Platone

PLATFORM FOR OPERATION
OF DISTRIBUTION NETWORKS

Platone

PLATform for Operation of distribution NEtworks

D6.3 v1.0

Ex-ante qualitative evaluation

The project PLATform for Operation of distribution NEtworks (Platone) receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement no 864300.

Project name	Platone
Contractual delivery date:	28.02.2021
Actual delivery date:	28.02.2021
Main responsible:	NTUA
Work package:	WP6 – Standardisation, Interoperability and Data Handling
Security:	P
Nature:	R
Version:	V1.0
Total number of pages:	42

Abstract

This deliverable performs an ex-ante qualitative analysis of standards discussed in D6.2 “Standard guidelines for each demonstration” and their relationship to the Platone demos. The analysis includes a per-demo and per-technical area discussion on the benefits and drawbacks of certain standards that are of interest to Platone, performed using related literature and technical expertise. Its goal is to assist the demo development. In addition, simulations of the telecommunication infrastructure of one of the Platone demos are performed to investigate the potential of issues arising in the case of increased traffic, such as congestions in the network.

Keyword list

Standards, platform, SCADA, DMS, EMS, AMI, DRMS, energy storage, battery storage, BEMS, cybersecurity, energy markets, blockchain, ex-ante evaluation, simulations

Executive Summary

In this report a theoretical and a technical (via simulations) evaluation of standards that are of interest to the Platone demos was performed. The objective of the evaluation is to ex-ante (i.e., pre-emptively) identify benefits or issues with the standards that are suggested in previous deliverables in order to advise the demo leaders in the implementation of their solutions.

In the first part of this report, a theoretical evaluation is performed on per demo basis. For the Italian demo, there was emphasis on SCADA standards in the IEC 60870-5 family [1], which can have issues with security and limited bandwidth and CIM [2] [3] which is labour intensive in its initial adoption. For communication protocols, Apache Kafka [4] needs special attention in its initial configuration. REST-API [5] comes with lack of state and security issues and MQTT [6] requires increased processing power and memory. For storage systems, the OCPP [7] protocol has the positive aspects that come with an open standard but is accompanied with the corresponding security concerns. For building management protocols, there is special consideration for the oBIX standard [8] which can deal with a large number of electrical and mechanical systems. Finally, Blockchain protocols of interest include the IEEE P2418 and IEEE P2144 families [9]. Potential issues include lack of broad implementation experience, ethical concerns with consensus and access as well as inequity, among other topics and privacy. In addition, as with all blockchain technologies, there is concern with how energy intensive it is going to be.

Regarding the SCADA related protocols of interest to the Greek demo, ICCP [10] is a popular option. Its drawbacks are mostly related to security, either from bypassing controls, authorization violation or information leakage. For PMUs, protocols of the IEEE C37.118 [11] family are of interest, Lack of a secure implementation of a transmission protocol makes such synchrophasors vulnerable to spoofing attacks. For DRMS standards, OpenADR [12] is one of the forefront choices, however, it has scalability issues along with security and privacy issues. Regarding cybersecurity, IEC 62351 [13] and ISO 27001 [14] are under consideration, with the former providing authentication, integrity and confidentiality of data and the latter for development of propriety information security management systems.

In the context of the German demo, for the most technical areas such SCADA, DMS/EMS, Cybersecurity and Blockchain, similar protocols to the previous demos are of interest and similar considerations apply. An area of higher importance to the German demo is Battery Energy Storage Systems, as an integral part of the German demo use case scenarios. Potential challenges are: volume and sometimes inflexibility for the OPC Unified Architecture (UA) [15] and lack of a security layer architecture for the BACnet protocol [16].

The second part of this document covers the simulation of the telecommunication infrastructure of the Greek demo pilot site which serves also as a test case for telecommunication related problems for all three demos. 30 endpoints and one remote host were simulated with the assumption of LTE/4G based telecommunication infrastructure. The simulation was performed using the NS3 event-based simulator. The test scenario involves the creation of congestion issues.

Authors and Reviewers

Main responsible		
Partner	**Name**	**E-mail**
NTUA		
	Panagiotis Pediaditis	panped@mail.ntua.gr
Author(s)/contributor(s)		
Partner	**Name**	
NTUA		
	Georgios Kiokes	
	Andreas Gatos	
	Panagiotis Pediaditis	
Reviewer(s)		
Partner	**Name**	
RWTH		
	Padraic McKeever	
BAUM		
	Manuel Haas	
Approver(s)		
Partner	**Name**	
RWTH		
	Padraic McKeever	

Table of Contents

1 Introduction

The project “PLATform for Operation of distribution Networks – Platone - aims to develop an architecture for testing and implementing a data acquisitions system based on a two-layer approach (an access layer for customers and a distribution system operator (DSO) observability layer) that will allow greater stakeholder involvement and will enable an efficient and smart network management. The tools used for this purpose will be based on platforms able to receive data from different sources, such as weather forecasting systems or distributed smart devices spread all over the urban area. These platforms, by talking to each other and exchanging data, will allow collecting and elaborating information useful for DSOs, transmission system operators (TSOs), customers and aggregators. In particular, the DSO will invest in a standard, open, non-discriminating, economic dispute settlement blockchain-based infrastructure, to give to both the customers and to the aggregator the possibility to more easily become flexibility market players. This solution will see the DSO evolve into a new form: a market enabler for end users and a smarter observer of the distribution network. By defining this innovative two-layer architecture, Platone removes technical barriers to the achievement of a carbon-free society by 2050 [17], creating the ecosystem for new market mechanisms for a rapid roll out among DSOs and for a large involvement of customers in the active management of grids and in the flexibility markets. The Platone platform will be tested in three European trials in Greece, Germany and Italy and within the Distributed Energy Management Initiative (DEMI) in Canada. The Platone consortium aims to go for a commercial exploitation of the results after the project is finished. Within the H2020 programme “A single, smart European electricity grid” Platone addresses the topic “Flexibility and retail market options for the distribution grid”.

WP6 focuses on the topics of standardization and legislation. With regards to standardization, the goal is to support the Platone demos by presenting and analysing the standardization ecosystem and to highlight standards that are relevant to Platone. This is important because this way the Platone project demos will have a clear reference on which standards can be used and which functionalities lack any standardization. In addition, the analysis provides an ex-ante qualitative analysis in Task 6.2.2.

1.1 Task 6.2.2

Task 6.2.2 aims to provide an ex-ante evaluation of the standards identified having relevance to the Platone demos in D6.2 [18]. The goal is to show qualitatively the pros or benefits of the standards used or of interest to Platone and bring up their cons or associated costs, using the existing literature, relevant technical reports and technical expertise. In the end, this task should assist the demo leaders when choosing standards for implementation or when implementing those standards.

1.2 Objectives of the Work Reported in this Deliverable

The objective of the work reported in Deliverable 6.3 is to perform an ex-ante evaluation of the standards identified in D6.2 [18]. The evaluation includes positive and negative aspects of standards that might arise in the case of their implementation during any of the Platone demos.

1.3 Outline of the Deliverable

Chapter 1 is the introduction of this deliverable. Chapter 2 is about the theoretical evaluation of the standards. In Chapter 3, an evaluation of telecommunication standards is performed via simulations of the infrastructure. Chapter 4 is the conclusion of the analysis.

1.4 How to Read this Document

The reader is advised to have read D6.2 [18], but this document can stand alone, also, since some basic description of the most relevant standards is part of this report, too. The reader is also advised to have some basic knowledge of the Platone demos and their highlights.

2 Theoretical analysis

This chapter is performing a theoretical qualitative discussion of the standards that were identified as applicable to Platone in D6.2 [18]. The focus is in analysing the literature and identify common issues of concern, limitations, or other problems that the Platone demos should be aware of. This is an ex-ante analysis that can potentially guide the Platone demos' deployment towards directions with lower cost-benefit ratio.

2.1 Italian demo

2.1.1 SCADA Communication:

There are currently two open communication protocols that provide for interoperability between systems for telecontrol applications. Namely, these are DNP 3.0 [2] and IEC 60870-5-101 [2]. DNP has a strong following in North America, South America, South Africa, Asia and Australia whereas IEC 60870-5-101 is strongly supported in the European region [1].

In the Italian demo, IEC 60870-5 is the standard that is being used. In the section below a short description is given about this standard.

IEC 60870-5 (Transmission Protocols): This part of IEC 60870 provides a detailed functional description for telecontrol equipment and systems for controlling geographically widespread processes (in other words for SCADA systems).

This standard is primarily used in the electrical industry but is not limited in such applications as it has data objects that are applicable to general SCADA applications in any industry.

The structure of IEC 60870-5 is depicted in the following list:

- Sections of Part 5:
  - 5-1: Transmission Protocols
  - 5-2: Link Transmission Procedures
  - 5-3: Structure of Application Data
  - 5-4: Definition of Application Information Elements
  - 5-5: Basic Application Functions
- Companion Standards of Part 5:
  - 5-101: Basic Telecontrol Tasks
  - 5-102: Transmission of Integrated Totals
  - 5-103: Protection Equipment
  - 5-104: Network Access

Special care is advised while adopting IEC 60870-5-101 and IEC 60870-5-104 as both standards lack inbuilt security mechanisms at application and data link layer [19].

Another challenge lies in the communication at data transit level, which are:

- Limited bandwidth, this leads to limited frame length of data being transferred (Example: Only 255 octets can be transmitted both by IEC 60870-5-101 & IEC 60870-5-104 protocols at a time).
- Unreliable media of communication (the communication medium may or may not have security mechanisms implemented) [2].

2.1.2 CIM

Regarding the representation of the topology of the grid, the IEC Common Information Model (CIM) will be used.

The CIM is standardised within three different IEC standard series, namely IEC 61970 [2], IEC 61968 [3] and IEC 62325 [13]. Each of them is shortly described in the following list.

- IEC 61970: These series of standards mainly deal with the definition of an Application Programming Interface (API) for EMS. The main objective of this standard is to provide a standard series including guidelines which support both the integration of multi-vendor

application systems for control centre and information exchange with systems being outside of the control centre environment like other transmission, distribution and generation systems. IEC 61970 consists of different parts each of them for different purposes. The main usage of this series is to describe grids in the transmission level such as elements, measurements geographical location and the necessary data to solve a power (or an optimal power) flow problem.

- IEC 61968: IEC 61968 is essentially an extension of IEC 61970 for distribution systems and can also describe information about assets, customers, load control etc. of a distribution grid.
- IEC 62325: This standard provides technology independent guidelines and requirements for e-business in energy markets, which are based on Internet technologies. It supports the communication aspect of e-business applications in deregulated energy markets with focus on system operator including interfaces between market participants.

CIM is a flexible model, which means that it is possible to implement only a subset of those classes according to the organisation's needs [20].

The result of adopting and implementing a subset of the CIM model classes is called a CIM profile. These profiles can be entirely a custom profile or a standard profile. In the European region a series of standard profiles is provided in order to depict the topology of a grid. It is called Common Grid Model Exchange Standard (CGMES) [21].

For the data modelling, the CIM model uses Universal Modelling Language (UML) to describe its own classes, associations and properties [22].

For the data exchange, the CIM model uses:

- Resource Description Framework (RDF) for the description of the associations between the classes [23] and
- eXtensible Markup Language (XML) for the data exchange [24].

The complete file for data exchanges with CIM is called CIM RDF XML or more shortly CIM XML.

The CIM model as described above consists of numerous classes and the classes consist of numerous properties. It becomes evident that it is quite a challenge for an organisation, especially in the beginning, to adopt the model and successfully implement it. For example, the organisation has to agree in the level of the desired detail concerning the grid topology. According to the level of the detail, the CIM classes or their properties may change.

Another challenge is the difficulty of mapping certain elements to their respective CIM classes. For example, a transformer element is not mapped directly to a CIM class PowerTransformer (according to CIM version 15). Depending on the windings of the transformer, this element will be mapped to a CIM class Power Transformer and associated with two or more CIM classes PowerTransformerEnd.

Moreover, the fact that the CIM model uses RDF and XML to describe its classes and exchange messages is quite a challenge due to the file size that is created. Consequently, an algorithm has to be created to correctly parse this file to extract the necessary data.

However, most of these challenges are overcome once a deeper knowledge of the CIM model is acquired.

The main advantage of adopting the CIM model, is that a large amount of time is saved when it is needed to exchange information about the topology (for example) of a grid with another entity without having to reach an agreement about the structure of the data because CIM is already a standard.

Current versions of the CIM are: CIM15, CIM16 and CIM17.

2.1.3 Communication protocols

Communication protocols which could be used in the Italian demo are:

- Apache Kafka: Apache Kafka is a community distributed event streaming framework capable of handling trillions of events a day. Initially conceived as a messaging queue, Kafka is based on an abstraction of a distributed commit log. Since being created and open sourced by LinkedIn

in 2011, Kafka has quickly evolved from messaging queue to a full-fledged event streaming platform [4].

Kafka has five primary components: producers, brokers, consumers, topics, and ZooKeepers.

Apache Kafka comes with a lot of advantages. It is a little challenging, however, to configure some parameters for Apache Kafka in its initial configuration (for example if message persistence on the broker is needed). As a result, deep knowledge of how Apache Kafka works and special care must be taken when designing the needs upon which this architecture will be built and function.

- REST-API: Representational state transfer (REST) is a de-facto standard for a software architecture for interactive applications that typically use multiple Web services. In order to be used in a REST-based application, a Web service needs to meet certain constraints; such a Web service is called RESTful. A RESTful Web service is required to provide an application access to its Web resources in a textual representation and support reading and modification of them with a stateless protocol and a predefined set of operations. By being RESTful, Web Services provide interoperability between the computer systems on the internet that provide these services. REST offers an alternative to, for instance, SOAP as method of access to a Web Service [5].

  One challenge when using REST-API is lack of state. Most web applications require stateful mechanisms. Suppose you purchase a website which has a mechanism to have a shopping cart. It is required to know the number of items in the shopping cart before the actual purchase is made. This burden of maintaining the state lies on the client, which makes the client application heavy and difficult to maintain.

  Another challenge is lack of security. REST doesn't impose security such as SOAP. This challenge however can be solved by simply wrapping the REST messages over another protocol which has security layer.

- MQTT: MQTT is an OASIS standard messaging protocol for the Internet of Things (IoT). It is designed as an extremely lightweight publish/subscribe messaging transport that is ideal for connecting remote devices with a small code footprint and minimal network bandwidth. MQTT today is used in a wide variety of industries, such as automotive, manufacturing, telecommunications, oil and gas, etc [6].

  One drawback is that MQTT operates over TCP protocol which requires more processing power and more memory than many of the lightweight, power constrained IoT devices have available to them. TCP uses handshake protocol which requires frequent wake up and communication time intervals. This affects battery consumption. Moreover, TCP connected devices tend to keep sockets open for each other which adds to memory/power requirements. Clients must also support TCP/IP.)

  Furthermore, centralized broker limits the scalability as each client devices take up some overhead. In order to avail scalability, local broker hub is used. Centralized brokers can be points of failure as client connections with the broker are open all the time.

  Finally, MQTT does not support advanced features such as flow control.

2.1.4 AMI

Regarding the AMI the IEC 62056 [25] applies.

IEC 62056 is a set of standards for electricity metering data exchange [25]. It is one of the most widely accepted specifications for AMI data exchange in Europe. In fact, it is a series of documents which define various methods for meter reading, tariffs notification and load control. It is based on Device Language Message Specification (DLMS) protocol and Companion Specification for the Energy

Metering (COSEM) model. DLMS is comparable to the set of rules or the common language, which standardize the communication protocol, the data objects and object codes. COSEM provides information about Transport and Application Layers for the DLMS protocol. To abstract various aspects of metering data, it specifies multiple object classes with their attributes and methods of modification. Object Identification System (OBIS) naming is used to identify COSEM objects to make them self-describing. DLMS/COSEM protocol is not limited to electricity metering, it can be also used for water, gas and heat metering.

2.1.5 Battery Storage and Energy Storage Systems

Regarding the Battery Storage and Energy Storage Systems OCPP [7] protocol can also be applied.

The Open Charge Point Protocol (OCPP) offers a uniform solution for the method of communication between charge stations and any central system. With this protocol, it is possible to connect any central system with any charge station, regardless of the vendor. With more than 20,000 installations and participants in 16 different countries, OCPP has become the de facto open standard for open charger to network communications in both Europe and parts of the United States.

A potential drawback of this highly versatile protocol is security threats which need to be taken into consideration when implementing it [26].

2.1.6 BEMS

For Building Energy Management System, protocols which can also be applied are:

- ISO 17800 [27] is an international standard for the Facility Smart Grid Information Model (FSGIM), which is currently under development. ISO 17800 is one of the International Organization for Standardization's group of standards for building environment design, and is the responsibility of ISO Technical Committee 205 (TC205).

- oBIX: oBIX (OASIS Open Building Information eXchange Technical Committee) is an industry-wide initiative to define XML- and Web services-based mechanisms for building control systems. oBIX will instrument the control systems for the enterprise. The purpose of the oBIX TC is to define a standard web services protocol to enable communications between building mechanical and electrical systems, and enterprise applications. This protocol will enable facilities and their operations to be managed as full participants in knowledge-based businesses. The oBIX specification will utilize web services for exchange of information with the mechanical and electrical systems in commercial buildings. Presently most mechanical and electrical systems are provided with embedded digital controls (DDC). Most of these devices are low cost and not enabled for TCP/IP. They are installed with dedicated communications wiring. Larger DDC controllers provide network communications for these dedicated controllers. There are several well-established binary protocols (BACnet, LonTalk, Modbus, and DALI) that are used on these dedicated networks in addition to numerous proprietary protocols. While these binary protocols can be used over TCP/IP networks - they have challenges with routers, firewalls, security, and compatibility with other network applications. There is an added challenge in that the industry is split between several largely incompatible protocols. Because oBIX integrates with the enterprise, it will enable mechanical and electrical control systems to provide continuous visibility of operational status and performance, flagging problems and trends for system analysis or human attention. oBIX provides a technology that enables facilities operators, owners and tenants to make decisions based on a fully integrated consideration of all life-cycle, environmental, cost, and performance factors [8].

2.1.7 Blockchain

Regarding the Blockchain Technology, the following protocols could be applied:

- IEEE P2418.5: It is a standard which provides an open, common, and interoperable reference framework model for distributed ledger technology (DLT), such as blockchain in the energy sector. It also covers three aspects: 1) Serve as a guideline for Blockchain DLT use cases in Electrical Power and energy industry value chains, covering the Renewable energy industry and their renewable related sources services of generation. 2) Create standards on reference

architecture framework, including interoperability, terminology, functionality, and system interfaces for blockchain DLT applications in the energy sector by building an open protocol and technology agnostic layered framework. 3) Evaluate and provide guidelines on scalability, performance, security, and interoperability through evaluation of consensus algorithms, smart contracts, and type of blockchain DLT implementation, etc. for the Energy sector [28].

DLT can be considered as a newer technology which needs additional time to be tested in various implementations and use cases in the future.

IEEE P2418.1: This standard provides a common framework for blockchain usage, implementation, and interaction with the Internet of Things (IoT). The framework addresses items such as security and privacy challenges with regards to Blockchain in IoT. Blockchain permissioned IoT blockchain, and permission-less IoT blockchain will be included in the IEEE P2418.1 common framework [29].

- IEEE P2144.1: A framework of blockchain-based Internet of Things (IoT) data management is defined in this standard. It identifies the common building blocks of the framework that blockchain enabled during IoT data lifecycle including data acquisition, processing, storage, analysing, usage/exchange and obsolescence, and the interactions among these building blocks [9].

- IEEE P2144.2: This standard defines the functional requirements in data compliance, governance and risk management in the operational process for Blockchain-based IoT data management systems [30].

- IEEE P2144.3: This standard defines the assessment framework for data compliance, governance and risk management in Blockchain-based IoT data management, provides performance metrics such as availability, security, privacy, integrity, continuance, scalability, etc [31].

Blockchain technology has ethical dimensions that should always be taken into account. Open information, building consensus, access and inequity, security, and governance each have aspects that influence ethical concerns. Major issues are associated with both individual and organizational privacy. Depending on information provided in the blockchain, specific individuals and personnel may lose their privacy. Worker rights may degrade depending on the level of detail attached to processes and transactions. Wages, identifying information, and their performance may be publicly available; care should be taken in these situations. Most of these are identity privacy issues. Organizational privacy may include information related to organizational intellectual property, performance, and costs without a broader picture. Proprietary information would need to be managed carefully in an environment where transparency of information is a goal. Thus, there will be tensions involved in how much and the type of information to be shared. These are usually associated with transaction privacy issues.

One major sustainability concern with blockchain and most digital technologies is the amount of energy needed to operate them. Although there may be efficiencies and optimization in energy trading and other efficient mechanisms offered by blockchain; a major concern is the amount of energy required to manage the distributed ledger system and proof-of-stake and proof-of-work. Computer technology and software development may be needed to further aid these efficiencies across the transportation supply chain [32].

2.2 Greek demo

2.2.1 SCADA

Regarding the SCADA communication the IEC 60870-5 (discussed in 2.1.1) and IEC 60870-6 (ICCP-TASE.2) are used.

IEC 60870-6 or ICCP or TASE.2 is the most widely adopted communications protocol available to the electric power industry today, with over 200 completed installations in the United States, and in many other countries, at transmission companies, energy companies, and grid operators. A wide range of hardware and software vendors support ICCP, allowing energy companies to implement the protocol inexpensively [33].

ICCP has various challenges that mostly concern security of data. The major threats to control centre data security are bypassing controls, integrity violation, authorization violation, indiscretion by personnel, illegitimate use, and information leakage. Motivations for control centre attacks include disgruntled current or previous employees (who initiate 80 percent of all data security attacks), financial rewards and the ability to demonstrate capability. NERC has identified malicious external hackers, disgruntled employees, unintentional employee errors, and “trusted” external users as the four general threats to the Inter-regional Security Network (ISN) [10].

2.2.2 PMUs

Regarding the PMU units, the IEEE C37.118.1-2011 [11] and IEEE C37.118.2-2011 [34] are used. The first one defines synchrophasor, frequency and rate of change of frequency measurements and the second one defines synchrophasor communication.

The drawbacks and challenges which are mentioned below concern the synchrophasor and not the above standards that also have to be taken into consideration.

One of the major drawbacks of synchrophasors [35] is the lack of transmission protocol, which makes them vulnerable to spoofing attacks. Spoofing is the act of disguising a communication from an unknown source as being from a known trusted source [36]. Spoofing can be used to gain access to a target’s personal information, spread malware through infected links or attachments, bypass network access controls, or redistribute traffic to conduct a denial-of-service attack. This challenge however can be solved by implementing a security layer for the transmission of the data.

The existing architecture is not scalable since it entails an initially high investment. NASPI’s research initiative task force (RITT) emphasizes optimal placement as a significant challenge but also one dependent on the nature of applications the utility intends to use them for.

More recently, managing and analysing large volumes of synchrophasor data has become increasingly challenging. Lack of standardized data management solutions for smart grid has only made this problem more challenging. The ubiquitous presence of these devices has expanded their attack surface, making them vulnerable to different types of attacks.

2.2.3 DMS and EMS

Regarding the DMS and EMS the IEC 61970 and IEC 61968 standards will be used which were mentioned in section 2.1.2.

2.2.4 AMI

Regarding the AMI, the IEC 62055 and IEC 62056 (discussed in section 2.1.4) standards are applied.

IEC 62055 specifies the application layer protocol of the standard transfer specification (STS) used for transferring units of credit and other management information from a point of sale (POS) system to an STS-compliant payment meter in a one-way token carrier system. It is primarily intended for application with electricity payment meters without a tariff employing energy-based tokens, but may also have application with currency-based token systems and for services other than electricity. It is intended for use by manufacturers of payment meters that have to accept tokens that comply with the STS and also

by manufacturers of POS systems that have to produce STS-compliant tokens and is to be read in conjunction with IEC 62055-5x series [37].

2.2.5 DRMS

Regarding the DRMS the OpenADR protocol is applied.

OpenADR is an open, highly secure, and two-way information exchange model and global Smart Grid standard. OpenADR standardizes the message format used for Auto-DR and DER management so that dynamic price and reliability signals can be exchanged in a uniform and interoperable fashion among utilities, ISOs, and energy management and control systems. While previously deployed Auto-DR systems are automated, they are not standardized or interoperable. OpenADR was created to automate and simplify DR and DER for the power industry with dynamic price and reliability signals that allow end users to modify their usage patterns to save money and optimize energy efficiency, while enhancing the effectiveness of power delivery across the Smart Grid [12].

One of the major issues facing the wide deployment of automatic demand response systems is scalability. In general, OpenADR systems are designed to operate in client/server architectures, but, as the number of households increases, scalability becomes a large concern. The Demand Response (DR) nodes share DR signals through the network, and it has been shown that event messages from VENs (known as Virtual End Nodes) generates approximately 100 TByte traffic per day in the case of one million DR clients. This amount of traffic can easily block the network that is connecting the nodes. Also, it has been shown that the large number of individual messages results in increased latency at the DR server (known as Virtual Top Node – VTN) as well. These problems call for innovative deployment architectures to make sure that DR events reach to the subscribed resources in time. For example, cloud-based deployment is suggested to alleviate the scalability problem as resources are abundant in cloud. However, cloud-based deployment carries additional challenges pertained to security and privacy.

Furthermore, the ADR process between the utility and the residential consumer is based on an agreed upon commodity contract where the goal of the automated process is to find an optimum between the time-varying energy price negotiated and the corresponding energy amount provided and consumed. That means that the ADR process, in order to find the optimal solution, has to rely on big data which have to be analysed in real time.

Another challenge that someone might face with the implementation of the OpenADR protocol is the risk of fraudulent approaches. While message exchange in OpenADR is carried by the Transport Layer Security (TLS), where client authentication is required for mutual authentication, there are still issues concerning fraud. One example of attack could be a malicious consumer who wants to cheat the OpenADR protocol in order to gain larger rewards by submitting false bids and not reducing the agreed upon amount of energy. Even worse this consumer could collaborate with an external adversary to inflict devastating damages to the system since the consumer is a legitimate agent in the OpenADR protocol and has access to a set of cryptographic keys required to respond to DR events.

Moreover, an issue that has to be taken into account is the privacy of the consumers' data. The process of invoking demand response entails the generation of significant amount of data which in some cases beyond the scope of Platone can be private. The data may reveal information about consumption behaviour, billing and financial information, consumers' identity, contact information as well as address of the houses. This information if it gets into the wrong hand can be shared with unauthorized parties or even sold for marketing purposes.

Although many automatic demand response programs are accompanied with incentives to encourage consumers to participate, there are still many challenges facing utilities in getting consumers' buy-in. Beside the issues of security and privacy, typical DR actions such as sustained load shedding can directly impact consumers, making some unwilling to participate in DR programs because they care very much about comfort and control. In other words, consumers are not yet into the idea of giving up their appliance operation decision to external entities [38].

2.2.6 Battery and Energy Storage Systems

Battery and energy storage systems are not used by the Greek demo.

2.2.7 Cybersecurity

Regarding Cybersecurity IEC 62351 and ISO 27001 are applied.

- IEC 62351 is a standard developed by WG15 of IEC TC57. This is developed for handling the security of TC 57 series of protocols including IEC 60870-5 series, IEC 60870-6 series, IEC 61850 series, IEC 61970 series & IEC 61968 series. The different security objectives include authentication of data transfer through digital signatures, ensuring only authenticated access, prevention of eavesdropping, prevention of playback and spoofing, and intrusion detection.

  The IEC 62351 standard addresses security concerns in power systems, providing in part authentication, integrity and confidentiality of data. The standard proposes both standardized technologies (e.g., TLS), and proprietary extensions to industrial protocols. The standard contains some inaccuracies (e.g., cipher suite designations), and unconventional choices (e.g., RSA signatures for IEC 61850). It also does not consider newer cryptographic algorithms that could provide the same security guarantees at a lower performance cost (e.g., elliptic curve cryptography).

  Nevertheless, the standard does provide a significant improvement in security in automation systems, providing authenticity, integrity and at times confidentiality of data. However, it is clear that the standard is to some extent constrained by requirements related to backwards compatibility, and hence does not always provide as much security as could be provided if backwards compatibility was sacrificed. Overall, the standard provides a balanced approach that can be implemented with reasonable effort and that provides a reasonable amount of security if implemented comprehensively [39].

- ISO/IEC 27001 is widely known, providing requirements for an information security management system (ISMS), though there are more than a dozen standards in the ISO/IEC 27000 family. Using them enables organizations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties [14].

  ISO/IEC 27001 gives organizations that are looking for securing their business a flexibility to develop their own information security management system (ISMS). This is because the standard does not specify any particular approach or method for developing ISMS. Instead, it defines requirements for ISMS. This gives organizations more freedom to choose their preferred risk management methodology for example. On the other side, this may create burden for some organizations that lack security knowledge and do not have competency for developing their ISMS [40].

2.2.8 Energy Market

Regarding the Energy Market IEC 62325 is applied which was discussed in section 2.1.2.

2.2.9 Blockchain

Regarding the Blockchain Technology IEEE P2418.5, IEEE P2418.1 (both of which were mentioned in 2.1.7) and ISO/TR 23455:2019 could be applied.

ISO/TR 23455:2019 is a document which provides an overview of smart contracts in BC/DLT systems; describing what smart contracts are and how they work. It also discusses methods of interaction between multiple smart contracts. This document focuses on technical aspects of smart contracts. Smart contracts for legally binding use and applications are briefly mentioned in this document [41].

2.3 German demo

2.3.1 SCADA

Regarding the SCADA communication IEC 60870-6 (ICCP – TASE.2) will be applied which was discussed in section 2.2.1.

2.3.2 DMS and EMS

Regarding the DMS and EMS MQTT, REST-API and Modbus TCP (all 3 discussed in section 2.1.3) and Python will be applied.

2.3.3 Battery and Energy storage

Regarding the Battery Storage and Energy Storage Systems OPC-UA, BACnet, IEC 60870-5 (discussed in 2.1.1) could be applied for the communication.

- OPC-UA: The OPC Unified Architecture (UA), released in 2008, is a platform independent service-oriented architecture that integrates all the functionality of the individual OPC Classic specifications into one extensible framework [15].
  A quite common challenge with OPC-UA is the difficulty faced in order to adopt it due to the volume of its manual. Another issue is that OPC-UA is sometimes inflexible especially when dealing with multiple data structures and heterogeneous devices.
- BACnet: BACnet was designed to allow communication of building automation and control systems for applications such as heating, ventilating, and air-conditioning control (HVAC), lighting control, access control, and fire detection systems and their associated equipment. The BACnet protocol provides mechanisms for computerized building automation devices to exchange information, regardless of the particular building service they perform [16].

  BACnet was not designed with security as a primary requirement, as early systems operated in isolated networks without any external connection. With the increasing connection of BAC networks to external facing networks, such as the Internet or enterprise networks for maintenance, the attack surface has increased. Although BACnet added additional features for security services (BACnet security services – BSS) there is still work underway to implement a completely secure layer for this protocol [42].

Apart from the above communication standards, the battery system is designed in compliance with the following standards:

IEC 61439-1: Lays down the general definitions and service conditions, construction requirements, technical characteristics and verification requirements for low-voltage switchgear and control gear assemblies [43].

IEC 61000-6-2:2016-05 for EMC immunity requirements applies to electrical and electronic equipment intended for use in industrial locations, as described below. Immunity requirements in the frequency range 0 Hz to 400 GHz are covered. No tests need to be performed at frequencies where no requirements are specified. This generic EMC immunity standard is applicable if no relevant dedicated product or product-family EMC immunity standard exists [44].

IEC 61000-6-4:2011-09: This part of IEC 61000 for EMC emission requirements applies to electrical and electronic apparatus intended for use in industrial environments. Emission requirements in the frequency range 0 Hz to 400 GHz are covered. No measurement needs to be performed at frequencies where no requirement is specified. This generic EMC emission standard is applicable if no relevant dedicated product or product-family EMC emission standard exists [45].

IEC 61619: Specifies a method for the determination of polychlorinated biphenyl (PCB) concentration in non-halogenated insulating liquids by high-resolution capillary column gas chromatography using an electron capture detector (ECD). Gives total PCB content; especially useful when a detailed analysis of PCB congeners is necessary [46].

UL 1642: These requirements cover primary (non-chargeable) and secondary (rechargeable) lithium batteries for use as power sources in products. These batteries contain metallic lithium, or a lithium

alloy, or a lithium ion, and may consist of a single electrochemical cell or two or more cells connected in series, parallel, or both, that convert chemical energy into electrical energy by an irreversible or reversible chemical reaction.

These specifications cover lithium batteries intended for use in technician-replaceable or user replaceable applications.

It contributes to reduce the risk of fire or explosion when lithium batteries are used in a product. The final acceptability of these batteries is dependent on their use in a complete product that complies with the requirements applicable to such product.

It helps to decrease the risk of injury to persons due to fire or explosion when user-replaceable lithium batteries are removed from a product and discarded.

This standard covers technician-replaceable lithium batteries that contain 5.0 g (0.18 oz.) or less of metallic lithium. A battery containing more than 5.0 g (0.18 oz.) of lithium is judged on the basis of compliance with the requirements in this standard, insofar as they are applicable, and further examination and test to determine whether the battery is acceptable for its intended uses.

It also covers user-replaceable lithium batteries that contain 4.0 g (0.13 oz.) or less of metallic lithium with not more than 1.0 g (0.04 oz.) of metallic lithium in each electrochemical cell. A battery containing more than 4.0 g (0.13 oz.) or a cell containing more than 1.0 g (0.04 oz.) lithium may require further examination and test to determine whether the cells or batteries are acceptable for their intended uses.

However, it does not cover the toxicity risk that may result from the ingestion of a lithium battery or its contents, nor the risk of injury to persons that may occur if a battery is cut open to provide access to the metallic lithium [47].

UN 38.3: Nearly all lithium batteries are required to pass section 38.3 of the UN Manual of Tests and Criteria (UN Transportation Testing). Intertek can test for conformance to the UN Transportation Testing requirements and help manufacturers avoid costly delays in getting their product to market.

It is important to note that lithium batteries have been identified as a Class 9 dangerous good during transport. To be safely transported (by air, sea, rail or roadways), they must meet the provisions laid out in UN 38.3. This standard applies to batteries transported either on their own or installed in a device (UN codes 3090/3091 for lithium, 3480/3481 for lithium-ion. And it applies to all points in the battery's transportation process: from sub-suppliers to end-product manufacturer; manufacturer to distributor; in or out of the product; in the field; during product returns or with non-original packaging.

UN 38.3 has been adopted by regulators and competent authorities around the world, thus making it a requirement for global market access. The protocol includes identifying/classifying lithium batteries; testing/qualification requirements; design guidance/conditions and packaging/shipping obligations [48].

2014/35/EU: The low voltage directive (LVD) (2014/35/EU) ensures that electrical equipment within certain voltage limits provides a high level of protection for European citizens, and benefits fully from the single market. It has been applicable since 20 April 2016 [49].

2014/30/EU: The electromagnetic compatibility (EMC) Directive 2014/30/EU ensures that electrical and electronic equipment does not generate, or is not affected by, electromagnetic disturbance.

The EMC directive limits electromagnetic emissions from equipment in order to ensure that, when used as intended, such equipment does not disturb radio and telecommunication, as well as other equipment. The directive also governs the immunity of such equipment to interference and seeks to ensure that this equipment is not disturbed by radio emissions, when used as intended [50].

2006/66/EU: The EU Battery Directive (2006/66/EC) regulates the manufacturing and disposal of batteries and accumulators in the European Union to protect human health and the environment from hazardous substances such as mercury and cadmium.

Companies are required to comply with the European Union's Battery Directive responsibilities in order to avoid fines and shipping barriers upon import into any of the 27 EU Member States. The EU Battery Directive requires producers to properly label their battery products. They must finance collection and recycling programs, as well as public awareness campaigns for battery waste disposal. In addition, they may not charge a fee for separate collection at the time of disposal [51].

2.3.4 Cybersecurity

Regarding the Cybersecurity the German demo is not planning on actively engaging with the cybersecurity standardization ecosystem.

2.3.5 Energy Market

Regarding the Energy Market the German demo does not consider an energy market context, but instead focuses on energy communities. To the best of our knowledge no energy community standards exist as of 2020.

2.3.6 Blockchain

Regarding the Blockchain technology the IEEE P2418.5, IEEE P2418.1 and ISO/TR 23455:2019 (all mentioned in 2.1.7) will be investigated and applied if possible.

3 Simulations

In this chapter, we perform a detailed simulation of the Greek demo pilot site communication infrastructure to identify possible issues that might hinder the development of the Platone solution. The results of this analysis can also serve as an indication for possible problems or benefits for the two other demos.

3.1 Theoretical background

3.1.1 Objective

The objective of this section is to present and analyse the underlying technology stack of the studied solution, i.e., data transfer from Electricity Smart Meters to remote server through a 4G-LTE network. 4G-LTE networks are based purely on packet switched network, which is mainly designed for high-speed data transfer across the network. Significant benefits of the technology are: improved data rate at cell edge, compatibility with other earlier releases, improved spectral efficiency, reduced transmission latency and reasonable power consumption for the end users compared to older wireless communication technologies (3G-UMTS).

3.1.2 Infrastructure Technology stack

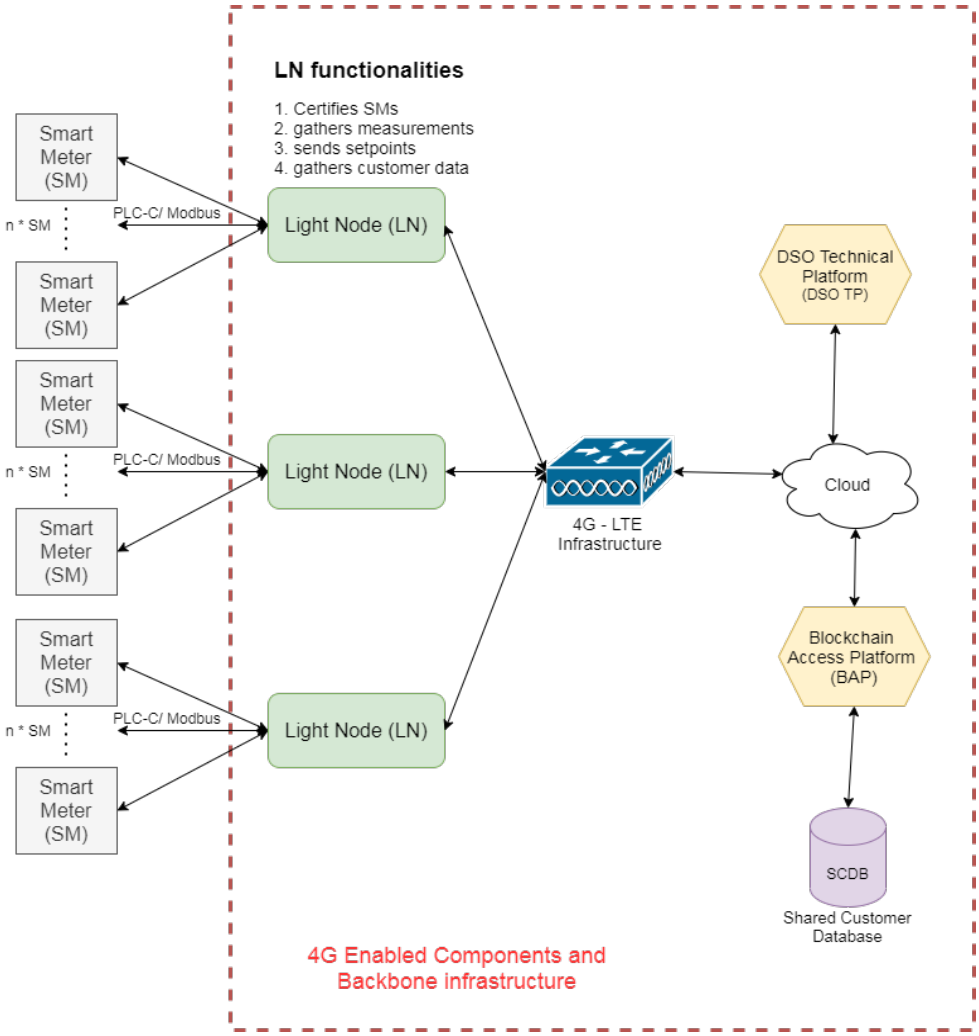

Figure 1 Use Case Technology Stack

The use case considers a multilayer representation of the Energy System, in which individual components communicate based on various network and application layer protocols. For this case

study, the focus lies on the network layer and specifically on the side of 4G-LTE enabled devices as well as the backbone of the network and the remote server where the main customers' database is located.

Figure 1 illustrates the abstract use case technology stack. The smart meters (SMs) installed in end users' properties collect energy related data. Each SM sends the data to the closest Light Node (LN) through a Modbus or PLC-C channel. Each light node collects data from its associated smart meters, certifies and transfers them to the Shard Customer Database through the Blockchain Access Platform (BAP). Moreover, the light nodes are capable of receiving set points from the DSO Technical Platform (DSOTP). The communication between LNs and the BAP, as well as between the LNs and the DSO TP are carried out on top of a 4G – LTE network.

For this case study, only components inside the red dashed line of Figure 1 are considered, i.e., smart meters are omitted.

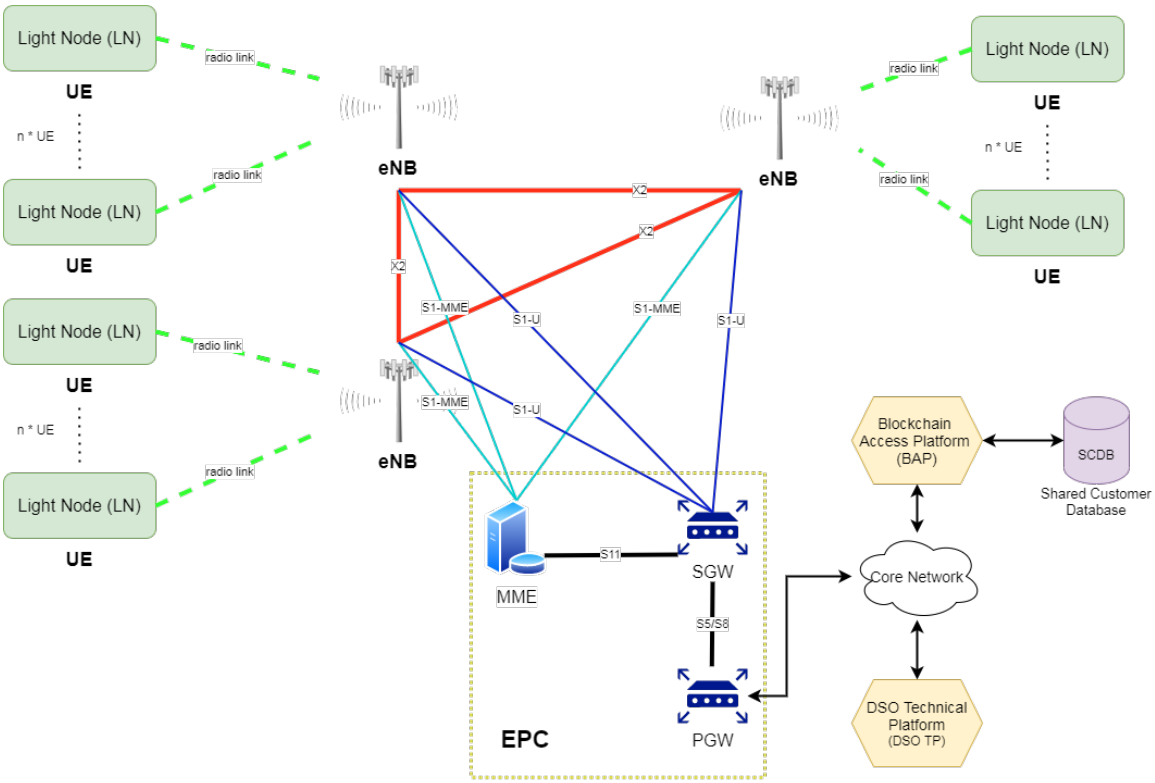

Figure 2 Case Study Infrastructure

A detailed view of the infrastructure shown in Figure 1 showing also 4G related components is provided in Figure 2. Light Nodes are essentially the User Equipment (UEs) of the LTE network. The E-UTRAN Node B (eNBs), the Mobility Management Entity (MME), the Serving Gateway (SGW) and the Packet Data Network Gateway (PGW) are all assets of the 4G – LTE core infrastructure.

3.1.3 LTE design criteria

Long Term Evolution (LTE) is a 3GPP standard [52] frozen in December 2008. Among the core objectives of the standard are:

- The continuity of competitiveness of 3G systems for the future.
- The minimization of design complexity.
- The cost reduction (both capital and operational).
- The optimization of a fully packet switched system.

- The requirement to continuously meet higher end user demand for increasing data rates and low latency.

In order to meet those objectives LTE/U-TRAN utilizes and fully Packet Switched Architecture. The peak data rate is expected to increase, in comparison to prior HSPA and UMTS technologies, as a direct cause of several technical changes.

On the physical layer, OFDMA with Cyclic Prefix is utilized to enable peak data rates of 100Mbps within a 20MHz downlink spectrum allocation. Whereas, SC-OFDMA CP is utilized for the uplink providing peak data rates of up to 50Mbps, considering a 20MHz uplink spectrum allocation.

E-UTRAN, i.e. Evolved Universal Terrestrial Ration Access Network, manages to simplify the system architecture, when compared to prior 3G technologies, by utilizing a flat design. eNBs operate both as base stations and Radio Network Controllers. This combination lowers the latency between UE—RNC communication to the minimum, while also removing RNC nodes, simplifies the network and lowers the overall cost. Moreover, the lack of RNCs and the ability of each eNBs to manage resources on their cell increases the overall performance and lowers the probability of failure since there control is distributed rather in a several RNCs [53].

Apart from OFDMA and Packet Switching, E-UTRAN utilizes MIMO schemas to lower the latency and increase throughput between eNBs and UEs.

3.1.4 LTE building blocks

LTE is a continuously evolving technology, which is enhanced in every new 3GPP release. A comprehensive overview of 3GPP releases related to the LTE, is provided by ETSI, the European Telecommunications Standards Institute [54].

Aside from algorithmic and design enhancements the main building components of LTE are the same since 3GPP release 8. Those components are:

1. User Equipment (*UE*)
2. evolved NodeB (*eNB*)
3. Mobility Management Entity (*MME*)
4. Serving Gateway (*SGW*)
5. Packet Data Network Gateway (*PGW*)

3.1.4.1 User Equipment (UE)

Any end user device capable of connecting to the LTE network for data exchange. The UE communicates directly with eNBs through a radio interface. The device is responsible of notifying for any geographical positioning changes, i.e. mobility information.

UEs are categorized in a number of downlink and uplink performance categories as specified by 3GPP [55].

3.1.4.2 Evolved NodeB (eNB)

eNBs are components installed on the edge of LTE infrastructure, providing access to the UEs of their associated cell. eNBs are the evolution of NodeBs of 3G UMTS, rather with increased responsibilities. In LTE, there are no RNC nodes to control the end user devices. This is among the duties of eNBs. This approach simplifies the overall architecture and minimizes the UE application latency.

eNBs are interconnected in most cases using the X2 interface, creating a mesh network, which provides more communication routes and thus improving the reliability of the network. eNBs are also connected to the Evolved Packet Core (EPC), which is the LTE core, through S1 interfaces [53].

3.1.4.3 Mobility Management Entity (MME)

The MME, part of the EPC, is the core control component of UEs. This node participates in the:

- activation and deactivation of the bearer – tunnel between UE and the Packet Data Network through a PGW.

- association of UEs to SGWs initially and during handovers.
- authentication of UE through Home Subscriber Server (HSS) and the allocation of temporal ids
- authorization of UE and enforcement of roaming restrictions [56], [57].

3.1.4.4 Serving Gateway (SGW)

The Serving Gateway is essentially an enhanced router device. It routes packets from UE to PDN and vice versa. During the process it keeps track of various IP related information for each UE. It supports the actual tunnelling implementation (bearer). An important feature of SGWs is the control of traffic forwarded from other mobile technologies (2G/3G) [56], [58].

3.1.4.5 Packet Data Network Gateway (PGW)

The Packet Data Network Gateway is the gateway of the LTE network. It provides UEs connectivity to outer networks, the internet. The node has packet screening, filtering and policy enforcement features along with charging and logging features. According to 3GPP releases on LTE, the technology shall support connectivity with other mobile-centric technologies such as WiMAX [59] and Wi-Fi [60]. PGW nodes are those in duty to integrate and route packets arriving from another mobile enabled network to the PDN [56], [61].

3.2 Simulation

3.2.1 Introduction and scope

Progress in technology is making possible the replacement of mechanical meters for electricity with digital smart meters showing advanced functionalities including the service use data, as well as information to and from other smart meters within the network. In the last few years, telecommunication industries development has focused on an intensive use of broadband systems and new wireless technologies for transmission energy data. To achieve the best trade-off between power consumption and communication range, meter designers in Europe are choosing bands in MHz like 1860 MHz, 868 MHz and 433 MHz.

This report documents the Greek demo pilot site implementation requirements from an application-level perspective. Upon definition of the requirements a telecommunication simulation is designed and implemented. The results of the simulation indicate whether LTE-4G can support the desired data electricity exchange schema.

3.2.2 Pilot Requirements

For the needs of the Hellenic Pilot site, a case consisting of 30 endpoints (UEs / LNs) and one remote host (RHost) is considered. The installed UEs gather energy related data using a sampling period of 15 minutes. The collected data are transmitted to the closest 4G-LTE enabled base station (eNB), which in turn sends the data through the Evolved Packet Core (EPC) backhaul to the remote host located 10 kilometres away from the studied site.

Taking into consideration the cell size, in which the UEs are to be installed (approximately 10km^2) and the minimization of the deployment cost, a single eNB is installed in the centre of the pilot site. The eNB is responsible of receiving and propagating packets from all the installed UEs.

A number of important system parameters are provided in Table 1.

Table 1 System Parameters

Positional Parameters	
Place of installation	Large City
Environment	Urban
Total Area	~10 square kilometres
Number of UE (LN) Devices	30
Site Distance to Remote Server	10 kilometres
ENB Installation Height	30m [62] [63]
Ues (LN) Installation Height	1.5m [63]
Application Parameters	
Sampling Rate	15min (96 packets per day per device) (*1)
UDP Packet Size	8kB
Network Level Parameters	
Cell Size	Pico-Micro Cell
Propagation Loss Model	Okumura Hata Propagation Loss Model [64] [65]
Frequency	1760MHz (uplink) [66]
Ul-Dl Bandwidth	5MHz (25 Resource Blocks)
Frequency Reuse Algorithm	No Frequency Reuse
Scheduler	Channel and QoS Aware Scheduler [67]

eNB transmission Mode	SISO
Carrier Aggregation	Not Utilized
eNB Antenna Type	Omnidirectional Antenna
eNB Antenna Gain	0dBi
eNB Transmission Power	24-37dBm => ~0.25-5W [62] [63]
eNB Noise Level	10dB
UE Antenna Type	Omnidirectional Antenna [63]
UE Antenna Gain	0dBi
UE Transmission Power	10dBm => 0.01W [62]
UE Noise Level	12dB
UE to eNB SrS Periodicity	80msec
EPC BackHaul to Remote Host data rate	10Gbps
EPC BackHaul to Remote Host Delay	2msec (0.2msec per Km)
EPC BackHaul to Remote Host MTU	1500 Bytes

(*1): NS3 is an event-based simulator, meaning there is no sense of real time beyond the simulated which is based on simulation events and delays.

Considering that, it is possible to abstract the idea of time and in contrast simulate the events which were to take place during the time.

Given a sampling rate of 15 min. and considering the total desired simulation time is 1 day, there are 96 consecutive slots of 15 minutes, i.e., 96 packets sent from each LN to the Remote Host each day or 32 packets per 8 hours.

3.2.3 Simulation Setup

The simulation is implemented utilizing NS3 event-based simulator [68]. For the needs of the simulation, specifically the congestion analysis part, the number of endpoints (UEs) increases among simulation sets, ranging from 5 to 40 nodes. To achieve this functionality a Random Disc Positioning System is utilized, where each UE is allocated to a randomly selected position as can be observed in Code Block 1.

```
ObjectFactory pos;
pos.SetTypeId("ns3::RandomDiscPositionAllocator");
pos.Set("Rho", StringValue("ns3::UniformRandomVariable[Min=25.0|Max=60.0]"));
pos.Set("Theta",
    StringValue("ns3::UniformRandomVariable[Min=0.0|Max=6.2830]"));  // [0,2π]
pos.Set ("X", DoubleValue(56.0));
pos.Set ("Y", DoubleValue(56.0));
pos.Set ("Z", DoubleValue(uesHeight));
Ptr<PositionAllocator> uesPositionAlloc =
    pos.Create()->GetObject<PositionAllocator>();
```

Code Block 1: UE Random Allocation

Figure 3 illustrates a topology with 20 UEs, as it is defined in NS3. All UE nodes are placed randomly inside a Disc (as expected based on definition of Code Block 1), while their mobility is set to constant, i.e. stationary.

Apart from the UEs, a single eNB is installed in the centre of the topological area to serve all the end devices. The Backhaul network is consisted of EPC nodes and the Remote Host. Specifically, for the EPC, PGW, SGW and MME nodes are installed and represented. All the required X2, S1, S5, S11 links are automatically set up by the NS3 “PointToPointEpcHelper”. The only connection requiring manual configuration is between PGW and Remote Host, which is defined using a data rate of 10Gbps, MTU of

2kB and Delay of 2msec (there is no notion of distance in wired NS3 communications and thus the delay is defined beforehand).

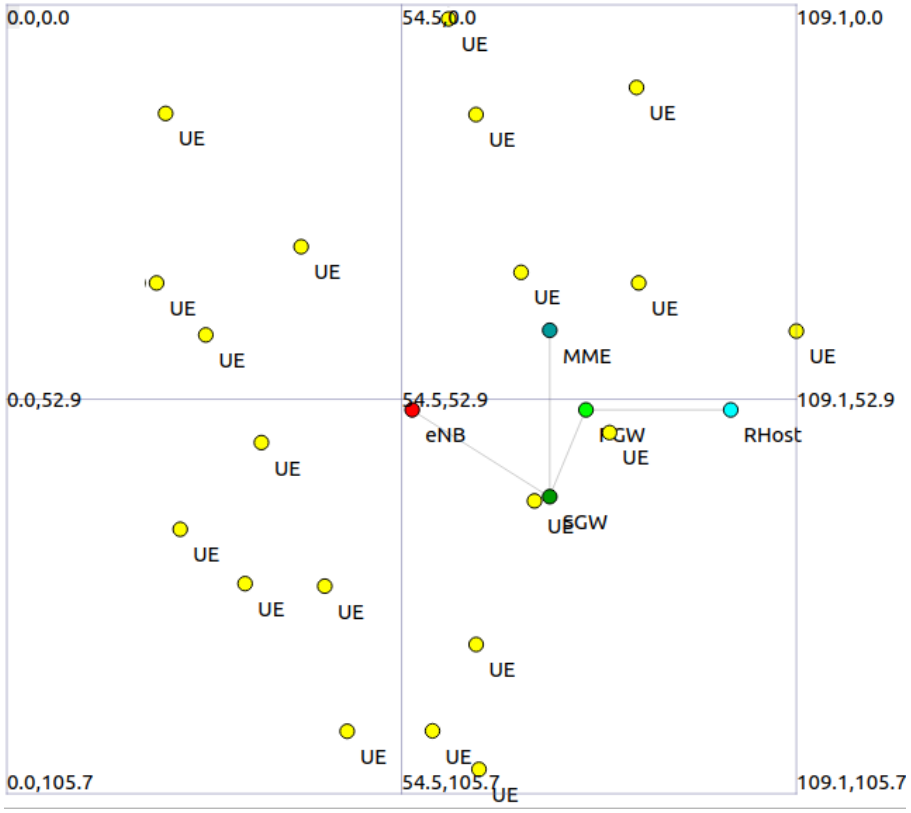

Figure 3 Topology consisting 20UEs and 1 ENB

According to a document [66] mentioning spectrum allocation from the Hellenic Telecommunications and Post Commission (EETT), 1710-1785MHz are the allocated uplink bands, while 1805-1880MHz are the allocated downlink and, for spectrum utilization by authorized companies. Based on this document and the fact that data are sent in the uplink direction, a frequency of 1760MHz is selected for the uplink and the wireless propagation loss model definition.

The cell size, approximately 10.000 square meters, which is eventually equivalent to a circle of radius 56 meters, can be considered both a pico cell or a micro cell. Thus, both the eNB and the UEs are expected to have transmission power below 5W and 0.01W respectively.

3.2.4 Simulation Results

The evaluation of the defined network is implemented in 8 consecutive simulation steps. Among simulation steps the number of UE nodes gradually increases from 5 to 40 nodes with a step of 5 nodes.

During each step a number of important network and physical layer metrics are monitored. The most important of these metrics, being mean end to end application level throughput, delay, jitter, lost packets and total transferred bytes across all UE nodes and the remote host (server), are extracted by utilizing NS3 Flow Monitor module [69].

NS3 provides also the means to extract all the monitored data in pcap file format for each IP enabled node in the simulation, as well as LTE radio specific metric in a text file format.

In order to automate the simulation, process a Perl [70] script is utilized, part of which is shown in Code Block 2. A short description of the script. Initially the required modules are defined.

Following the definition, a command is passed to waf [71] to build all required C++ sources as well as the required modules with the optimized flag to reduce the required runtime during each simulation.

Next, system outputs are defined and a for loop is utilized to run each individual simulation step. The results of each simulation are save under “scratch_results/$ue” created folder, where $ue is the number of UEs simulated in each step.

```
#!/usr/bin/perl
use strict;
use IO::CaptureOutput qw(capture qxx qxy);
use Statistics::Descriptive;

my $launch = "CXXFLAGS=\"-O3 -w\" ./waf -d optimized configure --enable-
static --enable-examples --enable-modules=lte --enable-modules=flow-monitor
my $out;
my $err;
capture { system($launch ) } \$out, \$err;

my @nUe = (5, 10, 15, 20, 25, 30, 35, 40);
foreach my $ue (@nUe)
{
   $launch = "./waf --command-template=\"%s
             --ns3::ConfigStore::Filename=scratch/custom-defaults.txt
             --ns3::ConfigStore::Mode=Load
             --ns3::ConfigStore::FileFormat=RawText --generateREM=false
             --animateNodes=false --packetInterarrivalTime=200
             --simTime=30 --numUENodes=$ue\"
             --run lte_hellenic_pilot --cwd scratch_results/$ue";
   print "$ue\n";
   capture { system($launch ) } \$out, \$err;
   $err =~ /real(.+):(.+)/;
}
```

Code Block 2: Simulation Steps Automation

Figure 4 and Figure 5 provide a graphical representation of the IPv4 addressing configuration per node interface and the packet exchange between each UE and the eNB respectively. The graphical representation provides a deeper intuition of the studied network and its corresponding topology.

Upon completion of all simulation steps, data are collected under the defined folder. The Flow Monitor module gathers data per end to end connection and thus an extra data processing step needs to take place in order to take the aggregated metrics. Simulation Results are collected, processed and visualized with Python3 [72], Pandas [73] and MatplotLib [74] modules. Code Block 3 shows the logic followed to calculate the desired performance metrics for each simulation step. Each results file is loaded as pandas dataframe, sanitized and the KPI metrics are calculated.

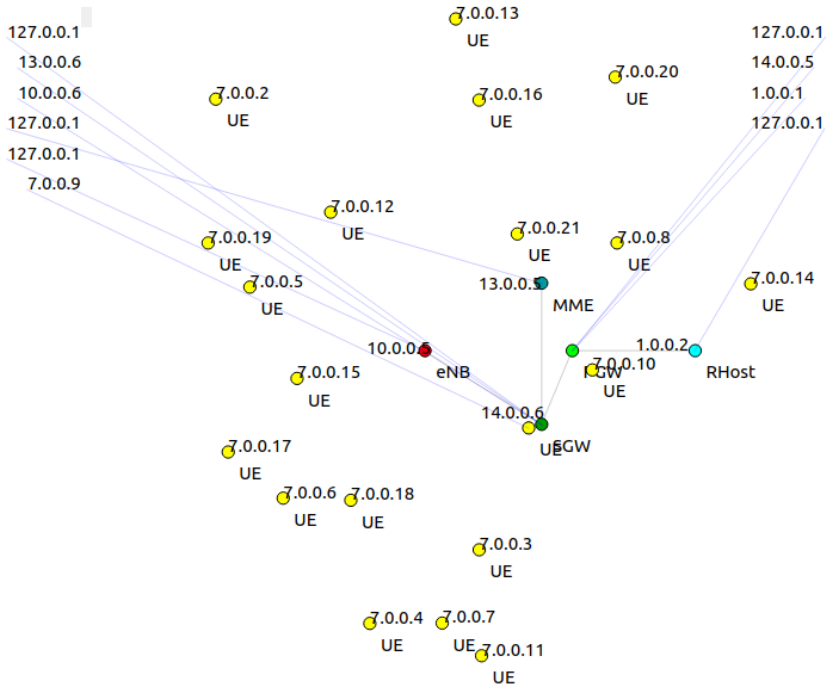

Figure 4 IPv4 Addresses per node and interface

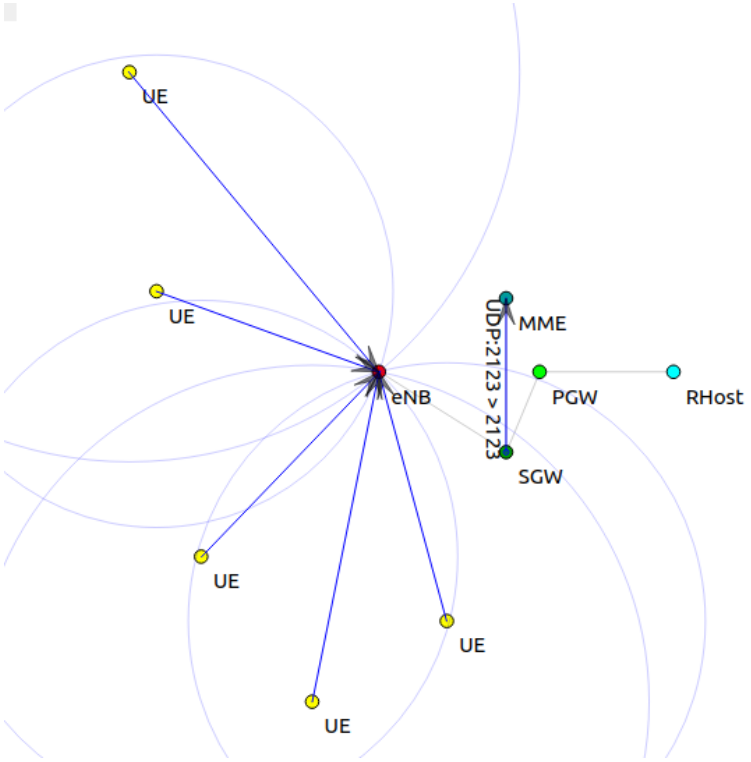

Figure 5 UEs to eNB Packets Exchange

```
import pandas as pd
import matplotlib.pyplot as plt
import json

Results = list()
for num_of_ues in [5,10,15,20,25,30,35,40]:
    data = pd.read_csv(f"{num_of_ues}/lte_results/flowMonitorKPIs.txt")
    #%% Clean the DataSet
    # First keep only data from UE devices (Subnet = 7.0.0.0)
    data.drop(data[list(map(lambda val: '7.0.' not in val,
      data.Source.values))].index, axis=0, inplace=True)
    # Ensure that destination IP is always the Remote Host IP
    data.drop(data[data['Destination'] != "1.0.0.2"].index,
      axis=0, inplace=True)
    # drop unnecessary columns
    data.drop(columns=['Flow', 'Source', 'Destination',
      'Tx Packets', 'Rx Packets'], inplace=True)
    # ------------------------------------------------------ #
    #%% Calculate KPIs
    Total_GBytes_Sent = data['Tx Bytes'].sum()/1e6  # GBytes
    Total_GBytes_Received = data['Rx Bytes'].sum()/1e6  # GBytes
    Lost_Bytes_percentage =
        100*(Total_GBytes_Sent-Total_GBytes_Received)/Total_GBytes_Sent
    Total_Lost_Packets = data['Lost Packets'].sum()
    Mean_Throughput_kbps = data['Throughput(bps)'].mean()/1e3  # kbps
    Std_Throughput_kbps = data['Throughput(bps)'].std()/1e3  # kbps
    Mean_Packet_delay_msec = data['Mean Packet delay(msec)'].mean()  # msec
    Std_Packet_delay_msec = data['Mean Packet delay(msec)'].std()  # msec
    Mean_Jitter_msec = data['Mean jitter(msec)'].mean()  # msec
    Std_Jitter_msec = data['Mean jitter(msec)'].std()  # msec
```

Code Block 3: Automated KPIs Calculation

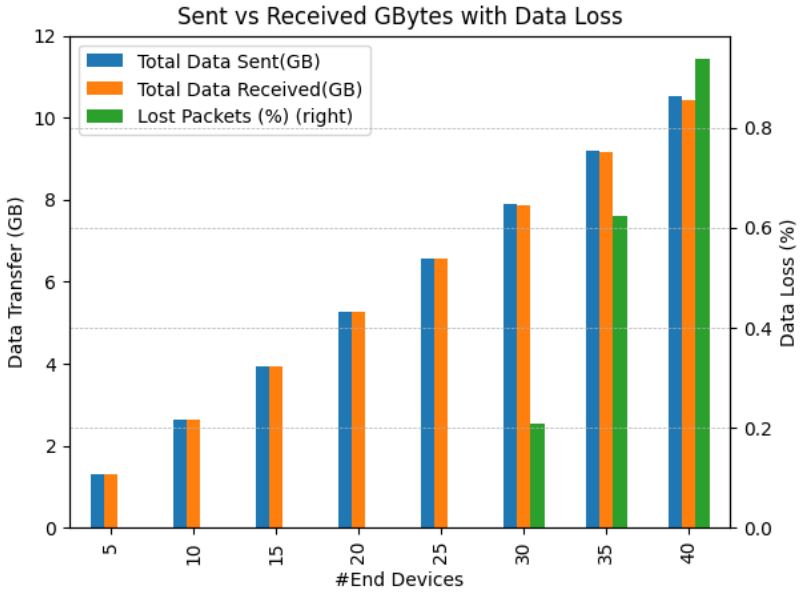

Figure 6 Application level Transferred GBytes

Figure 6 provides a bar plot consisting of 3 individual metrics, total transmitted data in GBytes, total received data in GBytes following the left-hand y-axis and data loss percentage following the right-hand y-axis. As shown, the total received data follows closely the associated transmitted data metric and as expected the volume of data increases with the number of simulated UE nodes. A peak packet loss ratio of 0.9% is observed for the case of 40 simulated nodes. As the number of UEs gradually increases in a Pico cell (small) area the interference between end devices increases too. This interference along with the fact that transmission power has to be below a threshold, leads to the observed packet loss.

Following in Figure 7, the reader may observe the mean end to end Throughput of the application layer along with the standard deviation in kbps. As the number of nodes increases, throughput slightly decreases. With more than 15 nodes, throughput drops to almost half its value and stabilizes thereafter. This behaviour can partially be addressed by adding more eNBs to the network, install eNB antennas higher or use directional antennas. Standard deviation among nodes of the same simulation step is low, a metric revealing that all UE nodes are equally served by the node station.

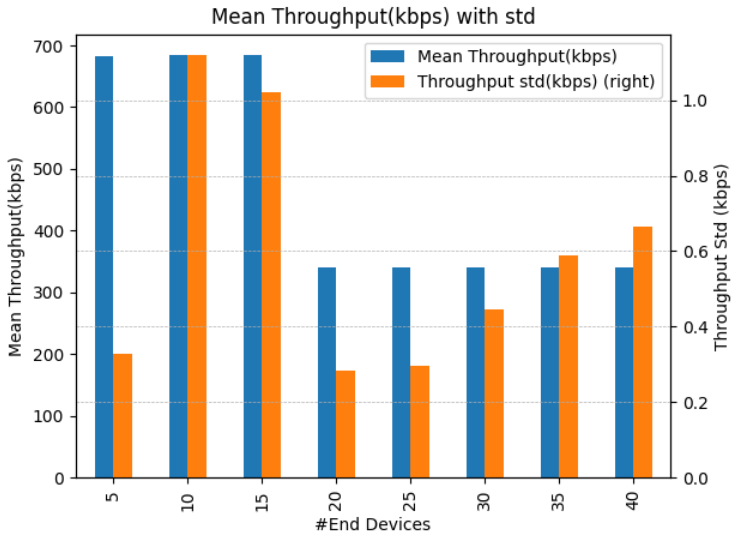

Figure 7 Application Level Mean Throughput and standard deviation

A visual comparison of mean packet delay and the equivalent jitter value is provided in Figure 8. While delay increases almost linearly with the number of end nodes, jitter drops back to lower levels after a 30% increase.

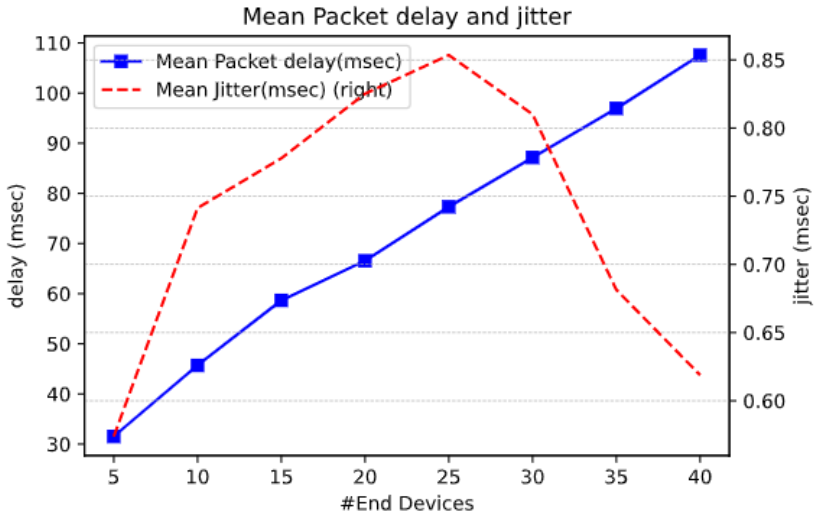

Figure 8 Packet Delay vs Jitter in milliseconds

Figure 9 and Figure 10 illustrate the mean packet delay and jitter with their standard deviation among simulated nodes respectively. In both figures, standard deviation increases making the nodes expected behaviour less predictable.

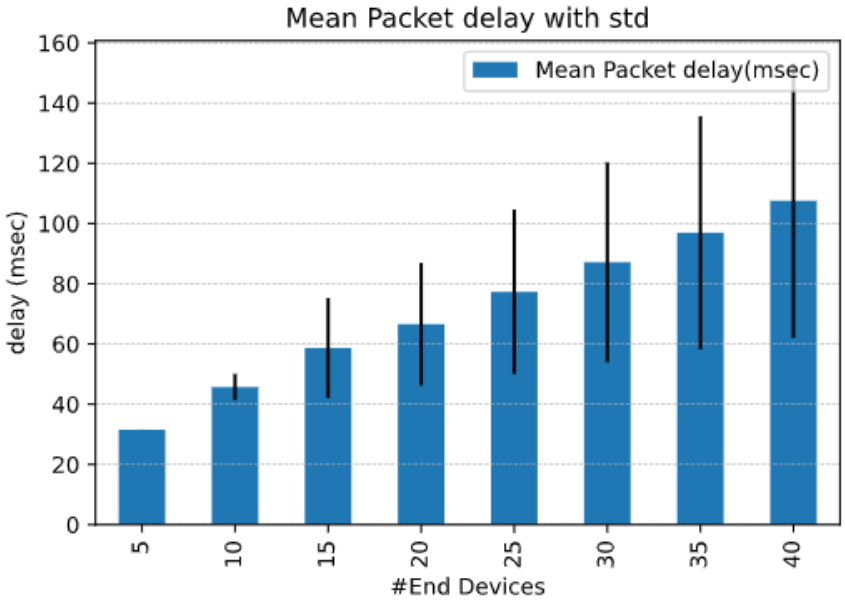

Figure 9 Mean Packet Delay and Standard Deviation in msec

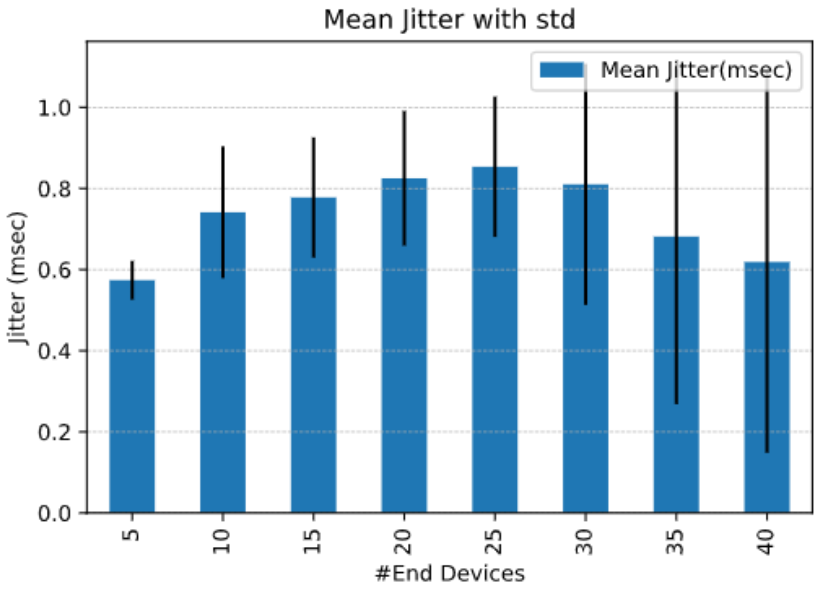

Figure 10 Mean Jitter with Standard Deviation in msec

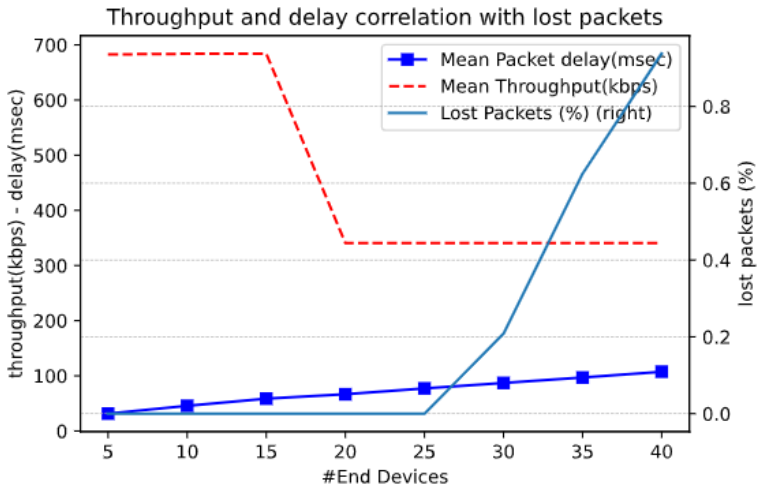

Figure 11 Throughput and delay correlation with lost packet percentage

Finally, Figure 11 shows the correlation between throughput, delay and the percentage of lost packets. As can be observed, delay increases steadily throughout simulation steps. Packet loss percentage on the other hand increases instantly after the threshold of 25 nodes, causing throughput to drop in order to prevent network instability. This behaviour provides reliability to the serving network.

4 Conclusion

This deliverable provided an ex- ante evaluation of the standards and the protocols which are applied or are of interest for the needs of the Platone project. In the theoretical part, standards and protocols for each field trial (i.e., the Italian demo, the Greek demo and the German demo) for every aspect of the grid, were discussed in terms of challenges and benefits they are associated with. In the simulations part, this ex-ante evaluation expanded to simulating the telecommunication infrastructure of the demos to identify possible issues with the deployment.

In Chapter 2, the theoretical analysis was performed. The potential challenges that were mentioned vary according to the standards and the needs they are designed to cover. It was pointed out that in most protocols, where information has to be transferred from one party to another, the major concerns are security and the complexity of the data structure. Security has gained ground in recent years and has become a cornerstone in every data exchange. Security vulnerabilities may cause serious impacts in many aspects of an organization and affect it as a whole (such as financial impact). Such an organization is responsible to ensure the security of the data from the beginning by investing in security protocols and by identifying the possible causes for potential security breaches.

The data structure and their subsequent possible complexity is another fact that has to be taken into consideration when interested parties have to decide the way in which information are going to be exchanged. Large complexity increases the amount of time needed to develop a model correctly (such as in the case of the CIM model). Overall, some issues may be difficult to overcome, especially at the beginning of the adoption and implementation of a standard. However, the benefits of implementing one outweighs the challenges as a significant amount of time is saved in the long term. A standard can be reused for the purposes of another project where the organizations involved will not have to search a new way to exchange data from the scratch.

In Chapter 3 of this report, the authors conducted research on a combined wireless – 4G LTE – and a wired – EPC and P2P – solution towards transferring energy application related data to a remotely placed host machine (server). The LTE architecture is designed to support high data traffic and a guaranteed Quality of Service for real time applications. Therefore, the communication infrastructure requires end-to-end reliable two-way communications, and interoperability between applications with sufficient bandwidth and low-latencies.

Design and implementation were both conducted in a simulation environment based on NS3 network simulator, with main objectives the cost minimization while preserving reliability, security and availability of the transferred data. In order to meet such targets, it is important to understand the impact of each LTE component on the throughput, delay and jitter which are considered as the most restrictive indicators for real time applications. These indicators depend heavily on the network configuration, geographical size and how much delay is consumed by the network components for different end devices. Simulation results indicate the suitability of the studied system topology for the specific case of electricity data exchange between LNs and a remote host. While delay increases almost linearly with the number of end nodes, jitter drops back to lower levels after a 30% increase in nodes. The pilot deployment is expected to range from 20 up to 30 end nodes (UEs).

Based on the study, the throughput, end to end delay and network availability in terms of lost packet metrics point towards the direction of supporting the proposed solution for energy metering data transfer.

5 List of Tables

6 List of Figures

7 List of References

[1] G. Clarke and D. Reynders, Practical Modern SCADA Protocols, Elsevier, 2004.

[2] “IEC 61970-1:2005: Energy management system application program interface (EMS-API) - Part 1: Guidelines and general requirements,” [Online]. Available: https://webstore.iec.ch/publication/6208.

[3] “IEC 61968-1:2020: Application integration at electric utilities - System interfaces for distribution management - Part 1: Interface architecture and general recommendations,” [Online]. Available: https://webstore.iec.ch/publication/32542.

[4] “Apache Kafka,” [Online]. Available: https://kafka.apache.org/.

[5] “REST-API,” [Online]. Available: https://restfulapi.net/.

[6] “MQTT: The Standard for IoT Messaging,” [Online]. Available: https://mqtt.org/.

[7] “Open Charge Point Protocol (OCPP),” [Online]. Available: https://www.openchargealliance.org/.

[8] “Open Building Information Xchange (oBIX),” [Online]. Available: http://www.obix.org/.

[9] “IEEE 2144.1-2020 - IEEE Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management,” [Online]. Available: https://standards.ieee.org/standard/2144_1-2020.html.

[10] “Inter-Control Center Communications Protocol (ICCP, TASE.2): Threats to Data Security and Potential Solutions,” [Online]. Available: https://www.epri.com/research/products/1001977.

[11] “IEEE C37.118.1-2011 - IEEE Standard for Synchrophasor Measurements for Power Systems,” [Online]. Available: https://standards.ieee.org/standard/C37_118_1-2011.html.

[12] “openADR Alliance,” [Online]. Available: https://www.openadr.org/.

[13] “IEC 62325-301:2018: Framework for energy market communications - Part 301: Common information model (CIM) extensions for markets,” [Online]. Available: https://webstore.iec.ch/publication/31487.

[14] “ISO/IEC 27001: Information Security Management,” [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html.

[15] “OPC Unified Architecture (UA),” [Online]. Available: https://opcfoundation.org/about/opc-technologies/opc-ua/.

[16] “BACnet,” [Online]. Available: http://www.bacnet.org/.

[17] European Commission, “2050 long-term strategy,” 2018. [Online]. Available: https://ec.europa.eu/clima/policies/strategies/2050_en.

[18] Platone, “D6.2 Report on standard guidelines for each demonstration,” EU comission, 2020.

[19] D. S. Pidikiti, R. Kalluri, R. K. S. Kumar and B. S. Bindhumadhava, “SCADA communication protocols: vulnerabilities, attacks and possible mitigations,” 2013.

[20] M. Uslar, M. Specht, S. Rohjans, J. Trefke and J. M. González, The Common Information Model CIM: IEC 61968/61970 and 62325 - A practical introduction to the CIM (Power Systems), Springer, 2012.

[21] “ENTSO-E,” [Online]. Available: https://www.entsoe.eu/digital/cim/cim-for-grid-models-exchange/.

[22] “Unified Modeling language (UML),” [Online]. Available: https://www.uml.org/.

[23] “Resource Description Framework (RDF),” [Online]. Available: https://www.w3.org/RDF/.

[24] “Extensible Markup Language (XML),” [Online]. Available: https://www.w3.org/XML/.

[25] B. Marcin, “Building Advanced Metering Infrastructure using Elasticsearch Database and IEC 62056-21 Protocol,” 2019.

[26] C. Alcaraz, J. Lopez and S. Wolthusen, “OCPP Protocol: Security Threats and Challenges,” 2017.

[27] “ISO 17800:2017: Facility smart grid information model,” [Online]. Available: https://www.iso.org/standard/71547.html.

[28] “P2418.5 - Standard for Blockchain in Energy,” [Online]. Available: https://standards.ieee.org/project/2418_5.html.

[29] “P2418.1 - Standard for the Framework of Blockchain Use in Internet of Things (IoT),” [Online]. Available: https://standards.ieee.org/project/2418_1.html.

[30] “P2144.2 - Standard for Functional Requirements in Blockchain-based Internet of Things (IoT) Data Management,” [Online]. Available: https://standards.ieee.org/project/2144_2.html.

[31] “P2144.3 - Standard for Assessment of Blockchain-based Internet of Things (IoT) Data Management,” [Online]. Available: https://standards.ieee.org/project/2144_3.html.

[32] L. Koh, A. Dolgui and J. Sarkis, “Blockchain in transport and logistics – paradigms and transitions,” 2020.

[33] “IEC 60870-6-503:2014: Telecontrol equipment and systems - Part 6-503: Telecontrol protocols compatible with ISO standards and ITU-T recommendations - TASE.2 Services and protocol,” [Online]. Available: https://webstore.iec.ch/publication/3760.

[34] “IEEE C37.118.2-2011 - IEEE Standard for Synchrophasor Data Transfer for Power Systems,” [Online]. Available: https://standards.ieee.org/standard/C37_118_2-2011.html.

[35] A. Sundararajan, T. Khan, A. Moghadasi and A. I. Sarwat, “Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies,” 2019.

[36] “Spoofing defined, explained, and explored,” [Online]. Available: https://www.forcepoint.com/cyber-edu/spoofing.

[37] “IEC 62055-41:2018: Electricity metering - Payment systems - Part 41: Standard transfer specification (STS) - Application layer protocol for one-way token carrier systems,” [Online]. Available: https://webstore.iec.ch/publication/28425.

[38] A. Yassine, “Implementation challenges of automatic demand response for households in smart grids,” 2016.

[39] R. Schlegel, S. Obermeier and J. Schneider, “A security evaluation of IEC 62351,” 2016.

[40] J. Alqatawna, “The Challenge of Implementing Information Security Standards in Small and Medium e-Business Enterprises,” 2014.

[41] “ISO/TR 23455:2019: Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems,” [Online]. Available: https://www.iso.org/standard/75624.html.

[42] M. Peacock, M. Johnstone and C. Valli, “An Exploration of Some Security Issues Within the BACnet Protocol,” 2018.

[43] “IEC 61439-1:2020: Low-voltage switchgear and controlgear assemblies - Part 1: General rules,” [Online]. Available: https://webstore.iec.ch/publication/32338.

[44] “IEC 61000-6-2:2016: Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity standard for industrial environments,” [Online]. Available: https://webstore.iec.ch/publication/25630.

[45] “Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments,” [Online]. Available: https://www.beuth.de/en/standard/din-en-61000-6-4/143517660.

[46] “IEC 61619:1997: Insulating liquids - Contamination by polychlorinated biphenyls (PCBs) - Method of determination by capillary column gas chromatography,” [Online]. Available: https://webstore.iec.ch/publication/5670.

[47] “UL Standard 1642,” [Online]. Available: https://standardscatalog.ul.com/ProductDetail.aspx?productId=UL1642.

[48] “UN 38.3,” [Online]. Available: https://www.intertek.com/energy-storage/un-transportation-testing/.

[49] “2014/35/EU (the low voltage directive-LVD),” [Online]. Available: https://ec.europa.eu/growth/sectors/electrical-engineering/lvd-directive_en.

[50] “2014/30/EU (the electromagnetic compatibility - EMC directive),” [Online]. Available: https://ec.europa.eu/growth/sectors/electrical-engineering/emc-directive_en.

[51] “2006/66/EU,” [Online]. Available: https://www.intertek.com/energy-storage/eu-battery-directive-services/.

[52] “LTE - 3GPP Release 8,” [Online]. Available: https://www.3gpp.org/specifications/releases/72-release-8.

[53] “LTE Overview,” [Online]. Available: https://www.3gpp.org/technologies/keywords-acronyms/98-lte.

[54] “Long Term Evolution (LTE),” [Online]. Available: https://www.etsi.org/technologies/mobile/4g.

[55] “LTE ue-Category,” [Online]. Available: https://www.3gpp.org/keywords-acronyms/1612-ue-cat.

[56] “The Evolved Packet Core,” [Online]. Available: https://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core.

[57] “Wireless and mobile technologies and protocols and their performance evaluation,” [Online]. Available: https://www.sciencedirect.com/topics/computer-science/management-entity.

[58] “Cisco SGW Serving Gateway,” [Online]. Available: https://www.cisco.com/c/en/us/products/wireless/sgw-serving-gateway/index.html.

[59] “WiMAX Forum,” [Online]. Available: https://wimaxforum.org/.

[60] “Wi-Fi Alliance,” [Online]. Available: https://www.wi-fi.org/.

[61] “Overview of Packet Data Network Gateway Functions,” [Online]. Available: https://www.juniper.net/documentation/en_US/junos-mobility11.2/topics/concept/gateways-mobility-pgw-function-overview.html.

[62] EETT, “EETT Base station data,” [Online]. Available: https://www.eett.gr/opencms/export/sites/default/admin/downloads/Informative_Documentation/hlktromagnitikh_Entypo_3.pdf.

[63] U. NTIA, “US National Telecommunications and Information Administration,” [Online]. Available: https://www.ntia.doc.gov/files/ntia/meetings/lte_technical_characteristics.pdf.

[64] “NS3 - NSnam,” [Online]. Available: https://www.nsnam.org/doxygen/classns3_1_1_oh_buildings_propagation_loss_model.html.

[65] Z. K. Adeyemo, O. K. Ogunremi and I. A. Ojedokun., “Optimization of Okumura-Hata model for long term evolution network deployment in Lagos, Nigeria.,” *International Journal on Communications Antenna and Propagation,* vol. 6, 2016.

[66] EETT, “EETT Radio Spectrum,” [Online]. Available: https://www.eett.gr/opencms/export/sites/default/admin/downloads/Consultations/RadioCommunications/PC-1800MHz.pdf.

[67] NSNAM, “NSNAM,” [Online]. Available: https://www.nsnam.org/doxygen/classns3_1_1_cqa_ff_mac_scheduler.html.

[68] “NS3,” [Online]. Available: https://www.nsnam.org/.

[69] G. Carneiro, P. Fortuna and M. Ricardo, “FlowMonitor: a network monitoring framework for the network simulator 3 (NS-3). In Proceedings of the Fourth International ICST Conference on Performance Evaluation Methodologies and Tools (VALUETOOLS ‘09),” 2009. [Online]. Available: http://dx.doi.org/10.4108/ICST.VALUETOOLS2009.7493.

[70] “Perl Programming Language,” [Online]. Available: https://www.perl.org/.

[71] “Waf Meta Build System,” [Online]. Available: https://waf.io/.

[72] “Python.org,” [Online]. Available: https://www.python.org/download/releases/3.0/.

[73] “Pandas Pydata,” [Online]. Available: https://pandas.pydata.org/.

[74] “Matplotlib,” [Online]. Available: https://matplotlib.org/stable/index.html.

8 List of Abbreviations

Abbreviation	Term
AMI	Advanced Metering Infrastructure
ANSI	American National Standards Institute
API	Application Program Interface
BACnet	Building Automation and Control Networking Protocol
BAP	Blockchain Access Platform
BEMS	Building Energy Management System
BESS	Battery Energy Storage System
CGMES	Common Grid Model Exchange Standard
CIM	Common Information Model
CIS	Customer Information Systems
COSEM	Companion Specification for Energy Metering
CSMA/CD	Carrier-sense Multiple Access with Collision Detection
DA	Distribution Automation
DDC	Direct Digital Control
DER	Distributed Energy Resources
DEMI	Distributed Energy Management Initiative
DLMS	Device Language Message Specification
DLT	Distributed Ledger Technology
DMS	Distribution Management System
DNP	Distributed Network Protocol
DR	Distributed Resources
DRMS	Demand Response Management Systems
DSO	Distribution System Operator
DSOTP	Distribution System Operator Technical Platform
ECD	Electron Capture Detector
EESS	Electrical Energy Storage System
EES	Electrical Energy Storage
EMC	Electromagnetic Compatibility
EMS	Energy Management System
eNB	evolved NodeB: A 4G capable base station
EPA	Enhanced Performance Architecture
EPC	Evolved Packet Core
EPS	Electric Power System
ETSI	European Telecommunications Standards Institute
EV	Electric Vehicle
E-UTRAN	Evolved Universal Terrestrial Ration Access Network
FSGIM	Facility Smart Grid Information Model
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communication
HEDNO	Hellenic Electricity Distribution Network Operator
HSS	Home Subscriber Server
HVAC	Heating Ventilation and Air Condition
HW	Hardware
ICCP	Inter-Control Center Communications Protocol
ICT	Information and Communication Technology
IEC	International and Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronic Engineering
INEA	Innovations and Networks Executive Agency
IoT	Internet of Things
IP	Internet Protocol

IPFS	InterPlanetary File System
IPv4	Internet Protocol Version 4
ISMS	Information Security Management System
ISN	Inter-regional Security Network
ISO	International Organization for Standardization
IT	Information Technology
ITU-T	Telecommunication Standardization Sector
KPI	Key Performance Indicator
LAN	Local Area Network
LLC	Logical Link Control
LN	A Light Node responsible to collect metering data from close PMUs and transit the to a remote server
LTE	Long-Term Evolution
LV	Low Voltage
LVD	Low Voltage Directive
MAC	Medium Access Control
MAN	Metropolitan Area Network
MIC	Maximum Input Capacity
MIMO	Multiple-Input and Multiple-Output
MME	Mobility Management Entity
MQTT	Message Queuing Telemetry Transport
MTU	Maximum transmission unit
MV	Medium Voltage
NASPI	North American Security and Prosperity Initiative
NERC	North American Electric Reliability Corporation
NS3	Network Simulation 3: A C++ library for network simulation study
NTUA	National Technical University of Athens
OBIS	Object Identification System
oBIX	Open Building Information Exchange
OCPP	Open Charge Point Protocol
OFDMA	Orthogonal Frequency-Division Multiple Access
OPC	Object Linking and Embedding for Process Control (Foundation)
OPC UA	Object Linking and Embedding for Process Control (Foundation) Unified Architecture
OpenADR	Open Automated Demand Response
P2P	Peer to Peer
PCB	Polychlorinated Biphenyl
PDC	Power Distribution Centre
PDU	Protocol Data Unit
PEV	Plug-in Electric Vehicles
PGW/PDN-G	Packet Data Network Gateway
PHY	Physical Layers
PLC	Power Line Communication
PMU	Phasor Measurement Unit
POS	Point Of Sale
PPP	Point-to-Point Protocol
PSTN	Public Switched Telephone Networks
PUC	Public Utility Commission
PV	Photovoltaic
RDF	Resource Description Framework
RES	Renewable Energy Source
REST	Representational State Transfer
RF	Radio Frequency
Rhost	A Remote Host Server in which data are collected for further processing
RITT	Research Initiative Task Force

RNC	Radio Network Controllers
RTU	Remote Terminal Unit
RS	Recommended Standard
SCADA	Supervisory Control and Data Acquisition
SCL	System Configuration Language
SGIRM	Smart Grid Interoperability Reference Model
SGW	Serving Gateway
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SSCP	Secure SCADA Communication Protocol
STS	Standard Transfer Specification
SW	Software
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TR	Technical Report
TLS	Transport Layer Security
TSO	Transmission System Operator
UDP	User Datagram Protocol
UE	User Equipment: In this specific study being the same as LN
UML	Unified Modelling Language
VEN	Virtual End Node
VTN	Virtual Top Node
WAN	Wide Area Network
WG	Working Group
WPAN	Wireless Personal Area Network
XML	Extensible Markup Language