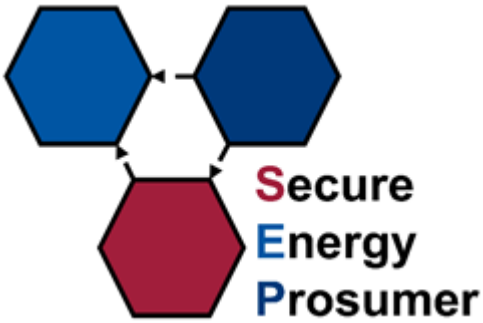
Forschungsbericht BWPLUS

Sichere Kommunikation in Smart Grids mit Prosumern in einem dezentralen regenerativen Energiesystem

(SecureEnergyProsumer)



von

Munkhtsetseg Baatar (THU), Falko Ebe (THU), Christoph Kondzialka (THU),

Jeromie Morris (THU), Gerd Heilscher (THU)

Christoph Groß (EKUT), Stefan Müller (EKUT),

Gunter Maetze (WBZU), Peter Pioch (WBZU)

Technische Hochschule Ulm (THU)

Universität Tübingen (EKUT)

Weiterbildungszentrum für innovative Energietechnologien

der Handwerkskammer Ulm (WBZU)

Förderkennzeichen: BWSGD18009, BWSGD18010, BWSGD18011

Die Arbeiten des Programms Lebensgrundlage Umwelt und ihre Sicherung werden mit Mitteln des Landes Baden-Württemberg gefördert

Oktober 2021

Kurzbeschreibung der Forschungsergebnisse (THU/EKUT/WBZU)

Dezentralisierung, Digitalisierung und Dekarbonisierung (3D's) sind die führenden Innovationstrends auf dem Weg zur erfolgreichen Energiewende. Für die Digitalisierung der Energiewende sind die Themen Internet of Things* (IoT), Smart Meter*, virtuelle Kraftwerke und Blockchain* wichtig. Im Projekt SecureEnergyProsumer (SEP) haben wir Blockchain- bzw. genauer gesagt Distributed Ledger-Technologie* für die Digitalisierung und Dezentralisierung des Energiesystems zur Anwendung gebracht, um eine sichere Informations- und Kommunikationsstruktur für ein dezentrales Energiesystem von Prosumern* abzubilden, da diese oftmals vielfältige, verteilte Energiesysteme wie PV-Anlagen, steuerbare Lasten, Batteriespeicher und E-Ladeinfrastruktur nutzen und betreiben.

Im Projekt wurde im Rahmen von AP1 und AP2 ausgewertet, wie die einzelnen Komponenten des digitalisierten Energiesystems verknüpft werden können, welche Angriffsmöglichkeiten bestehen und wie man Manipulation verhindern kann. Nach Analyse dieser Ergebnisse wurde ein Laboraufbau sowohl an der THU als auch an der EKUT sowie ein Demonstrations- und Lehraufbau am WBZU konzipiert und für AP3 und AP4 umgesetzt.

In AP3 wurde bewertet, ob eine inhaltliche Verifizierung dieser Kommunikation zwischen den Komponenten durch Blockchain/Tangles* nach aktuellem technischem Stand möglich ist. Zusätzlich wurde von der EKUT durch die Entwicklung und Umsetzung des enerDAG* eine Blockchain/Tangle-basierte Energiehandelsplattform für Prosumer und Konsumenten in lokalen Nachbarschaften realisiert., Mit enerDAG wurde eine inhaltliche Verifizierung dieser Kommunikation als auch die Speicherung und Validierung von Transaktionen durch den Einsatz des Tangle-Konzepts und das dynamische Kalkulieren und Handeln durch Smart Contract* innerhalb des Smart Grids ermöglicht. . Um Sicherheitslücken aufzuzeigen, wurde am Ende des AP ein Penetrationstest bzw. Konzeptreview des enerDAG unter Berücksichtigung der Analyse sicherheitsrelevanter Aspekte und der Erarbeitung verschiedene Angriffsszenarien von „Code White" durchgeführt. Insgesamt konnten neun Bedrohungskategorien identifiziert werden, die verschiedene Schutzziele (Integrität, Verfügbarkeit und Vertraulichkeit) des enerDAG verletzen und potenziell eine Bedrohung für seine Benutzer darstellen könnten. Ebenso wurden Mitigationen für die verschiedenen Bedrohungsfälle entwickelt und teilweise bereits umgesetzt.

Im Rahmen von AP4 wurde am WBZU eine Laborumgebung für Schulungszwecke aufgebaut sowie ein Schulungsangebot entwickelt.

Mit dem Projekt SEP konnte eine flexibel erweiterbare Plattform für den lokalen Energiehandel konzipiert und im Laboraufbau und in Simulationen erprobt und validiert werden. Damit ist ein Prosumer nicht mehr auf seine Liegenschaft beschränkt, sondern kann auf vielfältige Weise mit den anderen teilnehmenden Prosumern interagieren. Das eröffnet sowohl den Prosumern mit PV-Anlagen als auch Energiekunden ohne PV-Anlagen zusätzliche Möglichkeiten, um von der Energiewende zu profitieren.

Inhalt

Abbildungsverzeichnis

Kenndaten/Autoren/Durchführende Stellen

Titel	SEP-Abschlussbericht	
Einrichtungen	Technische Hochschule Ulm (THU) - Institut für Energie- und Antriebstechnik Eberhardt Karls Universität Tübingen (EKUT) - Lehrstuhl für Eingebettete Systeme Weiterbildungszentrum für innovative Energietechnologien der Handwerkskammer Ulm (WBZU)	
Erstellt von	Munkhtsetseg Baatar (THU) Falko Ebe (THU) Christoph Groß (EKUT) Peter Pioch (WBZU) Günther Maetze (WBZU) Jeromie Morris (THU) Christoph Kondzialka (THU) Gerd Heilscher (THU)	

1. Hintergrund, Stand der Technik und Ziele

1.1 Smart Grids und Smart Meter Infrastruktur (THU)

Stand der Technik und Forschungslücken

Der Ausbau erneuerbarer Energien sowie deren große Akzeptanz in der Bevölkerung, den Kommunen, aber auch vielen Unternehmen, stellt viele Stromnetze schon heute vor Herausforderungen.

1. Vernetzung von Prosumern: Der zunehmende Wandel vom klassischen Stromkunden hin zum eigenständig agierenden Prosumer verleiht einer intelligenten Vernetzung aller Energiesysteme in Baden-Württemberg zusätzliche Bedeutung.

   Die Vernetzung von Prosumern bietet neben großen Chancen für die Energiewende auch eine Reihe von Herausforderungen (s. unten). Gleichzeitig steht Baden-Württemberg vor dem Wandel des zentralen Energiesystems mit wenigen großen, zentralen Kraftwerken hin zu einem dezentralen Energiesystem mit Millionen dezentraler Einspeiser.

   Dezentrale Energiesysteme wurden bisher in ein Energiesystem integriert, das Top-Down organisiert ist. Im Rahmen des EEG wurden Sonderrollen für die lokalen Energiesysteme und die direkte Nutzung dieser Energie kreiert (z. B. Solarsteuer auf die lokale Nutzung der Energie). Ein zukünftiges verteiltes Energiesystem, das in ein intelligentes Stromnetz eingebettet ist, bietet völlig neuartige Möglichkeiten. Ein Prosumer, der selbst regenerative Energie im Überschuss bereitstellt und diese z. B. in einem Quartierspeicher zwischenspeichert, wird diese Überschüsse für andere Prosumer abrufbar machen oder diese selbst an anderer Stelle verbrauchen wollen. Das Projekt SecureEnergyProsumer hat die Machbarkeit dieser Energiesystem-dienstleistungen untersucht und in einem auf drei Standorte verteilten Laboraufbau demonstriert.

2. Der Sicherheitsaspekt, sowohl im System (Energieversorgung) als auch für die benötigte IKT (Informations- und Kommunikationstechnologie) der Smart Grid-Komponenten ist ein entscheidender Punkt für das Gelingen der Energiewende, nicht nur in Baden-Württemberg. Zunehmende, dokumentierte Angriffe auf die bestehenden Energiesysteme erfordern bereits beim Aufbau eines Smart Grids mit Millionen Teilnehmern besondere Aufmerksamkeit hinsichtlich der IT-Sicherheit.

3. Smart Meter Infrastruktur: Mit der verbindlichen Einführung der Smart Meter Infrastruktur für alle Solarstromanlagen ab einer Nennleistung von 7 kWp steht eine solide Grundlage für die Umsetzung dieser Ziele zur Verfügung.

   Die im Rahmen des Projekts verwendete Blockchain-Technologie ermöglicht die direkte Verbindung von Prosumern und deren Komponenten mit anderen

Prosumern oder Komponenten des Energienetzes. So könnten Prosumer den lokal zeitweise überschüssigen PV-Strom z. B. in einen Quartierspeicher (EnergyStorageasaService) laden, um diesen zu einem späteren Zeitpunkt verbrauchen zu können. [Abbildung 1].

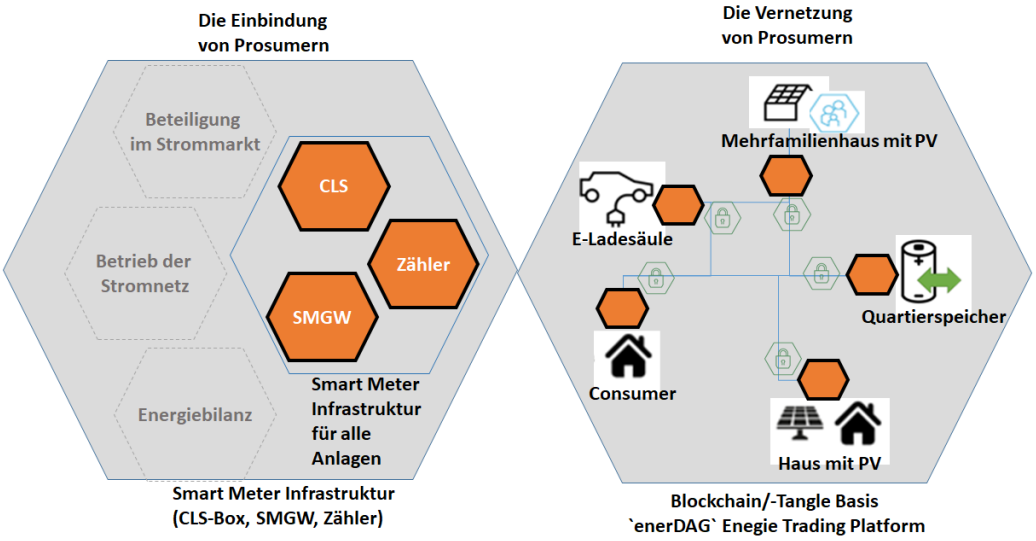


Abbildung 1: Konzept zur Umsetzung

Ausgangspunkt für die SEP-Entwicklung war die Smart Meter Infrastruktur, basierend auf Smart Meter Gateways* und Controllable Local Systems* (CLS-Steuerboxen). Im Projekt CLS-App hat die Hochschule Ulm bereits vier Anwendungen für CLS-Steuerboxen entwickelt (zur Kommunikation mit Solarwechselrichtern, elektrischen und thermischen Speichersystemen sowie E-Ladesäulen). Das Projekt SecureEnergyProsumer konnte auf diesen Ergebnissen aufbauen und setzt in Kooperation mit der Uni Tübingen Blockchain-/Tangle-Technologie ein, um diese nun als Anwendungen zu vernetzen.

1.2. Blockchain-Technologie (EKUT)

Stand der Technik und Forschungslücken

Die Smart Meter-Infrastruktur ermöglicht das Messen der Energienutzung in hoher zeitlicher Auflösung und bietet eine Infrastruktur für sichere Kommunikationsstrecken. Eine inhaltliche Verifizierung dieser Kommunikation für den lokalen Energiehandel ist jedoch schwer möglich. Der Einsatz der dezentralen Datenspeicherart „Blockchain“ beziehungsweise genauer der Distributed Ledger Technologie (DLT) sowie der Einsatz klassischer kryptographischer Funktionen tragen zur Lösung dieses Problems bei. Die erste Referenzimplementierung einer Blockchain wurde 2008 im Rahmen der Kryptowährung Bitcoin vorgestellt. Die Vorteile von DLTs sind das manipulations-sichere und dezentrale Speichern von Informationen, im Fall von Bitcoins der Transaktionshistorie.

Abbildung 2 zeigt die grundsätzliche Funktionsweise einer Blockchain. Jedoch beinhaltet diese Implementierung aus Sicht von eingebetteten Systemen, wie z. B. des Smart Meters, verschiedene Nachteile.

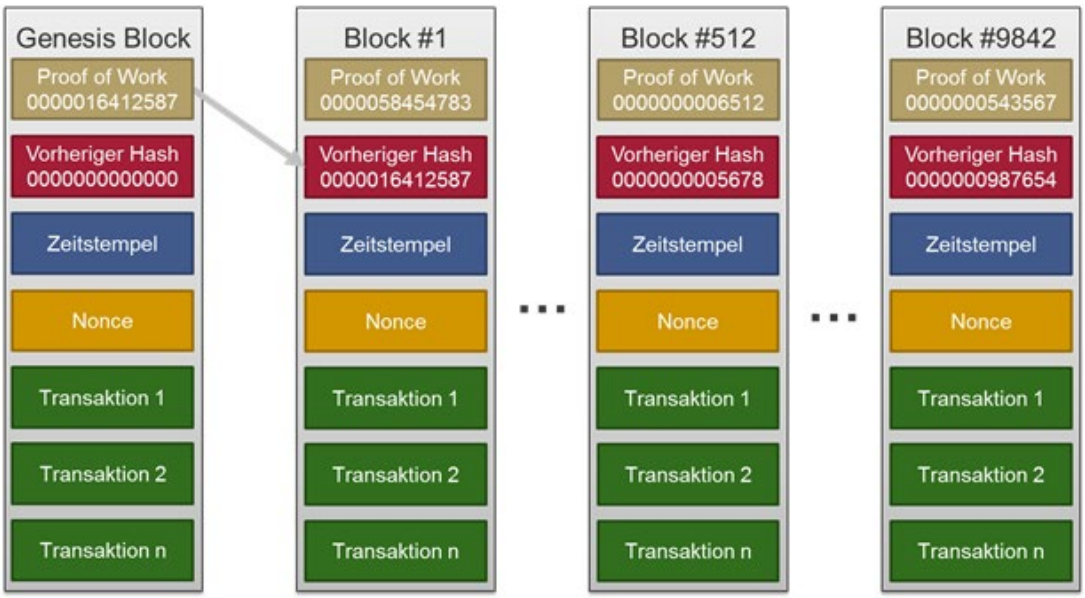


Abbildung 2: Beispiel für die Darstellung einer Verarbeitung in einer Blockchain

Zur Sicherstellung der Integrität der klassischen Blockchain muss die ganze Kette digitaler Datenblöcke vorgehalten werden, was im Laufe der Zeit zu riesigen Datenmengen führt, die auf jedem einzelnen Gerät vorgehalten werden müssen. Auch die Beschränkung der Transaktionen pro Zeit ist für ein Netz von vielen Teilnehmern, deren Transaktionen auf jeden Fall berücksichtigt werden müssen, von Nachteil. Ein Lösungsansatz, der diese beiden Probleme löst, ist die Datenstruktur des sogenannten „Tangles“. Hier werden keine starren Ketten, sondern gerichtete, azyklische Graphen, eine Art „Gewirr” aus Knoten und Kanten, eingesetzt (siehe Abbildung 3). Diese skalieren auch bei großen Teilnehmerzahlen, um die Transaktionen zu protokollieren. Ein weiterer Unterschied ist, dass bei Bitcoin und ähnlichen digitalen Währungen sogenannte “Coins”, also Wertgegenstände, ausgetauscht werden. Durch deren Verwendung als illegales Zahlungsmittel und damit verbunden dem meistens sehr hohen Energiebedarf von Blockchains, sind diese leider in Verruf geraten. Diese Eigenschaften treffen jedoch nicht grundsätzlich auf alle DLTs zu. Daher muss man für den angestrebten Verwendungszweck Unterscheidungen treffen und die passende DLT verwenden.

Abbildung 3: Graphennetzwerk als Erweiterung einer Blockchain (Tangle)

Des Weiteren kann eine zentrale Autorität die protokollierten Transaktionen validieren, verarbeiten und Snapshots* erzeugen. Snapshots enthalten nur den letzten Bereich des Tangles, der noch nicht als ausreichend verifiziert angesehen wird. Dieser wird wieder an die Teilnehmer verteilt, um weitere Transaktionen anzufügen. Hierdurch ist die Größe des Tangles, die von den Teilnehmern vorgehalten werden muss, beschränkt. Dadurch gewährleisten Tangles die Integrität und Sicherheit von Blockchains, bei gleichzeitiger Skalierbarkeit und effizienter Nutzung, auch in verteilten, eingebetteten Systemen wie bei Smart Grids. In Abbildung 3 ist eine von uns umgesetzte Variante des Tangles zu sehen. Zusätzlich erlaubt die Verwendung von Smart Contracts die automatisierte Vertragsdurchführung beim Energiehandel. Dies ermöglicht eine automatische, verifizierte Buchhaltung.

1.3. Ziele des Projekts (THU)

- **Dezentralisierung:** Erstellung der flexiblen Energiehandelsplattform “enerDAG”.
- **Sicherheit:** Der sichere Informationsaustausch zwischen Prosumern sowie zwischen Prosumer und Stromnetzbetreiber.
- **Regelungskonzepte und Betriebsstrategien**: Neben dem Informationsaustausch (Netzzustandsinformation) und aktiven Steuerbefehlen (Einspeisemanagement) sind auch Billinginformationen (Bezahlprozesse) Teil dieser Infrastruktur.
- **Datenschutz/Anonymität:** Auf die Anonymität wurde in enerDAG größter Wert gelegt. Die übertragenen Informationen und Befehle unterliegen hohen Ansprüchen an Datenschutz und Manipulationssicherheit. Da der Datenfluss durch eine Vielzahl von Systemen unterschiedlicher Besitzer geleitet, umgewandelt und aggregiert wird, ist es eine Herausforderung, diesen Ansprüchen gerecht zu werden und das Vertrauen der Prosumer in die Nutzung dieser Technologie zu gewinnen. Diese Herausforderung soll durch die

Anwendung von Kryptographie mittels eines Blockchain-Verfahrens gelöst werden.

- **Abrechnung und Abwicklung:** Durchführung durch Maintainer*: z. B. Messstellenbetreiber, Netzbetreiber, u. Ä.
- **Testsystem**: Mit dem trilateralen Reallabortest der Smart Grids Forschungsgruppe der Technischen Hochschule Ulm und dem Lehrstuhl für Eingebettete Systeme an der Eberhardt Karls Universität Tübingen (EKUT) wird die komplette Infrastruktur für den verteilten Test der Sicherheitsinfrastruktur für Prosumer unter realistischen Bedingungen, inklusive von Speichersystemen, steuerbaren Lasten und E-Ladesäulen aufgebaut. Zur Evaluation des Projektes werden Penetration Tests* durchgeführt. Zuletzt wird diese Infrastruktur innerhalb des WBZU auch zu Schulungszwecken genutzt.

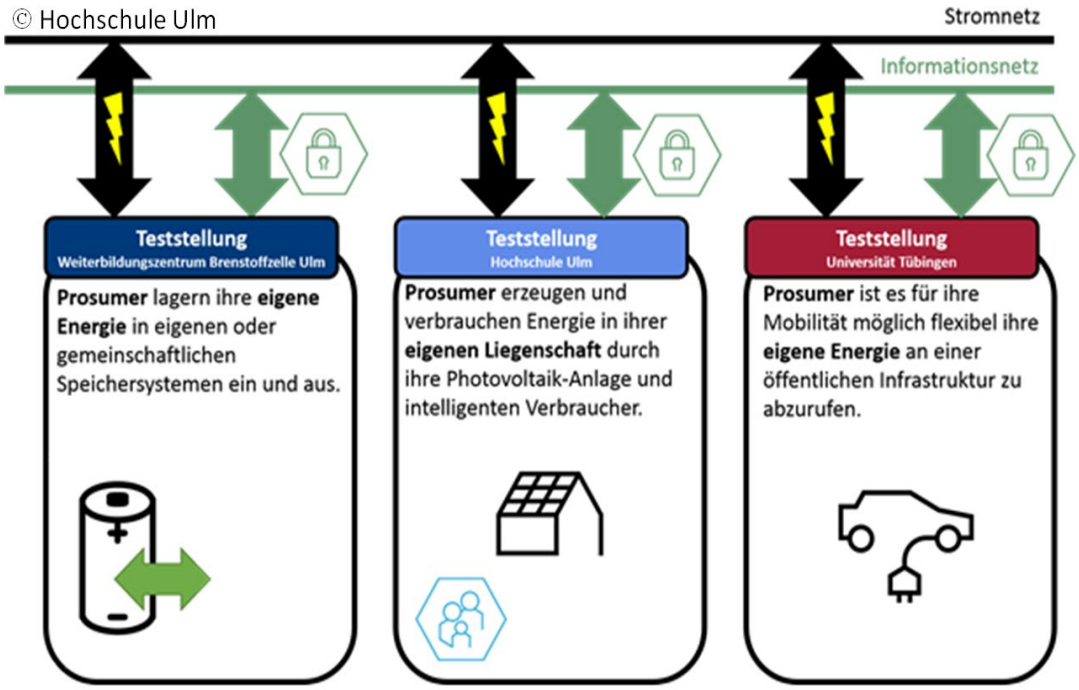
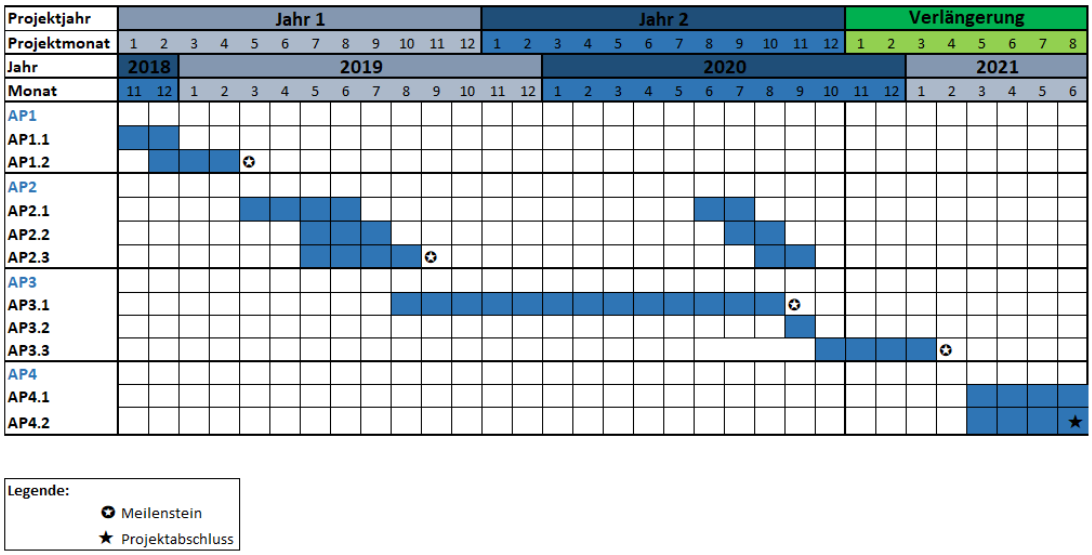


Abbildung 4: Umsetzung der verteilten Labortests bei den Projektpartnern

2. Projektablauf und Methodik

Das Projekt SecureEnergyProsumer bietet eine Lösung für den Umbau des Energiesystems in Baden-Württemberg und die Einbindung der Prosumer in ein dezentrales Energiesystem. Es bietet Möglichkeiten, die entstandenen Ansätze ggf. weiterzuentwickeln und in diversen Szenarien zu erproben. Darüber hinaus konnte ein sicheres Informations- und Kommunikationssystem bzw. eine Vernetzung zwischen Prosumern ermöglicht werden, so dass völlig neue Wege der Energieverteilung möglich sein können.

2.1 Zeitlicher Ablauf



Legende:
Meilenstein
Projektabschluss

2.2 Übersicht Arbeitspaket (THU)

Um dieses Projekt zu realisieren, wurden die gestellten Aufgaben in 4 Arbeitspakete mit Unterpaketen unterteilt und den beteiligten Projektpartnern nach Schwerpunkten zugeteilt. Die Inhalte der jeweiligen Arbeitspakete sind zur Veranschaulichung in der nachfolgenden Tabelle dargestellt.

APs	UAP	
AP1		**Grundlagen/Status Quo der IT-Security in der Energiewirtschaft**
	AP1.1	**Zusammenführung der Domains dezentrale Energiewirtschaft und IT- Security**
		Um eine gemeinsame Sprache und ein gemeinsames Verständnis über die Domains Energiewirtschaft und IT-Security zu haben, wurden in diesem AP die aktuellen Trends der Energiewirtschaft sowie die daraus resultierenden und darauf aufbauenden Herausforderungen und Lösungskonzepte beschrieben. Bezogen auf das Gesamtprojekt soll hierbei die Notwendigkeit des Einsatzes von IT-Systemen ausgeführt werden.
	AP1.2	**IT-Security in einer zukünftigen dezentralen Energiewirtschaft**
		Um des zukünftigen Szenariorahmens einer verteilten Energieversorgung mit Prosumern, Speichern, steuerbaren Lasten und E-Mobilität in einer digitalen Energiewirtschaf gerecht zu werden, haben wir die relevanten ersten Anwendungsfälle mit SGAM* definiert und daraus zwei gemeinsame Szenariorahmen, a und b, entwickelt.
AP2		**Anforderungsanalyse**
	AP2.1	**Systemanalyse: Generierung von Angriffsszenarien und deren Auswirkung auf das Realsystem**
		Anhand der Szenariorahmen a und b erfolgte die Risikoanalyse für die Umsetzung der im Szenariorahmen definierten technischen Systeme. Aus diesen Risiken wurden im Rahmen des AP2.2 die Anforderungen an die Sicherheitsarchitektur festgelegt und mit geeigneten Maßnahmen hinterlegt.
	AP2.2	**Anforderungsanalyse: Darstellung der momentanen Sicherheitsstandards und Kommunikationswege innerhalb des Smart Grid**
		Hinterlegung von Anforderungen an die Sicherheitsarchitektur und geeignete Maßnahmen aus der Szenario- & Risikoananalyse.

	AP2.3	**Anforderungsanalyse: Ausgestaltung des Laboraufbaus sowie Konzipierung des Demonstrations- und Lehraufbaus am WBZU**
		Design des Laboraufbaus sowie Konzipierung des Demonstrations- und Lehraufbaus am WBZU.
AP3		**Umsetzung und Test**
	AP3.1	**Implementierung der Blockchain-Infrastruktur im Testfeld des Smart Grid Labors (THU) und an der EKUT**
		Implementierung der Blockchain-Infrastruktur und Integration im Testfeld des Smart Grid Labors.
	AP3.2	**Penetration Test und Evaluation**
		Durchführung des Auswahlverfahrens für die unabhängige technische Evaluation des Forschungsgegenstands (Penetration Test, vgl. AP3.2); wurde unter Federführung des WBZU durchgeführt. (Kapitel 3.7)
	AP3.3	**Optimierung der IT-Sicherheit**
AP4		**Wissensvermittlung**
	AP4.1	**Umsetzung der Laborumgebung am WBZU zu Schulungszwecken**
		Aufbau der Laborumgebung für Schulungszwecke.
	AP4.2	**Schulungsangebot für Energiewirtschaft und Handwerk am WBZU**
		Entwicklung eines Schulungsangebots für Energiewirtschaft und Handwerk.

Tabelle 1 Arbeitspaketen und Unterpaketen

2.3 Meilensteine

Als relevante Meilensteine wurden folgende erfasst:

MS1: Abschluss des Szenariorahmens für ein regeneratives, verteiltes Energiesystem:

Es wurden Workshops zu den Themen „Energiewirtschaft/Energietechnik für Informatiker" sowie „IT-Security für Energietechniker" durchgeführt. Aufbauend auf die Workshops konnte ein gemeinsamer Szenariorahmen (vgl. AP1.2) für ein regeneratives, verteiltes Energiesystem entwickelt werden.

MS2: Abschluss der Anforderungs- und Systemanalyse:

Aufbauend auf den Szenariorahmen erfolgte die Risikoanalyse für die Umsetzung der im Szenariorahmen definierten technischen Systeme. Aus den daraus abgeleiteten Risiken wurden im Rahmen des AP2.2 die Anforderungen an die Sicherheitsarchitektur festgelegt und mit geeigneten Maßnahmen hinterlegt.

Die Kernerkenntnis aus der Szenario- & Risikoananalyse war, dass für den angedachten Handel zwischen Prosumern typischerweise kontinuierlich, aber dafür nur mit sehr kleinen Werten von sehr vielen Teilnehmern gehandelt wird. Die Evaluation bestehender technologischer Konzepte hat gezeigt, dass die Tangle-Technologie der verwandten Blockchain-Technologie gegenüber für diesen Anwendungsfall zu bevorzugen ist. Durch eine Szenario- & Risikoanalyse während der Implementierung des Systems konnten die funktionalen Anforderungen an das System für die nachfolgenden Arbeitspakete definiert werden.

MS3: Implementierung der Tangle-Infrastruktur auf den CLS-Komponenten:

Im Rahmen der Implementierung des Systems konnten wir sowohl die Verbindung zwischen dezentralen Anlagen (PV, E-Mobilität) und Handel als auch die Implementierung der Tangle-Infrastruktur auf den CLS-Komponenten abschließen.

MS4: Ergebnisse des Penetrationstests und Evaluation der Optimierung des IT-Sicherheitskonzeptes:

Vorbereitung und Durchführung eines Auswahlverfahrens für eine unabhängige technische Evaluation des Forschungsgegenstands (Penetration Test) unter Federführung des WBZU. Darüber hinaus konnte die Umsetzung der Optimierungsvorschläge fertig gestellt werden. Mehr zu den Ergebnissen des Penetrationstests und der Evaluation der Optimierung des IT-Sicherheitskonzepts finden Sie im Anhang.

3. Systementwurf

3.1. Hintergrund (THU)

Use Case PV Handel Lokal (THU) - SGAM (AP 1.2)

Für die Beschreibung der relevanten Anwendungsfälle haben wir mit Hilfe der Use Case-Methodik ein gemeinsames Verständnis über die jeweiligen Fachdomainen hinweg erstellt. Dieses orientiert sich an der DIN IEC/TS 62913-1: Generische Anforderungen an Smart Grids – Teil 1: Anwendung der Anwendungsfallmethodik.

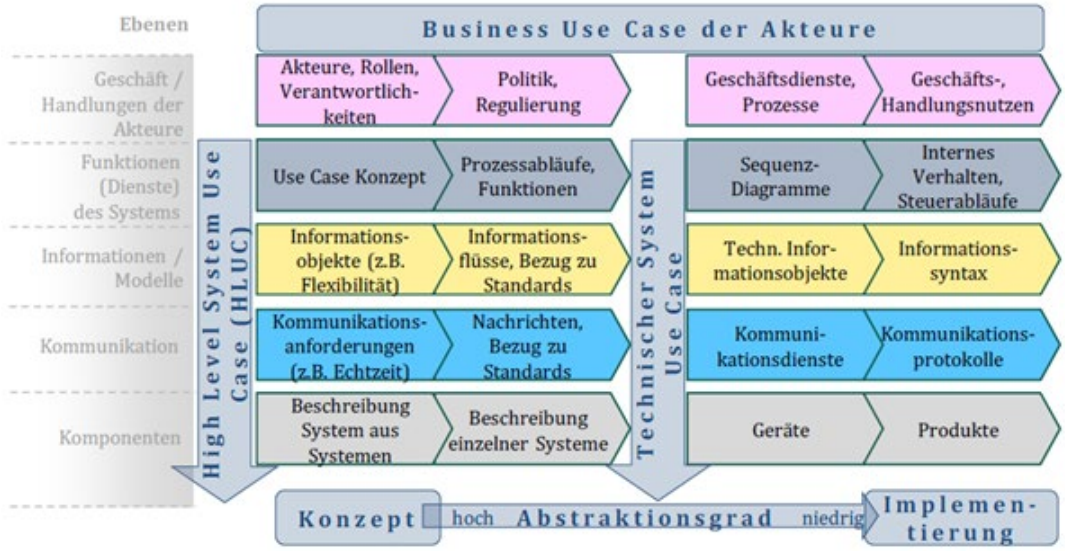


Abbildung 6: Darstellung der Use Case-Methodik zur Beschreibung des Anwendungsfalls

Grundlage war die Entwicklung des Szenariorahmens einer verteilten, digitalisierten Energieversorgung in zwei Schritten:

- Verteiltes Energiesystem mit Evolution des zentralen Energiehandels zu lokalem, zellenbasiertem Handel bis hin zum direkten Energieaustausch zwischen einzelnen Teilnehmern oder Komponenten.
- Definition der Interaktion zwischen Marktteilnehmern (Smart Contracts) mit Energienutzern, Prosumern, Energiespeichern und E-Mobilität.

3.2. Festgelegte Anwendungen zur Umsetzung

a. Mieterstromabrechnung

Das zuerst betrachtete Szenario stellt die Erweiterung des Mieterstrommodells und die Anwendung von Blockchain-Technologie in den Fokus der Untersuchung. Die Kernfrage stellt dabei der Wunsch des Kunden, vom lokal produzierten Strom einer Photovoltaikanlage zu profitieren und die Reststrommenge bei einem beliebigen Energieversorgungsunternehmen zu erwerben. Dabei sollen die Geschäftsprozesse der multiplen Akteure mit Hilfe von Smart Contracts und Blockchain-Technologie abgebildet werden.

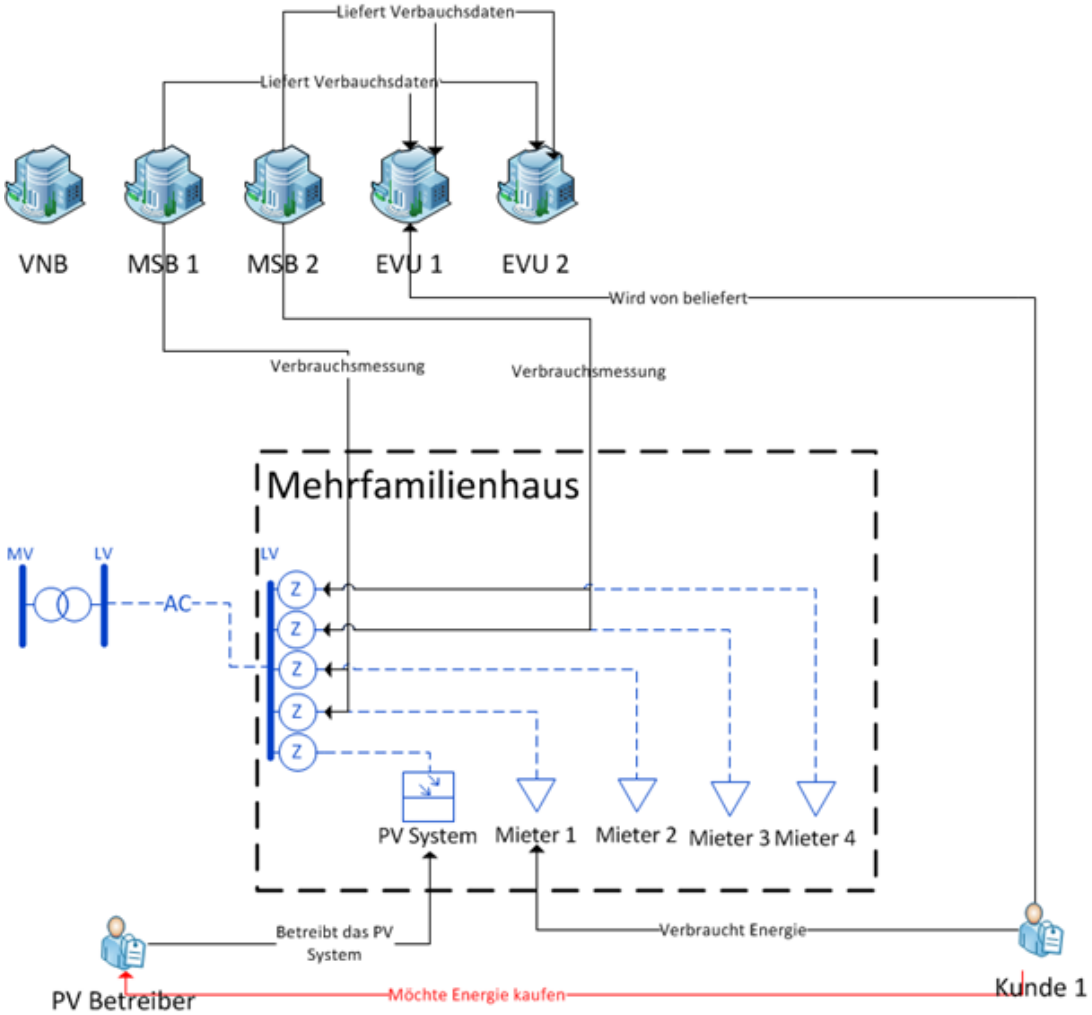


Abbildung 7: Vereinfachte-Darstellung des Multi-Mandanten-Mieterstrommodell

Transaktionen

Abbildung 8 zeigt Transaktionen, die einen bereits vergangenen Zeitschritt abrechnen. Links die Energieproduktion der PV-Anlage als vier Einheiten dargestellt. Einheit 1 wird basierend auf dem lokalen Handel an den Kunden 1 verkauft. Da dieser in unserem Modell seinen Gesamtbedarf noch nicht durch den lokalen Handel gedeckt hat, erfolgt bilanziell die Lieferung der Restmenge durch EVU* 1. Das Gleiche gilt für Kunde 2 und das zugeordnete EVU 2. Etwaige Restmengen werden an

überlagerten Märkten bzw. Börsen vermarktet und stellen eine generische Systemgrenze dar.

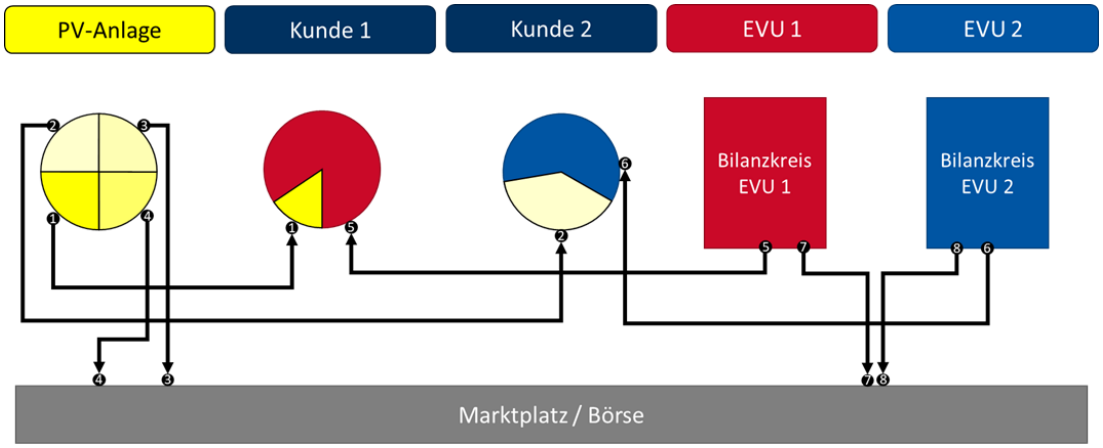


Abbildung 8: Transaktionen

Handelsprinzip bzw. Settlement auf Ex-Post Basis

Die Auflösung und Verrechnung der Energiemengen erfolgt nach Ablauf des jeweiligen Zeitschritts, da erst zu diesem Zeitpunkt alle Energiemengen exakt bekannt sind. Dies ist ersichtlich in Abbildung 9, die zeigt, wie „Verbraucher K1“ für den Zeitraum 09:00 bis 09:15 Uhr eine Energiemenge von 1,6 kWh von der PV-Anlage „PV1“ erwirbt. Dieses Prinzip wird auch als Ex-Post Handel bezeichnet. Die Entscheidung für den Ex-Post Handel ist während des Projektverlaufs gefallen, da für ein zweistufiges Verfahren zusätzlich die Aspekte Prognose und Weiterverrechnung berücksichtigt werden müssten.

Der Restmengenlieferant trägt natürlich ein gewisses Risiko hinsichtlich des Ausgangs der Transaktionen, welches durch Maßnahmen wie ausreichend großer Kundenstamm bzw. höhere Energiepreise für Restmengen entsprechend mitigiert werden muß.

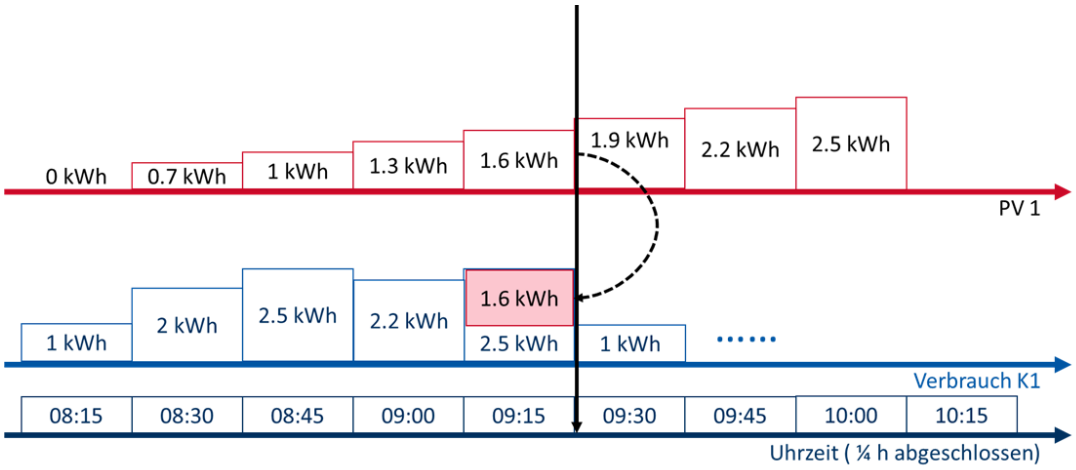


Abbildung 9: Handelsprinzip

b. Lokaler Multiversorgermarkt

Im Rahmen von AP3.1 haben wir ein umfassendes Konzept, ein potentielles Marktdesign und eine Simulation eines lokalen Energiemarktes von bis zu 200 Prosumern entwickelt. Unser Ansatz basierte dabei auf einer verteilten Informations- und Kommunikationstechnologie, z. B die der Smart Contracts zu einer speziellen Variante eines Tangles, der den dezentralen Charakter der lokalen Energiemärkte unterstreicht. Darüber hinaus haben wir im Rahmen von AP3.2 die technologische Bewertung der Tangle- /Blockchain-Technologie als wichtigste Informations- und Kommunikationstechnologie des lokalen Energiemarktes durchgeführt.

Abbildung 10 stellt die Erweiterung des ersten Anwendungsszenarios auf ein vollständiges Niederspannungsnetz dar, ergänzt durch die Ladeinfrastruktur.

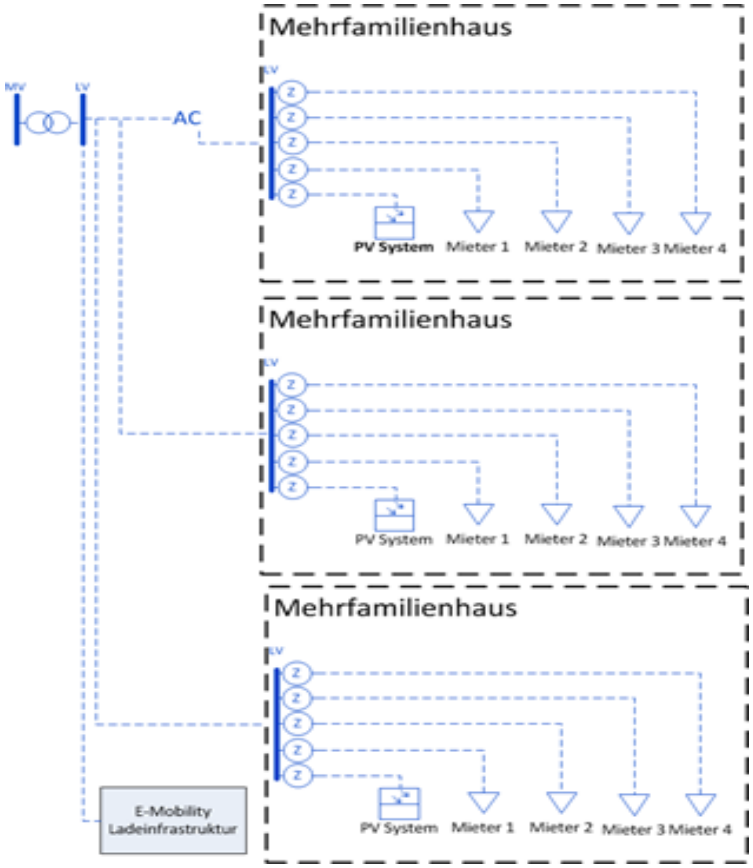


Abbildung 10: Schematische Darstellung des Anwendungsfalls Lokaler Markt

Unsere Kernerkenntnis aus der Szenario- & Risikoananalyse war, wie weiter oben bereits angeführt, dass beim angedachten Handel zwischen Prosumern typischerweise kontinuierlich, aber dafür nur mit sehr kleinen Werten von sehr vielen Teilnehmern gehandelt wird. Die Evaluation bestehender technologischer Konzepte hatte, wie ebenfalls bereits erwähnt, gezeigt, dass die Tangle-Technologie gegenüber der Blockchain-Technologie für den Anwendungsfall „Handel zwischen Prosumern“ zu bevorzugen ist. Diese ist dafür gut skalierbar und kann auf verschiedene Netze aufgetrennt werden, um den Rechenaufwand einerseits und die Datenübertragungsmenge andererseits für einzelne Teilnehmende auf einen geringen Wert zu reduzieren.

3.3. Threatmodellierung IT

Mit dem enerDAG konnte ein erster Prototyp erstellt werden, welcher die grundsätzliche Funktionsweise demonstriert und die Auswirkungen verschiedener Strategien auf die Netzlast simuliert.

Der Tangle ist ein gerichteter azyklischer Graph, welcher aus Transaktionen und deren Referenzen besteht. Jeder Knotenpunkt kann Transaktionen hinzufügen, indem er simple Regeln befolgt. Diese wären beispielsweise das Referenzieren von mindestens zwei älteren Transaktionen, welche –„Tips“ heißen, und das anschließende Veröffentlichen an seine Nachbarn. Alle anderen Knoten würden diese Transaktionen dann durch ein Gossip Protokoll* erhalten, würden diese – falls korrekt – akzeptieren und diese Transaktionen in ihre eigene Sicht der Tangle-Struktur einbauen.

Der Tangle ist auch eine chronologisch geordnete Datenstruktur, da neue Transaktionen nur ältere referenzieren können und dies auch nur innerhalb eines begrenzten Zeitrahmens. Daher wächst der Tanglegraph in eine Richtung (siehe Abbildung 11).

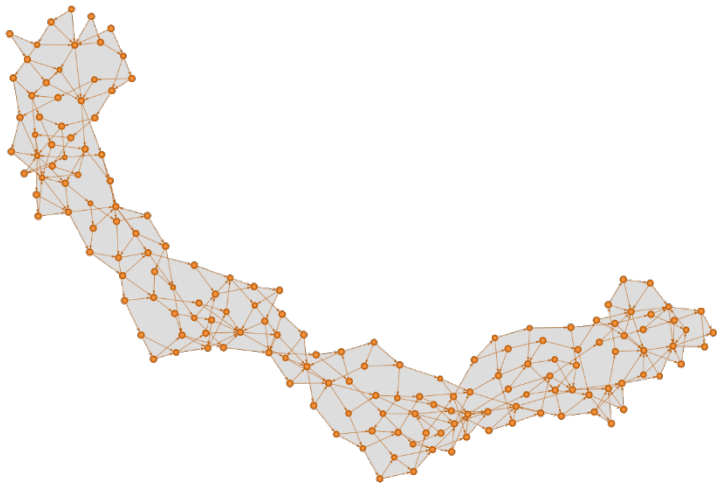


Abbildung 11: Tanglegraph

Das bedeutet, der Tangle ist einer Blockchain ähnlich, aber ohne Blöcke und ohne eine Kette und kann daher eine Vielzahl der Probleme der klassischen Blockchain lösen, wie z. B. Gebühren, Mining und die limitierte Anzahl von Transaktionen pro Sekunde.

Zusätzlich ermöglicht der Transaktionsfluss über die Zeit des Tangles das Löschen von älteren Transaktionen für freien Festplattenspeicher, da diese zu einem deutlich späteren Zeitpunkt nicht mehr referenziert werden. Und es erlaubt eine chronologische Sortierung, um zu überprüfen, welche Transaktion für die Verifizierbarkeit zuerst übertragen wurde.

Die Tangle Idee, welche wir für enerDAG bzw. SecureEnergyProsumer verwenden, stammt vom sogenannten IOTA's Tangle Konzept [Popov, Serguei, "The Tangle," 2018.] ab. Es wurden jedoch signifikante Änderungen des IOTA Protokolls vorgenommen. So verwendet unser System keine Tokens, und wir verwenden ein binäres anstatt eines tertiären Systems. Für dieses Projekt wurde, wie bereits weiter oben beschrieben, der Ex-Post Handel ausgewählt, da die Vorhersage und darauf basierendes Handeln der Energie ein eigenes, schwieriges Problem ist.

Ein zentraler Nachbarschaftsmarkt wird im enerDAG System als Smart Contract aufgesetzt, der in fixen 5- Minuten-Intervallen ausgeführt wird. Haushalte, die am Energiemarkt für einen bestimmten Zeitraum teilnehmen wollen, senden ihre Energiebilanz und Ein- bzw. Verkaufspreise an den Smart Contract. Zur Ausführungszeit wertet der Algorithmus des Nachbarschaftsmarkts alle eingesendeten Energiebilanzen aus und liefert die Ergebnisse des Energiehandels. Ein Knoten (hier: ein Haushalt) profitiert vom Smart Contract, solange folgende Bedingungen erfüllt sind:

- Er nimmt mit einem Angebot im gehandelten Zeitraum teil.
- Das Ergebnis des Smart Contracts ist eines, bei welchem die Überproduktion bzw. der Bedarf des Knotens gehandelt wird.
- Das Ergebnis, welches den Handel enthält, wird vom Gesamtnetzwerk als Mehrheitsergebnis akzeptiert.

Um am Markt teilnehmen zu können, sendet ein Knoten, wie oben beschrieben, eine Transaktion mit seiner Energiebilanz und seinem Preis an den Smart Contract. Per Definition des Smart Contract erlaubt der Marktplatz jedem Teilnehmer, nur ein Gebot zu senden. Dies reduziert die Anzahl an notwendigen Transaktionen auf ein Minimum. Der Marktalgorithmus ordnet dann Kauf- und Verkaufsangebote automatisiert zu. Alle teilnehmenden Knoten haben ein finanzielles Eigeninteresse, das Ergebnis des Smart Contracts innerhalb der Zeitspanne selbst zu berechnen. Da dies der normale Operationsmodus ist, werden Knoten natürlicherweise an der Berechnung und Absicherung des Resultats teilnehmen. Ein einzelner, lokaler Marktplatz umfasst dabei eine Nachbarschaft, welche auf Grund von Transportkosten durch den nächsten Transformator abgegrenzt wird. Dadurch beinhaltet ein Nachbarschafts-Smart-Contract 150 bis 200 Teilnehmer.

Aus diesem Grund ist es genauso akzeptabel, wenn einzelne Knoten zu einem Zeitpunkt nicht an der Ausführung eines Smart Contracts (z.B. auf Grund von Verbindungsproblemen), da eine Vielzahl von Teilnehmern weiterhin die Ergebnisberechnung korrekt ausführen und durch den Konsensmechanismus trotzdem ein Gesamtergebnis gefunden wird. Mit jedem weiteren teilnehmenden Knoten gibt es einen weiteren Akteur, welcher Anreize hat, sich korrekt zu verhalten, das korrekte Ergebnis des Marktalgorithmus zu berechnen und dieses mit seinen Nachbarn zu teilen.

Da enerDAG ein tokenloses, privates DLT ist, also keine Tokens bzw. Coins transferiert werden, müssen spezielle Aufgaben, wie die Validierung und die Abrechnung des Energieflusses zuverlässig ausgeführt werden. Daher können Energie- und Infrastrukturanbieter, wie z. B. ein Energieversorger oder ein Messstellenbetreiber, einen speziellen Knoten in jeder Nachbarschaft mitlaufen lassen, der sogenannte Nachbarschafts-Maintainer.

Ausgestaltung eines Smart Contracts

Smart Contracts werden innerhalb des enerDAG-Systems auf den Knoten gespeichert, die an diesem Vertrag teilnehmen. Wie jeder normale Knoten im Netzwerk, wird ein Smart Contract durch seine Adresse identifiziert. Um mit einem spezifischen Vertrag zu interagieren, können Transaktionen mit der Adresse des Smart Contracts als Empfängeradresse in der Transaktion versendet werden. Der Smart Contract an sich ist ein Programm, das regelmäßig in einem gewissen Intervall ausgeführt wird. Für enerDAG sind das zum größten Teil 5-Minuten-Intervalle.

Ein Smart Contract besteht dabei aus zwei großen Programmbausteinen:

- *Receive Transaction:* Hier werden eingehende Transaktionen mit der passenden Zieladresse verarbeitet und für den jeweiligen Smart Contract passende Funktionen ausgeführt.
- Execute Contract: Ist eine regelmäßig ausgeführte Aufgabe, z. B. für die Ausführung des Marktalgorithmus alle 5 Minuten. Das dabei entstehende Ergebnis wird zum Knoten für das weitere Verarbeiten und für Mehrheitsabstimmungen weitergeleitet.

Ergebnisse der Smart Contracts und Mehrheitsabstimmungen

Wenn ein neues Ergebnis für einen Smart Contract berechnet wird, wird versucht, dieses Ergebnis zu verifizieren, indem ein Konsens innerhalb des Netzwerks erzielt wird. Ein abweichendes Ergebnis kann bedeuten, dass der Teilnehmer selbst ein falsches Ergebnis berechnet hat (beispielsweise durch fehlende Transaktionen, Verbindungsverluste,...) und nun das korrekte Ergebnis von anderen Knoten übernehmen muss. Es könnte aber ebenso bedeuten, dass andere Knoten ein falsches Ergebnis verbreiten (bösartig oder unbeabsichtigt). Daher ist eine Zweidrittelmehrheit zum Überstimmen für ein verifizierbares Resultat notwendig.

Gossip Protokoll

Das Transportprotokoll ist eine Art verifiziertes Gossip Protokoll. Ein teilnehmender Knoten im Netzwerk erstellt eine neue Transaktion und verschickt diese an seine Nachbarn. Diese Nachbarn empfangen ihre Transaktionen, wissen aber nicht, wer diese Transaktion erstellt hat, nur, wer diese Transaktion an sie gesendet hat. Sie überprüfen und verifizieren die Transaktion auf formale Faktoren und falls diese korrekt sind, speichern sie diese in ihrer eigenen Datenbank ab und leiten die Nachricht an ihre eigenen Nachbarn weiter. Falls ein Nachbar eine bereits bekannte Transaktion erhält, passiert nichts. Dadurch entsteht eine Art Schneeballsystem, mit

welcher eine Transaktion schnellstmöglich durch das Netzwerk an Nachbarn geleitet wird. Es ist eine der Aufgaben des Maintainer-Knotens, das Netzwerk in einem dafür stabilen Zustand zu erhalten, sodass keine Engpässe oder sogar komplett separierte Netze entstehen. In der folgenden Abbildung 12 wird dies ersichtlich: Knoten 001 erstellt eine neue Transaktion und leitet diese an seine Nachbarn 002, 003 und 004 weiter. Diese senden die Nachricht ebenfalls an ihre Nachbarn weiter, solange sie die Nachricht nicht bereits kennen oder von ihren Nachbarnerhalten haben.

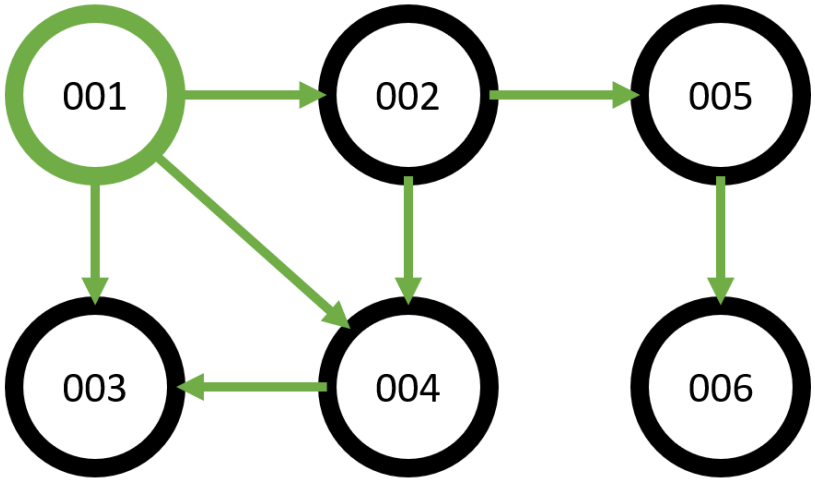


Abbildung 12: Gossip Protokoll

Synchronisationszustand

Wenn ein Knoten eine neue Transaktion erhält, deren referenzierte Transaktionen (Tips) unbekannt sind, speichert es diese neue Transaktion in einer separaten Liste für eine bestimmte Zeitspanne. Wenn es diese neue Transaktion nun von einer Mehrheit seiner Nachbarn innerhalb dieser Zeitspanne erhält, nimmt der Knoten an, dass er nicht mehr synchronisiert ist und erst wieder auf den aktuellen Stand gebracht werden muss. Er fragt daraufhin den fehlenden Tip von seinen Nachbarn an und speichert diesen in seiner Datenbank. Falls auch die Referenzen der neuen Transaktionen fehlen, fragt er auch diese weiter an. Sobald der Synchronisations-zustand aktiv ist, reicht es, wenn eine angeforderte Transaktion nur von einem Nachbarn geliefert wird. Da die Transaktion angefordert ist und keine Smart Contract-Funktionen aufgerufen werden, ist dies schnell und sicher.

Nachbarschafts-Smart Contract

Für den Kauf und Verkauf von Energie zwischen den Partizipierenden ist ein Marktplatz notwendig, auf welchem Angebote und Nachfragen gelistet und zum Ende eines Zeitslots erfüllt werden können. So werden alle Produzenten, Prosumer und Konsumenten einer strommäßig lokalen Nachbarschaft zu einem Marktplatz zusammengeschlossen. Innerhalb eines Zeitslots veröffentlicht dann jeder seine Energiebilanz und seinen Verkaufs- bzw. Einkaufspreis innerhalb des Smart Contracts. Diese werden dann bei der Ausführung verrechnet. Dabei wird nur der Energiebedarf

des letzten Zeitfensters verrechnet, um dadurch keine Annahmen für zukünftige Energiebilanzen treffen zu müssen.

Die grundlegenden Ziele des Nachbarschaftsmarktes sind:

- Anonymität und Pseudonymität: Teilnehmer sollten anonym bleiben können, um die Erstellung von Verbrauchsprofilen durch andere Haushalte vermeiden zu können. Die einzige Ausnahme von dieser Regel ist der Maintainer-Knoten (z. B. durch den Messstellenbetreiber), welcher für Kontrollzwecke einzelne Knoten auch nachträglich verifizieren können muss.
- Sicherheit: Nur Mitglieder einer definierten Nachbarschaft können am Markt teilnehmen oder deren Transaktionen entschlüsseln und mitlesen. Dem Maintainer sollte es möglich sein, sowohl Knoten zum Handel hinzuzufügen als auch deren weiteren Handelsbemühungen bei Missbrauch zu unterbinden.
- Korrektheit: Jedem Haushalt sollte es exakt einmal innerhalb eines Zeitraums möglich sein, seine Energiebilanz zu veröffentlichen und seine Preise festzulegen. Der Marktalgorithmus soll Beteilung und korrektes Verhalten entlohnen.
- Fairness: Kein Knoten soll einen Vorteil durch spezielles Verhalten wie das Warten auf alle Gebote oder das Versenden des Gebots als Letzter erzielen können.

Gebote und Handelspreise

Dem Quartierstromprojekt folgend wurde ein Doppelauktionsmechanismus für die Preis- und Angebotsfindung adoptiert. Jeder Teilnehmer sendet dafür die folgenden Informationen: Energiebilanz, maximaler Kauf- und minimaler Verkaufspreis.

Nachdem ein Marktplatz alle Gebote erhalten hat, werden die positiven Energiebilanzen mit dem niedrigsten Verkaufspreis mit den negativen Energiebilanzen mit dem höchsten Kaufpreis kombiniert. Diese Energiesumme wird gehandelt, bis es entweder nichts mehr zu kaufen oder zu verkaufen gibt. Der Preis setzt sich dabei aus dem Mittelwert von maximalem Kauf- und minimalem Verkaufspreis zusammen. Dies führt dazu, dass sowohl Käufer als auch Verkäufer den gleichen Vorteil haben und alle Haushalte dazu angeregt werden, einen niedrigen Verkaufs- und einen hohen Einkaufspreis festzulegen.

Authentizität und Korrektheit der Gebote

Um einen fairen und reibungslosen Prozess sicherstellen zu können, wird der Handelsprozess in mehrere Schritte unterteilt. In der ersten Phase werden die Verbräuche und Preise verschlüsselt und nach zufälligen Wartepausen an den Markt übermittelt. Um diese Gebote authentifizieren zu können, wird jedes mittels Validierungstokens, welche durch den Hashwert* der Kombination von einzigartigem Validierungsseed* und Vertragsausführungszeit erstellt wird, signiert. Dieses Token

kann durch erneutes hashen* mit einer Liste valider Hashes für diesen Zeitraum verglichen werden. Diese Liste wird in regelmäßigen Zeitabständen durch den Maintainer an die teilnehmenden Knoten verteilt. Dieser Mechanismus ermöglicht es ebenfalls, böswillige Knoten durch das Senden einer Blockliste zu stoppen und ihre Missbräuche untersuchen zu können. Gleichzeitig bietet dies eine gewisse Art Spamschutz, da der Marktalgorithmus Hashes nur einmal akzeptiert und damit böswillige Knoten an der mehrmaligen Teilnahme hindert.

In einer zweiten Phase werden dann die Verschlüsselungsschlüssel für die Gebote aus der ersten Phase versendet. Dadurch wird die Entschlüsselung aller Gebote und deren Marktausführung ermöglicht. Dieser Schritt eröffnet dann auch die abschließende dritte Phase, in der die berechneten Ergebnisse ausgetauscht werden.

Da jeder Teilnehmer alle Transaktionen auf dem Tangle mitlesen kann, werden alle Transaktionen innerhalb des Nachbarschaftsmarkts noch zusätzlich mit Hilfe von symmetrischer Verschlüsselung bei jedem Austausch von Nachrichten ent- und verschlüsselt.

Aufgaben eines Maintainer-Knotens

Der Maintainer-Knoten muss folgende Aufgaben erfüllen:

- Hinzufügen von neuen Knoten zu einer Nachbarschaft und das Anpassen der Nachbarschaftsstruktur. Beim Anpassen der Struktur werden die Nachbarn von Knoten zufällig zugelost, um den Einfluss von bösen Knotengewächsen zu verhindern.
- Veröffentlichen der Validierungslisten für den Nachbarschaftsmarkt.
- Sammeln und Validieren der Energieverbrauchsdaten jedes Haushalts.
- Abrechnungen erstellen.

Er unterstützt somit den Messstellenbetreiber und den Energieanbieter bei ihren Aufgaben.

a. Mieterstromabrechnung

Bei der Implementation der enerDAG Plattform wurde eine lokale Energiehandels-plattform erschaffen. Diese erlaubte es in ihrer ersten Version, einen Stromhandel innerhalb eines Apartmenthauses abzurechnen (z. B.: ein Vermieter mit PV + x Mieter). Dies passiert direkt und vor der Ausführung des Nachbarschaftshandels.

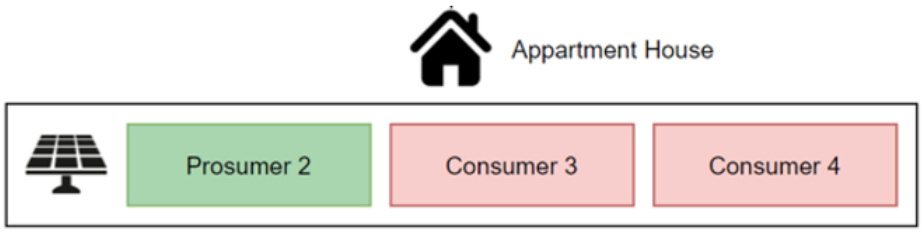


Abbildung 13: Mieterstromabrechnung

b. Lokaler Multiversorger

Zusätzlich kann in der lokalen Nachbarschaft der Strom größtenteils unabhängig von einer zentralen Stelle (z. B. Energiehändler) gehandelt werden. Dieser wird hauptsächlich zur Validierung der Handelsmengen bei der Abrechnung und der lokalen Teilnehmerregistrierung benötigt. Das wiederum passiert innerhalb des oben beschriebenen Nachbarschafts-Smart Contracts.

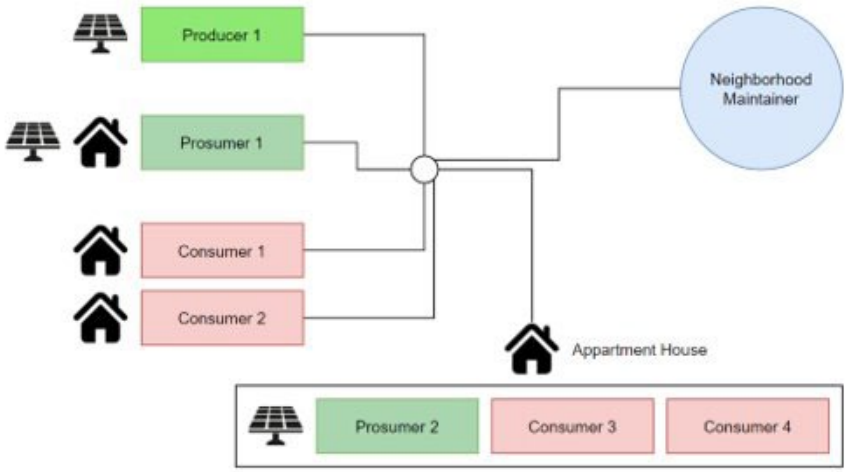


Abbildung 14: Lokaler Multiversorger

3.4. Threatmodellierung Energienetze (THU)

(OT (Operation Technologie)/Energietechnische Wirkungsweise)

Mit dem Einsatz von intelligenten steuerbaren Energiesystemen oder auch Energiemanagementsystemen nimmt auch die Bedeutung von informations- und kommunikationstechnischer (IKT) Sicherheit kontinuierlich zu. Insbesondere, da dezentrale Energiesysteme häufig in private Heimnetz-Infrastrukturen eingebunden sind, deren Umfeld nur über mangelhafte Sicherheitsmechanismen verfügt, wird der zuverlässige Netzbetrieb vor neue Herausforderungen gestellt. Photovoltaik-Systeme (PV), bestehend aus PV-Modul und Wechselrichter, stellen hierbei einen erheblichen Anteil an steuerbaren Systemen im Verteilnetz dar und haben dementsprechend einen signifikanten Einfluss auf die elektrischen Lastflüsse im Netz.

Intelligente Messsysteme (Smart Meter und Smart Meter Gateway) oder andere TLS*-gestützte Verbindungen stellen zwar einen sicheren Kommunikationskanal zu den verteilten Systemen bereit, doch das Umfeld der privaten, IKT-basierten Netzwerke bildet weiterhin eine Schwachstelle für sowohl unbeabsichtigte Fehlhandlungen als auch gezielte missbräuchliche Nutzung. Dies lässt sich durch Anwendung der IT-Sicherheitsnorm IEC 62443 (siehe Abbildung 15) veranschaulichen, indem man die relevanten Teilnehmer des Kommunikationsstranges betrachtet und den entstehenden Verantwortungs-bereichen bzw. Sicherheitszonen zuweist. Zu den relevanten Teilnehmern der Smart-Meter-Infrastruktur zählen beispielsweise der Messstellenbetreiber nach Messstellenbetriebsgesetz (MsbG), der Verteilnetzbetreiber gemäß Energiewirtschaftsgesetz sowie der Prosumer, der das PV-System betreibt. Teilnehmer, wie der Messstellenbetreiber und Netzbetreiber, erfüllen bereits relativ hohe Sicherheitsanforderungen, da sie ein übergeordnetes Interesse am zuverlässigen Netzbetrieb besitzen. An den exemplarischen, erreichten Sicherheitsniveaus (engl.: Achieved Security Level – SL) ist zu erkennen, welches Maß an Sicherheit in den jeweiligen Zonen umgesetzt wurde. Da das Prosumer-Umfeld der Privatsphäre unterliegt, können in diesem Bereich keine Sicherheiten gewährleistet werden, wodurch sich hier ein erreichtes Sicherheitsniveau von 0 ergibt. Aus dieser Analyse folgt, dass die Prosumer-Umgebung im Verbundsystem der dezentralen Energieversorgung grundsätzlich als Schwachstelle gilt.

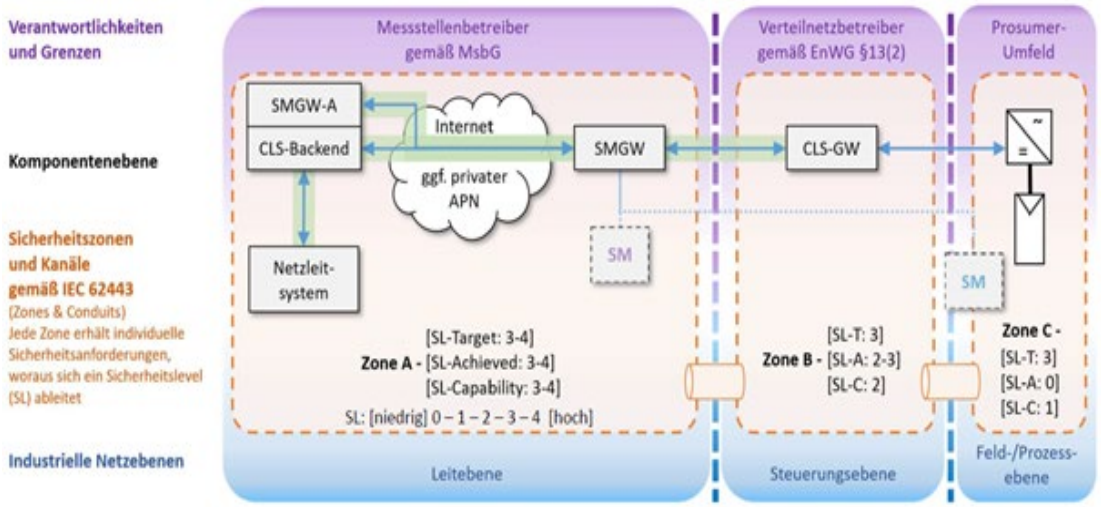


Abbildung 15: Kommunikationsmodell und Anwendung der IT-Sicherheitsnorm IEC 62443

Abbildung 15: Smart-Meter-Infrastruktur-basiertes Kommunikationsmodell mit schematischen Verantwortlichkeiten und der exemplarischen Anwendung der IT-Sicherheitsnorm IEC 62443. Zu erkennen sind den jeweiligen Verantwortlichkeiten zugewiesene Sicherheitszonen mit individuellen Sicherheitsniveaus (engl.: Security Level), wobei das Prosumer-Umfeld keine Sicherheit gewährleisten kann. Die industriellen Netzebenen verdeutlichen die Ähnlichkeit des zusammenhängenden Verbundsystems von dezentralisierter Energieversorgung mit einem automatisierten Prozessnetz, das in hierarchische Ebenen gegliedert ist.

Somit können mögliche Ereignisse mit negativem Einfluss auf den Netzbetrieb durch den Prosumer selbst sowie durch externe Angriffe aus dem Internet und den im privaten Heimnetzwerk angebundenen Energiesystemen erfolgen. Dabei werden Aktivitäten eines Prosumers an der eigenen Anlage geringere Auswirkungen auf das elektrische Netz haben, da der Netzbetreiber die ordnungsgemäße Betriebsführung nicht von einzelnen privaten Energiesystemen abhängig macht. Allerdings erhalten bestimmte Aktivitäten völlig neue Schadenspotentiale, wenn sie als ferngesteuerte Angriffe auf mehrere verteilte Systeme orchestriert werden. Gemeinsam mit den mangelhaften Sicherheitsmechanismen in Heimnetzwerken mit Internetzugang und angebundenen Energiesystemen gewinnen diese potentiellen Angriffe zusätzlich an Relevanz. Auch der fehlende Authentifizierungsmechanismus in verschiedenen Protokollen, wie etwa bei ModbusTCP*, wie es bei PV-Wechselrichtern angewendet wird, gilt in diesem Zusammenhang als Schwachstelle, die für kriminelle Aktivitäten ausgenutzt werden kann.

Als Beispiele für Bedrohungsszenarien, die von Energiesystemen ausgehen können, die in privaten Heimnetzen mit Internetzugang eingebunden sind, gelten auf der einen Seite die Manipulation von digitalisierten Messdaten, die gefälscht an übergeordnete Instanzen, wie Netzleitsysteme, weitergeleitet werden können. Auf der anderen Seite besteht die Möglichkeit mittels eines gefälschten ModbusTCP-Clients die eingespeiste Leistung von PV-Wechselrichtern zu manipulieren und diese

schlagartig abzuregeln. Beide dieser Szenarien können unter Umständen dazu führen, dass das sensible Gleichgewicht zwischen Erzeugung und Verbrauch aktiv und massiv gestört wird.

In Bezug auf eine koordinierte Ansteuerung und Manipulation mehrerer verteilter Energiesysteme konnte von anhand einer Simulationsumgebung eine vergleichbare Situation nachgestellt werden. Dabei wurde simulativ demonstriert, dass durch das gleichzeitige Einschalten mehrerer verteilter Lasten mit einem bestimmten Leistungsbedarf eine Frequenzabweichung provoziert werden kann, die unter Umständen einen Stromausfall verursachen kann. Die Effektivität bzw. die Auswirkung eines solchen Angriffs hängt von der Leistung der elektrischen Lasten und der Trägheit des Netzes ab in Form von Rotationsträgheit der Kraftwerks-Generatoren, die den Leistungsbedarf kompensieren könnten. Allerdings ist zu berücksichtigen, dass solche großen Veränderungen im Leistungsbedarf zuallererst Auswirkungen auf die Auslastung der Netzbetriebsmittel, wie Leitungen und Transformatoren, haben.

Dieses Verhaltensprinzip des elektrischen Netzes lässt sich auf das Angriffsszenario der Einspeiseleistungsmanipulation mittels gefälschtem ModbusTCP-Client übertragen, mit dem Unterschied, dass es sich nicht um elektrische Lasten, sondern um Erzeuger handelt. Würde eine bestimmte Anzahl PV-Wechselrichter an einem Tag mit idealen Bedingungen (beispielsweise einem sogenannten Clear Sky Day) gleichzeitig abgeschaltet bzw. abgeregelt werden, so entstünde schlagartig ein Leistungsdefizit. Abhängig von der gesamten PV-Leistung könnte dies unter Umständen zu einer signifikanten Frequenzabweichung und einem Stromausfall führen. Nicht zu vernachlässigen ist außerdem der abrupte Spannungsabfall. Die Fläche des Stromausfalls würde hierbei maßgeblich von der Reaktion der Netzbetreiber abhängen, die mit entsprechenden Regelungsmaßnahmen, wie etwa Lastabwurf, entgegenwirken müssten.

Beim Angriffsszenario der Messdatenmanipulation werden bewusst falsche Messdaten eingespeist, auch bekannt als False Data Injection (FDI). Dies kann sich auf den Betrieb von Verteilnetzen oder auch virtuellen Kraftwerken auswirken, da falsche Anlagen-Messdaten zu kontraproduktiven Reaktionen der jeweiligen Betreiber führen können. Dabei sind ähnliche Auswirkungen auf das elektrische Netz, wie im ersten Szenario beschrieben, nicht ausgeschlossen.

4. Validierung

4.1 Code White/Pentest (EKUT)

Im Rahmen des AP 3.2 wurde unter Federführung des WBZU ein Konzeptreview von enerDAG unter Berücksichtigung sicherheitsrelevanter Aspekte durch Code White durchgeführt. Zusätzlich wurden verschiedene Angriffsszenarien erarbeitet. Dabei wurden neun Bedrohungskategorien gefunden, welche verschiedene Schutzziele von enerDAG verletzten und potentiell eine Bedrohung für seine Benutzer darstellen könnten. Durch striktere Definitionen in den angewandten Prozessen können jedoch viele Angriffe präventiv verhindert werden. Die frühzeitige Identifizierung von Betrugsindikatoren und die detaillierte Protokollierung wurden ebenfalls als elementare notwendige Bestandteile herausgestellt. Zusätzlich wurde die Entwicklung von Notfallplänen für vereinfachtes und schnelles Störungsmanagement für verschiedene Angriffsszenarien angeraten.

Während des Penetration Tests wurden mögliche Angriffspunkte und Bedrohungen für enerDAG gesucht. Diese sind in der folgenden Grafik (aus Code White Konzeptreview) dargestellt:

Bedrohung	Szenario	Kritikalität	Eintrittswahrscheinlichkeit
Datenmanipulation	Fälschung Quantität	Sehr Hoch	Sehr Hoch
	Natürliche Zyklen	Medium	Sehr Hoch
	Großzügiger Spender	Sehr Hoch	Hoch
Majority Voting	100 % Überzeugung	Sehr Hoch	Niedrig
	Flooding	Hoch	Nicht Möglich
	Bottleneck	Sehr Hoch	Niedrig
Nachrichtenübermittlung	Manipulation of Votes	Sehr Hoch	Hoch
	Impersonierung	Hoch	Hoch
Synchronisation	Erschöpfen der Ressourcen	Medium	Medium
Anmeldung	Störung der Kommunikation	Medium	Hoch
	Störung des Votings	Medium	Niedrig
	Überlastung des Maintainers	Niedrig	Nicht Möglich
Anonymität und Identität	Energieprofile	Sehr Niedrig	Niedrig
	Identifikation	Niedrig	Nicht Möglich
Transaktionen	Flooding von Geboten	Niedrig	Nicht Möglich
	Flooding von Transaktionen	Niedrig	Niedrig
Kryptografie	Fehlkonfiguration	Sehr Hoch	Nicht Identifiziert

Abbildung 16: Angriffspunkte und Bedrohungen für enerDAG

Die größte Bedrohung stellt dabei die Datenmanipulation dar. Es werden zwar verifizierte Daten zum Energieverbrauch an den Messstellenbetreiber übermittelt, diese Zeitperioden stimmen allerdings nicht zwingend mit den verschiedenen Handelsoptionen überein, und andere Knoten haben auf diese Daten ebenfalls

keinen Zugriff zur Verifikation. Daher ist es beispielsweise für einen Angreifer möglich, falsche Handelsmengen anzugeben. Dies ist allerdings durch den MSB* leicht erkennbar und muss daher zwar beachtet werden, stellt aber kein unlösbares Problem dar. Weniger leicht zu erkennen ist es, wenn die Gesamtsumme innerhalb einer normalen Smart Meter Datenübertragungsperiode (15 Minuten) gleich bleibt und sich nur die Handelsmengen innerhalb der drei 5-Minutenperioden unterscheiden. Dies wäre insbesondere bei kurzzeitigen Produktionsschwankungen und damit rapide schwankenden Preisen eine mögliche Angriffs- und Gewinnsteigerungsoption. Allerdings wird dieser Prozess bereits durch die notwendigen Entgelte erschwert. Das Problem des „großzügigen Spenders" ist dadurch gelöst, dass der MSB immer die Tokens den einzelnen Teilnehmern zuordnen kann und es dadurch nicht zu komplett anonymen, nicht in Realität vorhandenen, Teilnehmern kommen kann, welche zu überteuerten Preisen einkaufen, aber nicht zuordenbar sind.

Beim „Majority Voting" kann es bei sehr ungeschickten Verteilungen bereits reichen, weniger als 22 % (3 von 14) Knoten zu überzeugen, für ein für einen Angreifer vorteilhaftes Ergebnis abzustimmen, anstatt das wahre Ergebnis zu propagieren.

Durch einen Fehler in der Nachrichtenüberprüfung war es zudem theoretisch möglich, sich fälschlicherweise als Nachbar und sogar als Maintainer auszugeben.

4.2 Konkrete Verbesserungsfelder

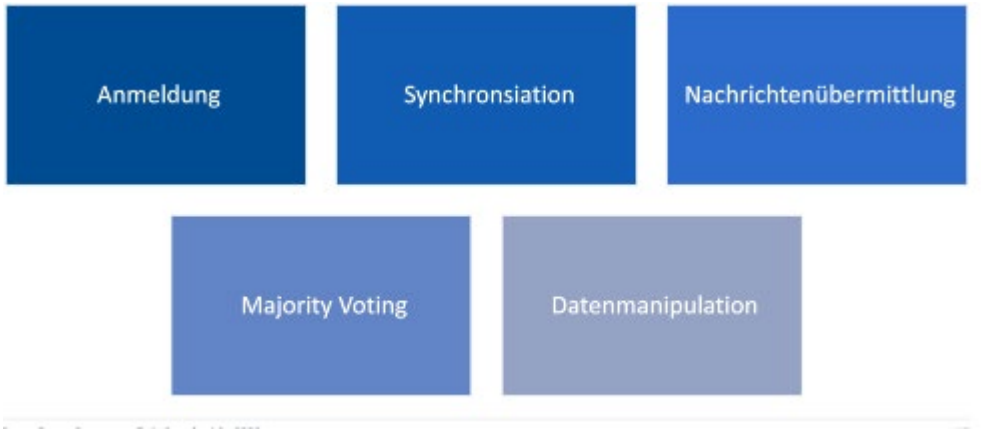


Abbildung 17: Verbesserungsfelder

Durch schnelles An- und Abmelden beim lokalen Messstellenbetreiber könnten geschickte Nachbarn gefunden werden, um das Majority Voting auszuhebeln. Daher sind Zeitsperren und Limits notwendig für das Neuregistrieren.

Durch das Delegieren der Validierung von älteren, unbekannten Transaktionen auf „Full Nodes“, wie z .B. den MSB, kann die Ressourcenbelastung verringert werden. Bei der Nachrichtenübermittelung wurde ein Bug* gefunden und anschließend behoben, bei dessen Überprüfung konnte eruiert werden, ob eine Nachricht vom Maintainer eine falsche Antwort geliefert hatte.

Durch eine Vergrößerung der einzelnen Gruppen von fünf auf sieben direkten Kommunikationsnachbarn kann die Angriffsschwierigkeit noch weiter erhöht werden.

Beim Thema der Datenmanipulation hat sich gezeigt, weshalb der Messstellenbetreiber die übermittelten Messdaten im Nachhinein für den Handel überprüfen und für die Abrechnung validieren muss.

5. Umsetzung

5.1. Tangle/enerDAG Plattform

Für die enerDAG Plattform wurde eine Webseite zur besseren Übersicht und für das Einstellen des eigenen Verkaufspreises und weiterer Eingaben entwickelt. Diese stellt auch die verschiedenen Bausteine der enerDAG Plattform sehr gut vor.

Ersparnisse:

Abbildung 18: enerDAG Plattform Webseite/Übersichtsseite

Die Webseite ist so aufgebaut, dass man zuallererst eine Übersichtsseite über die verschiedenen Ersparnisse, welche erzielt wurden, erhält. Sie zeigt an, wie viel Gewinn durch das direkte Verkaufen und Kaufen von Energie erzielt werden konnte im Vergleich zu den Standardpreisen direkt beim Energieversorger. Aktuell werden dort die täglichen, monatlichen und jährlichen Werte angezeigt.

Energiebilanz:

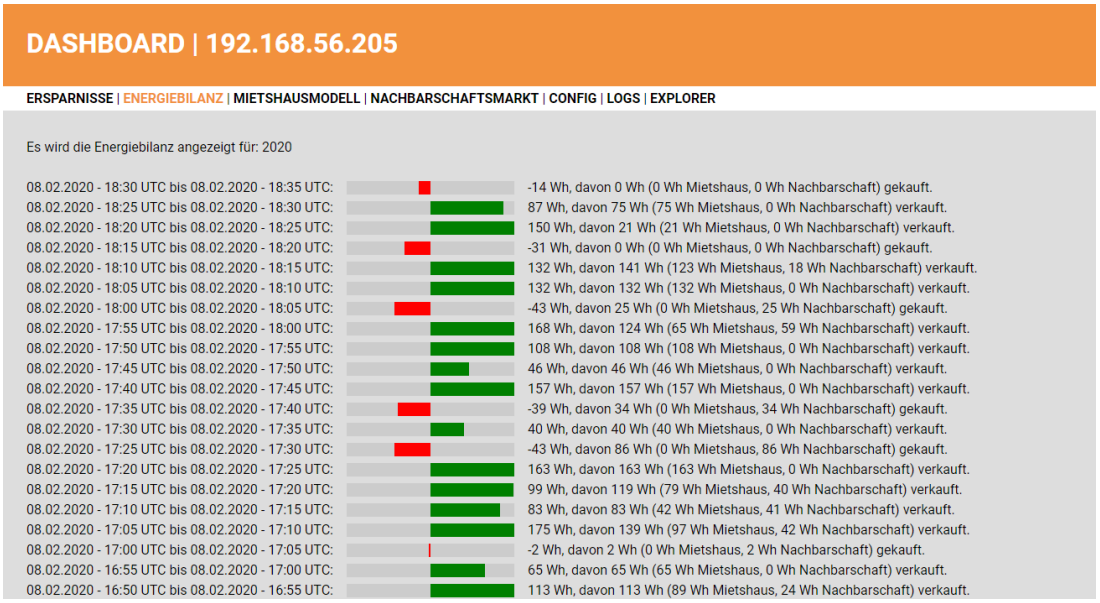


Abbildung 19: Beispielbild einer Energiebilanzseite mit zufälligen Werten

Die Energiebilanzseite zeigt die unterschiedlichen Bilanzen für die unterschiedlichen Zeiträume an. Am wichtigsten auf dieser Seite ist, dass man direkt sehen kann, ob es

möglich war, Strom sowohl im Appartmenthausmodell als auch in der Nachbarschaft zu kaufen/verkaufen. Falls die Handelsrunde noch nicht vollständig ausgeführt wurde, wird diese als noch nicht final angezeigt. Diese Seite liefert eine schöne Übersicht über die Energiebilanz eines Haushalts und dessen Zyklen über die Zeit hinweg.

a. Mietshaus/Appartmenthausmodell:

Abbildung 20: Miethausmodellseite

Das Miethausmodell gibt eine Übersicht über den Energiehandel innerhalb eines Miethauses, in welchem innerhalb des *Apartment House Smart Contracts,* z. B. auf dem Dach per PV erzeugte Energie, direkt an Mieter in einem Haus verkauft werden kann. Dies erfolgt über Direktvermarktung. Aktuell bestünden für dieses Modell rechtliche Schwierigkeiten, da auch hier die gleichen zusätzlichen Abgaben und Maßnahmen notwendig sind, als würde der Strom erst außerhalb des Hauses verkauft werden.

Auf dieser Seite sieht man jedoch für jede Handelsausführung den Zeitraum, die Energiebilanzen der einzelnen Teilnehmer, die fixen Preise, die Handelsabschlüsse und die Hashes des vorhergehenden Zeitraums als auch des Smart Contract Ergebnisses.

Die Anonymität der einzelnen Teilnehmer kann innerhalb einer so kleinen Teilnehmermenge nicht gewährleistet werden, da die wenigen, bekannten Teilnehmer systemseitig automatisch mit ihren Energiebilanzen zusammengeführt werden können.

b. Lokale Nachbarschaft

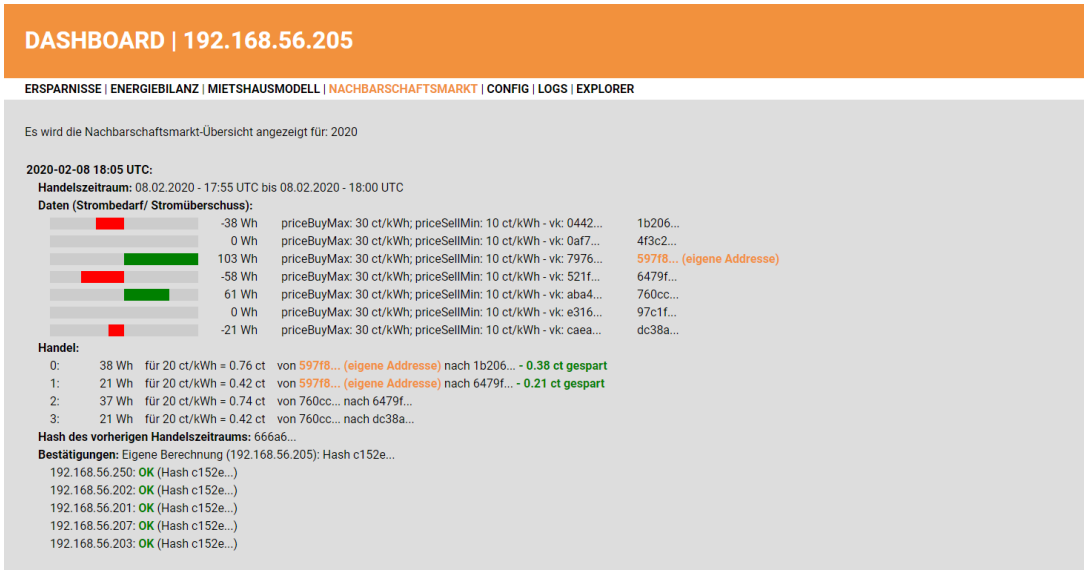


Abbildung 21: Nachbarschaftsmarktseite

Die Nachbarschaftsmarktseite gibt eine Übersicht über Handelsabschlüsse im eigenen Nachbarschaftsmarkt. Auch hier ist wiederum der Zeitpunkt der Marktausführung, die gemeldeten Energiebilanzen und Kauf-bzw. Verkaufspreise, die einzelnen Handelsabschlüsse mit ihren jeweiligen Preisen und Beträgen sowie den eigenen Einsparungen im Vergleich zu den Energiekosten beim Kauf/Verkauf direkt vom/an den Energieversorger zu sehen. Wie man hier sehen kann, kann es im Gegensatz zum Apartmenthausmodell mehr als einen Produzenten geben. Der anklickbare Hash des vorherigen Ergebnisses führt den Nutzer zur Tangle Explorer-Transaktion*, und es sind ebenfalls die Ergebnisse der Mehrheitsabstimmung des Vertrags und die Meinungen der Nachbarknoten sichtbar. Wenn ein grünes „OK" angezeigt wird, gibt es die gleiche Meinung wie beim eigenen Knoten zum Ergebnis des Handelszeitraums. Falls ein rotes “NICHT OK" angezeigt wird, liegt ein Konflikt auf Grund verschiedener Ansichten zum Ergebnis des Vertrags vor.

Konfigurationsseite

Auf der Konfigurationsseite werden für den Benutzer verschiedene Informationen über den eigenen Knoten zusammengefasst. Zusätzlich werden Informationen über die aktuellen Nachbarn, welche zufällig vom Maintainer zugewiesen wurden, ausgegeben. Oben auf dieser Seite ist es möglich, den maximalen Ein- und Verkaufspreis für den zukünftigen Energiehandel einzustellen.

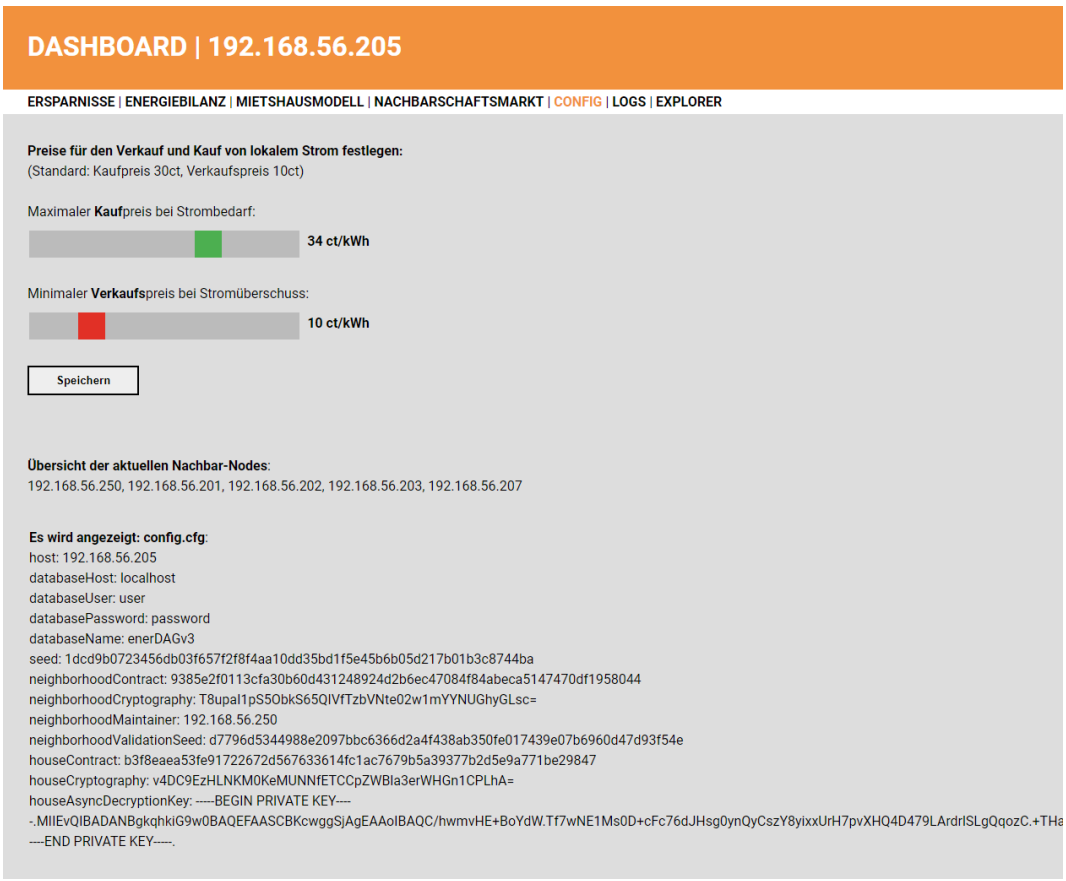


Abbildung 22: Configseite

Simulationen und Vergleich von verschiedenen Blockchain Technologien

In einer vorliegenden Abschlussarbeit (M.Stroh) mit dem Thema „Evaluierung der Effizienz verschiedener Blockchain-Ansätze für den effizienten lokalen Energiehandel“ wurden verschiedene Blockchaintechnologien auf ihre Lauffähigkeit bzw. Effizienz bzgl. eingebetteter Systeme verglichen. Der Knoten musste dabei jeweils ein vereinfachtes Minimalbeispiel des Nachbarschaftsmodells als Smart Contract lokal auf einem Raspberry Pi 3b+ über 16 Minuten (3 Handelszeiträume) hinweg ausführen. Anzumerken ist hierbei, dass Elrond* und Ethereum* es nicht geschafft hatten, ihre Berechnung rechtzeitig (innerhalb der jeweiligen Handelszeiträume) auszuführen und damit keine validen Resultate für diesen spezifischen Anwendungsfall lieferten. Ebenfalls ist in Abbildung 23 zu sehen, dass diese erste Version des Tangles sich akzeptabel geschlagen hat. Allerdings wurden auch Bereiche für Optimierung offensichtlich, welche im enerDAG des SEP-Projekts verbessert wurden. Dafür liegen aber noch keine neuen Simulationsergebnisse auf der Grundlage dieses Blockchain-Vergleichs vor.

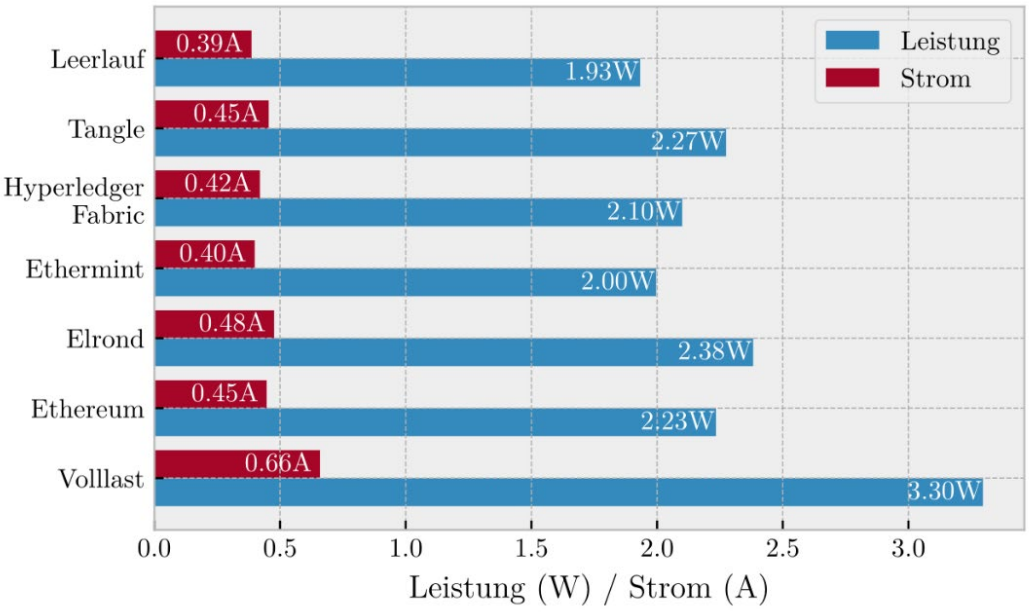


Abbildung 23: Ergebnis der Simulation aller Ansätze durch eine vereinfachte Darstellung nach Verbrauch (M. Stroh)

5.2. Anwendung E-Mobilität (THU)

Ziel der Anbindung einer E-Ladeinfrastruktur im Rahmen der Implementierung des Handelssystems „enerDAG“ ist es, einen Prototyp mit realer dezentraler Energieressource (DER), statt nur eines simuliertem DER zu verbinden und auch eine Beispiel-Nachbarschaft des lokalen Energiehandels zu präsentieren.

Als Architektur der Implementierung wurden die Systeme aus zwei Docker-Containern* als solch eine DER erzeugt und innerhalb der CLS Steuerbox/Gateway ausgeführt (vgl. auch FNN erweiterte Steuerbox).

Wie in Abbildung 24 dargestellt, wurde ein sogenannter „Tangle Node Container” eingefügt, der den bereitgestellten überschüssigen Strom/Energiebedarf über die lokale Energiehandelsschnittstelle auf der enerDAG Plattform vermarktet. Der andere „Go-Echarger Interface Container” sammelt fortlaufend Daten (überschüssigen Strom/Energiebedarf) von der Ladesäule über die Softwareschnittstelle der Go-Echarger Ladesäule. Diese Informationen werden zyklisch vom „Tangle Node Container“ abgefragt und auf der enerDAG Plattform vermarktet.

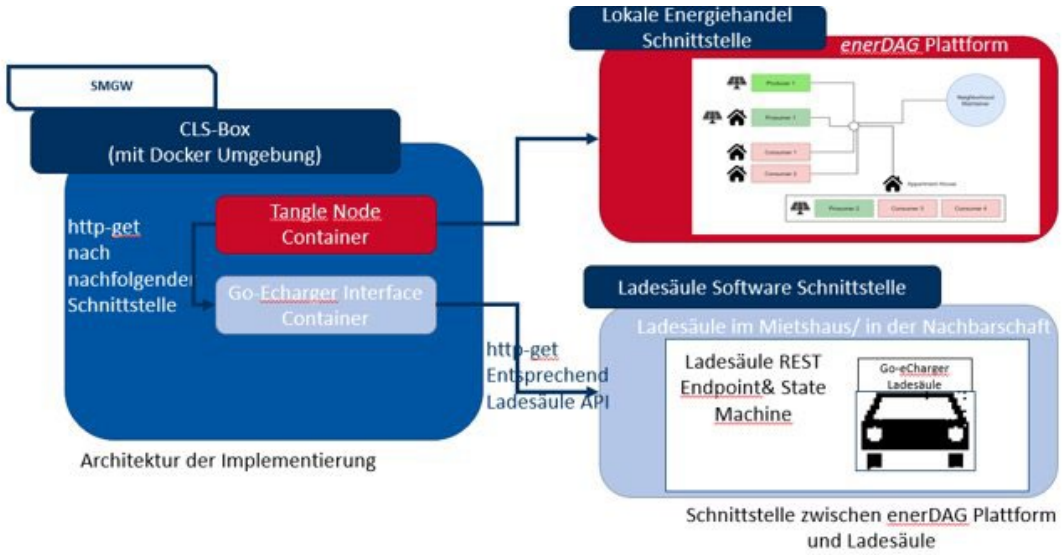


Abbildung 24: Anbindung E-Ladeinfrastruktur

Als dezentrale Energieressource haben wir in diesem Anwendungsfall ein AC-Ladegerät, den sogenannten „Go-eCharger“ für Elektromobilität verwendet. Der Go-eCharger hat eine REST-API* und stellt aggregierte Daten sowie Status-Daten an einem eigenen REST-Endpunkt bereit.

5.3. Anwendung PV (THU)

Ziel dieser Anbindung an das PV-System im Rahmen der Implementierung des Handelssystems „enerDAG“ ist die Anwendung der E-Mobilität mit einer realen dezentraler Energieressource (DER) statt nur einem simuliertem DER zu verbinden und diese Kombination auch in einer Beispiel-Nachbarschaft eines lokalen Energiehandels zu präsentieren. Über die Modbus-Schnittstelle des PV-System werden aggregierte Daten sowie Status-Informationen bereitgestellt.

Als Architektur der Implementierung wurden die Systeme aus zwei Docker-Containern (Go-Echarger, PV-System) innerhalb der CLS Box ausgeführt.

Wie in Abbildung 25 dargestellt, sieht man den Tangle Node Container, der den bereitgestellten überschüssigen Strom des PV-Systems über eine lokale Energiehandelsschnittstelle auf der enerDAG Plattform steuert.

Zudem kommt hier ein anderer „Go-Echarger Interface Container“ zum Einsatz, der fortlaufend Daten (überschüssigen Strom) des PV-Systems über dessen Software-Schnittstelle von der Ladesäule sammelt und zeitgleich mit dem „Tangle Node Container“ in bestimmten Zeitintervallen kommuniziert. Bei diesem Tangle Node Container handelt es sich um das enerDAG System.

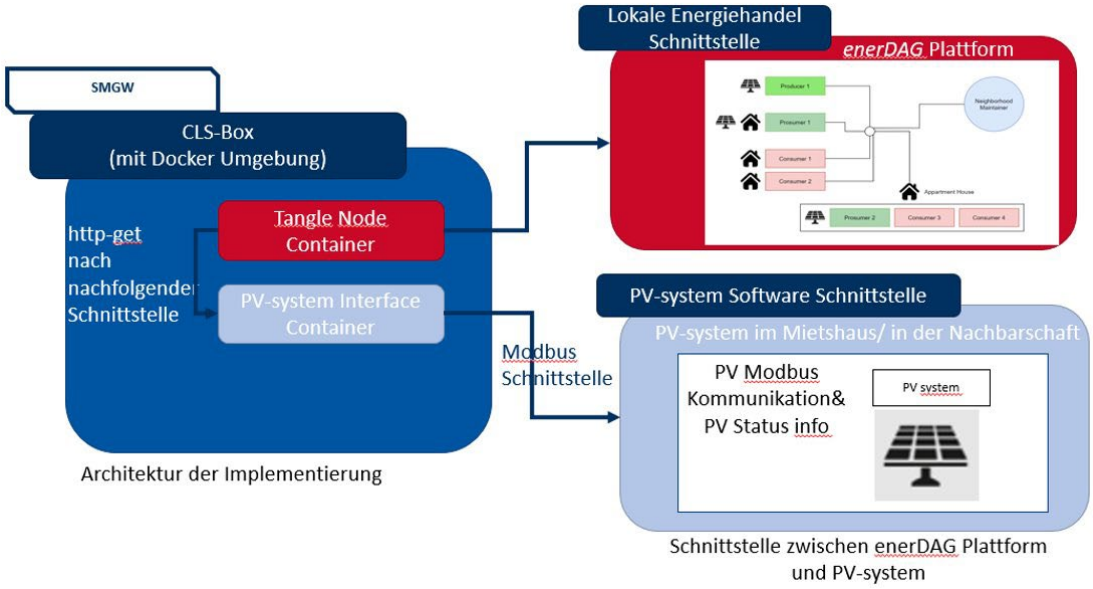


Abbildung 25: Anbindung PV

6. Test und Demonstration

6.1. Smart Grid Labor (THU)

Zuerst konzentrierten sich die Labortests der Smart Grids Forschungsgruppe an der Technische Hochschule Ulm (THU) auf den Aufbau der technischen Infrastruktur der Laborumgebung. In einem ersten Schritt wurde die Stromversorgung und die Bereitstellung des isolierten Internetzugangs für die Netzwerkinfrastruktur für die lokale Vernetzung der Komponenten (PV und E-Ladesäule) aufgebaut. Danach wurde die Smart Meter Infrastruktur(SMI)-Komponenten (mME*, SMGW, Steuerboxen und CLS-Modulen) installiert.

Nach dem Aufbau der Basisinfrastruktur erfolgte die Installation der Anwendungen, u. a. des Monitorings und der TeleControl PV-Anlage sowie der Abrechnungsprozesse der Elektrofahrzeuge und der Tangle-Technologie für den Handel zwischen Prosumern, welche im Laboraufbau umgesetzt und getestet werden konnten.

Laborumgebung

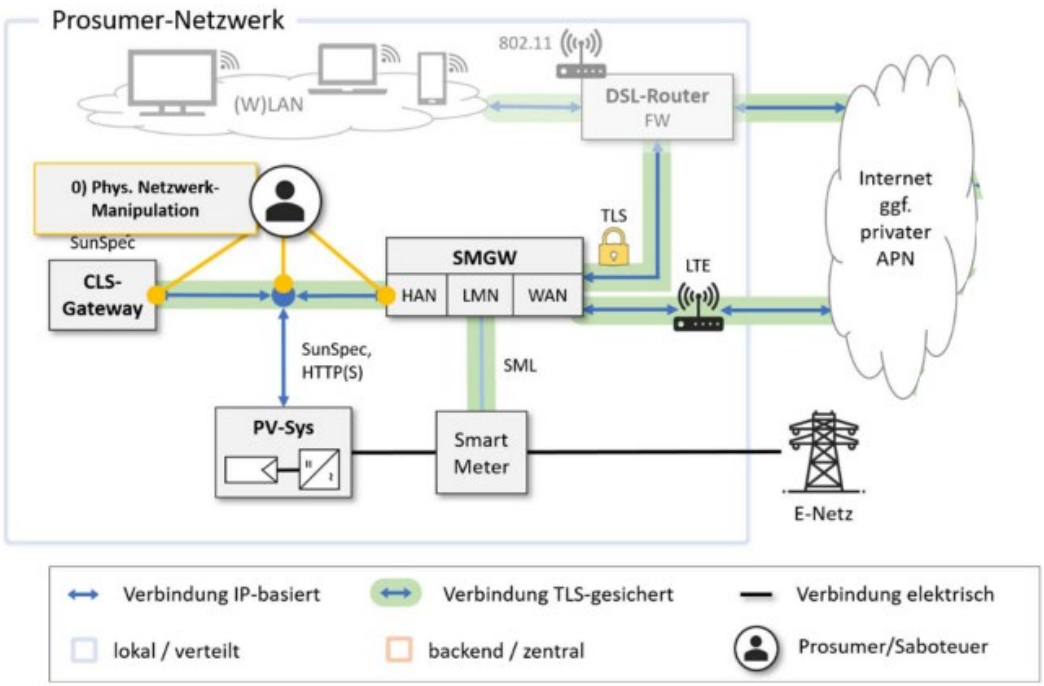


Abbildung 26: Laborumgebung

Bidirektionale Kommunikation zwischen den Komponenten in dieser Gemeinschaft

Um einen automatischen Handel innerhalb einer Nachbarschaft zu ermöglichen, erfordert es eine bidirektionale Kommunikation zwischen den Komponenten in dieser Gemeinschaft. Das wurde möglich, indem die Smart-Meter-Infrastruktur (SMI) für Demo-Prosumer in einer Wohngemeinschaft mit E-Ladesäule und PV-Anlagen im Labor implementiert wurde. Dazu gehörten u. a. der Stromzähler und das Kommunikationsgerät, genannt Smart Meter Gateway (SMGW). Das SMGW ist eine Kombination aus Datensammler für die Stromzählerstände und einem Kommunikationsmodem bzw. Router mit einem hochentwickelten Backend-System zur Gewährleistung der Cybersicherheit. Diese Gerätekombination ist in Abbildung 26 dargestellt.

Echtzeit-Messung von Bezug und Einspeisung

Eine Echtzeit-Messung von Bezug und Einspeisung sowie Bereitstellung von Messwerten mit 5-Minuten-Taktung und Abrechnung von Nachbar-Strom in einer theoretischen Wohngemeinschaft sowie eines lokalen Multiversorgermarkt konnte mit Hilfe der aufgebauten Smart-Meter-Infrastruktur demonstriert werden.

PV-Überschuss Direktvermarktung/Umverteilung

Sowohl der Nachbarschafts-Smart Contract als auch Tangle mit einer Reihe von Prosumern, die mit PV-Anlage ausgestattet sind, konnte in der Testumgebung implementiert und umgesetzt werden.

Abrechnung der E-Ladung

Für die Abrechnung der E-Ladung konnten wir erfolgreich einen Ladestromzähler aufsetzen und für den Projektablauf zum Einsatz bringen.

6.2. EKUT Tübingen (EKUT)

An der EKUT wurde die Ladesäule dann in die Testumgebung integriert und an enerDAG testweise angebunden. Leider gab es in einem Partnerprojekt Probleme mit der Anschaffung des eAutos für den Simulationsraum. Dadurch konnten nur Trockentests durchgeführt werden.

Abbildung 27: EKUT: Teil des trilateralen Reallabortests: enerDAG Energiehandelsplattform

Die restliche Umgebung wurde wie oben erwähnt mit simulierten Energiehandelswerten nachempfunden.

6.3 WBZU Labor (WBZU, THU)

Die Vorgabe für den Schulungsaufbau der Thematik CLS/SMGW/Integration in Liegenschaften zu Wohnzwecken war, eine für den Handwerker vor Ort vorzufindende Situation nachzubilden. Mit der Ausrichtung des WBZU als Teil der Handwerkskammer ist hier insbesondere das Thema Trennung der Aufgaben zwischen einerseits Aufgaben des Messstellenbetreibers und des Handwerksbetriebes andererseits zu betrachten. Dies umfasst die Themen Schnittstellen, Grundverständnis des neuen Smart Meter Messsystems sowie Integration in die bestehende Infrastruktur. Auch die Überführung von Liegenschaften hin zu einem Heimenergiemanagementsystem, das fähig ist, an lokalen Marktplätzen zu handeln ist ein Ziel des Schulungsaufbaus.

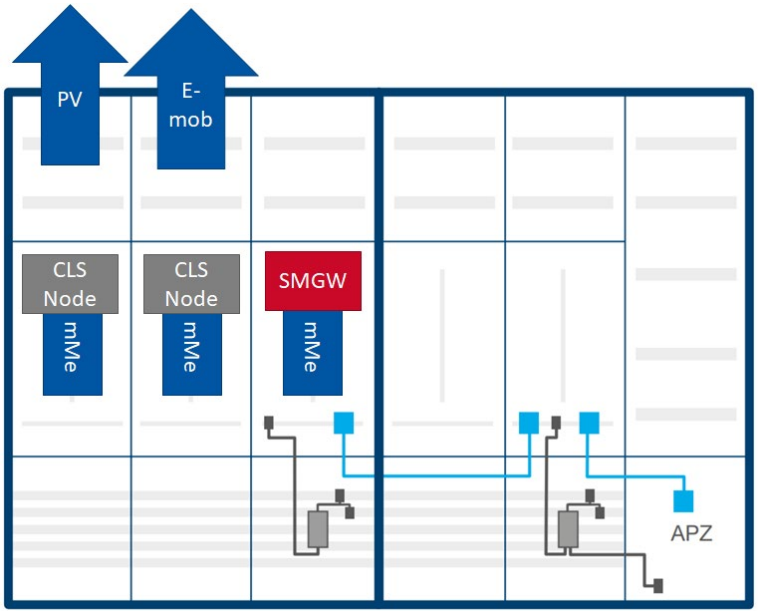


Abbildung 28: Umsetzung der Laborumgebung am WBZU zu Schulungszwecken

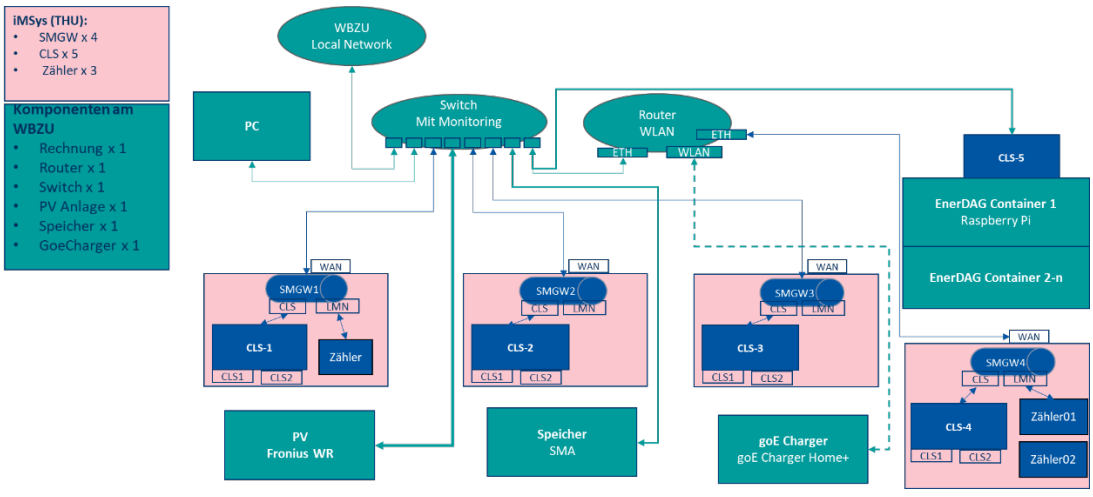


Abbildung 29: IT-technischer Verbindungsplan für den ganzen Testaufbau

Die nachfolgenden Bilder und Schema erläutern die einzelnen Knoten des Schulungsaufbaus. Durch das Symbol auf den Zähler (rechts unten um die Ecke) kann das Pairing-Status mit dem SMGW „erfolgreich gepaart“ erkannt werden. Die Messwerterfassung erfolgt in 15 Minuten Takt nach dem konfigurierten TAF7 Profil.

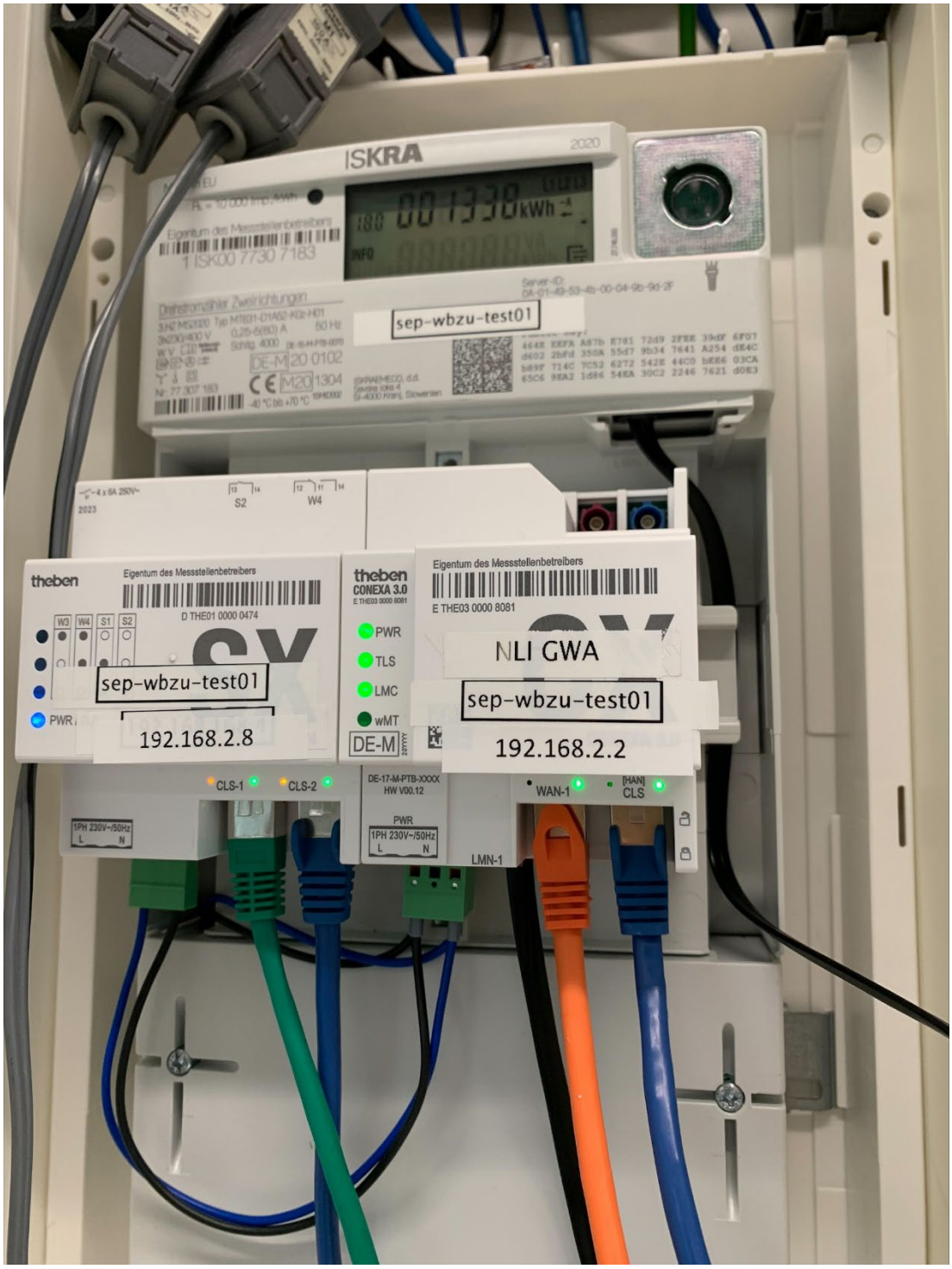


Abbildung 30: Aufbau vom Testsystem 01 mit vorkonfigurierten SMGW, Zähler und CLS-Gateway zur Integration von PV-Anlagen in das Heimenergiemanagementsystem und zur Anbindung an lokale Marktplätze.

Abbildung 31: Aufbau vom Testsystem 02 mit vorkonfigurierten SMGW und CLS-Gateway zur Integration von lokaler Lade-Infrastruktur in das Heimenergiemanagementsystem und zur Anbindung an lokale Marktplätze.

Abbildung 32: Aufbau vom Testsystem 03 mit vorkonfigurierten SMGW und CLS-Gateway zur Integration vom Batteriespeichern in das Heimenergiemanagementsystem und zur Anbindung an lokale Marktplätze. Der Zähler im Bild bietet nur Stromversorgung für die anderen zwei Geräte, der Zähler an sich gehört dem System 04.

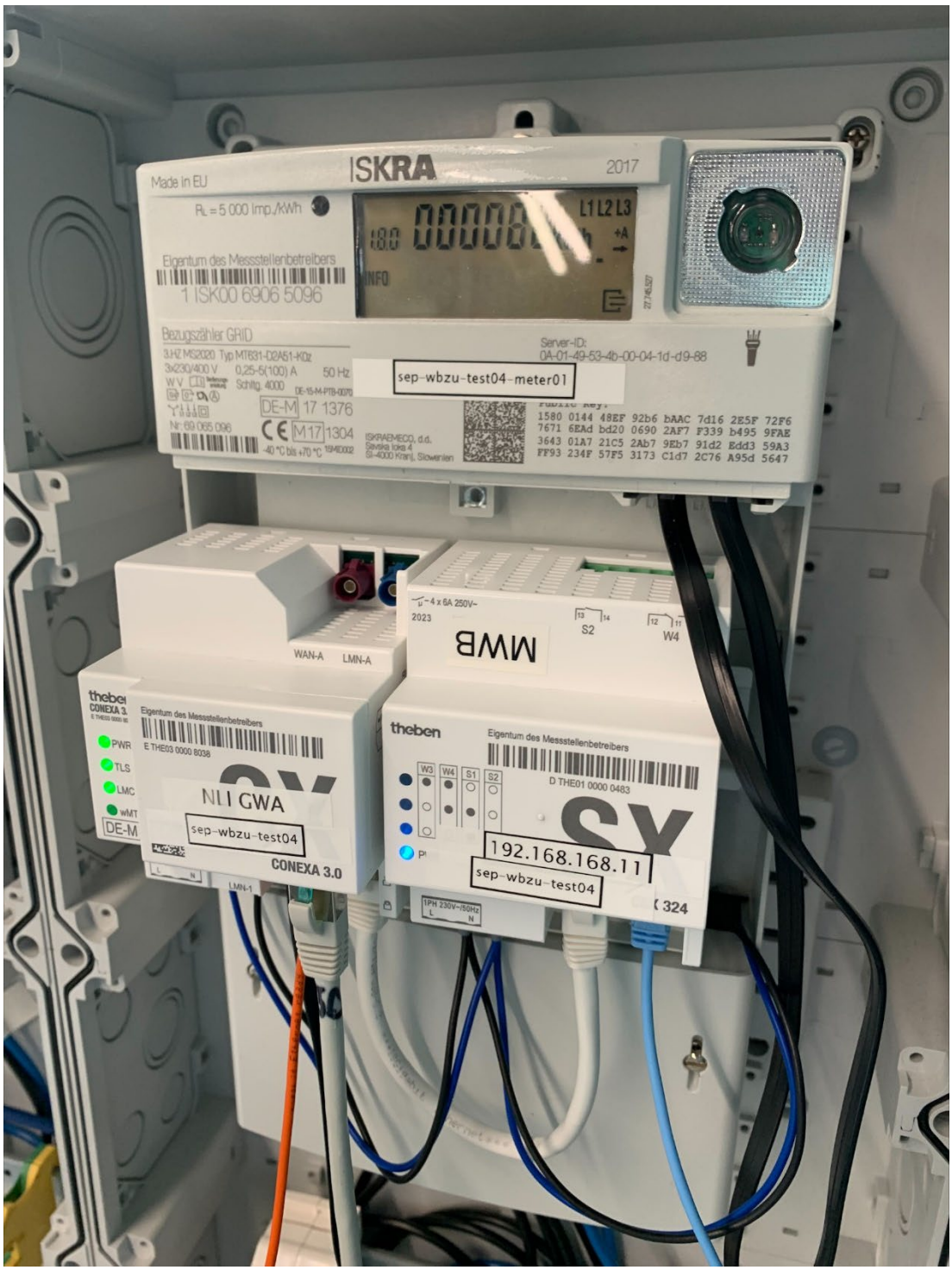
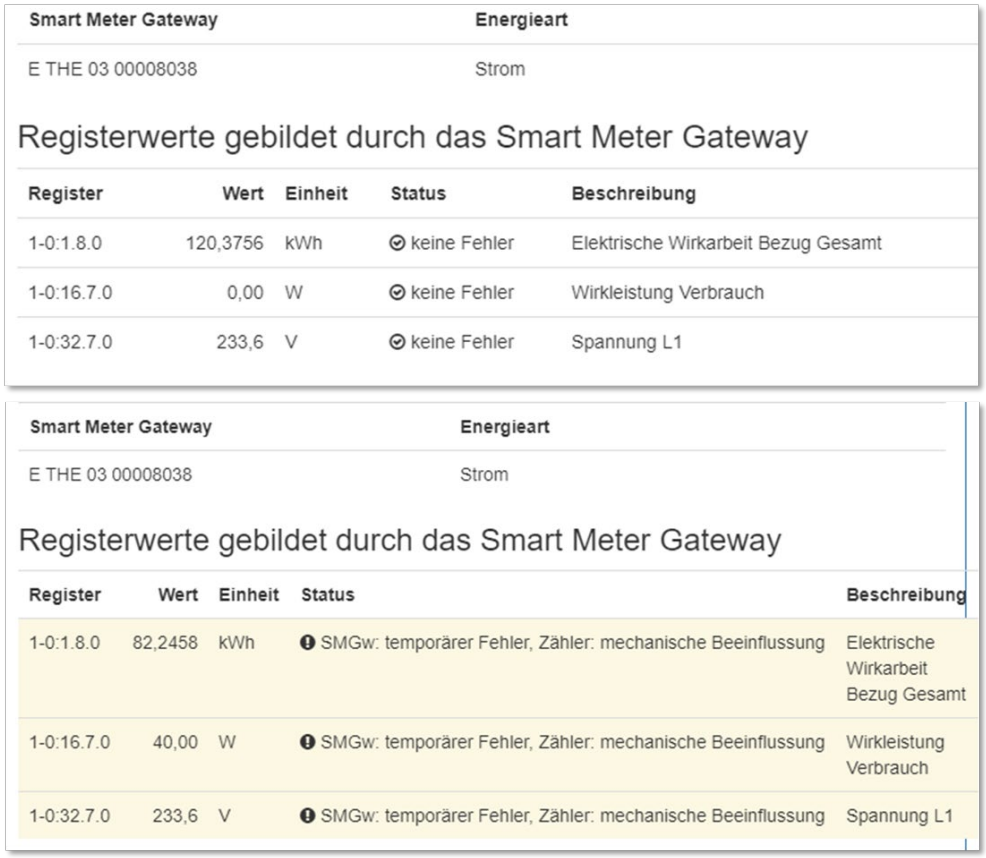


Abbildung 33: Aufbau vom Testsystem 04 mit vorkonfigurierten SMGW, Zählern und CLS-Gateway zum direkten Abruf von Messwerten über die TRUDI Schnittstelle des SMGWs sowie zur Darstellung des Parametrierung-Prozesses für das iMsys und das CLS-Gateway.



Smart Meter Gateway	Energieart
E THE 03 00008038	Strom

Registerwerte gebildet durch das Smart Meter Gateway

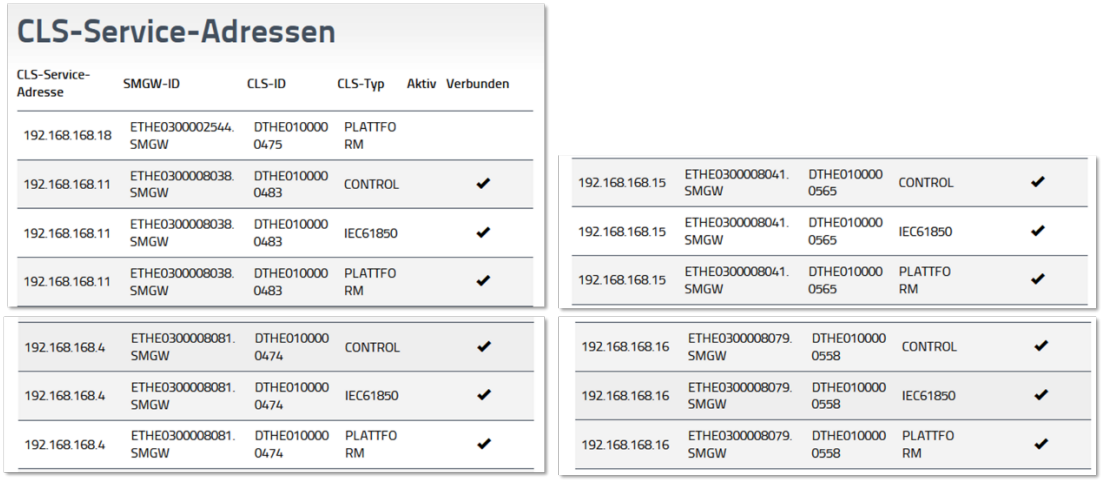
Register	Wert	Einheit	Status	Beschreibung
1-0:1.8.0	120,3756	kWh	keine Fehler	Elektrische Wirkarbeit Bezug Gesamt
1-0:16.7.0	0,00	W	keine Fehler	Wirkleistung Verbrauch
1-0:32.7.0	233,6	V	keine Fehler	Spannung L1

Smart Meter Gateway	Energieart
E THE 03 00008038	Strom

Registerwerte gebildet durch das Smart Meter Gateway

Register	Wert	Einheit	Status	Beschreibung
1-0:1.8.0	82,2458	kWh	SMGw: temporärer Fehler, Zähler: mechanische Beeinflussung	Elektrische Wirkarbeit Bezug Gesamt
1-0:16.7.0	40,00	W	SMGw: temporärer Fehler, Zähler: mechanische Beeinflussung	Wirkleistung Verbrauch
1-0:32.7.0	233,6	V	SMGw: temporärer Fehler, Zähler: mechanische Beeinflussung	Spannung L1

Abbildung 34: Durch die Messwertabfrage über TRUDI-Schnittstelle lässt sich der Status von den konfigurierten Messlokationen und TAF-Profilen überprüfen.



CLS-Service-Adressen

CLS-Service-Adresse	SMGW-ID	CLS-ID	CLS-Typ	Aktiv	Verbunden
192.168.168.18	ETHE0300002544.SMGW	DTHE010000 0475	PLATTFORM		
192.168.168.11	ETHE0300008038.SMGW	DTHE010000 0483	CONTROL	✔	
192.168.168.11	ETHE0300008038.SMGW	DTHE010000 0483	IEC61850	✔	
192.168.168.11	ETHE0300008038.SMGW	DTHE010000 0483	PLATTFORM	✔	
192.168.168.4	ETHE0300008081.SMGW	DTHE010000 0474	CONTROL	✔	
192.168.168.4	ETHE0300008081.SMGW	DTHE010000 0474	IEC61850	✔	
192.168.168.4	ETHE0300008081.SMGW	DTHE010000 0474	PLATTFORM	✔	
192.168.168.15	ETHE0300008041.SMGW	DTHE010000 0565	CONTROL	✔	
192.168.168.15	ETHE0300008041.SMGW	DTHE010000 0565	IEC61850	✔	
192.168.168.15	ETHE0300008041.SMGW	DTHE010000 0565	PLATTFORM	✔	
192.168.168.16	ETHE0300008079.SMGW	DTHE010000 0558	CONTROL	✔	
192.168.168.16	ETHE0300008079.SMGW	DTHE010000 0558	IEC61850	✔	
192.168.168.16	ETHE0300008079.SMGW	DTHE010000 0558	PLATTFORM	✔	

Abbildung 35: Der Übersicht-Dashboard vom CLS-Backend zeigt die Verbindungsstatus der konfigurierten CLS-Kanäle über SMGW. Es ist leicht zu erkennen, dass alle CLS-Verbindungen zu dieser Zeit aktiv sind.

Abbildung 36: Übersicht von den konfigurierten Smart-Meter-Systemen und dem go-E Charger

6.4 Schulungsangebot für Energiewirtschaft und Handwerk am WBZU

Den Vorgaben an die Umsetzung eines solchen Schulungsangebotes konnte Rechnung getragen werden. Somit kann die Verwertung der Projektergebnisse und auch der Demonstrationsaufbauten als erfolgreich angesehen werden durch die Entwicklung und die Durchführung von Schulungen am WBZU.

In einer solchen Schulung können nun folgende Themen behandelt werden:

Teil 1 Einführung:

Überblick, Grundlagen des Gesetzes zur Digitalisierung der Energiewende, Konzeption, Komponenten

Teil 2 Grundlagen IKT:

Informationsübertragung, Datenmodell, OSI*-Schichtenmodell, IP-Adressen, IT-Sicherheit, https, TLS, Public-Key-Infrastruktur

Teil 3 Technik 1: Smart Meter Infrastruktur und dezentrale Energiesysteme

Überblick über die Komponenten, moderne Messeinrichtung (digitale Zähler), SMGW, iMSys, CLS, Konfiguration, Profile, Zertifikate, Anbindung PV-WR*, Speicher, Wallbox, Heimnetzwerk

Teil 4 Technik 2: Smart Meter Infrastruktur und -Betrieb

Gateway Administration, CLS-Management, gEMT*, aEMT*, IT-Grundschutz, TRUDI*-Schnittstelle, Techniker-Tool

Teil 5 Anwendungen:

Messkonzepte, CLS-Anwendungen, TAF*, IT-Sicherheit

Teil 6 Ausblick:

BSI Roadmap, Digitaler Netzanschluss, Heimenergie-Management, Smart Home

Teil 7 Demonstration und Übungen zu folgenden Themen:

Zählertausch,-einbau SMGW und CLS-Gateway mit SILKE*

Inbetriebnahme und Überprüfung SMGW

Anschluss Energiesystem durch Elektrofachkraft

Visualisierung für Kunden

Anwendung Techniker-Tool

8. Veröffentlichungen

[1] C. Groß, M. Schwed, S. Mueller und O. Bringmann, „enerDAG – Towards a DLT-based Local Energy Trading Platform", *2020 International Conference on Omni-layer Intelligent Systems (COINS)*, Barcelona, Spain, 2020, pp. 1-8, doi: 10.1109/COINS49042.2020.9191415.

[2] Y. Mahmoodi, C. Groß, S. Reiter, A. Viehl, und O. Bringmann, „Security Requirement Modeling for a Secure Energy Trading Platform“, in CYBER 2020 : The Fifth International Conference on Cyber-Technologies and Cyber-Systems, Nice, France, Okt. 2020, S. 6.

[3] „Considerations on communicating with decentralized prosumer applications through Home Area Network and Wide Area Network”, in CIRED 2021 – September 2021. DOI:10.1049/icp.2021.1539

9. Literaturverzeichnis

[1] A. Bogensperge, F. Sebastian, K. Simon und K. Andreas, „Eine praktische Anwendungshilfe für die Use Case Entwicklung," URL, 2020.

[2] L. Ableitnera, A. Meeuwb, S. Schopfera, V. Tiefenbecka, F. Wortmannb und e. al., „Quartierstrom – Implementation of a real worldprosumer centric local energy market in Walenstadt, Switzerland," *http://arxiv.org/abs/1905.07242,* 2019.

[3] A. Panarello, N. Tapas, G. M. F. Longo und A. Puliafit, „Blockchain and iot integration: A systematic survey," *https://doi.org/10.3390/s18082575,* 2018.

[4] Q. ZHU, S. W. LOKE, R. TRUJILLO-RASUA, F. JIANG und Y. XIANG, „Applications of Distributed Ledger Technologies to the Internet of Things: A Survey," *ACM Computing Surveys 52(6).https://doi.org/10.1145/3359982,* 2019.

[5] A. Brenzikofer, A. Meuw, S. Schopfer, A. Wrner und et.al, „QUARTIERSTROM: A DECENTRALIZED LOCAL P2P ENERGYMARKET PILOT ON A SELF-GOVERNED BLOCKCHAIN," *https://www.scs.ch/wp-content/uploads/2019/06/CIRED2019_Quartierstrom_full_20190520.pdf,* 2019.

[6] A. Wrner, A. Meeuw, L. Ableitner, F. Wortmann, S. Schopfer und V. Tiefenbeck, „Trading Solar Energy within the Neighborhood: FieldImplementation of a Blockchain-Based Electricity Marke," 2019.

[7] A. Brenzikofer und N. Melchior, „Privacy-Preserving P2P EnergyMarket on the Blockchain," *http://arxiv.org/abs/1905.07940,* 2019.

[8] N.Ismailova, „Co-simulation of a tangle based distributed ledger and an exemplary electricity distribution grid," *https://www.embedded.uni-tuebingen.de/teaching/thesis/2018/12/01/sep-tangle-cosimulation/,* 2017.

[9] C. G. Schlussbericht, „das Energiesystem der Zukunft im Solarbogen Süddeutschlands," 2020.

[10] B. Sörries, M. Stronzik, S. Tenbrock, C. Wernick und M. Wissner, „Die Ökonomische Relevanz Und Entwicklungsperspektiven von Blockchain: Analysen Für Den Telekommunikations- Und Energiemarkt"," https://www.wik.org/uploads/media/WIK_Diskussionsbeitrag_Nr_445.pdf, URL, 2019.

[11] M. Stroh, „Evaluierung der Effizienz verschiedener Blockchain Ansätze für den effizienten lokalen Energiehande".

[12] „https://bitinfocharts.com/de/comparison/bitcoin-median_transaction_fee.html,".

[13] „https://cbeci.org".

[14] G. Heilscher, S. Chen, F. Ebe, S. Hess, T. Kaufmann, H. Lorenz und A. Schindlmeier, „CLS-App BW - 11 Anwendungen für die Steuerbox,“ in *Tagungsband: Zukünftige Netze für Erneuerbare Energien*, Berlin, 2018.