	EFH2.2	6	1,4						
NA 2 - gesamt	2	2								
NA 5	1	EFH5.1	22	4,04						
NA 5 - gesamt	1	1								
NA 6	1	EFH6.1	70	6,22						
NA 6	2	ZFH6.3.1	44	2,63						
NA 6		ZFH6.3.2	10	3,37						
NA 6	4	MFH6.2.1	74	4,27						
NA 6		MFH6.2.2	7	2,94						
NA 6		MFH6.2.3	33	3,43						
NA 6		MFH6.2.4	66	3,62						
NA 6 - gesamt	7	3								
NA 7	1	EFH7.1	21	6,9						
NA 7	1	EFH7.2	31	5,01						
NA 7	1	EFH7.3	30	4,7						
NA 7	1	EFH7.4	20	4,95						
NA 7	1	EFH7.5	46	8,63						
NA 7	2	ZFH7.6.1	45	4,95						
NA 7		ZFH7.6.2	60	4,49						
NA 7 - gesamt	7	6								
NA 8	1	EFH8.1	71	4,32						
NA 8	1	EFH8.2	41	5,52						
NA 8	1	EFH8.3	19	5,49						
NA 8	1	EFH8.4	9	8						
NA 8 - gesamt	4	4								

Tabelle 57: finale Parameter für die Lastkurven zu 2020 – Dorf 2.

6.4.2 2030

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	1	EFH1.1	1	3,24	8,4	5,3	7			11
NA 1 - gesamt	1	1								
NA 2	1	EFH2.1	3	6,62	7			18	3,2	11
NA 2	1	EFH2.2	6	1,4						
NA 2 - gesamt	2	2								
NA 5	1	EFH5.1	22	4,04	8,5	5,7	7,2	12	3	11
NA 5 - gesamt	1	1								
NA 6	1	EFH6.1	70	6,22						
NA 6	2	ZFH6.3.1	44	2,63	8,9					11
NA 6		ZFH6.3.2	10	3,37						
NA 6	4	MFH6.2.1	74	4,27						
NA 6		MFH6.2.2	7	2,94						
NA 6		MFH6.2.3	33	3,43						
NA 6		MFH6.2.4	66	3,62						
NA 6 - gesamt	7	3								
NA 7	1	EFH7.1	21	6,9						
NA 7	1	EFH7.2	31	5,01						
NA 7	1	EFH7.3	30	4,7						
NA 7	1	EFH7.4	20	4,95						
NA 7	1	EFH7.5	46	8,63						
NA 7	2	ZFH7.6.1	45	4,95						
NA 7		ZFH7.6.2	60	4,49						
NA 7 - gesamt	7	6								
NA 8	1	EFH8.1	71	4,32						
NA 8	1	EFH8.2	41	5,52						
NA 8	1	EFH8.3	19	5,49						
NA 8	1	EFH8.4	9	8						
NA 8 - gesamt	4	4								

Tabelle 58: finale Parameter für die Lastkurven zu 2030 – Dorf 2.

6.4.3 2045

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	1	EFH1.1	1	3,24	8,4	6,9	7,4			11
NA 1 - gesamt	1	1								
NA 2	1	EFH2.1	3	6,62	7			18	3,2	11
NA 2	1	EFH2.2	6	1,4						
NA 2 - gesamt	2	2								
NA 5	1	EFH5.1	22	4,04	8,5			12	3	11
NA 5 - gesamt	1	1								
NA 6	1	EFH6.1	70	6,22						
NA 6	2	ZFH6.3.1	44	2,63	8,9			21	3,4	11
NA 6		ZFH6.3.2	10	3,37						
NA 6	4	MFH6.2.1	74	4,27	9,2	7	7,7	40	3	11
NA 6		MFH6.2.2	7	2,94						
NA 6		MFH6.2.3	33	3,43						
NA 6		MFH6.2.4	66	3,62						
NA 6 - gesamt	7	3								
NA 7	1	EFH7.1	21	6,9						
NA 7	1	EFH7.2	31	5,01	9	7,2	7,5	13	3,5	11
NA 7	1	EFH7.3	30	4,7						
NA 7	1	EFH7.4	20	4,95	8,9					11
NA 7	1	EFH7.5	46	8,63						
NA 7	2	ZFH7.6.1	45	4,95						
NA 7		ZFH7.6.2	60	4,49						
NA 7 - gesamt	7	6								
NA 8	1	EFH8.1	71	4,32						
NA 8	1	EFH8.2	41	5,52	9,4	7,3	7,7	12,5	3,3	11
NA 8	1	EFH8.3	19	5,49						
NA 8	1	EFH8.4	9	8						11
NA 8 - gesamt	4	4								

Tabelle 59: finale Parameter für die Lastkurven zu 2045 – Dorf 2.

6.4.4 Vollausbau

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	1	EFH1.1	1	3,24	8,4	6	8	12,5	3,1	11
NA 1 - gesamt	1	1								
NA 2	1	EFH2.1	3	6,62	7	6,5	8,5	18	3,2	11
NA 2	1	EFH2.2	6	1,4	7,8	5,7	7	11	3	11
NA 2 - gesamt	2	2								
NA 5	1	EFH5.1	22	4,04	8,5	6,4	8,5	15	3	11
NA 5 - gesamt	1	1								
NA 6	1	EFH6.1	70	6,22	9,3	6,8	8,7	14,5	3,3	11
NA 6	2	ZFH6.3.1	44	2,63	8,9	5,6	7,9	20	3,4	11
NA 6		ZFH6.3.2	10	3,37						
NA 6	4	MFH6.2.1	74	4,27	9,2	9,2	12	39	3	11
NA 6		MFH6.2.2	7	2,94						
NA 6		MFH6.2.3	33	3,43						
NA 6		MFH6.2.4	66	3,62						
NA 6 - gesamt	7	3								
NA 7	1	EFH7.1	21	6,9	9,4	6,5	8,5	13,5	3,2	11
NA 7	1	EFH7.2	31	5,01	9	6,3	8,3	13	3,5	11
NA 7	1	EFH7.3	30	4,7	8,9	6,1	8,2	12,8	3,4	11
NA 7	1	EFH7.4	20	4,95	8,9	6,3	8,5	12	3,1	11
NA 7	1	EFH7.5	46	8,63	9,6	6,6	8,6	14,8	3	11
NA 7	2	ZFH7.6.1	45	4,95	9	7,7	10	17,9	3,2	11
NA 7		ZFH7.6.2	60	4,49						
NA 7 - gesamt	7	6								
NA 8	1	EFH8.1	71	4,32	9,2	6,2	8,3	12,2	3,1	11
NA 8	1	EFH8.2	41	5,52	9,4	6,5	8,5	12,5	3,3	11
NA 8	1	EFH8.3	19	5,49	9,3	6,5	8,6	12,8	3	11
NA 8	1	EFH8.4	9	8	9,3	6,6	9	13,2	3,3	11
NA 8 - gesamt	4	4								

Tabelle 60: finale Parameter für die Lastkurven zu Vollausbau – Dorf 2.

6.5 Vorstadt 1

6.5.1 2020

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat. [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	1	EFH1.1	3	6,62						
NA 1	2	ZFH1.2.1	1	3,24						
NA 1		ZFH1.2.2	2	4,5						
NA 1 - gesamt	3	2								
NA 2	1	EFH2.1	25	5,15						
NA 2	1	EFH2.2	26	4,21	6,8			16	3,3	
NA 2 - gesamt	2	2								
NA 5	1	EFH5.1	21	6,9						
NA 5	2	ZFH5.2.1	22	4,04						
NA 5		ZFH5.2.2	23	7,5						
NA 5 - gesamt	3	2								
NA 6	2	ZFH6.1.1	8	5,18						
NA 6		ZFH6.1.2	9	8						
NA 6	4	MFH6.2.1	4	2,66						
NA 6		MFH6.2.2	5	3,2						
NA 6		MFH6.2.3	6	1,4						
NA 6		MFH6.2.4	7	2,94						
NA 6 - gesamt	6	2								
NA 7	1	EFH7.1	11	3,89						
NA 7	1	EFH7.2	13	4,89						
NA 7	1	EFH7.3	15	3,4						
NA 7	1	EFH7.4	12	4,51						
NA 7	1	EFH7.5	14	3,26						
NA 7 - gesamt	5	5								
NA 8	1	EFH8.1	20	4,95						
NA 8	1	EFH8.2	17	5,92						
NA 8	1	EFH8.3	19	5,49						
NA 8	1	EFH8.4	15	3,4						
NA 8	1	EFH8.5	16	3,2						
NA 8	1	EFH8.6	18	5,74						
NA 8 - gesamt	6	6								

Tabelle 61: finale Parameter für die Lastkurven zu 2020 – Vorstadt 1.

6.5.2 2030

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	1	EFH1.1	3	6,62						
NA 1	2	ZFH1.2.1	1	3,24						
NA 1		ZFH1.2.2	2	4,5						
NA 1 - gesamt	3	2								
NA 2	1	EFH2.1	25	5,15	7,9	5,3	7,5			11
NA 2	1	EFH2.2	26	4,21	6,8			16	3,3	11
NA 2 - gesamt	2	2								
NA 5	1	EFH5.1	21	6,9	8					11
NA 5	2	ZFH5.2.1	22	4,04						
NA 5		ZFH5.2.2	23	7,5						
NA 5 - gesamt	3	2								
NA 6	2	ZFH6.1.1	8	5,18	7,8	6	8	20	3,3	11
NA 6		ZFH6.1.2	9	8						
NA 6	4	MFH6.2.1	4	2,66						
NA 6		MFH6.2.2	5	3,2						
NA 6		MFH6.2.3	6	1,4						
NA 6		MFH6.2.4	7	2,94						
NA 6 - gesamt	6	2								
NA 7	1	EFH7.1	11	3,89						
NA 7	1	EFH7.2	13	4,89						
NA 7	1	EFH7.3	15	3,4						
NA 7	1	EFH7.4	12	4,51						
NA 7	1	EFH7.5	14	3,26						
NA 7 - gesamt	5	5								
NA 8	1	EFH8.1	20	4,95	8,2					11
NA 8	1	EFH8.2	17	5,92						
NA 8	1	EFH8.3	19	5,49						
NA 8	1	EFH8.4	15	3,4						
NA 8	1	EFH8.5	16	3,2						
NA 8	1	EFH8.6	18	5,74						
NA 8 - gesamt	6	6								

Tabelle 62: finale Parameter für die Lastkurven zu 2030 – Vorstadt 1.

6.5.3 2045

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	1	EFH1.1	3	6,62	8,8	7,5	8,7	12	3,5	11
NA 1	2	ZFH1.2.1	1	3,24						11
NA 1		ZFH1.2.2	2	4,5						
NA 1 - gesamt	3	2								
NA 2	1	EFH2.1	25	5,15	7,9	7,2	8,5	13	3	11
NA 2	1	EFH2.2	26	4,21	6,8			16	3,3	11
NA 2 - gesamt	2	2								
NA 5	1	EFH5.1	21	6,9	8			12	3,5	11
NA 5	2	ZFH5.2.1	22	4,04						
NA 5		ZFH5.2.2	23	7,5						
NA 5 - gesamt	3	2								
NA 6	2	ZFH6.1.1	8	5,18	7,8	7	8,6	20	3,3	11
NA 6		ZFH6.1.2	9	8						
NA 6	4	MFH6.2.1	4	2,66						
NA 6		MFH6.2.2	5	3,2						
NA 6		MFH6.2.3	6	1,4						
NA 6		MFH6.2.4	7	2,94						
NA 6 - gesamt	6	2								
NA 7	1	EFH7.1	11	3,89	9			12,5	3	11
NA 7	1	EFH7.2	13	4,89						
NA 7	1	EFH7.3	15	3,4	8,9			14	3,6	11
NA 7	1	EFH7.4	12	4,51						
NA 7	1	EFH7.5	14	3,26						
NA 7 - gesamt	5	5								
NA 8	1	EFH8.1	20	4,95	8,2	7,5	9	11,5	3,2	11
NA 8	1	EFH8.2	17	5,92						
NA 8	1	EFH8.3	19	5,49						
NA 8	1	EFH8.4	15	3,4	8,8					11
NA 8	1	EFH8.5	16	3,2						
NA 8	1	EFH8.6	18	5,74						11
NA 8 - gesamt	6	6								

Tabelle 63: finale Parameter für die Lastkurven zu 2045 – Vorstadt 1.

6.5.4 Vollausbau

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	1	EFH1.1	3	6,62	8,8	7	9	12	3,5	11
NA 1	2	ZFH1.2.1	1	3,24	8,5	7,8	11	17,8	3,1	11
NA 1		ZFH1.2.2	2	4,5						
NA 1 - gesamt	3	2								
NA 2	1	EFH2.1	25	5,15	7,9	6,6	8,7	13	3	11
NA 2	1	EFH2.2	26	4,21	6,8	6,3	8,4	16	3,3	11
NA 2 - gesamt	2	2								
NA 5	1	EFH5.1	21	6,9	8	6,7	8,8	12	3,5	11
NA 5	2	ZFH5.2.1	22	4,04	8,6	7,3	10	18	3	11
NA 5		ZFH5.2.2	23	7,5						
NA 5 - gesamt	3	2								
NA 6	2	ZFH6.1.1	8	5,18	7,8	6,5	8,5	20	3,3	11
NA 6		ZFH6.1.2	9	8						
NA 6	4	MFH6.2.1	4	2,66	8,8	6	8	41	3,2	11
NA 6		MFH6.2.2	5	3,2						
NA 6		MFH6.2.3	6	1,4						
NA 6		MFH6.2.4	7	2,94						
NA 6 - gesamt	6	2								
NA 7	1	EFH7.1	11	3,89	8,6	5,7	7,7	12,5	3	11
NA 7	1	EFH7.2	13	4,89	8,5	6	8	13	3,4	11
NA 7	1	EFH7.3	15	3,4	8,9	5,7	7,7	14	3,6	11
NA 7	1	EFH7.4	12	4,51	8,4	6,2	8,2	13,2	3	11
NA 7	1	EFH7.5	14	3,26	8,6	5,8	7,8	12,4	3,1	11
NA 7 - gesamt	5	5								
NA 8	1	EFH8.1	20	4,95	8,2	6	8,2	11,5	3,2	11
NA 8	1	EFH8.2	17	5,92	8,7	6,5	8,6	12,9	3,2	11
NA 8	1	EFH8.3	19	5,49	8,5	6,8	8,9	12,8	3	11
NA 8	1	EFH8.4	15	3,4	8,8	5,9	8	11,8	3,4	11
NA 8	1	EFH8.5	16	3,2	8	6	8	11,6	3,2	11
NA 8	1	EFH8.6	18	5,74	8,6	7	8,5	12,8	3,1	11
NA 8 - gesamt	6	6								

Tabelle 64: finale Parameter für die Lastkurven zu Vollausbau – Vorstadt 1.

6.6 Vorstadt 2

6.6.1 2020

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	2	ZFH1.1.1	73	4,34						
NA 1		ZFH1.1.2	72	4,84						
NA 1	1	EFH1.2	74	4,27						
NA 1	1	EFH1.3	71	4,32						
NA 1	1	EFH1.4	70	6,22						
NA 1	1	EFH1.5	69	6,94						
NA 1 - gesamt	6	5								
NA 2	1	EFH2.1	51	2,39						
NA 2	1	EFH2.2	50	3,96						
NA 2 - gesamt	2	2								
NA 3	1	EFH3.1	56	5,56	7			13	3,5	
NA 3	1	EFH3.2	55	4,78						
NA 3 - gesamt	2	2								
NA 4	1	EFH4.1	52	4,36						
NA 4	1	EFH4.2	25	5,15						
NA 4 - gesamt	2	2								
NA 5	1	EFH5.1	54	6,09						
NA 5	1	EFH5.2	53	3,39						
NA 5 - gesamt	2	2								
NA 6	1	EFH6.1	68	5,23						
NA 6	1	EFH6.2	67	4,96						
NA 6 - gesamt	2	2								
NA 7	1	EFH7.1	62	5,22						
NA 7	1	EFH7.2	63	6,94						
NA 7	2	ZFH7.3.1	65	6,76						
NA 7		ZFH7.3.2	64	5,95						
NA 7 - gesamt	4	3								
NA 8	5	MFH8.1.1	61	4,57						
NA 8		MFH8.1.2	60	4,49						
NA 8		MFH8.1.3	59	6,54						
NA 8		MFH8.1.4	58	4,98						
NA 8		MFH8.1.5	57	4,29						
NA 8 - gesamt	5	1								

Tabelle 65: finale Parameter für die Lastkurven zu 2020 – Vorstadt 2.

6.6.2 2030

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	2	ZFH1.1.1	73	4,34						
NA 1		ZFH1.1.2	72	4,84						
NA 1	1	EFH1.2	74	4,27						
NA 1	1	EFH1.3	71	4,32						
NA 1	1	EFH1.4	70	6,22	8,1	5,8	7,5	14	3,5	11
NA 1	1	EFH1.5	69	6,94						
NA 1 - gesamt	6	5								
NA 2	1	EFH2.1	51	2,39	7,8					
NA 2	1	EFH2.2	50	3,96						
NA 2 - gesamt	2	2								
NA 3	1	EFH3.1	56	5,56	7			13	3,5	11
NA 3	1	EFH3.2	55	4,78						
NA 3 - gesamt	2	2								
NA 4	1	EFH4.1	52	4,36						
NA 4	1	EFH4.2	25	5,15						
NA 4 - gesamt	2	2								
NA 5	1	EFH5.1	54	6,09						
NA 5	1	EFH5.2	53	3,39	7,2					11
NA 5 - gesamt	2	2								
NA 6	1	EFH6.1	68	5,23						
NA 6	1	EFH6.2	67	4,96						
NA 6 - gesamt	2	2								
NA 7	1	EFH7.1	62	5,22	7,9	5,5	7,7			11
NA 7	1	EFH7.2	63	6,94						11
NA 7	2	ZFH7.3.1	65	6,76						
NA 7		ZFH7.3.2	64	5,95						
NA 7 - gesamt	4	3								
NA 8	5	MFH8.1.1	61	4,57						
NA 8		MFH8.1.2	60	4,49						
NA 8		MFH8.1.3	59	6,54						
NA 8		MFH8.1.4	58	4,98						
NA 8		MFH8.1.5	57	4,29						
NA 8 - gesamt	5	1								

Tabelle 66: finale Parameter für die Lastkurven zu 2030 – Vorstadt 2.

6.6.3 2045

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	2	ZFH1.1.1	73	4,34						
NA 1		ZFH1.1.2	72	4,84						
NA 1	1	EFH1.2	74	4,27	8,6					11
NA 1	1	EFH1.3	71	4,32						
NA 1	1	EFH1.4	70	6,22	8,1	7,4	8,6	14	3,5	11
NA 1	1	EFH1.5	69	6,94						
NA 1 - gesamt	6	5								
NA 2	1	EFH2.1	51	2,39	7,8	7	8,5	13	3,4	11
NA 2	1	EFH2.2	50	3,96						
NA 2 - gesamt	2	2								
NA 3	1	EFH3.1	56	5,56	7			13	3,5	11
NA 3	1	EFH3.2	55	4,78						
NA 3 - gesamt	2	2								
NA 4	1	EFH4.1	52	4,36	8,5	7,5	8,7	14	3,2	11
NA 4	1	EFH4.2	25	5,15						11
NA 4 - gesamt	2	2								
NA 5	1	EFH5.1	54	6,09						
NA 5	1	EFH5.2	53	3,39	7,2			13	3,4	11
NA 5 - gesamt	2	2								
NA 6	1	EFH6.1	68	5,23	8			12,5	3,2	11
NA 6	1	EFH6.2	67	4,96						
NA 6 - gesamt	2	2								
NA 7	1	EFH7.1	62	5,22	7,9	7,1	8,8	12	3	11
NA 7	1	EFH7.2	63	6,94	8,7					11
NA 7	2	ZFH7.3.1	65	6,76						
NA 7		ZFH7.3.2	64	5,95						
NA 7 - gesamt	4	3								
NA 8	5	MFH8.1.1	61	4,57				42	3,3	11
NA 8		MFH8.1.2	60	4,49						
NA 8		MFH8.1.3	59	6,54						
NA 8		MFH8.1.4	58	4,98						
NA 8		MFH8.1.5	57	4,29						
NA 8 - gesamt	5	1								

Tabelle 67: finale Parameter für die Lastkurven zu 2045 – Vorstadt 2.

6.6.4 Vollausbau

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	2	ZFH1.1.1	73	4,34	8,9	6,7	8,8	21	3,3	11
NA 1		ZFH1.1.2	72	4,84						
NA 1	1	EFH1.2	74	4,27	8,6	6,5	8,7	11,9	3	11
NA 1	1	EFH1.3	71	4,32	8,5	6,8	9	12,3	3,1	11
NA 1	1	EFH1.4	70	6,22	8,1	7	9,2	14	3,5	11
NA 1	1	EFH1.5	69	6,94	8,8	7,2	9,5	12,6	3,2	11
NA 1 - gesamt	6	5								
NA 2	1	EFH2.1	51	2,39	7,8	5,6	7,5	13	3,4	11
NA 2	1	EFH2.2	50	3,96	7,9	5,6	7,5	11,5	3	11
NA 2 - gesamt	2	2								
NA 3	1	EFH3.1	56	5,56	7	6,6	8,5	13	3,5	11
NA 3	1	EFH3.2	55	4,78	8	6	8,2	11	3	11
NA 3 - gesamt	2	2								
NA 4	1	EFH4.1	52	4,36	8,5	5,1	8,4	14	3,2	11
NA 4	1	EFH4.2	25	5,15	8,6	5,1	8,6	12	3,2	11
NA 4 - gesamt	2	2								
NA 5	1	EFH5.1	54	6,09	8,9	5,3	8,8	11,8	3,3	11
NA 5	1	EFH5.2	53	3,39	7,2	5,9	7,7	13	3,4	11
NA 5 - gesamt	2	2								
NA 6	1	EFH6.1	68	5,23	8	6,5	8,5	12,5	3,2	11
NA 6	1	EFH6.2	67	4,96	8,2	6,3	8,2	11	3	11
NA 6 - gesamt	2	2								
NA 7	1	EFH7.1	62	5,22	7,9	6,6	8,7	12	3	11
NA 7	1	EFH7.2	63	6,94	8,7	6,8	9	12,5	3,1	11
NA 7	2	ZFH7.3.1	65	6,76	10	8,7	10,5	15	3,2	11
NA 7		ZFH7.3.2	64	5,95						
NA 7 - gesamt	4	3								
NA 8	5	MFH8.1.1	61	4,57	10	9	15,7	49	3,3	11
NA 8		MFH8.1.2	60	4,49						
NA 8		MFH8.1.3	59	6,54						
NA 8		MFH8.1.4	58	4,98						
NA 8		MFH8.1.5	57	4,29						
NA 8 - gesamt	5	1								

Tabelle 68: finale Parameter für die Lastkurven zu Vollausbau – Vorstadt 2.

6.7 Stadt

6.7.1 2020

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	4	MFH1.1.1	49	3,79						
NA 1		MFH1.1.2	48	4,64						
NA 1		MFH1.1.3	47	4,23						
NA 1		MFH1.1.4	46	8,63						
NA 1 - gesamt	4	1								
NA 2	1	EFH2.1	11	3,89						
NA 2	1	EFH2.2	10	3,37						
NA 2 - gesamt	2	2								
NA 3	2	ZFH3.1.1	22	4,04						
NA 3		ZFH3.1.2	21	6,9						
NA 3 - gesamt	2	1								
NA 4	4	MFH4.1.1	15	3,4	6,8			41	3,5	
NA 4		MFH4.1.2	14	3,26						
NA 4		MFH4.1.3	13	4,89						
NA 4		MFH4.1.4	12	4,51						
NA 4 - gesamt	4	1								
NA 5	6	MFH5.1.1	19	5,49						
NA 5		MFH5.1.2	18	5,74						
NA 5		MFH5.1.3	17	5,92						
NA 5		MFH5.1.4	44	2,63						
NA 5		MFH5.1.5	45	4,95						
NA 5		MFH5.1.6	43	2,3						
NA 5 - gesamt	6	1								
NA 6	3	MFH6.1.1	54	6,09						
NA 6		MFH6.1.2	51	2,39						
NA 6		MFH6.1.3	50	3,96						
NA 6 - gesamt	3	1								
NA 7	2	ZFH7.2.1	30	4,7						
NA 7		ZFH7.2.2	29	3,68						
NA 7	10	MFH7.1.1	42	6,04						
NA 7		MFH7.1.2	41	5,52						
NA 7		MFH7.1.3	40	3,77						
NA 7		MFH7.1.4	39	5,17						
NA 7		MFH7.1.5	38	5,56						
NA 7		MFH7.1.6	37	3,47						
NA 7		MFH7.1.7	36	4,15						
NA 7		MFH7.1.8	35	6,69						
NA 7		MFH7.1.9	34	3,08						
NA 7		MFH7.1.10	33	3,43						
NA 7 - gesamt	12	2								

Tabelle 69 (Teil 1): finale Parameter für die Lastkurven zu 2020 – Stadt.

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 8	7	MFH8.1.1	1	3,24						
NA 8		MFH8.1.2	2	4,5						
NA 8		MFH8.1.3	3	6,62						
NA 8		MFH8.1.4	4	2,66						
NA 8		MFH8.1.5	5	3,2						
NA 8		MFH8.1.6	6	1,4						
NA 8		MFH8.1.7	7	2,94						
NA 8 - gesamt	7	1								

Tabelle 69 (Teil 2): finale Parameter für die Lastkurven zu 2020 – Stadt.

6.7.2 2030

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	4	MFH1.1.1	49	3,79						
NA 1		MFH1.1.2	48	4,64						
NA 1		MFH1.1.3	47	4,23						
NA 1		MFH1.1.4	46	8,63						
NA 1 - gesamt	4	1								
NA 2	1	EFH2.1	11	3,89						
NA 2	1	EFH2.2	10	3,37						
NA 2 - gesamt	2	2								
NA 3	2	ZFH3.1.1	22	4,04	7,4	5,7	7,5			11
NA 3		ZFH3.1.2	21	6,9						
NA 3 - gesamt	2	1								
NA 4	4	MFH4.1.1	15	3,4	6,8			41	3,5	
NA 4		MFH4.1.2	14	3,26						
NA 4		MFH4.1.3	13	4,89						
NA 4		MFH4.1.4	12	4,51						
NA 4 - gesamt	4	1								
NA 5	6	MFH5.1.1	19	5,49						
NA 5		MFH5.1.2	18	5,74						
NA 5		MFH5.1.3	17	5,92						
NA 5		MFH5.1.4	44	2,63						
NA 5		MFH5.1.5	45	4,95						
NA 5		MFH5.1.6	43	2,3						
NA 5 - gesamt	6	1								
NA 6	3	MFH6.1.1	54	6,09						
NA 6		MFH6.1.2	51	2,39						
NA 6		MFH6.1.3	50	3,96						
NA 6 - gesamt	3	1								
NA 7	2	ZFH7.2.1	30	4,7	7					11
NA 7		ZFH7.2.2	29	3,68						
NA 7	10	MFH7.1.1	42	6,04						
NA 7		MFH7.1.2	41	5,52						
NA 7		MFH7.1.3	40	3,77						
NA 7		MFH7.1.4	39	5,17						
NA 7		MFH7.1.5	38	5,56						
NA 7		MFH7.1.6	37	3,47						
NA 7		MFH7.1.7	36	4,15						
NA 7		MFH7.1.8	35	6,69						
NA 7		MFH7.1.9	34	3,08						
NA 7		MFH7.1.10	33	3,43						
NA 7 - gesamt	12	2								

Tabelle 70 (Teil 1): finale Parameter für die Lastkurven zu 2030 – Stadt.

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 8	7	MFH8.1.1	1	3,24						
NA 8		MFH8.1.2	2	4,5						
NA 8		MFH8.1.3	3	6,62						
NA 8		MFH8.1.4	4	2,66						
NA 8		MFH8.1.5	5	3,2						
NA 8		MFH8.1.6	6	1,4						
NA 8		MFH8.1.7	7	2,94						
NA 8 - gesamt	7	1								

Tabelle 70 (Teil 2): finale Parameter für die Lastkurven zu 2030 – Stadt.

6.7.3 2045

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	4	MFH1.1.1	49	3,79						
NA 1		MFH1.1.2	48	4,64						
NA 1		MFH1.1.3	47	4,23						
NA 1		MFH1.1.4	46	8,63						
NA 1 - gesamt	4	1								
NA 2	1	EFH2.1	11	3,89	8,6	7,5	8,8	11,8	3,1	11
NA 2	1	EFH2.2	10	3,37						
NA 2 - gesamt	2	2								
NA 3	2	ZFH3.1.1	22	4,04	7,4	7	9,2	19,2	3	11
NA 3		ZFH3.1.2	21	6,9						
NA 3 - gesamt	2	1								
NA 4	4	MFH4.1.1	15	3,4	6,8			41	3,5	11
NA 4		MFH4.1.2	14	3,26						
NA 4		MFH4.1.3	13	4,89						
NA 4		MFH4.1.4	12	4,51						
NA 4 - gesamt	4	1								
NA 5	6	MFH5.1.1	19	5,49						
NA 5		MFH5.1.2	18	5,74						
NA 5		MFH5.1.3	17	5,92						
NA 5		MFH5.1.4	44	2,63						
NA 5		MFH5.1.5	45	4,95						
NA 5		MFH5.1.6	43	2,3						
NA 5 - gesamt	6	1								
NA 6	3	MFH6.1.1	54	6,09						
NA 6		MFH6.1.2	51	2,39						
NA 6		MFH6.1.3	50	3,96						
NA 6 - gesamt	3	1								
NA 7	2	ZFH7.2.1	30	4,7	7			18	3,4	11
NA 7		ZFH7.2.2	29	3,68						
NA 7	10	MFH7.1.1	42	6,04						
NA 7		MFH7.1.2	41	5,52						
NA 7		MFH7.1.3	40	3,77						
NA 7		MFH7.1.4	39	5,17						
NA 7		MFH7.1.5	38	5,56						
NA 7		MFH7.1.6	37	3,47						
NA 7		MFH7.1.7	36	4,15						
NA 7		MFH7.1.8	35	6,69						
NA 7		MFH7.1.9	34	3,08						
NA 7		MFH7.1.10	33	3,43						
NA 7 - gesamt	12	2								

Tabelle 71 (Teil 1): finale Parameter für die Lastkurven zu 2045 – Stadt.

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 8	7	MFH8.1.1	1	3,24						
NA 8		MFH8.1.2	2	4,5						
NA 8		MFH8.1.3	3	6,62						
NA 8		MFH8.1.4	4	2,66						
NA 8		MFH8.1.5	5	3,2						
NA 8		MFH8.1.6	6	1,4						
NA 8		MFH8.1.7	7	2,94						
NA 8 - gesamt	7	1								

Tabelle 71 (Teil 2): finale Parameter für die Lastkurven zu 2045 – Stadt.

6.7.4 Vollausbau

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 1	4	MFH1.1.1	49	3,79	11	9,5	13	35	3,3	11
NA 1		MFH1.1.2	48	4,64						
NA 1		MFH1.1.3	47	4,23						
NA 1		MFH1.1.4	46	8,63						
NA 1 - gesamt	4	1								
NA 2	1	EFH2.1	11	3,89	8,6	6,7	8,6	11,8	3,1	11
NA 2	1	EFH2.2	10	3,37	7,8	5,3	7,5	12	3	11
NA 2 - gesamt	2	2								
NA 3	2	ZFH3.1.1	22	4,04	7,4	6,5	8,5	12,2	3	11
NA 3		ZFH3.1.2	21	6,9						
NA 3 - gesamt	2	1								
NA 4	4	MFH4.1.1	15	3,4	8,2	6,7	9	41,9	3,5	11
NA 4		MFH4.1.2	14	3,26						
NA 4		MFH4.1.3	13	4,89						
NA 4		MFH4.1.4	12	4,51						
NA 4 - gesamt	4	1								
NA 5	6	MFH5.1.1	19	5,49	10	9	15	55	3,5	11
NA 5		MFH5.1.2	18	5,74						
NA 5		MFH5.1.3	17	5,92						
NA 5		MFH5.1.4	44	2,63						
NA 5		MFH5.1.5	45	4,95						
NA 5		MFH5.1.6	43	2,3						
NA 5 - gesamt	6	1								
NA 6	3	MFH6.1.1	54	6,09	9	6	10	30	3,3	11
NA 6		MFH6.1.2	51	2,39						
NA 6		MFH6.1.3	50	3,96						
NA 6 - gesamt	3	1								
NA 7	2	ZFH7.2.1	30	4,7	7	5,6	8,3	18	3,4	11
NA 7		ZFH7.2.2	29	3,68						
NA 7	10	MFH7.1.1	42	6,04	11	11	21	100	3,5	11
NA 7		MFH7.1.2	41	5,52						
NA 7		MFH7.1.3	40	3,77						
NA 7		MFH7.1.4	39	5,17						
NA 7		MFH7.1.5	38	5,56						
NA 7		MFH7.1.6	37	3,47						
NA 7		MFH7.1.7	36	4,15						
NA 7		MFH7.1.8	35	6,69						
NA 7		MFH7.1.9	34	3,08						
NA 7		MFH7.1.10	33	3,43						
NA 7 - gesamt	12	2								

Tabelle 72 (Teil 1): finale Parameter für die Lastkurven zu Vollausbau – Stadt.

Netzab-schnitte	Anschlüsse	Gebäude	HH Kurve	Jahresverbrauch [MWh/a]	PV [kW]	Bat [kW]	Bat [kWh]	Heizlast [kW]	WP [JAZ]	LS [kW]
NA 8	7	MFH8.1.1	1	3,24	10	13	25	70	3,5	11
NA 8		MFH8.1.2	2	4,5						
NA 8		MFH8.1.3	3	6,62						
NA 8		MFH8.1.4	4	2,66						
NA 8		MFH8.1.5	5	3,2						
NA 8		MFH8.1.6	6	1,4						
NA 8		MFH8.1.7	7	2,94						
NA 8 - gesamt	7	1								

Tabelle 72 (Teil 2): finale Parameter für die Lastkurven zu Vollausbau – Stadt.

A4: Lastkurven für die Haushalte des Beispiels

1 Prosumerlastkurven

1.1 Dorf 1 – Ausgangssituation

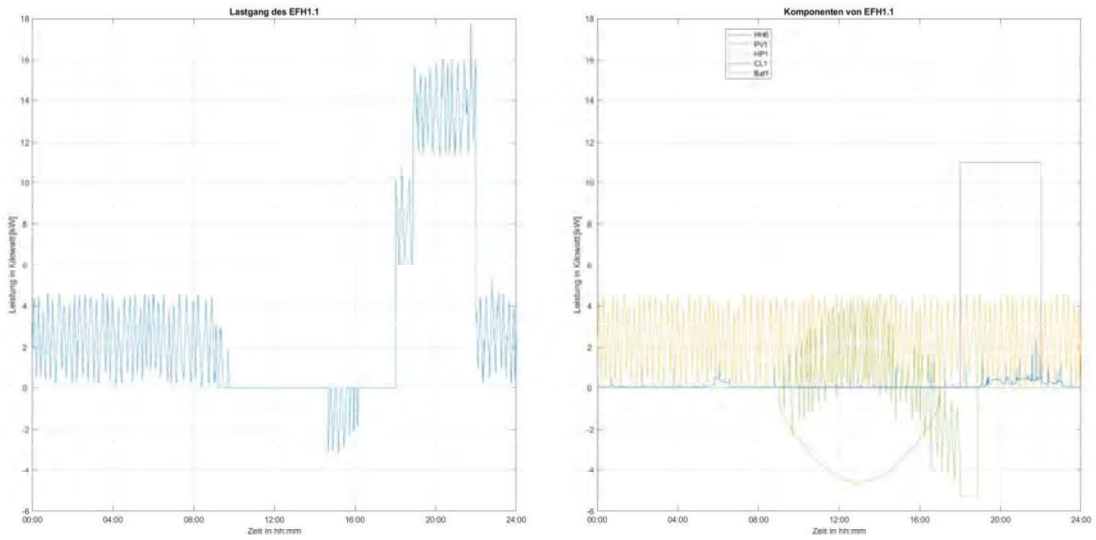


Abbildung 1: Gebäude EFH1.1 in der Topologie Dorf 1, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

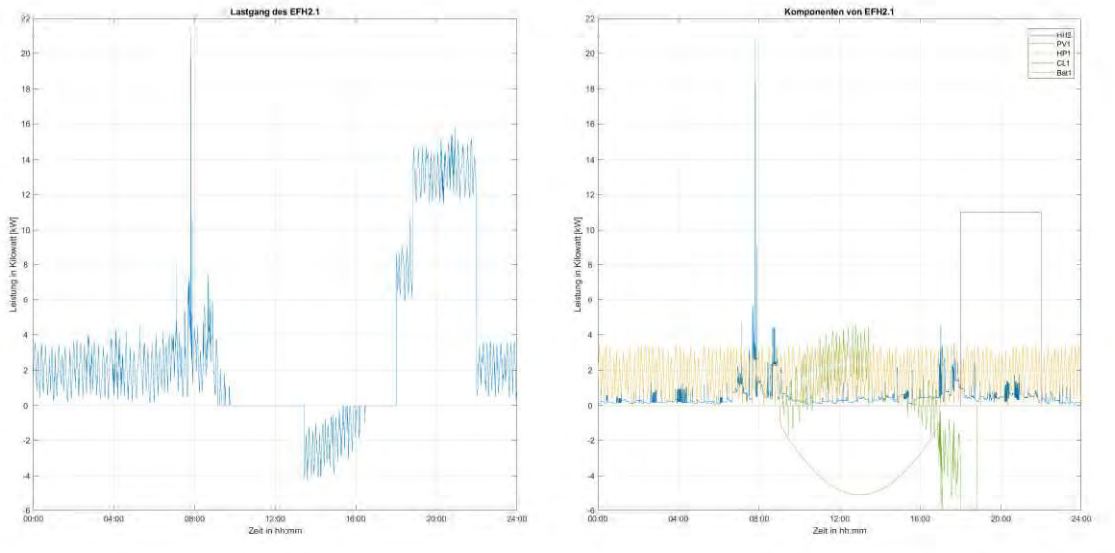


Abbildung 2:Gebäude EFH2.1 in der Topologie Dorf 1, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

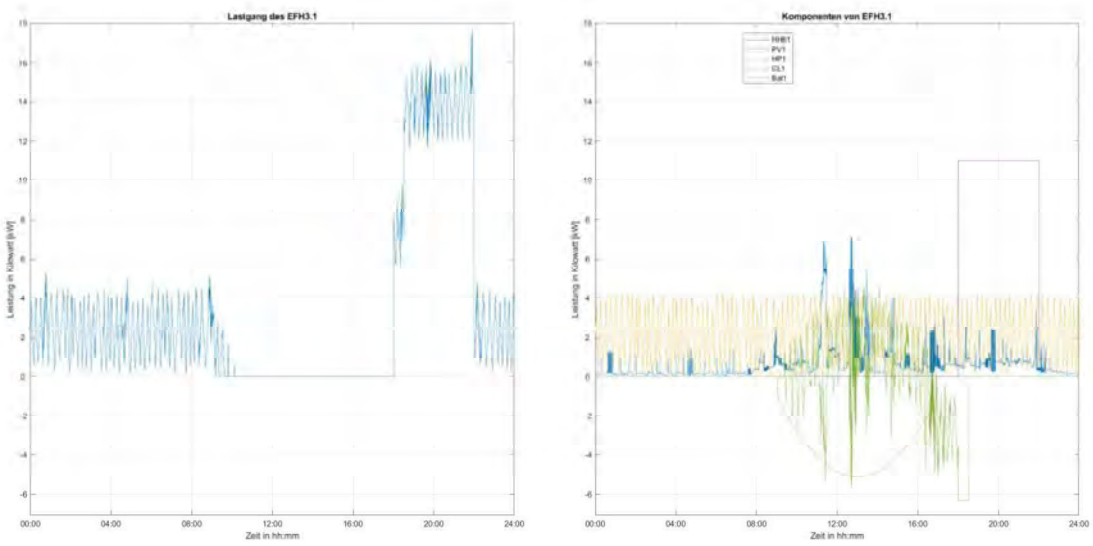


Abbildung 3:Gebäude EFH3.1 in der Topologie Dorf 1, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

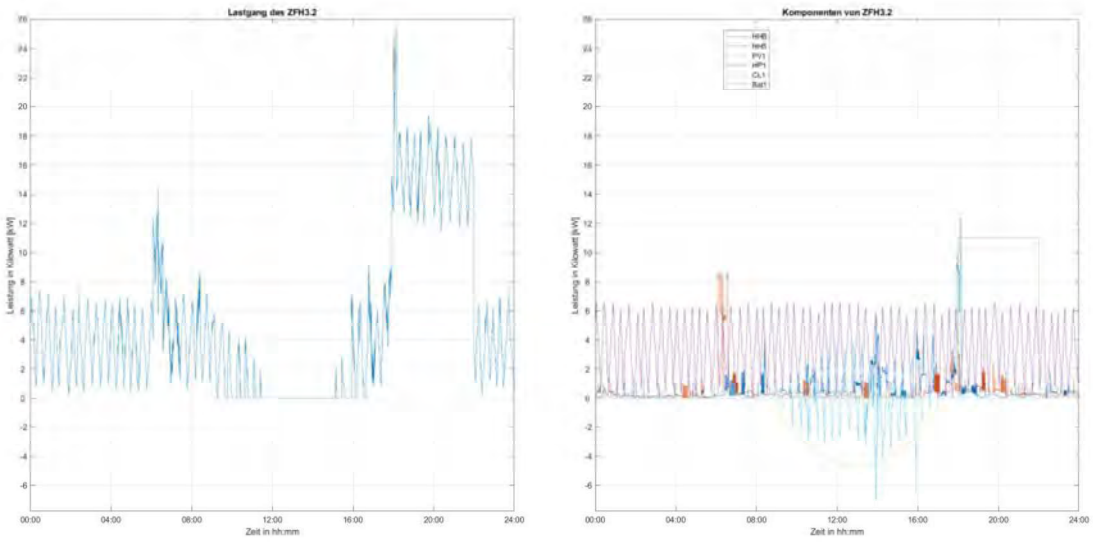


Abbildung 4:Gebäude ZFH3.2 in der Topologie Dorf 1, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

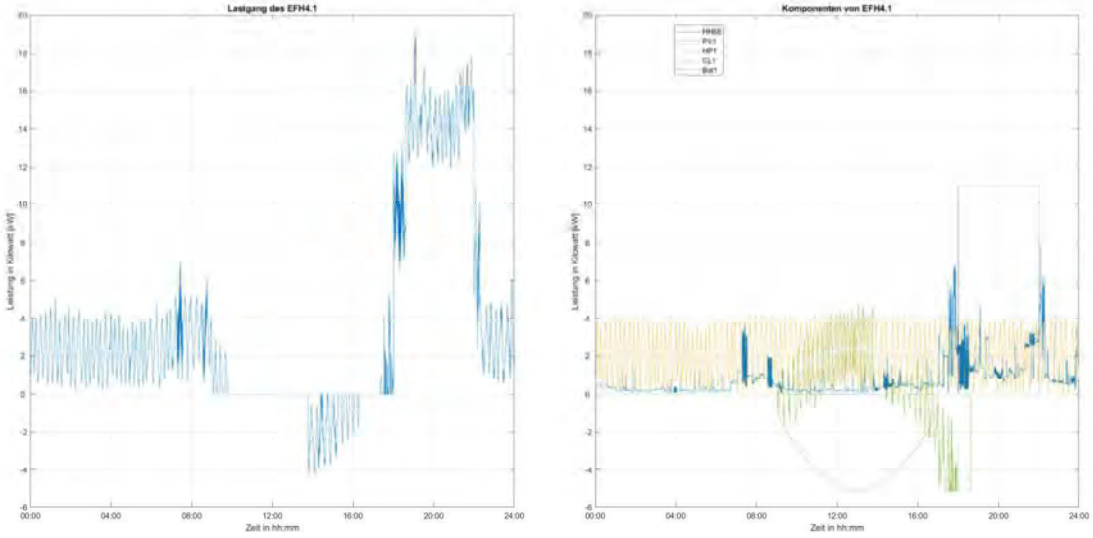


Abbildung 5:Gebäude EFH4.1 in der Topologie Dorf 1, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

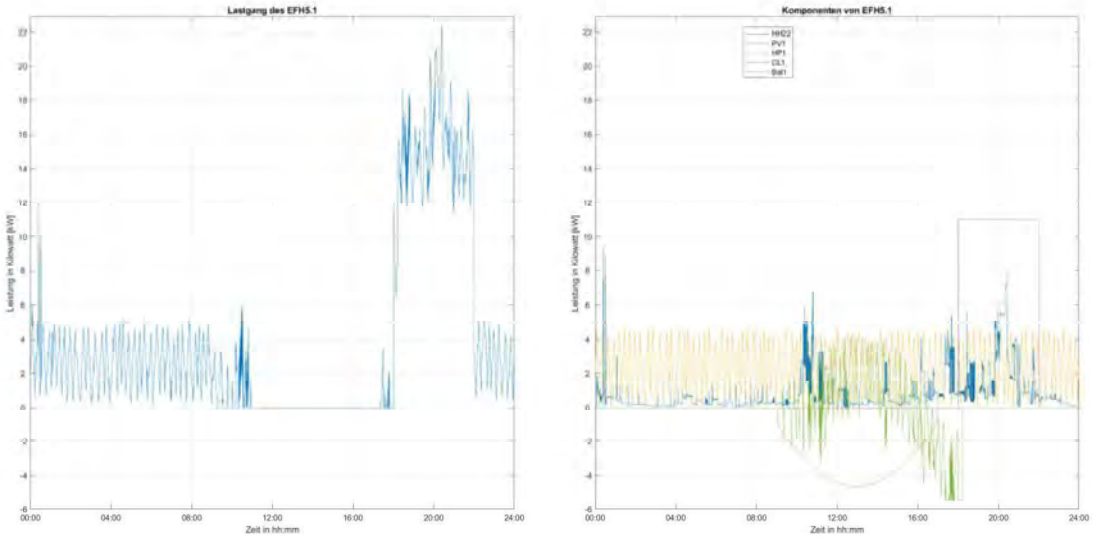


Abbildung 6:Gebäude EFH5.1 in der Topologie Dorf 1, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

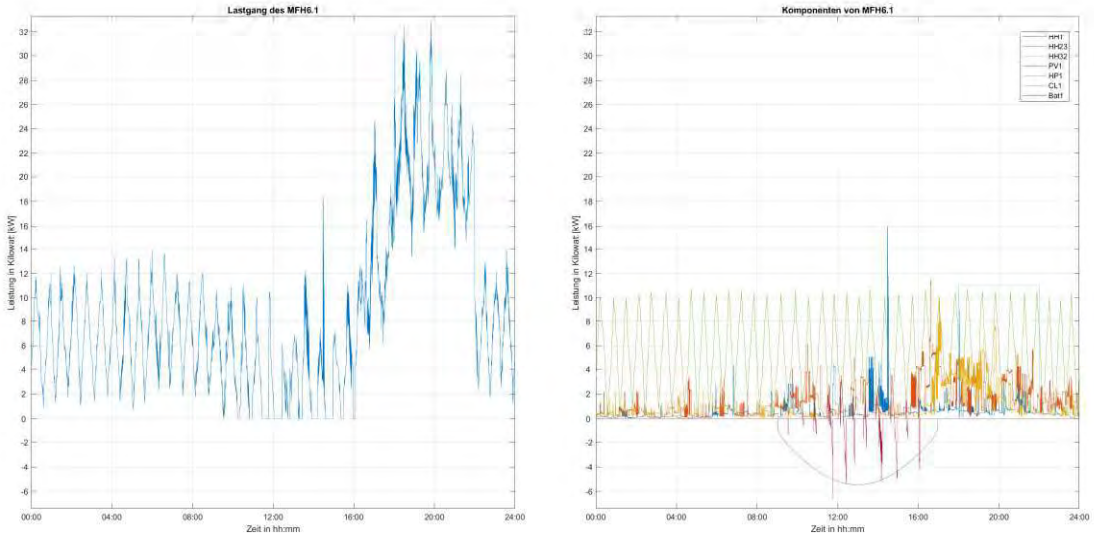


Abbildung 7:Gebäude MFH6.1 in der Topologie Dorf 1, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

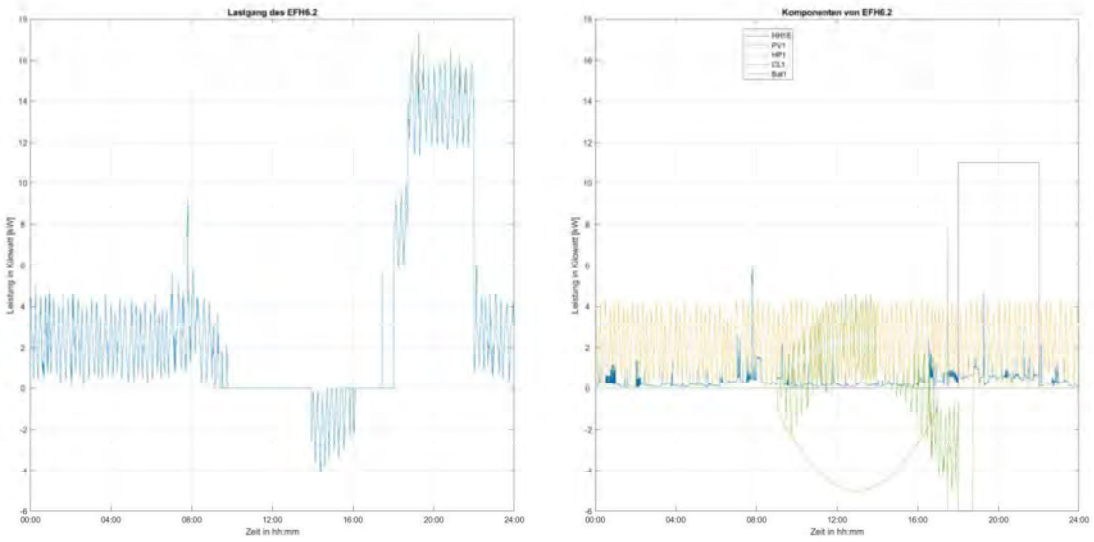


Abbildung 8:Gebäude EFH6.2 in der Topologie Dorf 1, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

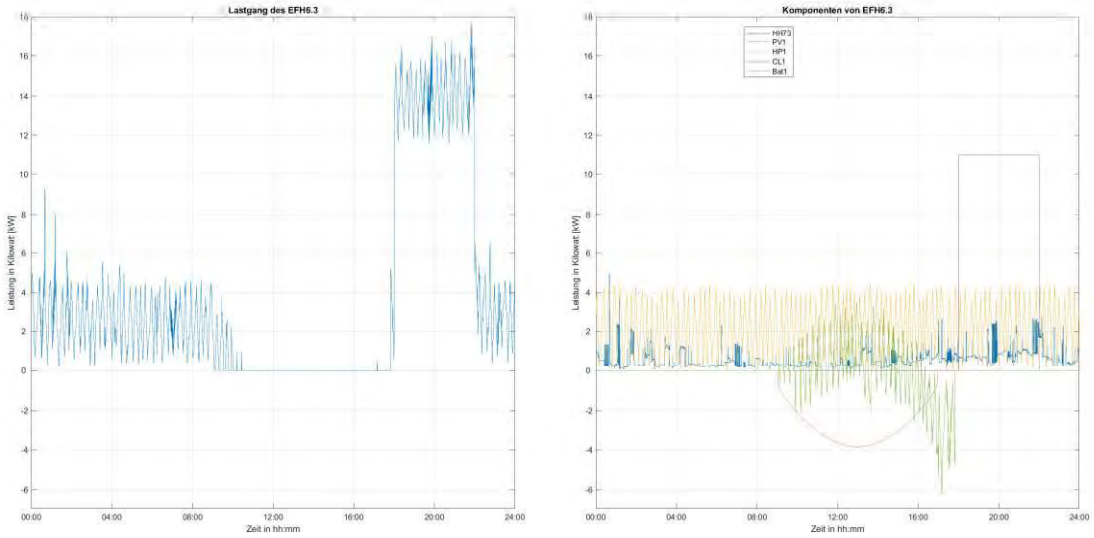


Abbildung 9:Gebäude EFH6.3 in der Topologie Dorf 1, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

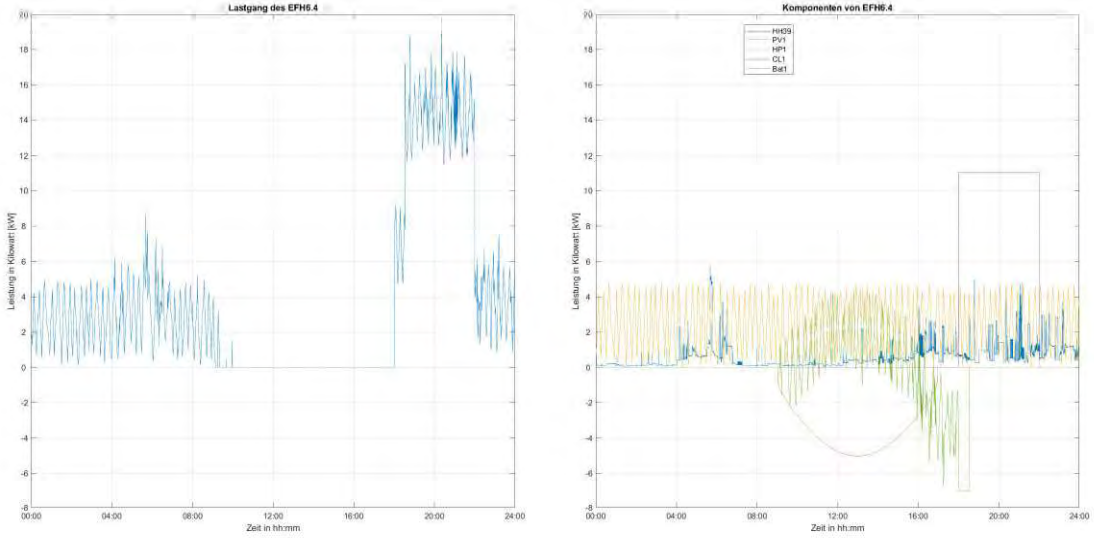


Abbildung 10:Gebäude EFH6.4 in der Topologie Dorf 1, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

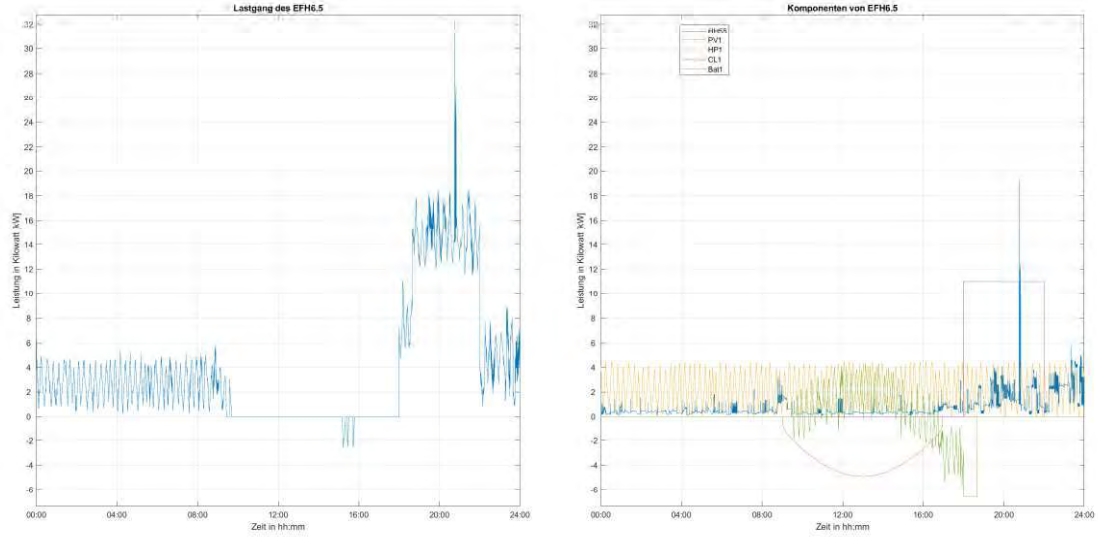


Abbildung 11:Gebäude EFH6.5 in der Topologie Dorf 1, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

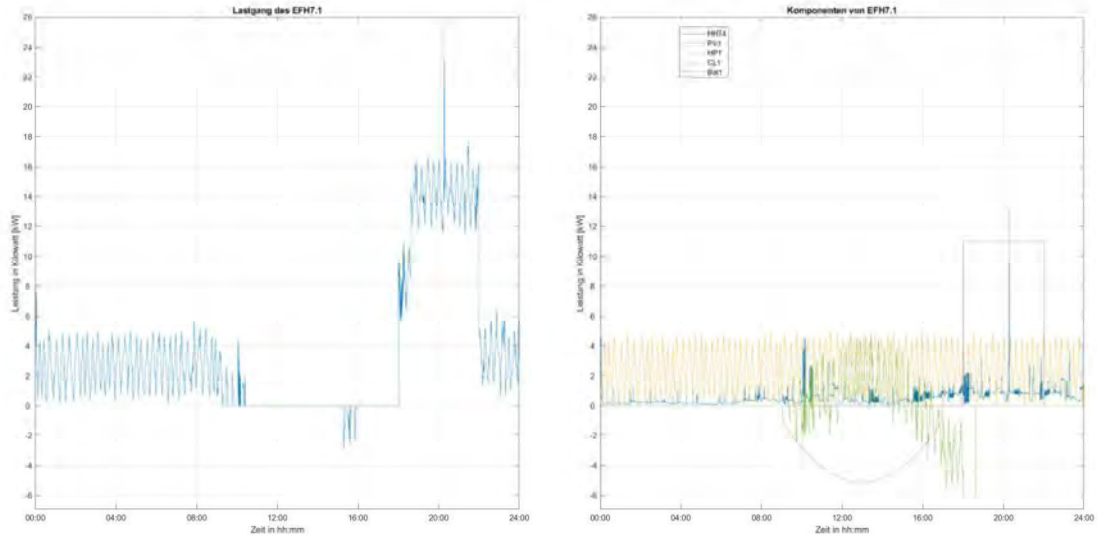


Abbildung 12:Gebäude EFH7.1 in der Topologie Dorf 1, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

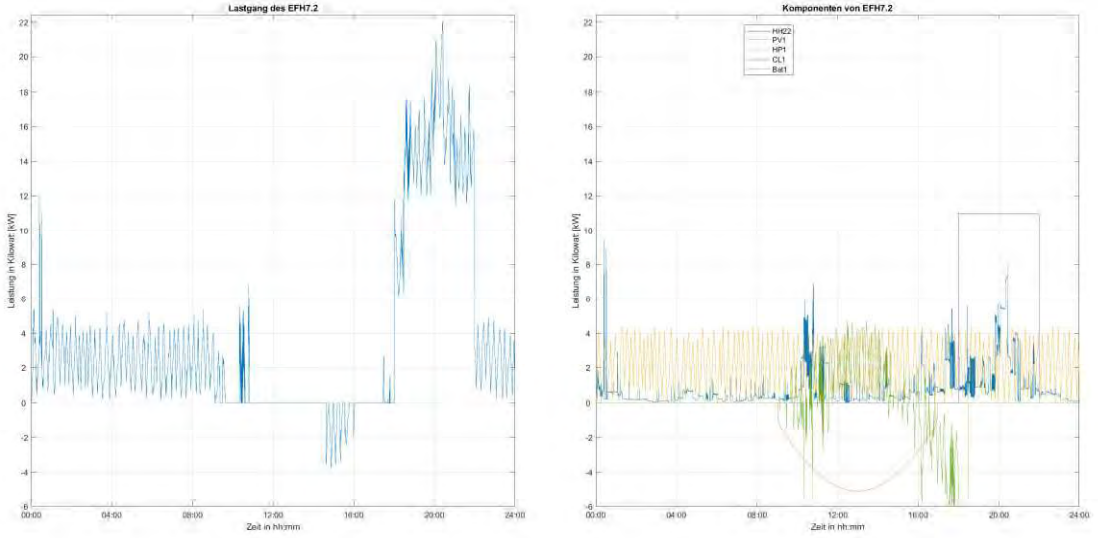


Abbildung 13:Gebäude EFH7.2 in der Topologie Dorf 1, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

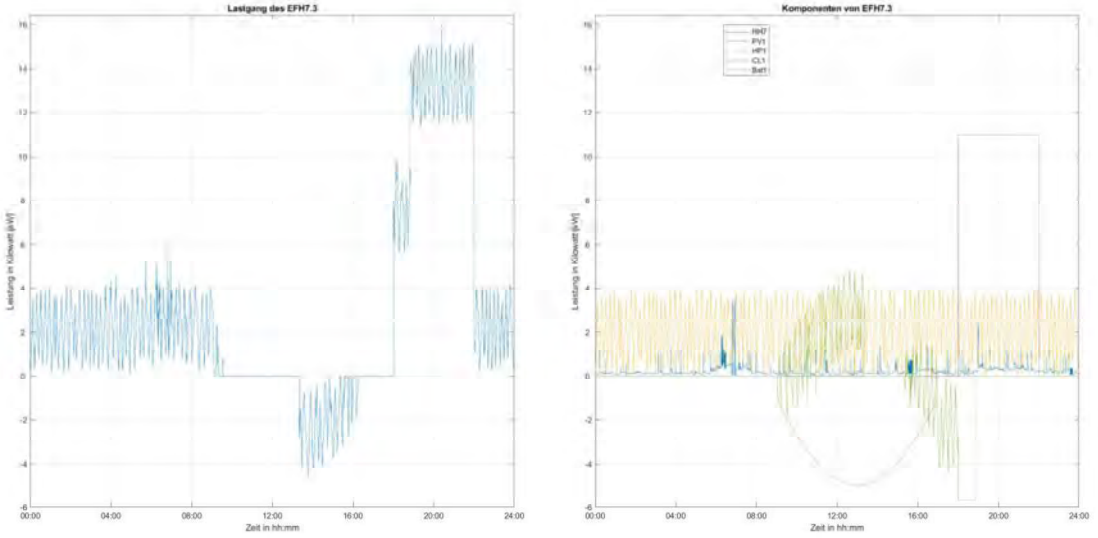


Abbildung 14:Gebäude EFH7.3 in der Topologie Dorf 1, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

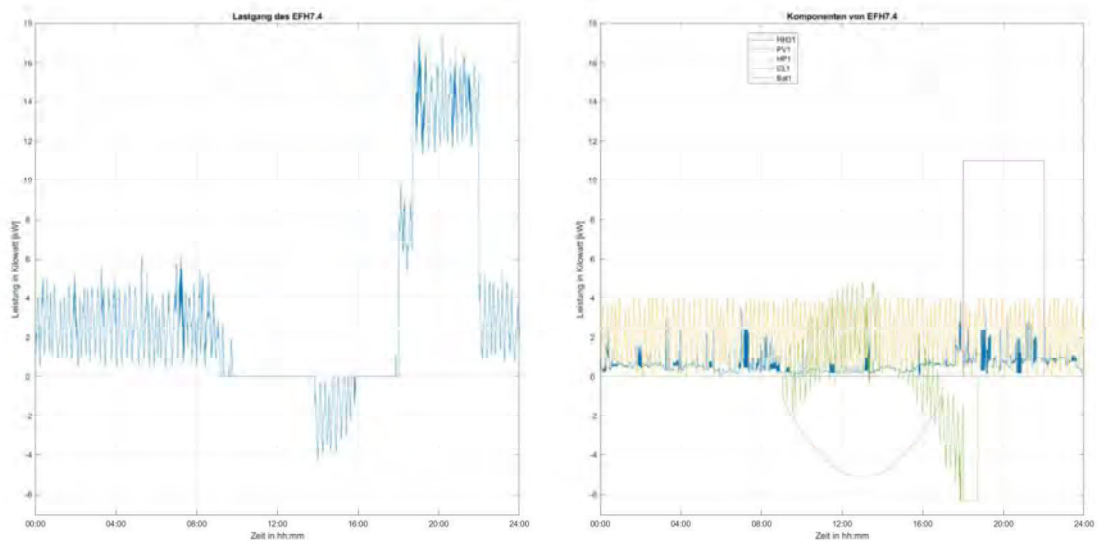


Abbildung 15:Gebäude EFH7.4 in der Topologie Dorf 1, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

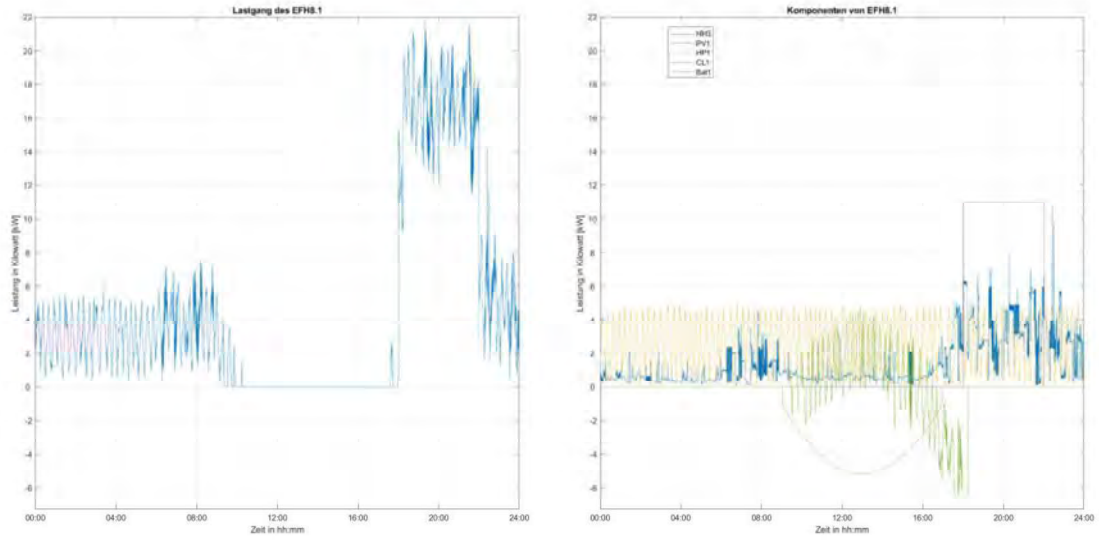


Abbildung 16:Gebäude EFH8.1 in der Topologie Dorf 1, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

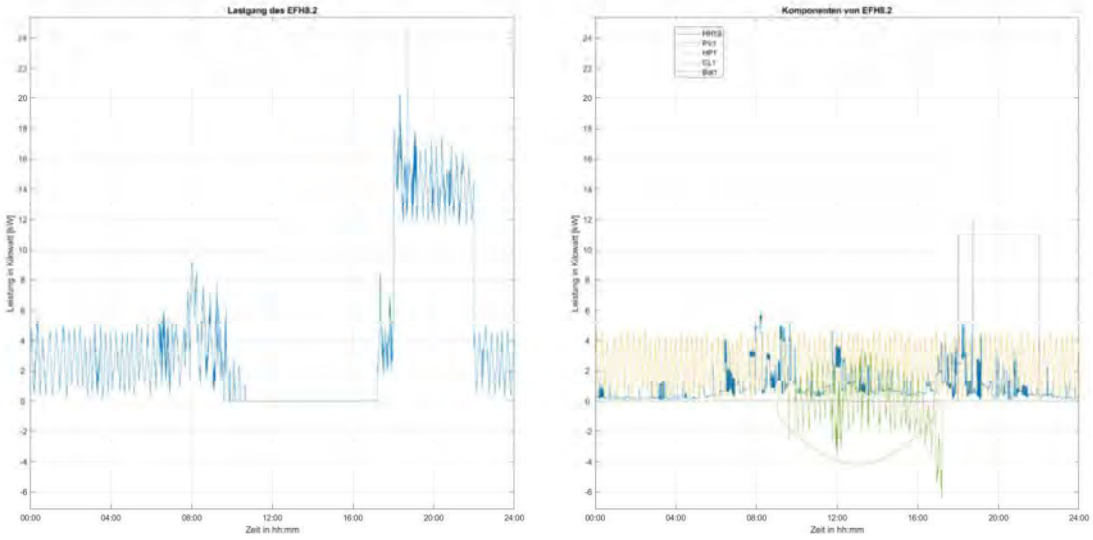


Abbildung 17:Gebäude EFH8.2 in der Topologie Dorf 1, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

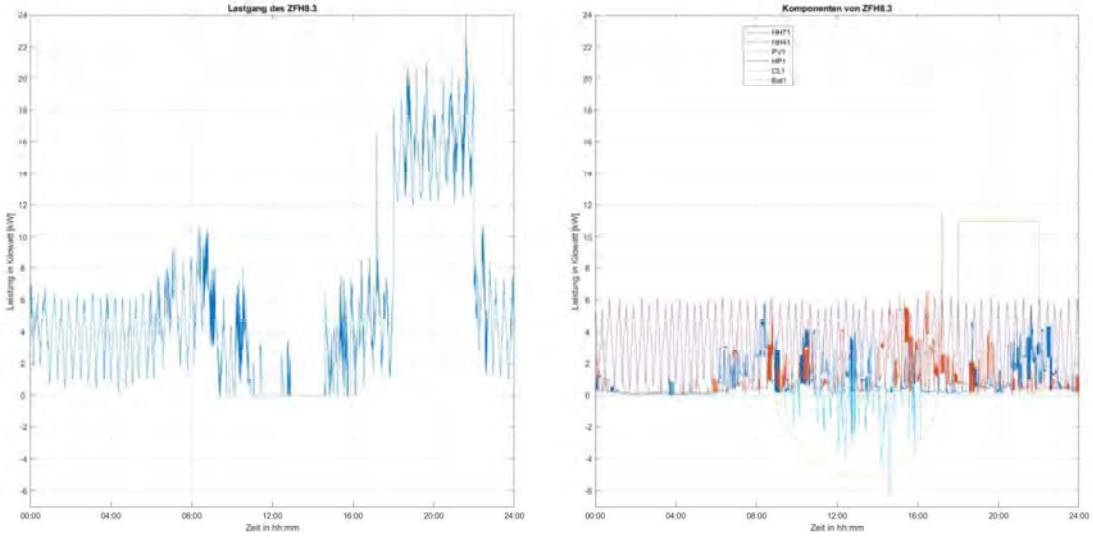


Abbildung 18:Gebäude ZFH8.3 in der Topologie Dorf 1, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

1.2 Dorf 1 – Eingriff (Abreglung der Ladesäulen um 50 %)

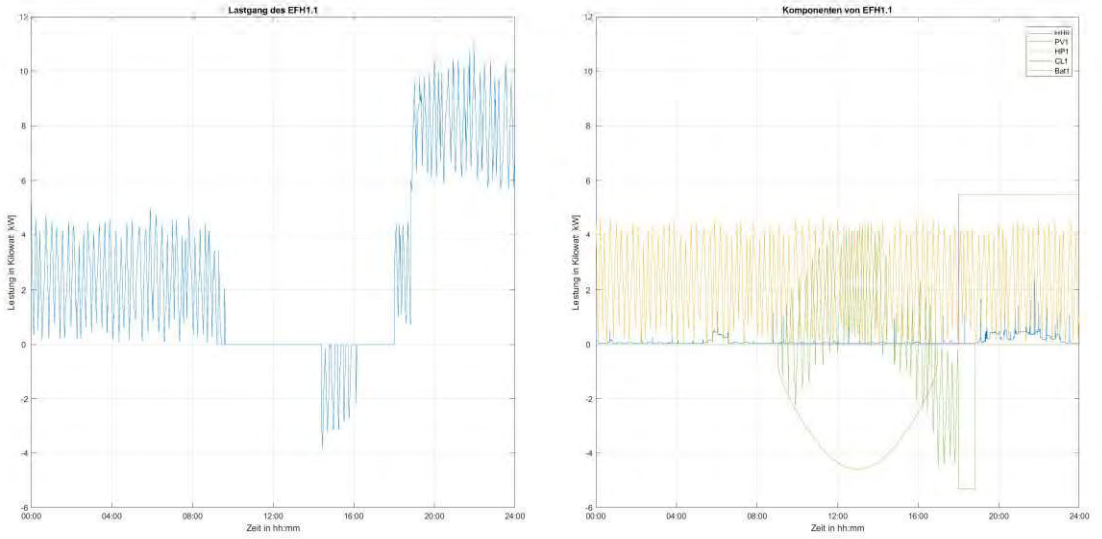


Abbildung 19:Gebäude EFH1.1 in der Topologie Dorf 1 mit Eingriff, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

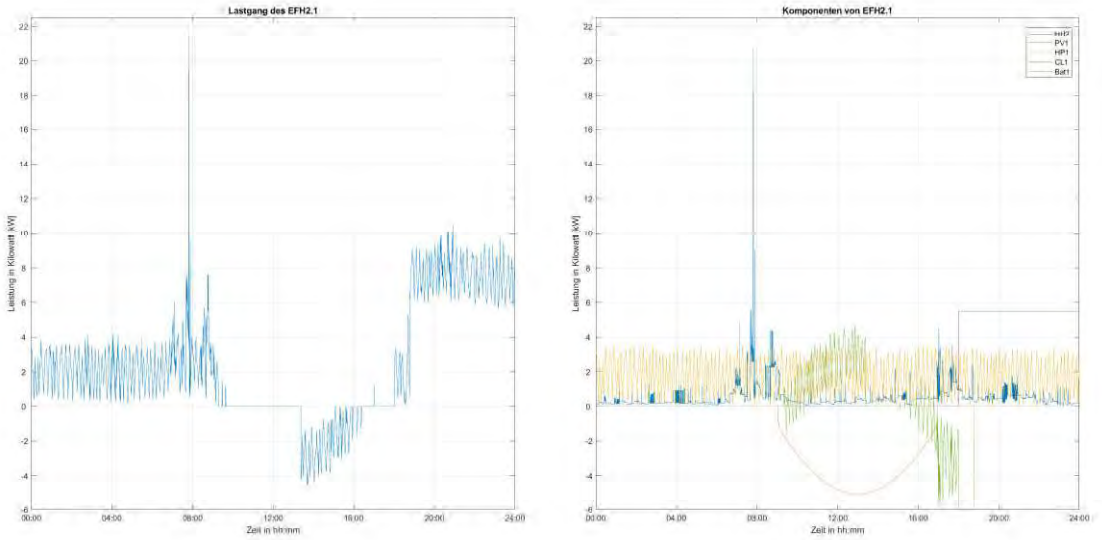


Abbildung 20:Gebäude EFH2.1 in der Topologie Dorf 1 mit Eingriff, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

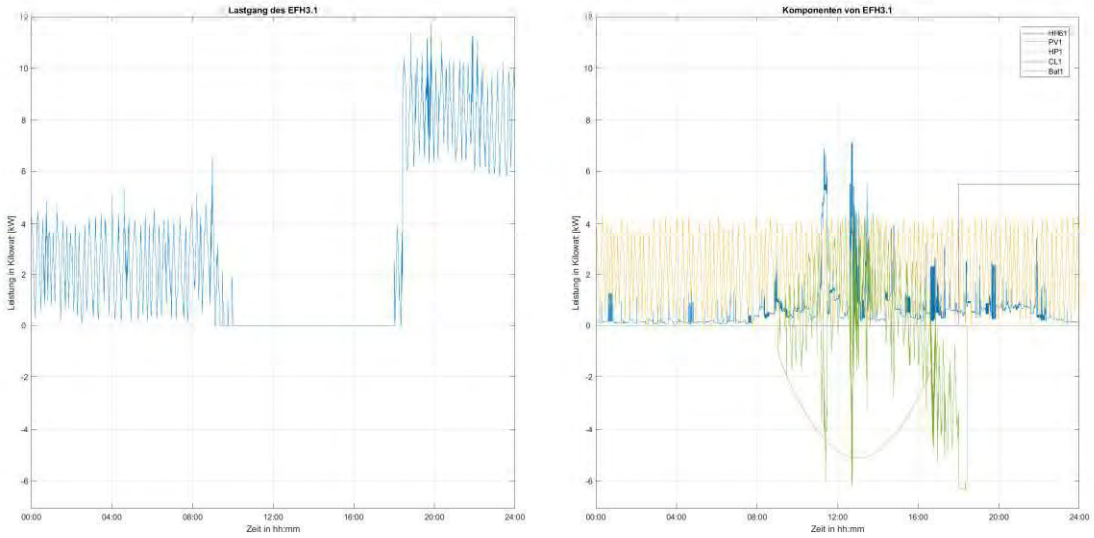


Abbildung 21:Gebäude EFH3.1 in der Topologie Dorf 1 mit Eingriff, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

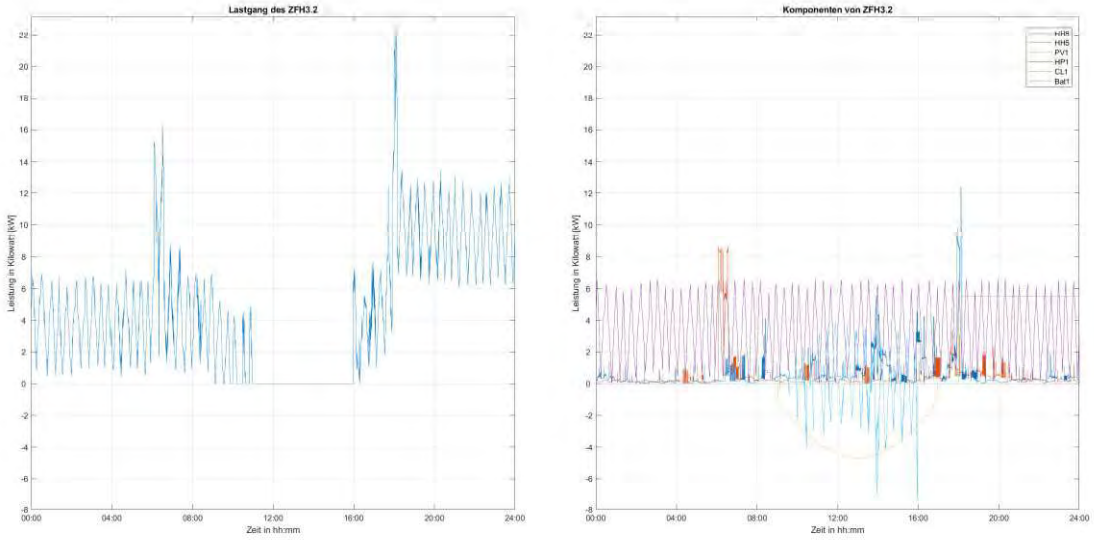


Abbildung 22:Gebäude ZFH3.2 in der Topologie Dorf 1 mit Eingriff, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

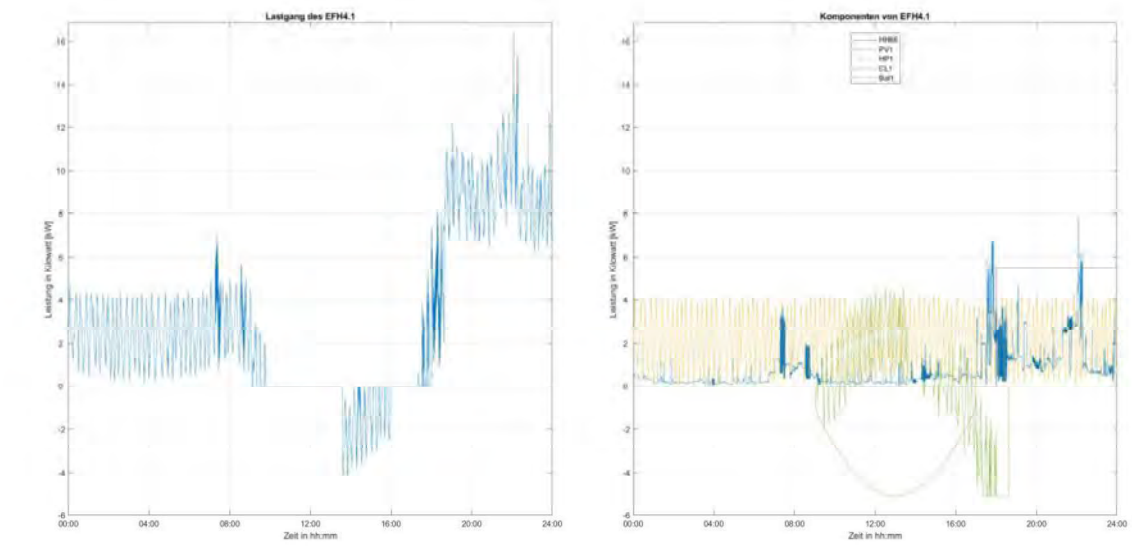


Abbildung 23:Gebäude EFH4.1 in der Topologie Dorf 1 mit Eingriff, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

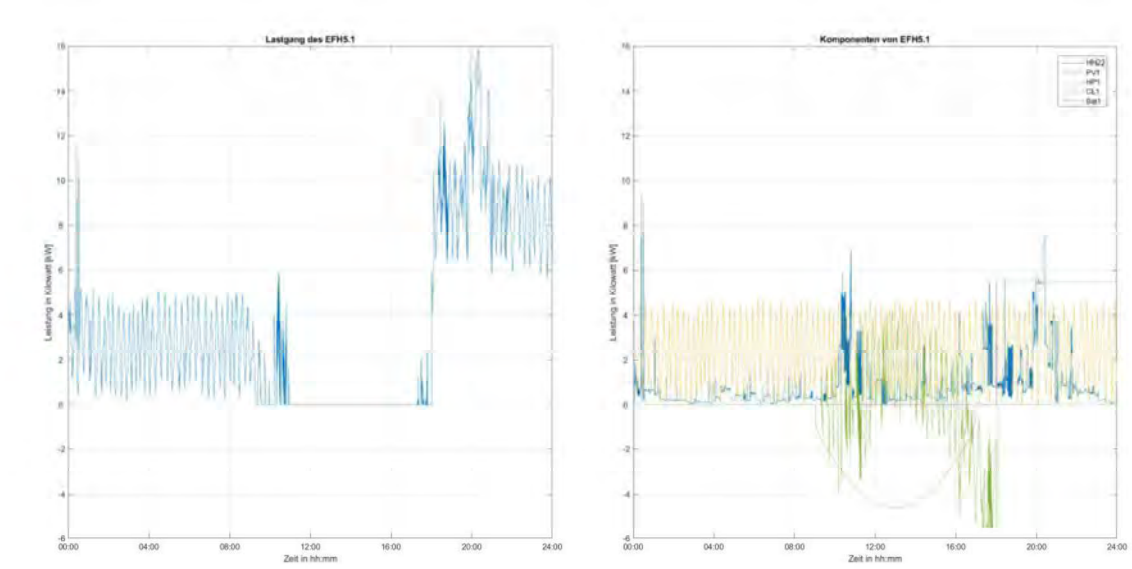


Abbildung 24:Gebäude EFH5.1 in der Topologie Dorf 1 mit Eingriff, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

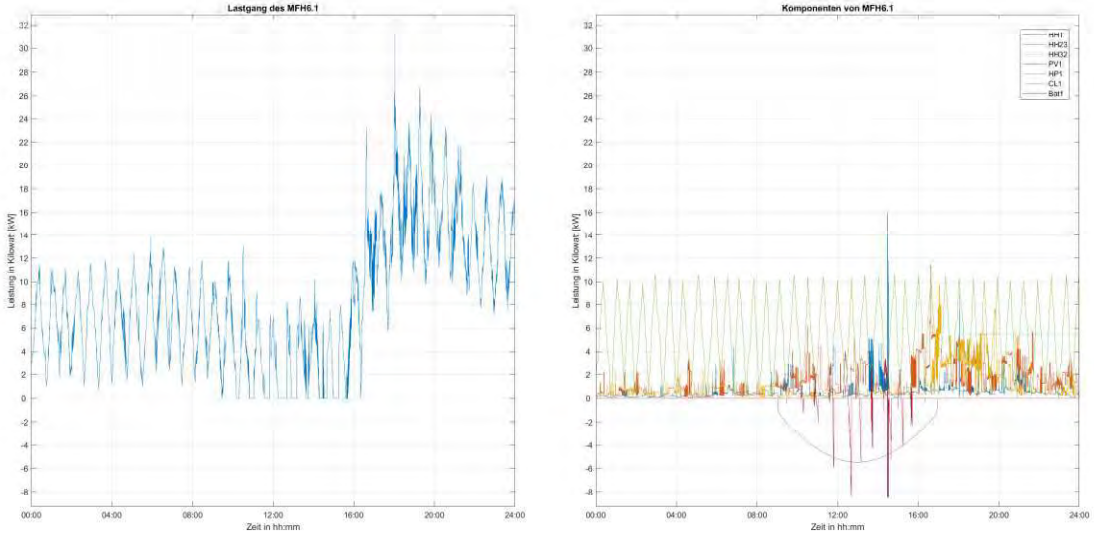


Abbildung 25:Gebäude MFH6.1 in der Topologie Dorf 1 mit Eingriff, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

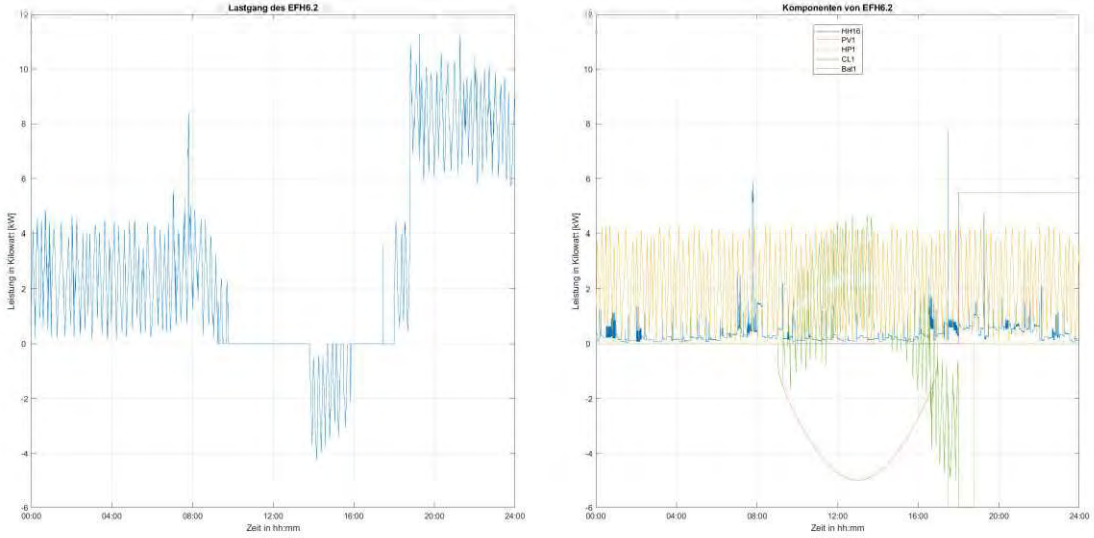


Abbildung 26:Gebäude EFH6.2 in der Topologie Dorf 1 mit Eingriff, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

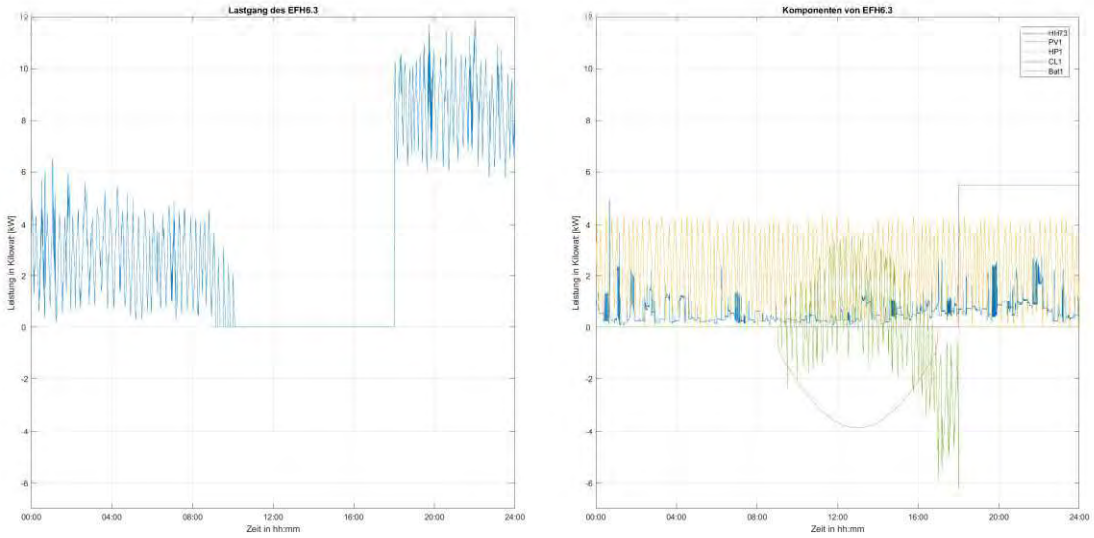


Abbildung 27:Gebäude EFH6.3 in der Topologie Dorf 1 mit Eingriff, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

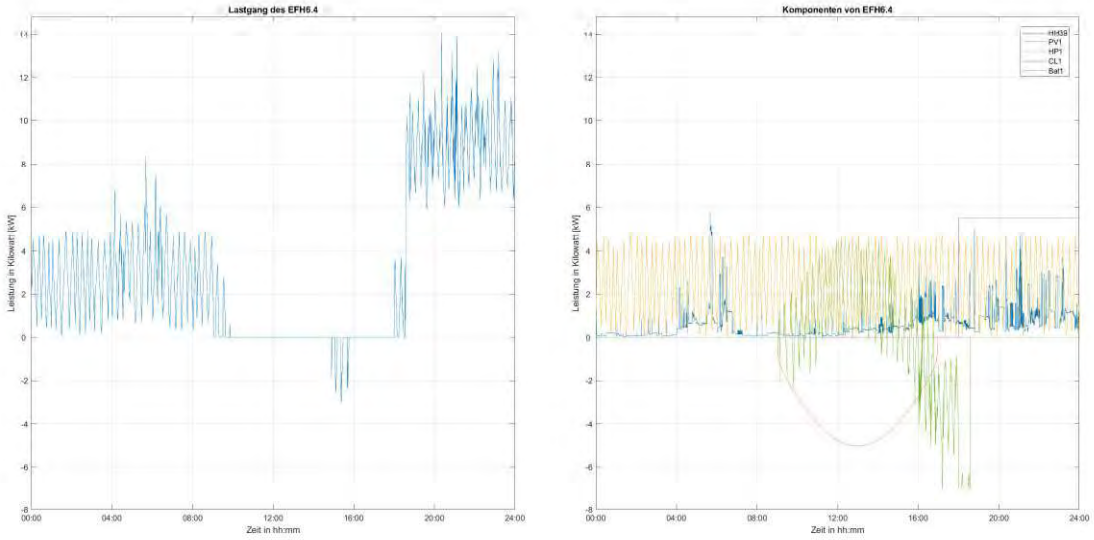


Abbildung 28:Gebäude EFH6.4 in der Topologie Dorf 1 mit Eingriff, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

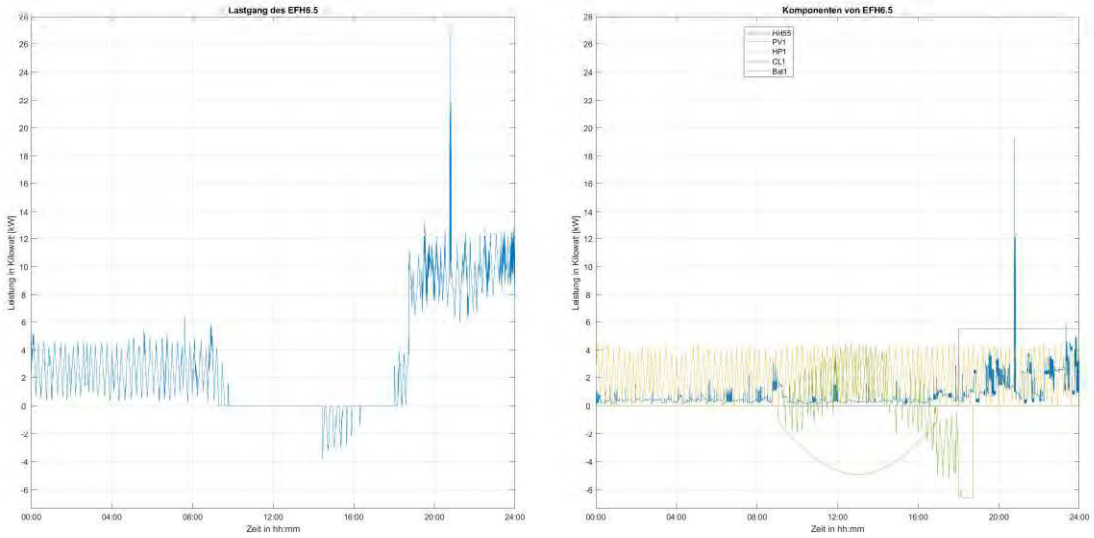


Abbildung 29:Gebäude EFH6.5 in der Topologie Dorf 1 mit Eingriff, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

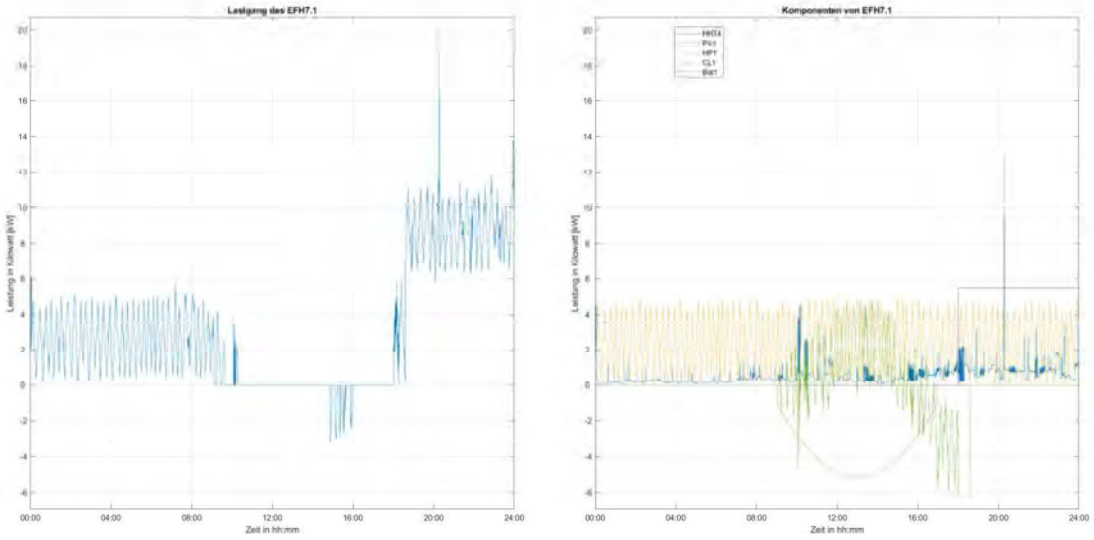


Abbildung 30:Gebäude EFH7.1 in der Topologie Dorf 1 mit Eingriff, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

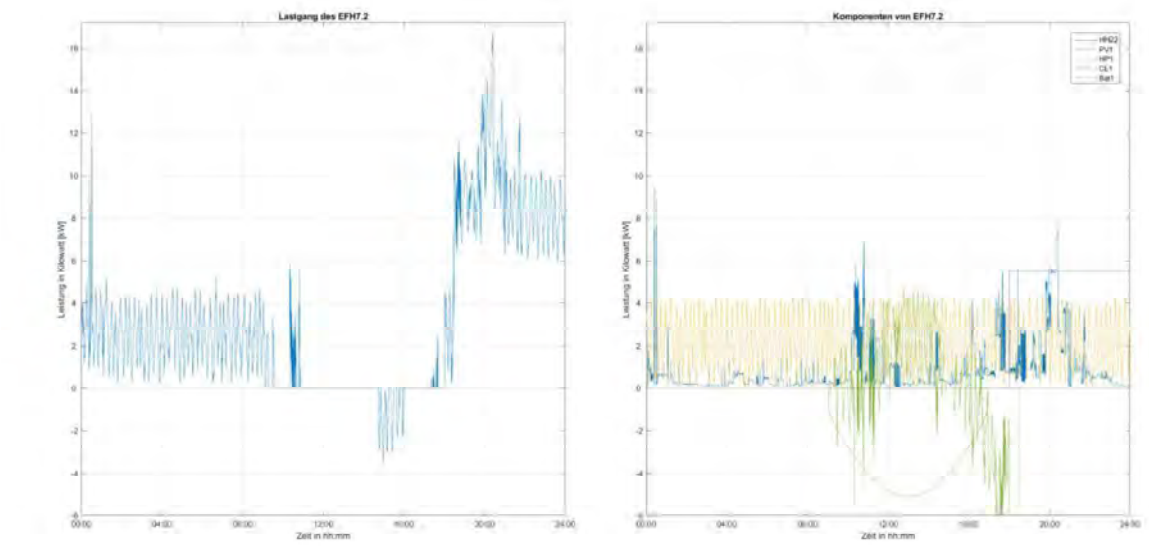


Abbildung 31:Gebäude EFH7.2 in der Topologie Dorf 1 mit Eingriff, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

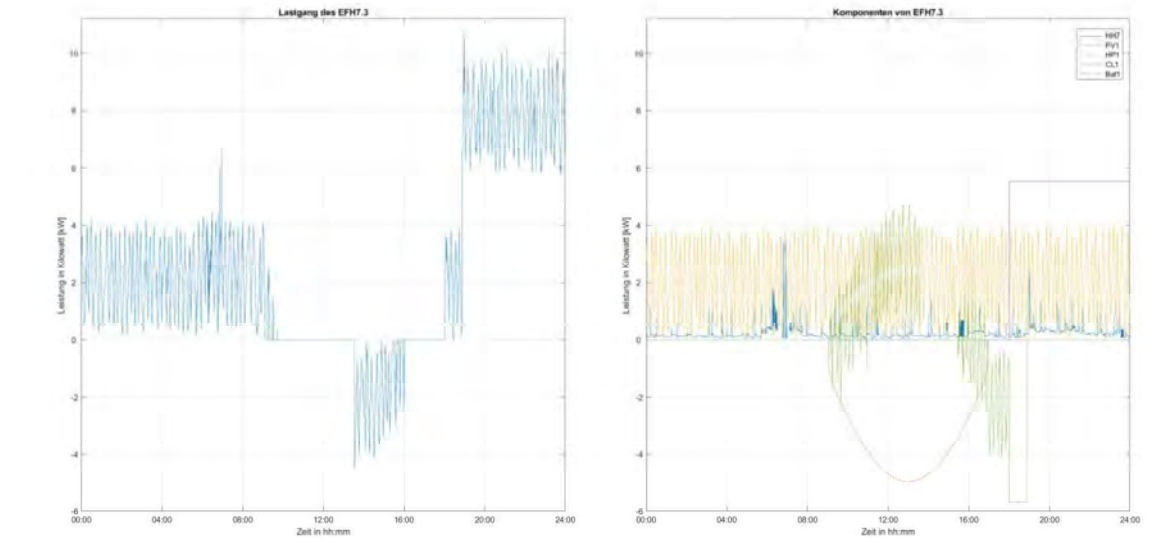


Abbildung 32:Gebäude EFH7.3 in der Topologie Dorf 1 mit Eingriff, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

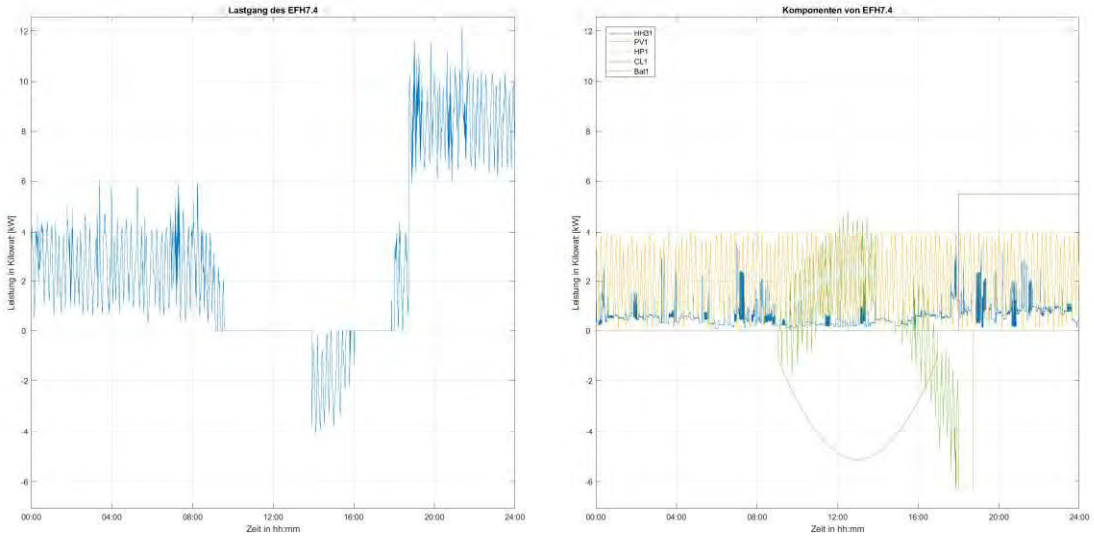


Abbildung 33:Gebäude EFH7.4 in der Topologie Dorf 1 mit Eingriff, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

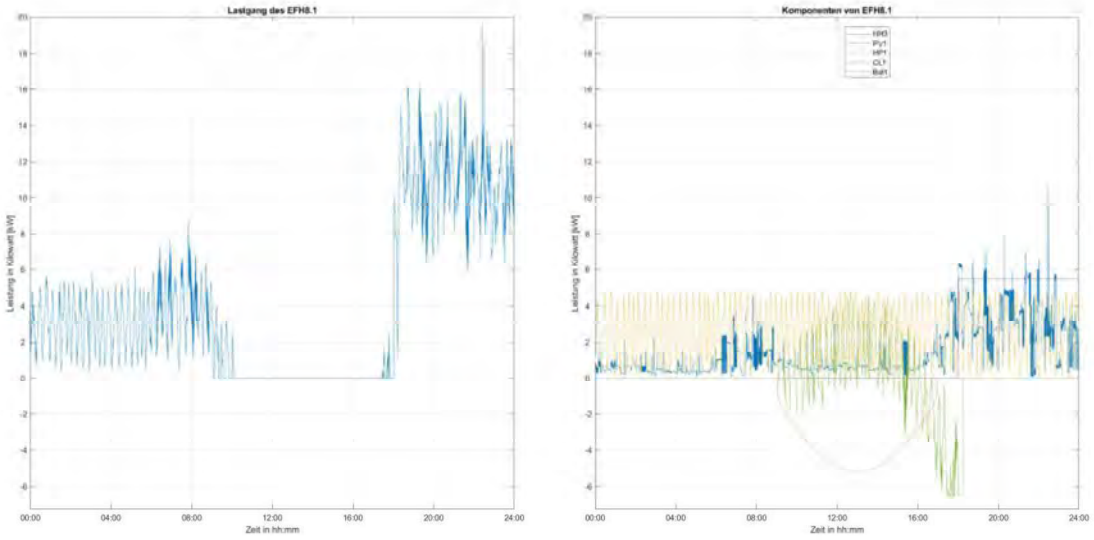


Abbildung 34:Gebäude EFH8.1 in der Topologie Dorf 1 mit Eingriff, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

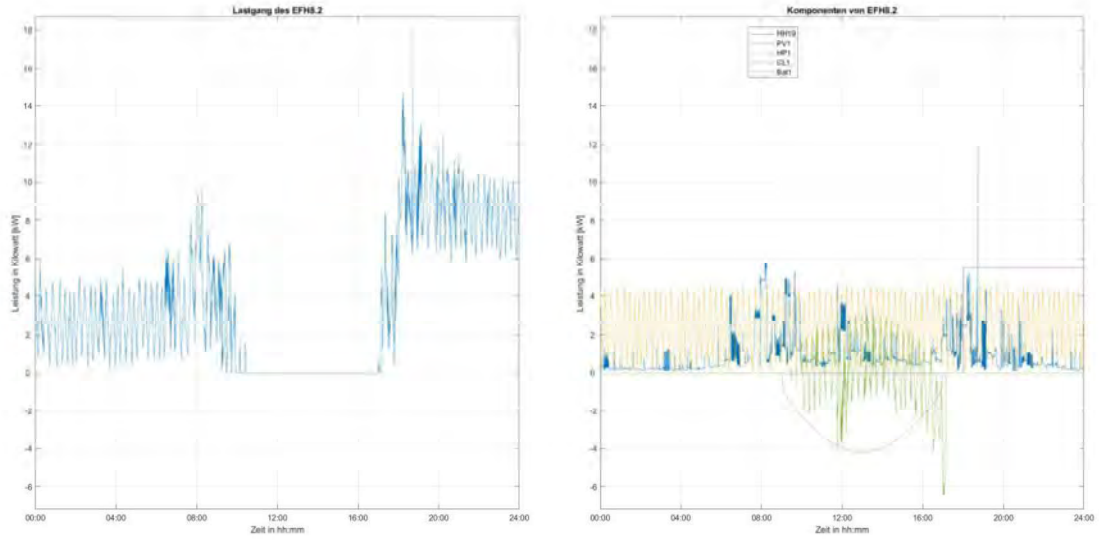


Abbildung 35:Gebäude EFH8.2 in der Topologie Dorf 1 mit Eingriff, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges

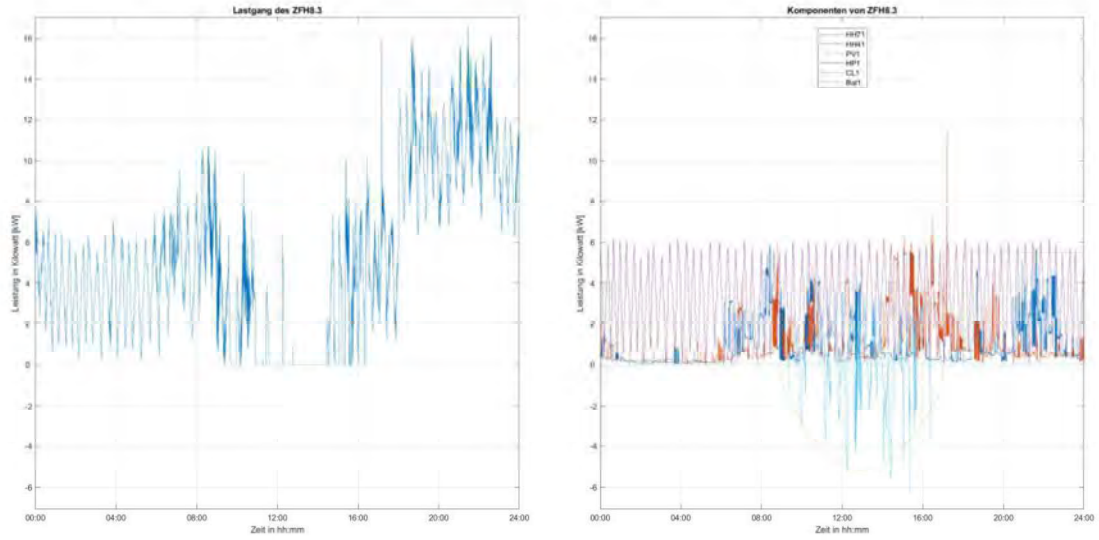


Abbildung 36:Gebäude ZFH8.3 in der Topologie Dorf 1 mit Eingriff, links Gesamtlastgang, rechts einzelne Bestandteile des Lastganges