RE-EMPOWERED

Renewable Energy EMPOWERing European & InDian Communities

D5.1: Report on interoperability standards and their relevance to the project

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Horizon 2020 Grant Agreement № 101018420.

This project has received funding from the Department of Science and Technology (DST) under ''India- EU Joint Call on Integrated Local Energy Systems''.

March 2022

Title	Document Version
Report on interoperability standards and their relevance to the project	2.0

Project number	Project acronym	Project Title
101018420	RE-EMPOWERED	Renewable Energy EMPOWERing European and InDian communities

Contractual Delivery Date	Actual Delivery Date	Type*/Dissemination Level*
31/03/2022	31/03/2022	R/ PU

Responsible Organization	Contributing WP
DTU	WP5

*Type	*Dissemination Level
R Document, report	**PU** Public
DEM Demonstrator, pilot, prototype	**CO** Confidential, only for members of the consortium (including the Commission Services)
DEC Websites, patent fillings, videos, etc.	**EU-RES** Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)
OTHER ETHICS Ethics requirement	**EU-CON** Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)
ORDP Open Research Data Pilot	**EU-SEC** Classified Information: SECRET UE (Commission Decision 2005/444/EC)
DATA data sets, microdata, etc	

DOCUMENT INFORMATION

Current version: V2.0

Authors: Kanakesh Vatta Kkuni (DTU), Mirza Nuhic (DTU), Guangya Yang (DTU), George Kiokes (ICCS-NTUA), Alkistis Kontou (ICCS-NTUA)

REVISION HISTORY

Revision	Date	Description	Author (partner)
V0.1	15.01.2022	TOC	DTU
V0.2	10.03.2022	Review of standards and communication protocols and technologies	ICCS-NTUA
V1.0	18.03.2022	First Draft for Review	DTU, ICCS-NTUA
V1.1	25.03.2022	Revision according to reviewers' feedback	DTU, ICCS-NTUA
V2.0	31.03.2022	Submitted version	DTU, ICCS-NTUA

REVIEWERS

Description	Name	Partner	Date
1	Stefanos Dallas	PROTASIS	23.03.2022
2	Anirudh Kumar	CSIR-CMERI	25.03.2022

COPYRIGHT STATEMENT

EXECUTIVE SUMMARY

One of the main objectives of the "RE-EMPOWERED" project is to develop and demonstrate novel digital tools that will accelerate the energy transition of the islanded /isolated communities. The digital tools will integrate the functions developed in the project that aids in the optimized management of multi-energy microgrid, demand-side management and increased community engagement.

The recent development in standardization and Information and communications technology (ICT) in the field of smart grid and smart cities have high relevance to the digital tools to be developed in the RE-EMPOWERED. To that end, this document reviews existing relevant standards and communications technologies that promote interoperability and replicability of the digital tools to be developed in the project. A thorough study on the interoperable standards, communication protocols, communication technologies is conducted, and relevance to RE-EMPOWERED, linking to the project's needs and use cases, is assessed and documented in this report. In addition, the considerations for cyber security for digital tools and security standards are outlined in this report. The task will also outline a set of testing measures to validate the digital tools developed in the project.

The state of the art analysis in ICT and standards presented in these will form the basis for the digital tool development performed in WP4 and WP5 and ensure the developed tools have high replicability and scalability in the EU and India.

KEYWORDS:

Smart Grid, Smart Cities, Communication Networks, Power Utility Automation, Safety Standard, Data Model, Communication Layers, Communication Protocols

TABLE OF CONTENTS

List of Figures

List of Tables

Acronyms

Acronym	Description
AMI	Advanced Metering Infrastructure
API	Application Programming Interface
CIM	Common Information Model
DAS	Day-Ahead Scheduling
DD	Day of Dispatch
DER	Distributed Energy Resources
DNP3	Distributed Network Protocol
DR	Demand Response
EMS	Energy Management System
EMS	Energy Management System
EPA	Enhanced Performance Architecture
ES	Electrical System
EV	Electric Vehicle Supply Equipment
FIT	Failure in Thousand
GOOSE	Generic Object Oriented System Event
GSM	Global System for Mobile Communications
HD	Hour of Dispatch
HIL	Hardware In the Loop
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technology
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IoT	Internet of Things
IP	Internet Protocol
LAN	local area network
LoRaWAN	Lo(ng) Ra(nge) Wide Area Network
LTE	Long-Term Evolution
MGCC	Microgrid Central Controller
MMS	Manufacturing Message Specification

MQTT	Message Queue Telemetry Transport
MTBF	Mean Time Between Failure
NIIPSs	Non-Interconnected Isolated Island Power Systems
NIIs	Non-Interconnected Islands
OCPP	Open Charge Point Protocol
OSI	Open Systems Interconnection
PDU	power distribution unit
PV	Photovoltaic
PaaS	Platform as a Service
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SO	Socio-economic Objectives
SSL	Secure Sockets Layer
SV	Sampled Values
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VPN	Virtual private network
WAN	Wide-Area Network

1 Introduction

1.1 Purpose of the document

This deliverable reports the analysis of the standards, their applicability, data model, and implementation suggestions, performed in T5.1 as a part of Work Package 5 (WP5) titled "Digitalization, Interoperability and system integration". This report identifies the standards and data models, communication protocols, and communication technologies relevant to the digital tools that will be developed in the project. The highlights of these technologies and standards are reported in this deliverable.

The report also analyses the communication considerations of the project while identifying the relevant standards related to cyber security aspects linked to the tools. The mapping of the technologies and standards to RE-EMPOWERED is presented in the report focusing on interoperability and security. The report also outlines testing measures for validating the project's digital tools to be developed. This document lays the foundation of the digital tool development linked to the project with considerations for scalability and replicability.

1.2 Structure of the document

This document begins with the defined executive summary, and the Introduction chapter follows. The report then introduces the digital tools that are being developed in the project and the overall objective. A review of the standards and data models relevant to the project is presented in section 3. Then, highlights of communication protocols and technologies employed in the digital tools and their associated references are reported in section 4. The communication considerations, in terms of reliability, security and latency, are presented in section 5. The testing measures to validate the digital tools being developed as a part of the project are outlined in section 6. Finally, the relevance of the reported standards and solutions and the mapping to RE-EMPOWERED tools are given in section 7, followed by a conclusion in section 8.

2 RE-EMPOWERED Objectives of the Digital tools

The project aims to develop novel digital tools that will accelerate the energy transition of the islanded /isolated communities. The primary objectives of the RE-EMPOWERED project and the developed digital tools are shown in Figure 1. RE-EMPOWERED objectives are organized in 3 pillars, each comprising a set of objectives. The first pillar includes 4 Technical Objectives (TO), the second pillar 3 Socio-economic Objectives (SO), and the third pillar includes 2 Coordination Objectives (CO). The pillars of the project and objectives and mapping with the ecotools are also shown in Figure 1. Although all the tools developed have some applicability for ICT, the most relevant for this report are ecoEMS, ecoMicrogrid, ecoDR, eco-Planning and ecoPlatform.

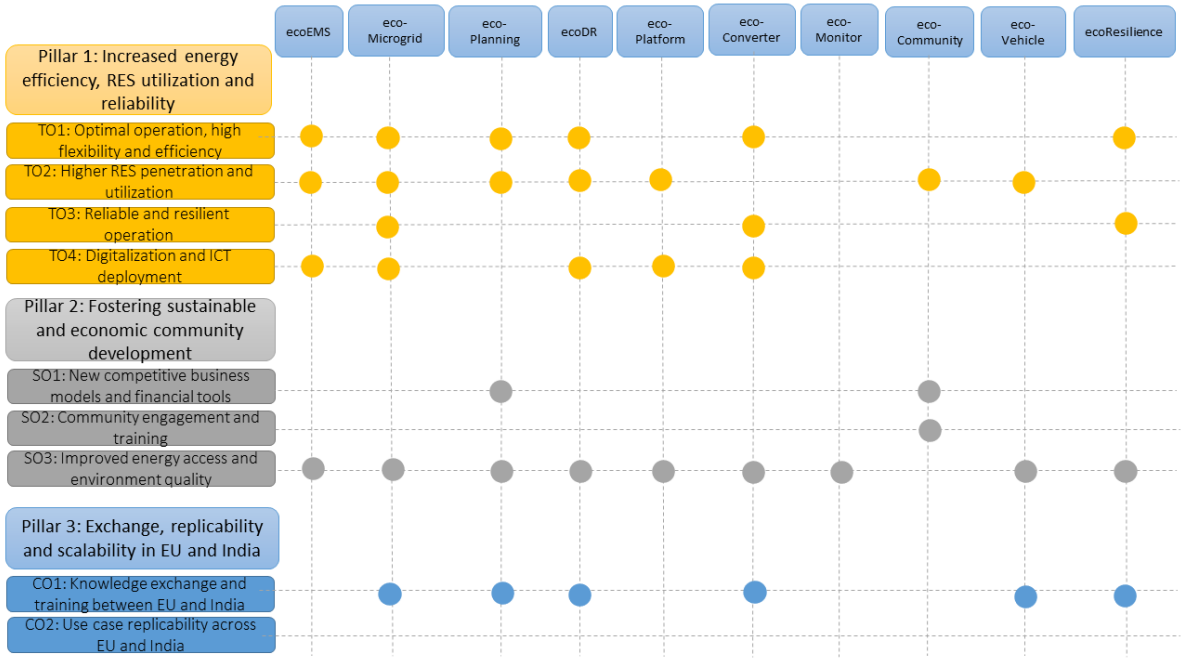

Figure 1 RE-EMPOWERED objectives and ecoToolset solutions

3 Standards and Data models

Several standards and data models are related to the project's information exchange and communication aspects applicable to ecotools and demo sites. The summary of relevant standards and data models, with their applicability and scope within the smart grid domain and suitable references, are shown in Table 1. The mapping between the standards and data models presented in Table 1 is presented in section 7.

Table 1: Standards and data models relevant to data collection, communication, and exchange

Standard	Applicability	Scope	Summary
OPC (Open Platform Communications) [1]	SCADA, IED, MGCC	Industrial communication	• It aims at a reliable and secure data exchange in industrial automation and also for other industries • Specifications For ○ The interface between Clients and Servers ○ Real-time data transfer between data acquisition system and SCADA ○ Unified Architecture
IEC 61850 [2]	Electrical substation	Ethernet communication between IEDs in a substation	Defines abstract data models, Communication requirements • Defines mapping of the data abstract services into actual protocols
IEEE 1547 [3]	DERs and power system interfaces	communications system for DER	• Communications capability, Capability, and performance • DER information exchange
Open Charge Point Protocol (OCPP) [4]	EV charging stations	communication between Electric vehicle (EV) charging stations and charging station network	• Aim for interoperability in the EV charging industry. • The protocol describes the exchange of charging data and information between electric vehicles and system administrators.
OPENADR [5]	DER	Communication for automated DR and DER management	• Facilitates interoperable information exchange among Smart Grid standards • an open, highly secure, and two-way

			information exchange model and Smart Grid standard
IEEE 2030 series [6]	End-Use Applications and Loads	Microgrid controller testing and smart grid interoperability	• A knowledge base addressing terminology, characteristics, functional performance and evaluation criteria • Specifications, requirements and testing procedures for microgrid controllers
IEC 60870 part 5 [7]	SCADA, IED, MGCC	Telecontrol equipment and systems in power transmission grids	• Provides a communication profile for sending basic telecontrol messages between a central telecontrol station and telecontrol outstations with permanent directly connected data circuits
Common Information Model (CIM) IEC 61968-11:2010 [8] IEC 61970-301:2020 [9]	All components	power systems data exchange	• An abstract data model for representing the objects in electric utility • CIM facilitates the interoperability of network applications from different vendors
Sunspec [10]	Distributed Energy Resource (DER)	DER parameters, settings, communication	• Provides standard Modbus communication interfaces for IEDs, DER, smart meters • Defines best practices in cyber security for DERs
IEC 62056 part 21 [11]	Electricity metering	Data exchange for meter reading, tariff and load control	• Describes hardware and protocol specifications

4 Communication Protocols and Technologies

4.1 MQTT

MQTT [12] is a messaging transport protocol based on the Client/Server Publish/Subscribe messaging pattern under the OASIS standard. The protocol is designed to be very lightweight and suitable for connecting remote devices while keeping the network bandwidth requirements low and leaving a marginal code footprint. The application of MQTT is varied in the context of the Internet of Things, and the usage ranges from manufacturing and telecommunication to the oil and gas industry. The operating principle of MQTT is based on two basic network concepts of clients and brokers. The MQTT clients send and receive messages from the broker, while the broker receives messages from clients and directs them to the correct destination clients. An MQTT client is any device that operates an MQTT library and is connected to an MQTT broker via a network infrastructure.

4.2 HTTPS

HTTPS (Hypertext Transfer Protocol Secure) is an internet communication protocol designed to protect the data being exchanged between the user and the web page in terms of integrity and confidentiality. HTTPS is an extension of the HTTP protocol, which has added an encryption layer of SSL (Secure Sockets Layer)/TLS (Transport Layer Security) to protect the traffic between users and web pages. The protocol should be trusted by the user if and only if the requirements put forth are valid and true. [13]

4.3 MODBUS

MODBUS [14] is an application-layer communication protocol that provides a platform for transmitting data between various electronic devices. MODBUS is an open protocol, which means that it is free to implement by the industry into their devices, and it has been an industrial standard since 1979. The MODBUS can be accessed through a system port 502 on the TCP/IP protocol stack. The services offered by the MODBUS protocol are determined by the function codes.

4.4 DNP3

DNP3 [15] is a free to use, standards-based, interoperable communication protocol designed for the electric utility industry. DNP3 is specifically intended to provide a communication platform for the SCADA (Supervisory Control and Data Acquisition) system, enabling data exchange between substation computers, RTUs, IEDs on one side, and master stations on the other side. The protocol incorporates standards of the IEC technical committee 57 for telecontrol applications. DNP3 has also been sanctioned by IEEE in 2010 as IEEE Std. 1815-2010.

4.5 Communication Technologies

Table 2: Communication technologies relevant to the project

Communication Technology	Short Description
WiFi (Wireless Fidelity)	• *"Most commonly used wireless communication technology and a primary medium for global internet traffic." [16]* • Based on the IEEE 802.11 standard
WAN (Wide Area Network)	• *"WAN is a collection of local-area networks (LANs) or other networks that communicate with one another. A WAN is essentially a network of networks, with the Internet being the world's largest WAN." [17]* • It provides a set of application layer services that are applicable in Advanced Metering Infrastructure (AMI).
LORAWAN (Long Range Wide Area Network)	• *"LoRaWAN is a low power wide area network with features supporting low-cost mobiles phones, to ensure two-way communication for the Internet of Things (IoT), machine-to-machine (M2M), smart city and industrial applications." [18]* • It was envisioned as a wireless protocol for low power communication over long range.
GPS (Global Positioning System)	• *"The Global Positioning System (GPS) is a U.S.-owned utility that provides users with positioning, navigation, and timing (PNT) services. This system consists of three segments: the space segment, the control segment, and the user segment. The U.S. Space Force develops, maintains, and operates the space and control segments." [19]* • GPS antennae use NMEA protocols to transmit data to other devices.
LTE-GSM (Long Term Evolution and Global System for Mobile communication)	• *"The Global System for Mobile Communications (GSM) is a standard for digital cellular communications developed by the European Telecommunications Standards Institute (ETSI)." [20]* • Deployed in Finland in 1991., the standard defines protocols for the second generation (so called 2G). • *"4G-LTE networks are based purely on packet switched network, which is mainly designed for high-speed data transfer across the network." [20]* • Some of the advantages of 4G are: improvements in data rates, improvements in

	spectral efficiency, latency improvements, compatibility with previous versions, etc.
ZigBee	• *"ZigBee is a wireless technology developed as an open global standard to address the unique needs of low-cost, low-power wireless IoT networks. The Zigbee standard operates on the IEEE 802.15.4 physical radio specification and operates in unlicensed bands including 2.4 GHz, 900 MHz and 868 MHz." [21]* • The protocol is designed for communication within noisy environments in industrial applications.

5 Communication Considerations

5.1 Reliability

Network availability is considered the most critical measure among confidentiality, integrity, and availability (CIA) triad principles of a security infrastructure [22]. Network availability specifies the probability of the percentage of time the network is available in a year. The network downtime in a power grid can have severe consequences and lead to blackouts; therefore, the availability requirements for power grid communication networks are more stringent than other networks. Some of the threats that can jeopardize the network availability are Denial of service attacks, hardware loss, and loss of power. For this reason, the network equipment used in the smart grid is required to be of greater reliability with a recommended use of "utility-grade" network equipment. A piece of utility-grade equipment enforces higher reliability with measures such as redundant processors, power supplies and the ability to operate in a harsher environment. The standards IEC 61850-3 [30] and IEEE 1613 [31] specify a hardened requirement for network equipment deployed in power plants and substations. Some useful metrics to quantify the reliability are Mean Time Between Failure (MTBF) and Failure in Thousand (FIT).

5.2 Security

A large amount of information is collected and exchanged within the smart grid infrastructure. The diverse nature of the smart grid architecture and deployed communication technologies present substantial challenges to the system's security. A security breach of the smart grid ICT infrastructure can be potentially exploited to trigger cascaded outages of the power grid and thus resulting in devastating consequences. With the possibility of leveraging cascading failures in the power grid, it may not even be necessary for an attacker to get access to large-critical resources/operators of the smart grid to cause an outage across a wide region. Even a security breach that gives the attacker access to consumer electronics is also a potential threat to system security [22]. In addition, the possible infringement of the consumer's privacy, which could open up avenues for fraud, is also a cause of concern in the smart grid.

Several of the security challenges are unique to the digitalization of power grids. For the majority of the commercial data transmission systems, a preference is given to security and confidentiality of the data over throughput, whereas in the smart grid, which requires real-time or near real-time information for reliable operation, data latency and throughput are considered vital [23]. Several solutions that enhance security, such as firewalls, intrusion detection systems (IDS), and message encryption, can conflict with lower latency and high throughput requirements in the smart grid [24]. For this reason, some of the most widely used communication protocols, such as MODBUS and DNP3, developed with the goal of communication efficiency, do not support security mechanisms. As a result, smart grid systems reliant on such unsecured process control networks, without the security measures such as encryption and authentication, are susceptible to messages being interrupted and altered by an attacker [24]. Such challenges are amplified by the need to use public ICT facilities to control costs.

Several smart grid standards are in place to improve the cyber security of the smart grid. In addition to emerging standards on cyber security related to power grids, some of the standards pertaining to ICT and industrial automation also have high relevance to smart grid security. [25] The following are some of the relevant standards for smart grid cyber security.

- ISO/IEC 27019 [26] standard advice on the security of control, communications technologies, and automation systems in the power system domain.
- IEC 62351-x [27]: provides a comprehensive series of documents on the security measures for power system data exchanges. The standard includes guidelines and reference models for increasing security on the system level. In addition, the standards can be applied directly to system deploying protocols such as IEC 61850 and IEC 60870-x.
- IEEE 1686: IEEE Standard for substation intelligent electronic devices (IEDs) cyber security capabilities [28]. The standard specifies the features and functions to be incorporated in the IEDs in the electric sector. In addition, the requirements related to control and communication port access, event logging, configuration and data retrieval from IEDs are addressed in this standard.
- IEC 62443 [29]: A series of standards defines the requirements for cybersecurity of control and industrial automation systems.

5.3 Latency

Smart grid operation consists of several tasks that need to be executed in real-time. Limiting the time delays can be crucial in faults and anomalous operations requiring timely information transfer. At the same time, larger delays in the order of a few hundred milliseconds can be tolerated in applications such as smart meters. The size of the data packet is one of the major contributors to the latency in the smart grid, a larger packet size results in larger delays. The processing time added with the inclusion of network security measures such as firewalls and encryption also significantly adds to the delays in the smart grids.

6 Testing measures for validation

Smart grid systems exhibit a very high level of complexity in terms of communication and interoperability in an interconnected network. Therefore, when conducting performance validation tests, there should be a predefined set of services and parameters to be validated, such as latency and packet loss measurements through Packet Error Rate (PER) or other values. The PER is the number of incorrectly transferred data packets divided by the number of transferred packets. A packet is assumed to be incorrect if at least one bit is incorrect.

Several approaches can be applied regarding communication validation; software simulation, hardware-in-the-loop, and field trials. Smart grid communication has the crucial requirements of fast authentication and encryption/decryption, low latency, interoperability, high reliability and accuracy. The testing of functions will be supported by a virtual environment set up that replicates the conditions expected at each demo site. After implementing the tools involved, the validation process will be carried out in the field. The feature that needs to be tested regarding communication is data transmission between two communication endpoints, which can vary from communication between specific tools to communication between a tool and a device.

- **ecoEMS**

  The objectives of the ecoEMS software are to enable the establishment and the solution of the Day-Ahead Scheduling (DAS) of the Non Interconnected Isolated Island Power Systems (NIIPSs), which consists the pillar of the short term energy and ancillary services market; at the same time, it may support the intraday energy market processes, according to the regulatory framework, with the publication of the correspondingly Dispatch Orders of the Economic Dispatch (ED), within the Day of Dispatch (DD) for every Hour of Dispatch (HD). Both the objectives described contribute toward the optimal dispatch of the centralized and decentralized energy resources installed in the Electrical System (ES). Epigrammatically, targets are:

1. Minimization of the operational cost of conventional energy production,
2. Maximize Renewable Energy Resources (RES) penetration as possible, respecting all operational constraints towards the safe and smooth operation of the ES.

   ecoEMS will communicate with all generation assets' SCADA systems through an intermediate SQL database developed as part of the ecoEMS tool. Finally. Communication between ecoEMS and ecoPlatform will be available through the Enterprise Service Bus (ESB). The following features will be tested remotely, as the deployment will be on ICCS-NTUA premises:

   - Ensure stable connectivity with SCADA systems
   - Collecting data of generation units and storing it in a local operational database.
   - Collecting forecasting data and storing it in a local operational database.
   - Collecting flexibility information from ecoDR.
   - Scheduling of generation units through Dispatch Orders.

- **ecoMicrogrid**

  The ecoMicrogrid is a tool for achieving optimal operation of smaller-scale local energy systems, like microgrids of a few kW. ecoMicrogrid will be capable of communicating with various assets in a real environment using DNP3, Modbus, IEC61850 and SQL.

The communication between ecoMicrogrid and ecoDR and between ecoMicrogrid and various devices (EV charging stations, converters, smart meters) will be through a data concentrator module, which ensures online data gathering. Furthermore, a SCADA system will be available for data monitoring, developed as part of the ecoMicrogrid tool. Finally, communication between ecoMicrogrid and ecoPlatform will be available through the Enterprise Service Bus (ESB). The following features will be tested virtually and validated in field test:

  - Collecting smart meter data and storing it in a local operational database.
  - Collecting data from EV charging stations and storing it in a local operational database.
  - Scheduling of controllable devices available and communicated to the devices.

- **ecoPlatform** is a cloud-based platform used as an intermediary for software-based tools. ecoPlatform can convey commands to controllable assets directly or indirectly through other tools. The communication between the various ecoTools and ecoPlatform will be through the Enterprise Service Bus (ESB), serving as the main communication platform for all modules. The features to be tested are:
  - Collecting data from dependable tools and storing it in a global cloud-based database.
  - Issue commands to controllable assets through dependable tools (ecoEMS, ecoMicrogrid).
  - Communicating pricing and other data to consumers through ecoCommunity.

- **ecoPlanning** tool allows performing simulations for studying the development program of Non-Interconnected Islands (NIIs) with respect to the deployment of new electricity generation units (from conventional and renewable resources) and the implementation of interconnections between NIIs. For the scope of the tool, an SQL database will be developed as part of the ecoPlanning tool.
  The tool will offer methods to estimate yearly demand and peaks for the next seven years, hourly system simulation up to 7 years, includes all RES technologies agreed and communicate with a database with data for all ESs. A summary of the simulation results will be projected in the browser tab, and analytical hourly reports will be stored in the server to retrieve if needed. The tool will be available as an online environment to create and store scenarios, and the following features will be tested remotely, as the deployment will be on ICCS-NTUA premises:
  - Collecting data of generation units and storing it in a local operational database.
  - Collecting load and RES time-series data and storing them in a local operational database.

7 Relevance to RE-EMPOWERED

The "RE-EMPOWERED" project aims to develop novel tools that can provide complete energy solutions for the islanded /isolated communities and microgrids. Although the developed toolset will be tailored to the four demo sites, the tools are being developed with high replicability and consequently have a high potential for further implementation of the eco tools around the world. The overview of the demo sites and the eco tools linked to the ICT application developed in the project are shown in Table 1 and Table 2. The report focuses on the standards, communication networks and systems for power utility automation applicable to the developed eco tools.

All the demo sites have diverse characteristics in terms of available infrastructure, technologies, actors and socioeconomic boundaries. For example, a SCADA system for control and monitoring of DERs and IEDs is already in place at the Kythnos and Bornholm demo sites, and the eco tools will be built with SCADA interfaces as a starting point. However, for the Indian demo sites, a SCADA system does not exist, and the eco tools will form the basic control and monitoring solutions.

Table 3: Overview of the demo sites

Demo Site	Energy Infrastructure	ICT Development
Kythnos	PV, Wind*, Desalination plant, Diesel Generation	SCADA system, Monitor and manage the DER, and Desalination plant, VPN connection
Gaidouromantra	PV, Wind, Battery, Diesel Generation, Controllable water pumps	Monitoring DER and load data, high accuracy power quality measurements at the ecoMicrogrid, control of flexible loads and data storage
Bornholm	PV, Wind, Straw boiler, electric boiler, Household loads	SCADA System, Monitoring for DER and district heating network, VPN connection
Keonjhar	Biomass, PV, EV charging station, House hold loads	Monitoring DER and load data, VPN connection
Ghoramara	PV,Wind, charging station, Household loads	Monitoring DER and load data, VPN connection

- Currently, the wind parks in Kythnos are out of order, but actions are planned for the repowering.

Table 4: Overview of the eco tools linked to ICT application

Tool	High-level description	Key ICT functions	Relevant Standards, Communication Protocols and Technologies
ecoEMS	Energy Management System for isolated and weakly interconnected energy system	Real-time system monitoring, data acquisition and data exchange	DNP3, OPC, Modbus, IEC61850, CIM, WAN, VPN connection, Sunspec, OPENADR, IEC 61850 – GOOSE, MMS, SV
ecoMicrogrid	Advanced energy management system for microgrids	Communication with controllable assets, Data concentration, storage and management, Real-time microgrid monitoring and data acquisition	IEEE 1547, IEC 61850, DNP3, Modbus, SQL Drive WAN, MQTT, Sunspec, OPENADR, OCPP, IEEE 2030, GOOSE, MMS, SV, WiFi, GPS, ZigBee, LoRaWAN, LTE-GSM
ecoPlanning	Allows performing simulations for studying the development plan of the ES	Communication with SQL database for static data, safe communication with deployment server for analytical results retrieval	MSSQL, VPN connection
ecoPlatform	Platform with a focus on interoperability, secure and reliable communication between the ecotools	Intermediary for software-based tools to convey commands to controllable assets, Data storage hub for dependent tools	MQTT, LORAWAN, WAN, CIM, TCP/IP, IEC62056-21/IS15959
ecoDR	Advanced metering infrastructure (AMI) with inbuilt load controller and protection functionalities	Energy monitoring, Scheduling of loads	WAN, CIM, DLMS/COSEM, IEC62056-21/IS15959
ecoCommunity	Digital platform developed aiming to enhance citizen engagement	Displaying the dynamic pricing Data security and privacy,	WAN, CIM, MQTT,

7.1 Applicability of Standards, Communication Protocols and Technologies for ecotools

The ecoEMS, an Energy Management System, has a primary ICT function of Real-time system monitoring, data acquisition and data exchange. The tool already has connectivity to commercial SCADA using DNP3, OPC, Modbus, IEC61850, ICCP. Among the data models, the IEC 61850, which defines the data models to facilitate interoperability of all the devices in a substation, is relevant to the ecoEMS in accessing and monitoring the controllable assets and metering devices interfaced to the SCADA systems. In addition, the ecoEMS is expected to communicate with other ecoTools wherein a CIM data model can be relevant to ensure the future replicability of the tool.

The ecoMicrogrid is an advanced energy management system for microgrids, with high-level functions that include forecasting, outage detection and communication to ecoTools. The tool connects directly with the MG devices via DNP3, IEC 61850 MMS and ModBus. The tool is expected to support a more comprehensive set of protocols and communication technologies to establish communication with all the MG devices in the different demo sites. The development of the tool will be based on essential standards for achieving interoperability, like IEEE 1547 and IEEE. The data exchange with the other ecoTools is suggested via the enterprise service bus, which can be implemented with the protocols such as HTTP, MQTT, or AMQP. Therefore, the ecoMicrogrid is also recommended to be capable of supporting these protocols, among others, to support communication with external tools and services.

The ecoPlatform is the Interoperability and integration platform, which serves as a service bus for data exchange between the eco tools capable of asynchronous operations, publish/subscribe, point to point and structured first in, first out capabilities. The service bus can be built over protocols such as HTTP, MQTT, or AMQP on top of TCP/IP protocol. In addition, the ecoPlatform also provides direct access to a limited set of sensors located in selected demo sites where there is a challenge in integrating these sensors with other tools. Wireless communication technology such as LORAWAN is a suitable choice in such scenarios.

The ecoDR is an advanced metering infrastructure (AMI) with an inbuilt load controller and protection functionalities. The lightweight MQTT protocol over TCP/IP can be used for ecoDR to interface with other eco tools. The unbundled smart meter data can be based on the standard CIM MeterReadings (IEC61968).

The ecoCommunity is a Digital platform developed to enhance citizen engagement. From the ICT perspective, the ecoCommunity communicates directly with ecoPlatform over a service bus by means of an API. Therefore, the ecoCommunity is suggested to have support for MQTT, TCP/IP. In addition, the ecoCommunity handles the data from smart meters and loads, which is communicated via ecoPlatform; thus, there is a need to support common data models such as CIM and IEC 61850.

7.2 Delays and Security

For smart grid applications, timely actions are required in the control system when the system experiences fault and anomalous behaviour. For the eco tools, simillar to other smart grid applications, timely and reliable delivery of certain messages and commands is important, especially for the tools engaged in the lowest level functions, such as ecoDR and ecoMicrogrid. IEEE-1646 standard [32], which specifies the time performance requirements for electric power substation automation, is highly relevant for the eco tools development in the project. The requirement of the delay and signal priority depends on the application. For example, the delay in communication for the protection and under frequency load shedding

components, to be handled by ecoMicrogrid, is to be kept in a few milliseconds. Priority for such signals, which is a quality of Service (QoS) parameter, also needs to be high. On the other hand, the message types such as "Text Strings " and "Processed Data Files", which are expected to be handled by ecoCommunity, can tolerate delays.

Some of the practical methods to reduce the threat of cyber-attack for the eco tools can be summarized as follows:

1. Separating the network into different zones with boundaries defined. The implementation of different eco tools achieves the segregation of networks in RE-EMPOWERED. For example, the ecoMicrogrid can be considered the deepest layer in the ecotools security zone. The ecoMicrogrid directly interfaces with the power grid components and only allows essential communication with the external network via ecoPlatform with additional information security measures.
2. Ensuring authorized access to the tools and components with authentication and authorization techniques.
3. Implementing firewalls and intrusion detection systems at higher levels of eco tools does not compromise the bandwidth of the data transfer between critical assets.

8 References

[1] "OPC Unified Architecture" Available [Online]. https://opcfoundation.org/products/view/opc-unified-architecture-book

[2] IEC TR 61850-1:2013, Communication networks and systems for power utility automation – Part 1: Introduction and overview.

Available [Online]. https://webstore.iec.ch/preview/info_iec61850-1%7Bed2.0%7Db.pdf

[3] IEEE Standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces in IEEE Std 1547-2018, Revision of IEEE Std 1547-2003, vol., no., pp.1-138, 6 April 2018

[4] "OPEN CHARGE POINT PROTOCOL 2.0.1" Available [Online]. *https://www.openchargealliance.org/*

[5] "OPEN CHARGE POINT PROTOCOL 2.0.1" Available [Online]. https://www.openadr.org/

[6] 2030-2011 - IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads in IEEE Std 2030-201, vol., no., pp.1-121, 10 Sept. 2011

[7] IEC 60870 part 5 Telecontrol equipment and systems - Part 5: Transmission protocols - ALL PARTS Available [Online].

https://webstore.iec.ch/publication/3755

[8] IEC 61968-11 Ed. 1.0 b:2010 - Application integration at electric utilities - System interfaces for distribution management - Part 11: Common information model (CIM) extensions for distribution Available [ONLINE] https://webstore.ansi.org/Standards/IEC/IEC6196811Ed2010

[9] *IEC 61970-301 Ed. 7.0 en:2020* - Energy Management System Application Program Interface (EMS-API) - Part 301: Common Information Model (CIM) Base Available [ONLINE] https://webstore.ansi.org/Standards/IEC/IEC61970301Eden2020?msclkid=2b767fd02d9a1ea5bc7c1df6651eda96&utm_source=bing&utm_medium=cpc&utm_campaign=IEC%20ROW&utm_term=IEC%2061970-301&utm_content=IEC2014

[10] "Specifications-SunSpecAlliance" Available [ONLINE] *https://sunspec.org/specifications/*

[11] “IEC 62056-21:2002 Electricity metering - Data exchange for meter reading, tariff and load control - Part 21: Direct local data exchange” Available [ONLINE] at https://webstore.iec.ch/publication/6398.

[12] MQTT Version 5.0 OASIS Standard 07 March 2019 Available [ONLINE] https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.pdf

[13] "Secure your site with HTTPS". Google Support. Google Inc. Archived from the original on 1 March 2015. Retrieved 20 October *2018. Available [ONLINE] Https://developers.google.com/search/docs/advanced/security/https?hl=en&visit_id=637824455306722205-3001416759&rd=1*

[14] "MODBUS APPLICATION PROTOCOL SPECIFICATION V1.1b3" Available [ONLINE] https://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf

[15] 1815-2010 - IEEE Standard for Electric Power Systems Communications -- Distributed Network Protocol (DNP3) vol., no., pp.1-821, 23 July 2010

[16] “Wi_Fi is…” Available [ONLINE] at https://www.wi-fi.org/discover-wi-fi

[17] "What is a WAN" Available [ONLINE] https://www.cisco.com/c/en/us/products/switches/what-is-a-wan-wide-area-network.html

[18] "What is LoraWAN Specification" Available [ONLINE] https://lora-alliance.org/about-lorawan/

[19] "What is GPS?" Available [ONLINE] at https://www.gps.gov/systems/gps/

[20] "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification" Available [ONLINE] at https://www.etsi.org/deliver/etsi_gts/04/0408/05.03.00_60/gsmts_0408v050300p.pdf

[21] "Understanding the ZigBee 3.0 Protocol" Available [ONLINE] at https://www.digi.com/blog/post/understanding-the-zigbee-3-0-protocol#:~:text=Zigbee%20is%20a%20wireless%20technology,900%20MHz%20and%2086 8%20MHz.

[22] Dabrowski, A., Ullrich, J., & Weippl, E. R. (2017, December). Grid shock: Coordinated load-changing attacks on power grids: The non-smart power grid is vulnerable to cyber attacks as well. In *Proceedings of the 33rd Annual Computer Security Applications Conference* (pp. 303-314).

[23] Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors*, *21*(18), 6225.

[24] El Mrabet, Z., Kaabouch, N., El Ghazi, H., & El Ghazi, H. (2018). Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering*, *67*, 469-482.

[25] Coordination Group on Smart Energy Grids Cyber Security & Privacy, CEN-CENELEC-ETSI Coordination Group on Smart Energy Grids (CG-SEG) Date: 2016-12

[26] ISO/IEC. (2013b). ISO/IEC TR 27019:2013: Information technology Security techniques Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry.

[27] IEC 62351-x Power systems management and associated information exchange – Data and 1606 communication security

[28] IEEE 1686: Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities

[29] IEC 62443 Industrial communication networks - Network and system security

[30] IEC 61850-3:2013 Communication networks and systems for power utility automation - Part 3: General requirements

[31] IEEE 1613-2003 IEEE Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations

[32] IEEE 1646-2004-IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation