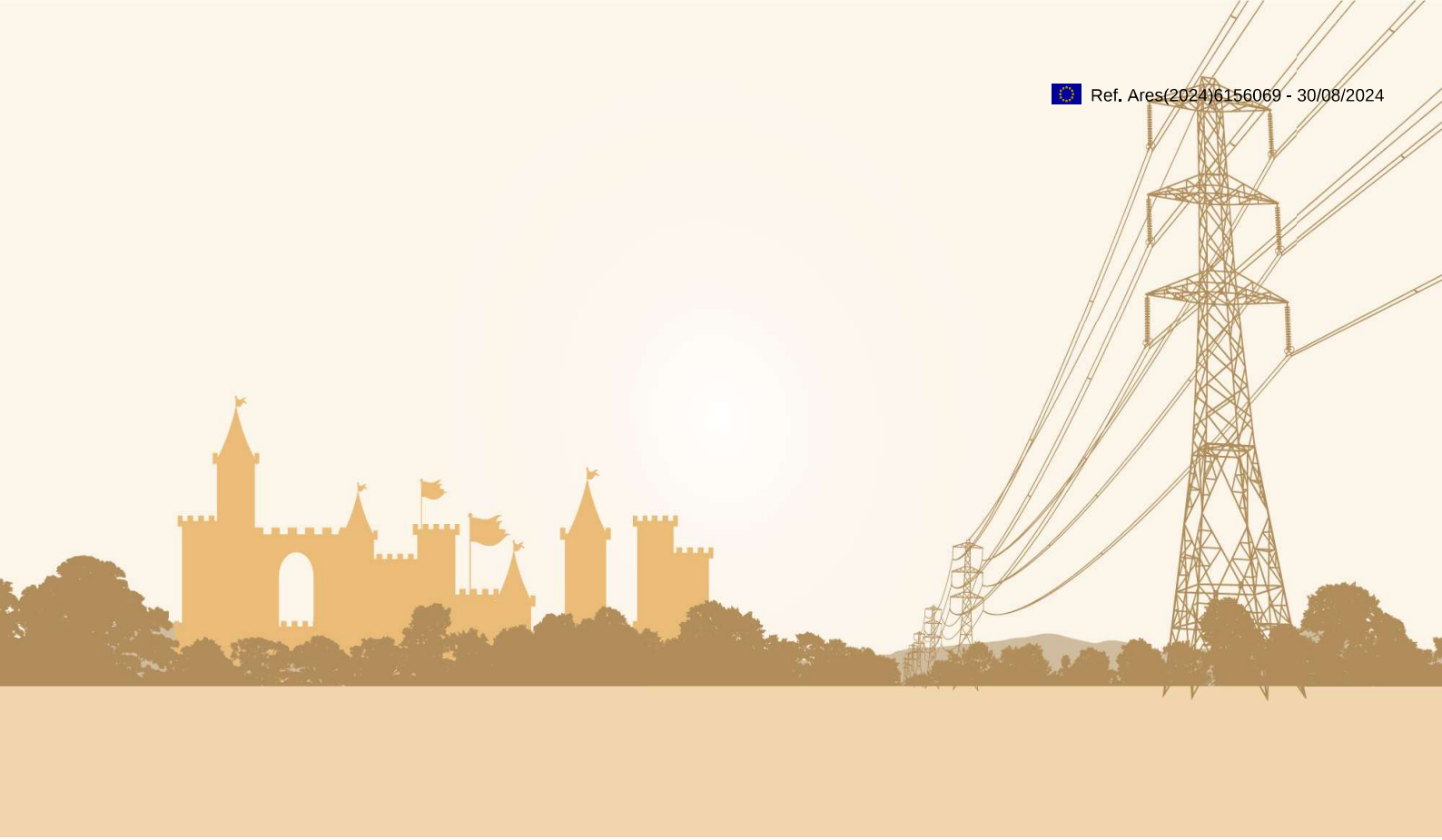

eFORT

Establishment of a FramewORk for Transforming current EPES into a more resilient, reliable and secure system all over its value chain

D2.3 Guidelines for secure and private data collection and sharing

Document details

Deliverable no	D2.3
Deliverable name	Guidelines for secure and private data collection and sharing
Version	1.0
Release date	31/08/2024 (M24)
Type	R
Dissemination level	SEN
Status	Final version
Author	Suite5, CIRCE, TENNET, SELTA-DP, CUERVA, SIA, COM, SCHN, JSC, ISOL

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

DISCLAIMER OF WARRANTIES

This document has been prepared by eFORT project partners as an account of work carried out within the framework of the EC-GA contract no. 101075665.

Neither Project Coordinator, nor any signatory party of eFORT Project Consortium Agreement, nor any person acting on behalf of any of them:

a) makes any warranty or representation whatsoever, expressed or implied,

   I. with respect to the use of any information, apparatus, method, process, or similar item disclosed in this document, including merchantability and fitness for a particular purpose, or

   II. that such use does not infringe on or interfere with privately owned rights, including any party's intellectual property, or

   III. that this document is suitable to any particular user's circumstance; or

b) assumes responsibility for any damages or other liability whatsoever (including any consequential damages, even if the Project Coordinator or any representative of a signatory party of the eFORT Project Consortium Agreement has been informed of the possibility of such damages) resulting from your selection or use of this document or any information, apparatus, method, process, or similar item disclosed in this document.

This work has been Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Climate, Infrastructure and Environment Executive Agency (CINEA). Neither the European Union nor the granting authority can be held responsible for them.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Document history

Version	Date of issue	Content and changes	Edited by
0.1	31/08/2023	First draft version	Suite5
0.2	21/10/2023	Second draft version	All contributors
0.3	23/01/2024	Third draft version	All contributors
0.4	17/05/2024	Peer reviewed	Suite5, COM
0.5	31/05/2024	Input added	All contributors
0.6	18/06/2024	Final version	Suite5, COM
0.7	30/06/2024	Final quality check and additions	SIA, SCHN
0.8	15/07/2024	Final version ready for review	Suite5, COM
0.9	15/08/2024	Internal review and final comments	CERTH, CIRCE
1.0	31/08/2024	Final quality check and submission	CIRCE, Suite5, COM

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Table of contents

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

List of figures

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

List of tables

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Abbreviations and Acronyms

Acronym	Description
ADMS	Advanced Distribution Management Systems
ABAC	Attribute-Based Access Control
AMI	Advanced Metering Infrastructure
APT	Advanced Persistent Threats
CEFACT	Centre for Trade Facilitation and Electronic Business
CGMES	Common Grid Model Exchange Standard
CHP	Combined Heat and Power plants
CPO	Charging Point Operators
CSMS	Cybersecurity Management System
DA	Data Access
DCFC	Direct Current Fast Charging
DCS	Distributed Control System
DERs	Distributed Energy Resources
DG	Distributed Generation
DNS	Domain Name Server
DoS	Denial of Service
DR	Demand Response
DSO	Distribution System Operators
EIA	Energy Information Administration
EMS	Energy Management System
EPES	Electrical Power and Energy Systems
ETSI	European Telecommunications Standards Institute
EVs	Electric vehicles
EVSE	Electric Vehicle Supply Equipment
FDIA	False Data Injections Attacks
GHG	Greenhouse Gas
GIC	Geomagnetically Induced Currents
HV, MV, LV	High, Medium, and Low voltage
HVAC	Heating Ventilating Air Conditioning
ICS	Integrated Control Systems
IEDs	Intelligent Electronic Devices
IoT	Internet of Things
IRPP	Integrated Resource and Resilience Planning

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Acronym	Description
IT	Information Technology
KIs	Key Indicators
MaD IoT	Manipulation of Demand via IoT
OCPP	Open Charge Point Protocol
OLE	Object Linking and Embedding
OPC	OLE for Process Control
OT	Operational Technology
PLC	Programmable Logic Controllers
PMU	Phasor Measurement Unit
RA	Risk Assessment
RTUs	Remote Terminal Units
SAREF	Smart Appliances REFerence ontology
SAS	Substation Automation Systems
SCADA	Supervisory Control and Data Acquisition
SDN	Software Defined Network
SGAM	Smart Grid Architecture Model
SO	System Operator
TCP	Transmission Control Protocol
UA	Unified Architecture
V2G	Vehicle to Grid
WP	Work Package
WSN	Wireless Sensor Networks

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Executive summary

The scope of this document is to report the activities performed in the context of T2.5 “Establishment of strategies for secure data collection and TSO-DSO data sharing”. From the task description, the goal of this task is twofold: a) to define the specifications for data collection from physical assets and b) proceed with the specification’s definition for secure information exchange among the different business actors acting as network operators.

At first, the aim of T2.5 is to provide a set of specifications referring to data collection mechanisms that should be developed in the frame of the eFORT architecture system towards establishing a secure and trustful data collection and sharing framework. In this context, the task initially focuses on reviewing the procedures and data collection methods as defined in the literature in order to ensure the prompt data gathering from the continuously increasing number of assets in the grid ecosystem (both DSO related assets, as well as DER/IoT devices installed at LV level). Apart from the literature review, the work in this task also focuses on refining the landscape of the relevant data sets involved in the project’s demonstrators and their metadata, thus creating a database of information sources that will be considered during the data collection activities.

In addition to the data gathering/collection framework definition, we aim to identify, monitor and analyse relevant security and privacy handling policies linked to the aforementioned data sets. This relates both to the business value and IPR handling of data, as well as to the confidentiality of the data that might be used during the implementation of the project and shall be safeguarded against any compromise. At first, the review of the relevant security and privacy policies as defined in literature is listed. Then, an elicitation approach is applied taking into account the demo and application needs and requirements. With regards to data security, confidentiality and privacy preservation, eFORT aim to adopt a twofold approach using the best of the breed technologies and mechanisms to holistically safeguard data exchanged between the eFORT platform and involved stakeholders. At DSO and consumer level, the concept of digital substation will be developed adopting up-to-date mechanisms for SCADA, DCS and ICS protection. On the IoT devices and DER levels, appropriate procedures and encryption mechanisms will be designed and developed to facilitate secure and trustful data sharing. The security services to be involved in the eFORT architecture system indicatively involve: end-to-end encryption services for data assets that are ingested through the Intelligent Platform and for key sharing to authorized data consumers, (b) attribute-based access control policies services that formally describe the circumstances under which access requests to data assets should be granted, and are easily interpretable into policy enforcement rules and (c) protocols for remote attestation of the trusted data containers and the core platform, in order to establish their integrity and inherently their trustworthiness. All in all, the task delivers a complete set of specifications for data security and privacy to drive the development of the eFORT business applications in WP3 and WP4 (special remark about the SecureBox in T4.5 and the eFORT intelligent platform in T4.6 as the two core components responsible for data gathering and management).

In parallel, the communication protocols and standards used in past TSO-DSO coordination projects are analysed, together with the relevance of this type to data exchange for the specific demos. In this aspect, get an actual view of the data exchange procedures in EU system operators, a questionnaire was distributed among project members and system

This project has received funding from the European Union’s Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

operator organizations, covering three relevant topics (TSO-DSO data exchange, exchanges of cybersecurity-related information, and coordination of response to cybersecurity incidents). Based on the anonymised analysis of the answers to this questionnaire, some recommendations are provided. In addition to this, the suitability of existing standards (e.g., VERIS Incident Framework, OASIS STIX 2.1, etc.) for different purposes related to the exchange of cybersecurity information is assessed, paying special attention to their different scope and characteristics, to be used by electricity system operators.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

1 Introduction

1.1 Purpose and scope of the document

The scope of the document as part of the work in T2.5 and stated in the Description of Actions (DoA) is *to provide, a set of specifications referring to data collection mechanisms that will be developed in the frame of the eFORT architecture system towards establishing a secure and trustful data sharing framework for all stakeholders involved in the project.*

The analysis performed is twofold: integration of data from physical assets as well as data exchange among the different business stakeholders in the energy value chain. Considering integration with the physical assets at DSO level, the concept of digital substation is developed adopting up-to-date mechanisms for SCADA, DCS and ICS data integration. On the IoT devices and DER integration level, appropriate procedures and data collection methods are examined in order to ensure the prompt data gathering from the continuously increasing number of assets in the grid ecosystem. Overall, will step on state-of-the art methods and design scalable and modular services to serve multiple data collection-related purposes, i.e.: (a) to handle the upstream, downstream and indirect collection of data assets from the supply-driven perspective of the data providers via APIs, through real-time data pipelines and/or batch files and (b) to receive real-time updates for data assets. Apart from the literature review, task 2.5 also focus on refining the landscape of the relevant data sets involved in the project's demonstrators and their meta-data, thus creating a database of information sources that will be considered during the data collection activities.

Furthermore, T2.5 aim to identify, monitor and analyse relevant security and IPR policies linked to the aforementioned data sets. More specifically appropriate security services will be designed that will set different layers for data security and privacy assurance. Again, a thorough review of the most prominent work is performed about the security services to be involved in the eFORT architecture system indicatively involve: (a) end-to-end encryption services for data assets that are ingested through the Intelligent Platform and for key sharing to authorized data consumers, based on hybrid techniques (taking the best of breed from Symmetric Searchable Encryption and Attribute-Based Encryption), (b) attribute-based access control policies services that formally describe the circumstances under which access requests to data assets should be granted, and are easily interpretable into policy enforcement rules etc…

At the business level and considering data exchange among the different stakeholders, T2.5 also lead the analysis for the specifications in the field of the information required by each key player of the energy network, and when and how it must be shared between them to assure the proper operation of the grid, maximising resilience and reliability. Starting with the analysis of ongoing initiatives and past projects' experience to identify how information is being exchange between DSOs and TSOs. In addition to this, for their application to the electricity sector, the suitability of existing standards such as VERIS Incident Framework, IETF IODEF, OASIS STIX 2.1, and OASIS OpenC2 is assessed (according to different purposes), presenting their main characteristics when implemented. Apart from the review of the relevant initiatives and standards, questionnaires were distributed among the DSOs and TSOs participating in the project, and SOs outside the project, to get an actual view of how

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

EU SOs exchange not only market and technical information, but cybersecurity information. Overall, some recommendations are provided for the energy grid players to share this information in a secure way.

There is no direct input from any other task performed in eFORT project. In addition, the data landscape and collection of data sources is tightly linked with the demonstration activities to be performed in the project and more specifically (T5.1 Comprehensive characterization of eFORT demo-sites) towards the definition of demo site specificities. On the other hand, the analysis performed in this task will highly contribute on the development of the work in T4.5 - SecureBox: edge device and functions for privacy management and T4.6 - eFORT Intelligent Platform: integration and interoperability. Moreover, the work reported in this task is tightly linked with the specifications about the communication infrastructure design and network security enhancement to be delivered in the project as part of the work in T2.6.

1.2 Structure of the document

The document is the report about the set of specifications referring to data collection mechanisms that will be developed in the frame of the eFORT architecture system towards establishing a secure and trustful data sharing framework for all stakeholders involved in the project. Therefore, the focus of the work is:

- In Chapter 1 the purpose and the scope of this document are presented.
- In Chapter 2, the results of the state-of-the-art analysis at the physical DER/IoT/DSO assets level is provided covering:
    - The different approaches in the field of data gathering/collection
    - Access policy alternatives for the data gathering/collection processes
    - Security related aspects for the data gathering/collection processes
- In Chapter 2, focus on the analysis of the data available at the demo sites of the project (data landscape analysis) in order to pave the way for the definition of specifications in eFORT project.
- In Chapter 3, the analysis is performed at business level towards specifying the procedures (relevant to eFORT project activities). for the energy grid players to share this information in a secure way.

In the last chapter, the key remarks and summary conclusions are provided.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

2 EPES secure and trustful data sharing

In this section, as stated also in the introductory section, the analysis performed is focusing on the definition of a secure and trustful data collection and sharing framework for the data assets gathered from the physical systems. At first the state-of-the-art analysis of data collection and sharing mechanism at EPES level is provided, considering also the need to specify the security and IPR policies that needs to be applied over the data made available at EPES level. As a follow up of the state-of-the-art analysis, the focus is on refining the landscape of the relevant datasets involved in the project's demonstrators (and their meta-data), thus creating a database of information sources that will be considered during the data collection activities. As a last step, and taking into account both the state-of-the-art analysis results but mainly the project specific requirements, the detailed specifications for the data collection and sharing framework to be delivered in the project are provided.

2.1 Guidelines for field data collection - Literature Review

The scope of this section is to provide a non-exhaustive list of data collection methods and processes from physical assets available at the grid level. The analysis is covering both data integration with DSO assets (at substation level) as well as data collection from the different IoT components (DER, BMS, etc…) that are now evolving within the electricity grid. It's important to note that the review analysis focuses on the scope and objectives of the eFORT project and is therefore limited to the asset types examined in the project.

The literature review takes into account the recent standardization as well as the relevant activities performed in the context of BRIDGE with special focus on the relevant sub groups "European (energy) data exchange reference architecture 3.0" [1] and "Contribution from BRIDGE projects to Standardisation" [2].

2.1.1 Data Collection methods at DSO/substation Level

In this section a reference to the key standardization is provided with focus on data ingestion from substation systems. The analysis is covering data integration from SCADA and DCS (mainly PMU and IED devices) devices to ensure the prompt data collection from grid level assets (with special focus on substation level data monitoring as examined in the project).

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

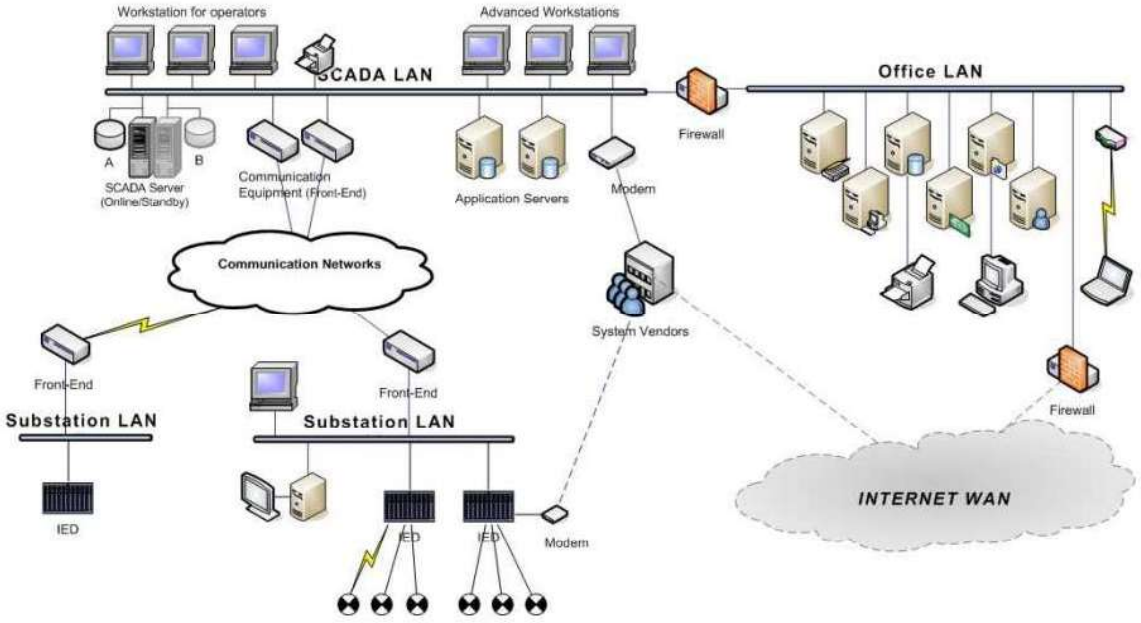

Figure 1 Simplified architecture of a power system with central SCADA and distributed substation automation systems (IEDs)[4]

Before proceeding into the details, we have to point out that the analysis is covering the information exchange part (as the details of the communication network are reported as part of the work in T2.6). A particular challenge when studying the power system control and operation systems is the mix of modern and legacy system components that are in operation. The typical lifespan of a power system control and operation system component is often very long. Especially equipment located in the primary substations tends to have a considerable age due to the cost and the difficulty of replacement: it is not uncommon to have 30-year-old equipment, e.g., Remote Terminal Units (RTUs), with similarly old proprietary communication protocols. At the same time, the central system in the control room can be relatively modern and can consist of a variety of third-party products, like relational databases and power applications from specific vendors.

With a history of proprietary system components from specialized vendors, the trend today is to increasingly rely on off-the-shelf products, both for hardware and for software, when developing and upgrading power system control and operation systems. The focus is on using standard communication interfaces to ensure interoperability between components from different vendors. Legacy protocols, such as Modbus and the proprietary protocols of equipment vendors, are slowly replaced by protocols standardized in the last decade for RTU/IED communication like *DNP3[3], 60870-5 for data acquisition and control[5], or IEEE C37.118-2005[6] for PMU data*. Moreover, communication and automation technology have changed at a faster pace in the past decade, especially with the fast deployment of substation-oriented protocols, like IEC 61850[3]. It is evident, that the standardization efforts today focus mainly on power system models like the Common Information Model (CIM) with the goal of easing the exchange of engineering data between and within utilities in a large variety of applications.

More details about the standards-based protocols as mentioned above, are provided as highly relevant to the project activities. Starting with the DNP3 protocol this is defined as the

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

IEEE 1815 standard and covers the data structure, functions, and application alternatives. A brief presentation of this model to support reliable and efficient communication between various devices such as Remote Terminal Units (RTUs), Intelligent Electronic Devices (IEDs), and master stations (control centers) is provided:

DNP3 is an open standard developed and maintained by the DNP Users Group[1]. DNP3 operates in a master/slave architecture. The master station (usually located in a control center) communicates with remote devices (slaves or outstations) in the field. The master initiates requests, and the outstations respond with relevant data. It supports various data types, including analog inputs, binary inputs, counter inputs, setpoint commands, and more. This versatility allows the protocol to handle different types of data commonly encountered in industrial control systems. Also, the model adopts an object-oriented structure for organizing data. Objects represent different types of data, and each object has specific attributes and behaviors. This structure enhances the clarity and efficiency of data representation.

DNP3 can operate over different data link layers, including serial communication (RS-232, RS-485) and TCP/IP (Ethernet). It includes error-checking mechanisms to ensure the integrity of transmitted data, and it supports features such as retransmission of lost or corrupted messages. DNP3 is scalable and can be deployed in various system sizes, from small installations to large and complex networks. This scalability makes it suitable for applications ranging from small substations to extensive power distribution networks. Last but not least DNP3 supports secure communication through features like authentication and encryption. Security measures are essential for protecting critical infrastructure from unauthorized access and cyber threats and more details about this aspect are provided below.

An indicative data format of the DNP3 protocol is provided below with more details to be made available in the following figure with more details to be available in the specifications of the DNP3 standard [3].

[1] DNP Users Group, https://www.dnp.org/About/DNP-Users-Group

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

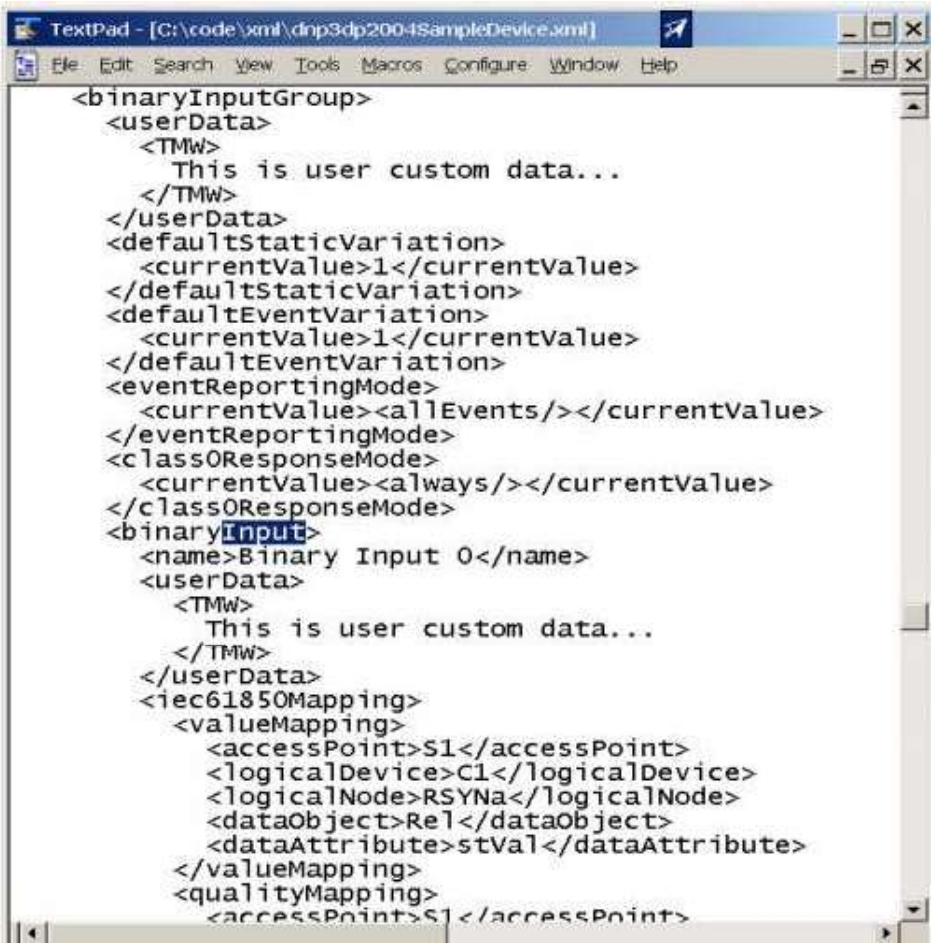

Figure 2 DNP3 device profile in XML format

In the recent years, a major shift towards the **IEC 61850** standard has been considered (also of interest in the project), and the following key features have been adopted widely as part of the specifications of the model:

- IEC 61850 is a substation object-oriented protocol that standardizes the signals as per electrical terminologies and primary equipment into the software world. The IEC working group has incorporated the Generic Object Models for Substation and Feeder Equipment concept into its standard, which is used to present substation data into objects or blocks. This approach makes it easy for the user to configure, understand, test, and maintain the substations from a centralized server within the substation in a cost-efficient and safe manner.
- IEC 61850 provides signal addressing in the form of intuitive names that are called logical nodes. This enhances the engineers' productivity during the time of commissioning to easily understand and map the signals in software databases. They no longer need to refer to a separate cumbersome signal list that dictates internal register addresses to actual signals, as in the case of Modbus or other earlier protocols.
- The multiple parts of IEC 61850 list the whole infrastructure of protocol with details included for manufacturers to help develop their devices with the same principles. This helps greatly and overcomes the challenge of interoperability between different

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

manufactures' devices. Complete device statuses for digitals, and analogs as well as controls are provided through application-layer MMS services of IEC 61850 protocol in a standardized way to share data between different systems in real time.

- IEC 61850 also governs a unique methodology of peer-to-peer communication to send highspeed signals across the network, which is called Generic Object-Oriented Substation Event (GOOSE) messaging. Along with the flexibility of logics in advanced numerical relays to configure various interlocks, these devices also take an advantage of their fast- 6 processing capabilities to perform functions on these high-speed GOOSE to replace conventional electrical hardwires between the relays. Comparing hardwired electrical cabling between different devices, GOOSE messaging reduces cost and time to send high-speed signals for intertripping, blocking, etc., over the Ethernet network and still maintains the same performance as required by the protection application.
- Part of the IEC 61850 standard also provides a secure and reliable method to transfer files from one device to another over the same Ethernet medium using MMS file transfer. IEDs, like protection relays, implement MMS file transfer to transfer data as files and to provide the hierarchal structure for those files to manage data. These files may include relay settings, Configured IED Description (CID) files and fault-event files to be collected from IEDs using MMS file transfer.
- The protocol implementation for IEC 61850 MMS services also includes an option of MMS authentication to enhance data transfer security. If MMS authentication is activated with IEDs, the MMS server makes sure that authentication keys (like passwords) are entered correctly by the MMS client before providing access to its services and files. There are also possibilities available in IEDs to activate and generate alarms in case the client enters the wrong key a multiple number of times, and the alarms can be monitored separately to raise security alerts.

With all the digital information available through substation IEDs, operators in the control centre can use the IEC 61850 data received over GOOSE messages to analyze and troubleshoot the fault in the holistic power system view.

Moreover, the brief presentation of the IEC 60870-5 is provided in this section as a high relevant standard in the field. IEC 60870 part 5, known as Transmission protocol provides a communication profile for sending basic telecontrol messages between two power systems, which uses permanent directly connected data circuits between the systems. More relevant standards are:

- IEC 60870-5-101 Transmission Protocols - Companion standards especially for basic telecontrol tasks
- IEC 60870-5-103 Transmission Protocols - Companion standard for the informative interface of protection equipment
- IEC 60870-5-104 Transmission Protocols - Network access for IEC 60870-5-101 using standard transport profiles

An indicative structure of the data as specified in the 60870-5-101 is provided in the following.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

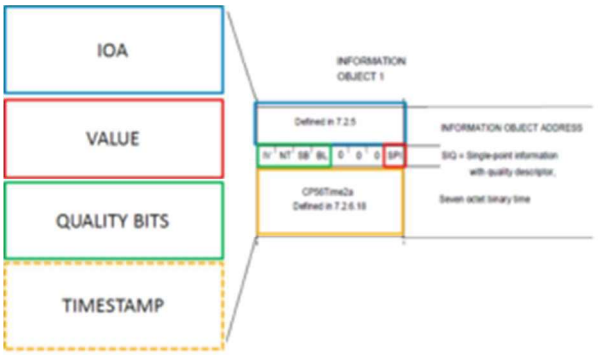

Figure 3 The format of the information object in 60870-5-101

More details about the standardization and modeling principles are provided in [5]. In addition to the IEC 60870 part 5, the IEC 60870 part 6 was also defined to provide a communication profile for sending basic telecontrol messages between two systems which is compatible with ISO standards and ITU-T recommendations. The main differentiation from the DNP3 and IEC 61850 standards presented above, was that none of these communication protocols were suited to the requirements of communicating between control centres.

Another standard that was mentioned above is IEEE C37.118 [7] protocol that specifies synchrophasor measurements/PMUs for power systems. This standard, officially titled "IEEE Standard for Synchrophasors for Power Systems," defines the communication and data exchange protocols for synchrophasor measurements in a way that allows for wide-area monitoring and control of power systems. The standard is divided into two parts:

- IEEE C37.118-1: This part defines the basic synchrophasor measurement standard, including data formats and communication protocols.
- IEEE C37.118-2: This part provides guidelines for using IEEE C37.118-1 in power system applications, including the use of synchrophasors for monitoring, protection, and control.

Key aspects of IEEE C37.118 protocol include:

a) the data format as the standard defines the format for synchrophasor data, including the representation of voltage and current phasors, frequency, and other related information. The data format ensures consistency and interoperability between devices from different manufacturers.

b) Communication Protocols: IEEE C37.118 specifies communication protocols for the exchange of synchrophasor data. Common transport protocols used include User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). It also defines the format of the data frames for communication.

c) Sampling Rates: The standard provides guidelines for high-speed sampling rates to capture the dynamic behavior of the power system. Typically, PMUs sample at rates ranging from 1 sample per cycle to several samples per cycle, allowing for detailed analysis of power system events.

d) Time Synchronization: Precise time synchronization is a critical aspect of synchrophasor measurements. The standard defines requirements for time

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

synchronization to ensure that the measurements from different PMUs are aligned and can be accurately correlated.

The data format of the IEEE C37.118 standard is provided below with a clear explanation of the different fields that set the message structure to be presented in [7].

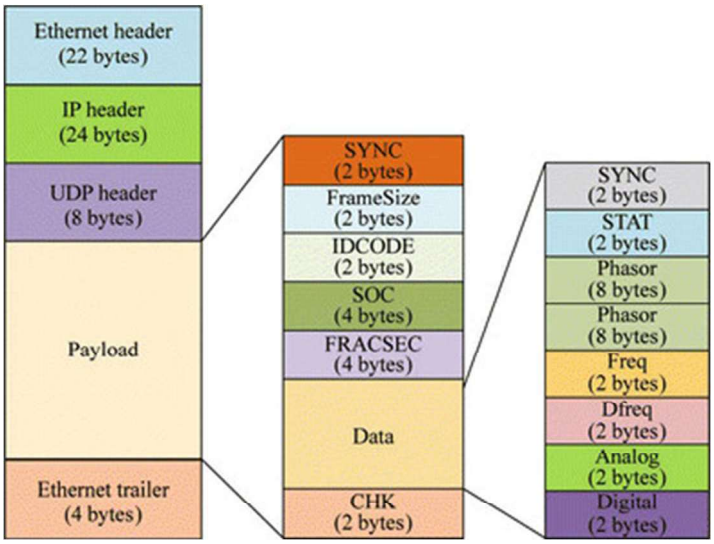

Figure 4 IEEE C37.118 standard Data Frame

We presented above the most prominent technologies considering the data collection form the field devices in the grid, as also highlighted by the IEC standardization in the following overview figure (and also in [8]). We have to point out that additional information model related standards are considered for communication of SCADA systems with the business applications of energy stakeholders. Special remark to the IEC CIM related standards (IEC 61970 for TSOs, IEC 61968 for DSOs and IEC 62325 for Market Operations) as presented also in Figure 5.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

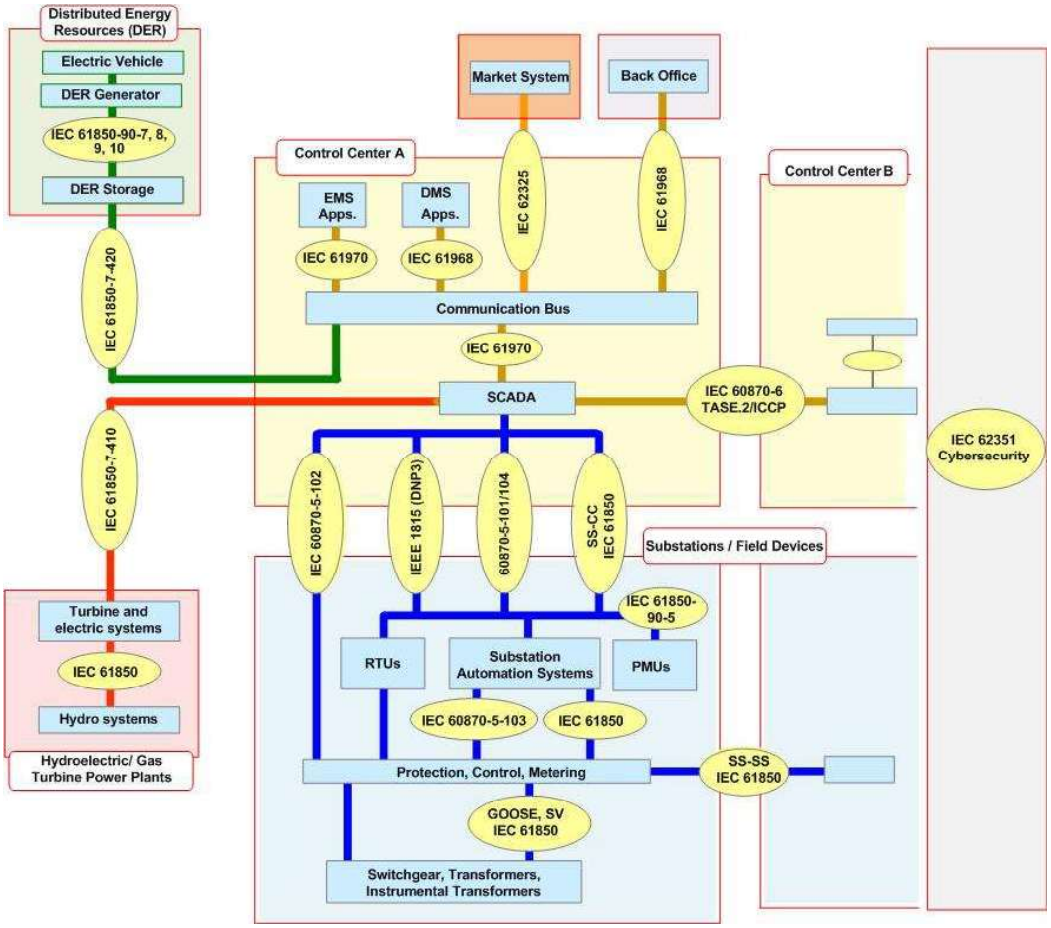

Figure 5 IEC smart grids standardization Overview

There are additional approaches in the domain, such as OPC (OLE for Process Control). OPC is not a communication protocol itself but rather a set of standards for interfacing different systems. OPC servers act as intermediaries between SCADA systems and field devices, translating information between different protocols. OPC DA (Data Access) and OPC UA (Unified Architecture) are common variations also considered in several power systems applications.

2.1.2 Data Collection methods at IoT/ DER Level

In the last decade, it is evident a mass penetration of new DER components at low/medium voltage grid level. Local generation, EV charging points, smart home/building automation systems are massively installed and thus there is an increasing demand for data integration and further incorporation of new assets in new business schemas and use cases. The data collection process from these new types of DERs is an important task, and a series of standards and guidelines (both at communication and semantic level) have been defined in order to ensure the smooth data integration. The most prominent standards/initiatives are presented in this section, focusing on the different types of assets examined in the project.

At first, data integration from generation and batteries assets is considered. The focus is about inverter-based devices (PV, small wind and batteries), nevertheless the standardization review is addressing additional generation-based assets (e.g. small generators) that may be available in premises.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

There is a series of relevant standards in the field addressing the integration of small-scale DER assets but the *IEEE 1547 (Standard for Interconnecting Distributed Resources with Electric Power Systems) is the standard of the Institute of Electrical and Electronics Engineers meant to provide a set of criteria and requirements for the interconnection of distributed energy resources into the power grid.* The standard is intended *to be universally adoptable, technology-neutral, and cover distributed resources as large as 10 MVA.* Based on the standard specifications, all DER—such as photovoltaic (PV) inverters, energy storage systems (ESSs), and synchronous generators—in those jurisdictions must include a standardized SunSpec Modbus [9], IEEE 2030.5[10], or IEEE 1815[11] (DNP3) communication interface.

The SunSpec Modbus is the most common instantiation of the Modbus communication protocol and more specifically the instance as specified by Sunspec Alliance, named as the Sunspec protocol. As stated in [9], there are more than 170 vendors and market ready solutions that have incorporated this protocol for information exchange via MODBUS. The key principles of Sunspec Alliance are presented:

- A trade alliance of global competitors, collaborators & trading partners pursuing smart distributed energy market
- Producer of “de facto” open information standards for Distributed Energy
    - Provides bridge to industry adoption of international standards such as IEC 61850
    - Full testing and certification service for protocols
- Solar PV and storage market focus

The SunSpec Alliance Interoperability Specifications describe the data models and Modbus register mappings for devices used in Renewable Energy systems. The document describes models for read-only inverter data (monitoring) as well as support of programmed, scheduled, and autonomous inverter control operations. In the next figure, an example of inverter models chained together to create an inverter implementation are presented.

This project has received funding from the European Union’s Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

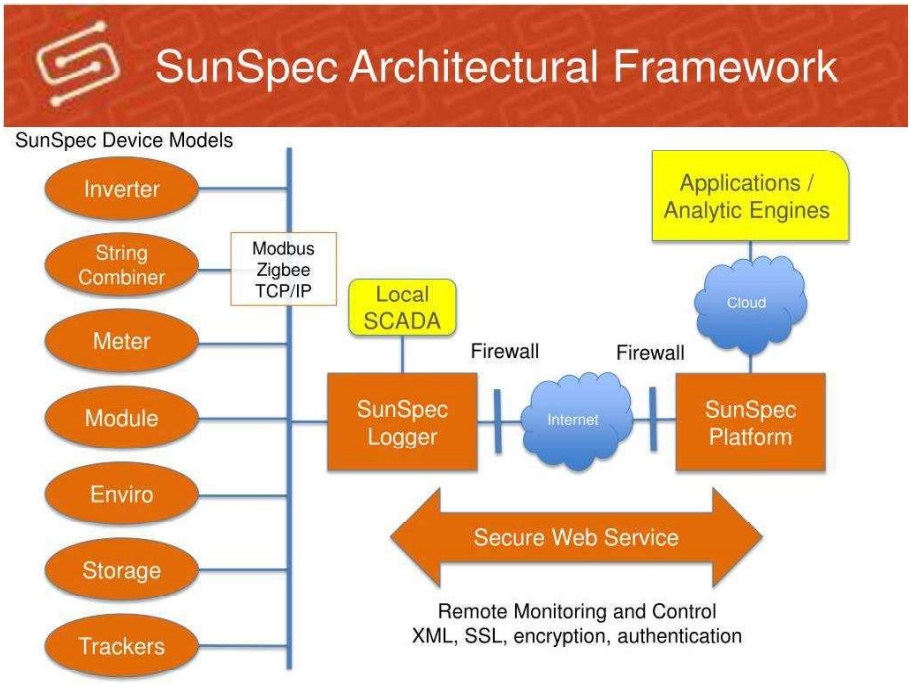

Figure 6 Functional synthesis of Sunspec architectural framework

As stated in the figure above, in the field of data communication, the Modbus protocol support different methods (i.e., Modbus plus, Modbus Serial via RS232 or via RS485) but the most common approach is Modbus TCP/IP over Ethernet which is massively used also in commercial applications.

Overall, a hierarchical & adaptive approach is adopted in the standard. The basis for all inverter data models is defined in the 100 series of the standard. Then, for each specific inverter model, a series of data classes are defined in order to address specific system functionalities. The basic SunSpec device structure Is shown below

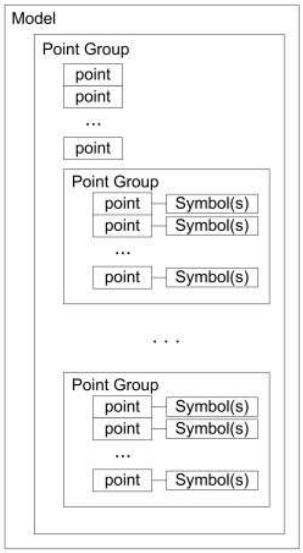

Figure 7 Hierarchical approach on Sunspec model

Apart from the inverter based DERs (addressing small generation/ battery systems), the EV charging points are also considered as a significant DER asset of the electricity grid.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Towards this direction, the OCPP protocol [12] is (among other approaches) the industry standard for the integration of EV CP/ EVSE data to external systems. The details of OCPP are provided in brief. Essentially this protocol has been designed to enable the communication between an EVSE and a CPO. Its current version is 2.0 and it was released in April 2018. This version contains 116 use cases. Summarizing the key functionalities OCPP supports:

- Authorize Charging Session
- Secure firmware updates
- Collecting transaction information for billing purposes
- Operate Charge point
- Reserving a charge point
- Smart Charging
- Device management (e.g., inventory reporting, error and state reporting, configuration, customizable monitoring)
- ISO 15118 Plug & Charge

The supported architecture and topology of OCPP is presented in Figure 8. In this specification the term *Charging Station (CS)* is used to describe the physical system used by an EV to be charged. Essentially, the CS may contain one or more EVSEs. The EVSE can deliver Energy to one EV at a time. Moreover, the specification is using the term Connector for an independently operated and managed electrical outlet of a CS. In some cases, the EVSE may have multiple socket types to serve different types of vehicles. This fundamental definitions of OCPP are illustrated in the following.

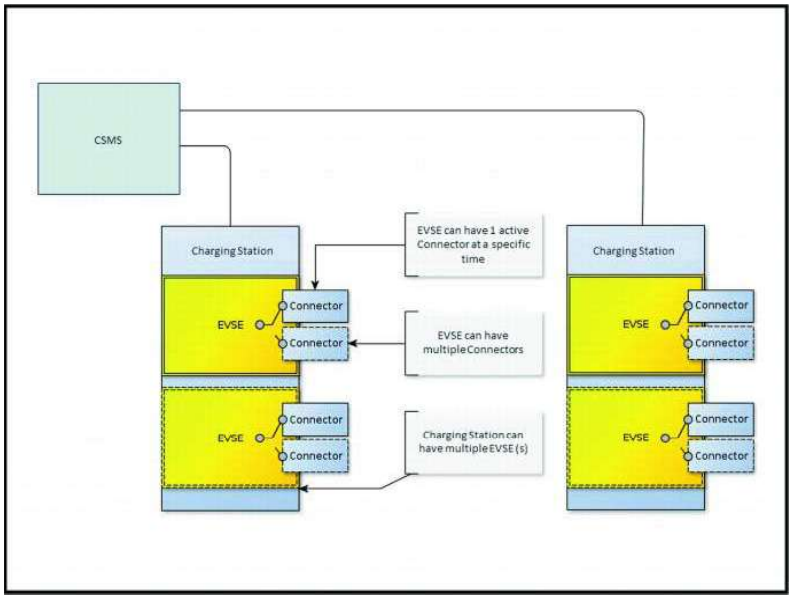

Figure 8 The OCPP 3-tier model

The focus of the review analysis is on the review of the data collection process as well as the security/authentication aspects handled by this standard (presented in section 2.1.4). OCPP has specified a detailed information model where objects and their properties are defined.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

This way, the information structure of the protocol is captured in a formal way enabling a consistent definition of messages and even an automated way for schema generation. The information model is defined using UML and is based on the IEC Common Information Model and to some extend to the CEFACT naming standards. The objects in the model are called Business Components and their properties are inherited from the IEC CIM IdentifierObject. OCPP also supports the so-called Device Model that is a generic scheme to enable any charging Station to report to any CSMS how it is build. This is needed by CSMS to manage the charging station. In order to do these a set of generic messages is defined to enable the communication with the charging station without knowing its internal structure beforehand. The Device model follows the aforementioned 3-tier architecture. In this Device model a charging station is considered to consist of a number of “Components” that represent physical devices, or logical functionality, or logical data entities.

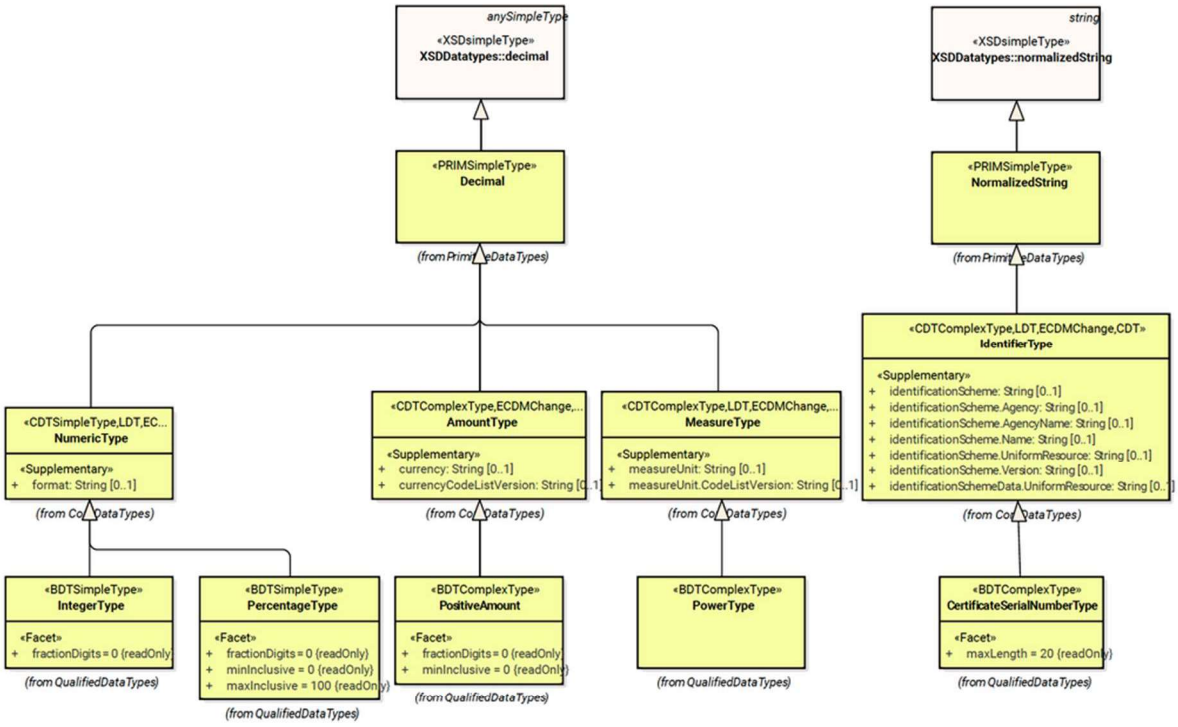

Figure 9 OCPP Data Model

Note that the use of the Device model may extend the capability of bi-directional communication among a CPO and an EVSE. For example, OCPP could potentially be used to report status changes on stand-alone battery packs

In addition to OCPP, IEC 63110[13] is rather new standard to provide communication links for the conductive charging station and electric vehicles. IEC 63110 is also known as the protocol for the Management of Electric Vehicles charging and discharging infrastructures. The IEC 63110 is responsible for a higher and swift level of interoperability in the front-end communication and signal distribution between smart grid infrastructures such as EVs and the conductive charging spots/stations. The IEC 63110 by design is complex based on the protocol standard. However, the procedure in its design ensures cybersecurity, interoperability, grid integration and scalability.

This project has received funding from the European Union’s Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Last but not least, the review analysis is covering smart/controllable assets available within the building environment. The incorporation of demand side assets in the smart electricity network operation is an emerging trend and therefore different initiatives/ standardisation bodies are working towards this direction. The most prominent activities in the field of smart energy management (both at communication as well as information management) at building level are presented. The starting point of the work is the SAREF model[14] and the adoption of this model as the relevant modelling work in the building environment as an effort to ensure interoperability at the building environment. The home systems are technically very heterogeneous, and standardized interfaces on a sensor and device level are required.

A part of what is needed is a unified data model for appliance - a reference ontology (protocol-independent semantic layer). The creation of device and technology abstraction layers and corresponding common Application Programming Interfaces (APIs) are enabled by such an ontology and can be addressed, without the need-to-know specifics of the various standards and for generic types of appliances, by the developers of energy-saving application. A reference ontology offers this, by explicitly specifying recurring core concepts in the smart appliances' domain, the relationships between these concepts, and mappings to other concepts used by different assets/standards/models. To propose this high-level model, the European Commission (EC) launched a standardization initiative, to be conducted by European Telecommunications Standards Institute's (ETSI) Smart Machine-to-Machine (M2M) Technical Committee. The SAREF Technical Specification has been already published by ETSI.

Currently, the SAREF ontology is a shared model of consensus aiming to facilitate the matching of existing assets (standards, protocols, etc.) in the smart appliances' era. It provides building blocks that allow separation/ recombination of different parts of the ontology to cover different needs. The general idea of the SAREF ontology is depicted in Figure 10 and further analysed below.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

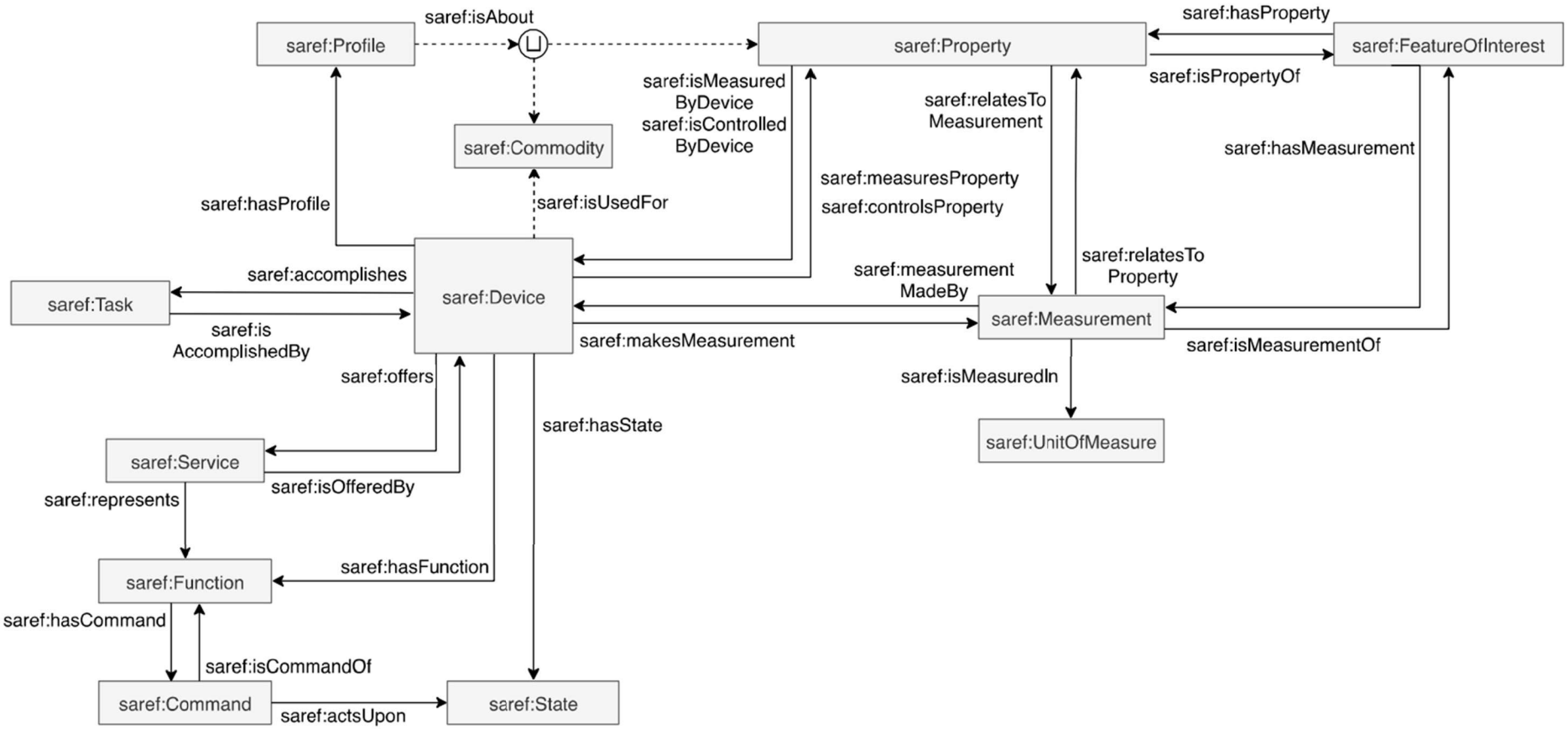

Figure 10 The SAREF Ontology

The SAREF model is currently being extended to add semantic models for data associated with multiple domains ranging from smart cities, industry and manufacturing, smart agriculture and the food chain, water, automotive, eHealth/ aging well and wearables. In particular, a multitude of different domains are currently on the roadmap turning SAREF into “Smart Anything REFerence ontology”, which enables better integration of semantic data from various vertical domains in the IoT arena

The SAREF model remains at a higher level addressing only the semantics for smart appliances data management. On the other hand, there are also numerous market-based implementations available to support the end-to-end integration of smart building assets. The main interest is about the different means of IoT devices communication with cloud platforms taking into account the type of devices, network conditions, and specific requirements of the IoT application. An overview of the common IoT-to-cloud communication protocols [15] and data collection methods is presented below:

- MQTT (Message Queuing Telemetry Transport) as a lightweight and efficient publish/subscribe messaging protocol. Widely used for IoT applications where low bandwidth and low power consumption are crucial. Suitable for scenarios with intermittent connectivity. Key features are the Minimal overhead, QoS (Quality of Service) levels for message delivery assurance, and support for lightweight clients.
- CoAP (Constrained Application Protocol) is designed for resource-constrained devices and networks. It is ideal for IoT devices with limited processing power and memory. Commonly used in constrained environments such as industrial automation and smart energy applications. Key features are the lightweight use, RESTful, and supports UDP for communication.
- HTTP/HTTPS (Hypertext Transfer Protocol/Secure) as the standard web protocols widely used for communication between IoT devices and cloud servers. It is suitable for scenarios where devices can handle the overhead of HTTP and require a more traditional web communication approach. Key features are the familiarity and well-support, support of request/response model (i.e., REST/JSON applications), secure communication with HTTPS.
- AMQP (Advanced Message Queuing Protocol): as another messaging protocol for message-oriented middleware. Suitable for scenarios requiring reliable message delivery and queuing. Often used in industrial automation and enterprise IoT applications. Key features are the support of multiple messaging patterns, such as publish/subscribe and request/response.
- DDS (Data Distribution Service): as a middleware protocol for real-time and scalable data communication. Common in applications that require low-latency, high-throughput communication, such as industrial automation and healthcare. Features: Publish/subscribe model, support for real-time data, and Quality of Service (QoS) settings.
- WebSockets is a full-duplex communication over a single, long-lived connection (as supported by OCPP mentioned above) Suitable for applications requiring low-latency communication and real-time updates. Features: Bidirectional

communication, low overhead, suitable for scenarios where devices need to push data to the cloud.

- LwM2M (Lightweight M2M) as the lightweight protocol for device management and communication. Supported by IPSO alliance is designed for managing device lifecycle (bootstrap, registration, reporting) and communication in IoT applications. Features: RESTful communication, efficient data representation, and device management capabilities.

We presented above the details about the information and communication aspects to be considered for data exchange in eFORT project. Apart from the information exchange analysis, special interest is about the definition of security and privacy preservation mechanisms to be considered for data exchange with the physical assets. Towards this direction, the state-of-the-art analysis is provided in the following section.

2.1.3 Data Security and Privacy for grid related assets

In relation to the standardization work presented above in section 2.1.1, the review of relevant aspects in terms of security (with focus on cyber security) and privacy are presented. An overview of the industry relevant standards is provided through the relevant IEC map[2]. As presented in the map but also in figure below (Figure 11), there is a core standardization effort (IEC 62351) in the domain of grid level fields devices integration. A series of standards have been defined under IEC 62351 family [16] in order to cover the security related aspects specifically for the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series as elicitated also in the analysis in section 2.1.1.

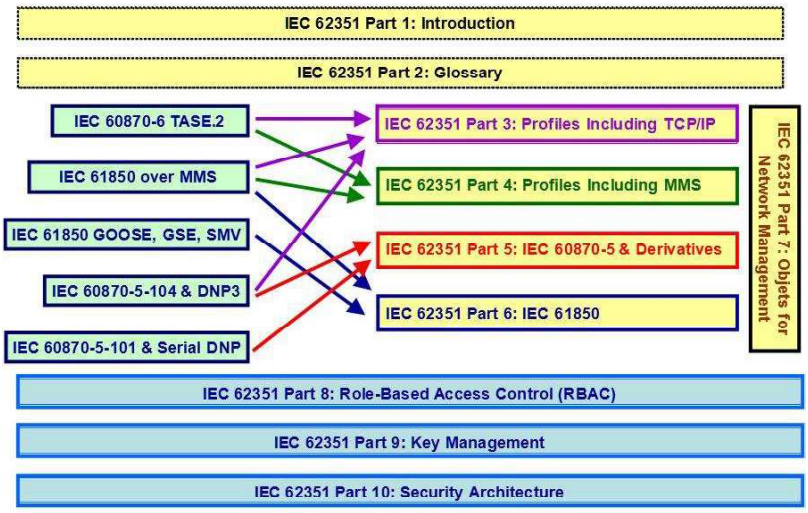

Figure 11 Mapping of IEC standards to IEC 62351

[2] https://mapping.iec.ch/#/maps/10

Another viewpoint of the different standards of IEC 62351 is presented below in order to show the level of application of the different principles.

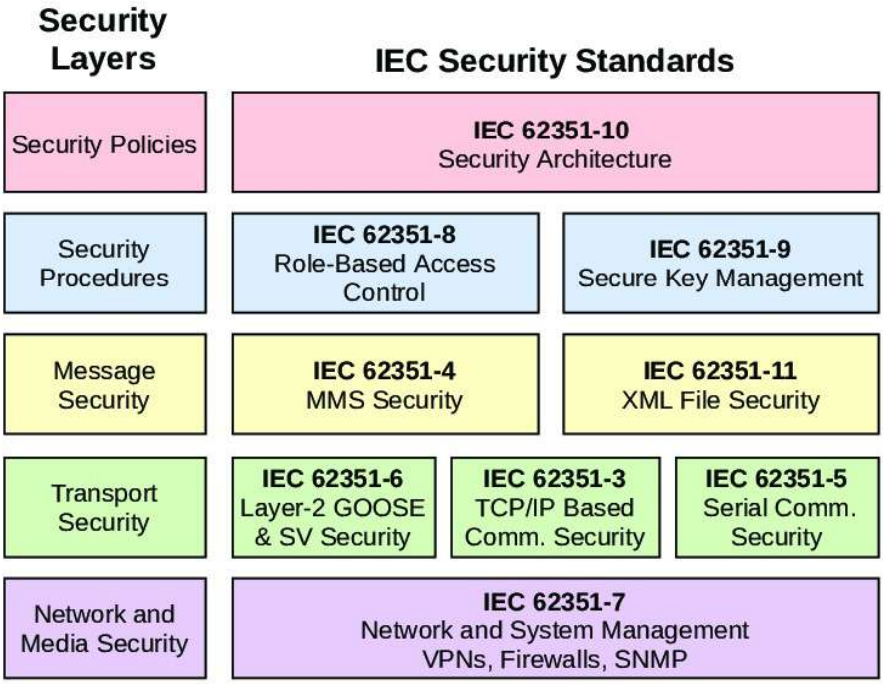

Figure 12 IEC 62351 security layers overview

The main focus in this task is about the transport and information layer analysis in order to ensure the prompt data security over the data collected from grid level/substation level assets. The security measures specified in IEC 62351 address various aspects of security, including:

- Access Control: IEC 62351 defines access control mechanisms to restrict unauthorized access to components and data. This involves user authentication, authorization, and role-based access control (RBAC) and is related mainly to the privacy of data. More details presented below.
- Data Security: IEC 62351 defines data security measures to protect sensitive IACS data from unauthorized access, modification, or disclosure. This includes data encryption, data integrity protection, and data loss prevention (DLP).
- Cryptographic Key Management: IEC 62351 outlines secure key management practices to protect cryptographic keys used for encryption and digital signatures. This includes key generation, storage, distribution, usage, and revocation.
- Security Management: IEC 62351 provides a framework for implementing security management practices, including risk assessment, incident response,

and continuous monitoring. It also emphasizes the importance of training and awareness programs for the relevant personnel.

There are additional measurements defined considering:

- Network Security[3]: IEC 62351 outlines network security measures to protect IACS networks from unauthorized access, data interception, and Denial-of-Service (DoS) attacks. This includes network segmentation, firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). Also IEC 62351 recommends using secure communication protocols, such as Transport Layer Security (TLS) or IPsec, to encrypt and authenticate data transmitted over networks.
- Device Security: IEC 62351 addresses device security by specifying secure device configurations, secure firmware updates, and secure communication protocols. It also promotes device hardening techniques to minimize vulnerabilities.

Special remark in this analysis in 62351-4 [17] and 62351-6 [18] as the relevant with IEC 61850 related assets as close to the project activities. Starting with the IEC 62351-4, the standard specifies requirements and provides guidelines for securing the communication protocols used in power systems. The key details covered within IEC 62351-4:

- Security Mechanisms: It defines various security measures and mechanisms to ensure the integrity, authenticity, and confidentiality of communication between different devices and components within power systems.
- Message Integrity: Ensures that data transmitted between devices remains unchanged and uncorrupted during transmission.
- Authentication Mechanisms: Specifies methods to authenticate the identity of devices and users participating in the communication process, preventing unauthorized access.
- Encryption: Addresses encryption techniques to protect sensitive data from being accessed or intercepted by unauthorized entities.
- Digital Signatures: Describes how to use digital signatures to verify the authenticity and origin of transmitted data.
- Security Management: Guidelines for managing security-related aspects, such as establishing policies, managing keys, and implementing security updates or patches.

---

[3] More details about network and device level security are provided in T2.6 and be reported in D2.4.

- Network and System Architecture Security: Recommendations for designing secure network and system architectures for power systems.
- Protection Against Cyber Threats: Addresses various cyber threats such as denial-of-service attacks, man-in-the-middle attacks, and other potential vulnerabilities.
- Interoperability and Compatibility: Ensures that the security measures do not hinder the interoperability of devices and systems complying with the standard.

IEC 62351-6 is an international standard for securing the operation of all protocols based on or derived from the IEC 61850 series. It specifies messages, procedures, and algorithms for securing communication between devices in a substation automation system (SAS) or telecontrol system. The goal of this standard is to enable interoperability by providing a standard method of testing protocol implementations, but it does not guarantee the full interoperability of devices. IEC 62351-6 details the following security measures:

- Authentication: This ensures that users are correctly identified and verified as authorized before accessing the system.
- Confidentiality: This protects data from being read or accessed by unauthorized individuals.
- Integrity: This ensures that data remains accurate and unaltered from its original state, protecting it from unauthorized modification.
- Non-repudiation: This ensures that the sender of a message cannot deny sending it.

The standard mandates robust methods for generating, distributing, storing, and retiring cryptographic keys, and it prescribes the use of approved cryptographic algorithms to ensure the security of data. From the different security related measurements defined above, special reference to the cryptographic algorithms specified in IEC 62351 standards. The cryptographic algorithms specified in IEC 62351 vary depending on the specific part of the standard, as the suite encompasses a range of security mechanisms for industrial automation and control systems. Namely, for the standards elicitated above, we have:

- IEC 62351-4 (Application Layer Security for IEC 61850):
    - AES-CCM: Symmetric-key encryption algorithm for MMS messages. NIST SP 800-38, Recommendation for Block Cipher Modes of Operation: Advanced Encryption Standard (AES)
    - ECDSA: An asymmetric-key signature algorithm used for MMS messages, compliant with FIPS PUB 186-4, the Digital Signature Standard (DSS).
    - HMAC-SHA-256: A Message authentication code (MAC) algorithm for MMS messages: FIPS PUB 198-A, The Keyed-Hash Message Authentication Code (HMAC)

  - RSA: Asymmetric-key encryption and signature algorithm for MMS messages and IEC 62351-9 certificates. PKCS #1, RSA Cryptography Standard
  - SHA-256: Hash function for generating message digests: FIPS PUB 180-4, Secure Hash Standard (SHS)
- IEC 62351-6 (Security for IEC 61850 GOOSE and SV Messages):
  - AES-CCM: This is a symmetric-key encryption algorithm that is used to encrypt and decrypt GOOSE and Sampled Value (SV) messages. AES-CCM is a well-established and widely used algorithm that provides strong confidentiality and integrity protection.
  - ECDSA: This is an asymmetric-key signature algorithm that is used to sign GOOSE and SV messages. ECDSA provides strong non-repudiation protection.
  - HMAC-SHA-256: This is a message authentication code (MAC) algorithm that is used to authenticate GOOSE and SV messages. HMAC-SHA-256 provides strong integrity protection.
  - RSA: This is an asymmetric-key encryption and signature algorithm that is used to encrypt and decrypt MMS messages, and to sign IEC 62351-9 certificates. RSA is a well-established and widely used algorithm that provides strong confidentiality, integrity, and non-repudiation protection.
  - SHA-256: This is a hash function that is used to generate message digests which are used to verify message integrity and generate digital signatures. SHA-256 is a well-established and widely used hash function that provides strong collision resistance.

Overall, IEC 62351 utilizes the following cryptographic concepts [20] in order to enhance the security of the data transmitted:

- Digital signatures: Used to ensure the integrity and authenticity of messages, preventing tampering or modification during transmission or storage. Digital signatures are generated using asymmetric-key cryptography, such as ECDSA, and verified using the corresponding public key.
- Public-key cryptography: Used to securely exchange encryption keys and digital signatures
- Message authentication codes (MACs): This ensures that data has not been tampered with or modified during transmission or storage. MACs are generated using symmetric-key cryptography and verified using the shared secret key.
- Hash functions: Used to generate unique message digests for integrity verification and digital signature algorithms

As the use of cryptographic concepts is of utmost importance in the domain IEC 62351, outlines secure key management practices to safeguard these keys from unauthorized access, modification, or disclosure, namely:

- Key Generation:

- Secure random number generator (RNG): IEC 62351 recommends using a strong and certified RNG to generate random keys with high entropy. This ensures that keys are unpredictable and resistant to brute-force attacks.
- Key length and algorithms: IEC 62351 specifies appropriate key lengths and algorithms for different cryptographic applications. For example, RSA keys should be at least 2048 bits long, while AES keys should be at least 128 bits long.

- Key Storage:
  - Secure key storage devices: IEC 62351 mandates storing cryptographic keys in secure hardware devices, such as tamper-resistant modules (TRMs) or hardware security modules (HSMs). These devices provide physical protection against unauthorized access and tampering.
  - Encrypted key storage: IEC 62351 recommends encrypting keys when stored in software or transmitted over networks. This adds an extra layer of security to protect keys from unauthorized access or disclosure.
- Key Distribution:
  - Secure key exchange protocols: IEC 62351 specifies secure key exchange protocols, such as Diffie-Hellman or Elliptic Curve Diffie-Hellman (ECDHE), to securely exchange keys between parties. These protocols protect keys from interception and eavesdropping during transmission.
  - Limited key distribution: IEC 62351 emphasizes the importance of limiting key distribution to authorized individuals and systems. This reduces the risk of unauthorized access, misuse, or disclosure of keys.
- Key Usage and Revocation:
  - Key rotation: IEC 62351 recommends rotating keys periodically to reduce the risk of key compromise. This involves generating new keys and replacing old keys.
  - Key revocation: IEC 62351 mandates revoking keys when they are suspected of being compromised or no longer needed. This prevents unauthorized use of compromised keys and protects the integrity of cryptographic operations.
- Key Management Infrastructure:
  - Key management center (KMC): IEC 62351 recommends implementing a KMC to manage the lifecycle of cryptographic keys. A KMC provides centralized control over key generation, storage, distribution, rotation, and revocation.
  - Access control and auditing: IEC 62351 mandates enforcing strict access controls and implementing auditing mechanisms for key

management operations. This ensures that only authorized individuals can manage keys and tracks key usage for accountability.

Apart from secure data communication, the secure data storage is a crucial aspect of cybersecurity, especially in sensitive grid assets related information IEC 62351 addresses secure data storage through various measures to protect the confidentiality, integrity, and availability of critical data.

- Use of secure hardware devices: IEC 62351 recommends using secure hardware devices, such as tamper-resistant modules (TRMs) or hardware security modules (HSMs), to store sensitive data. These devices provide physical protection against unauthorized access and tampering. More details about the usage of TPM are provided below.
- Encrypt data at rest: IEC 62351 mandates encrypting sensitive data at rest, even when stored on secure hardware devices, ensuring that data remains protected even if the device is physically compromised.
- Control access to storage devices: IEC 62351 emphasizes the importance of controlling access to storage devices through physical security measures, such as access control lists (ACLs) and multi-factor authentication (MFA).

In addition, best Secure Data Storage Practices and Measures are defined as part of the IEC 62351 standardization:

- Data storage minimization: IEC 62351 recommends minimizing the amount of sensitive data stored on devices and systems, reducing the attack surface and potential impact of data breaches. Deduplication techniques, such as cross-user data deduplication, may be considered to minimize the amount of stored data.
- Implement data classification: IEC 62351 suggests classifying data based on its sensitivity level to determine appropriate storage and access controls. This ensures that the most sensitive data receives the highest level of protection.
- Regularly back up data: IEC 62351 mandates regularly backing up sensitive data to prevent data loss due to hardware failures, cyberattacks, or other incidents. Backups should be stored in a secure and separate location.
- Data integrity verification: IEC 62351 recommends implementing data integrity verification mechanisms, such as checksums or digital signatures, to ensure that data has not been tampered with while in storage.
- Data erasure procedures: IEC 62351 emphasizes the importance of proper data erasure procedures when disposing of or decommissioning devices or storage media. This ensures that sensitive data is securely erased and cannot be recovered.
- Physical security measures: IEC 62351 mandates implementing physical security measures to protect storage devices and systems from unauthorized access, tampering, or damage. This includes physical barriers, surveillance systems, and access control protocols.

By implementing the secure data storage practices outlined in IEC 62351, organizations can safeguard sensitive information and maintain the confidentiality, integrity, and availability of critical data in their infrastructures.

On the other hand, data access control [19] (as also mentioned above) is a critical cybersecurity measure to restrict unauthorized access to sensitive information and thus enhance the privacy of the data as it aims to

- Protect sensitive data from unauthorized access: Data access control mechanisms restrict access to sensitive data based on user roles and permissions, preventing unauthorized individuals from gaining access to confidential information.
- Minimize the risk of data breaches and leaks: Data access control measures help identify and prevent unauthorized access attempts, reducing the likelihood of data breaches or leaks that could expose sensitive information.
- Ensure data integrity and availability: Data access control mechanisms protect data from unauthorized modification or deletion, ensuring the integrity and availability of critical information.

IEC 62351 emphasizes the importance of data access control and outlines various techniques to implement it effectively in a dedicated 62351-8 [19] standard, namely:

- User authentication: Verify the identity of users attempting to access data using robust authentication mechanisms, such as passwords, multi-factor authentication (MFA), or digital certificates.
- Authorization: Grant users access to specific data based on their roles and responsibilities, ensuring that only authorized individuals can access the information they need.
- Access control lists (ACLs): Define access rules for specific users or groups, explicitly granting or denying access to particular data resources.
- Role-based access control (RBAC): Assign access permissions based on user roles, simplifying access management and ensuring that users have access to the data they need to perform their tasks.
- Attribute-based access control (ABAC): Grant access based on attributes of the user, the data, or the current context, providing more granular control over access decisions.

The above methods and software-based techniques are critical for enhancing the security of data transfer. As marked, the use of secure hardware modules is also encouraged in order to enhance the security of the system components. This is the case of Trusted Platform Modules [21] (TPM) as hardware-based security components that provide a secure foundation for various security-related functions in computing devices. TPMs are typically integrated into the motherboard of a computer or added as a separate module in order to serve the different security functions such as:

- Secure Storage: TPMs can securely store cryptographic keys, passwords, and other sensitive information, protecting them from software-based attacks.

- Secure Boot: TPMs help ensure the integrity of the boot process by verifying the boot components, thereby preventing the loading of malicious or unauthorized code during the boot sequence.
- Attestation: TPMs can provide evidence (attestation) about the system's state, helping external entities verify that the system is in a trusted and secure state.
- Key Generation and Management: TPMs generate and manage cryptographic keys within the hardware, making it difficult for attackers to access or manipulate these keys.
- Platform Integrity: TPMs help ensure the integrity of the computing platform by detecting and preventing unauthorized changes to the system's configuration or software.
- Secure Communication: TPMs support secure communication protocols, allowing secure data exchange between the TPM and other system components.
- Encryption and Decryption: TPMs can assist in encryption and decryption processes, adding an extra layer of security to data.
- Device Identity: TPMs can be used to establish and manage the identity of a device, contributing to secure authentication and authorization processes.

TPMs are designed to protect user privacy by securely managing keys and sensitive data, preventing unauthorized access. TPMs play a crucial role in enhancing the overall security of computing devices and are commonly used in enterprise environments, secure systems, and platforms where data protection and system integrity are paramount. As highlighted in the DoA, the TPM approach will be considered for the remote attestation of the critical device. Remote attestation using a Trusted Platform Module (TPM) is a security feature that allows a remote party to verify the integrity and configuration of a computing platform. This process involves the TPM generating a signed attestation, which is a cryptographic proof that vouches for the system's state without disclosing sensitive information. In the following we provide a brief overview of how remote attestation with TPM works.

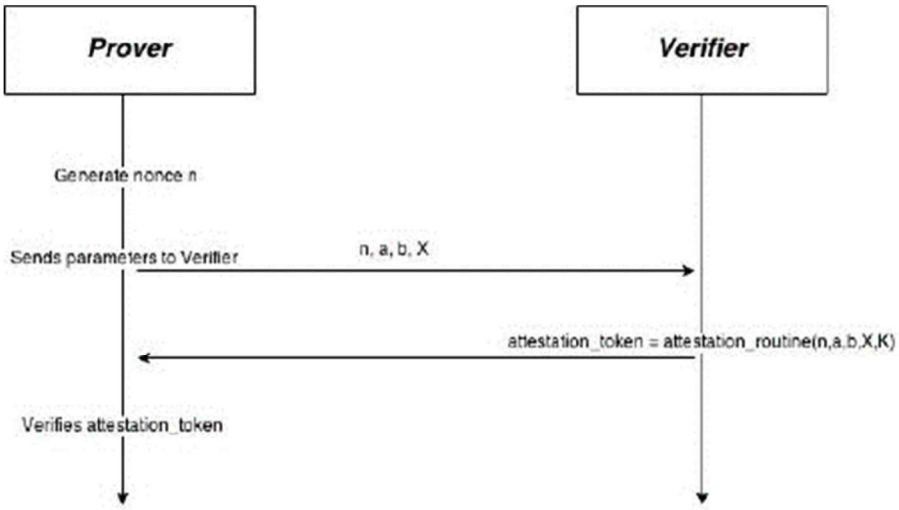

Figure 13 Remote attestation protocol overview

In brief,

- To initiate remote attestation, a remote party (verifier) sends a challenge to the local TPM. The challenge is a random value that the TPM uses to compute a response.
- The TPM combines the challenge with its internal state to generate a response, often called a "quote." This response includes the measurements and a signature generated by the TPM using its AIK.
- The quote is sent to the verifier, typically over a secure channel, ensuring confidentiality and integrity during transmission. The verifier, which can be a remote server or another device, verifies the authenticity of the attestation by checking the signature using the TPM's public key (corresponding to the AIK).

Based on the attestation results, the verifier can make policy decisions, such as granting access to certain resources or denying access if the system is not in a trusted state.

We present above a non-exhaustive list of security and privacy preservation mechanisms that apply according to the relevant specifications. In the following we provide the specifications for IoT/ DER assets.

2.1.4 Data Security and Privacy at IoT/ DER Level

Similar to the review of the different security/privacy preservation mechanisms that are considered for network level assets, the same analysis applies for the data collection methods defined for IoT/ DER Level.

Starting with the SunSpec/MODBUS data model the, *the mission of the SunSpec / Sandia DER Cybersecurity Work Group is to support the deployment of Distributed Energy Resources (DER) by defining best practices in cybersecurity for DER and driving the concepts that emerge from these best practices into relevant national and international standards.*

A series of specifications ([22][23][24]) have been defined by the alliance and a brief overview of them which are relevant to eFORT project is provided:

- TLS 1.2 encryption: This ensures that DER data is encrypted while in transit, protecting it from interception and eavesdropping.
- Message authentication code (MAC): This provides data integrity verification, ensuring that DER data has not been tampered with during transmission. The SunSpec Secure Modbus protocol uses the HMAC-SHA-256 algorithm to generate a MAC for enhancing the transfer of data.
- Client authentication: This verifies the identity of the client device requesting data from the DER device, preventing unauthorized access.

The SunSpec Secure RESTful Web Service provides a standardized interface for secure data exchange between DER devices and other applications. This interface supports HTTPS to ensure that DER data is encrypted while in transit using the HTTPS protocol and JSON Web Tokens (JWTs) used to authenticate clients and authorize access to DER data. In addition, Role-based access control (RBAC) is supported by SunSpec specifications to restrict access to DER data based on the role of the user or application.

In addition, the SunSpec Alliance has developed a set of data privacy principles to help ensure that DER data is protected. These principles include:

- Data minimization: DER data should only be collected and stored if it is necessary for a specific purpose.
- Data access control: DER data should only be accessed by authorized users. Access to DER data should be controlled using role-based access control (RBAC).
- Data anonymization: DER data can be anonymized to remove personally identifiable information (PII).

Overall, the core principles of the industry are supported by SunSpec Alliance for data security and privacy.

A very important standard in the field as named above is OCPP for EV Charging points management. Special emphasis is delivered also on security related aspects as specified in OCPP reference documentation. We have to point out that security enhancements were made available in the 2.0 version of the standard (OCPP 2.0.1 supports three security profiles). Overall, the security Functional Block was designed to fit into the approach taken in OCPP[25]. No application layer security measures are included. Based on these considerations, OCPP security is based on TLS and public key cryptography using X.509 certificates:

- Unsecured Transport with Basic Authentication: The Unsecured Transport with Basic Authentication profile provides a low level of security. Charging Station authentication is done through a username and password. No measures are included to secure the communication channel
- TLS with Basic Authentication: In the TLS with Basic Authentication profile, the communication channel is secured using Transport Layer Security (TLS). The

CSMS authenticates itself using a TLS server certificate. The Charging Stations authenticate themselves using HTTP Basic Authentication.

- TLS with Client-Side Certificates: In the TLS with Client-Side Certificates profile, the communication channel is secured using Transport Layer Security (TLS). Both the Charging Station and CSMS authenticate themselves using certificates.

In the field of users' authorization, OCPP protocol describes all the authorization-related functionalities at EV charging level; it contains different ways of authorizing a user, online and/or offline. Where OCPP 1.x only supported RFID, OCPP now also supports things like: credit card, PIN-code, a simple start button etc. While complex authorization process applies at the CP level this is not the case at the CSMS level. Because the CSMS usually acts as the server, different users or role-based access control on the Charging Station are not implemented in the standard. To mitigate this, it is recommended to implement access control on the CSMS.

In terms of data privacy, similar principles are considered also in OCPP documentation. In short, the Open Charge Alliance (OCA) has developed a set of data privacy principles to guide the handling of OCPP data:

- Purpose Specification: Clearly define the purpose for collecting and using OCPP data, ensuring it is necessary and proportionate to the intended use.
- Data Minimization: Collect and store only the data necessary for the specified purpose, avoiding unnecessary data collection and retention.
- Data Access Control: Implement role-based access control (RBAC) to restrict access to OCPP data based on authorized roles and responsibilities.
- Data Integrity: Protect OCPP data from unauthorized modification or tampering using cryptographic techniques and data validation procedures.
- Data Anonymization: Anonymize OCPP data to remove personally identifiable information (PII) when not necessary for the intended purpose.

When it comes to building IoT devices integration, we have elicitated HTTPS based data integration (through REST/JSON services) as well as MQTT for real time data streaming. For HTTPs based application the enhancement of security and privacy over the data is mature (as very widespread approach in different applications and domains) and some reference to the best practices were mentioned above as part of the SunSpec documentation. Therefore, in short, we present some security (and privacy preservation) related principles in order to enhance MQTT based communication (as defined in MQTT Security Model [26]):

- Use of TLS to encrypt the communication between MQTT clients and brokers. This ensures that data in transit is secure. Configuration of the MQTT broker to support secure connections, and ensure clients use TLS for encryption.
- In addition, encryption of the payload of MQTT messages, especially if it contains sensitive information. MQTT payload encryption solves the problem of protecting application messages from malicious listeners or untrusted MQTT clients.

- Enforce strong authentication for MQTT clients to verify their identities. Use mechanisms like username/password combinations, client certificates, or other secure authentication methods.
- MQTT brokers should authenticate clients before allowing them to connect.
- Implement access control lists (ACLs) to specify which clients are allowed to publish or subscribe to specific topics. Implement fine-grained access control to restrict clients' access to specific topics or actions. Define and enforce policies that determine which clients can publish or subscribe to particular topics.
- Careful management of MQTT sessions to control the state and duration of client connections. Configuration of appropriate session timeouts and consider using persistent sessions based on your application's needs.
- Set of appropriate keepalive and timeout values to manage the lifecycle of MQTT connections.

We presented above, the key security principles as defined in the relevant standardization as examined in the project. Before proceeding with data exchange specifications definition, an overview of the data landscape in the eFORT project is provided in the following section.

2.2 Data Collection and sharing – Demonstration Landscape

Apart from the state of the analysis towards the different data gathering and collection methods (as well as the security/privacy mechanisms that needs to be considered for data management and exchange), the analysis of project specific demo scenarios is required. For that reason, a detailed analysis of the different assets (and the associated data gathering methods as well as data collection characteristics) available at the demo sites of the project is required. In order to do so, an enhanced analysis of the available data at the demonstrators was performed utilizing the template.

						Data Asset Availability		
Dataset ID	Data Asset Title	Temporal Coverage	Relevant Standards	Temporal Resolution	Spatial Resolution	Accessibility Method	Frequency of Updates	Docum
[Unique identifier following the convention "Country#no"]	*The title of the data asset*	*[From ... To...]*	*[List the international standards to which a data asset complies]*	*[The temporal "granularity" of the data, e.g. per minute / hour / day / month]*	*[The spatial "granularity" of the data, e.g. at district / zone / building / area level]*	*[Through API, As downloadable file, As database extract, Other]*	*[Real-time, Every X minutes / hours, Daily, Weekly, Monthly, Yearly, other]*	*docume the AP sample for the pla*
ES01	SM_01	From 2022 to present	PLC Protocol	per hour	per building/asset	Through FTP	Daily	Protoc specif
ES02	SM_02	From 2022 to present	PLC Protocol	per hour	per building/asset	Through FTP	Daily	Protoc specif
ES03	SM_03	Daily	Modbus, IEC 60870-5 104	5-minutes	per building/asset	Through API	Every 5 minutes	Docum

Figure 14 Demonstration Landscape template

The details of the key categories of the template are then provided in brief:

- Data Assets Description: Providing the typology and a short description of the assets made available per demo site
  - Dataset ID: A unique ID for each dataset
  - Dataset Title: A unique title for each dataset

    - Description: A short description of the dataset
- Data Asset Features: Providing details about the volume of the data as well spatial and temporal granularity related aspects
    - Volume: A data size estimation ([X GBs / records / transactions per hour / day / month / in total])
    - Variety: Estimation of the data structure ([Structured / Unstructured / Semi-structured])
    - Velocity: Refers to the speed in which data is generated, distributed and collected ([Real-time, Near Real-time, Batch])
    - Temporal Coverage/Resolution: Refers to the temporal characteristics of the data asset and the time granularity level
    - Spatial Resolution: Refers to the spatial granularity of the data, e.g. at district / zone / building / area level
    - Type/Format: Refers to the specific format to handle the data
    - Relevant Standard: List the international standards to which a data asset complies
- Data Asset Availability: Providing details about the means of data integration, focusing on communication protocols and information model related details
    - Accessibility Method: The way to access the data from the physical assets, i.e. through API, as downloadable file, as database extract
    - Frequency of Updates: i.e. Real-time, Every X minutes / hours, Daily, Weekly, Monthly, Yearly, other
- Data Asset Rights: Providing details about the means of data protection, specifying the details about security and privacy over the data
    - License: The license details for the dataset e.g. CC Attribution-NonCommercial-ShareAlike (CC BY-NC-SA), or Case-by-Case Bilateral Agreement
    - Access Level/ License: The specifications about access level over the dataset and license details, i.e. Derivation, Reproduction, Share Alike, Offline Retention, Attribution, Distribution level
    - Encryption Details: Type of encryption required over the data
    - Anonymization Details: Type of anonymization required depending on whether the data asset contains sensitive or personal data

In the following, a short overview of each demo site of the project is provided, and then the data collection details (as specified above) are listed.

2.2.1 Demonstration in Spain

The distribution network in the village of Escúzar serves as the demo-site to validate the demonstration at both the microgrid and end-user levels. This area has 450 supply

points and a peak load close to 0.55 MW, the LV distribution grid serves mostly residential consumers and near the village there are 2 PV plants of 4 MW and 1.8 MW each one connected to the MV grid. In the area there are also deployed 28 residential households with self-generation (3 kW each one), 1 household with a private EV charger (7,4 kW) + self-generation (3 kW), 5 households with a control of the water boiler and 5 households with a control of the HVAC that have been considered in the scope of the eFORT project. Also, a public EV fast charger of 22 kW is available in the town and is projected the deployment for V2G chargers in some households. Various asset types (IoT/DER), as described in Section 2.1, are available for the demo activities at the ES demo site. Details of these assets are provided in the following table.

Table 1 ES Demonstration – Data Description

Dataset ID	Data Asset Title	Description	Volume
[Unique identifier following the convention "Country#no"]	*The title of the data asset*	*A brief description of the data asset - At least 2-3 lines to give an overview of the data*	*[X GBs / records / transactions per hour / day / month / in total]*
ES01	SM_01	smart meter data from consumers	Hourly demand data for each consumer. This means, for each consumer it will be: 1SM/25 rows/9 columns/per day All SM/ 867 KB per day/ 297 MB per year
ES02	SM_02	smart meter data from generation	Hourly demand data for each consumer. This means, for each prosumer it will be: 1SM/25 rows/9 columns/per day All SM/ 867 KB per day/ 297 MB per year
ES03	SM_03	DER counter	Approx. (10404 KB per day / 3,564 GBs per year)
ES04	EV_01	private EV Charger	Approx. (10404 KB per day / 3,564 GBs per year)
ES05	EV_02	public EV Charger	Approx. (10404 KB per day / 3,564 GBs per year)
ES06	PV_01	local PV generation	Approx. (10404 KB per day / 3,564 GBs per year)
ES07	IOT_01	Water Boiler Data	Approx. ~ 100 KB per day
ES08	IOT_02	HVAC Data	Approx. ~ 100 KB per day

Additional details for the data structure as well as the temporal and spatial characteristics are made available through the landscape analysis. In addition, information about the accessibility method is also reported in the following table.

Table 2 ES Demonstration – Data Features

Dataset ID	Format	Velocity	Temporal Coverage	Relevant Standards	Temporal Resolution	Spatial Resolution	Accessibility Method	Frequency of Updates
[Unique identifier following the convention "Country#no"]	*[csv, xml, json, other]*	*[Real-time, Near Real-time, Batch]*	*[From ... To...]*	*[List the international standards to which a data asset complies]*	*[The temporal "granularity" of the data, e.g. per minute / hour / day / month]*	*[The spatial "granularity" of the data, e.g. at district / zone / building / area level]*	*[Through API, As downloadable file, As database extract, Other]*	*[Real-time, Every X minutes / hours, Daily, Weekly, Monthly, Yearly, other]*
ES01	JSON	Batch	From 2022 to present	PLC Protocol	per hour	per building/asset	Through FTP	Daily
ES02	JSON	Batch	From 2022 to present	PLC Protocol	per hour	per building/asset	Through FTP	Daily
ES03	JSON	Near Real-time	Daily	Modbus, IEC 60870-5 104	5-minutes	per building/asset	Through API	Every 5 minutes
ES04	JSON	Near Real-time	Daily	Modbus, IEC 60870-5 104	5-minutes	per building/asset	Through API	Every 5 minutes
ES05	JSON	Near Real-time	Daily	Modbus, IEC 60870-5 104	5-minutes	per building/asset	Through API	Every 5 minutes
ES06	JSON	Near Real-time	Daily	Modbus, IEC 60870-5 104	5-minutes	per building/asset	Through API	Every 5 minutes
ES07	JSON	Near Real-time	Daily	Proprietary	5-minutes	per building/asset	Through API	Every 5 minutes
ES08	JSON	Near Real-time	Daily	Proprietary	5-minutes	per building/asset	Through API	Every 5 minutes

On the other hand, and at the DSO level, the Escúzar electrical substation, built in 2008, will be also used as a complementary demo-site to validate digital substation developments. It currently has two 30 MVA transformers operated at 66/20 kV. The 66 kV voltage is currently provided by ENDESA from the Híjar Border Point. It has two 20 kV bars with a total of 14 output lines (7 per bar), which provide electricity to different municipalities and the Profitegra industrial estate. The substation is undergoing expansion to include a new 132/66 kV position owned by CUERVA, which has a direct connection to Red Eléctrica (TSO) at 220 kV.

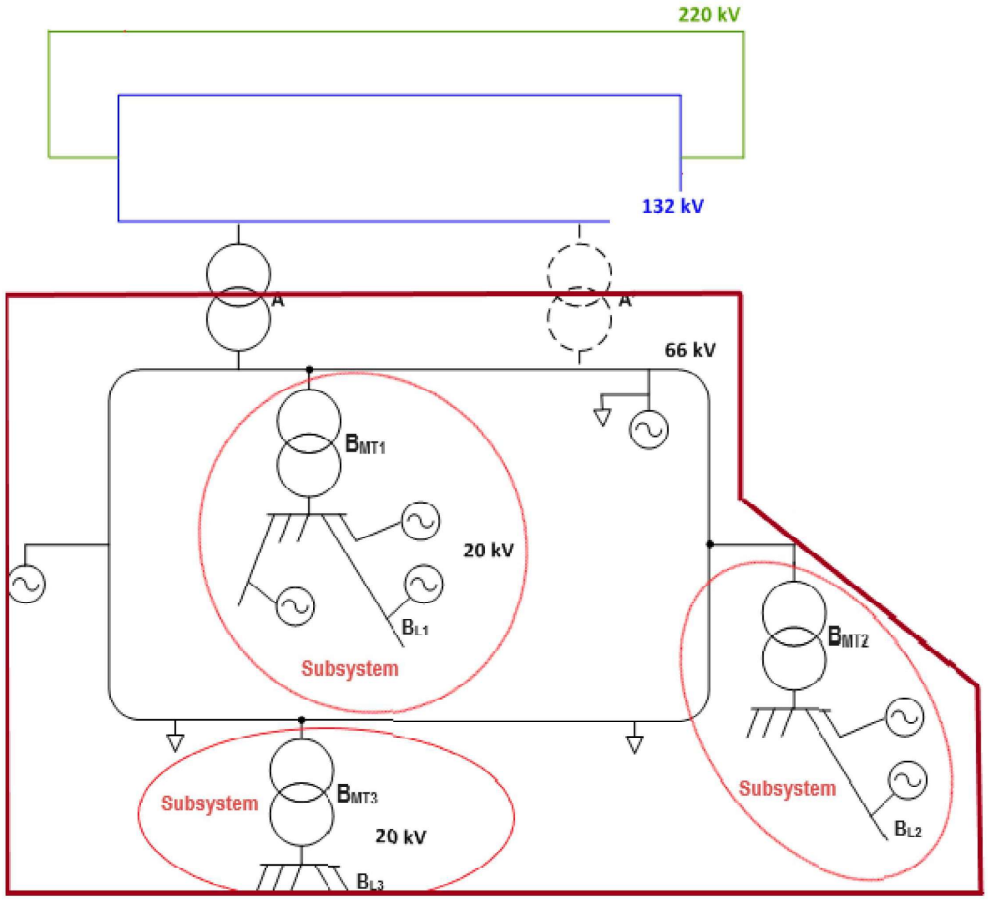

Figure 15 Indicative schema of Escúzar electrical substation

In addition, one of the main elements of the Electric Distribution Network is the Substation Automation System (SAS) which is a mission-critical task that allows to control and monitor the electric infrastructure. Gateways, controllers, protections relays, RTUs, etc., enclose serial and Ethernet communications by relying on industrial protocols, providing data logging capabilities, analogic and digital inputs/outputs, among other functions. These devices send real-time data in a reliable way to the SCADA so the operators would have an updated and accurate information on the status of the grids. An early estimation for the Escúzar electrical substation is few MBs (~5 MB) per day considering the number of input devices to be monitored as well as the sampling rates considered for data gathering (second level for the case of Escúzar electrical substation)

SCHN is going to provide a Remote Terminal Unit from PowerLogic T300 family for the Spanish demonstration. The RTU is an embedded device able to measure real-time information from the electric grid, and able to transfer it to either grid operators, or other elements of the eFORT architecture. The RTU selected for Cuerva substation, is able to monitor both the Medium Voltage and Low Voltage grid, being able to provide parameters like voltages, currents, power, or frequency, among others. Collected measurements, as well as other signals coming from other devices, can be exchanged by using industrial communication protocols like Modbus, IEC 60870-5-101/104, or protocols based on IEC 61850 standard. This is totally in line with the specifications of

eFORT project and the protocols to be supported by the SecureBox to be delivered in the project.

In addition, security and privacy related aspects over the data are specified by the demo partners. Considering the criticality of the data from the RTU/SCADA as well as the IoT devices that will be deployed at the ES demo site, these are considered as private datasets with restricted access and thus bilateral licence agreements are required for data exchange. RTU provides cybersecurity capabilities in order to protect both the data and the access to the device against non-authorized users. ABAC methods should be supported in order to ensure access over the data based on the user's roles. No specific requirements about additional encryption (apart from the default encryption that applies at communication exchange of the relevant protocol) over the data are defined at this stage, but the demo partners are interested to experiment with the data-level encryption mechanisms that are examined in the project. Last but not least, no particular need for anonymization of the data coming from RTU/SCADA as data for substations normally includes the aggregation of plenty of end users. On the other hand, IoT level data (considering also smart metering data) needs to be anonymized in order to ensure that any personal identifier has been removed from the data shared in the eFORT project.

2.2.2 Demonstration in Italy

The Italian demo site is located in Sarentino Valley in the centre of South- Tyrol, north of Bolzano (Italy). In this region EDYNA is operating as the main DSO, managing 8,608 km of network (HV, MV and LV) and supplying electric power to 230,000 customers. The pilot demonstration is going to be performed in the MV and LV grid supplied by the HV/MV Sarentino substation and consists of:

- 2x 66/20 kV transformers 25 MVA. / 5 MV feeders.
- (1 HV Hydroelectric plant 29 MVA connected to HV busbar).
- 10.4 MW of installed production in the MV and LV grid (3.6 MW hydroelectric, 2.7 MW PV and 4.1 MW thermal power generation).
- 2 local network installations connected to the MV grid, with other 10.6 MW of installed production (9.8 MW hydroelectric).
- 24.6 MW of total loads (3,000 LV and MV customers).

On the field side of the controlled smart grid, the bilateral flow of measurement and control signal for critical assets will be established though specific SELTA-DP peripherical equipment which is a Smart Grid Controller. This component plays an essential role for observability of the DSO grid and for the coordination during islanding operation mode as it allows the monitoring and the control functions. The tool interacts with SCADA system placed in the DSO control room through the private LAN. No direct interaction between SGC tool and substation/field equipment is delivered and thus it relies on the connectivity with the SCADA system in place.

From the aforementioned analysis, it is evident that the main interest is data gathering from the DSO substation level at the Italian demo site and the data landscape analysis results are provided in the following table. The data that are tracked from the Smart

Grid Controller are further made available to the eFORT project for further experimentation.

Table 3 IT Demonstration – Data Description

Dataset ID	Data Asset Title	Description	Volume
IT_01	Smart Grid Controller- Dataset 1	Measurements, estimations and load flow calculations	150 KB
IT_02	Smart Grid Controller- Dataset 2	Measurements, estimations and load flow calculations	300 KB
IT_03	Smart Grid Controller- Dataset 3	Single line diagram	85 kB
IT_04	Smart Grid Controller- Dataset 4	Feeder voltage profiles	45 kB

In addition to the high-level information as presented above, details about the spatial and temporal coverage and granularity are provided. In addition, specifications about the standards considered for information exchange are also mentioned in detail.

Table 4 IT Demonstration – Data Features

Dataset ID	Format	Velocity	Temporal Coverage	Relevant Standards	Temporal Resolution	Spatial Resolution	Accessibility Method	Frequency of Updates
IT_01	xlsx	Real time	From 2023	OPC UA	20 seconds	Primary substation subtended grid	FTP, Share point	Once a month
IT_02	HTML	Real time	From 2023	OPC UA	20 seconds	Primary substation subtended grid	FTP, Share point	Once a month
IT_03	jpeg	Batch	From 2023	OPC UA	20 seconds	Primary substation subtended grid	FTP, Share point	Once a month
IT_04	png	Batch	From 2023	OPC UA,	20 seconds	Primary substation subtended grid	FTP, Share point	Once a month

In addition, security and privacy related aspects over the data are specified by the demo partners. Considering the criticality of the data from the Smart Grid controller, these are considered as private datasets with restricted access and thus bilateral licence agreements are required for data exchange. ABAC control methods should be supported in order to ensure classified access over the data based on the user roles. No specific requirements about additional encryption (apart from the default encryption that applies at communication exchange of the relevant protocol) over the data are defined at this stage, but the demo partners are interested to experiment with the data-level encryption mechanisms that are examined in the project. Last but not least, no particular need for anonymization of the data coming from the smart grid controller as data from the grid include the aggregation of plenty of end users.

2.2.3 Demonstration in Ukraine

The demo in Ukraine consists of the substation (110/35/10 kV) related demo to guarantee the proper development and validation of the associated activities with an approach also supported by laboratory and field facilities. This substation is operated by JSC “Prykarpattyaoblenergo”, the DSO in the Ivano-Frankivsk region, which receives electricity from the United Energy System of Ukraine and from the Burshtyn Energy Island (TPP "Burshtyn"). It includes:

- Switching equipment from ABB (at 10/35/110 kV levels).
- Relay protection and automation are performed using microprocessor terminals of Kyivprilad and Hartron.
- Telemechanic equipment RTU-560 from ABB with 560 CMU-02 processor board. The substation is telemechanized by receiving status and position signals of all switching devices, and uses control commands for 110, 35 and 10 kV switches with discrete signals.
- Collection of all information from microprocessor terminals of protection 110, 35 and 10 kV are organized according on the Modbus-RTU protocol (current and voltage values, the fact of operation of certain protection or signalling stages, etc.).
- Data transfer from the substation to the SCADA system of the JSC branch is organized according to the protocol IEC60870-5-104. Between the branch and the dispatch service, the communication is performed according to the DNP 3.0 protocol.
- Data transfer from the substation to the server of the control point is performed using fibre optics and GSM.

The aforementioned high-level information is further presented in more details in the tabular form as a result of the data landscape analysis performed in the project.

Table 5 UA Demonstration – Data Description

Dataset ID	Data Asset Title	Description	Volume
UA03	SC4_DC_1	Domain Controller. Infrastructure server for authorization of dispatcher PC.	Some KBs
UA04	SC4_RTU_1	Remote Terminal Unit (RTU): to monitor the electric grid infrastructure	~ 3-5 MB/day
UA05	SC4_GC_1	Smart Grid Controller SATEK. Measurements, estimations and load flow calculations	150 KB
UA06	SC4_SCADA_1	SCADA server data from substation	~ 3-5 MB/day

UA07	SC4_SM_1	Smart meter data from substation	Hourly demand data for each consumer. This means, for each prosumer it will be: 1SM/25 rows/9 columns/per day All SM/ 867 KB per day/ 297 MB per year

In addition to the high-level information as presented above, details about the spatial and temporal coverage and granularity are provided. In addition, specifications about the standards considered for information exchange are also mentioned in detail.

Table 6 UA Demonstration – Data Features

Dataset ID	Format	Velocity	Temporal Coverage	Relevant Standards	Temporal Resolution	Spatial Resolution	Accessibility Method	Frequency of Updates
UA03	-	Real-time	Continuous	Kerberos (RFC 4757)	N/A	N/A	TCP/IP	Real-time
UA04	Other / as per the chosen communication protocols profiles	Real-time	Continuous	IEC 60255, IEC 61000, IEC 60068, IEC 60870-5-101/104, DNP3, IEC 61850, Modbus, IEC 62443, IEC 62351	Real-time, normally every few hundreds of milliseconds, or by exception	Depending on where the RTU is deployed. Normally it can monitor the electric values of a district/zone.	Through industrial communication protocols	Real-time
UA05	Text	Real time	Continuous	IEC 60255, IEC 61000, IEC 60068, IEC 60870-5-101/104, DNP3, IEC 61850, Modbus, IEC 62443, IEC 62351	20 seconds	Primary substation subtended grid	FTP, Share point	Once a month
UA06	Text	Real time	Continuous	IEC 60255, IEC 61000, IEC 60068, IEC 60870-5-101/104, DNP3, IEC 61850, Modbus, IEC 62443, IEC 62351	Real-time, normally every few hundreds of milliseconds, or by exception	Grid level selected in the project	Through industrial communication protocols	Real-time
UA07	Text	Real time	Continuous	PLC Protocol (programmable logic controller)	Per hour	Per station	Through FTP	Daily

SCHN is going to provide a Remote Terminal Unit from PowerLogic T300 family for the Ukraine demonstration. It is the same RTU than the one used for the Spanish demonstration, but without MV capabilities, as the need for this RTU in Ukraine has been to monitor the LV grid, being able to provide parameters like voltages, currents, power, or frequency, among others. Collected measurements, as well as other signals coming from other devices, can be exchanged by using the previously mentioned industrial communication protocols. Similar to the case of the Spanish demo site, the data will be collected from the SecureBox to be delivered as the eFORT gateway in the project.

In addition, security and privacy related aspects over the data are specified by the demo partners. Considering the criticality of the data from the RTU/SCADA and Smart controller, these are considered as private datasets with restricted access and thus bilateral licence agreements are required for data exchange. ABAC control methods should be supported in order to ensure classified access over the data based on the user roles. No specific requirements about additional encryption (apart from the default encryption that applies at communication exchange of the relevant protocol) over the data are defined at this stage, but the demo partners are interested to experiment with the data-level encryption mechanisms that are examined in the project. Last but not least, no particular need for anonymization of the data coming from RTU/SCADA as data for substations normally includes the aggregation of plenty of end users. On the other hand, smart metering data needs to be anonymized at source level in order to ensure that any personal identifier has been removed.

Note: It is evident that only the substation station /smart meter data is considered at the demo site in Ukraine and thus no other IoT/DER devices will be examined for the analysis performed in this section.

We presented above the specification details for data gathering from the ES, IT and UA demo site. There are no specifications provided for the NL demo site as the overall analysis and testing will be implemented on synthetic data (thus no actual integration with physical systems). The demo setup begins with a Real-Time Power System Simulation using technologies like RTDS (Real-Time Digital Simulator) and PowerFactory, which emulate the behavior of electrical power grids. These simulations feed data into Digital Substations that are integrated with real-time GPS clocks, ensuring precise synchronization and monitoring of the grid's operations on the basis of synthetic data provided from the local TSO. These substations (as modeled in the physical side) are connected via a Wide Area Network (WAN), enabling data and control signals to be transmitted to the Control Room of the Future. The overall communication is implemented using the OPC UA protocol as specified above for information exchange among the different IT/OT environments.

The Control Room for the NL demo site is defined as a high-tech environment where operators monitor the power grid in real-time. This control room is connected to an IT Network that includes various servers and workstations used for analyzing data, storing information, and facilitating communication between different components of the power system (Phasor Measurement Unit (PMU) database and SCADA (Supervisory Control and Data Acquisition) systems, which are crucial for real-time data acquisition and control in large-scale power systems). All in all, for the NL demo site, synthetic TSO data are considered for analysis while OPC UA is considered as the communication and information exchange protocol for the data exchange among the IT solution and the digital twin environment as emulated in the project. More details about the simulated TSO set up to be examined in the project will be provided in D4.1 (where the details of the Digital Twin implementation will be provided)

2.2.4 Business applications data exchange

Apart from the analysis of data acquisition from the demonstration sites (as presented above), we have to consider also the eFORT business application data exchange

needs. As the eFORT business application developments are going to consume data (or knowledge derived from the data) made available in eFORT Intelligent Platform (and vise-versa knowledge extracted from the different applications to be made available to the eFORT Intelligent Platform), we have to ensure that secure information exchange will apply between the eFORT Intelligent Platform and the eFORT business applications; these specification details are listed in the following table.

We have to point out that the analysis is performed following consultation with the business application responsible partners in order to list the data needs (as well security/privacy preservation requirements) to apply in any information exchange that is to be examined and tested in the project

Table 7 eFORT Business Applications– Information exchange Details

Software Tool	Responsible Partner	WP	Short Description	Integration Details
Vulnerabilities database and visualization tool	CERTH	WP2	A database including all the identified and characterized vulnerabilities as well as the visualization layer to visualize information regarding traffic (data packets) and overall EPES status, also depicting and localizing discovered threats in real-time	*This tool is defined as the front-end visualization tool of the SIEM engine and thus no integration requirements are defined. More details about SIEM integration are presented below.*
Dynamic Risk Assessment Tools: Physical Layer	RINA-C	WP3	Risk assessment tool to minimize and reduce service interruption; Prioritization of assets that need mitigation actions	Input data from the physical network (i.e. EPES characterization) are required to be retrieved while the output data of the RA may be stored in the eIP for further utilization
Dynamic Risk Assessment Tool: Cyber layer	COM	WP3	Estimate the risk of a given infrastructure to suffer a MaD IoT attack and provide a visualization tool for this purpose, thus contributing to increase the cybersituational awareness of the operator of the infrastructure.	Input data from the physical network (Infrastructure characterization with device model, firmware version, geolocation, consumption/generation (in .json)) set the input parameters through API. The results of the RA may be stored to the eIP for further utilization.
Islanding Operation Module	LINKS	WP3	Management of a portion of MV grid in islanding operation mode and involvement of the Distributed Energy Resources in making the grid more resilient	As this is executed in the edge device available in IT demo site, some aggregate results from the IT demo site will be made available to the eIP for further utilization
IDS (Intrusion Detection System)	CIRCE	WP3	Minimize or eliminate service interruptions caused by: - Undesired events, both physical and operational - Hidden security breaches	Running in SecureBox. Information about alarms/alerts will be sent to eIP for further utilization via API methods
SIEM for log analysis	CERTH	WP3	The SIEM gathers data logs from heterogeneous sources (including IDS) analyses and presents them harmonized, and homogeneous in the form of events: - timely detecting threats, anomalies and cyber-attacks, - perform advanced data analytics to early detect anomaly-based cyber-attack incidents	Running in different working environments to be examined in the project. Information about alarms/alerts will be made available from the eIP for further utilization.
ChatBot	LINKS	WP3	Web-based Chatbot able to collect from energy consumers valuable information such as geolocated multimedia content and able to provide to grid operators a better overview of the grid status in order to improve its management	Alerts and alarm/status information as these made available to the eIP will be retrieved from the eIP for further utilization.
Grid verification and monitoring layer by	CIRCE	WP3	Observability and tracking of the grid assets Log and consultation of inventory,	Information about the status of the grid as this defined in the app will be stored in the eIP for further utilization.

blockchain technology			operation and security events on a given asset Reduction of maintenance time and effort Enabling of remote maintenance activities	
SOAR (Reactive and preventive actions issued to the infrastructure)	TNO	WP3	Enhance option awareness allowing definition and re-use of courses of actions to (automatically) be issued to the EPES infrastructure.	API data exchange with the platform in order to support situational awareness analysis; data to be stored in the eIP for further utilization.
Development of power grid digital twins, DSS Op & Power Restoration, Self-Healing	TUD	WP4	Optimal Power Flow (OPF) solver for power system model. The algorithms are directly deployed on the demonstration site.	The results of the optimization made available to the eIP for further utilization.
Algorithms and strategies for secure grid operation modes and black start recovery	CIRCE	WP4	Delivery of the algorithms and strategies for secure grid operation modes and black start recovery in transmission and distribution grid	*No direct integration with the platform is foreseen for this application (to be tested only in test environment).*
SecureBox	CIRCE	WP4	This is the development of the edge-level software modules of the project in order to execute different on-site services	*Details about information exchange with the IP platform were presented above*

From the aforementioned analysis it is evident that there are specific applications running in the SecureBox or the eFORT Intelligent Platform and thus any data exchange information will be handled through the relevant specifications of these 2 components. From the rest of the tools/ business apps delivered in the project, any information exchange will be performed following standards and web-based methods (https-based communication via REST/JSON services) to be supported by the eFORT Intelligent Platform. Following discussion with the technical partners of the project, there are no app specific privacy or security requirements and needs about information exchange among the different business applications and thus the different tools will comply with the methods and services to be supported by the eFORT Intelligent Platform as reported in details in the following section. Special remark about authentication and users' authorization (through R/ABAC methods) in all business applications defined in the project.

2.3 Data Collection and sharing – Specifications Overview

The literature review as well as the demonstration landscape performed in the sections above are paving the way for the elicitation and further incorporation of the different data collection methods as well as the relevant data security and privacy mechanisms in eFORT tools and services, namely the Intelligent Platform (acting as the central data platform of the project *to ensure interoperability so that can be linked to different databases, services, and to different typologies of SecureBox or similar hardware units managing the data of the EPES assets*) and the SecureBox (as the edge device on the network which act as the gateway to the data communication with the eFORT Intelligent Platform).

Starting with the SecureBox, and taking into account the demo specific characteristics as well as the literature analysis, the following data integration details are considered:

- MQTT based communication for data integration with home/building level assets. Considering the deployment of smart home devices and integration of data to the SecureBox, MQTT has elicitated as the protocol to ensure smooth real time data transmission. The MQTT implementation will implement the best of breed security practices as mentioned above in order to enhance the level of security on information exchange.
- Support of MODBUS in order to enable integration with DER level assets. More specifically, integration with the inverter-based devices at generation level will be ensured. Similar to the MQTT case, the SecureBox will ensure the incorporation of the security principles of the MODBUS implementation as mentioned above.
- Support of OCPP protocol in order to support integration with the EV charging points available at the demo sites.

In addition, integration with the RTU installed at the ES/ UA premises is considered for the project needs. The details of the data attributes to be reported per demo site were presented above. Integration of this data applies through the SecureBox which is responsible to handle the communication with the smart component installed in local grid. Towards this direction, the security and privacy methods as mentioned above will be considered also for the integration of the data from the field devices at DSO level.

In the ES / UA demonstrators, it was presented that RTUs would be used for monitoring the grid. The signals / measurements to be finally used for each demonstrator are currently under definition. Nevertheless, a preliminary selection has been made already, including the indication of voltage presence, RMS currents/voltages, frequency, active/reactive/apparent power, or the power factor. The communication between the RTU and the Secure Box will be performed through Modbus protocol.

The data made available at SecureBox level are then transferred to the eFORT Intelligent Platform. In more details, we consider the role of the eFORT Intelligent Platform in the project, where the objective is twofold: (a) to integrate algorithms, control devices and decision support systems for the detection, prevention, mitigation, adaptation and restoration activities as delivered in WP2- WP4, including integration and/or interaction with the visualization tool, the risk assessment tools, the system for grid self-sealing and defend against cascading effects, and (b) **to ensure its interoperability** so that it can be linked to different databases, services, and to different typologies of SecureBox or similar hardware units managing the data of the EPES assets. In relation to the latter (which is the main objective of the analysis performed in this document), the eFORT Intelligent Platform will have to align with the data transfer mechanisms defined in the project.

Towards this direction and taking into account the data needs and specifications of the project as listed in previous section, the eFORT Intelligent Platform will support files uploads as well as integration with REST API services in order to ensure the prompt data management. More details about the REST API are provided as part of the work in the dedicated task (4.6) but an overview is provided in the following:

- Communication protocol: Communication should be done using standard network protocols. HTTP and HTTPS allowing POST,GET, PUT, and DELETE requests.
- Authentication & Security: For the API of the intelligent platform, the HMAC protocol with SHA-256 encryption has been selected to be implemented as a security system to ensure the integrity of the data and the authentication of each message.
- Structured Data Format: The data that the device sends to the API must be structured according to the JSON format specified in this document. In addition, the different endpoints to be used to ensure the correct functioning of the API will also be reflected in it.
- Error Handling and Relay: The device should be designed to handle error situations and, if necessary, be able to perform send retries in the event of connectivity failures.
- Frequency & Timing: This point is very important, considering the number of devices that will participate in the exchange of data on our platform, to ensure the availability of the API the device must comply with the frequency of requests to the API as agreed. Certain limits in the API usage will be considered and in the event that this frequency is exceeded, it is possible that those requests that exceed that frequency will be rejected.
- Version Management: The API will be adapted to the needs of the partners and therefore several versions of it will be released, the changes between versions and the specification of each of them will be perfectly documented. The device should be able to adapt to new API versions or updates without significant disruption.

Special remark about the semantic mapping of the data coming from the physical systems to the common data model defined in the project. The core principles of the data model definition (at the level of the platform but the same principles to be adopted at the level of SecureBox) are provided below while the final full version of the common information model of the project will be reported as part of the work of the T4.6.

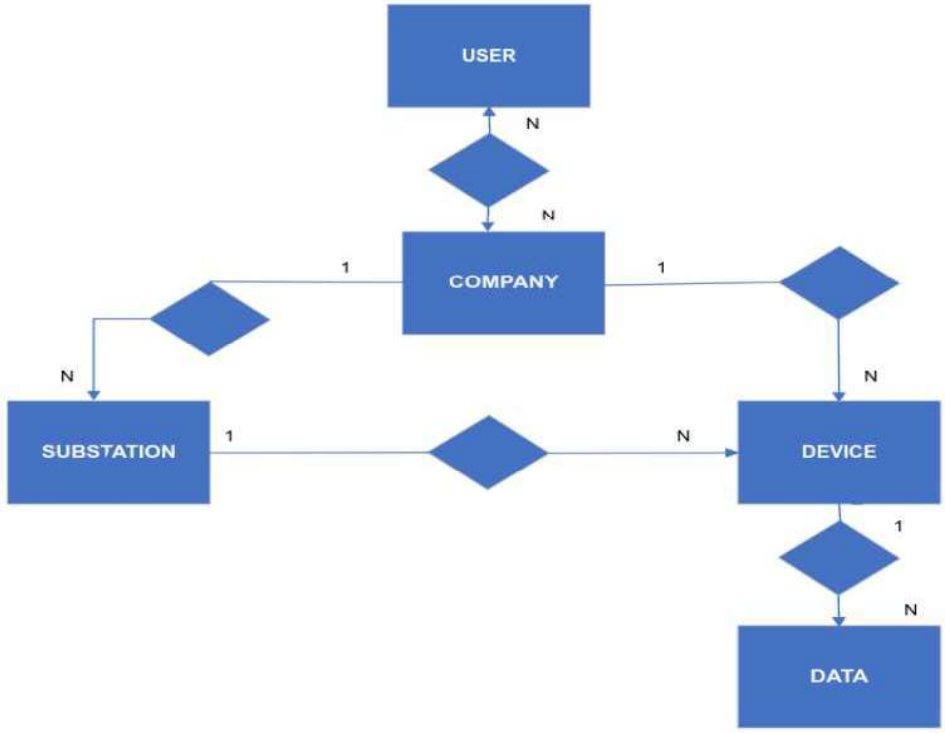

Figure 16 eFORT common data model principles

It is evident that the data model version should aim to capture the different business roles as well as the physical assets (with the linked measurements) to be examined in the project. This is a typical approach as followed in the literature but further extensions (as well as detailed specifications) will be made available as part of the testing and demonstration activities of the project where the actual data streams from the demo sites will be made available.

Apart from the eFORT project data landscape specifications, the specifications about the security and privacy mechanisms to be considered in the eFORT architecture are defined (an outcome of the literature as well as the needs expressed by the demo partners/application developers). As stated also above, the overall framework should ensure.

- Access Control through mechanisms to restrict unauthorized access to components and data. This involves user authentication, authorization, and role-based access control (RBAC) or attribute-based access control (ABAC) over the data made available to the platform.
- Message Integrity ensuring that data transmitted between devices remains unchanged and uncorrupted during transmission.
- Anonymization incorporating anonymization techniques to remove any personal information from the data in case of non interest.
- Encryption incorporating encryption techniques to protect sensitive data from being accessed or intercepted by unauthorized entities. Encryption for data assets that are ingested through the SecureBox and for information exchange

among the Intelligent Platform and the business applications. In addition, encryption for key sharing to authorized data consumers will be considered.

- Cryptographic Key Management / key sharing outlining secure key management practices to protect cryptographic keys used for encryption and digital signatures. This includes methods and practices to ensure key generation, storage, distribution, usage, and revocation.

In addition, best Secure Data Storage Practices and Measures as defined as part of the IEC standardization are listed as specifications for the implementations performed in eFORT project, namely:

- Data storage minimization minimizing the amount of sensitive data stored on devices and systems. This reduces the attack surface and potential impact of data breaches. In relation to this, different deduplication techniques (i.e. cross-user data deduplication) may be considered in order to minimize the number of the data stored in the relevant environment.
- Implement data classification classifying data based on its sensitivity level to determine appropriate storage and access controls
- Regularly back up data mandating regularly backing up sensitive data to prevent data loss due to hardware failures, cyberattacks, or other incidents.
- Data integrity verification implementing data integrity verification mechanisms, such as checksums or digital signatures, to ensure that data has not been tampered with while in storage.
- Use of secure hardware devices by using secure hardware devices, such as tamper-resistant modules (TRMs) or hardware security modules (HSMs), to store sensitive data. These devices provide physical protection against unauthorized access and tampering.

We presented above the extensive list of specifications to be considered at the development of the different eFORT project applications in order to ensure secure data collection and information exchange[4]. We have to point out that as the project evolves and the final developments will be made available, minor updates on the aforementioned specifications may apply (to be reported as part of the work in the development and demonstration activities of the project in WP3 and WP4 respectively considering also the final version of the ex-ante demo site analysis in WP5- T5.1).

[4] Note: As stated above, the analysis is covering aspects in relation to communication protocol and information exchange. Additional mechanisms (i.e Intelligent Platform will provide a VPN for communication encryption between all the parties (tools, Securebox) will be defined as part of the work in T2.6 and be reported in D2.4.

3 Information sharing and data exchange between TSOs and DSOs

3.1 Introduction

In this section, the communication protocols and standards used in past TSO-DSO coordination projects are analyzed, developing a map that relates the most used standards with the information exchanges they could cover. To get an actual overview of the protocols, standards, and procedures currently used by EU system operators to exchange different type of information, apart from the review of the relevant initiatives, a questionnaire was distributed, covering three topics: TSO-DSO data exchange, exchanges of cybersecurity-related information, and coordination of response to cybersecurity incidents.

In addition to this, the suitability of existing standards (e.g., VERIS Incident Framework, OASIS STIX 2.1, etc.) for different purposes related to the exchange of cybersecurity information is assessed, paying special attention to their different scope and characteristics.

Overall, the main objective of this section is to provide some recommendations and aspects to consider for the energy grid players to share information in a secure way.

3.2 Methodology

For the analysis of the information that can be exchanged between DSOs and TSOs during the normal operation of the grid or during a system service market process, the communication protocols and data models used in other European projects such as OneNet, CoordiNet or SmartNet were considered [27]. Based on this analysis, standards and information profiles were mapped to better identify which standards can be used for the exchange of which information.

To better identify information currently exchanged between system operators, the cybersecurity measures adopted in these exchanges, and which mechanisms are in place to confront cybersecurity incidents, a questionnaire (see Annex A) was distributed among project participants (system operators and other participants' contacts) and also among the members of organisations such as EE-ISAC, ENTSO.E, and E.DSO, although with reduced participation by these last.

The questionnaire focused on determining the information required by key players of the electricity system, specifically when and how data must be shared between them to ensure the proper operation of the grid and to better understand what mechanisms are activated when a cybersecurity incident takes place.

The information asked in this questionnaire was mainly related to data exchanges that would take place in a market process, such as a system services market. The reason for this is that eFORT demos were still being defined and a market process usually requires intensive information and data exchange between participants, where TSO-

DSO coordination is essential. Therefore, such process constitutes a good approach to identify information gaps.

Due to confidentiality and security reasons, the results of the questionnaire are presented in an aggregated form in this document to avoid the mapping of information to a specific system operator. In total, six system operators answered to the questionnaire, of which only three answered to all the topics asked. Figure 17 shows the countries where the respondents operate, and Figure 18 shows their specific role (83% were DSOs and 17% cover both distribution and transmission networks).

Figure 17. Countries where the entities that answered the questionnaire operate.

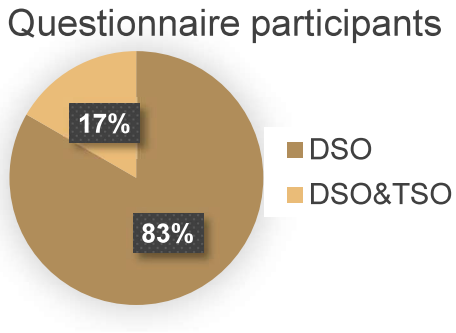

Figure 18. Role of questionnaire participants.

3.3 Reference standards

3.3.1 Standards for information exchange

In 77[27] , the communication protocols and standards used in use cases of five EU-funded projects on TSO-DSO coordination (SmartNet, CoordiNet, TDX-Assist, INTERRFACE, and EU-Sysflex) were analyzed, providing information on the most common ones and their role. Since these projects commonly used the Common Information Model (CIM), IEC 61850-7, and IEC 61968, Table 8 has been elaborated to summarize the potential coverage and application of these standards for the exchange of information between power system stakeholders.

IEC 61850 is being widely implemented by SOs, and its main characteristics were analyzed in section 2.1.1. In most of these projects, CIM was implemented as the main information model. The aim of CIM is to facilitate the exchange of network and market data between organizations, as well as data between systems within a single organization [28]. The core of CIM is mainly defined in two families of standards: IEC 61970 standards, focused on the definition of Energy Management System (EMS) Application Program Interfaces (APIs), and IEC 62325 standards, which define CIM for energy market communications. In addition to this, IEC 61968 standards provide CIM extensions for the exchange of network models and distribution network data (e.g., network constraints), not only for their exchange between DSOs, but also with other stakeholders (TSO).

The core CIM standards defining EMS APIs can be used to represent the main data objects used in utility operations (IEC 61970-301), models for stability analysis (IEC 61970-302), information for state estimation and power flow applications (IEC 61970-452), steady-state solutions of these applications (IEC 61970-456) or dynamic models (IEC 61970-457).

To facilitate the exchange of operation and grid planning information for TSOs, the Common Grid Model Exchange Standard (CGMES) was created, promoted by ENTSO-E. Defined by IEC 61970-600-1 & 2 standards, it supports the adoption of network codes related to capacity calculation, congestion management, and system operation. Nevertheless, its adoption by DSOs must still be validated [29].

Despite CIM standards cover a wide variety of information (Table 8), its implementation may raise some issues related to extensions, harmonization with other standards (e.g., IEC 61850), and validation of model instances [30]. In particular, the experience in the EU-SysFlex project [31] showed that CIM needs improvements when involved in some data privacy processes such as data aggregation and anonymization, consent management, data logs exchange, and authentication information. Since CIM is an information model and does not directly include cybersecurity measures, its secure implementation by SOs relies on the proper adoption of the IEC 62351 standards (except for market communications, IEC 62325), which were comprehensively analyzed in section 2.1.3.

In terms of communication protocols, two main options for exchanging grid data were identified in the analysis in [27]: the Inter-Control Center Communications Protocol (ICCP or IEC 60870-6/TASE.2) and Data Exchange Platforms (DEPs).

ICCP is traditionally used for the exchange of grid data (including scheduling information, control operations, and time-series data) between the control centres of TSOs and DSOs [32], using wide and local area networks. In terms of cybersecurity, legacy implementations of standard ICCP may lack enough protection [33][34]. The default version of ICCP does not provide authentication and encryption of data and communications and, being a wide-area network protocol, it may be susceptible to Man-in-the-middle (MITM) attacks and Denial of Service (DoS) attacks [35]. For this reason, the implementation of secure ICCP version [34][36] is recommended for the direct communications between SCADA systems, as it includes payload encryption, access authentication through certificate management, and the use of TLS. In addition

to this, it is recommended the application of the data and communication security measures defined by IEC 62351-3 & 4, which cover the profiles used by ICCP.

The other main option, the use of DEPs, is the one usually preferred in innovation projects (usually, demonstrating a system service market for SOs), so that the system to access all types of data (smart metering data, grid data, and market-related data) can be the same and new agents (e.g., aggregators, flexibility service providers, other SOs, etc.) can easily connect without investing in an ICCP link. These platforms usually implement multiple internet/IoT communication protocols which increase the interoperability of these platforms and their suitability for the exchange of different types of data. For example, for the demonstration of the "Flexibility platform" in EU-SysFlex, the Estfeed platform was used for all the interactions between TSOs and DSOs, providing its own specification [37] supporting "Publish" and "Request-Response" communication mechanisms and adapters for other applications. In other projects, such as INTERRFACE and TDX-Assist, ENTSO-E Communication & Connectivity Service Platform (ECCo SP), which is a standardized communication platform for the Energy market, was used for different data exchanges. ECCo SP supports different communication protocols, such as AMQP (mentioned in section 2.1.2), Web Services, and File System Shared Folder (FSSF) [38].

In addition to this, the development and implementation of HTTP-based REST APIs for the data exchange between systems of SOs has also been observed in recent EU-funded projects (UMEI in EUniversal [39], and APIs involved in OneNet demos [40]). Although not all the data exchanges have the same requirements, some best security practices to apply to REST APIs are the use of OAuth and authentication tokens; throttling and quotas, which allow optimal response times and better management of service demand peaks; a Zero Trust Network Access policy; endpoint verification to protect against MITM attacks; and Least-privilege access.

Since the technologies involved in DEPs are mostly Information Technologies (IT), and given the importance of the information systems involved, the security practices and guidelines defined by the ISO/IEC 27000 family of standards should be followed by SOs. More specifically, those included in ISO/IEC 27002 and 27019, which cover systems for the generation, transmission, distribution, and storage of electricity. These standards include security measures regarding access control, cryptography, physical security, operations security, and communications security. It also sets guidelines for the management of information security incidents, including the proper coordination with those entities that can be affected by the same incident or that may be affected by the consequences. To guarantee that a SO properly follows the guidelines of ISO/IEC 27000, it should undergo audits and get certified by an accredited body.

TSO-DSO data exchange in eFORT demos

Regarding TSO-DSO data exchange within the project demos, or that could be affected by the demos, the following was reported:

- The Ukrainian demo does not expect any alterations in the TSO-DSO data exchange. The different solutions demonstrated in eFORT are expected to be carried out in a testbed / lab environment replicating the substation described in

section 2.2. In addition to this, the DSO does not currently exchange information with the TSO for the operation of this substation.

- The Italian demo does not expect any alteration in the TSO-DSO data exchange. No data is exchanged with other DSOs, but in HV substations, like Sarentino substation in the demo, the data exchanged with the TSO in real-time using IEC 60870-5-104 (security provided by IEC 62351) is specified by Annex 6 of the Italian Network Code "Data acquisition criteria for telecontrol"[5]: position status of the switches; active, reactive power, and current of HV lines; active and reactive power in the transformers; and voltage of busbars. However, these data would not be affected by the demo, and the data collected through the Smart Grid Controller implemented will be only for internal use and the scope of the project.
- The Spanish demo does not expect any alteration in the TSO-DSO data exchange. The Escúzar substation is a "frontier" substation, which means that it connects with the transmission network and another DSO's network, as described in section 2.2. The substation data that is exchanged are status and monitoring data (e.g., position and status of breakers and switches, active and reactive power, position of local/remote regulators, etc.), as required by the TSO for the control and operation of the system. These data are transmitted in real time to the TSO using both versions of ICCP and these communications are redundant with two additional communication channels (fiber and radio link), and two additional servers that guarantee communications. With other DSOs, the data exchanged regarding the "frontier" substations are the same as with the TSO.

[5] https://download.terna.it/terna/20220701_Allegato_A.6_8da5b792cadec35.pdf

Table 8 Summary of standards coverage and applicability for the exchange of specific types of information. Own elaboration based on [29] and standards specifications.

		IEC 61850-7	IEC 61968-11	IEC 61968-13	IEC 61970-301	IEC 61970-302	IEC 61970-452	IEC 61970-456	IEC 61970-457	CGMES (IEC 61970-600-1 &2)	IEC 62325-451-4	IEC 62325-451-5	IEC 62325-451-6	IEC 62325-451-7	IEC 62325-451-2	IEC 62325-301	ESMP (IEC 62325-351)
Assessing services, market, and network requirements on data standardisation for both DSO/TSO	Market results												X	X			
	Product prequalification results																X
	Market participant pre-qualification information																X
	Basic participant information																X
	Invoicing data										X						
	Settlement data										X		X				
	Aggregated data																X
	Network data of distribution system			X						X			X				
	Network demand forecast			X						X			X				
	Network information						X			X							
	Network reconfiguration data												X				
TSO-DSO information exchange	Flexibility resources													X			
	Flexibility Resources Qualification results										X	X	X	X	X		
	Scheduling process: activation signal correction / counter action														X		
	Execution order														X		
	Baselines reports												X				
	Connection state forecast									X							
	DER structural data	X	X	X		X											
	Development plans for distribution network						X			X							
	Dynamic Line Rating forecast for overhead lines												X				
	Energy clearing results										X				X	X	X
	Flexibility needs										X				X	X	X
	Forecast data			X						X			X				
	Grid congestions status											X				X	
	Limits and margins for capacity (by zone)															X	X
	Grid constraints assessment												X				
	Network characteristics (internal) information						X			X							
	Possible temporary limits on balancing capacity bids				X								X				
	Power flow simulation						X	X	X	X							
	Resource optimization information														X		
	Short circuit power forecast													X			
	State estimation data						X	X									
	System parameter control schema/instructions						X	X									

3.3.2 Suitability of cybersecurity information exchange standards

Two main types of cybersecurity information may be exchanged between entities: cybersecurity incident information and threat intelligence information.

Cybersecurity incident information includes information about specific events or occurrences that may indicate a security anomaly. On the other hand, threat intelligence information *"is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."* [6]

This section evaluates the suitability of four of the most widely used cybersecurity information standards for system operators: the VERIS Incident Framework, IETF IODEF, OASIS STIX 2.1, and OASIS OpenC2 (as stated also in the DoA). A short overview of these standards is provided in this section.

VERIS Incident Framework

The Vocabulary for Event Recording and Incident Sharing (VERIS) is a community-driven framework that addresses the lack of a commonly accepted taxonomy for security incident reporting, providing a set of metrics to do so in a structured, useful, and complete manner. It organizes incident information into five sections:

- Incident Tracking: General information about the incident.
- Victim Demographics: To describe the organization affected by the incident.
- Incident Description: Actors, Actions, Assets, and Attributes (A4 model by Verizon's RISK Team).
- Discovery & Response: Timeline of the events.
- Impact Assessment: This consists of loss categorization, loss estimation, and impact rating.

The main purpose of VERIS is to facilitate the cooperative post-incident analysis between organizations to learn from cybersecurity experiences and better manage risk in the future.

IETF IODEF

The Incident Object Description Exchange Format (IODEF) is a data representation standard defined by the Internet Engineering Task Force (IETF) specifically designed

[6] https://www.gartner.com/en/documents/2487216

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

for security incident information. It allows Machine-to-Machine (M2M) exchange of incident reports, automated processing, and response activities between Computer Security Incident Response Teams (CSIRTs) and other entities. The good machine-readability of the IODEF documents allow a high degree of automation of security operations. The following information is covered by IODEF, among other: attack pattern, platform information, vulnerability and weakness, countermeasure instruction, computer event logs, and severity assessments.

Among the main advantages of IODEF is its wide adoption and support by CSIRTS, government agencies, and industry groups. The format of its messages can be XML or JSON, which can be transmitted over various communication protocols, and it provides interoperability with IDMEF (Intrusion Detection Message Exchange Format), which is focused on intrusion detection and prevention. The main disadvantages of IODEF are related to its implementation in an organization: it may require a significant effort for organizations with limited cybersecurity expertise or upgrading legacy systems.

OASIS STIX

The Structured Threat Information Expression (STIX) is a language for sharing and analysing threat intelligence information. It offers a structured way to represent various aspects of cyber threats such as indicators, actors, and Tactics, Techniques, and Procedures (TTPs). STIX allows to indicate relationships between different threat elements, providing more contextual information about threats.

Although not strictly necessary, STIX is usually implemented with OASIS TAXII, an application layer communication protocol to exchange cyber threat information. It supports different communication mechanisms such as request-response (TAXII collection) and publish-subscribe (TAXII channel), facilitating the automation and scalability of threat intelligence information sharing. However, since STIX's default format is JSON, other communication protocols such as HTTPS or AMQP can be used for the exchange of information. It is also compatible with CybOX (Cyber Observable eXpression), which focuses on characterizing observable cyber entities. However, the main disadvantage of STIX is its complexity, as several parameters must be considered [41] and mistakes are common [42]. This is hindering its fast adoption despite its completeness to represent cybersecurity threats [42].

OASIS OpenC2

OASIS Open Command and Control (OpenC2) aims to provide a standard for the control of technologies involved in cyber defenses, so it is not really focused on the exchange of cybersecurity information. It addresses the response (acting) segment of

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

cyber defense by defining its architecture[7] and language[8] to send commands to security devices and services, facilitating the automation of responses to cybersecurity threats. It allows to discover the capabilities of devices, so that they can be managed taking advantage of their specific features. OpenC2 messages are encoded and transmitted securely using existing protocols (HTTPS[9] or MQTT[10]) and standards [43].

Although OpenC2 provides great interoperability between cyber defense technologies, the organizations adopting it may need to update or replace some of the security tools and system used.

Table 9 Summary of main characteristics of the standards considered.

	VERIS Incident Framework	IETF IODEF	OASIS STIX 2.1	OASIS OpenC2
Scope	Incident reporting and classification	Incident reporting and response	Threat intelligence sharing and analysis	Command and control of cybersecurity devices
Key characteristic	Structured taxonomy for incidents	Detailed description of incidents	Detailed information about threats	Granular control in security actions
Open standard	✓	✓	✓	✓
Complexity	Depends on usage	Medium	High	Depends on usage
Data format	JSON	XML, extended to JSON	JSON	JSON
Customisation	High	Medium	High	Medium (specific devices)
Automation	Limited	Supported	Supported	Supported

[7] https://docs.oasis-open.org/openc2/oc2arch/v1.0/cs01/oc2arch-v1.0-cs01.html

[8] https://docs.oasis-open.org/openc2/oc2ls/v1.0/oc2ls-v1.0.html

[9] https://docs.oasis-open.org/openc2/open-impl-https/v1.1/cs01/open-impl-https-v1.1-cs01.html

[10] https://docs.oasis-open.org/openc2/transf-mqtt/v1.0/transf-mqtt-v1.0.html

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Suitability of standards according to different purposes

The four standards considered serve different purposes and can complement each other. However, the simultaneous adoption of these standards by SOs would increase the complexity of managing cybersecurity information and responding to incidents, so their specific suitability is assessed.

Starting with the VERIS Incident Framework, it may be the least suitable solution for the exchange and classification of incidents between SOs. The possibilities of automation with VERIS are very limited, since the classification of incidents using this framework requires subjective judgement. This could raise some interpretation problems on the receiver's side. Furthermore, its adoption would require complementing it with other solutions, since it does not cover threat intelligence information. However, although VERIS is found not to be the best option for information exchange between SOs or other organizations, it could be used to disclosure information about past incidents, so that the research community can investigate them. In this case, SOs would have full control over what information they make public, thanks to the high degree of customization that the framework allows and its easiness to be generated manually.

To report cybersecurity incidents and exchange their information, IODEF is the most widely used by CSIRTs and government agencies, so it may be the best option for the exchange of information between SOs (many SOs across Europe have it already implemented), providing interoperability with the IDMEF (Intrusion Detection Message Exchange Format), which focuses on incident detection. It provides XML and JSON formats, which can be transmitted over various protocols. However, if, apart from information exchange, the storage of IODEF documents is foreseen, the use of JSON is recommended. The format of IODEF documents is a bit complex, making it unlikely to generate them manually, so the Incident Handling System (IHS) needs to be able to import and export IODEF documents to exchange information in a fast, effective way.

IODEF is focused on providing a detailed description of cybersecurity incidents that have already taken place (reactive approach). Nevertheless, given the criticality of the electricity infrastructure, SOs may adopt a proactive approach and exchange threat intelligence between them and other organizations (e.g., service providers) to take preventive actions before an incident occurs. In such case, the implementation of OASIS STIX could be a good solution, since it allows a detailed description of complex cyber threats. The main drawback of STIX is its complexity. If implemented, SOs should collaborate on using it in the same way to minimize the risk of interoperability problems. This could include common guidelines and personnel training so that the parameters are correctly interpreted at both sides (sender and receiver) and to avoid errors in the information transmitted. Furthermore, SOs should agree on the communication protocol to be used with STIX based on their expertise and already-implemented communication links, since the use of TAXII (commonly used with STIX) may require a greater system adaptation effort. In addition to this, when the cyber threat is simple, STIX may add too extra complexity, making it inefficient: a simpler format may be more effective [44], but it will require further collaboration between SOs to agree on the data model for these cases.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Regarding OASIS OpenC2, it is not a standard for the exchange of information between different entities, but to control technologies involved in cyber defense. OpenC2 can be used once an incident has been detected and a decision to act has been made, assuming that the senders and receivers of the commands have been authenticated and authorized by other means. Therefore, its implementation heavily depends on the capabilities and existing compatible devices/systems implemented by each SO at an individual level.

However, OASIS OpenC2 is relevant for the project. As part of Task 3.7 ("Reactive and preventive actions issued to the infrastructure"), the SOARCA[11] (Security **O**rchestrator for **A**dvanced **R**esponse to **C**yber **A**ttacks) tool is being developed. SOARCA is an open source, playbook-driven response automation tool that natively supports OASIS OpenC2, HTTP(s), and SSH as transport mechanisms, with the potential extension to MQTT. It aims to be compliant with the CACAO Security Playbooks v2.0[12], which defines the schema and taxonomy for the cybersecurity playbooks of organizations. Thus, for the use of this tool, it would be convenient that the cybersecurity playbooks of SOs are defined according to CACAO v2.0.

3.4 Analysis of questionnaire results

In this section, and taking into account the results of the state-of-the-art analysis as presented above, we proceed with the questionnaire circulation to the network stakeholders in order to get direct feedback towards specifications definition for information exchange. The details of the questionnaire analysis are provided in this section.

3.4.1 TSO-DSO information exchange in market

A common system service market usually consists of five phases [45] where information can be exchanged:

1. **Preparation:** Phase in which the product is defined, registered, and technically prequalified to check its compliance with the technical requirements.
2. **Forecasting:** Phase in which the grid status is estimated (i.e., forecasted), determining future needs.
3. **Market operation:** Phase in which bids are collected and the market process clearing is carried out. Market clearing may involve economic and technical data.

[11] https://github.com/COSSAS/SOARCA

[12] https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.html

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

4. **Monitoring and activation:** In this phase the network operation is monitored and the selected flexibility service providers are activated.
5. **Measurement and settlement:** Phase in which measurement data from Flexibility Service Providers (FSPs) is obtained and the financial settlement is performed.

Table 11 in Annex B shows the pieces of information corresponding to each market phase where the respondents to the questionnaire reported data such as the actors involved, the information and communication standard, the criticality of information (detailed results in Annex B) or the type of infrastructure used (see Annex A).

Figure 19 shows the type of communications infrastructure (proprietary or public) used in the information exchange per market phase. At an aggregated level, that is, considering all the respondents' answers, approximately half of the information is transmitted using a public infrastructure (provided by a telecommunications company) but adopting measures such as the use of a Virtual Private Network (VPN) and encryption for certain data. The use of public infrastructure is common for small system operators and system operators with insufficient capabilities (technical or economic) to operate their own telecommunications network, but must make sure that necessary security measures are adopted by the provider of this infrastructure.

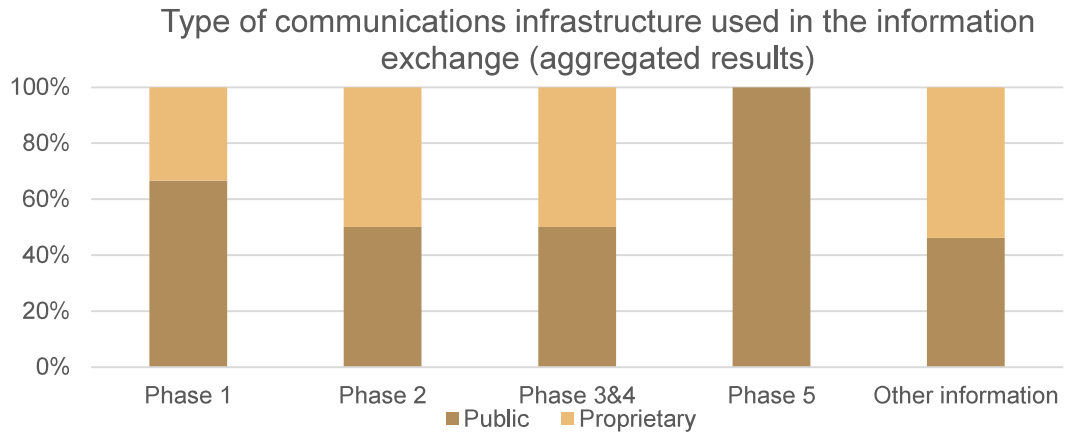

Figure 19 Type of communications infrastructure used in the information exchange per phase. Aggregated results.

For the information exchanged in **Phase 1: Preparation**, communications with the market operator (market participant prequalification information, basic participant information, and invoicing data) are exchanged on request commonly using a web communication protocol defined by the market operators. The criticality of this information is moderate. However, more critical information exchanged in real time between TSO and DSO (flexibility resources information and grid constraints) make use of SCADA-SCADA coupling (ICCP or IEC 60870-6) or IEC 60870-5-104, while having adopted the cybersecurity measures from ISO 27001, 27002, and 27019. In this case, as commented in section 3.3.1, the adoption of IEC 62351 is recommended to increase the security of the ICCP communications. As an outlier, one system operator reported that the exchange of limits and margins for capacity was done through email or phone (no security measures were reported), which would not be the best approach, as these communication channels may be subject to multiple types of cyberattacks, such as man-in-the-middle or fishing attacks.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

For the information exchanged in **Phase 2: Forecasting**, the technologies are similar to those in Phase 1. Baseline reports, development plans for the distribution network, and prediction of maintenance periods, considered highly critical by the respondents, are exchanged periodically or under request, not following any automated approach: this information is exchanged via email, phone or through dedicated web portals. Other information may require to be exchanged in real time. This is the case for information such as grid congestions status, network demand forecast or general forecast data, for which the respondents of the questionnaire reported the use of ICCP or IEC 60870-5-104. As for weather forecast data, respondents used direct access to a database, web services, or Secured File Transfer Protocol (SFTP).

Regarding **Phase 3 and 4: Market Operation and monitoring and activation**, only two respondents provided information regarding the exchange of market results and execution orders. For the first, the common approach is to use a web standard (e.g., HTTPS REST API) defined by the market operator, whereas execution orders rely on ICCP to be transmitted.

For **Phase 5: Measurement and settlement,** only one respondent provided information on how the flexible resources metering data is exchange by using an ad hoc communication standard used by the market clearing system whose security complies with ISO 27001, 27002 and 27019 standards.

Finally, there are pieces of information that may be exchanged during operation and not during a specific market phase. Real-time, highly critical data such as network characteristics and information, aggregated data, resource optimization information and network reconfiguration data are transmitted using IEC 61870-5-104. Respondents were not sure about how power flow simulation results are exchanged nor about their criticality.

3.4.2 Cybersecurity information exchanges

The exchange of information regarding cybersecurity threats and incidents can be extremely useful for the electricity sector to avoid cascading effects and take advantage of the lessons learned.

In Europe, regulation is evolving towards demanding more coordination and knowledge-sharing regarding cybersecurity. The Network and Information Security 2 (NIS2) Directive [46] sets that authorities designated at a national level should be notified about significant cybersecurity incidents and threats. With the entry into force of Article 16 of NIS2 Directive, the European cyber crisis liaison network (EU CyCLONe) was created. EU CyCLONe is a cooperation network for the national authorities in charge of cyber crisis management. Its main aims, among others, are to support coordinated management and response to cybersecurity incidents and crises, ensure the exchange of information among institutions, and evaluate potential consequences and propose mitigation measures [46].

A more recent regulation, the Network Code on Cybersecurity [47], focuses on the electricity sector and, more specifically, the cybersecurity of cross-border electricity flows. Chapter V of this regulation (articles 37-42) set rules on information flows, cyberattacks, and crisis management. It discusses the development and functions of

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Electricity Cybersecurity Early Alert Capabilities (ECEAC) to enable timely threat intelligence sharing and improve situational awareness in the electricity ecosystem, setting up requirements for incident reporting, classification of cyberattacks, and threat information sharing.

In addition to this, with a more general scope, a provisional agreement on the "cyber solidarity act" [48] was recently achieved, amending the cybersecurity act (CSA). The "cyber solidarity act" aims to support the detection of cybersecurity threats and incidents and to strengthen solidarity through the establishment of a "cyber security alert system" for the EU.

Given the expected advancements regarding the exchange of cybersecurity incidents information, to get an overview of the status of SOs, Topic 2 in the questionnaire asked some questions regarding participation in cybersecurity organizations, the exchange of incident information with other stakeholders, and conditions for this type of exchange.

Figure 20 shows that, when asked about participation in cybersecurity information exchange initiatives (e.g., knowledge sharing), two out of the six participants reported to be members of associations such as ENCS or EE-ISAC. From the remaining four, only one has plans of becoming a member of such type of associations.

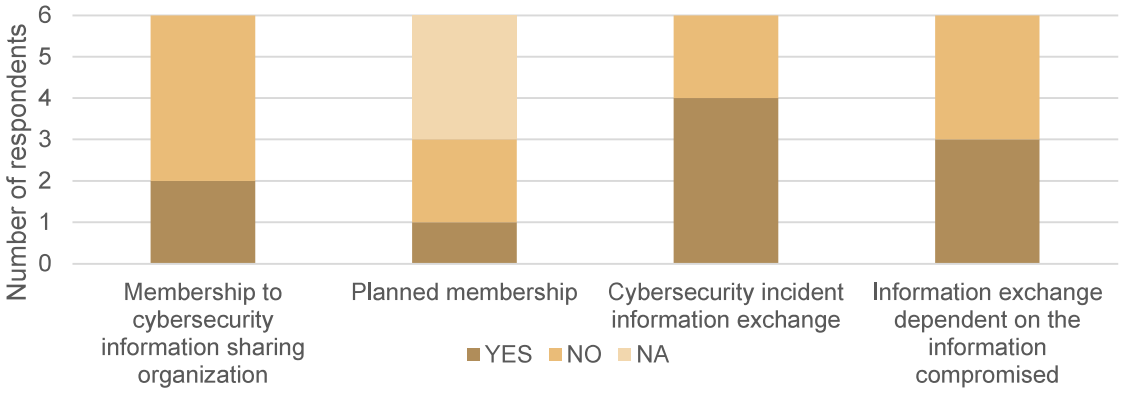

Figure 20 Summary of the answers given to questions regarding Topic 2 in the questionnaire.

When asked about information exchange, most respondents reported that they currently exchange cybersecurity incident information with other actors and three of them reported that this information depends on the type of information compromised (Figure 20). Only one respondent declared that no cybersecurity information was exchanged with any other entity. One respondent reported that incidents were mainly classified into data breaches, operational disruptions, ransomware attacks, and Advanced Persistent Threats (APTs); depending on the type, different information is exchanged to better address the incident. Another one reported that the information depends on the format provided by the designated national authority to notify the incident.

3.4.3 Coordination of response to cybersecurity incidents

European SOs may exchange information regarding cybersecurity incidents among them and/or communicate about them to entities at a national level. Although this

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

information exchange may be just informative, it could also be used to coordinate the response to the incident, as national electricity systems involve multiple stakeholders.

All the participant SOs except one answered that they are able to coordinate the response to cybersecurity incidents with other stakeholders: four reported that TSOs and DSOs were involved in this coordination, three also coordinate with the corresponding national entity and their service providers, and only two involve the market operator in this coordination (Figure 21).

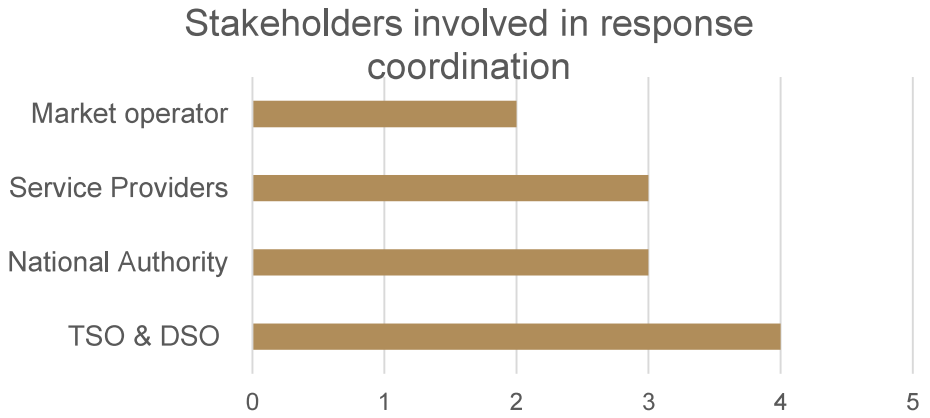

Figure 21 Stakeholders involved in response coordination to cybersecurity incidents according to questionnaire respondents.

There are different ways in which the response coordination can take place. The following approaches have been reported by the participants of the questionnaire:

a) The incident is first notified to the national authority which, based on a Traffic Light Protocol (TLP), notifies the relevant actors and coordinates the response.
b) TSO and DSO exchange specific information (critical signals and status information to increase the observability of the connected system operator) in real or semi-real time to guarantee the functioning of the electricity system.
c) The actions of all the actors involved are coordinated during the ongoing cybersecurity incident, using the pre-defined Points of Contact, after notifying the national authority. This way, all the actions are aligned towards solving the incident in an effective manner without the duplication of measures.

All these approaches would have the following requirements in common:

- **Incident classification and prioritization.** The more is known about the incident, the better the response can be by using the minimum resources.
- Define **roles** and **responsibilities**. Regardless of the approach, one entity should lead, to some extent, the response to the incident. This is clear in the case of the centralised approach (a national entity), but it should be pre-defined for the other approaches, either depending on the type of incident, its range of action, or the actor involved.
- **Clear communication channels**. Interoperability is key. Communication protocols and data models should be clearly defined, and the systems involved in the information exchanges should be fully interoperable and secure.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

- **Training**. Electricity systems stakeholders must be trained in the incident response coordination, so that they are prepared when a real incident takes place.

We presented above the detailed results as gathered from the feedback provided by the SOs through the questionnaire survey. The analysis performed is deriving a set of specifications that may be considered in order to ensure TSO-DSO information exchange in market, cybersecurity information exchanges as well as coordination of response to cybersecurity incidents. The feedback gathered from the questionnaire analysis may be further contribute to the standardization definition as well as the project specifications related to the information exchange on the topics mentioned above.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

4 Conclusions

The aim of the work in T2.5 as reported in this deliverable is to provide a set of specifications referring to data collection mechanisms that should be considered at the development in the frame of the eFORT architecture system towards establishing a secure and trustful data sharing framework for all stakeholders involved in the project. The analysis is covering both the data collection and handling from the physical assets as well as the data sharing principles among business actors (network operators).

In this context, the task initially focuses on refining the landscape of the relevant data sets involved in the project's demonstrators and their metadata, thus creating a database of information sources (from physical systems) that will be considered during the data collection activities. In addition, and in order to develop holistic risk management systems for EPES, there is a need for improving collection and homogeneous representation of data coming from legacy equipment and modern communication devices (e.g., IoT and DERs). For legacy systems, various open-source approaches exist for data aggregation over SCADA, Distributed Control System (DCS) and Integrated Control Systems (ICS) such as Rapid SCADA and Tango, whereas for modern communication devices they are mostly based on solutions collecting data over IP networks. Our analysis in this document step on state-of-the art methods and design scalable and modular services to serve multiple data collection-related purposes, i.e.: (a) to handle the upstream, downstream and indirect collection of data assets from the supply-driven perspective of the data providers via APIs, through real-time data pipelines and/or batch files and (b) to receive real-time updates for data assets.

A key issue for data handling has to do with privacy/security-preserving data computation and privacy/security-preserving data aggregation. Therefore, the work in this deliverable aim to identify, monitor and analyse relevant security and IPR policies linked to the aforementioned data sets. This relates both to the business value and IPR handling of data, as well as to confidential and private data that might be used during the implementation of the project and shall be safeguarded against any compromise. Towards this direction, appropriate security services are reviewed in order to set different layers for data security and privacy assurance in the project. Moreover, the IPR policies to apply over the data to be considered in h project are specified as part of the work in this deliverable.

Last but not least, the aim of this document is also to provide some recommendations for the secure information exchange between energy grid players. Starting with a review analysis of how TSOs and DSOs exchange information and its relevance for the demos, suitability of existing standards (such as VERIS Incident Framework, IETF IODEF, OASIS STIX 2.1, and OASIS OpenC2) for different purposes is assessed. In addition, to get an actual overview of the information sharing among EU system operators, a questionnaire was distributed among the DSOs and TSOs covering three topics (TSO-DSO data exchange, exchanges of cybersecurity-related information, and coordination of response to cybersecurity incidents) and different recommendations for a secure and effective data exchange are provided based on the answers collected.

Overall, the definition of the specifications in this document will pave the way for the development of the SecureBox in T4.5 (SecureBox: edge device and functions for

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

privacy management) and the eFORT Intelligent Platform in T4.6 (eFORT Intelligent Platform: integration and interoperability) as the key components that are considered for the data gathering and data sharing from the demo assets. In addition, key principles as defined in this document (and will be part of the implementation of the eFORT Intelligent Platform) will pave the way for the integration of the different business applications that will be delivered in the project (and will exchange information with the eFORT Intelligent Platform). In addition, the work reported in this task is tightly linked with the specifications about the communication infrastructures to be delivered in the project as part of the work in T2.6 (and will also complement the specifications definition for the eFORT Intelligent Platform).

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

References

[1]. BRIDGE "European (energy) data exchange reference architecture 3.0" , https://op.europa.eu/en/publication-detail/-/publication/dc073847-4d35-11ee-9220-01aa75ed71a1/language-en

[2]. BRIDGE "Contribution from BRIDGE projects to Standardisation", https://bridge-smart-grid-storage-systems-digital-projects.ec.europa.eu/node/476

[3]. DNP3 standard, https://www.ensotest.com/dnp3/introduction-to-the-ieee-1815-dnp3-standard/

[4]. IEC 61850, https://iec61850.dvl.iec.ch/

[5]. IEC 60870-5, https://webstore.iec.ch/preview/info_iec60870-5-104%7Bed2.0%7Den_d.pdf

[6]. IEEE C37.118-2005, https://www.osti.gov/biblio/1504742

[7]. Description of the IEEE C37.118 protocol and its implementation. https://www.typhoon-hil.com/documentation/typhoon-hil-software-manual/References/c37_118_protocol.html

[8]. IEC standardization mapping, https://mapping.iec.ch/#/maps/1

[9]. SunSpec Modbus, https://sunspec.org/

[10]. IEEE 2030.5, https://www.qualitylogic.com/wp-content/uploads/2020/06/QL-Intro-to-2030.5-Webinar.pdf

[11]. IEEE 1815, https://standards.ieee.org/ieee/1815/5414/

[12]. OCPP Protocol, https://openchargealliance.org/protocols/open-charge-point-protocol/

[13]. IEC 63110, https://webstore.iec.ch/publication/60000

[14]. SAREF model, https://saref.etsi.org/

[15]. IoT-to-cloud communication protocols, https://iot.telenor.com/iot-insights/what-is-iot-communications-protocols/

[16]. IEC 62351, https://iec61850.dvl.iec.ch/what-is-61850/technical-principles/61850-cybersecurity/

[17]. IEC 62351-4- Application Layer Security for IEC 61850, https://ieeexplore.ieee.org/iel7/6287639/8948470/09115626.pdf

[18]. IEC 62351-6- Security for IEC 61850 GOOSE and SV Messages, https://webstore.iec.ch/preview/info_iec62351-6%7Bed1.0%7Db.pdf

[19]. IEC 62351-8: Role-Based Access Control for Power System Management, https://webstore.iec.ch/publication/61822

[20]. IEC 62351-9: Key Management, https://webstore.iec.ch/publication/66864

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

[21]. Trusted Platform Module Overview, https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/

[22]. SunSpec Modbus Certification Procedures for Data and Communications Security of DER, https://sunspec.org/sunspec-cybersecurity-specifications/

[23]. SunSpec Modbus Recommendations for Trust and Encryption in DER Interoperability Standards https://sunspec.org/wp-content/uploads/2020/01/Recommendations-for-Trust-and-Encryption-in-DER-Interoperability-Standards-SAND2019-1490.pdf

[24]. SunSpec Modbus Roadmap for Photovoltaic Cyber Security https://sunspec.org/wp-content/uploads/2020/01/Roadmap-for-Photovoltaic-Cyber-Security-SAND2017-13262-4-10-2018.pdf

[25]. OCPP Protocol Security, https://www.openchargealliance.org/news/enhanced-security-for-ocpp-16/

[26]. MQTT Security Model, https://www.hivemq.com/mqtt/mqtt-security-fundamentals/

[27]. Rodríguez Perez, N., Domingo, J. M., Lopez, G. L., Avila, J. P. C., Bosco, F., Croce, V., Kukk, K., Uslar, M., Madina, C., & Santos-Mugica, M. (2022). ICT architectures for TSO-DSO coordination and data exchange: A European perspective. IEEE Transactions on Smart Grid, 1-1. https://doi.org/10.1109/TSG.2022.3206092

[28]. EPRI. (2015). *Common Information Model Primer: Third Edition* (3002006001; p. 188).

[29]. Kapetanios, A., Sakas, V., Kotsalos, K., Suljanovic, N., Oliveira, F., Ivanov, C., Happ, S., Haghgoo, M., Anderson, E., Augusto, C., & Bosco, F. (2022). *Report on Extended Data, Platform and Service Interoperability* (D5.6). OneNet Project.

[30]. Kim, H. J., Jeong, C. M., Sohn, J.-M., Joo, J.-Y., Donde, V., Ko, Y., & Yoon, Y. T. (2020). A Comprehensive Review of Practical Issues for Interoperability Using the Common Information Model in Smart Grids. *Energies*, *13*(6), 1435. https://doi.org/10.3390/en13061435

[31]. Kukk, K., Winiarski, L., Requardt, B., Suignard, E., Effantin, C., Sochynskyi, S., Tkaczyk, A., Lambert, E., Anton, P., Rossøy, O., Good, N., Jover, R., Trees, K., & Albers, W. (2021). *Proposal for data exchange standards and protocols* (Deliverable 5.5; p. 175). H2020 EU-SysFlex.

[32]. Lambert, E., Morais, H., Reis, F., Alves, R., Taylor, G., Souvent, A., & Suljanovic, N. (2018). Practices and Architectures for TSO-DSO Data Exchange: European Landscape. *2018 IEEE PES Innovative Smart Grid Technologies Conference Europe*, 1-6. https://doi.org/10.1109/ISGTEurope.2018.8571547

[33]. Franz, M. (2007). ICCP Exposed: Assessing the Attack Surface of the “Utility Stack”. *SCADA Security Scientific Symposium*, 15.

This project has received funding from the European Union’s Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

[34]. M.J. Rice, G.K. Dayley, C.A. Bonebrake, & L.J. Becker. (2017). *Secure ICCP*. Pacific Northwest National Laboratory, U.S. Department of Energy.

[35]. Malviya, N. (2020, febrero 13). *Exploring TASE 2.0 & ICCP: Key Protocols in ICS/SCADA Networks*. INFOSEC Institute. https://www.infosecinstitute.com/resources/scada-ics-security/tase-2-0-and-iccp/

[36]. Michalski, J. T., Lanzone, A., Trent, J., & Smith, S. (2007). *Secure ICCP Integration Considerations and Recommendations*. Sandia National Laboratories.

[37]. Estfeed. (2020). *Estfeed Protocol v3* (Technical Specification Y-1029-15; p. 38).

[38]. Bartol, J., Kodek, T., Souvent, A., Oliveira, F., Lambert, E., Petrovič, N., & Suljanović, N. (2019). Utilization of ECCo SP for secured and reliable information exchange between system operators. *2019 27th Telecommunications Forum (TELFOR)*, 1-4. https://doi.org/10.1109/TELFOR48224.2019.8971052

[39]. Silva, C., Marques, P., Milzer, G., Saetre, N., Dyvik Eide, Ø., Crucifix, P., Debray, A., Dumont, C., Marzano, G., Ruggoo, P., Kaffash, M., & Sinitsyna, K. (2022). *Market enabling interface to unlock flexibility solutions for cost-effective management of smarter distribution grids* [Deliverable D2.6]. EUniversal. https://euniversal.eu/wp-content/uploads/2022/08/EUniversal_D2.6_UMEI.pdf

[40]. Ziegler, D. U., Troncia, M., Mejía, E. C. O., Pérez, N. R., Rivera, O. M. V., & Ávila, J. P. C. (2023). *Cluster Demo results evaluation and success metrics analysis Western Demo D9. 8*. http://www.onenet-project.eu/wp-content/uploads/2024/01/OneNet_D9.8_V1.0.pdf

[41]. Czekster, R. M., Metere, R., & Morisset, C. (2022). *cyberaCTIve: A STIX-based Tool for Cyber Threat Intelligence in Complex Models* (arXiv:2204.03676). arXiv. http://arxiv.org/abs/2204.03676

[42]. Jin, B., Kim, E., Lee, H., Bertino, E., Kim, D., & Kim, H. (2024). Sharing cyber threat intelligence: Does it really help? *Proceedings 2024 Network and Distributed System Security Symposium*. Network and Distributed System Security Symposium, San Diego, CA, USA. https://doi.org/10.14722/ndss.2024.24228

[43]. Mavroeidis, V., & Brule, J. (2020). A nonproprietary language for the command and control of cyber defenses – OpenC2. *Computers & Security*, *97*, 101999. https://doi.org/10.1016/j.cose.2020.101999

[44]. Skiadopoulos, S. (2018). *D2.2 Threat sharing methods: Comparative analysis*. H2020 Cyber-Trust Project.

[45]. Chaves, J. P., Matteo Troncia, Leslie Herding, Nicolás Morell, Orlando Valarezo, Kris Kessels, Annelies Delnooz, Janka Vanschoenwinkel, José Villar, Jan Budke, Joao Falcao, Pedro Marques, Carlos Cândido, Dominik Falkowski, Miroslaw Matusewicz, Nicolas Métivier, Gesa Milzer, Thomas Gueuning, & Pierre Crucifix. (2021). *Identification of relevant market mechanisms for the*

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

procurement of flexibility needs and grid services (Deliverable D5.1). EUniversal Project. https://euniversal.eu/wp-content/uploads/2021/02/EUniversal_D5.1.pdf

[46]. European Commission. (2022). *EU directive 2022/2555 (NIS 2 Directive)*. https://eur-lex.europa.eu/eli/dir/2022/2555

[47]. European Commission. (2024). *EU electricity supply – sector-specific rules on cybersecurity (network code)*. European Commission. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13101-EU-electricity-supply-sector-specific-rules-on-cybersecurity-network-code- en

[48]. Mammonas, D. (2024). *Cyber solidarity package: Council and Parliament strike deals to strengthen cyber security capacities in the EU*. Council of the EU. https://www.consilium.europa.eu/en/press/press-releases/2024/03/06/cyber-solidarity-package-council-and-parliament-strike-deals-to-strengthen-cyber-security-capacities-in-the-eu/

[49]. Stine, K., Kissel, R., Barker, W. C., Fahlsing, J., & Gulick, J. (2008). *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*. U.S. Department of commerce.

[50]. Association of Edison Illuminating Companies. (2009). *"Demand Response Measurement & Verification: Applications for Load Research*. https://www.naesb.org//pdf4/dsmee_group2_040909w5.pdf

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Annex A: Questionnaire template

Introduction

The present questionnaire is part of T2.5 *"Establishment of strategies for secure data collection and TSO-DSO data sharing" in eFORT*.

This questionnaire aims at determining the information required by each key player of the electricity system, and when and how it must be shared between them to ensure the proper operation of the grid. This questionnaire will also help to understand what mechanisms are activated when a cybersecurity incident takes place.

The information asked in this questionnaire mainly refers (but it is not limited to) to data exchanges that would take place in a market process, such as a system service markets. The reason for this is that eFORT demos are still being defined and a market process usually requires an intensive information and data exchange between participants, where TSO-DSO coordination is essential.

Based on this questionnaire, and on the analysis of ongoing initiatives, our objective is to identify potential vulnerabilities and threats in DSO-TSO data exchange to provide recommendations.

This questionnaire is intended for organization. Therefore, for each organization:

1 organization: 1 questionnaire answer

For any doubt you may have regarding the questionnaire, please, write to:

Néstor Rodríguez Pérez: nestor.rodriguez@iit.comillas.edu

Definitions

Information's criticality: The expected impact of having the information compromised in any sort of way (e.g., its confidentiality, integrity, or availability). Possible values [49]:

1. **Low**: If the information is compromised, it would have a limited adverse effect on organizational operations, assets, or individuals. For example: "*(i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals*"
2. **Moderate:** If the information is compromised, it would have a serious adverse effect on organizational operation, assets, or individuals. For example: *"(i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries."*

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

3. **High:** If the information is compromised, it would have a severe or catastrophic adverse effect on organizational operation, assets, or individuals. For example: *"(i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries."*

Baseline reports: Baselines of FSPs. These are based on measurements made by FSPs regarding variations in end-user customers' electric consumption from their typical consumption patterns as a result of [50]:

1. changes in electricity price over time.
2. incentive payments designed to encourage consumers to use less electricity when wholesale market prices are high.
3. requests to support the reliability of the system when it is threatened.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Questionnaire

Background information	
Please, indicate the country where your organization is based:	
Please, indicate the role of your organization (e.g., TSO, DSO):	

Topic 1 – TSO-DSO INFORMATION EXCHANGE IN A MARKET PROCESS
Please, fill in the following table with your knowledge and experience about information that may be subject of exchange between TSO-DSO-Other in a system service market, where your entity may participate. **If your entity does not participate in such type of market, but does exchange information with other entity (e.g., a DSO or TSO), just leave the "MARKET PHASE" boxes empty.** **For some information, the market phase is already marked. This is just an estimation; feel free to indicate the correct market phase if it does not match with your process.** **If the information exchanged is not identified within the list, please, add it at the end of the table in a new row.** **Feel free to modify the width and height of the columns and rows as you wish for better readability**

Table 10 shows the common phases in a system service markets

Table 10 Common phases in a local flexibility market.

Market phase	Name and brief description
1	**Preparation.** Phase in which the product is defined, registered, and technically prequalified to check its compliance with the technical requirements.
2	**Forecasting.** Phase in which the grid status is estimated (i.e., forecasted), determining future needs.
3	**Market operation.** Phase in which bids are collected and the market process clearing is carried out. Market clearing may involve economic and technical data.
4	**Monitoring and activation.** In this phase the network operation is monitored and the selected flexibility service providers are activated.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

5	**Measurement and settlement.** Phase in which measurement data from Flexibility Service Providers (FSPs) is obtained and the financial settlement is performed.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

INFORMATION	MARKET PHASE (see Table 10)					YOUR ROLE AND SYSTEM NAME	THIRD PARTY INVOLVED AND SYSTEM NAME (if known)	INFORMATION AND COMMUNICATION STANDARD(s) used for the exchange	CYBERSECURITY STANDARD THAT IS APPLIED TO EXCHANGE THIS INFORMATION (if any)	DEPENDENCE ON COMMUNICATIONS LATENCY (i.e., real-time vs non-real-time)	CRITICALITY	TYPE OF COMMUNICATIONS INFRASTRUCUTRE USED (Public / Proprietary)	COMMENTS (e.g., clarifications, any other security measures applied etc.)
	1	*2*	*3*	*4*	*5*	*Sender / Receiver / Both*							
e.g., Dummy Information	☐	☐	☒	☐	☐	*e.g, Receiver, SCADA*	e.g., TSO SCADA	*e.g., IEC 61850 MMS, REST API, ICPP*	*e.g., IEC 62351*	*e.g., YES (requires real-time)*	*3-High*	e.g.,Public (contracted with telecom company, using VPN)	
Product prequalification results	☒	☐	☐	☐	☐						*Select one*		
Market participant pre-qualification information	☒	☐	☐	☐	☐						*Select one*		
Basic participant information	☒	☐	☐	☐	☐						*Select one*		
Invoicing data	☒	☐	☐	☐	☐						*Select one*		
Flexibility resources information	☒	☐	☐	☐	☐						*Select one*		
Flexibility Resources Qualification results	☒	☐	☐	☐	☐						*Select one*		
Limits and margins for capacity (by zone)	☒	☐	☐	☐	☐						*Select one*		
Grid constraints assessment	☒	☐	☐	☐	☐						*Select one*		
Baselines reports	☐	☒	☐	☐	☐						*Select one*		
Connection state forecast	☐	☒	☐	☐	☐						*Select one*		
Development plans for distribution network	☐	☒	☐	☐	☐						*Select one*		
Dynamic Line Rating forecast for overhead lines	☐	☒	☐	☐	☐						*Select one*		
Flexibility needs	☐	☒	☐	☐	☐						*Select one*		
Forecast data	☐	☒	☐	☐	☐						*Select one*		
Grid congestions status	☐	☒	☐	☐	☐						*Select one*		
Network demand forecast	☐	☒	☐	☐	☐						*Select one*		
Prediction of maintenance periods	☐	☒	☐	☐	☐						*Select one*		
Short circuit power forecast	☐	☒	☐	☐	☐						*Select one*		
Weather forecast (IEC 62325 package environmental)	☐	☒	☐	☐	☐						*Select one*		
Energy clearing results	☐	☐	☒	☐	☐						*Select one*		

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Market results	□	□	⊠	□	□						*Select one*			
Execution order	□	□	□	⊠	□						*Select one*			
Scheduling process: activation signal correction / counter action	□	□	□	⊠	□						*Select one*			
Flexible Resource Metering data	□	□	□	□	⊠						*Select one*			
Settlement data	□	□	□	□	⊠						*Select one*			
Network characteristics (internal) information	□	□	□	□	□						*Select one*			
Aggregated data	□	□	□	□	□						*Select one*			
Resource optimization information	□	□	□	□	□						*Select one*			
DER Structural data	□	□	□	□	□						*Select one*			
Power flow simulation results	□	□	□	□	□						*Select one*			
Network information	□	□	□	□	□						*Select one*			
Network reconfiguration data	□	□	□	□	□						*Select one*			
Solutions to avoid outage plans incompatibilities	□	□	□	□	□						*Select one*			
State estimation data	□	□	□	□	□						*Select one*			
System parameter control schema/instructions	□	□	□	□	□						*Select one*			
Possible temporary limits on balancing capacity bids	□	□	□	□	□						*Select one*			
Other information to be considered: *(add below)*	□	□	□	□	□						*Select one*			
	□	□	□	□	□						*Select one*			
	□	□	□	□	□						*Select one*			
	□	□	□	□	□						*Select one*			
	□	□	□	□	□						*Select one*			

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Topic 2 – EXCHANGES OF CYBERSECURITY-RELATED INFORMATION					
Do you belong to any cybersecurity information sharing organization(s)? For example, the European Network for Cyber Security (ENCS) or the European Energy Information Sharing & Analysis Centre (EE-ISAC)					
[Please, describe here]					
If not, is it within your organization's short-term / medium-term plans to become a member of this type of organizations? Can you indicate which one(s)?					
Do you have mechanisms and protocols in place to exchange information on cybersecurity incidents with the other actors of the electricity sector?					
☐ Yes			☐ No		
Which ones (e.g., public specifications/standards applied)?					
[Please, describe here]					
Who participates in these information exchanges?					
☐ TSO	☐ DSO	☐ Customers	☐ Energy service providers (e.g., aggregators)	☐ Market operator	☐ Other [Describe here]
Do these mechanisms depend on the type of information compromised?					
☐ Yes			☐ No		
[Please, describe here]					
Are there specific types of information exchanged per type of cybersecurity incident?					
☐ Yes			☐ No		
[Please, describe here]					

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Topic 3 – COORDINATION OF RESPONSE TO CYBERSECURITY INCIDENTS					
Do you coordinate your response to cybersecurity incidents with the other actors of the electricity sector?					
☐ Yes			☐ No		
Who participates in this coordination?					
☐ TSO	☐ DSO	☐ Customers	☐ Energy service providers (e.g., aggregators)	☐ Market operator	☐ Other [Describe here]
In which way? (e.g., exchanging close-to-real-time information about current status of the network)					
[Please, describe here]					

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Annex B: TSO-DSO Coordination questionnaire outcomes

Topic 1

Table 11 Information per market phase.

Market phase	Information
Phase 1	• Market participant pre-qualification information • Basic participant information • Invoicing data • Flexibility resources information • Limits and margins for capacity (by zone) • Grid constraints assessment
Phase 2	• Baselines reports • Development plans for distribution network • Forecast data • Grid congestions status • Network demand forecast • Prediction of maintenance periods • Short circuit power forecast • Weather forecast (IEC 62325 package environmental)
Phase 3 & 4	• Market results • Execution order
Phase 5	• Flexible Resource Metering data
Other information	• Network characteristics (internal) information • Aggregated data • Resource optimization information • Power flow simulation results • Network information • Network reconfiguration data • State estimation data • System parameter control schema/instructions • Possible temporary limits on balancing capacity bids

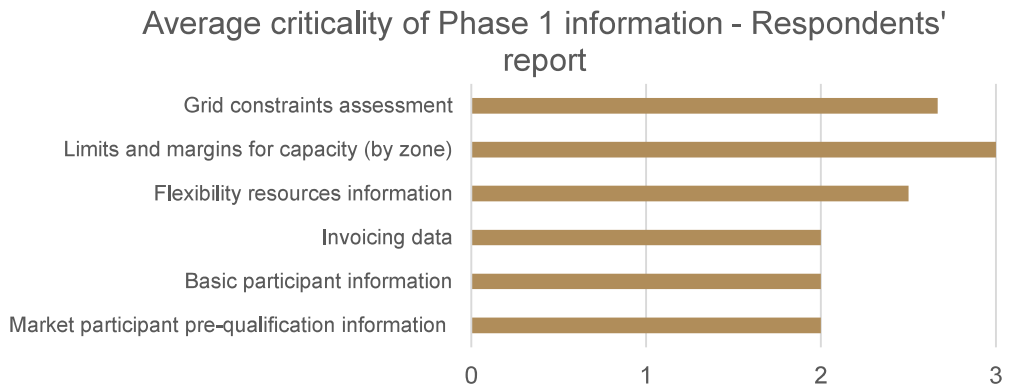

Figure 22 Average criticality of Phase 1 information – Respondents 'report

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

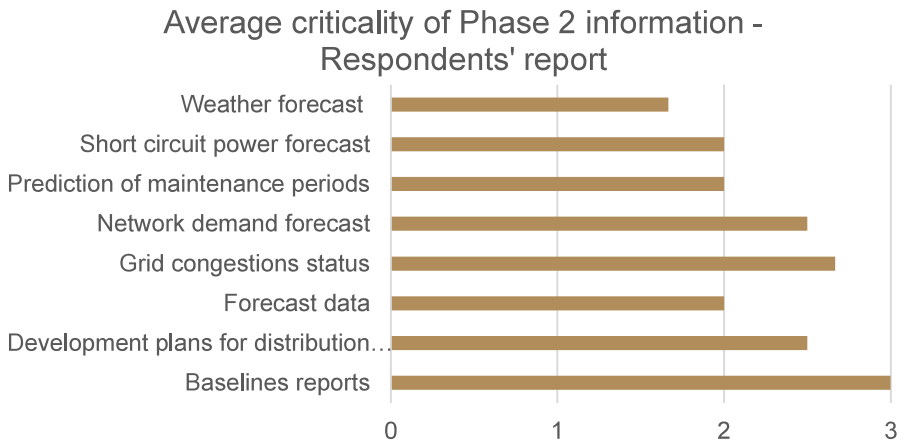

Figure 23 Average criticality of Phase 2 information - Respondents' report

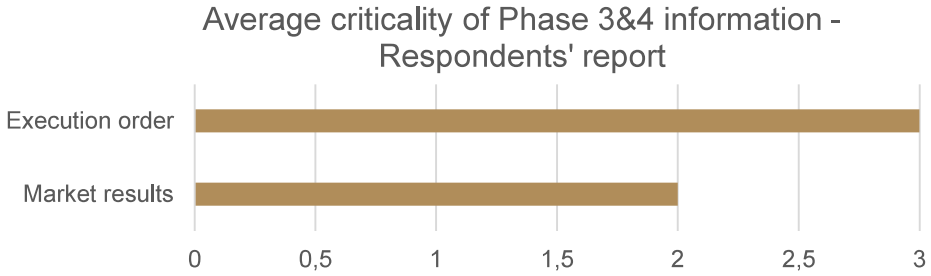

Figure 24 Average criticality of Phase 3&4 information – Respondents' report

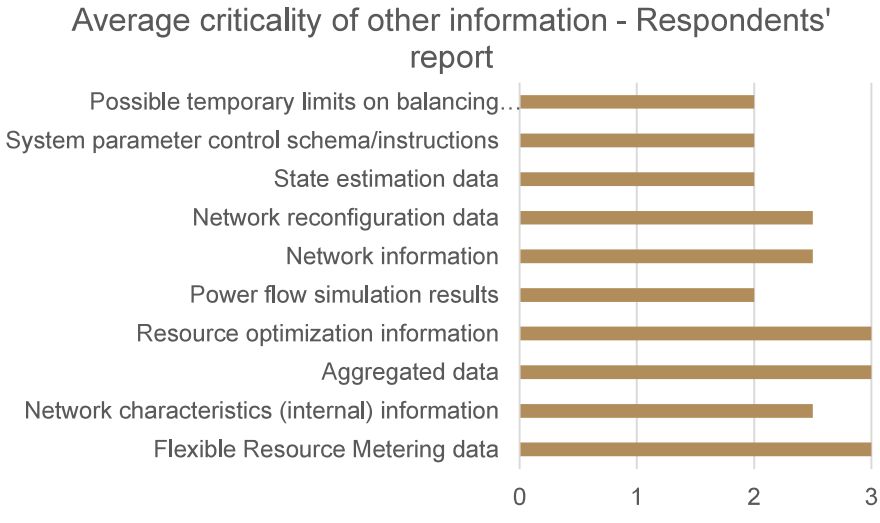

Figure 25 Average criticality of other information - Respondents' report

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.