GLocalFlex

Innovation Action
HORIZON-CL5-2022-D3-01

D6.1

Technical standards and recommendations

WP6

TASK 6.1

NOVEMBER 1

glocalflex.eu

AUTHOR(S):

Tomasz Gorecki (CSEM), Diya Achi (CSEM), Arttu Tamminen (VTT), Dharmendra Sharma (VTT), Pirkko Kuusela (VTT), Pascal Chaussumier (EDF), Regine Belhomme (EDF)

This project has received funding from the European Union's Horizon-IA research and innovation programme under the Grant Agreement n°101096399.

Funded by the European Union

DISCLAIMER

The content of this deliverable reflects only the author's view. The European Commission is not responsible for any use that may be made of the information it contains.

This deliverable has not yet been reviewed by the European Commission and is therefore not in its final version.

COPYRIGHT NOTICE

DOCUMENT INFORMATION

Grant agreement	
Project title	A **G**lobal as well as **Local Flex**ibility marketplace to demonstrate grid balancing mechanisms through cross-sectoral interconnected and integrated energy ecosystems enabling automatic flexibility trading
Project acronym	GLOCALFLEX
Project coordinator	Klaus Känsälä - VTT
Project duration	1st January 2023 – 31st December 2026 (48 Months)
Related work package	WP 6 – Replication and verification
Related task(s)	Task 6.1 - Review of applicable standards and recommendations
Lead organisation	CSEM
Contributing partner (s)	CSEM, EDF, VTT
Due date	M6 – 6.2023
Submission date	27.6.2023
Dissemination level	Public

HISTORY

Date	Version	Submitted by	Reviewed by	Comments
26.06.2023	N°1.0	VTT	VTT, EDF, CSEM	First submission
01.11.2023	N°1.1	CSEM	VTT, CSEM	Small correction for publication on glocalflex website

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS

Acronym	Description
(H)EMS	(Home) energy management system
DR	Demand response
TSO	Transmission system operator
DSO	Distribution system operator
BRP	Balance-responsible party
XML	Extensible Markup Language
UML	Unified modelling language
OWL	Ontology web language
IEC	International electrotechnical commission
USEF	Universal smart energy framework
TLS	Transport layer security
FCR	Frequency containment reserve
aFFR	Automatic frequency restoration reserve
mFFR	Manual frequency restoration reserve
DA	Day-ahead
ID	Intra-day
DLT	Distributed Ledger Technology
DID	Decentralized Identity
SSI	Self-Sovereign Identity

DAG	Directed Acyclic Graph
VC	Verifiable Claim
VCI	Verifiable Credential Issuance
VP	Verifiable Presentation
HVAC	Heating, ventilation and air conditioning
ToU	Time of use

Executive Summary

The GLocalFlex project will demonstrate the provision of flexibility services to the electricity system across a range of markets, business use cases and deployment scenarios thanks to its implementation in 6 different pilot locations. Power grids operation, including more recently flexibility, is a heavily regulated area and many technical standards exist to cover aspects ranging from smart meter certification, communication technologies to be used for various grid and grid-connected components and equipment, interoperable modelling, and information models, etc.

This deliverable provides an overview of relevant standards that could be applicable in the pilots and platforms.

First, a high-level recap of existing flexibility markets and services is provided, and structured in 4 categories defined by USEF, depending on the party buying flexibility and the technical characteristics of the flexibility. The first is constraint management services, which optimize grid operation taking into account physical constraints and impact on markets. The second is adequacy services, which increase security of supply by organizing sufficient long-term peak and non-peak generation capacity. The third is wholesale energy services, which help BRPs decrease sourcing costs, mainly on Day-Ahead (DA) and Intraday (ID) energy markets. Finally, balancing services include all services specified by the TSO for frequency regulation.

Second, a description and comparison of standards is provided. It is organized in different topics, namely ontologies / data models; recommendations for flexibility verification practices; communication protocols and security practices.

Ontologies / Data models

We have identified 5 main relevant standards whose characteristics are summarized as follows (copy of Table 2)

Ontology / Data model	Authors	Scope	Modelling language	Recommended / associated communication protocol
CIM	IEC	Power grids, energy markets	UML	NA
IEC61850 data models	IEC	Distribution substations, DERs	UML/XML	GOOSE / MMS

SAREF4ENER	ETSI	Energy domain	OWL	NA (agnostic)
EEBus ontology	EEBus association	Home and industrial energy management	OWL	SPINE - Data model SHIP - Network TCP - Transport WebSockets- Application
OpenADR information model	OpenADR alliance	DR events and tariffs for	XML for messages	XMPP + HTTP - Application
Matter data model	Connectivity standards alliance	Home energy management	None	Thread

Verification

Verification refers to the process required to validate that flexibility has been delivered. The most relevant resource for this is the extensive analysis provided by USEF in their various working documents.

While details would depend on the type of service considered, some general concepts apply.

- Energy supply and flexibility are two separate things: typically, it should be so that the aggregator takes responsibility for flexibility activation and the supplier for energy supply. However, these roles (energy supplier and aggregator) can be shared by the same stakeholder. Three principles are applied to this separation: the aggregator's responsibilities are restricted to activation periods, activated assets, and deviations from baselines; the aggregator does not need to take responsibility for the active customer's energy supply; and the effects of flexibility activation for the supplier and BRP should be identifiable for compensation.
- Several key aspects are to be considered when defining rules for flexibility services:
    - Under what conditions sub-metering must / can be used for flexibility measurement
    - The rebound effect, whereby activation during a given time interval can cause modifications in consumption at other times prior to or after the activation.
    - The baseline methodology to be considered, i.e., in the event of a flexibility activation, against which level of consumption/production should the flexibility be compared
    - Possible interactions between explicit flexibility and implicit flexibility (e.g., in the presence of variable tariffs)

Communication

Communication englobes the connectivity solutions, protocols, regulations, and security measures in place to ensure the connection between actors, systems and devices to provide flexibility services. We focus here on communication with smart meters as it is particularly relevant to the topic of flexibility (but certainly not comprehensive)

Smart meters generally rely on a gateway for communication, which allows for lighter communication technologies, lower power consumption, and reduced costs. However, there is still an option for a direct connection between the smart meter and the cloud. Therefore, there are three possible connection segments:

- Smart meter to gateway
- Gateway to cloud,
- Smart meter to cloud.

It is important that these segments implement solutions that can penetrate walls and buildings. The communication solutions and protocols for these segments are summarized based on a review from emnify [34] and complemented with other selected solutions.

The communication technologies vary depending on the connection segment.

- Wired: Ethernet/Fibre-optic or Ethernet/DSL, Power Line Communication, M-Bus
- Wireless: Wireless M-Bus, LoRaWan, Zigbee, WiFi, Cellular, Sigfox

The communication stack is completed by other protocols. These protocols are numerous, some tailored for energy and smart grid applications, and some more general ones.

- General: ANSI C12.18, TCP/IP, UDP/IP, MQTT, AMQP, CoAP, WebSockets, XMPP, Modbus, MMS, GOOSE, Zigbee, HTTP
- Energy/smart grid specific: DLMS/COSEM, OSGP, OCPP, SHIP, Matter

We refer to the well-known OSI model in Section 4.4 to describe the coverage of these various protocols. Some of the most widespread protocols for energy and smart grid applications are Zigbee, DLMS/COSEM, OSGP, and Matter, which are further detailed in Section 5.

It is important to note that the choice of the specific protocol depends on multiple factors:

- The equipment and hardware implemented.
- The application or services targeted.
- The exact service architecture and the compatibility of the different elements.

Therefore, there is no single communication protocol that outperforms the others in all situations. However, some general recommendations are to be kept in mind when choosing the protocol. It

is useful to select a widespread protocol, which is compatible with most the hardware and services in place in order to promote interoperability and facilitate the operations, maintenance, and upgrades. For the same reasons, it is also useful to select protocols which are compatible, or built on other standard, non-application specific protocols.

Security

The EU Commission is gradually emphasizing the importance of cybersecurity in the energy sector. In fact, the NIS Directive 2 [1] published in 2022, identifies the energy sector as a critical infrastructure with cybersecurity requirements. The energy sector has three distinct features: the need for real-time responses, the potential for cascading effects, and the coordinated management of both new and old technologies [2].

The security requirements for the energy sector, even though not addressed specifically, follow the General Data Protection Regulation (GDPR), enforced in 2018. It highlights seven key data protection principles:

- **Lawfulness, fairness, and transparency** when processing data.
- Data processing must be **limited to legitimate purposes** known by the data subject.
- **Data** collection and processing must be **minimized** to the strict necessary.
- Personal data **accuracy** must be ensured.
- **Storage limitation** must be guaranteed.
- Data processing should ensure data security, **integrity, and confidentiality.**
- The data controller is **accountable** for GDPR compliance with the principles.

The implementation of specific policy, organisational, and technical measures, detailed in Section 4.5.4, ensure that the requirements are met.

The European Union Agency for Cyber Security (ENISA) and the NIS Cooperation Group Security Measures are two leaders in the field of cybersecurity. They mention 3 key standards in security:

- ISO/IEC 27000 establishes a framework for information security management systems (ISMS) and their requirements, on which an organization can be audited and certified.
- IEC 62443 ensures the security of Industrial Automation and Control Systems (IACS). It is implemented with a risk-based strategy where the most valuable assets and their vulnerabilities are identified to set up the most appropriate cybersecurity measures.
- NIST SP800-53 is a framework developed by the National Institute of Standards and Technology (NIST) in the United States for managing and securing information systems. It provides a catalogue of implementable security and privacy controls.

When developing a service, it is necessary to conduct a risk assessment for security and privacy, and then implement the appropriate cybersecurity measures and controls to mitigate the risks and remain in line with the GDPR. This is also applicable when choosing the communication protocols, which already incorporate some security measures, as seen in Section 4.5.5.

Blockchain – Distributed Ledger Technology (DLT)

The most revolutionizing aspect of the blockchain or DLT technology is the ability to create trust between parties without third-party authority through collective trust of recording information on transparent and permanent record. In regards of flexibility trading, DLTs possess multiple preferred features such as:

- Low-transaction costs
- Transparency with privacy
- Decentralized validation
- Security

EC has been looking into the possibility of utilising a DLT for the digitalisation of the energy system as part of "Fit for 55" package [3]. Some blockchain based flexibility marketplaces are already operational in EU.

One of the most critical aspects of the blockchain technologies is the verification mechanism or consensus mechanism. It is the method through which the system agrees on which transactions are valid and are added to the "chain" or the ledger. These methods are varying, and have usually specific purposes due to their possible constraints in one of three areas [4]:

1. Decentralization
2. Scalability
3. Security

A general view of the blockchain technology is provided as well as few most common consensus mechanisms "Proof of Work", "Proof of Stake" and "Directed Acyclic Graph (DAG)". Possibilities to utilise a DAG based IOTA for the flexibility platform will be looked into during this project in order to achieve private, secure, low-cost energy flexibility marketplace platform.

European Commission rolled out a regulation "eIDAS" in 2014 in order to have standards for electronic identification and trust services. The next step proposal "eIDAS 2.0" aims to extend the online identification to physical services [5] and to develop digital identity credentials (European Digital Identity – EUDI).

Chapter 6 contains also discussion on cases where blockchains are used directly in flexibility trading such as Energy Web Decentralised Operating System as well as brief pointers to recent blockchain related developments that are relevant for the GLocalFlex project.

Keywords

Flexibility, standards, communication protocols, data models, information models, ontologies, measurement & verification, smart grids, smart metering

1. Introduction

1.1. Scope of document

This document focuses on compiling relevant standards and recommendations applicable to the design, implementation, and deployment of flexibility services for electrical networks. We focus primarily on technical aspects.

The document is structured as follows:

- **Section 2** gives a brief overview of existing flexibility markets.
- **Section 3** provides an overview of the flexibility services architectures.
- **Section 4** provides a review of relevant standards and recommendations. It is dividing the discussion in the following subtopics: data model and ontologies; communication; security; measurement and verification.
- **Section 5** dives into specific available standards of particular relevance.
- **Section 6** covers the role of blockchain in the domain of flexibility.

1.2. Relation to the rest of the project

This deliverable is aimed to inform technical and business development in the rest of the project. On the technical side, it will serve as a working document for pilot site implementation (WP2/WP3) as it compiles possible options to follow for various aspects of implementation including communication protocol with devices / aggregators, process for flexibility verification and validation, and more. At the other end, it will also inform the development of the flexibility platform in WP4, as it will list relevant standards on security, data models, etc.

The business aspects of the project are primarily handled in WP5, however this document will start touching on some key organizational concepts around flexibility, as multiple topics concern both technical implementation and business organization of the services. This includes the following section 2 that briefly presents existing flexibility markets and standards, and recommendations for flexibility verification which is covered in section 4.3. It is expected that these topics will be further studied in subsequent activities of WP5 (T5.1, and T5.2) with a more specific focus on the various pilot sites of the project.

2. Flexibility markets

This section gives an overview of different types of markets where flexibility can be remunerated and outlines broad technical requirements. The exact rules for participation in those markets are

in most cases described in national or regional instantiations of those markets. We will **not** cover in detail the specific regulations of those national/regional markets, but rather point towards widely valid elements.

2.1. Overview

According to the USEF framework document [6], flexibility markets can be grouped in 4 broad categories :

- **Constraint management services** help the transmission and distribution grid operators (TSO and DSO) to optimize grid operation considering the physical constraints.
- **Adequacy services** aim to increase security of supply by organizing sufficient long-term peak and non-peak generation capacity. Adequacy services can be provided to either the TSO or the Balancing Responsible Parties (BRP), depending on market design.
- **Wholesale services** help BRPs to decrease sourcing costs (purchase of electricity) – mainly on Day-Ahead (DA) and Intraday (ID) energy markets.
- **Balancing services** include all services procured by the TSO for frequency regulation and balancing.

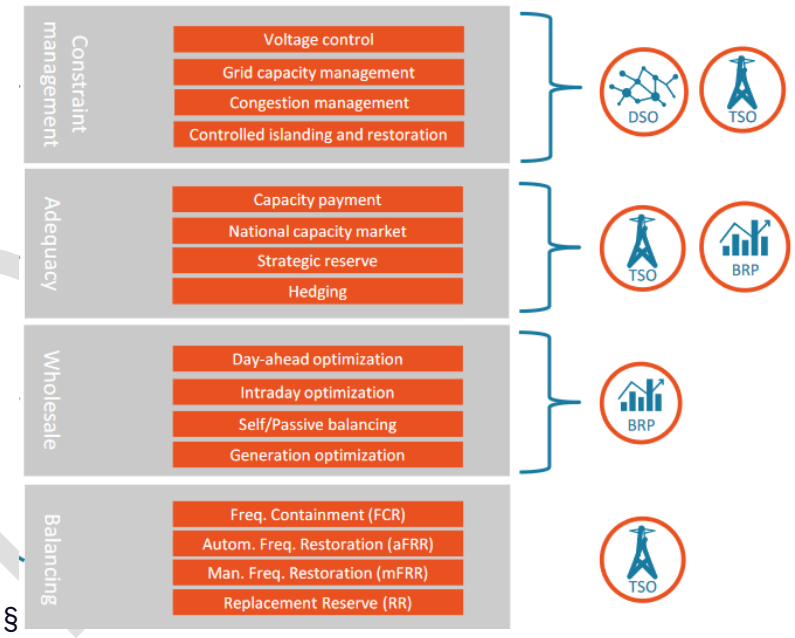

Figure 1. Taxonomy of flexibility markets. Source: USEF [6].

We give next some further details and relevant references on the most relevant categories when it comes to demand-side flexibility. In complement to this analysis, we also refer the following past analyses:

- [7] is a deliverable from the European project MAGNITUDE[1] which gives an overview of existing services towards the electricity system and a more detailed comparative analysis of frequency regulation and balancing markets, day-head and intraday energy markets, adequacy mechanisms as well as congestion management services for 7 countries: Austria, Denmark, France, Italy, Spain, Sweden, and the United Kingdom.
- [8] is a deliverable from the European project Coordinet[2] which gives an overview of balancing and imbalance markets with specific focus on Spain, Greece, Sweden, as well as some elements on aggregation rules.

2.2. Balancing markets

Thanks to recent regulations in Europe, there has been a trend towards harmonization of the balancing markets in European countries. Namely, the Electricity Balancing (EB) commission Regulation 2017/2195 governs the establishment of three different balancing platforms (for FCR, aFRR, mFRR) by requiring Transmission System Operators (TSOs) and a process platform for imbalance netting [9].

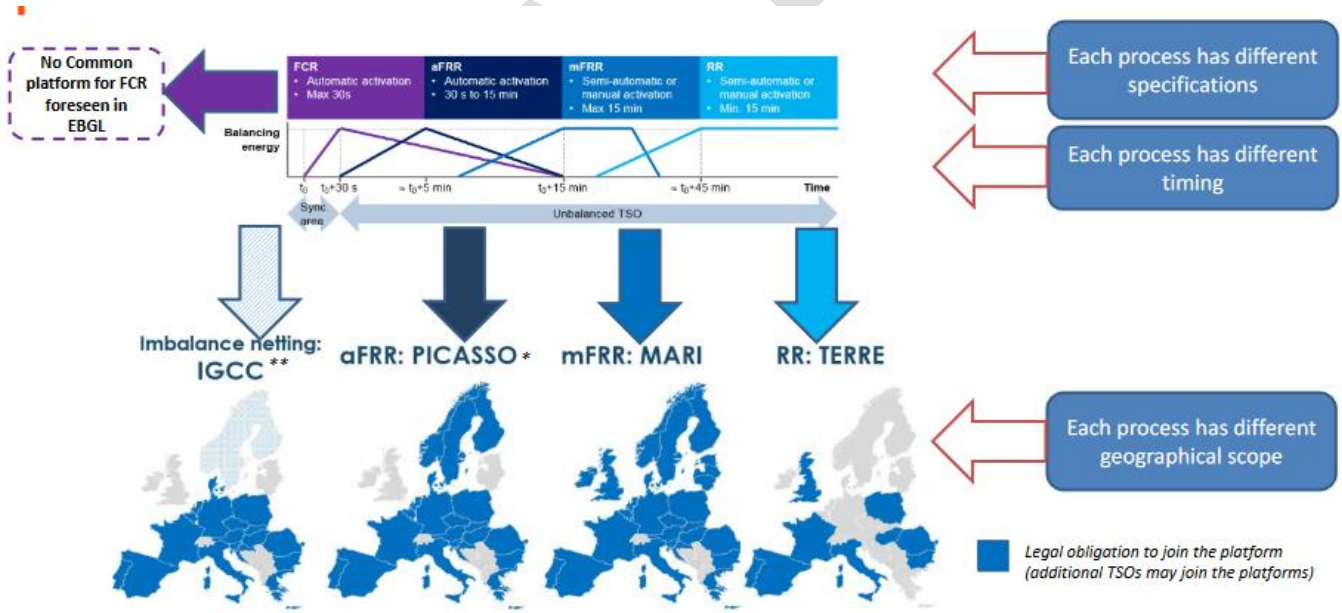

Figure 2. Summary of balancing platforms and projects. Source: ENTSO-E

[1] https://www.magnitude-project.eu/ , https://zenodo.org/communities/magnitude/
[2] https://coordinet-project.eu

2.2.1. Frequency containment reserve (FCR)

According to ENTSO [10], the characteristics of FCR are:

- *Symmetric product (meaning that upward and downward FCR are procured together).*
- *Duration of product delivery: usually 4 hours, subject to daylight saving time shift.*
- *TSOs allow divisible and indivisible bids. Indivisible bids can have a maximum bid size of 25 MW in all the participating countries.*
- *Minimum bid size is 1 MW and resolution is 1 MW as well.*
- *In accordance with SO GL (Annex VI "Limits and requirements for the exchange of FCR"): Core shares and maximum transfer capacities (export limits) exist as limitations in the FCR market.*
- *The full activation time is the fastest of the balancing services considered in this Section 2.2, typically around 30s. This activation time is not yet harmonized between all the different EU countries.*

The Austrian, Belgian, Dutch, Danish, French, German, Slovenian and Swiss TSOs currently procure their FCR in a common market.

2.2.2. Automatic Frequency Restoration Reserves (aFRR)

According to ENTSO-E [11]:

The Platform for the International Coordination of Automated Frequency Restoration and Stable System Operation (PICASSO) is the implementation project endorsed by all TSOs through the ENTSO-E Market Committee to establish the European platform for the exchange of balancing energy from frequency restoration reserves with automatic activation. This platform went live in June 2022. The generally accepted characteristics of aFRR are:

- **Capacity:** aFRR is procured with a capacity mechanism.
- **Automatic:** aFRR is activated automatically to ensure a quick response to frequency deviations.
- **Response Time:** The response time of aFRR should be within a few seconds. The full activation time is typically a few minutes.
- **Duration:** aFRR should be available for a specific duration, typically between 15 to 30 minutes, to provide sufficient time for other balancing services to be activated.

2.2.3. Manual Frequency Restoration Reserves (mFRR)

The Electricity Balancing Regulation outlines the tasks and timeline for implementing a European platform for exchanging balancing energy from frequency restoration reserves with manual

activation. This platform aims to create a cross-border balancing market that is economically efficient and financially neutral for TSOs. European TSOs established the MARI project, which is designated as the European implementation project for the mFRR platform. The project involves designing a technical solution that reflects the views of the founding parties and could be acceptable for potential new parties joining the initiative. The project has received the support of 28 TSOs with four additional TSOs as observers.

The MARI platform went live in October 2022.

The characteristics of mFRR are:

- **Capacity:** mFRR is procured with a capacity mechanism with accepted capacities generally lower than for aFRR
- **Manual:** mFRR is activated manually.
- **Response Time:** The response time of mFRR should be within a few minutes. The full activation time is typically 15 minutes.
- **Duration:** mFRR should be available for a specific duration, typically between 15 to 60 minutes.

2.2.4. Replacement reserves

According to the implementation guide for the new replacement reserve platform (TERRE), replacement reserves are used to restore/support the required level of FRR to be prepared for additional system imbalances. This category includes operating reserves with activation time from typically 15 minutes up to hours. Currently each TSO chooses the exact desired characteristics of its replacement reserves. For example, the French TSO RTE applies the following rules[3]:

Replacement Reserve (RR) can be activated in less than 30 minutes and up to 1.5 hours per activation. RTE may activate replacement reserve a maximum of 4 times in a one-day period and without exceeding 3 hours of cumulated duration per day.

The TERRE project was approved in 2016 to become the European platform for exchanging balancing energy from replacement reserves, and it is monitored by the National Regulatory Authorities and ACER. The Replacement Reserves Platform (RR Platform) enables the exchange and optimized activation of a standard product for balancing energy. The RR Platform is based on the LIBRA solution, a common IT system that supports the exchange of balancing energy. The TERRE project has been operational since January 2020 and is continuously working towards

[3] https://www.services-rte.com/en/learn-more-about-our-services/respond-to-the-manual-frequency.html

enabling stable operations and improving the optimization algorithm. The project also cooperates with MARI and Nordic LIBRA projects. Currently, the TERRE project consists of 8 TSOs, including operational and non-operational members and observers.

2.3. Flexibility services for wholesale energy markets

Flexibility services for wholesale energy markets can be considered explicit or implicit distributed flexibility services depending on the conditions. They aim at reducing BRPs sourcing costs of electricity and BRP imbalances. They typically involve suppliers (most common), generators, large consumers, or energy trading market parties [6]. The different processes involved on the wholesale energy markets are further detailed below.

2.3.1. Day-ahead optimization

Day-ahead optimization aims to shift electricity consumption from higher-priced intervals to lower-priced ones. This strategy involves trading electricity a day before its production while taking into account the entire following day [6].

Day-ahead trading takes place on the spot market (day-ahead market), where electricity can be bought or sold at the market clearing price determined by the power exchange, or through bilateral agreements [12] .

The day-ahead market is characterized by several features such as lead times, trading intervals, minimum quantities, auction pricing process, and gate closure. However, these characteristics vary from country to country [13].

2.3.2.Intraday optimization

Intraday optimization is similar to day-ahead optimization, but it takes place closer to delivery time and can be effected through continuous trading or through auctions. In continuous trading, the trading occurs at a more granular level, with intervals usually set at 15 minutes, 30 minutes, or 1 hour, and is executed immediately following a buy-sell order match [12]. In parallel to this continuous trading, in several EU countries, intraday optimization also takes place through one or several successive auctions. For example, EPEX spot runs continuous and auction-based trading[4].

Intraday optimization can be performed via the intraday exchange or through bilateral agreements. In Europe, the Single Intraday Coupling (SIDC) codes connect intraday markets, facilitating and promoting cross-border trading [12].

[4] See https://www.epexspot.com/en/market-data?market_area=&trading_date=2023-06-19&delivery_date=2023-06-20&underlying_year=&modality=Auction&sub_modality=Intraday&technology=&product=15&data_mode=map&period=&production_period= for different products

Intraday optimization enables BRPs to compensate for deviations from their day-ahead forecasts, thus limiting imbalance costs and improving system stability. Therefore, intraday trading provides another layer for balancing the market before the deployment of control reserve [14].

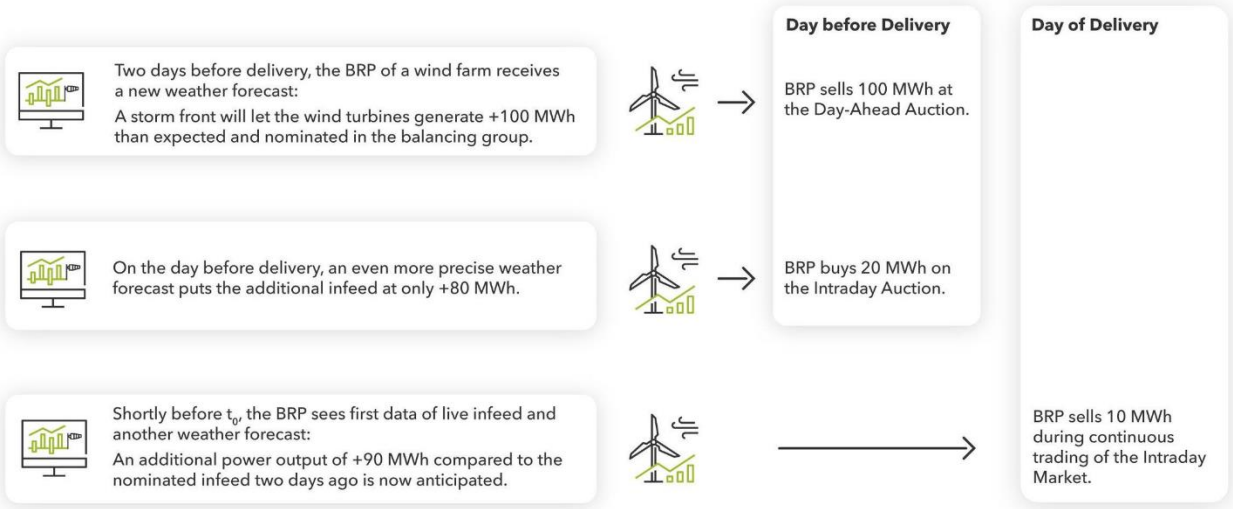

Figure 3. Day-ahead and intraday optimization example in Germany. © Next Kraftwerke [13].

2.3.3. Self-balancing and passive balancing

Self-balancing refers to the action taken by BRPs to reduce portfolio imbalance and avoid imbalance charges. Aggregators can provide flexibility that allows BRPs to optimize their portfolio positions, and the flexibility is traded through bilateral agreements [6].

Passive balancing is another process in which the TSO rewards BRPs for adjusting their portfolio positions to reduce system imbalance. For this process, the TSO provides real-time data that allows BRPs to anticipate imbalance prices and establish a real-time market price for electricity. However, it also poses certain risks related to the predictability of the total imbalance, and the final prices. The Aggregator, with a BRP role, can participate in this service by creating imbalance in their portfolios [6].

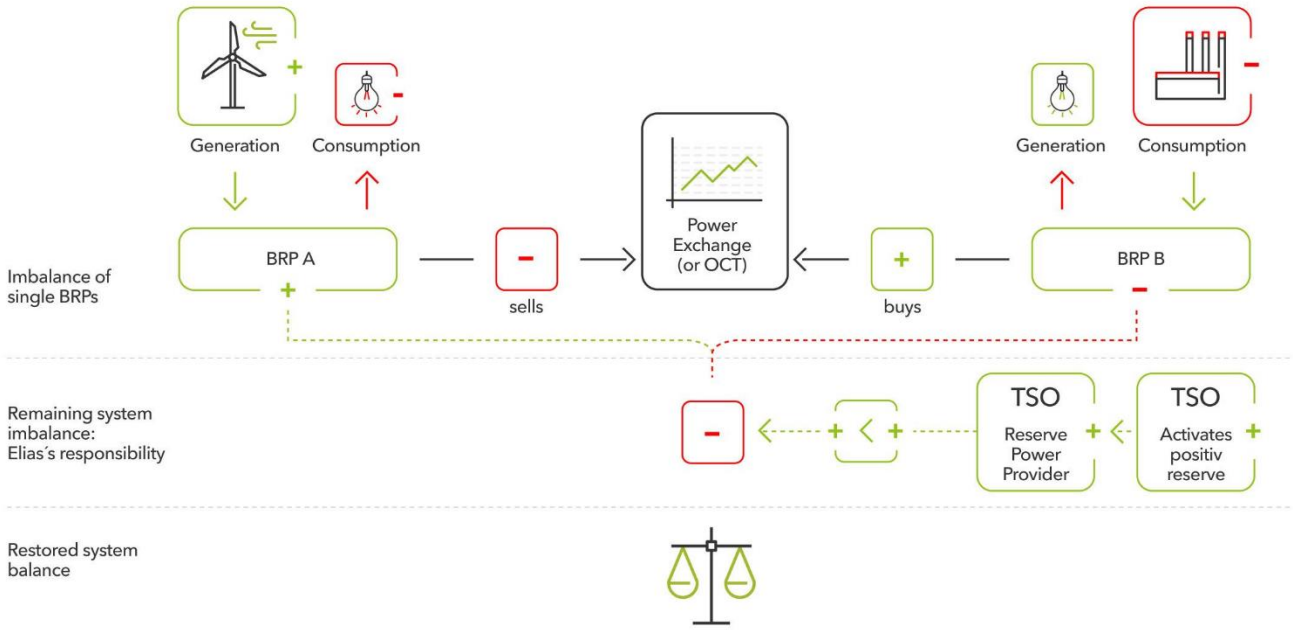

Figure 4. Example of BRPs and imbalances visualisation in Germany © Next Kraftwerke [9].

2.3.4.Generation optimization

Generation optimization involves optimizing the operations of central production units to prepare for the following hour planned production volume. Due to the limited control speed of conventional power units, they need to anticipate by ramping up or down ahead of time. However, to avoid imbalance, the output may require some overshoot, which would negatively impact the unit's lifetime and increase their consumption. The use of distributed flexibility can prevent this situation by providing more precise balancing from distributed units [6].

2.4. Constraints management service/markets

Constraints management services are procured by network operators to help alleviate potential issues linked to the physical limitations of the grids. For prosumers connected at distribution level, services provided to the DSO are particularly relevant. Typically, there are not yet fully established open marketplaces for the procurement of those services, especially at the distribution level, but various pilot projects have demonstrated proof of concept implementations. In some cases, they can be procured through aggregators or Demand Response (DR) programs.

2.4.1. Voltage management services

Voltage issues may arise when solar PV systems, wind farms or other distributed generation units produce substantial amounts of power, causing a surge in voltage levels within the grid's vicinity. Employing Demand Flexibility (DF) as a means to either increase the load or decrease generation

can prevent the voltage from surpassing any preset limits. DF can, therefore, lessen the necessity for grid investments, such as automatic tap changers, or prevent the need for generation curtailment. One specificity of voltage management services is that they can be provided through reactive power compensation, a service that can be provided by resources with inverters such as PV systems, wind turbines and batteries.

2.4.2. Congestion management services

The management of congestion involves preventing system components from becoming overloaded by reducing peak loads, which could cause failure situations. Congestion management is a temporary solution, and the long-term solution is usually grid reinforcement. In most European countries, congestion management is a highly regulated mechanism that is currently available to TSOs. Various initiatives are ongoing to extend it to DSOs in the future. For example, [15] provides a thorough discussion of possible solutions involving distributed flexibility for congestion management on distribution grids.

In the current existing mechanisms, the TSOs may have direct access to demand-side resources, such as load curtailment through smart meter infrastructure. Various congestion management mechanisms are more market-oriented, allowing aggregators to participate.

2.4.3. Islanded operation and restoration

The goal of controlled islanding is to avoid interruptions to the power supply in a particular grid section caused by malfunctions in any of the sections that supply it. DF can be employed to better match local supply with demand. In the event of a power loss, DF can assist the DSO in restoring loads more quickly and efficiently in a depleted network environment. This might involve using flexibility to reduce the load, allowing for the recovery of other non-flexible loads.

3. Service architectures

Depending on several factors such as the types and sizes of resources providing flexibility, the types of customers owning or operating these resources, and the markets that are targeted, various service architectures may be possible. Architectures are useful to represent:

- **Organizational architecture:** The interactions of the different stakeholders participating in the flexibility value chain and their roles.
- **Technical infrastructure:** The interactions between the different technical components such as measurement devices, computing infrastructure, UIs, communication channels / protocols, and message content descriptions.

They provide an overview of the numerous ways through which flexibility services can be built. Generally, it is not possible for small to medium size consumers to directly enter the market and offer flexibility to the final service buyer, for example the transmission system operator. Therefore, one or several levels of aggregation are necessary. The role of the aggregator is to pool different kinds of resources and coordinate them to offer services on the market on behalf of the final customers. This relies on various IT tools to collect data, forecast flexibility, request, and dispatch activations, etc.

3.1. Organizational architecture

3.1.1. Needs and position of GLocalFlex platform

The need for novel consumer-oriented flexibility markets can be discussed based on findings on an existing market structure. A blockchain-based Crowd Balancing Platform (CBP) EQUIGY is designed for today's existing ancillary service markets with the intention of unlocking new flexibility from DERs. According to the market analysis of EQUIGY [16] one of the main barriers identified to incentivize potential market participants and unlock their existing potential is the low economic benefits for participating in the market.

> *"We have identified technical and regulatory barriers for the participation of DERs as flexibility providers in ancillary services. These barriers are interdependent and many of the technical and regulatory barriers are closely connected to the barrier of economic benefits, meaning that even though it is assumed that in case the technical and regulatory barriers are lowered or removed, the incentives to participate in the market are still too low to unlock the full potential available in the market. Nevertheless, lowering and removing technical and regulatory barriers will have to some extent a positive impact on the economic benefit barrier. The identified barriers can be a higher obstacle for small and independent aggregators to participate in ancillary services. "*

Although the above conclusion is made in the context of EQUIGY, it indicates that the concept of the GLocalFlex marketplace is highly relevant. One of the main tasks is to demonstrate how consumers and small energy actors can bring their flexibility directly to the market.

The GLocalFlex marketplace solution is based on an open system flexibility trading platform[5] which is automated and designed to achieve the lowest possible entry barrier to increase the participation of consumers and small players. This market is designed to operate without aggregators . In particular, the GLocalFlex solution has its place in supplementing co-existing

[5] https://fleximarex.com/

flexibility solutions that are typically grid oriented and targeted for larger transactions, but in turn posing barriers for consumers.

The GLocalFlex flexibility marketplace will have a neutral and well-defined rule base that is applicable to all energy stakeholders (buyers, sellers, aggregators, end-consumers, etc.), irrespective of their offer size, consumer class, locality, or their business category. Therefore, GLocalFlex is in line with the customer empowerment goals of the EU's new Clean Energy Package 2018. The implementation of the GLocalFlex marketplace utilizes blockchain based technologies in various ways, focusing on economical trading of small batches of flexibility. In this way prosumers can participate in the GLocalFlex market directly without any intermediary aggregator.

Different market models with the GLocalFlex platform

With the GLocalFlex platform, the consumer level flexibility is incentivized differently from the currently existing ways. Furthermore, the role of a consumer is empowered due to the ability to decide on personal data, market presence, and pricing of flexibility. Figure 5 illustrates the GLocalFlex marketplace from flexibility providers and consumers' point of views.

Ideally, there are many flexibility buyers at the GLocalFlex marketplace. This improves the utilization of flexibility resources, and consumers benefit from the possibility of getting a better price for their flexibility. In particular, the consumers are no longer tied to one aggregator. Depending on the price, the seller-buyer relationship changes for each bid. Naturally, this requires that the GLocalFlex marketplace takes the responsibility of bids activation, verification etc. that are currently the responsibilities of an aggregator in a consumer-aggregator relationship.

Flexibility buyers at the GLocalFlex marketplace can be various actors, e.g.:

- **Aggregators** who possibly combine GLocalFlex flexibility with more controllable energy resources and bid flexibility further to other markets with suitably long-time windows for services. GLocalFlex fits well to the needs of aggregators.
- **DSOs** who use consumer flexibility to solve grid congestion.
- **BRPs** who need to adjust balances.

The GLocalFlex marketplace can be integrated into energy communities, infrastructures, and markets in multiple ways. An example of a full integration is illustrated here, whereas pilots implement slightly different ways of utilizing the GLocalFlex platform.

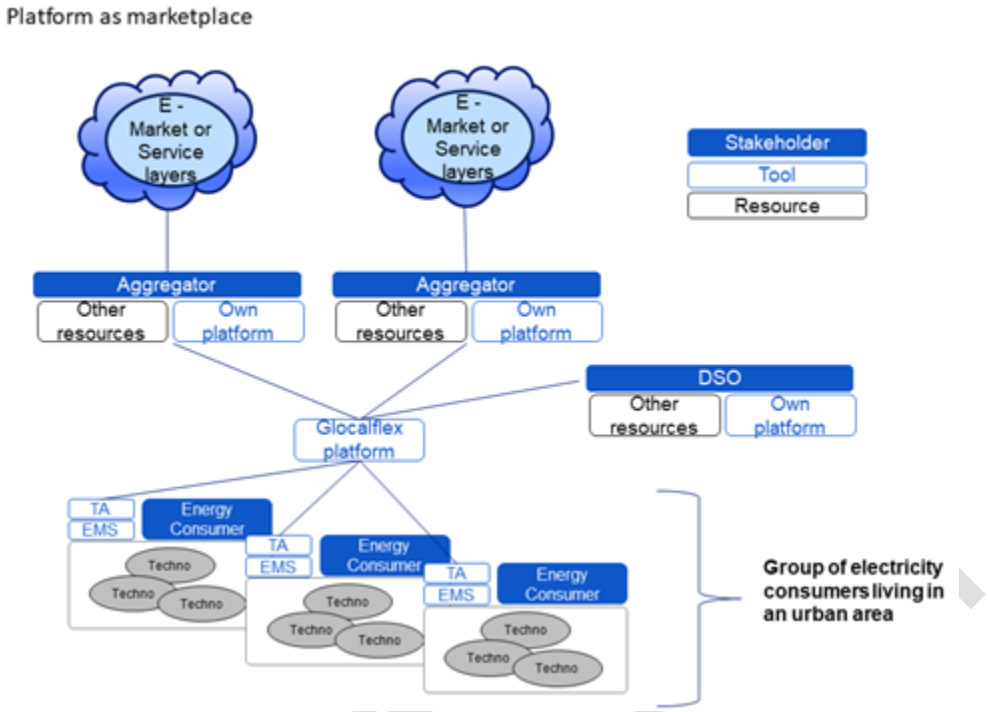

Figure 5. Example of the GLocalFlex platform as marketplace.

3.1.2. Variants of architecture

We depict below 4 variants of architectures for flexibility services. Each variant identifies the roles of the stakeholders, tools, and resources involved in the system, including the envisioned position of the GLocalFlex platform.

The variants are:

Table 1. Architecture variants for flexibility services with the GLocalflex platform.

Variant	Figure	Description / remarks
a) Single aggregator	Figure 6	A first level of aggregation relying on the GLocalFlex platform allows end prosumers to bid flexibility which can be purchased by a market aggregator that bids it on the market.
b) Integrated platform	Figure 7	Similarly to the single aggregator, the platform is accessed by end prosumers, and there is a single buyer for the flexibility which uses it for its own internal purpose. Typically, this buyer would be the DSO, which will utilize flexibility to e.g. mitigate grid congestion, voltage support, etc.

		In practice, the fact that there is a single buyer makes it so that the buyer can itself operate the platform. In addition, compared to a case where flexibility is further sold on an open market, the buyer can apply its own standards in terms of verification process, accuracy required, etc.
c) Multiple aggregators	Figure 8	This is similar to the first case but allows multiple aggregators to access the flexibility bid submitted by users. Note that recommendations for flex markets (see section 4.3.2) promote the possibility for multiple flex buyers to access the same resources (although not simultaneously). This has several advantages: avoiding duplicates infrastructure, increasing competition that should benefit end users. On the other hand, it also brings more complexity because i) a separate independent party needs to operate the platform, ii) multiple aggregators accessing the same resources requires corrections in energy supply schedules between BRPs (see also section 4.3.2)
d) P2P	Figure 9	There is no higher-level buyer or flex market involved. In this case, it should be noted that the distinction between P2P energy and flex trading are not clearly distinguishable

Note that in practice, these models can be combined in hybrid scenarios such as depicted in Figure 5. As of the time of writing, the proposed architecture for the French pilot follows architecture a), the Swiss and German pilot architecture b), and the Finish pilot a mix of b) and d).

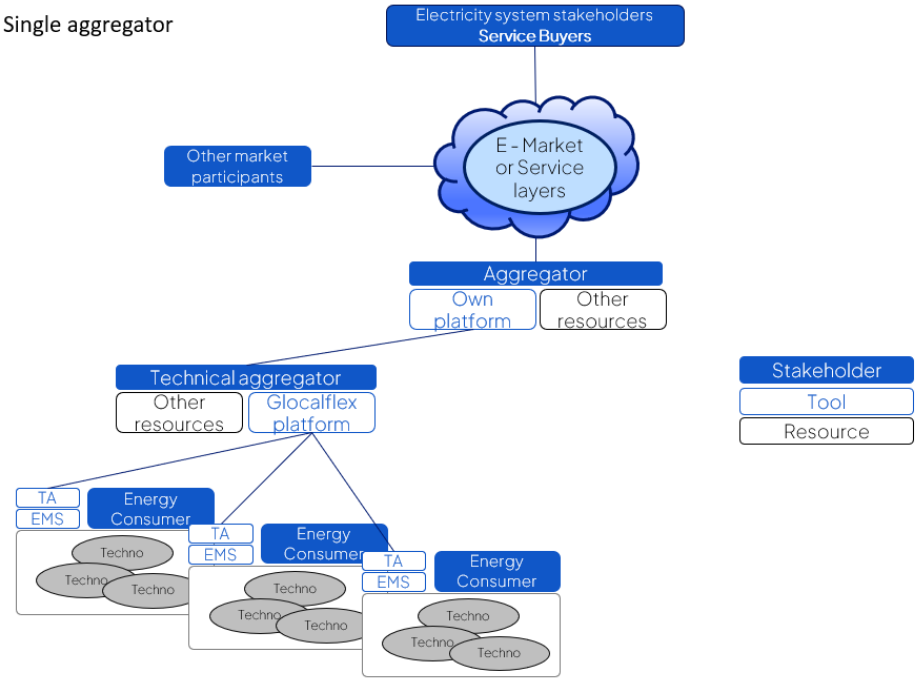

Figure 6. Overview of single aggregator model. Source: EDF

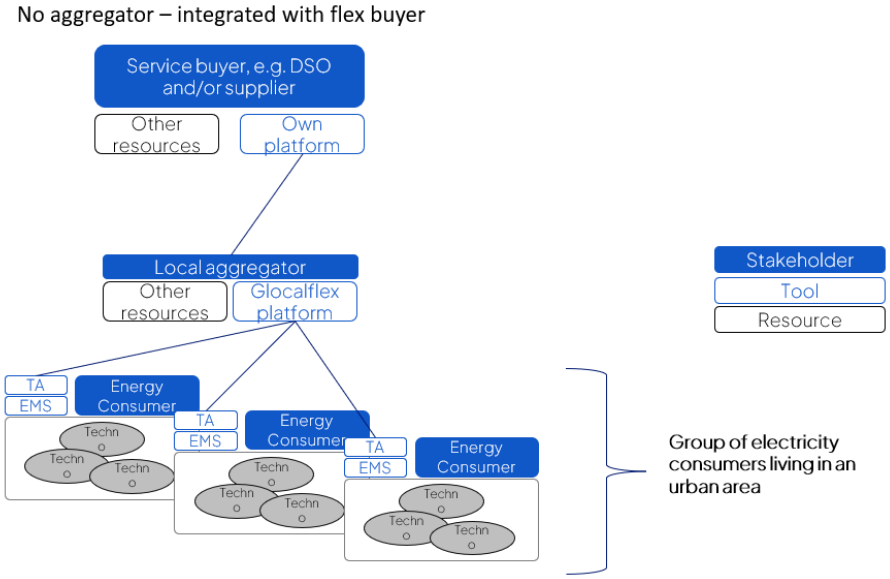

Figure 7: Overview of integrated buyer platform.

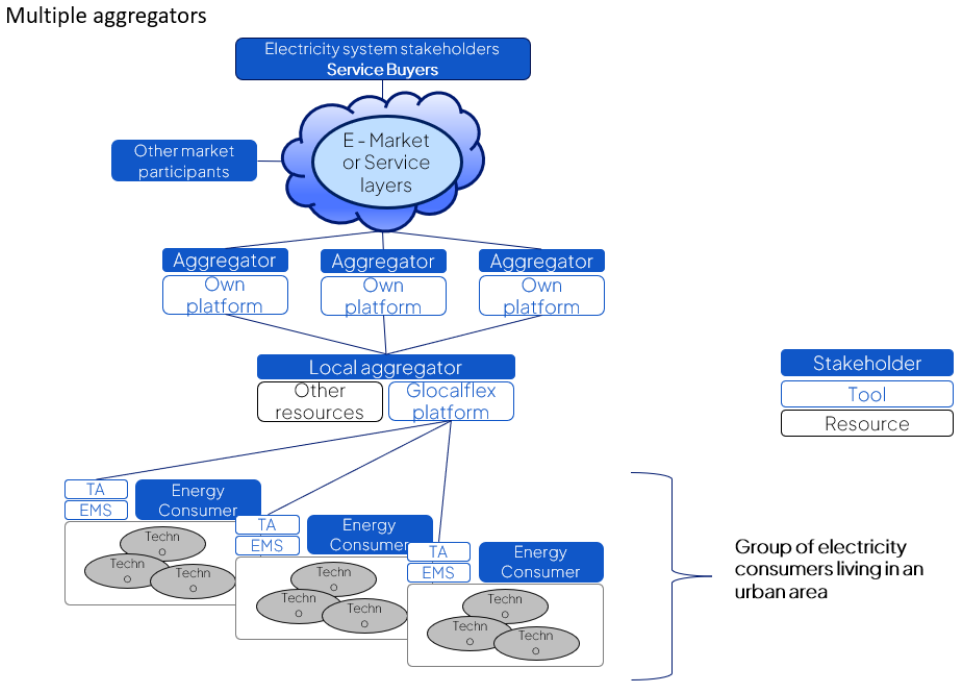

Figure 8: Overview of multiple aggregator architecture.

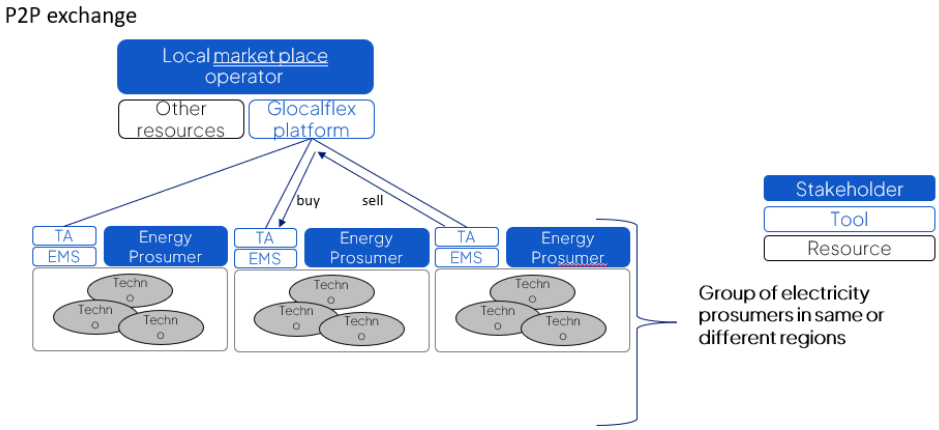

Figure 9: Overview of P2P exchange model.

3.2. Example of French pilot

We provide here a detailed description of the architecture for the French pilot, including the technical architecture which will be similar in other sites but are not all currently finalized.

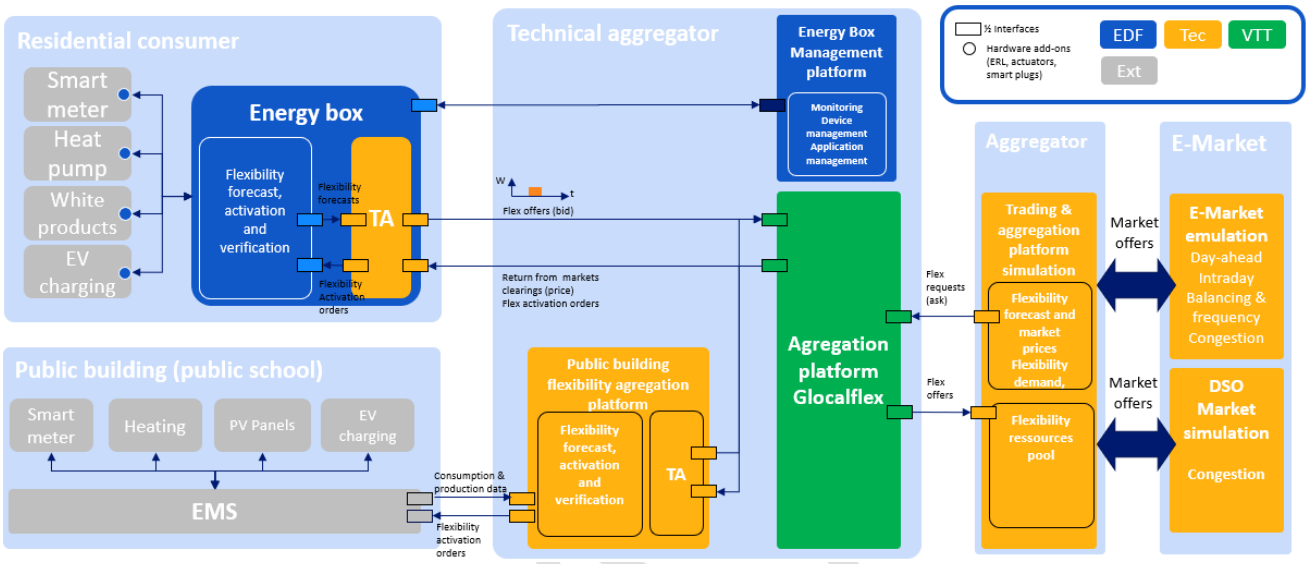

Figure 10. Proposed architecture for French pilot. Source: EDF

3.2.1. Organizational architecture

In the French pilot, the GLocalFlex platform implements a flexibility marketplace between energy consumers and a market aggregator. Hence, the platform could be run by a "primo aggregation" entity, depicted as “technical aggregator” that aggregates the flexibility offered by a variety of energy consumers, from non-residential households to public infrastructures and buildings or sport facilities.

In addition to the aggregation of a variety of small flexibilities to build a flexibility product eligible for the market aggregator, the primo aggregator must deal with the deployment of hardware add-ons and software to communicate with the flexible assets. To that aim, multiple scenarios are possible:

- Deployment in the buildings of an energy management system and its IoT ecosystem, managed by the primo aggregator. This option will be considered for the residential households.
- Deployment of a remote communication with an existing energy management system. This option will be deployed for the non-residential households.

To optimize the economic value of the flexibility, the primo aggregator must deploy a trading agent (TA), whose role is to assess a price for the flexibility, based on multiple criteria defined in D2.1, and to implement the application interface with the Glocalflex platform.

Hence, the role of the primo aggregator is to elaborate the best flexibility offer to the market aggregator, resulting from the aggregation of a variety of individual flexibilities. The primo aggregator is responsible for the technical layer required to remotely manage the flexible assets, and its underlying complexity due to the variety of configurations, while the market aggregator is dedicated to interacting with the energy and flexibility markets.

Depending on the flexibility services targeted, the primo aggregator can aggregate flexibilities at a local or global level.

- Flexibility offers for the DSO will aggregate flexibilities of energy consumer behind a specific group of substations.
- Flexibility offers for balancing and frequency regulation services will aggregate flexibilities of energy consumer on a much larger scale, to reach the amount of energy eligible for the market aggregator.

Finally, the primo aggregator must have in its portfolio additional resources to compensate or cover to the extent possible the risk of non-delivery by the end-consumers.

3.2.2. Technical architecture

The technical component architecture aims at representing the components that must be deployed on the premises of the different involved stakeholders to make the business scenarios happen on the French pilot site.

The arrows represent the circulation of the data between the components.

For the residential participants, the energy box acts as an energy manager that interacts with an ecosystem of IoT objects deployed to control existing appliances. The communication between the gateway and the connected objects relies on a Zigbee network, coordinated by the gateway. The application layer of the Zigbee protocol offers a standardized way to exchange application data for a broad range of equipment category known as clusters. For example, the gateway will extensively use the “electrical measurement” and “smart metering” clusters to interact with the smart meter through the ERL (Linky Radio Emitter).

The energy box, as well as the energy management systems of the non-residential consumers, communicate with the technical aggregator platform through the internet and using MQTT/TLS and HTTPS protocols. The application layer will rely on the Glocalflex platform interface specifications.

The communication between the Glocalflex platform and the (market) aggregator, which will be simulated by a “simulated buyer” developed in WP4 is ensured with standard internet protocols like HTTPS or MQTT/TLS. The application layer relies on the Glocalflex platform, and the standards used for flexibility markets, like CIM-MARKET.C V

4. Cartography of relevant standards

Starting from the architecture, we list relevant standards that are pertinent to various aspects of flexibility, provide references to documents describing these standards, and summarize how they are relevant (a few paragraphs maximum).

4.1. Overview

As a broad concept, flexibility connects to most aspects of power grids/smart grids and therefore practically all standards for power systems and smart grids can be considered relevant to the topic flexibility. While we will focus in the next sections on a subset of the standards that we consider most relevant, we provide pointers here in order to help navigate the very large body of standards.

4.1.1. Standardization bodies and other relevant organizations

Several key standardization bodies are relevant for smart grid standards. The main ones are:

- **IEC:** Founded in 1906, the IEC (International Electrotechnical Commission) is the world's leading organization for the preparation and publication of international standards for all electrical, electronic, and related technologies.
- **CENELEC:** CENELEC, the European Committee for Electrotechnical Standardization, is an association that brings together the National Electrotechnical Committees of 34 European countries. It prepares voluntary standards in the electrotechnical field, which help facilitate trade between countries, create new markets, cut compliance costs, and support the development of a Single European Market. CENELEC supports standardization activities in relation to a wide range of fields and sectors including: Electromagnetic compatibility, Accumulators, primary cells and primary batteries, Insulated wire and cable, Electrical equipment and apparatus, Electronic, electromechanical and electrotechnical supplies, Electric motors and transformers, Lighting equipment and electric lamps, Low Voltage electrical installations material, Electric vehicles railways, smart grid, smart metering, solar (photovoltaic) electricity systems, etc.
- **ETSI:** ETSI was set up in 1988 by the European Conference of Postal and Telecommunications Administrations (CEPT) in response to proposals from the European Commission. ETSI is an independent, not-for-profit standardization organization in the telecommunications domain (equipment makers and network operators) in Europe, with worldwide projection. ETSI produces globally applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies.

We refer the reader to the previously published report[6] [17] for a more detailed presentation of those organizations

4.1.2. Smart grid standards map (SGSM)

This online resource [18] offered by the IEC references smart grid standards and organizes them according to various criteria. The main page offers a graphical map where relevant standards can be listed for different clusters representing business domains.

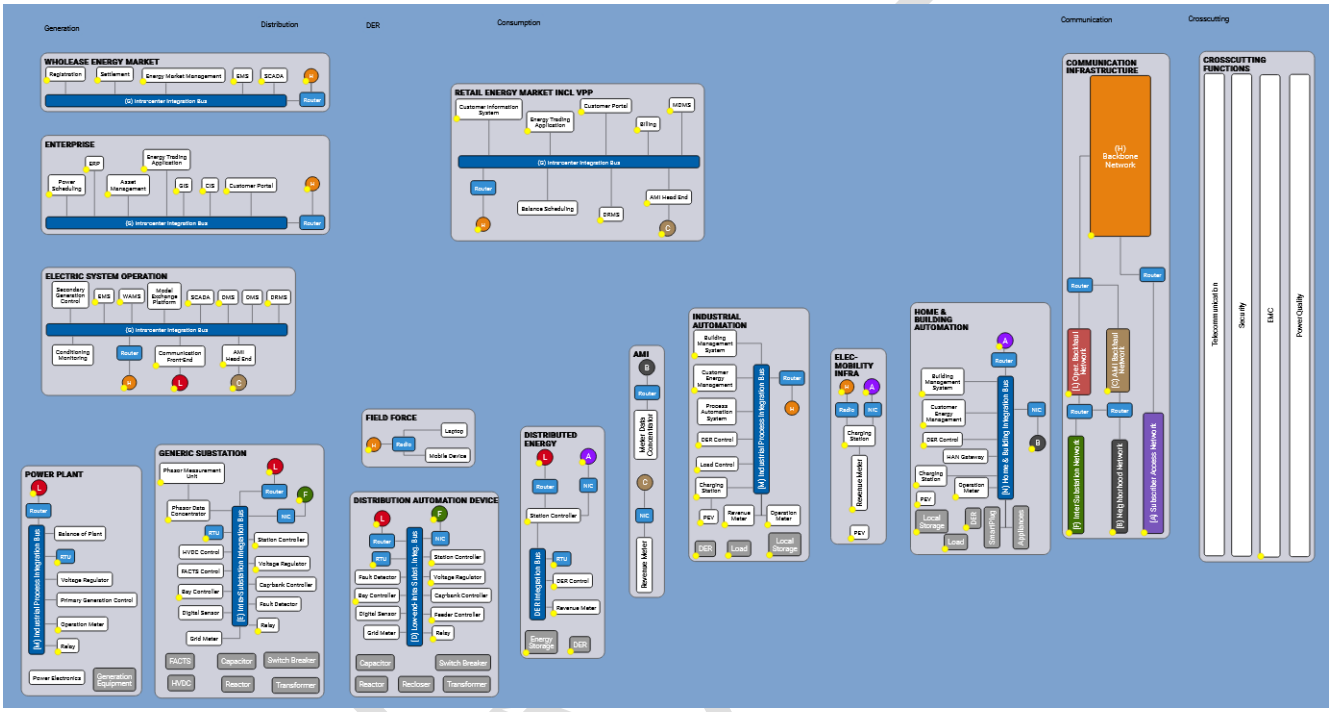

Figure 11. Screenshot from IEC SGSM resource [18].

The most important clusters for Glocalflex pilots are *industrial automation, home & building automation, elec-mobility infra, distributed energy* and *automated metering infrastructure (AMI)*, while the cluster *retail energy market including VPP is* also relevant to the platform. Specific aspects of other clusters can also be of interest.

In addition, the SGSM, allows to also cluster standards by use cases. The most relevant use cases listed for flexibility are:

- BEMS control of DER and HVAC

[6] Proposal for data exchange standards and protocols, D5.5, EU project EU-Sysflex, available at: https://eu-sysflex.com/wp-content/uploads/2021/05/Deliverable-5.5-report-FINAL-2021.04.29.pdf

- CIM model from IEC 61850
- Consumer portal: EV management
- Consumer portal: DER management
- Customer implements demand response
- Demand response: Load profile management via pricing mechanisms
- Demand response: Load profile management via reliability-based signal
- DER management
- Energy scheduling, billing, and settlement
- Energy storage and DER
- EV load management
- HEMS

4.1.3. SGAM

A robust and established tool [19] to model interactions (primarily exchange of information) between different entities in smart grid applications is the Smart Grid Architecture Model[20]. It uses a three-dimensional model to represent different entities.

- **One dimension spans the electrical energy conversion chain, partitioned into 5 domains:** Generation, Transmission, Distribution, DER (Distributed Energy Resources) and Customers' Premises
- **The second dimension the hierarchical levels of power system management, partitioned into 6 zones:** Market, Enterprise, Operation, Station, Field, and Process
- **The third one the 5 superimposed interoperability layers:** Business, Function, Information, Communication and Component

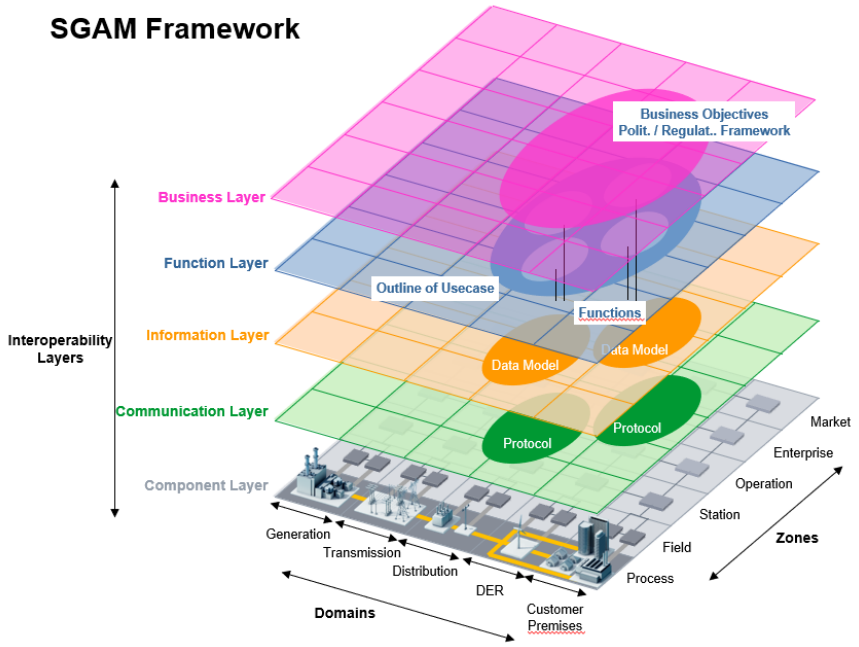

Figure 12. SGAM 3D-model. © CEN and CENELEC, reproduced with permission. Source: SGAM user manual [21]

From a technical point of view, the three bottom layers are of main interest and are in the scope of this deliverable. In particular, the domain-zone-interoperability breakdown of SGAM is helpful to visualize the scope of different standards.

4.1.4. Standards for information exchange

Exchange of information and data is a particularly important aspect of smart grids and is maybe the most widely covered topic in standards. The topic of how information is exchanged can be separated into several levels or layers, such as formalized in the open systems interconnection (OSI) model [22]. For our purpose, we propose the following high-level separation:

- **Ontology**, also known as data model, to describe the content of message payloads: what data and metadata can be exchanged, possibly also modelling relationships between data. This corresponds to the information layer in the SGAM model.
- **Communication and transport** that concern how information is encoded and physically transmitted between emitters and receivers. This corresponds to the communication (and sometimes component) layer in SGAM.

We refer to the excellent analysis provided in section 2.4 of this report [17]for an analysis of a broad range of information exchange standards and their coverage of various business use cases.

4.2. Smart energy ontologies, data models, vocabularies

4.2.1. Purpose and definitions

According to SAREF:

ontology: *formal specification of a conceptualization, used to explicit capture the semantics of a certain reality.*

From Wikipedia [23]:

In computer science and information science, an ontology encompasses a representation, formal naming, and definition of the categories, properties, and relations between the concepts, data, and entities that substantiate one, many, or all domains of discourse. More simply, an ontology is a way of showing the properties of a subject area and how they are related, by defining a set of concepts and categories that represent the subject.

The main goals of using ontologies are:

- **Help humans to interpret data:** ontologies work with concepts and relationships in ways that are close to the way humans perceive interlinkages.
- **Enable interoperability:** in other words, allowing distinct devices to exchange information and perform tasks together automatically.
- **Automate reasoning about data:** by having the essential relationships between concepts built into them, they can enable to implement e.g., data storage technologies such as semantic graph databases that use ontologies as their semantic schema.

4.2.2.Relevant data models and associated standards

Historically, different standards have been developed and focusing specifically on seemingly distinct domains. This leads to some level of heterogeneity which recent standardization efforts are attempting to reduce through harmonization

Note that in many cases, standards define both the data models together with other aspects such as communication protocols, which are presented in more detail in section 4.4 of this document.

4.2.2.1. IEC data models

IEC and in particular its technical committee 57 (TC57) have historically developed two main data models that address different zones (as understood in the SGAM framework):

- Common information model (CIM) for the market, enterprise, and operation.
- IEC 61850 for the station, field, and process.

The coverage of those two elements is illustrated in the Figure below. Both cover the full range of domains, except the customer premise which can be managed with various other data models

depending on the type of devices concerned, and due to the fact that the standards applicable to those were not necessarily developed with smart grid applications as the only or primary purpose.

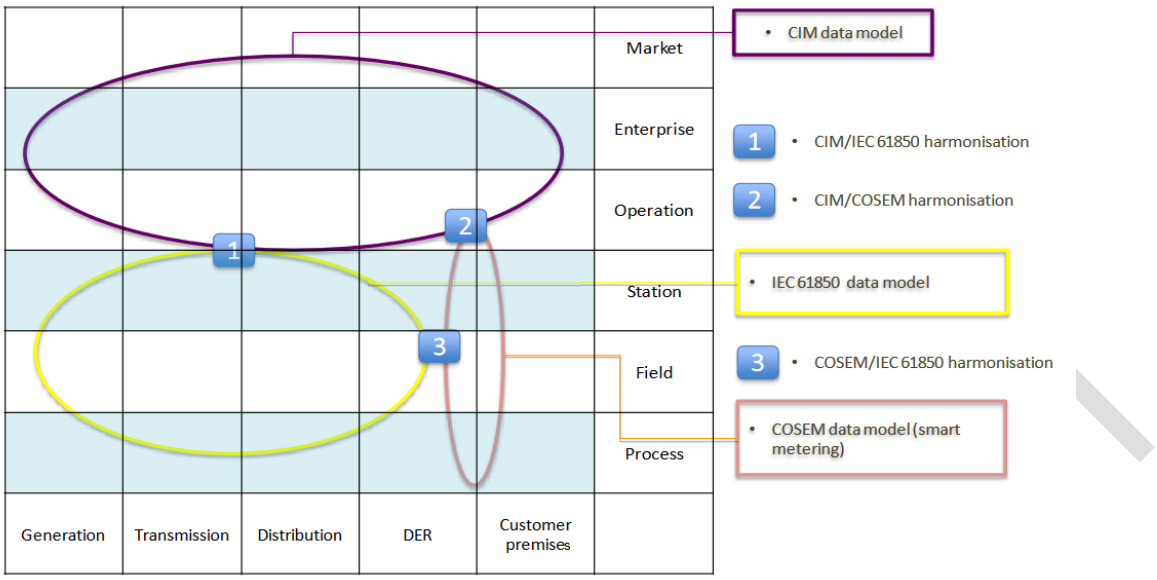

Figure 13: Data modelling harmonization. © CEN and CENELEC, reproduced with permission. Source: SGAM User Manual [21].

CIM

CIM allows application software to exchange information about an electrical network and related business domains and CIM relies on UML to structure information.

CIM covers different aspects defined in separate standard document.

- Core CIM is defined in IEC 61970-301, with a focus on the needs of electricity transmission, where related applications include energy management system, SCADA, and planning and optimization.
- Network model exchanges are covered in IEC 61970-501 and 61970-452.
- Needs of electrical distribution are covered in the IEC 61968 series of standards, where related applications include distribution management system, outage management system, planning, metering, work management, geographic information system, asset management, customer information systems and enterprise resource planning.
- Energy markets communications, in particular wholesale market in IEC 62325-301.

IEC 61850

IEC 61850 is a standard defining communication protocols for intelligent electronic devices at electrical substations. It includes abstract data models defined in IEC 61850 that can be mapped to a number of protocols. It is broken down in multiple parts and has been extended to cover other

aspects beyond substations, including DERs in IEC 61850-7-420, power converters of DERs in 61850-90-7, and even e-mobility in IEC 61850-90-8.

Useful links and documents for further information on CIM and IEC 61850 include:

- https://www.entsoe.eu/digital/common-information-model/
- https://docstore.entsoe.eu/publications/electronic-data-interchange-edi-library/Pages/default.aspx for a list of implementation guides for various CIM aspects, published by ENTSO-E
- CIMdraw[7] is an open-source tool to draw using CIM.
- https://www.youtube.com/watch?v=j5RnjRnlaow : overview of both IEC61850 and CIM
- Openiec61850 is open-source library that implements the standard.
- [24]: publication on interrelation of CIM and IEC 61850

4.2.2.2. SAREF/SAREF4ENER

According to the SAREF homepage [25], "**The Smart Applications REFerence (SAREF)** ontology is a shared model of consensus that facilitates the matching of existing assets in the smart applications domain." As such its purpose of use is very broad. SAREF uses OWL for its specifications, which allows more expressive power than uml.

SAREF is developed by the ETSI and was initially designed with IoT as the primary focus. Nevertheless, it is extensible by design and numerous extensions have been developed, including one dedicated to energy applications, called SAREF4ENER.

SAREF4ENER [26] was jointly developed in collaboration with the EEBus [27] initiative and Energy@Home initiative. SAREF4ENER focuses on demand response scenarios, in which customers can offer flexibility to the Smart Grid to manage their smart home devices by means of a Customer Energy Manager (CEM).

The definition document for SAREF4ENER is available publicly [28].

4.2.2.3. EEBus ontology

The ontology underpinning the EEBus data model is compatible with SAREF4ENER, as SAREF4ENER was built on top of the EEBus architecture. A full description of the EEBus suite is provided in Section 5.3.

4.2.2.4. OpenADR

OpenADR is an open, highly secure, and two-way information exchange model and global Smart Grid standard. OpenADR standardizes the message format used for Auto-DR and DER

[7] https://github.com/danielePala/CIMDraw

management so that dynamic price and reliability signals can be exchanged in a uniform and interoperable fashion among utilities, ISOs, and energy management and control systems. Open ADR has seen adoption centred in the United States but is also present in other parts of the world. The current version of OpenADR is version 2.0 which was published in 2013. The International Electrotechnical Commission (IEC) approved the OpenADR 2.0 Profile Specification as IEC 62746-10-1 in 2018. It mostly focuses on communication, not on individual equipment but between local energy management systems and upper levels: aggregators or network operators to help them establish DR programs. It has been used on a large scale in DR programs in the US, and there are currently more than 200 commercials certified with OpenADR.

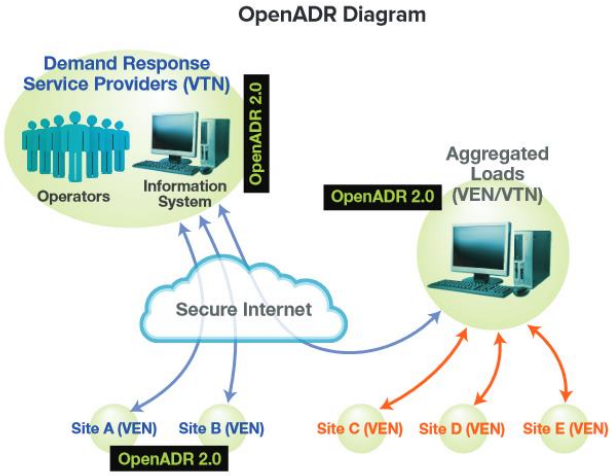

Figure 14. OpenADR diagram. Source: OpenADR alliance [29].

It specifies the communication between so-called virtual top nodes (VTNs, servers) and virtual edge nodes (VEN's, clients). It uses XML payloads and uses communication over internet (with TLS 1.2). Two levels of specifications have been published : OpenADR 2.0a in 2012 and OpenADR 2.0b [29] in 2015 with the use of OpenADR2.0b being compulsory for VTNs.

OpenADR relies on an information model and specifies several types of messages that can be used in communications enabling participation of demand-side resources in DR programs and events. Message types supported in OpenADR 2.0b are the following (source: OpenADR specification document)

- **Registration (EiRegisterParty):** Register is used to identify entities such as VEN's and parties. This is necessary in advance of an actor interacting with other parties in various roles such as VEN, VTN, tenderer, and so forth.
- **Event (EiEvent):** The core DR event functions and information models for price-responsive DR. This service is used to call for performance under a transaction. The service parameters and event information distinguish distinct types of events. Event types include reliability events, emergency events, and more – and events MAY be defined for other actions under a transaction.

- **Reporting or Feedback (EiReport):** The ability to set periodic or one-time information on the state of a Resource (response).
- **Availability (EiAvail):** Constraints on the availability of Resources. This information is set by the end node and indicates when an event may or may not be accepted and executed by the VEN with respect to a Market Context. Knowing the Availability and Opt information for its VENs improves the ability of the VTN to estimate response to an event or request. (Planned for future releases).
- **Opt or Override (EiOpt):** Overrides the EiAvail; addresses short-term changes in availability to create and communicate Opt-in and Opt-out schedules from the VEN to the VTN.

Other types of messages have been specified for future specifications but are not part of OpenADR 2.0b, such as availability, or messages for distributing complex dynamic prices such as block and tier tariff communication.

There exists an open source VTN and VEN reference implementation of OpenADR by EPRI, but it is old (2014), as well as more recent ones, e.g. OPENLEADR [30] is a python package to implement OPENADR.

4.2.2.5. Matter data model

The matter standard data model is used to specify devices. It is documented in the online documentation of Matter[8]. A full description of matter is provided in section 5.5.

4.2.2.6. Summary comparison

Table 2: Summary of ontologies proposed for the energy domain.

Ontology / Data model	Authors	Scope	Modelling language	Recommended / associated communication protocol
CIM	IEC	Power grids, energy markets	UML	NA

[8] https://developers.home.google.com/matter/primer/device-data-model

IEC61850 data models	IEC	Distribution substations, DERs	UML/XML	GOOSE / MMS
SAREF4ENER	ETSI	Energy domain	OWL	NA (agnostic)
EEBus ontology	EEBus association	Home and industrial energy management	OWL	SPINE - Data model SHIP - Network TCP - Transport WebSockets- Application
OpenADR information model	OpenADR alliance	DR events and tariffs for	XML for messages	XMPP + HTTP - Application
Matter data model	Connectivity standards alliance	Home energy management / Home automation	None	Thread

4.2.2.7. Other relevant ontologies

There exists a large number of partial or complete ontologies to address domains with some overlap with energy. We provide here a quick summary table of potentially relevant efforts, categorized in groups.

Table 3: Summary of other relevant onotologies

Category	Ontology
Home automation, smart home	KIM (linked to KNX protocol), standard EN 50090-6-2:2021[9]
	OpenHab semantic model (linked to open-source smart home system OpenHAB)
	BACnet (BACnet objects) [31]

[9] Home and Building Electronic Systems (HBES)- Part 6-2 IoT Semantic Ontology model description.

Building domain, including building automation	bricks
	SAREF4BLDG
	EEPSA ontology
	BIM standards
IoT	OneM2M
	Thing description ontology (web of things)
Device-specific	SunSpec (for solar inverters)

4.3. Verification

4.3.1. Definitions

In all instances of flexibility, an important part of the process is to verify if flexibility requested was effectively delivered. A flexibility activation is to be understood as a deviation in energy consumption/production with respect to a reference, usually called ***baseline***.

The baseline for a flexibility activation should be understood as the consumption/production in a "business-as-usual" scenario, where no flexibility is provided. A baseline can concern a single device, a flexibility provider or aggregation of devices.

In practice, as it is impossible to know exactly what would happen with and without a given flexibility event, there needs to be agreed-upon rules for determining the baseline.

Verification which is part of the settlement phase is the step that is required to verify if the flexibility was actually delivered and involves comparing the baseline and the actual consumption/production, based on metered data.

4.3.2.Relevant standards and recommendations

Depending on the type of flexibility service provided, and possibly the type of flexibility provider, the verification process and data will be different.

4.3.2.1. USEF recommendations

USEF provides a very comprehensive approach to flexibility market design. It conceptualizes roles involved in flexibility and describes the full process of flexibility provision from contracting to requests in different scenarios (in particular, congestion management scenarios), verification and financial settlements. While USEF provides a well-known conceptual overview of flexibility, it is not a standard and does not attempt to make connections to existing rules in various real-world flexibility markets.

Below is an excerpt of the framework description document of USEF, related to verification.

When separating supply and flexibility, the Aggregator takes responsibility for the activation of flexibility and the Supplier for the energy supply. In this attempt to separate flexibility from supply, we apply three main principles:

1. *The responsibilities of the Aggregator (and their BRP) are restricted to:*
   - *(i) the activation periods. For the activation period the so-called rebound effect needs to be considered.*
   - *(ii) flexibility assets that are activated.*
   - *(iii) for each activated asset, the deviation from its baseline.*
2. *The Aggregator does not need to take responsibility for the Active Customer's supply of energy.*

The effects of the flexibility activation for the Supplier and the related BRP should be identifiable such that Supplier could be compensated. These principles entail the arrangement of certain key aspects that determine Aggregator, BRP and Supplier relationship, information exchange, effects on sourcing and balancing position. The next section further explains these key aspects. In addition to the aggregator arrangements, one of the main challenges of deploying explicit flexibility is the flexibility delivery validation. While validating supply is straightforward through the main meter reading, validating flexibility delivery is more complex and so other methods are needed. The following complexities should be considered:

- ***Measurement and validation:*** *Ensuring correct and trustworthy data. Since flexible assets are typically behind-the-meter, the Aggregator may apply sub-metering to have a better visibility of the asset performance and quantify the delivered flexibility.*
- ***Baseline methodology:*** *The baseline determines the expected load/consumption pattern without flexibility activation. The baseline is used to validate the delivered flexibility by calculating the difference between the actual measurements and the baseline. Therefore, determining the baseline methodology and related responsibilities is key.*
- ***Relationship between*** *implicit and explicit flexibility: When an Active Customer is making use of both types of services, explicit and implicit flexibility, it is necessary to quantify both impacts unambiguously.*
- ***Rebound effect:*** *After a period in which flexibility has been activated, a rebound effect may occur. For instance, a reduction in energy consumption could lead to demand being shifted to a later time. The impact of this effect should be studied and taken into consideration.*

USEF describes in detail different processes for verification (which is part of the settle phase), with the sequence of information exchanged between systems / stakeholders. One important complexity discussed is that activation of flexibility by an aggregator will affect the energy balance of the balancing group of the resource that provides the flexibility. In the case that the

balancing group is distinct from the perimeter of the aggregator resources, this creates additional need for corrections in the balancing group schedules to avoid balancing penalties. This is referred to as "perimeter correction" in the USEF terminology. USEF provides a deep-dive into this topic in its document [15].

Additionally, section 6 of this same document provides a number of specific high-level recommendations related to the afore-mentioned topics. We provide a condensed summary table (Table 4) of some key excerpts of the recommendations.

Table 4: List of USEF recommendations for verification. Source: [15].

Topic	Recommendation
Measurement & Verification	A flexible resource (asset) can only be operated by one Aggregator at the same time. Contracts with different Aggregators should be sequential in time.
	The market rules should allow two or more Aggregators to be active at the same Prosumer at the same time, provided they operate a mutually exclusive set of resources. In this case, sub-metering is necessary.
	If a Prosumer engages with an Aggregator on the main meter level, no other Aggregators are allowed during the contract period. This should be included in the contract between the Aggregator and the Prosumer.
	Roles, responsibilities, and methods with respect to the quantification of the flexibility delivered by the Prosumer to the Aggregator (as opposed to delivered by the Aggregator to the market), do not need to be regulated.
	If the baseline methodology of a flexibility service is based on a nomination by the Aggregator, then the meter data, used for calculating the baseline, can be collected by the Aggregator, provided the meter meets the technical requirements of either TSO, DSO or other flexibility buyer, depending on the type of product.
	The validation of data, used as input for the Transfer of Energy, needs to be performed by a meter data company (MDC). Since the responsibilities with respect to the main meter (i.e., on connection level) are already well defined, this specifically applies to sub-metering, assuming the baseline methodology is applied on the level of the sub-meter.
	In general, the Aggregator should be allowed to propose the same flexibility to different markets, but to sell it only once.

	The requirements on the accuracy level for sub-meters in the Residential segment can be less strict, compared to the C&I segment. The accuracy only needs to be reached on aggregated level.
Baseline method	The baseline methodology used as basis for the Transfer of Energy (when applicable) is equal to the baseline used for flexibility service quantification (thus the volumes for delivered flexibility, perimeter correction and Transfer of Energy are equal).
	The baseline methodology should be defined by the purchaser of the flexibility service, *e.g.,* the TSO for balancing services, the DSO for congestion management. The regulator may need to approve this methodology, depending on its exact role and responsibility.
	The baseline methodology for wholesale markets should be defined by the regulator.
	For FCR, the baseline methodology should be a 'Meter-Before/Meter-After' (MBMA) method. ▪ The baseline for each event is a constant, equalling the most recent measured power level ▪ The measurement resolution is prescribed by the FCR product ▪ The baseline should be determined on unit (resource) level The requirement to fully base the baseline on actual measurements can be eased for the Residential segment in case no ToE occurs.
	Similarly, recommendations for baselines are proposed for aFRR, tertiary control, intraday and day-ahead (recommendations 205, 206, 207, 208, section 6.2 of USEF report)
Information & confidentiality	Recommendations 301 to 308, section 6.3
Transfer of energy between BRP's	Recommendation 401 to 410, section 6.4
Compatibility of explicit and implicit DR	In general, the combination of implicit and explicit DR should be allowed. Extensive details on which types of tariffs are compatible with which types of flex services are provided in USEF report.
	The baseline methodology should include the effects of implicit DR

	Demand side flexibility cannot be traded through explicit DR at day ahead markets if this flexibility is subject to a time-of-use (ToU) supply contract. This should be enforced by the regulator.
	No special arrangements should be made to facilitate a transfer of energy when flexibility is activated with customers for which wholesale settlement is based on synthetic profiles. Rather, the regulatory framework should support the settlement of all customers based on (smart) meter data. Consequently, customers that are allocated based on synthetic profiles, can only participate in DR services that are not subject to a ToE.
Rebound effects	Recommendations 601 to 604, see section 6.6
Portfolio conditions (specificity of portfolio vs single resource)	Aggregators (or their BRP/BSP) should be allowed to offer flexibility services on portfolio level for all relevant markets. This includes the possibility to pre-qualify portfolios rather than individual assets (e.g., for balancing services).
	Aggregator (or their BRP/BSP) should be allowed to offer different flexibility services from the same portfolio at the same time.
	In theory, the flexibility of a resource per ISP can be split in smaller pieces that are sold on different markets. This should (at least) be limited to markets that use the same or similar baseline methodology.

USEF also established a specification for a flexibility trading protocol focusing on the exchange between Aggregators and TSO and detailed in [32].

4.3.2.2. Other baseline calculation resources

The report [33] provides an excellent overview of different baseline methodologies in the context of Demand Response programs. This publication is US-focused and refers to multiple methodologies that have been or are currently used as DR programs have been popular in the US for a long time. As DR programs target final users with no obligation to announce their forecasted consumption in advance, the baseline methodologies referred in this document are based on previous consumption data and can either be based on selecting one or a set of similar past days as reference, with or without baseline adjustment to account for the impact of weather, or on building a regression model to predict the consumption of the consumer. Note that a baseline methodology based on forecasting is likely to work better in larger sites as aggregation typically reduces the uncertainty of the load consumption. Further discussion is provided in the document

[34]. These two publications are quite focused on the US market conditions. [35] analyses their possible transposition to Europe.

4.4. Communication

Communication is generally defined by 7 layers according to the Open Systems Interconnection (OSI) model. It is characterized by the connectivity solutions, protocols, regulations, and security measures to prevent interception (covered in Section 4.5).

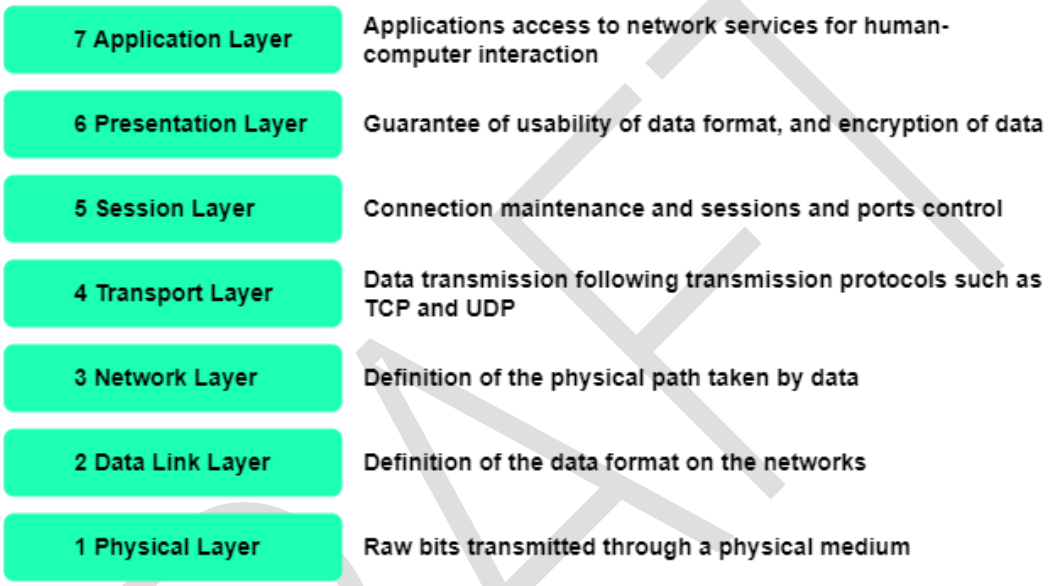

Figure 15. OSI model communication layers.

To provide flexibility services, smart meters need to be connected to their corresponding network. Generally, smart meters are not directly connected to the cloud, but rather rely on a gateway for communication to ensure lighter communication technologies, consuming less power and with lower economic costs. However, a direct connection between the smart meter and the cloud remains an option. Therefore, 3 connection segments are possible:

1. Smart meter to gateway
2. Gateway to cloud
3. Smart meter to cloud

Given the role of smart meters in energy, these connection segments need to implement solutions capable of penetrating walls and buildings. A summary of the communication solutions and protocols is provided in this section based on the review from emnify [36], and completed with other relevant solutions.

4.4.1. Communication technologies

This section covers the base communication technologies possible depending on the connection segment between the smart meter and the cloud. These technologies include at least the physical or data link layer from the OSI model, and specify in some cases other protocols for the other layers. The rest of the layers for each technology can be completed by multiple communication protocols, which are shown in Table 8.

4.4.1.1. Smart meter to gateway

Smart meters require light communication technologies for low power consumption.

Table 5. Smart meter to gateway communication.

Type	Connection	Description	Advantage	Drawback
Wired	Ethernet / Fibre-optic	Data sent to the gateway with TCP/IP or UDP/IP	Connections considered in new buildings No data limitations	Not encrypted (physical access needed to tamper with the device)
	Power Line Communication (PLC)	Data transmission through power lines Data sent to the gateway with TCP/IP	Simple solution No additional network infrastructures needed	Interference between data signals and electrical current
	Meter Bus (M-Bus) [37]	Includes physical (**M-Bus**), data (IEC 870), network, and application (EN1434-3) layers (HAN interface implements M-Bus)	European standard Widely used in buildings Developed for smart meters	No transport, session, or presentation layers Gateway needed to convert data to TCP/IP for transport to the cloud
Wireless	Wireless M-Bus [38]	Wireless version of M-Bus standard Includes physical (**M-**	Widely available in Europe Protocol standardized by the Open Metering System Group	Gateway needed to convert data to TCP/IP

		Bus), data, and application (user-defined) layers	Three different frequencies depending on the mode of a meter or gateway Sub-GHz for signal to travel far and penetrate walls and buildings	
	LoRaWAN [39]	Long Range Wide Area Networks Open-source technology Unlicensed frequency bands Includes physical (LoRa), data, and network layers. Star network topology	Networks widely available Possibility to connect to these networks or deploy their own Longer range than WiFi or Bluetooth Beneficial in remote areas with poor cellular network coverage	Each provider covers a specific region No roaming agreements with Mobile Network Operators (new service provider needed depending on the region of deployment)
	MIOTY	Developed for large-scale industrial IoT applications Low-Power Wide-Area Network (LPWAN) It includes the physical and data layers Data divided into subpackets by telegram splitting, and sent at different time	Reduce interference Limited infrastructure needed	Relatively new technology

		and frequencies		
	Zigbee [40]	Mesh network topology to extend coverage It includes physical (IEEE 802.15.4), data, network, and application layers	Open standard Self-organizing-self-healing mesh topology Pairable with Smart Energy Protocol	Devices need to be within range of each other (short range) Unlicensed 2.4GHz frequency band with low wall and building penetration (interference)
	WiFi	Data sent to gateway with TCP/IP OR UDP/IP	-	Not suited for smart meter communications Same drawbacks as Zigbee Requires integrating device with customer's infrastructure (security risk) Consume more power than other solutions

4.4.1.2. Gateway to cloud

Gateways are directly connected to a power outlet, thus do not have power limitations on their communication solution. Moreover, the gateway receives data from multiple meters, therefore should support higher data flows.

Table 6. Gateway to cloud communication.

Connection type	Connection	Description	Advantage	Drawback
Wired	Ethernet/DSL (Digital subscriber Line); Ethernet / Fibre-optic	Data is sent to the cloud with TCP/IP or UDP/IP DSL uses telephone lines (older buildings)	Integrated in building's layouts.	Not encrypted (physical access needed to tamper with the device) Liability questions

Wireless	WiFi	Data sent to the cloud with TCP/IP OR UDP/IP	-	Reliance on customer's infrastructure (liability) Short range and poor penetration High risk of interference
	Cellular	SIM card to connect Data set to gateway with TCP/IP OR UDP/IP	Infrastructure available globally High indoor coverage and penetration capabilities	-

4.4.1.3. Smart meter to cloud

When a single smart meter is deployed on-site, it is possible to avoid the deployment of a gateway and implementing direct communication between the smart meter and the cloud.

Table 7. Smart meter to cloud communication.

Connection type	Connection	Description	Advantage	Drawback
Wireless	Sigfox [41] [42]	Software based communication solution Network and computing complexity handled by the cloud (transmission translated to TCP/IP) It includes physical, data, network, and transport layers	Low energy consumption Low costs of connected devices	Limited payload (12 bytes)
	Cellular	LTE-M and NB-IoT Data sent to the cloud with TCP/IP with MQTT or UDP/IP with CoAP	Power Saving mode and Discontinuous Reception Over-the-Air firmware updates	-

4.4.2. Communication protocols

The communication protocols vary across the devices, and the base communication technology implemented.

Table 8. Communication protocols.

Protocol abbreviation	Protocol name	Origin	Description	OSI Communication layers
DLMS/COSEM (IEC 62056) [43] [44]	DLMS – Device Language Message Specification COSEM – Companion Specification for Energy Metering	IEC – International standards for smart meters	COSEM – Smart meter data with object modelling DLMS – Syntax specification Different protocol stacks based on the network type	DLMS - Layer 4 – Transport; Layer 5 – Session COSEM- Layer 6 – Presentation
ANSI C12.18 [45]		ANSI – American National Standards Institute	Two-way communication ANSI Type 2 Optical Port Data transfer definition between meter and client	Layers 1-7 (All) Layer 1 – Physical: Optical port (ANSI Type 2)
OSGP	Open Smart Grid Protocol	ETSI – European Telecommunication Standards	OSI model combined with open standards (ANSI C12.18, IEC 62056) Supports multiple communication technologies Multi-application architecture Implements security features	Layers 1-7 (All) Layer 1 – Physical: Power line communication; Radio frequency; Cellular
TCP/IP	Transmission Control Protocol/Internet Protocol	DARPA – Defense Advanced Research Projects Agency	Popular communication protocol for smart meters Accuracy is prioritized over speed	TCP – Layer 4 – Transport IP – Layer 3 - Network

			Allows manufacturers to use multiple communication systems and adapt modules and standards as needed	
UDP/IP	User Datagram Protocol/Internet Protocol	David P. Reed - RFC 768	Alternative to TCP/IP Speed is prioritized compared to accuracy No correction of transmission errors	UDP – Layer 4 – Transport IP – Layer 3 - Network
MQTT	Message Queuing Telemetry Transport	IBM and Arcom	Lightweight protocol Generally combined with TCP/IP Little bandwidth or network resources needed Publish (smart meters/gateways) / Subscribe (network entity) via an MQTT broker	Layer 7 - Application
CoAP	Constrained Application Protocol	IETF – Internet Engineering Task Force CoRE – Constrained RESTful Environments Working Group	Designed for "constrained" networks Generally paired with UDP Highly efficient	Layer 7 – Application
HTTP	Hypertext Transfer Protocol	CERN	Widely used for internet navigation	Layer 7 – Application

			Resource-heavy One-to-one communication Not ideal for smart meter Paired with TCP/IP	
WebSockets		IETF – Internet Engineering Task Force	Simultaneous, bidirectional, real-time communication between a client and a server High power consumption	Layer 7 – Application
XMPP	Extensible Messaging and Presence Protocol	Jeremie Miller - RFC 6120 IETF – Internet Engineering Task Force	Built on XML (Extensible Markup Language) Open-source technology In development for IoT-related features	Layer 7 – Application
OCCP [46] [47] [48]	Open Chart Point Protocol	OCA – Open Charge alliance	Open source Networked EV stations Compatibility between any charger and management software	Layer 7 – Application
Modbus [49] [50]		Schneider Electric	Client/server architecture Widely used for Building Management Systems and Industrial Automation Systems Open protocol	Layer 7 – Application

			Versions for serial lines (RTU and ASCII) and Ethernet (TCP)	
SHIP [51]	Smart Home Internet Protocol	EEBus initiative -Germany's Federal Ministry of Economics	IP-based protocol Machine-to-machine communication Secure communication	Layer 3 - Network
MMS (ISO 9506) [52] [53]	Manufacturing Message Standards	ISO – International Organizational for Standardization IEC – International Electrotechnical Commission ISO/TC 184 Technical committee – Industrial automation systems and integration	Virtual Manufacturing device – Object oriented design Packet and data structure standard Service for data object General communication environment, independent of functions Real-time data interaction	Layer 7 - Application
GOOSE (ISO 61850) [54]	Generic Object-Oriented Substation Events	IEC – International Electrotechnical Commission	Rapid, direct, and secure communication Transmit time sensitive and high priority information Publish-subscribe protocol Multicast messages Message exchange between devices via Ethernet network	Layer 7 - Application

			Application layer directly transported using data link layer	
Zigbee [55]	-	CSA - Connectivity Standards Alliance	Open standard Built on IEEE 802.15.4 Two-way wireless communication Self-organizing-self-healing mesh topology Low-power communication Pairable with Smart Energy Protocol	Layers 1, 2, 3, 7
Matter [56] [57]	-	CSA – Connectivity Standards Alliance	Open-source protocol IP-based Wi-Fi, Threat, and Ethernet network layers Bluetooth Low Energy for commissioning Designed with security measures	Layer 7 - Application

4.5. Security

The EU Commission is gradually highlighting the importance of cybersecurity in the energy sector. In fact, the NIS Directive 2 [1], published in 2022, a legislation suggesting measures that aim to achieve a high and consistent level of cybersecurity across all member states of the EU, identified the energy sector as a critical infrastructure with cybersecurity requirements. In particular, the Commission determined that the energy sector has three distinct features with respect to cybersecurity: the need for real-time responses, the potential for cascading effects, and the coordinated management of both new and old technologies [2].

4.5.1. Security guidelines

USEF provides a comprehensive list of privacy principles to follow in its report "USEF: privacy and security guidelines" [58]. The principles address nine key privacy and security aspects, well defined in Figure 16. These aspects definitions are valid for the remainder of this section.

1	Privacy-value creation trade-offs	Individuals and business can both benefit from sharing certain privacy sensitive data. It might allow for tailor made propositions to the end-user or more efficient management of the energy system. How do we accommodate all legitimate interests and objectives?
2	Data management	Data management includes, among others, the collection, storing, processing and mining of data. What data are collected and for which purpose? How long are the data retained and why? When should it be possible to trace data back to its origin? Who owns what data?
3	Data communication	Smart energy systems will generate a lot of data that needs to be transported over an infrastructure to the point(s) where they are used. What is the desired security level for different types of data communication?
4	Confidentiality	Confidentiality refers to limiting information access and disclosure to authorized resources and preventing access by or disclosure to unauthorized resources. The consequences of a breach are different for the different stakeholders (loss of privacy for a Prosumer, loss of goodwill, competitive disadvantage for a retailer). What are necessary and acceptable levels of confidentiality for the different parts of the system?
5	Integrity	Integrity means that data cannot be modified undetectably. Where in the smart energy system is integrity more important than availability, or more important than confidentiality?
6	Availability	Availability refers to the availability of information resources including systems, processes and data elements. What are necessary and acceptable levels of availability for the different components of a smart energy system?
7	Disaster Recovery	No (security) system is perfect. What needs to be done in the case of unforeseen situations? How to mitigate the fall-out from a security/privacy breach? How are responsibilities divided between parties?
8	Identification, Authentication, Authorization	Identification is the process of showing who you are. The identification is validated through the process of authentication, which verifies that you are who you say you are. Authorization is the process of verifying that "you are permitted to do what you are trying to do."
9	**Risk assessment**	Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat.

Figure 16. Aspects of privacy and security in smart energy systems. Source : USEF [58].

The principles are presented in the structure of Figure 17. It includes a description of the principle, the explanation behind the principle, and its possible consequences.

Principle	Each principle starts with a self-explaining name about the principle. It is provided as a short sentence stated in the imperative. Example: 'principles are stated in the imperative'. ID#
Description	In the description, an explanation of the principle is provided. It is limited to the 'what' of the principle, describing what is exactly meant, without giving the reasons. Example: 'a principle is a sentence in the imperative explaining what the principle is about. It contains at least a subject and a predicate; verbs like 'should' are prohibited.'
Rationale	The rationale is the why of the principle. It states why it is important to follow the principle, and what the relevance is of the principle (especially in a smart grid). Example: 'using the imperative indicates that using a principle is not a free choice, but a directive that must be complied with.'
Consequences	Following a principle may have consequences, either positive or negative. This section the possibility to state consequences that are foreseen. Example: 'by explicitly prescribing the format of a principle, commonly used principles might be rephrased (e.g. 'need to know' is reformulated as 'data is processed on a need to know basis').

Figure 17. Security principles patterns. Source: USEF [58].

The principles will not be detailed in this document, as the goal is to provide an overview of existing guidelines and standards.

4.5.2. Security requirements [59]

The security requirements for the energy sector are governed by the General Data Protection Regulation (GDPR). It imposes regulations on any organization which collects or processes data from EU citizens. The regulation was enforced in 2018.

It includes seven data protection principles, similar to the ones presented by USEF:

- **Lawfulness, fairness, and transparency** when processing data.
- Data processing must be **limited to legitimate purposes** known by the data subject.
- **Data** collection and processing must be **minimized** to the strict necessary.
- Personal data **accuracy** must be ensured.
- **Storage limitation** must be guaranteed.
- Data processing should ensure data security, **integrity, and confidentiality.**
- The data controller is **accountable** for GDPR compliance with the principles.

The implementation of necessary technical measures, detailed in Section 4.5.4, allows to meet the requirements. Furthermore, a data protection by design approach allows to prioritize data protection, ensuring that it becomes the baseline of all new products or activities, by considering the data protection principle.

The regulation also states the conditions in which it is legal to process personal data. It includes:

- **Unambiguous consent** from the data subject.
- Necessary processing **to enter a contract** involving the data subject.

- **Compliance with legal obligations.**
- Processing data to **save a life.**
- Conducting tasks in the **public interest**
- Processing based on **legitimate interest**. It is the most flexible lawful basis, but it must be weighed against the fundamental rights and freedoms of the data subject, particularly in the case of a child's data.

However, the GDPR principles do not address the energy sector specifically but remain applicable.

4.5.3. Security standards

The European Union Agency for Cyber Security (ENISA), and the NIS Cooperation Group Security Measures, established by the NIS Directive, are two leaders in the field of cybersecurity in the EU. They reference 3 key standards in security.

4.5.3.1. ISO/IEC 27000 [2]

ISO/IEC 27000 is a family of standards that establish a framework for information security management systems (ISMS). An ISMS is a systematic approach to managing sensitive company information so that it remains secure.

The core of the ISO/IEC 27000 family is the ISO/IEC 27001 standard, which specifies the requirements for an ISMS, on which an organization can be audited and certified.

ISO/IEC 27019 [60] is a standard that provides guidance for ISMS in the energy utility industry. It is based on ISO/IEC 27002 and covers a range of systems used in process control, monitoring, and automation technology for the production, generation, transmission, storage, and distribution of energy, including electricity. It covers communication technology, digital controllers and automation components, energy management systems, smart grid environments, software and firmware, and premises housing the equipment and systems. The standard also allows the adaptation of the ISO/IEC 27001 risk assessment and treatment processes to the specific needs of the energy utility industry.

4.5.3.2. IEC 62443 [61]

IEC 62443 is a series of standards developed to ensure the security of Industrial Automation and Control Systems (IACS) during their lifecycle. Initially drafted for the industrial process sector, IACS are now implemented in various fields and industries, including critical infrastructure like power and energy supply and distribution, and transport. Unlike IT standards, IEC 62443 is appropriate for IACS as it considers their unique performance, availability, and lifetime requirements. Implementing IEC 62443 can prevent and mitigate the impact of cyber-security breaches, hence reducing costs over the lifecycle. The standard takes a holistic approach to

cybersecurity, considering the technology in addition to the work processes, countermeasures, and employees. It is implemented with a risk-based strategy where the most valuable assets and their vulnerabilities are identified to set up the most appropriate cybersecurity measures.

4.5.3.3. NIST SP800-53 [28]

The NIST SP800-53 publication is a framework developed by the National Institute of Standards and Technology (NIST) in the United States for managing and securing information systems.

The publication provides a catalogue of security and privacy controls that organizations can use to protect their systems and data from a variety of threats and risks. It is designed to be flexible and customizable, allowing organizations to tailor their security programs to meet their specific needs and requirements. This framework also provides an assessment of the controls, including the strength, the robustness, and the reliability of the controls, in order to obtain an evaluation of the information system in place.

4.5.4. Security measures

The NIS directive tool [63] provides a list of "Minimum Security Measures for Operators of Essentials Services" with their associated standards.

ENISA also compiles a list of security measures and good practices in its report "Baseline Security Recommendations for IoT" [64]. These measures are compiled from a wide range of sources. Some key references include ISO27001, NIST publications such as SP 800-53, and NERC CIP.

4.5.4.1. Policies

Policies are intended to enhance information security and make it more robust and tangible.

- Security by design
- Privacy by design
- Asset Management.
- Risk and Threat Identification and Assessment

4.5.4.2. Organisational, People and Process measures

The way an organization manages its personnel plays a crucial role in ensuring good security practices and proper management of processes related to information safety. It is also important to hold contractors and suppliers accountable when it is applicable. The organization should also have a plan in place that clearly outlines responsibilities, evaluation, and response procedures, in the case of a security breach.

- End-of-life support
- Proven solutions

- Management of security vulnerabilities and/or incidents
- Human Resources Security Training and Awareness
- Third-Party relationships

4.5.4.3. Technical Measures

These measures are necessary to reduce the vulnerabilities of IoT. These measures should be adapted to the application architecture.

- **Hardware security:** Implementing physical security measures to protect hardware components from unauthorized access, tampering, or theft.
- **Trust and Integrity Management:** Ensuring the authenticity and integrity of hardware, software, and data.
- **Strong default security and privacy:** Implementing strong security and privacy settings by default in systems, applications, and devices to reduce the risk of attacks.
- **Data protection and compliance:** Ensuring that data is protected and managed in compliance with legal and regulatory requirements.
- **System safety:** Implementing safety controls to protect against system failures or errors that could compromise security or safety.
- **Secure Software / Firmware (patch management, malware protection):** Managing software and firmware updates to fix known vulnerabilities and protect against malware attacks.
- **Authentication:** Verifying the identity of users or devices attempting to access a system or resource.
- **Authorisation:** Granting or denying access privileges to users or devices based on their identity and the permissions they have been granted
- **Access Control - Physical and Environmental security:** Restrict accesses to authorized individuals.
- **Cryptography, Encryption:** Encode data to restrict its access to authorized parties with the corresponding decryption key.
- **Secure and trusted communications:** Ensuring that communications between systems, devices, or networks are secure and trusted using cryptographic protocols or other security measures.
- **Secure interfaces and network services:** Implementing security controls for interfaces and network services, such as firewalls, intrusion detection and prevention, network

segmentation, and vulnerability scanning, to protect against unauthorized access or attacks.

- **Secure input and output handling:** Ensuring that input and output data are securely processed to prevent data leakage, tampering, or other security risks.
- **Logging:** Capturing and storing logs of system events and user activities to aid in incident response, forensics, and compliance.
- **Monitoring and Auditing:** Monitoring systems and applications for security threats or anomalous behaviour and conducting regular audits to ensure compliance with security policies and regulations.

4.5.5. Communication protocols security measures

Protocol abbreviation	Independent security protocol	Security measures
DLMS/COSEM (IEC 62056) [65]	-	Entity authentication Role-based access Message protection Data protection Secure image transfer Communication port protection Security logs
ANSI C12.18	X	X
OSGP [66]	-	Authentication Encryption Access control
TCP/IP [67]	SSL (Secure Sockets Layer) TLS (Transport Layer Security) SSH (Secure Shell) IPSec (Internet Protocol Security)	Encryption Authentication Integrity Role-based access control Authorization
UDP/IP [68]	DTLS (Datagram Transport Layer Security) IPSec (Internet Protocol Security)	Encryption Authentication Integrity Automatic key management Security against replay attacks
MQTT [69]	SSL (Secure Sockets Layer) Servers IPSec (Internet Protocol Security)	Identity (SSL; client identifier, user ID, public digital certificate) Mutual authentication (SSL) Authorization (provided by servers)

CoAP [70]	DTLS (Datagram Transport Layer Security)	Encryption Authentication (server) Integrity Automatic key management Security against replay attacks
HTTP [71]	HTTPS - TLS (Transport Layer Security); SSL (Secure Sockets Layer)	Authentication Encryption Integrity
WebSockets	WSS - TLS (Transport Layer Security); SSL (Secure Sockets Layer)	Authentication Encryption Integrity
XMPP	SASL TLS SCRAM (Salted Challenge Response Authentication Mechanism) OTR (Off-the-Record)	Authentication Encryption Integrity
OCCP [72]	-	Secure communication Encryption Integrity Mutual authentication Firmware updates Logging Monitoring
Modbus [73] [74]	Modbus security protocol – TLS (Transport Layer Security)	Encryption Authentication Integrity Role-based access control
SHIP [75] [74]	TLS (Transport Layer Security)	Encryption Authentication Integrity
MMS (ISO 9506) [52]	-	Authentication Access control
GOOSE (IEC 61850) [76]	IEC 62351-6	Authentication (via digital signature) Integrity (via digital signature) Security against replay attacks
Zigbee [55]	AES-128 bit Symmetric cipher Message integrity check	Encryption Authentication Integrity
Matter [56] [57]	AES-128 bit	Authentication Authorization End-to-end encryption

		Integrity Access control Data minimization Firmware updates

5. Review of specific standards applicable to flexibility

In this section, we deep-dive into a subset of the standards & recommendations that are considered particularly crucial to the design and technical implementation of flexibility services.

5.1. OSGP [77]

5.1.1. Main characteristics and applications

The Open Smart Grid Protocol (OSGP) is a protocol used in smart grid systems englobing a family of specifications. It is an **open standard**, initially developed by ETSI, and currently maintained by OSGP alliance, a non-profit organization composed of energy utilities, manufacturers, and other stakeholders in the smart grid industry. It is specified by the CEN/CENELEC CLC/TS 50586.

It supports multiple communication technologies, including powerline, radio frequency, and cellular networks, making it a **flexible** protocol for smart grid systems [78] [79]. Moreover, this protocol provides **security features**, such as encryption, authentication, and access control. Therefore, it ensures the confidentiality, integrity, and availability of data transmitted over the smart grid network [78]. OSGP is a **multi-application architecture** designed to support various applications in smart grid systems, including advanced metering, and demand response. Furthermore, by enabling the communication and operability of numerous devices and systems, the protocol promotes **interoperability** within the smart grid system and improves both the efficiency and the reliability of the smart grid system, while reducing costs. In addition, it supports **remote firmware updates**, allowing the devices to easily remain updated.

Overall, OSGP provides a flexible, secure, and reliable communication protocol with a multi-application architecture for smart grid systems, ensuring interoperability for the deployment of a wide range of applications.

5.1.2. Reach and coverage

OSGP is widely used in smart grid systems around the world, in many countries, particularly in Europe and Asia. More than 5 million devices, including smart meters, implement OSGP following

their certification. However, the frequency of usage of this protocol may vary across regions and utilities due to the high number of communication protocols available for smart grid systems.

5.1.3. Technical description

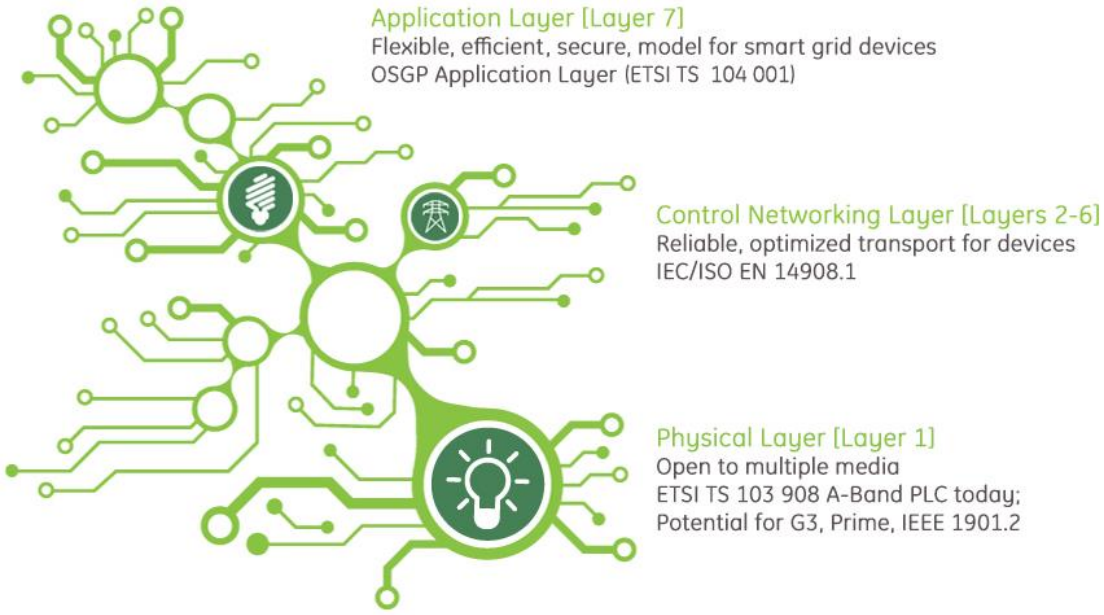

Figure 18. OSGP layers. Source: OSGP Alliance [80].

OSGP follows the separation principle from the OSI model.

5.1.3.1. Application Layer

The application layer is characterized by an efficient table-oriented data storage and command system based on ETSI TS 104 001. OSGP provides a query language that is both efficient and flexible, similar to SQL databases. It provides bandwidth efficiency by allowing the reading and writing of single attributes, multiple elements, or entire tables. Furthermore, OSGP allows any device to serve as message repeater through an adaptive and directed meshing system, hence optimizing the bandwidth use.

On the one hand, OSGP improves the energy management of users, while ensuring reliable service. On the other hand, it supports DSOs through the energy transition, which requires the increase in distributed energy resources, including renewable energy sources, and further electrification of technologies, such as electric vehicles.

5.1.3.2. Networking Layers

For the networking layer, EN14908-1 is implemented in addition to security, authentication, and encryption measures. The intermediate layer implements a control networking standard, widely

used for smart grid multi-application systems, ISO/IEC 14908. It is characterized by its efficiency, scalability, and reliability, with low bandwidth requirements.

5.1.3.3. Physical Layer

At the physical layer, OSGP can be implemented with different communication layers (power line communication, cellular, or radio frequency). In fact, the implementation of a media independent networking layer ISO/IEC 14909 grants OSGP its flexibility. For media with moderate raw data rates, it guarantees performance and reliability.

Currently, OSGP is mostly used with ETSI TS 103 908 with power line communications for cost and efficiency advantages, allowing reliable transport of packets over extended distances and unfavourable conditions. Furthermore, ETSI TS 103 908 is widely deployed on the market with more than 40 million smart meters and grid devices in operation.

5.1.4. Security [66]

5.1.4.1. Measures

OSGP also includes both authentication and encryption, as well as access control, for all exchanges to protect the integrity and privacy of data as is required in the smart grid. Given the lightweight protocol stack, the encryption is done with RC4 stream cipher, coupled to message authentication through linear digest function. Moreover, the broadcast is said to be secure. Furthermore, the protocol uses session keys or encryption deriving from a single principal key for authentication.

5.1.4.2. Limitations

However, these security measures have some limitations. The encryption is not part of the NIST recommended cryptographic primitives (AES), and the digest function is non-standard. This combination facilitates cryptographic keys and messages attacks. Moreover, the broadcast security is undefined, and does not provide any clear measures on source authentication. Since the broadcast is used to send firmware updates, it can be the source of security breaches. Finally, the session keys can be accessed by compromising the main authentication key, which is used with a weak algorithm.

5.2. DLMS/COSEM [81]

5.2.1. Main characteristics

DLMS/COSEM (Device Language Message Specification/Companion Specification for Energy Metering) is a standard protocol for data exchange between smart meters and data concentrators. It targets smart management and advanced control of energy (electricity, gas, heat) and water. It is developed and promoted by the DLMS User Association, a non-profit organization, which has over 300 members from more than 60 countries, including

manufacturers, utilities, system integrators, and other stakeholders from the energy management industry.

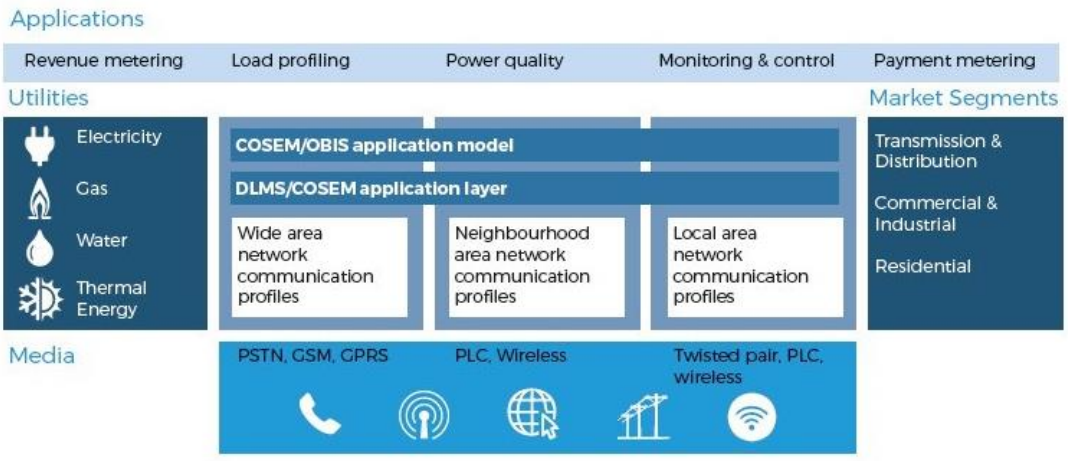

Figure 19. DLMS/COSEM overview. Source: DLMS User Association [81].

The main advantage of this protocol is its **interoperability**. The protocol is internationally recognized and has increasingly been adopted by numerous manufacturers and device types. The protocol is **flexible** with respect to communication methods, data types and data structures. In fact, it is compatible with multiple communication technologies as it is designed to be end-to-end, application-to-application. The object identification system allows to adapt to a wide range of applications. On the application layer level, the protocol can be customized to meet specific requirements based on the application of interest by implementing custom methods, procedures, and data objects. Finally, DLMS/COSEM provides security features, including authentication, encryption, and access control to prevent unauthorized access and tampering.

5.2.2. Reach and coverage

DLMS/COSEM has been recognized globally as a standard for data exchange for smart devices since 2002 in the IEC / EN 62056 and the EN 13757 standard suites. It is widely implemented internationally. It is in fact implemented in over 60 countries, with more than 150 vendors, and covers over 1500 certified device types for various applications.

5.2.3. Technical description

5.2.3.1. Components

The DLMS/COSEM has three principal components.

COSEM – Companion Specification for Energy Metering

The COSEM or Companion Specification for Energy Metering model defines a set of standardized data objects, with a given set of attributes and methods, which enable interoperability and compatibility between different devices from different manufacturers.

The COSEM model includes a wide range of data objects, covering all functions of the meter, independently of the supported functions, their implementation, and the data transportation. Each data object is represented by a unique object identification system (OBIS) code, independent of the manufacturer, which enables clients to identify and access the data objects on the server.

COSEM also defines a set of standardized services that enable clients to interact with the data objects, based on the specific access rights granted, such as reading, writing, and executing data.

OBIS – Object Identification System

OBIS (Object Identification System) is a standardized system that uniquely identifies and describes the data objects used in electricity, gas, water, and thermal metering, as well as abstract data. OBIS identifies the attributes of the data objects in a hierarchical structure, starting with a high-level category and ending with a specific instance of the object, hence allowing a proper classification of the data characteristics.

DLMS – Device Language Message Specification

The DLMS or Device Language Message Specification protocol defines the structure and format of messages communicated across devices, such as data objects, methods, and services. It specifies the protocol for exchanging and accessing data stored in the COSEM model, therefore promoting interoperability by allowing communication between devices from different manufacturers. The DLMS protocol supports various communication technologies, including wired and wireless communication.

5.2.3.2. Communication model

In the DLMS/COSEM protocol, end devices, such as meters, act as servers, while Head End Systems or concentrators serve as clients. The DLMS/COSEM application layer offers ACSE services to establish connections between clients and servers, and xDLMS services to access data stored in COSEM objects following an Application Association (AA).

5.2.3.3. Application layer

The services available are the same across all objects, therefore allowing the integration of new objects independently of the application layer. In fact, the protocol can be customized to meet specific requirements based on the application of interest, allowing the implementation of COSEM objects of interest, and determining which xDLMS features are to be used.

Additionally, the application layer constructs ADPUs (Application Protocol Data Units) messages, while applying and verifying cryptographic protection, and supports the transfer of long messages in blocks. The protocol can be used over various communication media, with optimization mechanisms available to tailor traffic to media characteristics.

5.2.3.4. Transport layer

The DLMS/COSEM protocol supports several communication profiles (set of protocol layers).

5.2.4. Security [65]

DLMS implements numerous security measures in order to guarantee confidentiality, integrity, and the availability of information and services.

5.2.4.1. Measures

DLMS implements various security mechanisms. These mechanisms are multi-faceted, end-to-end and application-to-application, allowing to protect messages and data regardless of the transport media.

- **Entity authentication:** A client and the server need to be mutually authenticated to establish a connection and exchange messages. This is done by exchanging arbitrary challenges to be processed cryptographically, followed by the outcomes of the challenges.
- **Role-based access:** It is possible to increase or restrict the extent of the access rights (read, write) to COSEM objects depending on the role of an entity.
- **Message protection:** The messages communicated are protected by encoding the service primitives. Three superimposable message protection layers (encryption, authentication, digital signature) are available for the COSEM object attributes and methods. They ensure that data can only be accessed by protected messages.
- **Data protection:** The data carried by the message is additionally protected, independently from the previous mechanism, in particular when sensitive data is exchanged, or multiple parties are involved. The encryption is done through intermediate data protection or protected buffer objects with the necessary security measures.
- **Secure image transfer:** It is possible to deploy firmware upgrades through an image transfer mechanism, where the protection is ensured while verifying the image.
- **Communication port protection:** In the case of suspicious traffic, the communication port is temporarily disabled to mitigate the risk of replay and brute force attacks.
- **Security logs:** Security logs are stored by profile generic objects, to track possible breaches.

Three possible authentication layers are possible (no security, low level security, high-level security) [82].

These security services are ensured through several algorithms. Confidentiality and data integrity is guaranteed by the AES-GCM algorithm (encryption only, authentication only, or authenticated encryption). The digital signature is managed by ECDSA elliptic curve digital signature algorithm, coupled with hash algorithms. The Key Wrap algorithm manages key transport while the ECDH elliptic curve Diffie-Hellman Key Agreement algorithms handle key agreement in addition to hash algorithms. The efficiency is preserved by compressing the transferred messages' length.

5.2.4.2. Limitations [82]

Some vulnerabilities are still apparent despite all the security measures.

At the transport layer, the security can be compromised through message replacement, stream cipher, and authentication downgrade attacks. Some other apparent weaknesses at the transport layer are the weak randomization at the encryption key, and the short authentication tag.

On the other hand, the authentication security is threatened by information leakage, one challenge authentication, or parallel session authentication. In particular, the low-level security is exposed to secret disclosure, and brute force attack, while the high-level security can be compromised by an offline brute force attack.

5.3. EEBus

5.3.1. Main characteristics

EEBus is developed by the EEBus initiative, founded in 2012 by Germany's Federal Ministry of Economics. EEBus is an open, two-way information model designed to facilitate information exchange between:

1. Demand response (DR)/distributed energy resources (DER)/smart devices and a gateway device/energy management system
2. Between the gateway/energy management system and other energy system actors. It also covers "grid interactions".

5.3.2.Reach and coverage

The industry alliance has about 60 partner companies including Bosch and Siemens. The number of commercially available devices compatible with EEBus is limited, with providers concentrated around Germany.

5.3.3. Technical description

The EEBus architecture contains an 'information layer' (Specification Smart Premises Interoperable Neutral Message Exchange – SPINE) and a 'communication layer' (Smart Home IP – SHIP), following the separation principles of the Smart Grid Architecture Model. The ontology underpinning the EEBus data model is compatible with SAREF4ENER, as SAREF4ENER was built on top of the EEBus architecture. EEBus has also published a set of use case documents with fully described examples (messages, sequence diagrams, etc.).

The SPINE protocol defines the information layer proposed in EEBus. It is defined in the SPINE protocol V1.1.1 documentation and CENELEC EN 50631-1, which contains an introduction, a protocol specification document, and a resource specification document. SPINE defines a neutral layer which helps connecting different communications technologies to build a smart home / smart grid system. It only defines messages and procedures on application level (OSI layer 7) and is therefore independent from the used transport protocol. Any technology that supports the bi-directional exchange of arbitrary data can in principle be used for SPINE, but the SHIP communication protocol was specifically designed to be used with SPINE. The SPINE protocol relies on XML-format messages that follow a specific form defined in XML schema definition files (.xsd files).

Advantages

- The initiative is supported by industry actors and therefore specific equipment are using the SPINE protocol out-of-the-box.
- The protocol specification defines high-level functions such as device discovery that are useful to automate some aspects of the applications.

Drawbacks

- Although the industry alliance has about 60 partner companies including Bosch and Siemens, the number of commercially available EEBus-compatible devices is not so large, and the providers tend to be centred around Germany.
- The architecture is rich but somewhat complex, and therefore not straightforward to use.
- There is a lack of reference implementations for the EEBus protocol suite. As of writing this report, the ones that have been found are:
    - Third-party implementation in Go: https://github.com/enbility/eebus-go
    - Partial reference implementation in .NET framework (only SHIP at the moment, not SPINE): https://github.com/barnstee/EEBUS.Net

5.3.4. Security

In theory, any transport protocol can be paired with EEBus, however an IP approach with SHIP has been selected for its cybersecurity advantages. EEBus implements the standard security mechanism TLS (Transport Layer Security) [75] which guarantees end-to-end encryption, authentication, and data integrity [74]. The TLS coupled with elliptic curves hence ensure a secure communication.

5.4. Zigbee and Smart Energy

5.4.1. Main characteristics

5.4.1.1. Zigbee [83]

Zigbee is an open-standard solution for a two-way wireless communication protocol. The protocol was developed by the Connectivity Standard Alliance (CSA), formerly known as the Zigbee Alliance, which is a non-profit association of companies and organizations promoting this technology. It is typically used in home, building, and industrial automation; hence serving residential, commercial, industrial, energy and utilities markets.

Zigbee provides a self-organizing, self-healing mesh topology, scalable up to thousands of nodes, which increases the network's reliability and stability. Moreover, it is suitable for low-power and ultra-low power consumption, hence extending battery life. In fact, it exploits ultra-low power RF silicon with energy harvesting features. Zigbee provides Zigbee Direct allowing to integrate Zigbee and Bluetooth Low Energy technologies. It also provides the variant Zigbee PRO, with enhanced security measures. Finally, Zigbee can be coupled with Smart Energy.

5.4.1.2. Smart Energy [84]

Smart Energy is a standard protocol, developed by CSA, dedicated to smart energy applications. This includes the monitoring, control, and automation of multiple resources consumption, such as energy, water, and gas. It is suited for the same markets as Zigbee. It is useful for diverse applications, such as metering, demand response and load control, and pricing. Hence, it is relevant to reduce energy consumption and the environmental impact.

5.4.2. Reach and coverage

Zigbee is a widely adopted open-standard solution, which has been implemented in over 500 million chipsets worldwide. It is backed by the CSA, which includes over 400 international companies, such as Apple, Amazon, Schneider Electric, Ikea, etc. Smart energy has been deployed in 40 million electric meters in the US, it has been selected as the standard in the UK and has been implemented in millions of meters in France.

5.4.3. Technical description

The Zigbee protocol is a wireless communication protocol that operates on the IEEE 802.15.4 standard [10]. It is designed for low-power communication in IoT devices. The protocol is built on a mesh network topology, ensuring reliability, and robustness.

The protocol has 4 main layers.

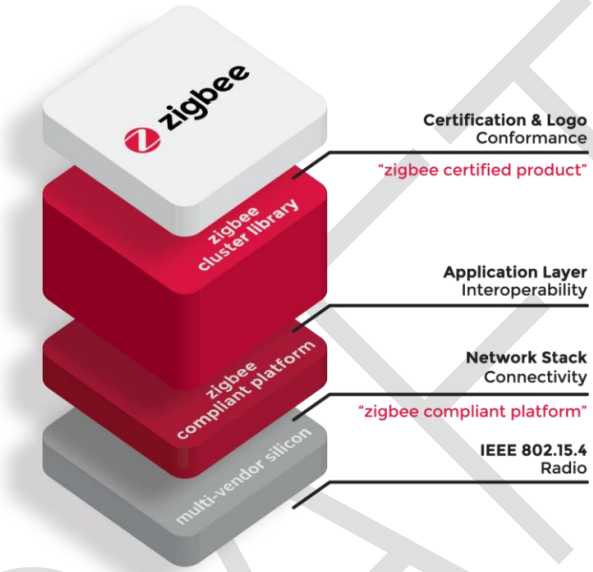

Figure 20. Zigbee protocol stack. Source: CSA [86].

Physical layer

The physical layer (PHY) is responsible for defining the characteristics of the radio waves used in the Zigbee protocol. This includes the modulation, data rate, and channel frequency. Zigbee is based on the IEEE 802.15.4 physical radio standard and operates in unlicensed bands. It supports four physical radio standards globally, operating at 2.4GHz, as well as 915Mhz (in the Americas) and 868Mhz (in Europe).

Data layer

The data layer or Media Access Control (MAC) layer is also defined by the IEEE 802.15.4 standard. The MAC is in charge of managing access to the radio channel and implements either a Carrier sense multiple access – collision avoidance (CSMA-CA) or Listen Before Talk (LBT) mechanism,

[10] "The physical layer (PHY) and medium access control (MAC) sublayer specifications for low-data-rate wireless connectivity with fixed, portable, and moving devices with no battery or very limited battery consumption requirements are defined in this standard." [85]

depending on the MAC/PHY used. It's also responsible for tasks such as transmitting beacon frames, synchronization, and ensuring the reliability of the transmission.

Network layer

The network layer in Zigbee protocol supports three types of topologies - star, tree, and mesh. In a star topology, a single device called the Zigbee coordinator manages the network and communicates directly with end devices. In mesh and tree topologies, the Zigbee coordinator initiates the network and selects key parameters, but routers are used to extend the network. In tree networks, routers follow a hierarchical routing strategy to move data and control messages. In this case, beacon-oriented communication, specified in IEEE 802.15.4, is implemented. In mesh networks, full peer-to-peer communication is supported, but ZigBee routers do not emit regular IEEE 802.15.4 beacons. The ZigBee protocol only specifies intra-PAN networks, which are networks that begin and terminate within the same network, except for the inter-PAN feature which enables the ZigBee stack to be bypassed for out-of-band initialization of network settings.

Application layer

The application layer includes the application support sub-layer (APS), the Zigbee Device Objects (ZDO), and the manufacturer-defined application objects.

The APS is responsible for connecting the network and application layers. It consists of a data entity, which is responsible for the data transmission services between two applications on the same network. It also has a management entity, which provides several services to application objects, and stores them in a database.

The application framework supports up to 254 application objects, identified by their endpoint address. Developers can create interoperable applications through agreements called application profiles.

The ZDO serve as a bridge connecting the application objects, device profile, and the APS through a base class of functionality. It connects the application framework and the APS. It provides various functions such as initializing the APS, NWK, and Security Service Provider, gathering configuration information from end applications for discovery, security management, network management, and binding management. The ZDO also provides public interfaces for the application objects to control device and network functions. The ZDO manages address management, discovery, binding, and security functions in the application framework layer.

Overall, the application layer of the Zigbee protocol is responsible for defining the behaviour and functionality of Zigbee devices in specific applications and for ensuring interoperability between different devices.

Smart Energy Standard

The Smart Energy Standard is an application profile built on top of Zigbee, specifically for smart energy applications.

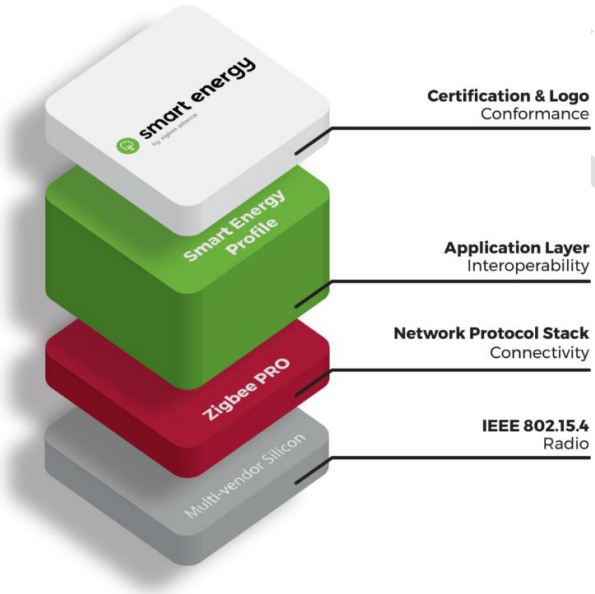

Figure 21. Smart Energy protocol stack. Source: CSA [87].

5.4.4. Security [88]

5.4.4.1. Measures

Zigbee was designed to be secure and has various security measures in place.

The built-in security features of Zigbee use AES 128-bit encryption to guarantee communication between nodes is secure. These features include key establishment, key transport, frame protection, and device management. Security in Zigbee is simple, direct, and end-to-end. Each layer secures frames, and nodes exchange keys directly, so data is transmitted without intermediary decryption and encryption. The AES algorithm ensures message integrity, confidentiality, and authentication. However, the encryption is simplified by keeping the same key at each layer.

To maintain data privacy and integrity, Zigbee uses a symmetric cipher and message integrity check. It also prevents forwarding attacks by using sequential freshness counter of frames order. Authentication is maintained in the NWK and APS layers through the active network and link keys, respectively. This allows information to be synchronized between devices while providing authenticity. Zigbee provides a trust centre to manage new devices and update network shared keys regularly.

Zigbee uses master, network, and link keys, each with different security functions. The NWK layer ensures secure frame transmission, and the APS layer securely establishes and manages cryptographic keys.

5.4.4.2. Limitations

The Zigbee standard has undergone numerous improvements to ensure its efficiency and security since its initial release in 2004. However, because of its low computing power, it is vulnerable to network attacks, such as sniffing the network key that is transmitted in plaintext.

The attacks on Zigbee can range from eavesdropping the radio channel to adding a malicious node to overwrite the memory of a normal node or replaying old packed. They can be split into three main categories: layers attacks, method attacks, and target attacks.

Layers attacks

- Transport Layer Attacks: Flooding and de-synchronization attacks.
- Network Layer Attacks: Wormholes and selective forwarding attacks.
- MAC Layer Attacks: Link layer jamming.
- Physical Layer Attacks: Jamming to eavesdrop or tamper with data packet frames.

Method attacks

- Active Attacks: Intercepting and modifying data or injecting fault data frames.
- Passive Attacks: Monitoring data traffic without affecting its integrity but compromising its confidentiality.

Target attacks

- Sink Attacks: Malicious node announces shortest path to attract network traffic, usually combined with wormhole attack.
- Source Attacks: Compromising one legitimate node to act as black hole node, selectively dropping, or not receiving packets to trick other nodes.
- Neighbour Attacks: Sending HELLO message with high transmission power to trick receiving nodes into considering malicious node as a neighbour, leading to wasted energy and congestion.
- Member Attacks: Outcast attacks where the attacker node is a member of the network, insider attacks where a malicious node is a member of the network either by compromising the network or providing a fake profile.
- Energy Depletion Attack (Ghost Attack): Sending fake messages to deplete a node's energy intentionally to launch DoS and reply attacks.

5.5. Matter

5.5.1. Main characteristics [56] [89]

Matter is an open-source protocol developed by the CSA for smart home devices. It is based on contributions from well-established smart home devices, developed by the likes of Amazon, Apple, and Google, to promote the protocol's development and its benefits. Some of the smart home devices supported are lighting, thermostats, safety, and security sensors.

The Matter protocol is IP-based and will enable device manufacturers to build devices that can work with various smart home and voice services, including Alexa, Siri, and Assistant, hence promoting interoperability.

5.5.2. Reach and coverage [57]

Matter devices are interoperable with existing smart home, as many platforms and devices brands are committed to upgrading their technologies, including Apple, Amazon, and Google. In fact, CSA is rolling out millions of Matter devices through software updates.

5.5.3. Technical description [56]

The Matter protocol specifies the application layer and various link layers to ensure interoperability. The Matter protocol is coupled with widely used existing technologies. In fact, it is based on the universal IPv6 communication protocol. The first version of the Matter protocol runs on Wi-Fi, Thread, and Ethernet network layers and uses Bluetooth Low Energy for commissioning.

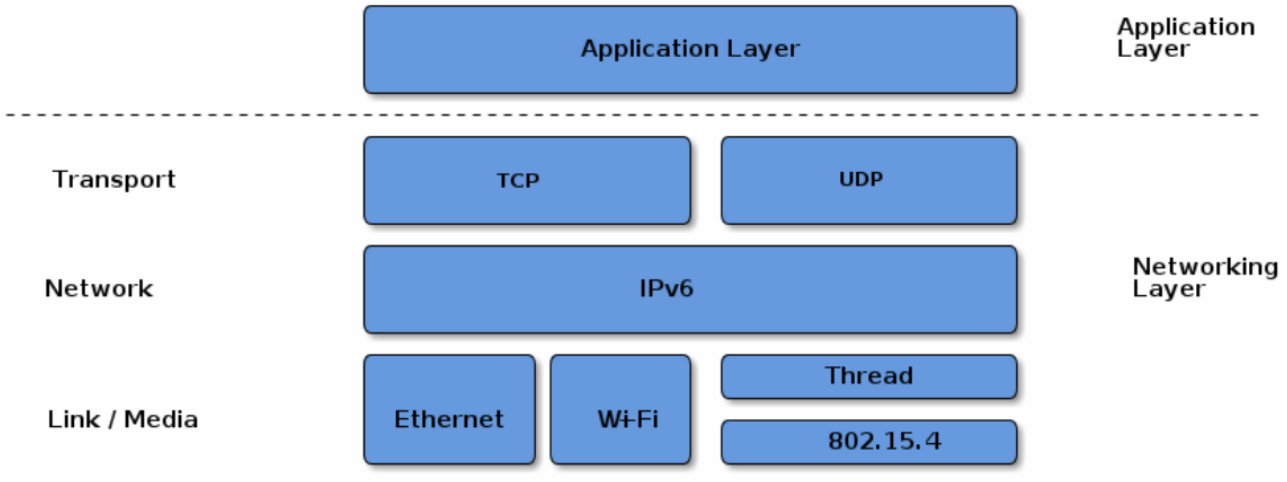

Figure 22. Network and application stack. Source: CSA [56].

Furthermore, Matter supports bridges enabling the use of other protocols, such as Zigbee, and Z-wave.

5.5.4. Security [90]

Matter implements a layered approach for security, through authentication, commissioning attestation, message protection through end-to-end encryption, and over-the-air firmware updates. The security measures provided by Matter are self-contained, and do not rely on the security of the layers under Matter. In fact, these measures are part of the core specification of Matter, such as no additional security features are required.

Matter implements standard and well-established cryptographic primitives.

- AES-128 bits in CCM mode for confidentiality and integrity.
- AES in CTR mode for identifier protection, hence for their privacy protection.
- SHA-256 for integrity.
- ECC with "secp256r1" curve for digital signatures and key exchanges, standard key derivation schemes and truly random number generators.

Furthermore, Matter adopts a modular design in order to easily adapt to new cryptographic primitives. Moreover, secure sessions for onboarding, attestation, and operation are established with standard passcode-base session, and certificate-base protocols. This is coupled with a strict device attestation concept, going through the Distributed Compliance Ledger technology to validate the certification of Matter devices.

Given all the measures in place, the data exchanged between Matter devices have their confidentiality and integrity preserved. In addition, the protocol follows the data minimization principle, therefore reducing the impact of a potential breach.

Finally, device manufacturers are free to choose their platform security according to their device's use case and risk analysis. However, it should not compromise the usability and functionality of Matter devices.

6. Potential role of blockchain for flexibility applications

This section provides a brief overview of the most important blockchain based solutions in power/flexibility management. A review of blockchains used in European projects and commercial projects in the field of energy and flexibility is also presented.

Potential use cases in the field:

1. Blockchain used directly in flexibility/balancing trading.

2. Blockchain used in (smart)contracting, accounting, money transfer.

6.1. Brief overview on blockchain technology

The advancing digitalisation of the European energy system for the "Fit for 55" Package [3] and ultimately the achievement of the European Green Deal goal of net-zero carbons emissions by 2050, calls for decentralized, safe and energy efficient solutions for the energy flexibility markets. In 2021 the European Commission published a vision for digital transformation by 2030 [91] where blockchains are recognized, and where it is stated that they need to follow the European values and ideals regarding the legal and regulatory framework.

EC wants to support the "gold standard" for blockchain technologies [92] in Europe that includes:

- **Environmental sustainability:** Sustainable and energy efficient.
- **Data protection:** Compatible where possible with Europe's strong data protection and privacy regulations.
- **Digital Identity:** Needs to respect and enhance evolving Digital Identity framework. This includes being compatible with e-signature regulations, such as electronic Identification, Authentication and Trust Services (eIDAS), and supporting a sensible, pragmatic decentralised and self-sovereign identity network.
- **Cybersecurity:** High levels of cybersecurity.
- **Interoperability:** Required interoperability among blockchains and legacy systems in the outside world.

Following these guidelines, the blockchain technology can be utilized in many sectors of the economy and industry. However, a careful review of this technology is required to effectively apply it [93].

Blockchain defined by IBM: "*Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved*" [94]. Whereas cryptocurrency is a digital currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority. Cryptocurrency is a digital payment system that doesn't rely on banks to verify transactions. It's a peer-to-peer system that can enable anyone anywhere to send and receive payments. Instead of being physical money carried around and exchanged in the real world, cryptocurrency payments exist purely as digital entries to an online database describing specific transactions. When we transfer cryptocurrency funds, the transactions are recorded in a public ledger. Cryptocurrency is stored in digital wallets [95].

The most revolutionizing aspect of the blockchain technology is the ability to create trust between parties without third-party authority through collective trust of recording information on a transparent and permanent record. This record is a blockchain, where data is recorded and synchronized in “chains” using a cryptographic technique enabling data consistency, integrity, and immutability. Blockchain data structure is presented in Figure 23. Transactions or information are submitted to the blockchain network and are transmitted to all nodes or participants over this peer-to-peer (P2P) network. Information is then validated and stored in the blocks and shared to all participants in this network [96]. Additionally, data of the transaction is stored by all participants of the blockchain, and the state of the system can be independently calculated. Decentralization of the blockchain allows more robust and secure system by “eliminating” the risk of having centralized system for trust. We must however look into the new risks emerging from this system.

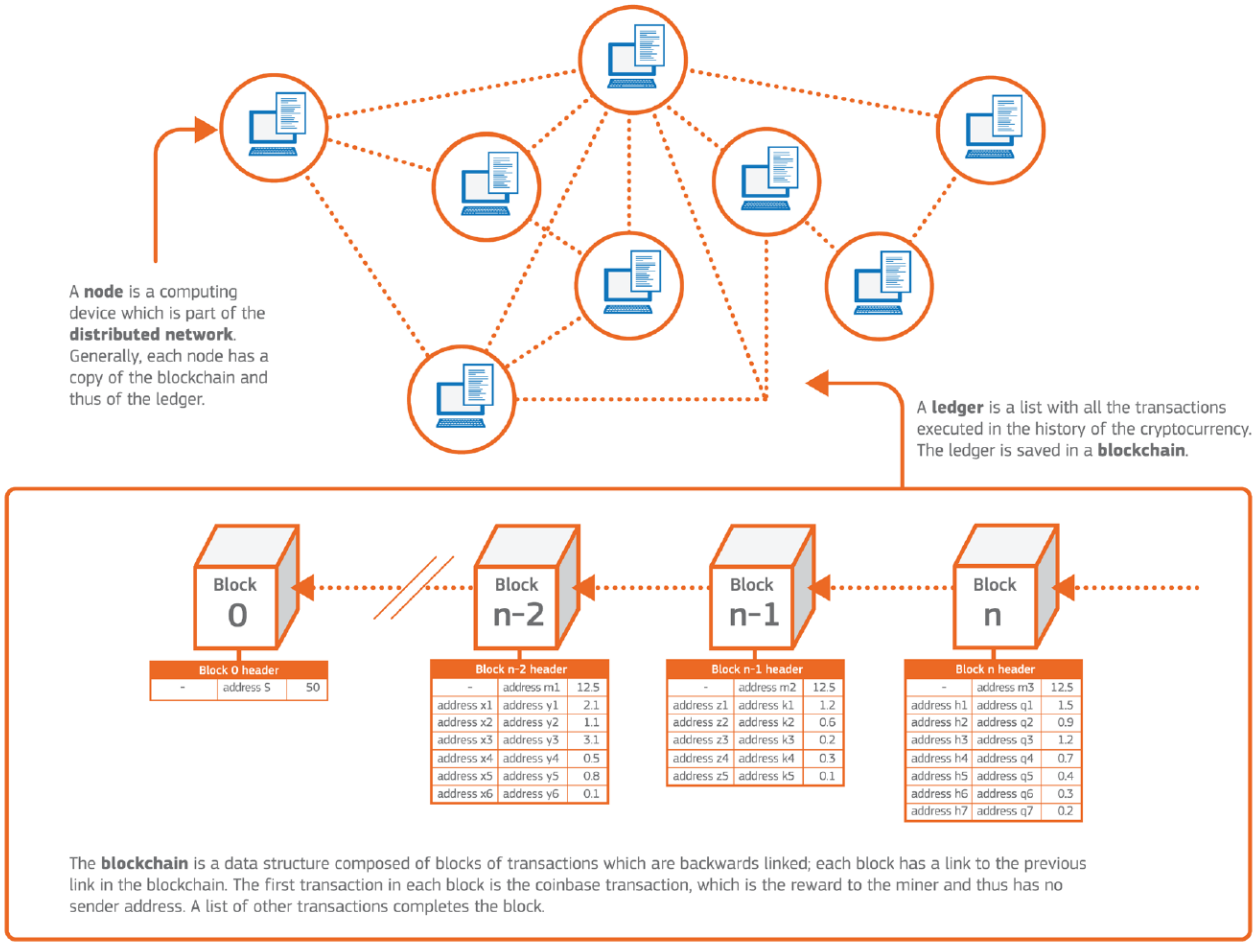

Figure 23. Use case presentation of blockchain in cryptocurrency. Source EC [93]

As long as one user is active on the chain, the system can resume from the latest state, thus creating a stable system. Depending on the use case, the blockchains can be public or private. In public chains, anyone can access, read or fetch the contents of the system. This can also be

restricted to only allow users with authorization. Decision on which one to use requires careful consideration on the needs of the use case.

Consensus Mechanisms

One of the most critical aspects of the blockchain technologies is the verification mechanism or consensus mechanism. It is the method through which the system agrees on which transactions are valid and are added to the "chain" or the ledger. The consensus mechanisms are used to verify the honesty of the users or entities. The "Proof of X" methods are varying and have usually specific purposes due to their possible constraints in one of three areas [4]:

1. Decentralization
2. Scalability
3. Security

For these reasons, it is important to acknowledge the strengths and weaknesses of the consensus mechanisms of the different distributed ledger technologies (blockchains).

Table 9. Two mostly used consensus mechanisms and IOTA's DAG

Proof of Work (PoW) [97],[98]	Networks participants are required to solve complex "cryptographic puzzles" to add new blocks to the blockchain. Since these "puzzles" are processing all the information of the previously recorded chain, the generation of the new block becomes larger and more energy consuming over time. This method ensures that decentralization is rewarded, and that the system is not being misused. This creates a form of "trust" in the system between unknown parties and makes it a highly immutable and secure method.
Proof of Stake (PoS) [97], [99]	In this system, the node of the network must provide a proof (set a "stake") by providing a certain amount of cryptocurrency if they want to participate in the validation of transactions. In case of misuse of data, they may lose some of or all the stakes. Unlike proof of work, this method does not require large amounts of energy for validation but possesses a risk from parties that own large amount of cryptocurrency to influence the validation.
Directed Acyclic Graph (DAG) [100], [101]	Instead of having "chains" or series of blocks of data, the DAG utilizes a Tangle protocol. It creates a net of transactions which allows for parallel validation (Figure 24). To validate a transaction, it has to be confirmed by the previous two connected nodes. This allows for very fast processing times with low transaction fees and lightweight programs. On the downside, the attacker requires only 34 % of hashing power instead of 51% as in PoW, meaning that it is more vulnerable to attacks.

There are many more other consensus mechanisms introduced to the markets with new ones being made and previous ones expanded upon. This was a light overview on the topic.

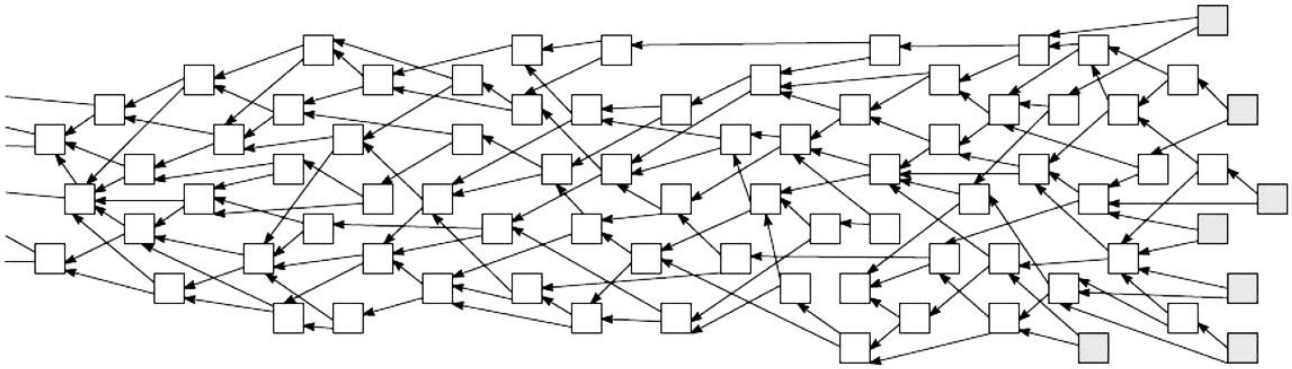

Figure 24. Tangle protocol example image [101]

6.1.1. Blockchains or Distributed ledger technologies in enabling low-cost flexibility trading

Blockchains or distributed ledger technologies (DLT) have been looking for their places in mainstream technological use cases and their reputation is not the highest among populace due to their infame in “stock trading” cases. In case of GLocalFlex project, we want to test them in order to allow low-cost flexibility trading.

In regards of flexibility trading, DLTs possess multiple preferred features such as:

- Low-transaction costs
- Transparency with privacy
- Decentralized validation
- Security

As we strive towards more sustainable energy systems in Europe, the possibilities to utilize DLTs effectively need to be studied. There are numerous cases already in Europe that are investigating these possibilities, as discussed in the next chapter 6.2. IOTA’s DLT was initially chosen for GLocalFlex’s energy platforms legacy project (FlexiMar) due to its efficiency to handle fast large number of transactions through its DAG protocol. Unlike in the proof of work consensus mechanism, the DAG does not require computational power for hash algorithms, meaning that the energy requirements are lower and the transactions per seconds (TPS) are much higher [102]. Additionally, IOTA supports the use of smart contracts as well as Decentralized Identities / Self-Sovereign Identities (SSI) [103], [104]. During the GLocalFlex project, the feasibility of using DLT will be analysed through implementations.

6.1.2. DLT used with Decentralized Identity

Decentralized Identity (DID) [105] is a new type of identity format based on self-sovereign identity (SSI) concept, which states that users are in control of their own identity [106] and do not depend on centralized verification entity such as governmental identity provider, big tech or certified authorities This enables a cost-effective identification of flexibility providers. DIDs have documentation that will provide means on how to use that specific DID [107]. Document will need to contain three things minimum:

- minimum proof purposes
- verification methods
- service endpoints

Proof purposes and verification methods function together for proving purposes such as purpose of verification. These can be specified to be cryptographic public key or pseudonymous biometric protocol as a verification method to verify a proof for authentication. Service endpoints allow trusted interface to work with the DID controller.

Since the DIDs are not linked to any attributes of the user they need to be coupled with Verifiable Claims (VC). DID itself is only the "identity of the user" and does not contain other information and thus allows the user to be in control what information is provided for the third parties. VC is the subject that will be shared with the third party while providing the verification that the DID is indeed the owner of the said subject. For example, VC can be an age of the user or certificate from school or governmental body. The issuer of VC for the DID needs to be trusted or a certified party to be able to link the VC for the DID. Third party can verify both DID and VC legitimacy through cryptographic methods e.g., such as DAG or other DLT. With this, the user can specify what attributes or pieces of information are provided to the third parties. This will enable more secure privacy and personal data protection.

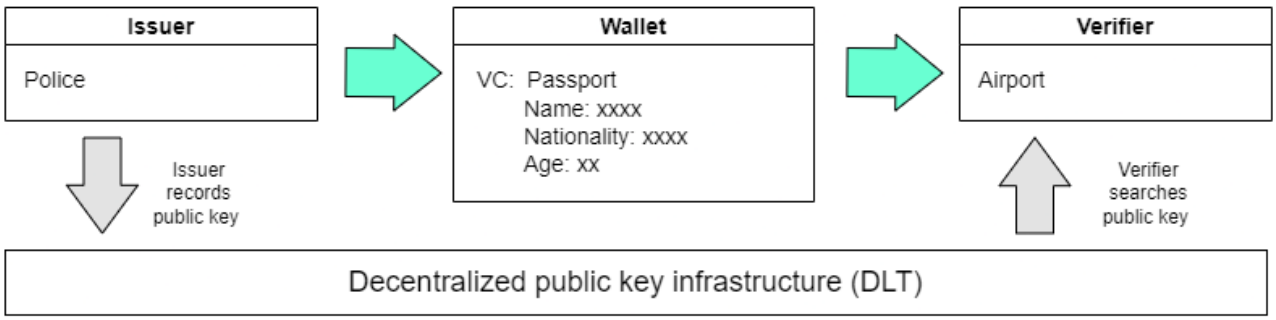

Figure 25 Example of DID in use (based on [108]).

Example of using the DID is presented in Figure 25. Issuer entity (police e.g.) will issue a credentials (verifiable credential) for the holder of the DID wallet (passport in this example) that contains some attributes such as name, nationality, or age. Verifier that is requesting information from the DID

wallet owner can verify the authenticity of entity of the VC by accessing the decentralized public key infrastructure where issuer has recorded that this VC indeed was issued for the owner of this DID wallet.

In GLocalFlex project, the VC can be "reputation of user" as a buyer and/or seller of flexibility and the issuer can be the entity the user is trading flexibility with, or the marketplace can itself be an issuer of VC. This topic will be returned in work package 4 of the project where flexibility trading platform will be developed.

European Commission rolled out a regulation "eIDAS" in 2014 in order to have standards for electronic identification and trust services. The eIDAS , quote[109],:

- "*ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services available online in other EU countries*"
- "*creates a European internal market for trust services by ensuring that they will work across borders and have the same legal status as their traditional paper-based equivalents*."

EC is currently developing the next step of electric identification. Proposal "eIDAS 2.0" will aim to extend the online identification to physical services [5]. It is built on top of existing eIDAS framework and aims for digital identity credentials (European Digital Identity – EUDI). The proposal suggests use of Self-sovereign identity approach to digital identity that gives individuals control over the information they use to prove who they are to websites, services, and applications across the web. This will be European Digital Identity Wallet that will contain core identity from the governmental eID [110].

During the project a close look into the standards will be done in order to be ready for the new eIDAS 2.0 regulation that is scheduled to be launched in 2024 [111]. Studying and possible application of standards from OpenID Foundation [112] such as OpenID VC and VCI for "Verifiable Presentation" and "Verifiable Credential Issuance" will be included in project activities.

6.2. Cases of blockchain used directly in flexibility trading

6.2.1. Energy Web's solution for Grid Flexibility from Distributed Energy Resources

DERs can participate in markets if the grid operators can "see" and trust what the DER resources are, where they are, and whether they perform when requested upon. Solving these challenges can then allow grid operators, utilities, and regulators to incorporate DERs into flexibility markets. More practically, a solution that supports DER integration provides several benefits for grid operators:

1. Situational awareness of DER capacity and expected performance forecast.

2. Secure communication with DERs directly or through the aggregator to coordinate their activity.
3. Simplified prosumer and device onboarding participation in flexibility markets.

Energy Web Decentralized Operating System (EW-DOS), by a worldwide consortium of companies, provides decentralized identity and access management (IAM) and messaging protocols so that grid operators can identify, and coordinate grid flexibility services provided by the flexibility service providers (e.g., consumers, aggregators, DERs, renewable energy communities. EW-DOS is an open-source blockchain-based, multi-layer digital infrastructure. Their mission is to develop and deploy an open and decentralized digital operating system for the energy sector in support of a low-carbon, customer-centric energy future. Below are three broad applications of EW-DOS in scaling access to grid flexibility and applied industry use cases.

- **Application 1 - Prosumer Coordination:** In the current grid architecture, service operators at various levels of energy transmission, distribution, and aggregation do not have an open method for collectively identifying and orchestrating DERs.
- **Application 2 - Demand Flexibility:** Grid operators employ a variety of strategies to ensure that the grid operates reliably in times of extreme stress. One of these tools is demand flexibility: rather than treating electricity demand as fixed at any given time and adjusting supply to meet it, grid operators increasingly try to adjust demand as well. Without a system of shared identity for customers and resources, it is difficult for grid operators to know which customers and resources will be participating in grid flexibility programs and at what scale. This makes it difficult to forecast how effective demand-flexibility will be in balancing the grid supply.
- **Application 3 - Application and IoT Management:** Distributed grid assets such as residential batteries and PV inverters do not have unique identifiers that comply with an open, shared protocol. This makes it challenging to define these assets' life cycle and performance. Such insights should be kept for the consumers, possibly the manufacturers, or company operating and maintaining the equipment for the consumer.

More info: Scaling Access to Grid Flexibility - Energy Web Digital Infrastructure (gitbook.io)

6.2.2. Power Ledger's solution for Grid Flexibility

Power Ledger's Marketplace for Optimisation of Distributed Energy (MODE) is a marketplace, which enables DER owners and flexible loads to provide grid services to monetise their assets.

Their platform MODE Flex is a marketplace for the new energy system. MODE Flex is a forward-facing smart trading platform that enables market, system, and network operators to procure flexibility services at competitive prices taking grid needs into account. This platform is blockchain enabled - making it different to any existing marketplace. The blockchain is used to execute and verify flexibilities and energy services.

More info: MODE Flex (powerledger.io)

6.3. Relevant blockchain related developments for GLocalFlex

The following table summarizes various interesting initiatives, platforms and projects that are relevant for GLocalFlex. The purpose of the table is to point towards potential information sources, benchmarks and ongoing development.

Table 10. Relevant blockchain related developments for GLocalFlex

Regulation and recommendations remarks	Relevance to GLocalFlex
A pan-European regulatory sandbox by the EC and the European Blockchain Partnership; data spaces, smart contracts, digital identity, smart energy [113]	After the GLocalFlex project, such a sandbox could allow further piloting and promoting GLocalFlex solutions on a path towards real-life deployment.
Recommendations by Joint Research Centre (EC's science and knowledge service) towards blockchain deployment for energy transition [93]	GLocalFlex contributes towards data hubs/platforms, marketplace, market rules
Research projects	**Relevance to GLocalFlex**
Parity EU project [114]: Flexibility market platform based on blockchain and IoT paves the way for smart energy grids Pro-sumer AwaRe, Transactive Markets for Valorization of Distributed flexibilITY enabled by Smart Energy Contracts | PARITY Project | Fact Sheet | H2020 | CORDIS | European Commission (europa.eu) Parity H2020 – Parity H2020 (parity-h2020.eu)	The EU-funded PARITY project is working on a local flexibility market platform that seamlessly integrates IoT and blockchain technologies. The solution also includes active network management tools to address the present 'structural inertia' of the distribution grid. PARITY's solution is expected to increase grid durability and efficiency, facilitating the penetration of renewable energy sources in the electricity energy mix beyond 50 %.
cityxchange EU project [115]: Local Distributed Positive Energy Block trading market tool Home - +CityxChange	Enable a fair deal to all consumers through a local flexibility market and innovative financing

Blockchain based decentralized local energy flexibility market projects such as H2020 BRIGHT , H2020 eDREAM [116] https://www.brightproject.eu/ https://edream-h2020.eu/	They cover different market designs than GLocalFlex, but it is possible to consider adapting algorithms and contracts.
Technology development	**Relevance to GLocalFlex**
Test bed experiments and simulation scaleup studies by EU Joint Research Centre on blockchain based services for flexibility, energy community, and smart-metering use cases (European platform for Internet Contingencies and Blockchain Analysis (EPIC-BA) and the Smart Grid Interoperability Laboratory (SGI-Lab), Hyperledger Fabric for blockchain) [93]	Testbed showed robust and straightforward implementation of blockchain solutions, simulations implied scalability. Transaction speeds easily allow flexibility in the range of GLocalFlex services. They demonstrated the use of smart meters to communicate and send transactions to a blockchain system. They demonstrated overall robustness of the system, resilience to cyber-threats, capacity to scale and adequate maturity.
Blockchain enabling intelligent smart meters [117]	Smart meter capabilities are dominant enablers or disablers of the GLocalFlex market participation. Metering and flexibility verification is a central topic in the GLocalFlex market.
Blockchain energy platforms	**Relevance to GLocalFlex**
EQUIGY [118], crowd balancing platform (CBP) blockchain-based ancillary service market for TSO, DSO and Aggregators to increase utilization of consumer level flexibility. TSO initiated. Active in 5 countries. The European Investment Bank supports its growth.	In EQUIGY the consumers are present via aggregators. An aggregator could acquire flexibility from the GLocalFlex market and construct a bid to EQUIGY (aggregation and risk management involved). One of EQUIGY's main barriers is low economic benefits for participating in the market and challenges of aggregators. GLocalFlex approach may respond better to these challenges.

Blockchain energy platforms: EnerChain (live during 2019-2021), Volt Markets/Pylon/LO3 Energy project (decentralized P2P trading platforms) https://enerchain.ponton.de/ https://www.energy21.com/ https://voltmarkets.com/ https://pylon-network.org/ https://lo3energy.com/	Although all these platforms target different problems and markets, topics like smart contracts and market rules/penalties are relevant to GLocalFlex platform in an adapted form.
Most topical research papers	**Relevance to GLocalFlex**
A blockchain based lightweight peer-to-peer energy trading framework for secured high throughput micro-transactions [119]. This paper claims first comprehensive method for blockchain in energy trading using IOTA.	Relevant performance testing, and IOTA specific solutions.
Smart contracts in energy systems: A systematic review of fundamental approaches and implementations [120]	GLocalFlex needs smart contracts at various energy system layers. Sample "Energy Smart Contract" as open-source code, recommendations, insights of industrial and demonstration projects

Bibliography

[1] "NIS 2 Directive." https://www.nis-2-directive.com/ (accessed Apr. 23, 2023).

[2] European Commission, "Commission staff working document accompanying the document Commission recommendation on cybersecurity in the energy sector," European Commission, Bruxelles, SWD(2019) 1240 final, Apr. 2019. Accessed: Jul. 17, 2020. [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/swd2019_1240_final.pdf

[3] "Fit for 55," Apr. 27, 2023. https://www.consilium.europa.eu/en/policies/green-deal/fit-for-55-the-eu-plan-for-a-green-transition/ (accessed May 19, 2023).

[4] CertiK, "The Blockchain Trilemma: Decentralized, Scalable, and Secure?," *CertiK*, Oct. 04, 2019. https://medium.com/certik/the-blockchain-trilemma-decentralized-scalable-and-secure-e9d8c41a87b3 (accessed May 22, 2023).

[5] "eIDAS 2.0 - Introduction to The European Digital Identity Wallet & The Evolution of Self-Sovereign Identity," Aug. 18, 2022. https://utimaco.com/current-topics/blog/eidas-2-the-european-digital-identity-wallet (accessed Jun. 07, 2023).

[6] USEF, "USEF: THE FRAMEWORK EXPLAINED, update 2021," 2021. [Online]. Available: https://www.usef.energy/app/uploads/2021/05/USEF-The-Framework-Explained-update-2021.pdf

[7] L. Cauret *et al.*, "D3.1 – Benchmark of markets and regulations for electricity, gas and heat and overview of flexibility services to the electricity grid," Apr. 2019, Accessed: Jun. 22, 2023. [Online]. Available: https://zenodo.org/record/4783519

[8] Coordinet project, "Market and regulatory analysis: Analysis of current market and regulatory framework in the involved areas," D1.1, 2019. [Online]. Available: https://private.coordinet-project.eu/files/documentos/5cdc65b97fb00COORDINET%20D1.1.pdf

[9] "Balancing Energy Platforms | www.acer.europa.eu." https://www.acer.europa.eu/electricity/market-rules/electricity-balancing/balancing-energy-platforms (accessed Apr. 23, 2023).

[10] "Frequency Containment Reserves." https://www.entsoe.eu/network_codes/eb/fcr/ (accessed Apr. 23, 2023).

[11] "PICASSO." https://www.entsoe.eu/network_codes/eb/picasso/ (accessed Apr. 23, 2023).

[12] "Basics of the Power Market | EPEX SPOT." https://www.epexspot.com/en/basicspowermarket#day-ahead-and-intraday-the-backbone-of-the-european-spot-market (accessed Apr. 25, 2023).

[13] "What is Day-Ahead Trading of Electricity?" https://www.next-kraftwerke.com/knowledge/day-ahead-trading-electricity (accessed Apr. 25, 2023).

[14] "Intraday trading: Definition, theory and practice," *Next Kraftwerke .com*, Feb. 14, 2019. https://www.next-kraftwerke.com/knowledge/intraday-trading (accessed Sep. 04, 2019).

[15] USEF, "WORKSTREAM ON AGGREGATOR IMPLEMENTATION MODELS," 2017. Accessed: Apr. 06, 2023. [Online]. Available: https://www.usef.energy/app/uploads/2017/09/Recommended-practices-for-DR-market-design-2.pdf

[16] "Ramboll-for-publication.pdf." Accessed: May 24, 2023. [Online]. Available: https://equigy.com/wp-content/uploads/2022/11/Ramboll-for-publication.pdf

[17] EU project Sysflex, "Proposal for data exchange standards and protocols," 2021.

[18] "Mapping tool viewer." https://mapping.iec.ch/#/maps/1 (accessed Apr. 23, 2023).

[19] "SGAM Toolbox – Modelling aid for the Smart Grid Architecture Model." https://sgam-toolbox.org/ (accessed Apr. 23, 2023).

[20] CEN-CENELEC-ETSI Smart Grid Coordination Group, "SG-CG/ M490/F_ Overview of SG-CG Methodologies," 2014. Accessed: Jun. 13, 2023. [Online]. Available: https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Smart%20Grids%20and%20Meters/Smart%20Grids/2_sgcg_methodology_overview.pdf

[21] "SGAM User Manual Applying, testing & refining the Smart Grid Architecture Model (SGAM)." Accessed: May 08, 2023. [Online]. Available: https://syc-se.iec.ch/wp-content/uploads/2019/10/SGCG_Methodology_SGAMUserManual.pdf

[22] "OSI model," *Wikipedia*. Mar. 26, 2023. Accessed: Apr. 23, 2023. [Online]. Available: https://en.wikipedia.org/w/index.php?title=OSI_model&oldid=1146735354

[23] "Ontology (computer science)," *Wikipedia*. May 06, 2023. Accessed: May 09, 2023. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Ontology_(computer_science)&oldid=1153481400

[24] A. Schumilin, C. Duepmeier, K.-U. Stucky, and V. Hagenmeyer, "A Consistent View of the Smart Grid: Bridging the Gap between IEC CIM and IEC 61850," in *2018 44th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, Aug. 2018, pp. 321–325. doi: 10.1109/SEAA.2018.00059.

[25] "SAREF Portal." https://saref.etsi.org/ (accessed Apr. 23, 2023).

[26] "SAREF4ENER." https://saref.etsi.org/saref4ener/latest/saref4ener.html (accessed Sep. 05, 2019).

[27] "home - EEBus - Empowering the digitalisation of Energy transition." https://www.eebus.org/ (accessed Apr. 23, 2023).

[28] "SAREF4ENER: an extension of SAREF for the energy domain created in collaboration with Energy@Home and EEBus associations." https://saref.etsi.org/saref4ener/v1.1.2/ (accessed Apr. 23, 2023).

[29] OpenADR alliance, "OpenADR 2.0b Profile Specification v1.1." 2015.

[30] “OpenLEADR: a friendly and compliant OpenADR implementation for Python.” https://openleadr.org/ (accessed Apr. 23, 2023).

[31] B. Swan and A. Technologies, “The Language of BACnet-Objects, Properties and Services”.

[32] USEF, “USEF Flexibility Trading Protocol Specification.”

[33] AEIC, “Demand Response Measurement & Verification,” 2009.

[34] M. L. Goldberg and G. Kennedy Agnew, “Measurement and Verification for Demand Response,” 2013.

[35] Will Gifford, “Measurement and Verification: Making AMI Data Smart for Demand Response,” 2014. Accessed: Apr. 06, 2023. [Online]. Available: https://energy-evaluation.org/wp-content/uploads/2019/06/2014-berlin-will-gifford.pdf

[36] “How do smart meters communicate? | emnify Blog.” https://www.emnify.com/blog/how-smart-meters-communicate (accessed Apr. 21, 2023).

[37] “3 – Overview of the M-Bus – M-Bus.” https://m-bus.com/documentation-wired/03-overview-of-the-m-bus (accessed Apr. 24, 2023).

[38] V. Mohan, “An Introduction to Wireless M-Bus”.

[39] “What Is LoRaWAN? | IoT Glossary.” https://www.emnify.com/iot-glossary/lorawan (accessed Apr. 21, 2023).

[40] “Zigbee Protocol - an overview | ScienceDirect Topics.” https://www.sciencedirect.com/topics/engineering/zigbee-protocol (accessed Apr. 24, 2023).

[41] “Technology,” *Sigfox 0G Technology*. https://www.sigfox.com/technology/ (accessed Apr. 21, 2023).

[42] *What Is The Sigfox Protocol Stack?*, (Aug. 02, 2017). Accessed: Apr. 24, 2023. [Online Video]. Available: https://www.youtube.com/watch?v=tGmFgaxKPRU

[43] DLMS User Association, “Overview.” https://www.dlms.com/dlms-cosem/overview (accessed Jan. 27, 2023).

[44] “Analysis of DLMS Protocol.” Accessed: Apr. 21, 2023. [Online]. Available: https://www.fit.vut.cz/research/publication/11616/.en

[45] “IEEE Standard for Optical Port Communication Protocol to Complement the Utility Industry End Device Data Tables,” *IEEE Std 1701-2011*, pp. 1–50, Feb. 2011, doi: 10.1109/IEEESTD.2011.5716536.

[46] “Open Charge Alliance - Global Platform For Open Protocols.” https://www.openchargealliance.org/ (accessed Dec. 03, 2018).

[47] “What is OCPP? — ChargeLab.” https://www.chargelab.co/industry-advocacy/ocpp (accessed Apr. 21, 2023).

[48] “What Is Open Charging Point Protocol (OCPP)? | EV Connect — EV Connect.” https://www.evconnect.com/blog/what-is-open-charging-point-protocol (accessed Apr. 21, 2023).

[49] "The Modbus Organization." https://modbus.org/ (accessed Apr. 21, 2023).

[50] "Modbus - an overview | ScienceDirect Topics." https://www.sciencedirect.com/topics/computer-science/modbus (accessed Apr. 21, 2023).

[51] "Ship," *EEBus - Empowering the digitalisation of Energy transition.* https://www.eebus.org/divi_overlay/ship/ (accessed Apr. 24, 2023).

[52] "ISO 9506-1:2003(en), Industrial automation systems — Manufacturing Message Specification — Part 1: Service definition." https://www.iso.org/obp/ui/#iso:std:iso:9506:-1:ed-2:v1:en (accessed Apr. 24, 2023).

[53] "Manufacturing Message Specification - an overview | ScienceDirect Topics." https://www.sciencedirect.com/topics/engineering/manufacturing-message-specification (accessed Apr. 24, 2023).

[54] H. Grasset and C. Bloch, "An introduction to IEC 61850 GOOSE messaging".

[55] "ZigBee Specification," 2017.

[56] CSA, "Matter Specification," Sep. 2022.

[57] "Matter FAQs | Frequently Asked Questions," *CSA-IOT*. https://csa-iot.org/all-solutions/matter/matter-faq/ (accessed Apr. 26, 2023).

[58] USEF, "USEF: The privacy and security guideline," USEF Foundation, Nov. 2015. Accessed: Feb. 02, 2023. [Online]. Available: https://www.usef.energy/app/uploads/2016/12/USEF_PrivacySecurityGuideline_3nov15.pdf

[59] "What is GDPR, the EU's new data protection law?," *GDPR.eu*, Nov. 07, 2018. https://gdpr.eu/what-is-gdpr/ (accessed Apr. 21, 2023).

[60] 14:00-17:00, "ISO/IEC 27019:2017," *ISO*, Aug. 15, 2016. https://www.iso.org/standard/68091.html (accessed Apr. 21, 2023).

[61] "Understanding IEC 62443." https://www.iec.ch/blog/understanding-iec-62443 (accessed Apr. 21, 2023).

[62] "SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC." https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (accessed Apr. 23, 2023).

[63] "Minimum Security Measures for Operators of Essentials Services," *ENISA*. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/minimum-security-measures-for-operators-of-essentials-services (accessed Apr. 21, 2023).

[64] European Union Agency for Network and Information Security., *Baseline security recommendations for IoT in the context of critical information infrastructures.* LU: Publications Office, 2017. Accessed: Apr. 20, 2023. [Online]. Available: https://data.europa.eu/doi/10.2824/03228

[65] M. Kozole and G. Kmethy, "Security in DLMS," DLMS User Association, White paper, Nov. 2019. Accessed: Jan. 27, 2023. [Online]. Available: https://www.dlms.com/files/DLMS-White-Paper-Security_November_2019.pdf

[66] K. Kursawe and C. Peters, "Structural Weaknesses in the Open Smart Grid Protocol," in *2015 10th International Conference on Availability, Reliability and Security*, Aug. 2015, pp. 1–10. doi: 10.1109/ARES.2015.67.

[67] "What Is Transmission Control Protocol (TCP)?," *Heimdal Security Blog*, Feb. 16, 2023. https://heimdalsecurity.com/blog/what-is-tcp/ (accessed Apr. 24, 2023).

[68] S. Cooper, "A guide to UDP (User Datagram Protocol)," *Comparitech*, Jan. 08, 2019. https://www.comparitech.com/net-admin/guide-udp-user-datagram-protocol/ (accessed Apr. 24, 2023).

[69] "IBM Documentation," Apr. 03, 2023. https://www.ibm.com/docs/en/ibm-mq/7.5?topic=mobile-messaging-m2m (accessed Apr. 21, 2023).

[70] T. ghamedy, A. Lasebae, and M. Aiash, *Security Analysis of the Constrained Application Protocol in the Internet of Things*. 2013.

[71] "Why is HTTP not secure? | HTTP vs. HTTPS," *Cloudflare*. https://www.cloudflare.com/learning/ssl/why-is-http-not-secure/ (accessed Apr. 24, 2023).

[72] "Improved security for OCPP 1.6-J: edition 3 FINAL, 2022-02-17," 2022.

[73] D. Desruisseaux, "Modbus Security – New Protocol to Improve Control System Security," *Schneider Electric Blog*, Aug. 30, 2018. https://blog.se.com/industry/machine-and-process-management/2018/08/30/modbus-security-new-protocol-to-improve-control-system-security/ (accessed Apr. 24, 2023).

[74] "What is Transport Layer Security? | TLS protocol," *Cloudflare*. https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/ (accessed Apr. 24, 2023).

[75] "What is EEBUS?," *EEBus - Empowering the digitalisation of Energy transition.* https://dev.eebus.org/what-is-eebus/ (accessed Apr. 24, 2023).

[76] G. Elbez, H. B. Keller, and V. Hagenmeyer, "Authentication of GOOSE Messages under Timing Constraints in IEC 61850 Substations," presented at the 6th International Symposium for ICS & SCADA Cyber Security Research 2019, Sep. 2019. doi: 10.14236/ewic/icscsr19.17.

[77] "OSGP Alliance." http://osgp.org/en (accessed Apr. 23, 2023).

[78] "NES Implementation of OSGP." https://www.networkedenergy.com/en/news-events/nes-implementation-of-osgp (accessed Apr. 23, 2023).

[79] G. Contributor, "Smart metering and power line communications for utilities," *Enlit World*, Apr. 14, 2022. https://www.enlit.world/digitalisation/smart-metering/smart-metering-and-power-line-communications/ (accessed Apr. 23, 2023).

[80] "technical information." http://osgp.org/en (accessed Apr. 23, 2023).

[81] "Overview | dlms." https://www.dlms.com/dlms-cosem/overview (accessed Apr. 21, 2023).

[82] N. Luring, D. Szameitat, S. Hoffmann, and G. Bumiller, "Analysis of security features in DLMS/COSEM: Vulnerabilities and countermeasures," in *2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Feb. 2018, pp. 1–5. doi: 10.1109/ISGT.2018.8403340.

[83] "Zigbee FAQs | Frequently Asked Questions," *CSA-IOT*. https://csa-iot.org/all-solutions/zigbee/zigbee-faq/ (accessed Apr. 26, 2023).

[84] "Smart Energy FAQ | Frequently Asked Questions," *CSA-IOT*. https://csa-iot.org/all-solutions/smart-energy/smart-energy-faq/ (accessed Apr. 28, 2023).

[85] "IEEE SA - IEEE 802.15.4-2020." https://standards.ieee.org/ieee/802.15.4/7029/ (accessed Apr. 30, 2023).

[86] "Zigbee | Complete IOT Solution," *CSA-IOT*. https://csa-iot.org/all-solutions/zigbee/ (accessed Apr. 28, 2023).

[87] "Smart Energy | Green Homes | IOT Solution," *CSA-IOT*. https://csa-iot.org/all-solutions/smart-energy/ (accessed Apr. 28, 2023).

[88] S. Khanji, F. Iqbal, and P. Hung, *ZigBee Security Vulnerabilities: Exploration and Evaluating*. 2019. doi: 10.1109/IACS.2019.8809115.

[89] "Build With Matter | Smart Home Device Solution," *CSA-IOT*. https://csa-iot.org/all-solutions/matter/ (accessed Apr. 26, 2023).

[90] CSA, "Matter Security and Privacy Fundamentals," Mar. 2022.

[91] "2030 Digital Compass: the European way for the Digital Decade." Accessed: May 19, 2023. [Online]. Available: https://commission.europa.eu/system/files/2023-01/cellar_12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02_DOC_1.pdf

[92] "Blockchain Strategy | Shaping Europe's digital future," Mar. 21, 2023. https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy (accessed May 19, 2023).

[93] European Commission. Joint Research Centre., *Blockchain solutions for the energy transition: experimental evidence and policy recommendations.* LU: Publications Office, 2022. Accessed: May 19, 2023. [Online]. Available: https://data.europa.eu/doi/10.2760/62246

[94] "What is Blockchain Technology - IBM Blockchain | IBM." https://www.ibm.com/topics/blockchain (accessed Jun. 20, 2023).

[95] "What is cryptocurrency and how does it work?," *www.kaspersky.com*, Jun. 09, 2023. https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency (accessed Jun. 20, 2023).

[96] DataFlair, "What is Public Key Cryptography in Blockchain," *DataFlair*, Jun. 12, 2018. https://data-flair.training/blogs/public-key-cryptography/ (accessed May 22, 2023).

[97] D. R. Houben and A. Snyers, "Cryptocurrencies and blockchain".

[98] "Understanding Proof Of Work – Forbes Advisor." https://www.forbes.com/advisor/investing/cryptocurrency/proof-of-work/ (accessed May 22, 2023).

[99] "What Is Proof of Stake? How Does It Work? – Forbes Advisor." https://www.forbes.com/advisor/investing/cryptocurrency/proof-of-stake/ (accessed May 22, 2023).

[100] Crypto.com, "How to Agree: Different Types of Consensus for Blockchain." https://crypto.com/university/different-types-of-consensus-for-blockchain (accessed May 23, 2023).

[101] "Direct Acyclic Graph Tangle (DAG)." https://tokens-economy.gitbook.io/consensus/chain-based-dag/direct-acyclic-graph-tangle-dag (accessed May 23, 2023).

[102] B. Cao *et al.*, "Performance analysis and comparison of PoW, PoS and DAG based blockchains," *Digit. Commun. Netw.*, vol. 6, no. 4, pp. 480–485, Nov. 2020, doi: 10.1016/j.dcan.2019.12.001.

[103] "IOTA Smart Contracts | Shimmer Wiki." https://wiki.iota.org/shimmer/smart-contracts/overview/ (accessed May 24, 2023).

[104] "Introduction to Decentralized Identity | IOTA Wiki." https://wiki.iota.org/identity.rs/decentralized_identity/ (accessed May 24, 2023).

[105] "Decentralized Identifiers (DIDs) v1.0." https://www.w3.org/TR/did-core/ (accessed Jun. 07, 2023).

[106] G. Weston, "Self Sovereign Identity & Decentralized Identity - An Unlimited Guide," *101 Blockchains*, Jul. 18, 2022. https://101blockchains.com/self-sovereign-identity-and-decentralized-identity/ (accessed Jun. 20, 2023).

[107] "eidas_supported_ssi_may_2019_0.pdf." Accessed: Jun. 07, 2023. [Online]. Available: https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf

[108] "What are Verifiable Credentials? | Decentralized Identity Developer Docs." https://didproject.azurewebsites.net/docs/verifiable-credentials.html (accessed Jun. 22, 2023).

[109] "eIDAS Regulation | Shaping Europe's digital future." https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation (accessed Jun. 07, 2023).

[110] S. Schwalm, D. Albrecht, and I. Alamillo, *eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI*. Gesellschaft für Informatik e.V., 2022. doi: 10.18420/OID2022_05.

[111] "eIDAS 2.0 - Roadmap, Toolbox, and The European Digital Identity Wallet Architecture," Feb. 20, 2023. https://utimaco.com/news/blog-posts/eidas-20-roadmap-toolbox-and-european-digital-identity-wallet-architecture (accessed Jun. 07, 2023).

[112] "OpenID - OpenID Foundation." https://openid.net/ (accessed Jun. 08, 2023).

[113] “Sandbox Project - EBSI -.” https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Sandbox+Project (accessed Jun. 21, 2023).

[114] “Parity H2020 – Parity H2020.” https://parity-h2020.eu/ (accessed Jun. 21, 2023).

[115] “Home,” *+CityxChange*. https://cityxchange.eu/ (accessed Jun. 21, 2023).

[116] “eDREAM - blockchain based Demand Response technologies.” https://edream-h2020.eu/ (accessed Jun. 21, 2023).

[117] M. Tahir, N. Ismat, H. H. Rizvi, A. Zaffar, S. M. Nabeel Mustafa, and A. A. Khan, “Implementation of a smart energy meter using blockchain and Internet of Things: A step toward energy conservation,” *Front. Energy Res.*, vol. 10, 2022, Accessed: May 23, 2023. [Online]. Available: https://www.frontiersin.org/articles/10.3389/fenrg.2022.1029113

[118] “Home - Equigy.” https://equigy.com/ (accessed Jun. 21, 2023).

[119] N. R. Pradhan *et al.*, “A blockchain based lightweight peer-to-peer energy trading framework for secured high throughput micro-transactions,” *Sci. Rep.*, vol. 12, no. 1, Art. no. 1, Aug. 2022, doi: 10.1038/s41598-022-18603-z.

[120] D. Kirli *et al.*, “Smart contracts in energy systems: A systematic review of fundamental approaches and implementations,” *Renew. Sustain. Energy Rev.*, vol. 158, p. 112013, Apr. 2022, doi: 10.1016/j.rser.2021.112013.