Funded by the European Union

Project Number:	774145
Project acronym:	Net2DG
Project title:	Leveraging Networked Data for the Digital electricity Grid
Contract type:	H2020-LCE-2017-SGS

Deliverable number:	**D3.1**
Deliverable title:	**ICT Analysis and Gateway Design (version without Annex)**
Work package:	WP3
Due date of deliverable:	M12 – 31/12/2018
Actual submission date:	M12 – 28/12/2018
Start date of project:	01/01/2018
Duration:	42 months
Reviewer(s):	Manfred Reitenspiess (GD), Jan Dimon Bendtsen (AAU-AC)
Editor:	Nicola Nostro (RT)
Author:	Hans Peter Schwefel (GD), Domagoj Drenjanac (GD), Rasmus Løvenstein Olsen (AAU-WCN), Kamal Shahid (AAU-WCN), Francesco Brancati (RT), Rosaria Esposito (RT), Nicola Nostro (RT), Francesco Rossi (RT), Enrico Schiavone (RT), Christoph Winter (Fronius), Nicole Diewald (Fronius), Karsten Handrup (KAM)
Contributing partners:	Resiltech, GridData, AAU-WCN, Kamstrup, Fronius

Dissemination Level of this Deliverable:	**PU**

Public	*PU*
Confidential, only for members of the consortium (including the Commission Services)	*CO*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 774145. Further information is available at www.net2dg.eu.

Document history

Version nr.	Date	Authors	Changed chapters
1.0	22/12/2018	See first page	Final version - Ready for submission

Statement of Originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Table of Contents

List of Figures

List of Tables

1 Executive Summary

The ICT Gateway represents the central entity within the overall Net2DG solution. It aims at collecting data from the field through different subsystem HeadEnds that act as point of contact. Collected data are then organized and properly stored in order to make them available to the application layer ICT Gateway also interacts with the Grid Observability Model to get an estimation and validation of data when they are not available from the field.

This deliverable lays the foundations for the identification of the existing (and not existing) interfaces with each Subsystem HeadEnd, aiming at identifying the characteristics that the existing systems are able to provide and the features that any HeadEnd systems to be developed should be able to provide. Additionally, it is provided an analysis of data types and the data volume created by each of the HeadEnds, which are considered in the project in order to ensure that the ICT Gateway and the related architecture are properly designed from software, hardware and network point of view.

As a result, an initial design of the ICT Gateway architecture is provided together with definition of data model, which represent a relevant input for the next implementation of the ICT Gateway. Finally, the deliverable also collects the results of fault and threat analysis carried out on the ICT Gateway architecture, taking into consideration both the relevant functions of the ICT Gateway and the interfaces with other systems. The final results of the analysis are the identification of potential countermeasures aiming at mitigating the scenarios of failure or attacks in the ICT Gateway, according to the next prioritization of hazards and threats.

2 Background and Introduction

This section provides the background and work done in this deliverable, and gives an introduction to the covered topics. Moreover, an overview of the state of the art is also presented in Section 2.2.

2.1 Overview and Structure of Deliverable

In Deliverable [D1.2] a sketch of the communication architecture in Net2DG is described. The high level view of this is here shown in Figure 1. This view provides a rough framework to describe functionalities and entities in the project, and aims to clarify and simplify the Net2DG system, as it is fairly complex and distributed in nature.

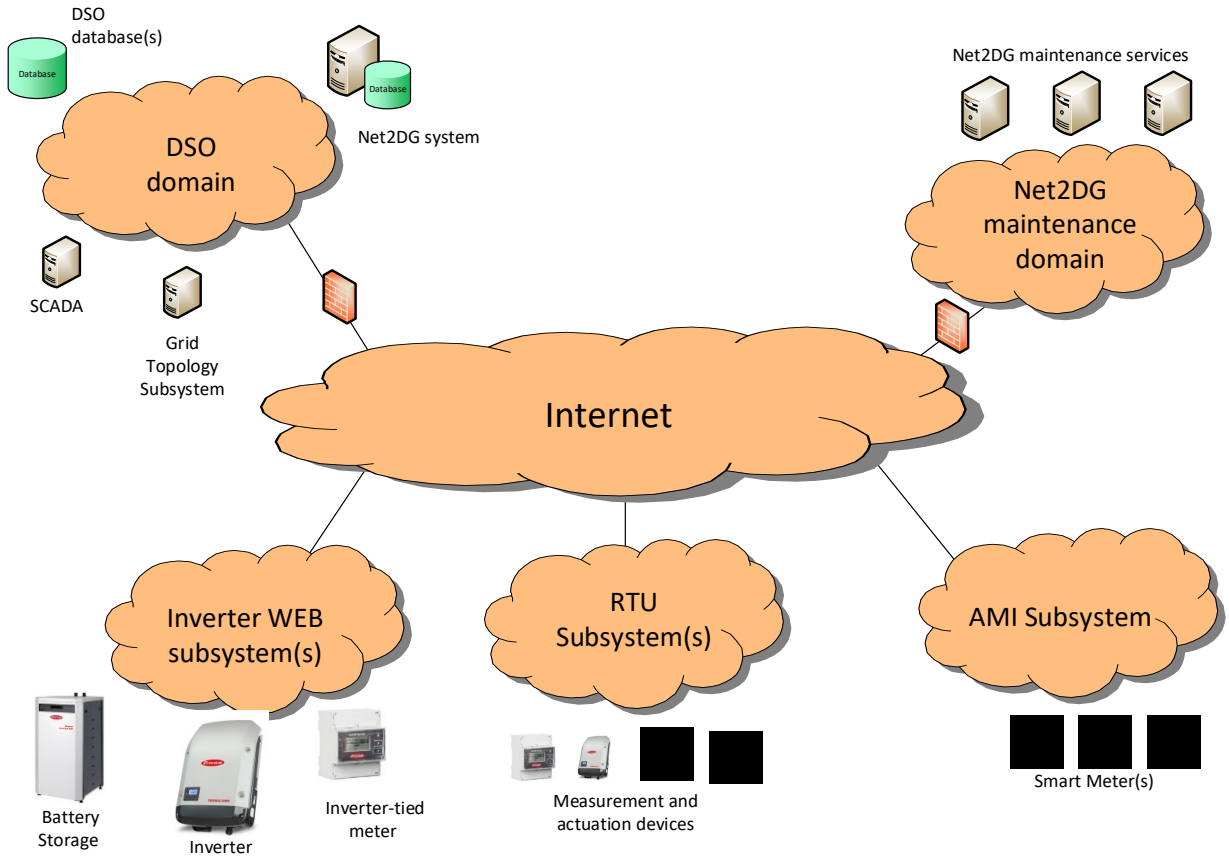

Figure 1: High-level Division of Access Domains and Subsystems (Deliverable D1.2 [1])

The main domains, which are also described in the Deliverable D1.2 [1] are summarized here:

- **DSO Domain**: DSO controlled and operated communication infrastructure
- **Net2DG maintenance domain**: a distributed set of services and functionality hosted at various Net2DG partners to support and maintain Net2DG functionality. This entails placeholders for log files, code repository, data traces, etc.

- **Subsystem domains** (Inverter WEB, RTU subsystem, AMI subsystem): Any system that provides useful information to the Net2DG system. A subsystem often hides a lot of internal complexities, optimizations etc., that is out of scope for the Net2DG project.

The main location of Net2DG functionalities is found in the DSO domain, while interfaces to subsystems are provided by the various system operators of the particular domain. As the work in Work Package 3 intends to detail interfaces, functionality and in general architecture, the structure of this document is such that subsequent to this overview, it provides an overview of system level state-of-the-art with the purpose of positioning the core aspect of Net2DG relative to other existing frameworks at both commercial and research level.
Thereafter in Section 3, the deliverable details existing interfaces to the subsystem with the aim to provide the reader with a full overview of the existing building blocks and their capabilities. This overview is important as it sets interaction possibilities, limitations and constraints in regards to subsystems, needed for the later design of the system.
Since all these data sources potentially produce a vast amount of data, a rough analysis of the data volume created to support the Net2DG system is provided in Section 4. It is important here to state that this is only a rough estimate, as more accurate data volume estimates require full understanding of application behaviours which at current state is not available. However, the aim is to ensure that the DSO domain networks and entities have enough capacity to handle the amount of traffic and data that is expected. Later measurements and assessments can then be done to validate the estimates for dimensioning the platform capacity for a final system deployment.
In Section 5 the initial design of the main components of ICT Gateway are described. This design is a first draft of an ICT platform that enables implementation and operation of the various applications based on subsystem interactions. Implementation of the described architecture is expected shortly after the release of this deliverable and will bring in valuable experiences for a second iteration of the architecture. Hence, an update is expected of this architecture later in the project.
To interface to the various subsystems, additional components are required, such as data format normalization, protocol conversions, various local optimizations (e.g. caching), security establishment etc. They will need to be addressed and handled individually. In Section 6, the components that will be needed for the selected subsystems will be designed and described. Later implementation of these components will similarly require an update of the internal structures later in the project.
Finally, in Section 7 an initial security and fault assessment is carried out on the sketched system concept. This part is important, as it allows to understand and prioritize problems and issues in relation to a first trial setup. In particular, this part plays a key role as to serve as documentation in accordance with the GDPR requirements for handling potentially sensitive data that the project has performed the required analysis and that it is enforcing the right level of protection and mitigations in the trial setups.
The deliverable ends with a conclusion in Section 8, which is followed by some appendices with useful information such as detailed interfaces, lists of information and events from subsystems, that are too large to include in the main document.

2.2 Concept State-of-the-Art Overview

The challenge of making data from different IT subsystems accessible and to enable data-intensive services on top of such heterogeneous data has been previously investigated in different application scenarios in the context of IoT platforms: Reference [2] provides a survey of different so-called IoT platforms, among them vendor specific solutions like Bosch Bezirk (allowing ad-hoc and peer-to-peer access), Vodafone IoT platform to connect to data sources via SIM card and cellular access and open platforms developed in consortia like FIWARE and OpenIoT. In the view of Net2DG, such IoT platforms can be seen equivalent to the sub-systems that the ICT Gateway of Net2DG connects to so Net2DG is not developing a new IoT platform, rather a solution to connect to existing data subsystems and to make distribution grid related data usable for data analytics applications that provide a benefit to the DSO. Abstracting from the specific usage purpose, the Net2DG solution to connect to subsystems has a similar ambition and purpose as interoperability solutions that have been developed in the BigIoT project, see [3]. However, the BigIoT solution is centered around a marketplace for data that uses semantic representations. While such approaches are useful for a wide variety of IoT use-cases, the focus of Net2DG is delimited to the DSO data sources, and the openness of an IoT marketplace is not (yet) required for the digitalisation of the distribution grids as considered in Net2DG.

In comparison to Net2DG, eSmart systems [4] also provide a platform that develops digital intelligence for the energy industry and smart communities. The eSmart system provides software solutions to the energy industry, service providers and smart cities, where the platform is designed to handle and exploit IoT, Big Data and Analytics technologies in real time. Common to all applications are vast data quantities gathered from sensors, which are analyzed using advanced prediction and optimization models. However, this platform is designed for Big Data from the ground up without legacy, wherein as stated above, Net2DG will be based on connecting the “existing” data subsystems and making distribution grid related data usable for data analytics applications that benefit the DSOs.
According to [5], currently a limited number of MV/LV substations are equipped with SCADA to exchange data. Reference [6] provides a review of recent implementations of advanced SCADA systems within TSO and DSO environments, a roadmap for a future system architecture, and integration and functionality requirements to meet the needs of the digital grid. It is also worth to mention here that SCADA systems can leverage industrial IoT technology to improve existing ICT infrastructure [5]. Moreover, in order to cope with future challenges (specially related to distributed generation) the Danish DSOs have published plans to install and employ SCADA systems in the near future [7]. Since the SCADA protocols introduce high network load [5] as well as the system performance is affected by the number of clients [5], it is worth to explore at this stage accurate data volume estimates for a full understanding of the various Net2DG applications in context of this deliverable.

Systems like eSmart provide more full-fledged BigData IoT platforms, but more restricted data analytics solutions are currently used in this field, too. This can be dedicated analytics or Business Intelligence (BI) solutions build by larger DSOs for their specific purposes - an example is Agder Energi

[8]. They have built a solution based on Microsoft's Azure technologies, which combines data from smart meters, substation monitoring, MV/HV monitoring and sources like weather and forecasting data. The Business Intelligent solution combines this to support daily operation (outage detection, voltage quality problems, etc.) as well as for planning purposes. Similar analytics solutions are provided by vendors in the market and resemble the Net2DG solution by combining multiple sources and some visualization to drive decision making.

The paper in [9] reviews the detailed applications of data analysis in smart grids, including predictive maintenance and fault detection with advanced metering infrastructure.

Distribution System State Estimation (DSSE) [10] is an analytical method for providing a reliable source of information related to the state of the grid, by filtering the raw data and detecting gross errors. Ideally, it makes use of near-real-time data to provide a good estimation. In many cases, this data is insufficient or unavailable. Traditional historic analytics generate pseudo-measurements which can build predictive outputs useful for DSSE and remedy to the lack of information. However, there is a higher error probability in the pseudo-measurements [11]. Data analytics should be built on a platform leveraging both historical and near-real-time analysis.
Authors of [11] tested the functionality of a DSSE algorithm and analyze the capabilities of processing large amounts of historical batch data. At the same time, the test aims to characterize the performance and bottlenecks of parallel processing of both stream and batch data types, taking into account parameters such as memory usage, processing time and in memory processing behaviour [11]. A summary of pros and cons of the aforementioned analytics for DSSE is presented in [12]. As historical-data-based analytics are useful to build periodic reports for strategic and long-term decisions, they are also limited by the temporal effects. Historical data may not give a true pattern of a data trend, if this has changed with time. While near-real-time analytical tools can address the temporal dependency, they are also platform sensitive [12].

In the Smart Grids, Machine-to-Machine (M2M) communication networks are fundamental to enable managing the huge number of sensors and actuators distributed all over the LV and MV networks. Power Line Communications (PLC) technologies represent a trade-off between technical (e.g., low latency, high availability), and economic perspectives (e.g., low deployment and operational costs).
The paper in [13] highlights some of the most relevant challenges in the area of PLCs and presents a set of cutting-edge *software tools* which are being developed to overcome them, facilitating the planning, deployment, and operation of this kind of networks. It presents a tool focused on diagnosing problems in operational networks based on monitoring them and analyzing collected traffic traces.
The authors also describe simulation tools for PRIME and MV-BPL (Broadband over Medium Voltage Power Lines) networks, the main goal of which is to facilitate their planning and performance evaluation. They believe this kind of tools would help DSOs in troubleshooting existing deployments [13].
As reported by [13], several companies and universities are actively exploring how to use tools and technologies to *realize a smarter grid*. Example projects from the US include:

- The Illinois Institute of Technology (IIT) and partners proposed to develop and demonstrate a system and supporting technologies to achieve *Perfect Power* at the main campus of IIT. Plans are for a self-healing, learning and self-aware smart grid that identifies and isolates faults, reroutes power to accommodate load changes and generation, dispatches generation and reduces demand based on price signals, weather forecasts, and loss of grid power [14].
- Some utilities are using predictive tools utilizing *phasor measurement data* for forecasting possible geomagnetic disturbances and protecting transformers from damage [15].
- A popular application is asset management where utilities are utilizing *predictive analysis* to determine when their assets require maintenance [16].
- Tollgrade Communications company provides data mining and machine learning-based analytics on historical events data in an integrated hardware-software platform for real-time event detection. This demonstrates the use of predictive grid-analytics on data collected by the company's proprietary smart-grid sensors for preventing blackouts to occur. The platform identifies anomalies on a distribution feeder before they magnify and thus enables a proactive, predictive strategy for managing real time events, similar to the concept envisaged for predictive detection of unintentional islanding in feeders. Utilities like Western Power Distribution have used this platform and have experienced improved reliability indices [17].

The authors of [13] also report some examples of smart grid projects and related tools from the UK:

- Network Constraints Early Warning Systems: the projects by Scottish Power Energy Networks aim to utilize large-scale, distributed smart meter data to monitor and detect the risk of power surges and voltage excursions beyond technical operational limits in different parts of the distribution network (or subnetworks). With millions of consumers, one cannot collect data in real time from every smart meter/consumer in the network, therefore an important question to answer is what data granularity is needed for different parts of the network to detect these excursions and provide early warnings of potential vulnerabilities [13].
- Thames Valley Vision by Scottish and Southern Electricity Networks: The project was the first scaled deployment of LV substation monitoring of real time electricity data and their integration into a distribution management system. Data were used for substation categorizations, aggregation and forecasting of future network loading [18].

Moreover, another recent project, named UpGrid project [19], has been done under the H2020 program, developed by a European consortium that includes seven European countries (Spain, Portugal, Poland, Sweden, United Kingdom, France and Norway). The target of this project was to develop and validate solutions to enable the implementation of advanced functionalities over existing technology, to form an integrated intelligent system. Additionally, improvement of the monitoring and controllability of LV and MV grids was also targeted as a way to anticipate technical problems associated with large-scale integration of Distributed Energy Resources (DERs), bringing the end users closer to system operation and planning. In this context, reference [19] as outcome of the UPGRID project describes the usage and implementation of the Common Information Model (CIM), standardized through the IEC 61970, IEC 61968 and IEC 62325 series, as the reference data model for the project, which provides highly useful knowledge for Net2DG. The primary benefit of CIM is that it models the static as well as dynamic information that defines a power system to facilitate integration of applications such as an energy management system and a distribution management system

developed independently by different vendors. As the grid topology subsystem in Net2DG is specific to the individual DSOs (from Stadtwerke Landau and Thy-Mors Energi), not only a common language is required to interoperate between the working groups but also a common messaging between applications has to be developed in the project. For this, Section 5.2 provides details of the "CIM inspired" grid topology model that will be used in Net2DG.

The authors of [20] developed a simulation platform as a, performant, modular and parallelizable tool to automatically analyze large LV network sets. Their environment is capable of analyzing a high number of networks and performing various in-depth studies, including the calculation of the maximal hosting capability per feeder for a high number of scenarios.

Reference [21] considers the scenario of information integration of different information sources for grid outage analysis. It provides a high-level data model as well as a high-level view of using a universal service bus to connect different data sources. However, the publication does not go into details or evaluation of its realization, neither does it present and analyse concrete algorithms.
Regarding Data Models, both the Modbus protocol specification and also the specification of IEC 61850 for substation automation [22] contains data models that are candidates to use for the ICT Gateway.
In order to cope with the increasing complexity of the power grid, due to higher penetration of distributed resources and the growing availability of interconnected systems, there has been an ever-increasing interest in multi-sensor data fusion technology, driven by its versatility and diverse areas of application. In this context, reference [23], presents a review of the data fusion state of the art, exploring its conceptualizations, benefits, and challenging aspects, as well as existing methodologies. Similarly, reference [24] proposes a computational framework for power systems data fusion, based on probabilistic graphical models. According to [24], this framework is capable of combining heterogeneous data sources with classical state estimation nodes and other customized computational nodes. The fused information is demonstrated to reduce the effect of noise in the various data sources, and occurrences of missing or erroneous data are easily overcome and diagnosed. However, this work is based on the assumption of having fully known measurement functions without highlighting the impact of variable information from heterogeneous sources. Further, reference [25] introduces a data fusion method based on an ordered weighted averaging operator for smart grids that is meant for fast and accurate fault detection and diagnosis to isolate faulty components and avoid further complications.

Other standardization frameworks exist in the area of electricity distribution and metering. For metering the most commonly used standard is DLMS/Cosem, which is standardized in the DLMS forum and adopted by IEC as IEC 62056. DLMS/Cosem defines the communication protocol (DLMS) and the inherent data/object model (Cosem), the latter uses OBIS codes as data type identifiers.
On higher level, the market trend is to build integrations on the IEC 61968 family of standards. It includes the definition of the Common Information Model (CIM) as well as the interface specification (IEC 61968-9) and its adaptation to specific scenarios like metering or substation control. Objects within the CIM model are identified by a CIM code (an 18-element dotted notation, described in

IEC61968-9, annex C). This notation allows a very detailed expression of the measurement data (type, unit, measurement method, etc.).

3 Analysis and Overview of Existing Interfaces

3.1 Interface Overview

For interfacing between various subsystems, the ICT Gateway needs some way to be able to use a variety of interfaces, protocols and data models. In Figure 2 the concept that Net2DG has taken is illustrated at an abstract level.

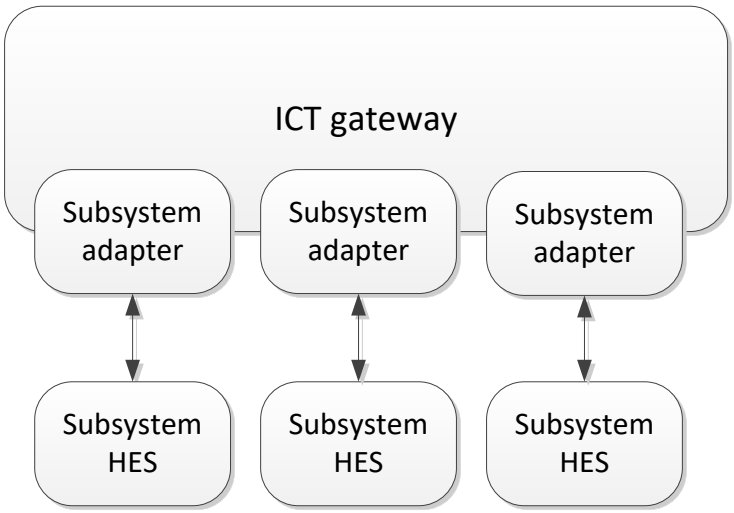

Figure 2: Simplified Overview of Interfacing Concept Between Subsystems and ICT Gateway

For each subsystem two components are defined to ensure the interaction:

- A subsystem adapter: A software piece that ensures the ICT Gateway is able to communicate via the appropriate protocol for the specific subsystem
- A HeadEnd System (HES): is a centralized software entity that bridges the complex network of information sources to the single link towards the ICT gateway (via the adapter).

This approach is taken as a natural decision as most existing subsystems already have some sort of HES available, for the purpose of hiding internal management of nodes and communication, and to provide a clean interface to client software such as the ICT gateway (via adapters). Other subsystems such as PQ measurement devices do not yet have such a structure, but the intention is to keep this design approach consistently for all, as it allows flexible extension and management of the fleet of devices deployed. Doing so releases the ICT gateway from a number of otherwise potentially complex operations, such as device and service discovery, security and trust establishment, dynamic IP address mapping and distributes pre-processing load for e.g. data validation etc. such it is not all located on a single machine.

In all circumstances, the first step of applying this concept is to understand existing interfaces and interaction possibilities, which is done systematically in the following sub sections. Later, in Section 5 and 6, details on how these adapters (and their responsive HES) are integrated in the architecture is detailed. Each of the following sub sections describes interfaces between such an adapter and HES as illustrated in Figure 2.

3.2 AMI HE to ICT GW

The electricity meters come with an integrated radio unit which is able to communicate with other meters and data concentrators. Each meter relays communication between other meters, and together they form a tight mesh infrastructure with hundreds of alternative communication lines. The many alternative communication lines create a highly stable and secure network, even when meters are decommissioned, moved or added. An advanced metering infrastructure (AMI) network is just as dynamic as the distribution network which it is commissioned to control. The data concentrator manages and optimises the communication lines automatically to retain reliability, stability and performance and thereby serving as the AMI HeadEnd system. The smart meters are able to generate alarms in case of poor power quality, tamper detection, etc. These alarms are pushed through the radio mesh network to the data concentrators with priority and then further pushed through the HeadEnd system to the ICT GW. The ICT GW system is used for storing and working with meter date. The HeadEnd supplies data to other business systems such as billing systems, distribution management systems and operation management systems. The data concentrators contain distributed intelligence for the autonomous collection of metering values and power quality events throughout the day. As soon as the data has been collected by the concentrators it is forwarded to a HeadEnd system.

Table 1 and Table 2 identify the interface options between AMI HE and ICT GW, and the list of data and event loggers, respectively.

Table 1: Subsystem Interface Options

System AMI HE to ICT GW	ICT GW to HE	HE to ICT GW
Request-Reply(	Request(logger[x])	Reply(logger[x])
Publish	N/A	Send logger upon request
AsyncRequest(order(x))	Request for asynchronous execution of order(x)	OK or Not-OK
SyncRequest(order(x)	Request for synchronous execution of order(x)	OK or Not-OK
Reply(status, [result])	Reply from order request, in case of asynchronous request, it contains a status on the acceptance of the order request (OK/Not-OK). For the synchronous request, it contains an execution status and optionally an order result.	

Table 2: List of data and event loggers

List of data loggers	List of event loggers
Load Profile[1] (5, 15, 30, 60min)	Voltage Quality
Analysis Logger	Power quality
Power Quality	Meter RTC
Daily Logger	Breaker
Debitlogger	Neutral fault
Earth fault	Earth fault
Temperature	

The representation and specification of the data models used in the AMI HE to ICT GW are presented in Table 3.

Table 3: Data models and representation

AMI HE to ICT GW	Specification
Voltage Quality	Phase, event, mean/max/min. value
Load Profile	Active & Reactive energy
Power Quality	Frequency counter, voltage variation ±10%, rapid voltage changes, power interrupts, voltage dips and swells, voltage THD L1 to L3, current THD L1 to L3.

Table 4 presents the possible time synchronisation interfaces between AMI HE and ICT GW. Considering that the ICT GW may be synchronised via an NTP server, the HE may preferable be time synchronized to the same NTP server, but in cases where this is not possible, the ICT GW may need time synchronisation signals from all subsystems to be able to determine a common time base.

Table 4: Time Synchronisation

AMI	ICT GW to AMI HE	AMI HE to ICT GW
Time synchronisation	The units are synchronised to an NTP (Network Time Protocol) source	The HeadEnd System receives its time from the server it is attached to.

A brief list of alarms sent from AMI HE to the ICT GW is given in Table 5.

Table 5: List of alarms

[1] Active energy, Reactive energy, Quality, Status

AMI HE to ICT GW	Description
Over voltage L1 to L3	Set if overvoltage on phase
Under voltager L1 to L3	Set if undervoltage on phase
Missing phase fault L1 to L3	Set if phase is missing
Phase Voltage sequence	Set if phase voltage sequence is reversed
Earth Fault	Set if earth fault is detected
Magnetic detection	Set if magnetic field is detected - Tampering
ReversePhaseCurrent L1 to L3	Set if reverse current is detected on phase
VoltageAsymmetryStatus	Set if voltage asymmetry is above 2%
Power fail	Set if power fail is registered
NoPhaseCurrent L1 to L3	Set if no current is registered on phase

Table 6 lists the required components and their description for the installation, operation and maintenance of communication between AMI HE and ICT GW.

Table 6: Required system infrastructure for installation, operation and maintenance

Infrastructure component	Description
LAN infrastructure and WAN infrastructure	As required
Domain controller	Directory domain controller must be available for user verification and management, the domain controller is required to obtain role-based access to the system.
Active Directory Federation Services	AD FS must be available for role/right services for easy administration
Active Directory Certificate Services	AD CS must be available to support role/right service.
Network naming services DHCP, WINS, DNS	IP address management.
Backup infrastructure	For data protection, a backup solution must be available. The backup solution must be able to backup file systems.
FTP server	An FTP server is required to support firmware uploads. The FTP server can be closed down when not in use.
NTP server	An NTP server is required for network time synchronisation.
VPN terminator	A VPN server acts as either a hardware appliance or a virtual server. Both solutions use pfSense.

3.3 Solarweb Server to ICT Gateway Interface

The prioritized communication path between inverter subsystems and the ICT Gateway is via the Fronius cloud system Solarweb (SW). Therefore, the IEEE 2030.5 communication protocol offers not only possibilities to read data, but also to actively send control commands for grid voltage dependent reactive power, to change the power factor cos phi and to reduce grid voltage dependent power. The

IEEE 2030.5 protocol implements a client/server model based on a representational state transfer (REST) architecture utilizing core HTTP methods [26].
The communication between Solarweb and the ICT gateway can take place using an adapter. Table 7 and Table 8 identify the interface options between SW and ICT GW, and the data model from SW to ICT GW with their representation, respectively:

Table 7: Subsystem Interface options via IEEE 2030.5

SW	SW to ICT GW	ICT GW to SW
Subscribe(type[x])	list of end devices; DER control commands	monitoring data, status information and alarms
Publish	monitoring data, status information and alarms	changes to the end device list, changes of DER control commands
Get(order(x))	request device capabilities, end device list, grouping assignments of inverters, der control commands (default values, events, curves) for groups	N/A
HTTP PUT	send inverter specific status, capability, settings, availability	N/A
Reply(status,[result])	HTTP 200,..	HTTP 200,..
Data format supported	XML	XML

Table 8: Data models and representation

SW to ICT GW	Parameter	unit	meta data
Monitoring Data	Real (Active) Power	Watts	Time stamp, data qualifier (not specified, minimum, maximum or average)
	Reactive Power	VArs	Time stamp, data qualifier
	Frequency	Hertz	Time stamp, data qualifier
	Voltage	Volts	Time stamp, data qualifier
Events	Status Information		Time stamp
	Alarms + return to normal		Time stamp

The list of alarms and status information sent from SW to the ICT GW is given in Table 9.

Table 9: List of alarms and status information

SW to ICT GW	parameter	description	resolution
Alarms	Over Current	Out of boundaries depending on the country regulations	Posted as they occur
	Over Voltage		
	Under Voltage		
	Over Frequency		
	Under Frequency		
	Voltage Imbalance	Asymmetric voltage in the grid	
	Low Input Power	To be defined	
Status Information	Operational State	To be defined, most likely: standby Inverter is off Inverter is shutting down Inverter starting Inverter working normally Power reduction is active One or more faults present Inverter is currently being updated	To be defined
	Connection Status	No communication possible	

The details of the data model from ICT GW to SW is presented in Table 10.

Table 10: Data models and representation

ICT GW to SW	parameter	unit	meta data
Control commands	DefaultDERControl	Control values	
	DER Control	Control values	Start and stop time
	DER Curve	x-y curve	
Additional Information	Changes in End Device List		
	Changes in Group Memberships		

Table 11 presents registration methods to support communication between SW and Web HE.

Table 11: Registration methods supported

SW	SW to Web HE	Web HE to SW
Subsystem Registration	Inverter ID	Acknowledge
Capability registration	Web HE has lists with measurement and actuation capabilities as meta data	
Time synchronisation	NTP based time synchronisation from external server in SW	

Table 12 and Table 13 outline the supported security options and requirements for service support interfaces for communication between SW and ICT GW, respectively.

Table 12: Security options supported

SW	Type	Additional
Encryption	TLS v1.2	
Authentication	Mutual authentication during TLS handshake by exchanging and authenticating each other's certificates (specified by Inverter Web HeadEnd)	
Key	Preshared keys	
Integrity protection	TLS V.1.2 provides data integrity because transmitted messages include a message integrity check using a message authentication code to prevent undetected loss or alteration of data during transmission.	
Subsystem internal protection mechanism		

Table 13: Service support interfaces and requirements

SW	SW to ICT GW	ICT GW to SW
Time synchronisation	Time synch. signal to HE (SW time master, HE is slave)	
Metadata	Web HE hosts metadata for ICT gateway requests	

3.4 Inverter RTU HeadEnd to Local Inverter Interface

The communication between the RTU HeadEnd and the Inverter via Modbus TCP requires a local unit (Inverter RTU), which provides a VPN connection. This local unit could for example be a router or a small computer. The RTU HE could also be included in the ICT gateway as an adapter.
The inverter RTU HE is only described as a possible supporting solution and is not intended to be used in the project. Table 14 and Table 15 identify the possible interface options between Inverter RTU and RTU HE, and the data model with their representation, respectively:

Table 14: Subsystem Interface Options

System Inverter	Inverter RTU to RTU HE	RTU HE to Inverter
Subscribe(type[x])	Not supported	Not supported
Publish	Not supported	Not supported
Notify	Not supported	Not supported
AsyncRequest(order(x))	Data types (voltage, power, etc.)	Request values via Modbus TCP Sunspec Standard
SyncRequest(order(x))	Depending on RTU HE	
Data format supported	Modbus TCP Big Endien (there are standard functions for Modbus to convert data into other data formats)	

Table 15: Data Models and Representation

RTU HE to Inverter	Register	Meta data
Models:		
Fronius register	Inverter state codes, store and delete data, change data types, aggregated values (power, daily/yearly energy, total energy of the system)	ID, length of register
Common & Inverter Model	Request device information (sunspec ID, model, serial number, SW version,…); Request AC total and phase currents, AC total and phase voltages, AC power and frequency, apparent power, reactive power, power factor, DC current, DC voltage and DC power, events)	ID, length of register
Nameplate Model	Request nominal values of inverter	ID, length of register, scale factors
Basic Settings Model	Set power output, voltage at PCC (point of common coupling), settings for maximum apparent power and	ID, length of register, scale factors

RTU HE to Inverter	Register	Meta data
	maximum reactive power, minimum power factor	
Extended Measurements and Status Model	Request additional measurement and status values (inverter connection status to the grid, active inverter controls [power reduction mode, constant reactive power specification, constant power factor], source for time synchronisation, current time)	ID, length of register
Immediate Controls Model	Inverter settings: • deactivation of inverter's grid power feed operation (connection control) • constant reduction of output power • specification of a constant power factor cos phi • specification of a constant relative reactive power [%]	ID, length of register, scale factors, time windows
Meter Model	Request Fronius Smart Meter data: AC total and phase currents, AC total and phase voltages, AC total and phase power (active, reactive apparent), AC frequency, aggregated values over lifetime, events	ID, length of register, scale factors

Table 16 presents registration methods to support communication between Inverter and RTU HE, while Table 17 and Table 18 list the security options and service support interface requirements for this communication.

Table 16: Registration Methods Supported

Inverter RTU	Inverter to RTU HE	RTU HE to Inverter
Subsystem Registration	Open TCP/IP port and acknowledge request of RTU HE	Via IP address (static address required) and port (can be defined when the interface is activated on the inverter); RTU HE sends request to inverter to establish TCP/IP connection
Capability registration	Reply capabilities	Request available Sunspec models (there are differences for battery

Inverter RTU	Inverter to RTU HE	RTU HE to Inverter
		systems and if the inverter has one, two or three phases)
Time synchronisation	No timestamp available via Modbus TCP	

Table 17: Security Options Supported

System Inverter RTU	Type	Additional
Encryption	No encryption	
Authentication	No authentication	
Key	No keys	
Integrity protection	No integrity protection	
Subsystem internal protection mechanism	No security measures because it is an internal interface, no public interface; it can only be used locally and after manual activation	

Table 18: Service support interfaces and requirements

Inverter RTU HeadEnd	
Time synchronisation	No time stamp available for Modbus TCP requests, it just gets actual data at the moment when the data is requested. The timestamp must be added by the Inverter RTU HeadEnd – therefore the ICT gateway time can be used

3.5 Mobile PQ to RTU Interface

A mobile PQ (M-PQ) is a power quality measurement instrument designed to facilitate monitoring, recording and display of data on four voltage channels and four current channels simultaneously. The MAVOWATT 270 M-PQ device can monitor power configurations as (a) Single Phase, (b) Split Phase, (c) 3 Phase, Four Wire Wye, (d) 3 Phase (Floating or Grounded) Delta, (e) 3 Phase 2-Watt Delta, (f) Generic Circuit, (g) 2½ Element without Vb, and (h) 2½ Element without Vc. (For details of each configurations, please refer to the complete operating instructions in [27]). However, measuring and monitoring power quality (PQ) parameters require several calculations, i.e. RMS values of voltage and current, etc. Depending on the type of parameter measured, calculations are performed using samples of monitored waveforms or using every sample cycle for quick disturbance detection (see [27] for details of each parameter used in PQ calculations). In the Net2DG setup, the measurements

stored/captured by this instrument will be made accessible by the Remote Terminal Unit – HeadEnd (RTU-HE) via a communication channel. Here, RTU-HE will collect measurements from all connected M-PQ devices and transfer those to the ICT Gateway.

Currently, M-PQ devices can be used for:

- Long time recordings, where the instrument is set to use periodic measurements only (this setting is used for long-term statistical studies and benchmarking field-based equipment testing and evaluation)
- Continuous data logging (short intervals), where the instrument is set to log RMS and power values once per "x" seconds until memory is filled or for a specified time period.

However, a communication interface does not exist in the available devices (i.e. no transmission/reception of measurements/requests). Therefore, an interface first needs to be created before the designed RTU is able to access the required information. Table 19 identifies the possible interface options for communication between Mobile PQ and RTU HE, while Table 20 lists the default settings for the threshold parameters in aforementioned monitoring modes.

Table 19: Subsystem interface options

Mobile PQ to RTU Interface	Mobile PQ to RTU	RTU to Mobile PQ
Request-Reply()	Reply(logger[x])	Request(logger[x])
Publish	Not Supported	Not Supported
AsyncRequest(order(x))	Not Supported	Not Supported
SyncRequest(order(x))	Not Supported	Not Supported
Reply(status, [result])	Not Supported	Not Supported
Data format supported by mobile PQ device	Graphics are saved as images in .bmp format while alphanumeric content is saved as XML file	

Table 20: List of default settings for the threshold parameters in each monitoring mode

Parameters	Standard Power Quality	Fault Recorder	Long-term Timed Recording	Continuous Data Logging	Energy Audit
Volts	10 Minutes	Off	10 Minutes	1 Second	10 Minutes
Amps	10 Minutes	Off	10 Minutes	1 Second	10 Minutes
Power	10 Minutes	Off	10 Minutes	1 Second	10 Minutes
Demand	15 Minutes	Off	10 Minutes	Off	5 Minutes
Energy	10 Minutes	Off	10 Minutes	10 Minutes	10 Minutes
Harmonics	10 Minutes	Off	10 Minutes	Off	10 Minutes
Flicker (Pst)	10 Minutes	Off	10 Minutes	Off	Off
Flicker (Plt)	2 hours	Off	2 hours	Off	Off

Table 21 and Table 22 list the communication and security options as well as the time synchronisation synchronisation option supported by the Mobile PQ device, respectively.

Table 21: Communication and Security Options Supported

Mobile PQ system	Type	Description
Data Communications Options	Ethernet IP Connection (Wired)	Mobile PQ device (MAVOWATT 270) can be connected to any Ethernet network (10/ 100 MBaud Ethernet) using Ethernet/IP software protocols. Configurations using the Ethernet/IP protocol require an IP Address for network communication and a Gateway address to effectively communicate with the host device. Connection through HTTP requires connection authentication with user name and password.
	Wireless (WiFi) network connection	Identical to a standard Ethernet connection except that it requires a wireless local area network (WLAN) access point or hotspot based on any of the 802.11x standards
	Bluetooth connection	The Bluetooth interface uses a PAN network that is only available on PC based devices.
	VNC connection	Can be Virtual network computing (VNC)-enabled so that any VNC Client can access the instrument remotely, provided the correct password is entered. VNC software allows to view and interact with the mobile PQ device (MAVOWATT 270) from any other computer or mobile device anywhere using the Internet.
	Modbus connection	Can also be connected for real-time measurement reading via Modbus/TCP protocol.
Security	Passwords, Security Type and Encryption must be obtained depending on the network you want to connect to.	

Table 22: **Time Synchronisation**

Mobile PQ	Mobile PQ to RTU	RTU to Mobile PQ
Time synchronisation	Time sync options include GPS, NTP or Real Time Clock (RTC). Each Time Sync Source button toggles the respective source enabled or disabled.	The RTUs receive time from the server they are attached to.

Mobile PQ	Mobile PQ to RTU	RTU to Mobile PQ
	If all three are enabled, time sync is sourced by the instrument in the following priority order: If GPS is available, then it is used. If not and NTP is available, then NTP is used. If neither GPS nor NTP is available, then RTC is used.	

3.6 Stationary PQ (Janitza Device) to RTU Interface

The Janitza device UMG96RM is a measurement device for electrical parameters that can be used for building installations as well as for bus bar trunking systems in LV grids [28]. These devices will be used in Net2DG for substation measurements and also for selected measurements in junction boxes and at customer sites in the StwLan field trial. Also, the Janitza devices are candidates for deployment at grid nodes in the TME field trial for validation purposes.

The Janitza device supports reading and writing values from a client software communicating with the Janitza device, where the communication between the two is performed by utilizing the Modbus TCP protocol.

The Janitza device provides the following types of measured values which can be accessed by providing the address of internal registers, which internally in the device are updated every 200ms [29]:

- Measured values: A measured value is an effective value which is formed over a period (measuring window) of 200ms. A measuring window is 10 periods in the 50Hz network and it has a start time and an end time.
    - In addition, the peak value negative and peak value positive are measured as the highest negative/positive value in the last 200ms interval.
- Mean value of measured values: For each measured value, a sliding mean value is calculated over the selected averaging time which can be configured on Janitza devices independently for current, voltage and power.
- Min and max of measured values: The max value of the measured value is the largest measured value which has occurred during the observation interval. Similar holds for min value of the measured value.
- Max of mean values: The max value of the mean value is the largest mean value which has occurred.

Each value can either be requested as type float (4 bytes) or short (2 bytes).

Timestamps: Resolution of timestamps for interval specification is 2ns. The accuracy of the start time and end time depends on the accuracy of the internal clock (typically drift +- 1 minute/month). In order to improve the accuracy of the internal clock, it is recommended that the clock in the device is compared with a time service and reset. The Clock in the device is represented with separate read/write registers for year, month, day, hour, minute and second.

Averaging intervals: By default, the averaging interval is set to a period of 480s (8min). The interval can be varied from 5s to 900s. The mean values for the adjusted sliding window are calculated every 200ms.

Table 23 lists the data models and their specification for the Janitza device Modbus interface:

Table 23: Data models and representation

Janitza device Modbus interface (Measured Parameters)	Specification	Meta data
Voltage	Voltage values for each phase to neutral or phase to phase. Zero sequence, positive and negative sequence.	Start and end time of averaging window; resolution and measurement errors are parameter specific, see Tables in [4]
Current	Currents per phase and their vector sum over 3 phases. Zero sequence, positive and negative sequence.	
Phase	Phase angles between voltage and currents on each phase, cos-phi per phase	
Power	Real and apparent power for each phase to neutral	
Energy	All per phase: Real energy, real energy consumed, real energy delivered, reactive energy, reactive energy inductive, reactive energy capacitive, apparent energy	
Harmonics	THD On voltages per phase, THD on currents per phase, 0^{th} to 39^{th} harmonics on each phase on U and I (on U also phase-to-phase)	
Frequency	Measured frequency	

Table 24 and Table 25 describe the communication and security options as well as the time synchronisation options supported for communication between Janitza device and RTU.

Table 24: Communication and Security Options Supported

Janitza device	Type	Description
Data Communications Options	Modbus over IP over Ethernet Connection (Wired)	Basic principle of this interface is that Modbus addresses that are specified in [4] are used to access a specific measurement type (with a fixed unit given by the same table) or to set a certain parameter.
	Serial Port	Modbus protocol where the data can be changed and retrieved with the help of Modbus address list.
	User interface on device	A screen with two buttons for reading out values and setting basic parameters, e.g., fixed IP address.
Security	There is no authentication method applied when accessing device registers with the help of Modbus address list.	

Table 25: Time Synchronisation

Janitza device	Janitza device to RTU	RTU to Janitza device
Time synchronisation	Janitza device supports reading and setting UTC system time with the help of Modbus address list.	The RTUs receive time from the server (HeadEnd) they are attached to and thus can use time provided by ICT Gateway to perform synchronisation. RTU can then timestamp all the values it receives from Janitza device.

3.7 Streetlight to RTU Interface

The streetlight control is done via an analogue switching relay, which has two states (ON and OFF). There is no existing digital interface, but a self-designed RTU would need to directly control this relay.

In most LV grids, the street lights are on separate feeders in the LV grids (directly connected to the substation), and furthermore the future evolution is towards LED lights with low consumption (currently most street lights in the Stadtwerke Landau area have a 125W consumption per light). Therefore, it is not yet clear whether street light activation is able to usefully contribute to Automatic Voltage Regulation and hence more analysis on this in WP2 and WP4 will first be done, before analysing and designing the interfaces to the street lights. This task is therefore conditionally scheduled for Q2/2019.

3.8 Grid Topology to Grid Topology HE Interface

As the grid topology subsystem is specific to the individual DSOs, the following sections describe separately the two different DSO subsystems.

3.8.1 Grid Topology Subsystem of Stadtwerke Landau

The grid topology subsystem of Stadtwerke Landau consists of the GIS system with its Database and is complemented by different data sets that are stored in additional (mostly xls) files. The interface used in Net2DG will rely on export of this stored data to files that are then accessible by the Grid Topology HeadEnd. Data are exported in various files where each file represents data related to one entity, e.g., a file with all house connections, a file with all cables, etc. The following entities are provided by the grid topology subsystem:

- House connection
- Photovoltaics
- Substation
- Junction box
- Sleeve and
- Cables

Each file corresponding to one entity is described in Annex A.

Additionally, the grid topology subsystem also provides data about street lights, but due to the insufficient metadata about street light systems, street light data are currently not processed in detail. The only information that is used is the total length of the feeder to which the street lights are connected, the maximum power of the lights, and the number of street lights on this feeder.

Since the grid topology subsystem exports files on a file system, the Grid Topology HE has to have read access to that same file system and has to know the names of files in order to access and read the topology data. The workflow is captured in the Table 26.

Table 26: Grid topology Subsystem (GTS) to Grid Topology HE Interface Options

GTS to Grid Topology HE Interface	Grid Topology HE to GTS (file system)	GTS (file systems) to Grid Topology HE
Request-Reply()	Request(file[x]) from file system where GTS stores data	**Not supported**
Publish	Not supported	Different files exported periodically to file system (periods of few weeks)
AsyncRequest(order(x))	Not supported	Not supported
SyncRequest(order(x))	Not supported	Not supported
Reply(status, [result])	Not supported	Not supported
Data format supported by GTS	Files with proprietary GTS format where each row represents one entry in GTS. Values in row are separated with semicolon.	

3.8.2 Grid Topology Subsystem of TME

Grid topology system uses a Common Information Model (CIM) that supports for a manual export of stored data via a secure FTP link. As in Section 3.8.1, the interface used in Net2DG will rely on export of this stored data to the file that is then accessible by the Grid Topology HeadEnd. The data are exported in a single file (in XML format) that represents data related to the whole TME grid. In total, there are 22 entities with associated attributes provided by the GIS system, some of which are (the complete list is in Annex B):

- Assets
- Location of assets
- Substations
- Terminals
- Fuses
- Power Transformers
- Etc.

The description and associated attributes of each entity is provided in Annex B.

Since this XML file will be exported via a file system, the Grid Topology HE should have access to that file system in order to access and read the topology data. The workflow is captured in the Table 27 below.

Table 27: Grid Topology (GIS) to Grid Topology HE Interface Options

GIS to Grid Topology HE Interface	Grid Topology HE to GIS (file system)	GIS (file systems) to Grid Topology HE
Request-Reply()	Request(file[x]) from file system where GIS stores data	Not supported
Publish	Not supported	CIM based XML file exported to file system
AsyncRequest(order(x))	Not supported	Not supported
SyncRequest(order(x))	Not supported	Not supported
Reply(status, [result])	Not supported	Not supported
Data format supported by GTS	Single file with CIM based XML format	

4 Initial Data Volume Analysis

As the ICT Gateway is on the receiving side of lots of information sources, which may provide data from a large range of data sources, it is relevant to assess the data volume that can be expected on this node to ensure a proper dimensioning of the software and hardware, including also network capacity. This section aims to assess individually the data volume created by different subsystems under different conditions, and create a set of cases under which the ICT gateway must be able to work under. The cases heavily depend on the type of field that is being considered; hence the assessment is divided into four cases:

- Case 1.1: field test case A (~100 households for Landau)
- Case 1.2: field test case B (~2000 household for TME, potential largest extent of field trial)
- Case 2: full TME grid (~50.000 households)
- Case 3: full scale, a large medium sized DSO level (~500.000)

Since each subsystem creates data in their own context, the cases will need to be mapped into an individual parameter setting, which enables the four scale levels to be properly used. Later in Section4.8, an attempt to assess the expected overall data traffic volume will be assessed considering all subsystems are enabled and used. The outcome will give an indication on whether the DSO domain is suitable for the planned data streams in terms of network, hardware and software capacities. It is most likely that the field tests will create magnitudes less traffic volume as scoping and other limitations will play, but the assessment will serve also for long term assessments of system feasibility and requirements. Lastly, in this section there will be a pre-study of the network capabilities of the two DSOs with respect to setting-up the planned field tests.

4.1 AMI HE to ICT GW

The network is able to deliver 130 kByte data per metering point per day at a cluster size of 100 meters and 150 kByte data at a cluster size of 500 meters. On top of this, there is sufficient capacity to make over-the-air firmware upgrades and to perform additional on-demand services. The network even has surplus capacity to do network maintenance. The network supports prioritised commands so that high priority commands can be carried out immediately.
Examples of normal daily usage per meter at a cluster size of 500 meters is provided in Table 28.

Table 28: Overview of Data Capacity

Data type	Data amount (byte)	Capacity exploitation (%)
Load profile 4-quadrants 60-minute interval	289	
Day logger	60	
Power quality (estimated: 2 events/day)	10	
Analysis logger 4-channel	3,456	

Data type	Data amount (byte)	Capacity exploitation (%)
5-minute interval		
Utilised in total	3,815	26
Total capacity (cluster size = 500 meters)	14,800	100

In the example above, it is apparent that there is almost 75 % surplus capacity for OTA firmware upgrades, on-demand readings, demand side management, configurations and network maintenance. Network maintenance uses approximately 10 % of this capacity. The daily amount of data typically transferred between the data concentrators and the HeadEnd system is 2 MB per concentrator at a cluster size of 500 meters per concentrator.

From the HES to the ICT gateway, the total amount of traffic also needs transport, and assuming that happens fairly evenly distributed over a full day, and data is accessible when needed, this puts the following requirements shown in Table 29.

Table 29: Daily amount of data and transfer rates

Case	Daily amount of data	Data rates (if 1 hr. transfer)	Data rates (if 1 min. transfer)	Data rates (if 1 sec. transfer)
1.1: 100 households	382kB	106 B/s	6.3 kB/s	382 kB/s
1.2: 2000 households	7.6MB	2.1 kB/s	127 kB/s	7.6 MB/s
2: 50.000 households	191MB	53 kB/s	3.2 MB/s	191 MB/s
3: 0.5 mio households	1.9GB	528 kB/s	31.7 MB/s	19 GB/s

As Table 29 shows, for the larger sets it is not really realistic to transfer very fast, as it would require practically a private fiber line to the HES, and server/client capacity to send and receive data very fast. However, for the smaller setup, and if data transfer time is in the order of minutes, most network connections will do. Depending on the exact location of the ICT gateway in relation to the HES/adapter, private (non-shared) communication lines may be considered if timing is crucial while scaling the system to larger DSO's.

4.2 Inverter Modbus to RTU Interface

Based on previous applications, the data volume gathered via the Modbus TCP interface of Fronius inverters results in around 70MB for one PV system over one day, with an overhead of approximately 50% for the protocol for data exchange. This value is the result of requesting a majority of available data channels every second, thus can be seen as a worst case scenario and can be used as a basis for the following data volume estimations.

For Net2DG it is planned to request the monitoring data less frequently, in 5 minutes intervals. Therefore, the value can be scaled down which results in a data volume of 0.23MB per day. Adding the overhead of 50%, 0.35MB per PV system per day will be used in the further calculations.

Table 30 maps the defined scenarios of households into an estimated number of PV systems. The overall amount as well as the current number of Fronius inverters in both field test scenarios is a given value by the participant DSOs. The number of possible Fronius inverters that could be employed in the field test is a maximum value of inverters that could be retrofitted for Net2DG (by either adding a "Data Manager" which allows existing Fronius inverters to be connected to the internet, or replacing inverters of other manufacturers). Scenario 2 was scaled using the same penetration of inverters/Fronius inverters as already in the field in the Denmark test region. Scenario 3 is based on the averaged inverter penetration between the Danish and the German test region.

Table 30: Data volume estimation for Fronius Modbus interface

Scenario	Number of PV systems	percentage of PV systems in relation to households	Current number of Fronius inverters / after possible retrofitting measures	percentage of current / possible Fronius inverters in relation to households	worst case data volume per day
Scenario 1.1: 100 Households (Landau field test)	22 *information from Landau	22%	6 / 10	6% / 10%	3.5MB
Scenario 1.2a: 200 households (reduced TME field test)	23 *information from TME	11.5%	3 / 10	1.5% / 5%	3.5MB
Scenario 1.2b: 2000 households (full TME field test)	230 *scaled	11.5%	30 *scaled	1.5%	10.5MB
Scenario 2: 50000 households (full TME grid)	5750 *scaled	11.5%	750 *scaled	1.5%	263MB
Scenario 3:	83750	16.8%	18750	3.8%	6.6GB

Scenario	Number of PV systems	percentage of PV systems in relation to households	Current number of Fronius inverters / after possible retrofitting measures	percentage of current / possible Fronius inverters in relation to households	worst case data volume per day
5e5 households	*scaled		*scaled		

4.3 Inverter Web HE to ICT GW

Since the server-level interface that will be used for Net2DG is still under development, there are no exemplary data requests yet that can be used as a reference for a data volume analysis. However, the overhead in the IEEE 2030.5 protocol seems to be significantly higher. Therefore, the double amount of data volume compared to the local Modbus interface can be used as an estimation.

4.4 Mobile PQ to RTU Interface

Currently, Thy-Mors Energi possesses 2 Mobile PQ devices. However, it is assumed that there will be at most 5 devices available. Since a communication interface does not exist in the available devices (i.e. no transmission/reception of measurements/requests), an interface first needs to be created before the designed RTU is able to access the required information. Therefore, several issues/requirements need to be addressed/fulfilled. For instance:

- The actual size of measurements data needs to be confirmed.
- It should be decided how many times the measurement data needs to be fetched from each M-PQ device.

The measured information can be accessed after the data has been logged for “x” seconds/minutes depending on the type of data logging mechanism. Therefore, the sampling has to be stopped while transmitting to the RTU.

The transmission of measured data is expected to take place in the form of bursts. The process of sampling the measured data and its transmission will take the form of a square signal pattern, where the period of this square pattern is configurable via RTU, i.e.

- Time to sample data
- Time to transmit data

The configuration of this pattern (sampling + transmitting) depends on the way traffic is generated, as it has a large impact on our analysis. For instance, it does matter if there is a burst of data of “x” Megabytes or burst of data transmission for “y” seconds/minutes. As stated in Section 3.5, measuring and monitoring PQ parameters require several calculations, i.e. RMS values of voltage and current, etc. Depending on the type of parameter measured, calculations are performed using samples of monitored waveforms or using every sample cycle for quick disturbance detection. These calculations/measurements are available in four different formats i.e.:

- Screens – contain all screen snapshots not associated with a mini report
- Reports – contain the Mini Reports

- Setups – contain the Setup files
- Archive – contains the ddbx data folders

At this stage, it is assumed that it is possible to obtain each individual measurement that from the M-PQ device, e.g. RMS values of voltage and current. Further, assuming that each individual measurement is described by a double value, takes up 8 bytes of memory, with an addition of a unit value of 8 bits (char or unsigned byte). Thus, the raw data will take up 2x3 data elements of each 9 bytes that equals 54 bytes. Now, since there are several overheads attached to the raw data, the following assumptions are made:

- Application layer overhead = 50% of the raw data (i.e. 27 bytes)
- Overheads from L3 to lower layers = 63 bytes (see Section 4.5)

This gives a total of ~144 bytes per measurement.
The calculation of total bytes (B_{Total}) can be expressed via (1) as:

$$B_{total} = (N * 3 * (8 + U) + M)\left(1 + OH_{App}\right) + OH_{L_{1-3}} \quad (1)$$

Here,

- N → number of required measurements, where 3 represents a measurement for a 3-phase system and 8 is for double into bytes (this could be an integer, but assumed to be double value here)
- U → a unit value (assumed to be one byte/char in the above example)
- M → Meta data
- OH_{App}: OH of the application layer protocol, which is assumed to be 50% (thus, 1 + OH_{App} = 1.5)
- OH_{L1-3}: OH from L3 and lower layer protocols

The above calculation is done for a case where only one voltage (or current) measurement is transmitted. Since the measured data from M-PQ device will not be sent frequently, so as a rough estimation:

- Worst case: 144 Bytes are sent ten times a day per M-PQ device (0.5 per hour) i.e. 60 Bytes/hour
- Average case: 144 Bytes are sent twice a day per M-PQ device (0.1 per hour) i.e. 12 Bytes/hour

Now considering a case when all measurements (in all formats, as ascertained above) are being sent together, let's assume a payload of 10 kB. Then the following traffic volumes per hour result from the linear scaling of the number of M-PQ devices:

Table 31: Data traffic volume from M-PQ device

Scenario	Number of times data is transferred per hour	Total Volume of payload per hour
1 M-PQ device	0.5	4.2 kB
	0.1	~ 1 kB
2 M-PQ devices	0.5	8.4 kB

	0.1	2 kB
10 M-PQ devices	0.5	42 kB
	0.1	10 kB
100 M-PQ devices	0.5	420 kB
	0.1	100 kB

4.5 Stationary PQ (Janitza Device) Interface

The interfacing to the stationary PQ measurement devices of type Janitza requires inspection at different interface points:

Interface device to RTU: The interface from the device towards the RTU is implemented in the Janitza device and will be operated by a Raspberry Pi that is locally connected to the device.

Table 32 shows how many bytes each protocol level adds up to a packet exchanged between the RTU and Janitza device. In general, three packets are exchanged for a request-based measurement data access: (1) RTU sends the request, (2) Janitza sends the response, and (3) RTU sends an acknowledgement.

The example below is derived from an experiment in which the RTU requests a voltage reading from one Janitza device for only one phases L1. Moreover, it requested value of type short and received value represented by 2 bytes.

The observed payload sizes can be utilized to calculate the data volume on all phases and also for other measures, e.g., current, power, etc.

Table 32: Number of bytes each protocol level adds up to a packet

Direction	Protocol level			
	IP – size [B]	TCP – size [B]	Modbus – size [B]	Packet size [B]
PC → Jan (REQ)	20	32	12	64
Jan → PC (RES)	20	32	11	63
PC → Jan (ACK)	20	32	0	52

A high-volume measurement scenario would look as follows:

- The RTU accesses the Janitza device every 5 seconds: rationale for this high frequency of access is that the RTU will derive events such as voltage crossings based on the accessed values. The interaction with the Head-end and subsequently with the ICT Gateway will be much less frequent, i.e. on a 15min time-scale.
- The RTU requests 10 measurands (3 voltages, 3 currents, 4 others) and for each max, min, mean, so in total 30 values.

If all these 30 values are requested individually, then there is a total volume of 30*179B=5.370B transferred every 5 seconds, which results in 1.074 B/s ≈ 8,4kb/s per Janitza device on the local connection between RTU and device.

Data volumes on interface RTUs to HeadEnd and HeadEnd to ICT Gateway:

We assume 10 Janitza devices in a single LV grid area (behind a single secondary substation) in the field tests, so one Janitza device for approximately 100 customers. For larger grids, the assumption is reduced to 2 Janitza devices per 100 customers.
As the RTU will be aggregating values to 15min intervals, the data volumes per RTU in the communication to the Gateway can be assumed to be about 5kB (same order of size as above) per 15min interval. This results in the following data volumes per hour for the different grid sizes:

Table 33: Data volume per hour for different grid sizes

Size of Grid	100 cust.	2000 cust.	50000 cust	0.5 Mio cust.
Number of Janitza devices	10	200	1000	10.000
Resulting traffic volumes per hour	50 kB	1MB	5MB	50MB

Even though the Head-end to Gateway connection may further aggregate data more efficiently, we for now assume as upper limit the same data volumes on the HE-IGW connection as in the table above.

4.6 Streetlight to RTU Interface

The current field test area of Stadtwerke Landau has about 80 households and about the same number of street lights. Therefore, it is assumed for this approximate estimation that the number of street lights is equal to the number of households. However, there will always be groups of connected street lights activated, so the number of actuation units is assumed to be 10 per 100 grid customers.

Street light activation however will not be done frequently, so for a first rough estimation, it is estimated: Average case 1 activation/deactivation commands per day per street light actuation RTU.

Assuming that the HeadEnd sends ‘Are you Alive’ probing requests to every street light actuation RTU every hour, and assuming that both a probing and activation/deactivation method will consume a Layer-3 payload of 500 bytes, the following traffic volumes per hour result from the linear scaling with the number of street lights equalling number of households:

Table 34: Data traffic volumes per hour with different number of street lights

Scenario	Number of Street Lights Actuation units	Number of Probing Messages on HE-RTU interface per hour	Avg. Number of activation/deactivation Messages per hour (on IGW-HE and on HE-RTU interfaces)	Total Volume of L3 payload per hour (500 Bytes per Message) on HE-RTU interface	Total Volume of L3 payload per hour on IGW-HE interface
Scenario 1.1: 100 Households	10	10	0.42	5.5kB	0.2 kB
Scenario 1.2: 2000 households	200	200	8.3	104kB	4kB
Scenario 2: 50000 Households	5000	5000	208	2.5MB	100kB
Scenario 3: 5e5 households	50000	50000	2000	25 MB	1MB

For the required data rates, as it can be seen most modern communication technology will be able to provide this data rate. Due to the distribution of the lights, cellular networks may be a good option, depending on the interface cost. In that case, though, coverage may be an issue in some places, but would be expected to be a minor issue since lightings systems are normally installed in city areas which usually have good connectivity.

4.7 Grid Topology to Grid Topology HE Interface

As the grid topology subsystem is specific to the individual DSOs, the two different DSO subsystems are analysed separately in the following subsections.

4.7.1 TME Grid Topology

The size of the file that results from the export of the field trial area is 495 MB. Linear scaling leads to the following total data volumes that are accessed during one update of the grid representation (see Table 35):

Table 35: Data volumes for TME grid topology with different number of households

Scenario	Topology data representation: Total file size	Throughput requirement for update to be finished within 1 hour	Throughput requirement for update to be finished within 1 min	Throughput requirement for update to be finished within 1 sec
Scenario 1.1: 100 Households	0.99MB	0.275 kB/s	16.5 kB/s	990 kB/s
Scenario 1.2: 2000 households	19.8MB	5.5 kB/s	330 kB/s	19.8 MB/s
Scenario 2: 50000 Households	495 MB	137.5 KBytes/s	8.25 MB/s	495 MB/s

For the TME case it is hardly realistic to exchange the full set of grid topology data within second, however, considering the possibility for the full grid topology being exported only once with no or only little time constraints (even 2 hrs. and more would be acceptable as a first time). Once the huge topology set has been exchanged, only differences will be exchanged, makes the scenario with order of 100 households most realistic in a day to day operation. If the network provides at minimum in the order of 100 kB/s data rate, this seems fair to support a “realtime” operation of the grid topology subsystem. Most modern Ethernet based infrastructure offers more than enough capacity to ensure this data rate, and externally TME is connected with Fiber, so capacity is not expected to be an issue. This is also considering that data is not a continuous stream, but rather a burst for a well known duration.

4.7.2 Landau Grid Topology

The sizes of the files that result from the export of the field trial area (LV grid behind single trafo at secondary substation) are shown in the following Table 36.

Table 36: Size of files resulting from the export of the field trial area

Landau file	Size [kB]
House connections	9.9
Photovoltaics	4.3
Substations	0.46
Junction boxes	2.5
Cables	19.4
Sleeves	0.77

This results in a total data volume of ca. 37.5 kB for the field trial region Scenario 1.1, and linear scaling leads to the following total data volumes that are accessed during one update of the grid representation (see Table 37):

Table 37: Data volumes for Landau grid topology with different number of households

Scenario	Topology data representation: Total file size	Throughput requirement for update to be finished within 1 hour	Throughput requirement for update to be finished within 1 min	Throughput requirement for update to be finished within 1 sec
Scenario 1.1: 100 Households	37.5 kB	11 Bytes/s	0.625 kB/s	37.5 kB/s
Scenario 1.2: 2000 households	750 kB	220 B/s	12.5kB/s	750 kB/s
Scenario 2: 50000 Households	18.75 MB	5.5 kB/s	312.5 kB/s	18.75MB/s = 150Mb/s

Similar to the TME case, the data rates and communication technology required for this is achievable, as long it is not expected to be able to transfer the largest set over very short time interval, i.e. scenario 2 within one second. Similarly, the full topology is expected to be transferred into an initial state, followed by only updates of smaller sizes, more resembling case 1.1 as a worst case. However, it appears the requirement is less, and reasonable results should be expected if the network can accommodate in the order of 15 kB/sec., which most modern communication networks offers.

4.8 Complete Analysis of Data Volume on interfaces of ICT Gateway

This section aims to collect all the previous analysis of each subsystem, in order to provide an estimate of the various cases at a full system scale level. Since there are different setups and subsystems at the two DSOs, the analysis is reflecting this by doing one analysis next to the other one (see Table 38). All data are per day, and all are approximate values.

Table 38: Estimation of total data volume for the various cases at full system scale level

Case	AMI	Inverter web	Inverter modbus	Stationary PQ	Streetlight	Grid topology	Total
1.1	382kB	7MB	3.5MB	50kB	4.8kB	37.5kB	11MB
1.2	7.6MB	21MB	10.5MB	1MB	96kB	22.5MB	62.7MB
2 (Land)	191MB	526MB	263MB	5MB	2.4MB	18.75MB	1GB
2 (TME)	191MB	526MB	263MB	5MB	2.4MB	0.5GB	1.5GB
3 (Land)	1.9GB	7.8GB	3.9GB	50MB	24MB	187.5MB	13.9GB

3 (TME)	1.9GB	7.8GB	3.9GB	50MB	24MB	5GB	18.7GB

For Case 1.1 and Case 1.2 the traffic expected by these rough estimates, are acceptable and manageable, but still quite high on a daily basis. As a continuous data stream, there should be absolutely no issues in collecting the data, as this amount in average would require for the worst case approximately 130 B/sec. of efficient data transfer (~1 kbit/sec without protocol overhead).

Considering the Net2DG system will need to be running all time, preferable without breaks or interruptions, the accumulated amount of data will quickly grow in particular if historical data for months should be visible. Even for the best and most optimistic case, a month of history would mean nearly 0.35 – 1.9 GB of data, so data scalability in cases with historical data analysis can easily become an issue even for the smaller setup.

Case two, which aims towards a more realistic small setup, the data volume becomes even more visible. If data is arriving in a continuous stream, the required data rate would be for the worst case in the order of 17kB/sec, which is easily achievable with today's communication technologies (~136kbit/sec without protocol overhead). The problem starts to arise here with the scalability of the long term storage. For storage and processing this case yields for a month 30-45GB of data. Although hard drives are cheap, doing operations on such large data sets e.g. sorting or searching will pose a challenge, so thoughts into planning data storage will be important for the project.

Case three illustrates the worst case with 500.000 households/devices in the field. This yields for the worst case a requirement of data rates around of 216kB/sec (~1.7 Mbit/sec without protocol overhead), which seems also to be fair. If data arrives in bursts, though, it might be a problem to transfer all data in near real time.
Again here, the issue is not the data rate, but rather post processing of large amounts of data which for a month of data in best case runs into the order of 0.4TB of data and worst 0.6TB of data. While storage may be cheap, performing analysis of this amount of data is clearly something that needs to be considered seriously in the design and implementation. In particular if years of data should be stored and post processed.

In summary to the analysis, it is clear that the apparent data rate most modern communication technologies can provide yields no huge issue, considering data does not arrive in bursts. However, the large data volume over time leads to potential issues for doing certain post processing operation on the data sets, which clearly needs to be considered in the final design. For the field tests these may be doable, but even here care must be taken such that operations and analysis will not take hours. In particular, if long term historical data is stored remotely and needs to be accessed via the ICT Gateway before processing at the application level, care must be taken to include filtering so that the gateway does not suddenly require the download or upload of a terabyte file each time the operator wishes to search data. One proposal is to include a storage adapter/storage HES to allow flexible and efficient search queries. Such solutions can easily be adopted into the existing design, however, for the first

version of the ICT GW this is not in scope. Later versions may include advanced functionality to detect and store data features instead of the raw data, for really long term data management, as storage capacity requirements will explode the overall costs of a system that can support large DSO's.

4.9 Initial Connectivity and Planned Performance Measurements for the Field Tests

The basic ICT architecture for the field trials in the grids of StwLan and TME has been described in D1.2, Chapter 10 [1]. In order to early become aware of constraints and performance limitations in the actual deployment, the following tests are planned for early execution in the field-trial deployments:

- Use ICMP Ping messages to check for reachability and for initial characterizations of round-trip time delays and message losses
    - Procedure:
        - Configure machines and firewalls
        - Start ping applications for all communication pairs as stated bold-faced in the table below
        - If connectivity is confirmed, then restart with another 5000 ping measurements and record round-trip times and fraction of lost messages
- After the basic connectivity measurements, an existing network performance measurement tool, iperf (https://sourceforge.net/projects/iperf/), will be used to record the following
    - Minimum, average and maximum TCP throughput
    - Minimum, average and maximum UDP throughput

  Minimum, average and maximum are thereby obtained from at least 10 repetitions of the measurement.
- Perform signal strength measurements for cellular networks in remote locations that are intended to be connected via cellular networks, in particular the secondary substation of the field test and selected junction boxes.

Purpose of the tests above is to identify feasible ranges and expected performance behaviour early for the end-2-end connection, in particular:

- To verify that communication between entities is possible and that there are no 'extreme' end-to-end performance characteristics (i.e. that ping RTT delays are below 1 second, except when 2G links are present, then up to few seconds).
- To use the throughput measurements to verify that the data volume estimates derived in the previous sections are actually feasible to be carried across to the end-to-end connections.

Note that measurements of connection availability (up and down times) are not planned in this initial step, but may be done later in 2019.

For the very first deployment, the ICT GW and all HeadEnd servers at DSO sites will be operated on virtual machines on the same physical machine. A very first measurement of the local communication on a Windows 10 machine using Ubuntu VMs lead to achievable throughput in the range of 190-650

Mbit/s. Obviously, this value will mainly depend on the processing power of the used machine and on configurations of the operating system. A detailed analysis of the latter is not necessary at this stage, but our main conclusion is that a few hundred Mbit/s is the realistic throughput range for internal communication on sockets between VMs.

The external communication to remote HeadEnds in the field trials will be performed via Internet connections with connection throughput between 50Mbit/s and 1Gbit/s. Be aware these are the raw bit rates at Layer 1, while the data rates discussed in Section 4.8 are data rates at Layer 3-7.

5 Initial ICT Gateway Design/Architecture

5.1 Gateway Core

This section introduces the core functionalities that will be provided by the ICT Gateway to the other components in the system. Core functionalities are captured inside different modules that are reflected in Figure 4, while Figure 3 shows a high-level view of the ICT Gateway architecture.

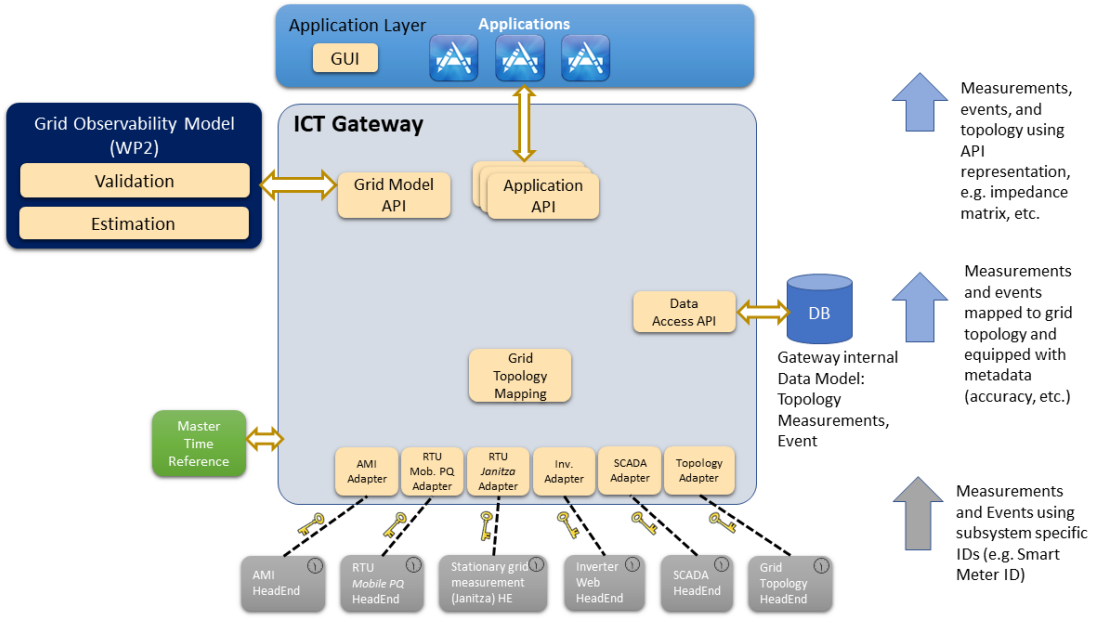

Figure 3: High Level View of the ICT Gateway Architecture

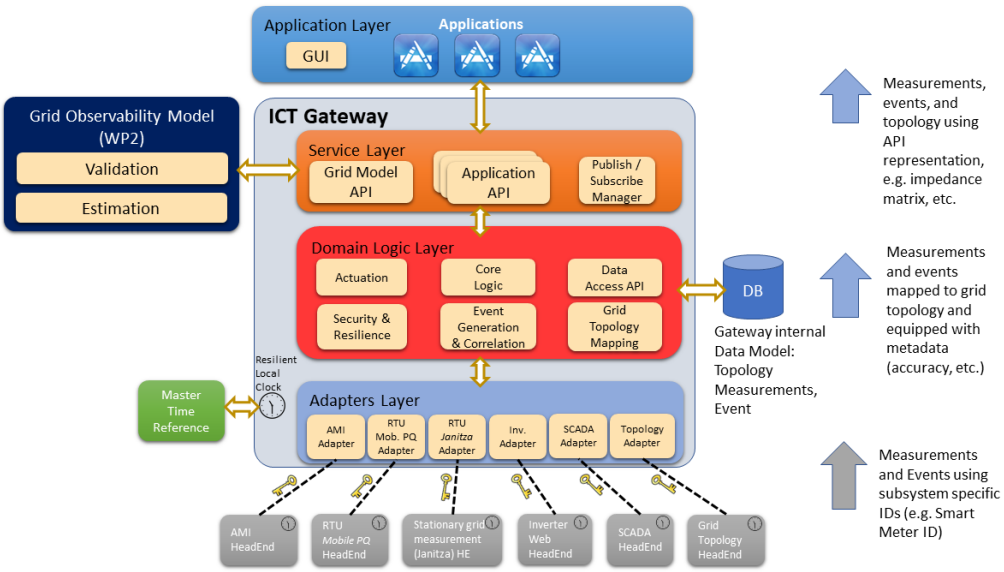

Figure 4: ICT Gateway Architecture

The following are the main building blocks of the ICT Gateway divided into different application layers:

- **Service Layer in ICT Gateway**
- **Domain Logic Layer in ICT Gateway**
- **Adapters Layer in ICT Gateway**
- **Application Layer**

Service Layer in ICT Gateway encompasses the following modules:

- **Grid Model API**
  - Triggers validation and estimation from the Grid Model.
  - Specifies how the ICT Gateway can communicate with the Grid Model.
  - Provides an endpoint where the Grid Model can publish results of validation and estimation.
- **Application API**
  - Allows applications to issue a query in order to retrieve particular data from a HeadEnd.
- **Publish / Subscribe Manager**
  - Supports publish/subscribe and request/reply communication paradigms.
  - Allows applications to subscribe on particular information, i.e., specific data types or events.

Domain Logic layer in ICT Gateway encompasses the following modules:

- **Actuation**
  - Handles interactions with actuation subsystems (through HeadEnds), e.g., Inverter-systems, Load Activation, Generation curtailment, and OLTC.
- **Security & Resilience**
  - Fault and Attack detection mechanisms, functions and controls implemented to provide security, resilience and robustness (towards, e.g., failing devices or lack of communication).
- **Core Logic**
  - Core business functions of the ICT Gateway, which acts as mediator between data sourcing and actuation subsystems and domain applications.
  - Communicates with the Grid Model through Grid Model API.
  - Uses validation and estimation capabilities of the Grid Model.
- **Event Generation and Correlation**
  - Generates events correlating multiple measurements.
- **Data Access API**
  - Provides access to data stored in the DB, according to the Gateway Internal Data Model (e.g., Topology Measurements, Events, Metadata).
- **Grid Topology Mapping**
  - Identifies the generator of an event/data and associates it with node id defined in the Grid Topology.
  - Enriches data with metadata available from the Grid Topology.

Adapters Layer encompasses the following modules:

- **AMI Adapter**
  - Connects the ICT Gateway to AMI HeadEnd System.
- **RTU Mob. PQ Adapter**
  - Connects the ICT Gateway to the RTU-HE.
- **RTU Janitza Adapter**
  - Connects the ICT Gateway to the RTU-HE specific for Janitza measurement devices.
- **Inv. Adapter**
  - Connects the ICT Gateway to the Inverter WEB HeadEnd.
- **SCADA Adapter**
  - Connects the ICT Gateway to the SCADA HeadEnd.
- **Topology Adapter**
  - Connects the ICT Gateway to the Grid Topology HeadEnd.

Application Layer encompasses the following modules:

- **GUI**
  - Provides input and output (mostly visualization) for all domain applications and for ICT Gateway functionalities of the Net2DG system.
  - Enables the interaction with the human operator on site.
- **Grid Outage Diagnosis**
  - Provides outage diagnostics capabilities and implements support for the outage diagnostics use-case.
- **Grid Efficiency**
  - Enables the deployment of measurements for loss reduction in the LV grid taking into account the specific dynamic behaviour of the LV grids.
- **Voltage Quality**
  - Allows a measurement-based detection and diagnosis of current voltage problems; includes voltage variation, voltage dip/sag, short and long voltage interruptions, voltage unbalance.

Besides the four layers described so far, the following are the other elements constituting the ICT Gateway Architecture or interacting with it:

- **Resilient Local Clock**
  - Each HE or subsystem has its own time (received from the server/subsystem it is attached to).
  - Implements a low-intrusive software clock in charge of synchronizing local times to a *Master Time Reference*, providing also a synchronisation uncertainty [30].
- **Data Base (DB)**
  - Stores the data models: measurements, events and grid topology. The data can be equipped with metadata, as well as subscriptions information.

Grid Observability Model

- Validation
  - Validation check of measured data (e.g., before pushing the information to applications which subscribed for it).
- Estimation

- Calculates missing information (e.g., estimating measurement values before pushing information to applications which subscribed for it).

5.2 ICT Gateway Internal Data Model

Before introducing the data model, it is provided a brief description of the naming conventions.

- Tables are written in upper camel case, as for example `GridElement` entities, with all the words starting with a capital letter and no intervening spaces or punctuation.
- Columns are in lowercase and separated by underscores, as for the `number_of_phases` attribute. An exception is constituted by the attributes containing names of entities, e.g., `GridElement_id`, where the entity is written following tables convention.
- Suffix `_id` is used for identifiers. Other examples of suffixes used are: `_size`, and `_present`.
- Data types, as `INT`, where already specified, follow the convention of mySQL keywords.

The object notation used in Figure 5, and Figure 6, is the MySQL Workbench default one. As can be seen in Figure 6:

- A primary key is indicated by a key icon;
- Indexed fields are indicated by a different colored diamond icon.
- Both primary keys and indexed fields are in red when indicates a foreign key.

The relationships in Figure 5 and Figure 6 are expressed in Crow's Foot diagramming convention technique:

- Continuous lines model identifying relationships;
- Dashed lines model non-identifying relationships

According to Crow's Foot notation, the cardinality of the relationships is:

- One and only one: equals symbol;
- One or many: crow's foot followed by a line.

Details regarding the meaning of relationships and cardinality are provided in the following.

5.2.1 Grid Topology

The hierarchical data model reflecting a grid topology is constituted of multiple tables, where each table corresponds to an entity in the grid topology. In particular, the entity at the top level is called `GridElement`, which indicates any element that can be found in the topology data model. Any `GridElement` can be either a `Cable` or a `GridNode`, as shown in Figure 5. Each record in `Cable` table is connected to two records in `GridNode` table, representing the start-node and the end-node respectively.

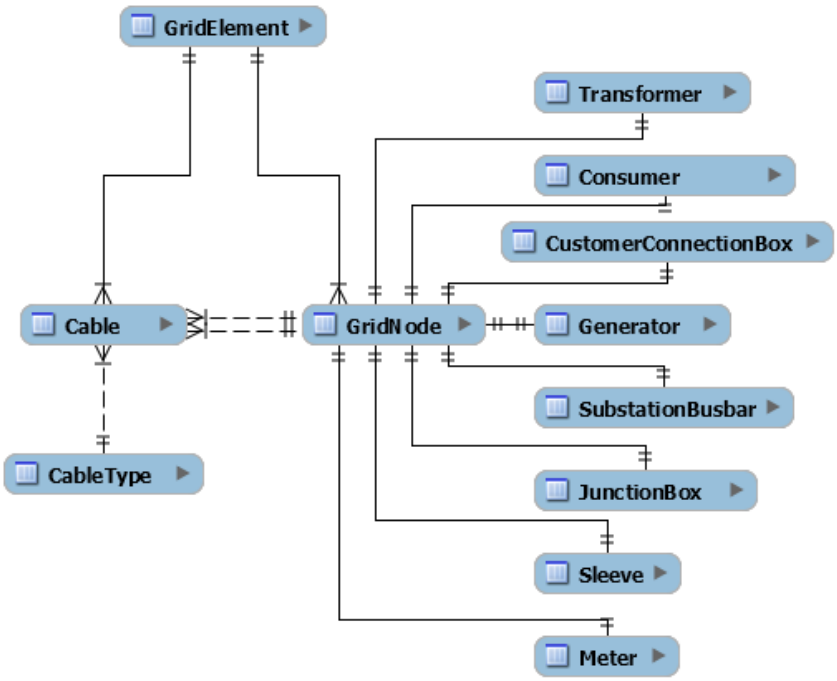

Figure 5: High Level View of the Grid Topology Data Model

Then, at the third level of the hierarchy, there are multiple entities child nodes of `GridNode`, each of them representing a different type of node on the grid:

- `Transformer`
- `Consumer`
- `CustomerConnectionBox`
- `Generator`
- `SubstationBusbar`
- `JunctionBox`
- `Sleeve`

`MeterAs` for the `GridNode` element, also the `Cable` entity possesses a child table, which is named `CableType` and specifies details not expressed in the parent entity. In the following, it is provided a detailed analysis of the characteristics of the elements in the grid topology data model. Figure 6 contains the entities listed above showing also their attributes, data types and relationships.

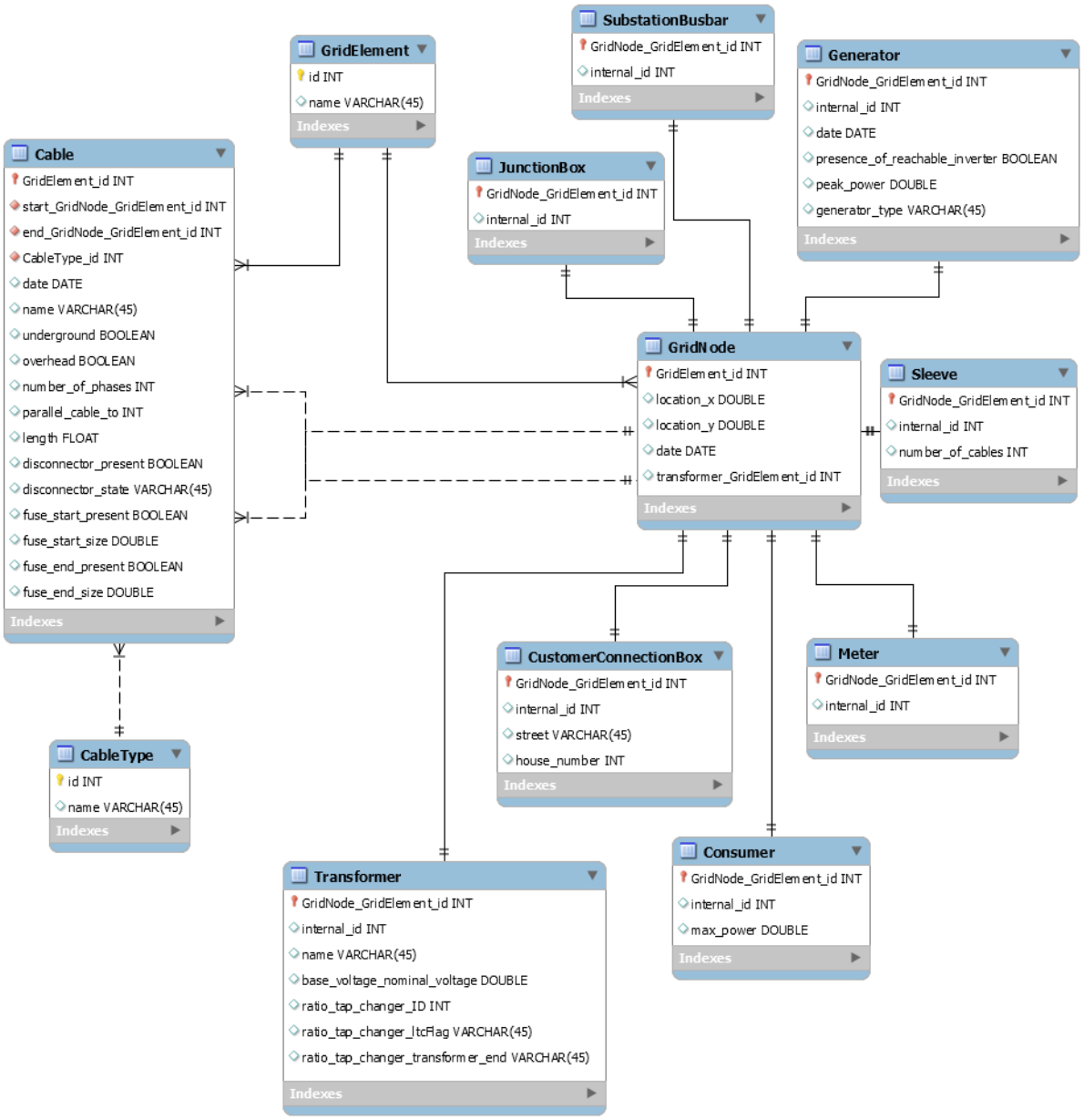

Figure 6: Detailed EER Diagram of the Grid Topology Hierarchical Data Model

Regarding the notation[2] in Figure 6, all the continuous lines express identifying relationships, where a child object cannot exist without the parent object. In fact, the primary key of the parent entity (e.g., id for `GridElement`) is the primary key of the child entity (`Cable` or `GridNode`), and the existence of a row in a child table depends on the existence of a corresponding row in a parent table.

On the other hand, dashed lines express non-identifying relationships: the primary key of the parent entity is included in the child entity but not as primary key. This is the case of `GridNode` and `Cable`: a `Cable` has `start_GridNode_GridElement_id`, and `end_GridNode_GridElement_id` attributes, but

[2] As discussed before, the so-called Crow's foot notation

they are not a primary key for a Cable, which instead is identified by its own GridElement_id. This makes sense, because between two GridNode there can be several Cable.

Regarding the cardinality of relationships: 1:1 is expressed by a means that a single instance of GridNode can only be one instance of its child nodes. And the opposite is valid too.
The 1:n cardinality of the relationship establishes that a single instance of GridNode can be a start_GridNode (or end_GridNode) of many Cable instances. While a single instance of Cable cannot have multiple start_GridNode (or end_GridNode). Other 1:n relationships exist between GridElement and its child tables, as well as between CableType and Cable entities.

The following tables provide further description of the entities in the grid topology data model and their attributes.

Table 39: Entity GridElement

Entity	Description	Attributes (column_name)	Data Type	Unit (optional)
GridElement	Element used on highest level; it can be either a Cable or a GridNode	id	INT	
		name	VARCHAR	

Table 40: Entity GridNode

Entity	Description	Attributes (column_name)	Data Type	Unit (optional)
GridNode	General grid node concept	GridElement_id	INT	
		location_x	DOUBLE	
		location_y	DOUBLE	
		date	DATE	
		transformer_GridElement_id	INT	

Table 41: Entity Cable

Entity	Description	Attributes (column_name)	Data Type	Unit (optional)
Cable	High level concept used for Cables. It is a wire or combination of wires, with consistent electrical characteristics, building a single electrical system, used to carry alternating current between points in the power system. Used	GridElement_id	INT	
		start_GridNode_GridElement_id	INT	
		end_GridNode_GridElement_id	INT	
		CableType_id	INT	
		date	DATE	
		name	VARCHAR	
		underground	BOOLEAN	
		overhead	BOOLEAN	
		number_of_phases	INT	
		parallel_cable_to	INT	

Entity	Description	Attributes (column_name)	Data Type	Unit (optional)
	for cables and overhead lines.	length	FLOAT	
		disconnector_present	BOOLEAN	
		disconnector_state	VARCHAR	
		fuse_start_present	BOOLEAN	
		fuse_start_size	DOUBLE	
		fuse_end_present	BOOLEAN	
		fuse_end_size	DOUBLE	

Table 42: Entity CableType

Entity	Description	Attributes (column_name)	Data Type	Unit (optional)
CableType	This entity will specify details not contained in the parent entity.	id	INT	
		name	VARCHAR	

Table 43: Entity Transformer

Entity	Description	Attributes (column_name)	Data Type	Unit (optional)
Transformer	An electrical device consisting of two or more coupled windings, with or without a magnetic core, for introducing mutual coupling between electric circuits. Transformers can be used to control voltage and phase shift (active power flow).	GridNode_GridElement_id	INT	
		internal_id	INT	
		name	VARCHAR	
		base_voltage_nominal_voltage	DOUBLE	
		ratio_tap_changer_id	INT	
		ratio_tap_changer_ltcFlag	VARCHAR	
		ratio_tap_changer_transformer_end	VARCHAR	

Table 44: Entity Consumer

Entity	Description	Attributes (column_name)	Data Type	Unit (optional)
Consumer	The customer of the DSO and the final consumer of energy	GridNode_GridElement_id	INT	

	delivered via the distribution grid. Can be a household, an SME, a large industry, etc.	internal_id	INT	
		max_power	DOUBLE	W

Table 45: Entity CustomerConnectionBox

Entity	Description	Attributes (column_name)	Data Type	Unit (optional)
CustomerConnectionBox	Type of box that serves as secure and protection environment for electrical wires at customer premises	GridNode_GridElement_id	INT	
		internal_id	INT	
		street	VARCHAR	
		house_number	INT	

Table 46: Entity Generator

Entity	Description	Attributes (column_name)	Data Type	Unit (optional)
Generator	Machine that transforms mechanical power into electric power	GridNode_GridElement_id	INT	
		internal_id	INT	
		date	DATE	
		presence_of_reachable_inverter	BOOLEAN	
		peak_power	DOUBLE	W
		generator_type	VARCHAR	

Table 47: Entity Meter

Entity	Description	Attributes (column_name)	Data Type	Unit (optional)
Meter	Generic entity representing measurement devices (e.g., smart meters)	GridNode_GridElement_id	INT	
		internal_id	INT	

Table 48: Entity Sleeve

Entity	Description	Attributes (column_name)	Data Type	Unit (optional)
Sleeve	Connects multiple cables (in most cases 2, sometimes 3).	GridNode_GridElement_id	INT	
		internal_id	INT	
		number_of_cables	INT	

Table 49: Entity SubstationBusbar

Entity	Description	Attributes (column_name)	Data Type	Unit (optional)
SubstationBusbar	A conductor, or group of conductors, that serves to connect other conducting equipment within a single substation.	GridNode_GridElement_id	INT	
		internal_id	INT	

Table 50: Entity JunctionBox

Entity	Description	Attributes (column_name)	Data Type	Unit (optional)
JunctionBox	Type of box that serves as secure and protection environment for electrical wires where they connect before moving on.	GridNode_GridElement_id	INT	
		internal_id	INT	

When an application requests a topology from the ICT Gateway, it can specify whether is it interested in: 1) obtaining the whole topology, 2) a single GridNode (and implicitly all nodes below that one), or 3) all the nodes within a geographic rectangular region.

In any case, a response consists of the following:

- List of GridNode entities:
  <GridNode_GridElement_id, GridNode entity type, [optional attributes of entity, …]>
- List of Cable entities:
  <Cable_GridElement_id,
  start_GridNode_GridElement_id,
  end_GridNode_GridElement_id,
  [optional attributes: CableType_id, length, …]>

Finally, an application can also request measurements and events produced by or related to a GridElement_id.

5.2.2 Measurements

The main focus of a data model that reflects measurements is to associate this information with the respective source. Consequently, measurements will be captured in a specific data model, but coupled with the related GridElement_id. It has to be noticed that in our data model not only a GridNode can produce measurements, but also a Cable, and this is why the association is made with the entity at the highest level. Moreover, in some cases a measurand (e.g., current, and power) can be produced by both the GridElement entities: the measurand entity possesses two GridElement_id attributes[3].

[3] Further details are in Annex E

Together with a `GridElement_id` of the node/cable that produced the measurements, all entities will have an associated `measurement_id` and a `timestamp`. Other attributes will depend on the type of measurand.

When an application is interested in specific measurement, it can obtain them either by subscribing to data or by making a data request. In any case, the application has to provide the following parameters:

- List of GridElement_id
- Time-interval of interest (which can be correlated to `timestamp` attributes)

For example, a request could be for all available measurements from a `GridElement` that have been taken within a specific time-interval.

The reply/notify contains in both cases:

- List of <`GridElement_id`, `measurement_id`, `timestamp`, `measurement`, [unit, accuracy, metadata], [`measurement_id`, …]]>.

In Annex E all the measurands foreseen so far has been described, showing - where applicable - their attributes, source and related Net2DG applications.

5.2.3 Events

As for measurements, also the events will be captured in a specific data model. Each event contains the following elements:

- Event creator
  - `GridElement_id`
  - `event_id`
  - `timestamp`

Examples of event categories are:

- Parameter exceeds thresholds (e.g. voltage measurement exceeds threshold)
- New measurement data available
- Non-reachability of measurement device
- Shut down of component

In Annex E, together with the measurands, the events foreseen so far and their attributes, source and related Net2DG applications are described.
Further event attributes will be identified later. Some events may be created by the ICT Gateway or any subsystem based on correlating multiple measurements.

5.3 API Design to the Net2DG Applications

Generally, the prototype applications that are developed in WP2 in parallel require the following types of data: Grid Topology, voltages/currents/power/energy at certain grid points, and ICT reachability of measurement nodes. See D2.1 Chapter 5 [31] for a detailed list.
For the interfaces to the applications and to the grid observability model, the following two levels of interface implementation will be made available:

- In order to allow rapid prototyping of new application variants, the prototype applications and the grid observability model can issue direct SQL queries to the internal database of the ICT Gateway. This direct SQL interface gives full flexibility to the applications and grid observability model. Due to the undesired dependence on the data format in the internal DB of the ICT Gateway, this interface is expected to be disabled when the applications and the higher-level API design have reached maturity.

- In order to be independent of the ICT gateway internal DB format, the API will also provide interface functions that translate the data to different, commonly required formats. The design of the second type of interface functions will evolve with the application evolution and the grid model evolution.

In the following, some example interface functions for different types of data access corresponding to needs of selected application designs from D2.1 [31] are described. It is worth to point out, in this initial phase, that the APIs are defined on high-level without specifying all parameters and functions. However, specified APIs will be refined and extended in Task 3.2 based on the first specification of algorithms for grid estimation and for the three observability applications, provided in D2.1 [31]. Moreover, APIs will adapt and evolve together with the prototype applications.

5.3.1 Access to Grid Topology

According to the data model described in Section 5.2, the following terms are used in the text:

- 'Node' is anything that is placed at any cable end, specifically it can be a substation, junction box, sleeve, CustomerConnectionBox, etc., see Section 5.2.

- A Fuse and Circuit Interruption is however not a node but rather a cable attribute ('there is a fuse at the beginning or end of the cable').

- An element can be either a node or a cable.

In order to provide a compact representation of topologies of sub grids of the LV grid, the following functions are provided:

Table 51: Grid Topology API

Grid Topology API	
	listAllTopologies
Call	GET Request
Response	List with topology IDs and metadata for each topology

Description	Returns all topologies maintained by ICT Gateway but without any nodes and cables.
	listAllElementsInTopology
Call	Get Request + parameter: topology ID
Response	List with all element types and corresponding element IDs
Description	Does not return details for each element, but just lists with IDs
	getElementDetails
Call	Get Request + parameters: topology ID + element type + element ID
Response	Get all information for a specific element in the grid topology
Description	Returns all information for a specific element in the grid topology
	getAllSubElements
Call	Get Request + parameters: topology ID + node ID
Response	List with all elements underneath the specified node ID
Description	For provided node ID, return all sub elements, i.e., nodes and cables
	getMatrix
Call	Get Request + parameters: topology ID + node ID (SubstationID or SubstationFeederID or JunctionBoxID) + matrix type (resistance, impedance)
Response	resistance matrix R or impedance matrix Y
Description	Numerically enumerate all relevant nodes (substation, junction box, sleeve, Houseconnection, HCwithPV, ...) 'below' the requested node/feeder with sequential ids resulting in Range 1...N, requested substation/junctionbox thereby is assigned internal ID=1. Assemble the R (and Y, etc.) as NxN matrix for this type of enumeration. Return also the node types and a list of node attributes. The optional return parameter of fuse representation matrix is a non-symmetric NxN matrix, where f_ij=a if and only if there is a fuse at the beginning of cable i-->j with size (max current) a.

Listed functions reflect initial API used by prototype applications, i.e., Grid Outage Detection and Loss Minimization. When observing call parameters for a function, it shall be possible to infer which function provides those parameters as an output, e.g., to list all elements in topology, it is required to provide topologyID which can be obtained from a list of all topologyIDs maintained in ICG.

High-level API function design:

- Determine all relevant nodes (nodes are substations or junction boxes or sleeves or household-connections or generators without households, or other types of future nodes)
- Make sequential enumeration to attach a numerical node id in the range 1...N with Id1 assigned to the requested 'root' node

- Create output matrices and matrices via DB requests and post-processing

Further aspects to be discussed for inclusion in future versions:

- Uncertainties of cable parameters: Instead of single R matrix, it may be given as a matrix with Rmin and Rmax values to allow to represent ranges of values,
- Uncertainties of node parameters: to be reflected in attributes, e.g. PV max generation can be a range,
- Uncertainties of topology (there may be a cable, but maybe not): possibly return multiple R matrices with different entry placements and an assigned likelihood

In addition to the functions above, there may also be specific interface functions to create topology formats for specific tools that are used by applications or the grid observability model. These will be determined when the WP2 decision on any used tools is stable (D2.1 [31]).

5.3.2 Access to ICT Reachability Information for Specified Grid Nodes

Table 52: ICT Reachability API

ICT Reachability API	
	getICTReachabilityStatus
Call	GET Request + parameters: topology ID + set of node IDs + doActiveProbing
Response	For each grid node ID, a data structure with following elements is returned - Number of measurement devices at the node: 0,1,… - Latest Timestamp that a message was received from any measurement device at that grid node - AdhocRequestIssued: values: 0=no active request possible at this grid node; -1=active request(s) issued but timed out; 1=active request was issued and succeeded at latest timestamp; 2= active request could be possible, but last successful communication was too recent to make it worth issuing an active request.
Description	• Used by Outage Detection (Odet) application, Outage Diagnosis (Odiag) application • Determine whether there is at least one reachable measurement device at a certain grid node • The ICT Gateway will check what is the highest timestamp of a successful message reception from any measurement device at that grid point. If the corresponding entry in DoActiveProving is non-zero, then the ICT Gateway will try to probe the grid point via all capable measurement devices and wait for a reply until a subsystem specific timeout.

High-level API function design:

- SQL request to determine all relevant measurement devices
- SQL request to determine latest time stamp of message exchanges

Further aspects to be discussed for inclusion in future versions:

- If a node is not reachable, ICT Gateway can generate an alarm and make an application aware of it.

5.3.3 Access to Voltage Measurements in Specified Grid Nodes

Although the table below shows the API that an application utilizes to retrieve voltage measurements from different nodes in a grid topology, the same API can be easily adapted for access to current, power and energy measurements.

Table 53: Voltage Measurements API

Voltage Measurements API	
	subscribeToData
Call	POST Request + parameters: measurement type (voltage, current, etc.) + topology ID + set of node IDs + timeInterval
Response	Subscription confirmation with subscription ID
Description	• Returns subscription ID which has to be provided to unsubscribe • Can be uniform for any type of subscription, e.g., from power measurements to the generated events
	unsubscribe
Call	DELETE Request + parameter: subscription ID
Response	Confirmation that the corresponding subscription is cancelled
Description	Stops pushing data to a registered application
	getVoltages
Call	Get Request + parameters: topology ID + set of node IDs + useGridModel + timeInterval
Response	For each grid node ID, a data structure with the following elements is returned • Average voltage [V], standard deviation [V] • Max voltage [V], Min voltage [V]
Description	• LC application, GMon application, AVR application

	• The ICT Gateway will check for each grid node if there is a corresponding voltage measurement for the given time interval. If UseGridModel<>0 then the ICT Gateway will call the GridModel to improve or extrapolate the voltage value using all measurements in the corresponding feeder. • GridModelUsed: values: 1 = single measurement source was available and no need to call grid model; -1=no measurement data available and grid model could not be used due to insufficient input; 2=Grid model was used to correct set of existing measurements; 3=no measurement available and grid model was successfully used

As it was already pointed out in D1.2 Section 8.5.1 [1], the connection between applications and ICT Gateway will be realized by means of WebSockets. Therefore, it is necessary to define the messages, i.e., a protocol, that will be exchanged between the two types of entities and that will support the API methods defined in the table above.

High-level API function design:

- SQL request to determine all relevant measurement devices
- SQL request to determine relevant voltage values
- If UseGridModel<>0, get topology of the feeder and all available other measurements for this feeder to call grid observability model
- A request can be propagated to an adapter which forwards it to a corresponding HeadEnd system

Further aspects to be discussed for inclusion in future versions:

- Extend API with filtering parameters that will be based on the outcome of D2.1 [31]

5.3.4 Auxiliary Interfaces

- Access to currents/power/energy in specified lines
- Access to certain selected event types in parts of the LV grid (more to come later, e.g. THD, presence of fuses/breakers)
- Write back results to the ICT Gateway
  - Outage events
  - Voltage profiles
  - More depending on WP2 applications
- Actuation and modification set points

See also Section 8.5.1 in D1.2 [1] for general WebSocket interface design for registrations of applications and subscriptions to data and events.

5.4 Gateway Adapters

This section introduces general design directions that will be addressed by all adapters running inside the ICT Gateway. Consequently, the figure below reflects the generic adapter architecture. Similar to the ICT Gateway, the adapter architecture follows a layered approach where different modules reside on different layers.

The following modules constitute a generic adapter, while some other optional modules may be included in a specific HeadEnd system.

- **Adapter API**
  - Upon successful registration of a subsystem, the Adapter API is used to forward the registration data to the ICT Gateway, and in particular to the Core Logic (see Figure 4).
  - It also receives application requests coming from the ICT Gateway.
- **Processing & Management**
  - Main role: to ensure the ICT Gateway is able to communicate with the appropriate protocol for the specific subsystem.
  - Periodically retrieves parsed data from a HeadEnd system.
  - If a certain subsystem does not support push of data and events, this module of the adapter should implement the functionality on its behalf.
  - Once the data is formatted, it pushes it to the ICT Gateway.
- **Format Translation**
  - Normalize the data retrieved from a HeadEnd system to a unique format (the same for all the adapters)
- **Authentication and Registration**
  - Specifies the registration protocol and message types that have to be exchanged between an adapter and a HeadEnd.
  - Provides functionalities for identity-based authentication and data-in-transport protection based on encryption mechanisms.
  - Whether it will be used or not depends on the behaviour of HeadEnd system.

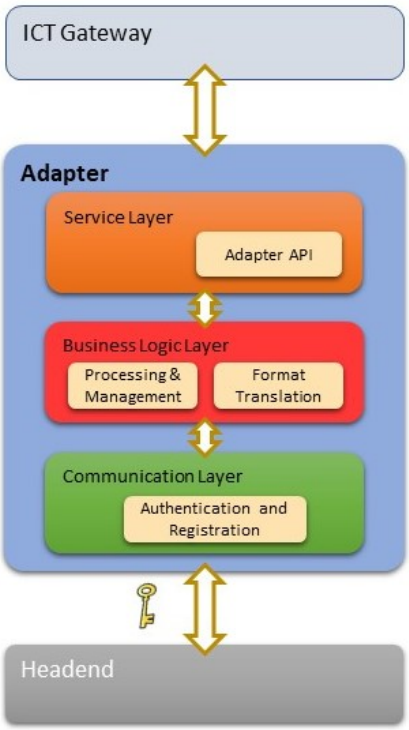

Figure 7: General Adapter Architecture

5.4.1 Grid Topology System Adapter

Since the major processing of grid topology data takes part at the corresponding HeadEnd, the adapter will be focused on periodically retrieving parsed data from the HeadEnd and forwarding it to the ICT Gateway.

Moreover, the adapter should be able to recognize changes in Grid Topology. This can be achieved by comparing the new data with the data from the previous or initial step of topology processing and then forwarding only changes to the ICT Gateway. Changes subsume that there is either a new entity in grid topology, or an existing one is deleted or modified.

Communication with the corresponding HeadEnd system will be realized by means of HTTP REST calls that will return the current data of grid topology. One call will fetch data related to one entity, e.g., one call to get all house connection, another call to get all cables, etc.

5.4.2 Inverter Web Adapter

It is decided that Inverter Web will be implemented as an adapter rather than as a HeadEnd server.

From the view of the IEEE 2030.5 communication protocol, the Adapter in the ICT GW will have the role of the utility. Main workflows are proceeding as follows:

DER Registration

For the registration process an EndDevice instance for every device is created. The adapter should only register authorized devices. For unauthorized devices, an error code should be returned. The

registration can be an out-of-band or an in-band registration. Using an out-of-band registration, the adapter creates the EndDevice instance corresponding to authorized devices at start-up, prior to any client device connecting to the adapter. Using an in-band registration, the DER posts its EndDevice instance to the EndDeviceList and needs to be verified by the adapter. For both cases the adapter receives a list with authorized end devices via an out-of-band process (can be provided by Solarweb or can be provided for the adapter from the beginning for Net2DG).

Solarweb Registration

Solarweb is an aggregator for the adapter and is therefore a special EndDevice. When the aggregator starts up, the EndDeviceList is queried by the adapter and it receives a list with its own instance as well as all EndDevice instances under its management, including group assignments of the EndDevices.

Subscriptions

Subscriptions can be posted from the aggregator to the adapter as well as the other way around in order to receive information as described in Table 7.

Besides these brief descriptions, the official CSIP (Common Smart Inverter Profile) Implementation Guide (March 2018, current Version 2.1) offers information on any other relevant workflow for the IEEE 2030.5 implementation [26].

5.4.3 AMI Adapter

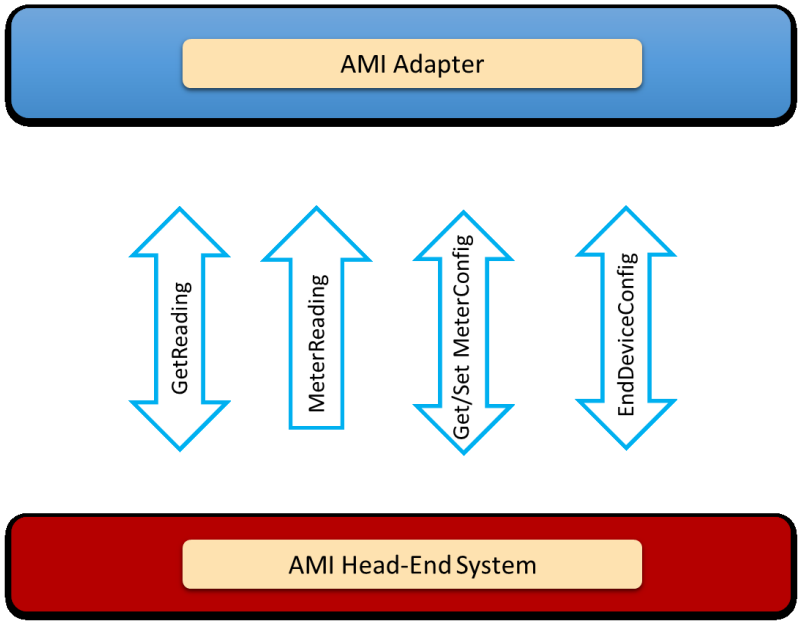

Figure 8: Communication AMI Adapter to AMI HeadEnd Which is Handled by the Network Management System

The network management system is used for two main purposes:

- It enables daily maintenance of already established communication networks. When a communication network is to be established in a utility area, the Network Management system imports usage point data. The meters are automatically assigned to the most optimal concentrators based on a set of rules. The assignment is based on signal strength, signal quality and finally the network is load balanced to achieve the fastest data collection.
- The Network Management system monitors the communication network and handles the collection of data from the network.

Order execution from the AMI HeadEnd system is optimised so that only one data request is required to query multiple meters. One job order can contain many meters as well as multiple commands (e.g. load profile readings, configuration change and breaker command) in one order. All orders are posted to the network, executed and results returned in one step.

5.4.4 RTU Adapters (Janitza)

In the first design and development iteration of Net2DG, RTUs will only be used for the substation and junction box measurements through the Janitza devices. As such, this section focuses on this RTU Adapter. RTUs for mobile PQ measurement systems and for street lights will be revisited later during Year 2.

An RTU Adapter for communication with remote and distributed Janitza devices interacts with an RTU HeadEnd server that acts as the access point for those remote Janitza devices. Therefore, all communication between the RTU Adapter and end devices (Janitza devices) goes through the mediator, i.e., RTU HeadEnd.

As the Section 3.6 already introduced the capabilities of a Janitza device, i.e. different types of measurements, the focus in this section is on the RTU Adapter design and its interaction with the RTU HeadEnd. Consequently, identified are the following main workflows that should be supported by the adapter:

- RTU HeadEnd authentication and end device registration,
- Managing subscriptions,
- Managing notification,
- Interacting with an end device, and
- Data processing.

The following paragraphs describe these workflows.

An RTU Adapter has a WebSocket server that listens for incoming connections from a local network. In the same local network resides the RTU HeadEnd which either has a configured IP address and port for contacting a WebSocket server or it automatically discovers the access point of the WebSocket server. To successfully establish a connection with an RTU Adapter, it will expect that the first message sent by the RTU HeadEnd is an **authentication** message. Only after the successful authentication, the RTU Adapter will request for **registration** of the RTU HeadEnd. Registration assumes that the RTU HeadEnd sends a list of all end devices together with their device IDs, capabilities (measurement data) and sampling rate. The RTU Adapter maintains a local register of the end devices and also propagates this information to the ICT Gateway, in particular to the component Adapter Register. Registration and

authentication procedures are triggered at the initialization of the RTU HeadEnd or after the RTU HeadEnd recovers after the connection with the RTU Adapter was lost.
The RTU Adapter can make a **subscription** with the RTU HeadEnd in order to periodically receive the following data (measures):

- All measures from all end devices,
- All measures from the subset of end devices,
- Subset of measures from all end devices, and
- Subset of measures from the subset of end devices.

Moreover, the RTU Adapter will receive the following **notifications** from the RTU HeadEnd by utilizing the existing WebSocket connection established during the authentication and registration procedure:

- A notification when a new end device connects to RTU HeadEnd, and
- A notification when an existing device disconnects from RTU HeadEnd.

So far, the focus was only on receiving information from the RTU HeadEnd and end devices. However, an RTU Adapter can also issue **control** messages to end devices. It can send the following control messages either to all end devices, a subset of end devices or to a single end device:

- isAlive message that acts as a ping message and its purpose is to prove reachability,
- Timestamp synchronisation message that triggers an end device or an RTU to synchronize its internal clock,
- A message to change the data sampling rate, and
- A message to get immediate reading of values on remote end device.

Data processing, to be more accurate measurements processing, at the RTU Adapter includes the following procedures:

- Observe timestamps that each end device sends together with measures and generate an alarm if the timestamp deviation, for consecutive *x* measurements, is more than *y*,
- Do the same for each measurement type and compare them to some input values that provide the range in which measurements have to be sent,
- Generate alarms accordingly and propagate them to the ICT Gateway.

In order to realize the listed workflows and interactions, it is required to develop the set of messages (protocol) that will be exchanged between RTU Adapter and RTU HeadEnd. Later on, the same shall be defined for communication between RTU HeadEnd and RTU abstracting end devices.

5.5 Gateway GUI

This section introduces the proposal for user interface design in the ICT Gateway. The figures below visualize different views in a user interface:

- Main view,
- Node view, and
- Alert view.

In the Main View, an operator can select desired grid topology from a dropdown list. After the grid topology has been selected, basic information about topology is shown on the left-hand side, e.g., the total number of nodes in the topology, the number of different node types and the number of online

nodes. At the same time, on the right-hand side a map is presented with visualized nodes and lines/cables. What will be visualized on the map, is controlled with the buttons in the pane on the left-hand side.
Moreover, each item rendered on the map is clickable. This means that the operator can check the details of each node and line just by clicking on it.

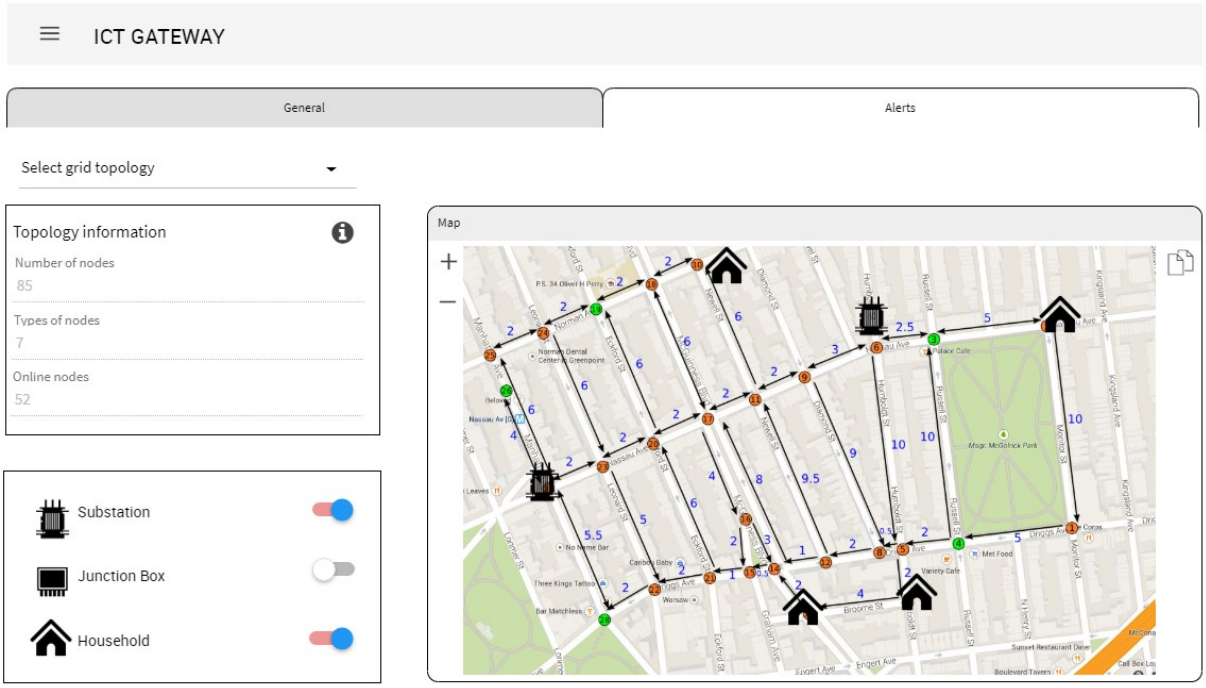

Figure 9: ICT Gateway UI - Main View

Figure 10 shows the details of a node selected on the map presented in Main View. This view shows for each node the textual information as well as the graphical representation of measurements generated on it. Among the other information, it is listed when the ICT Gateway has heard from that node for the last time. In addition, there can be a list containing all events that happened on the selected node, e.g., the “node lost connection” with the system and then reconnected after a couple of minutes. Another information that will be presented on this view, is about the presence of alerts on the selected node.

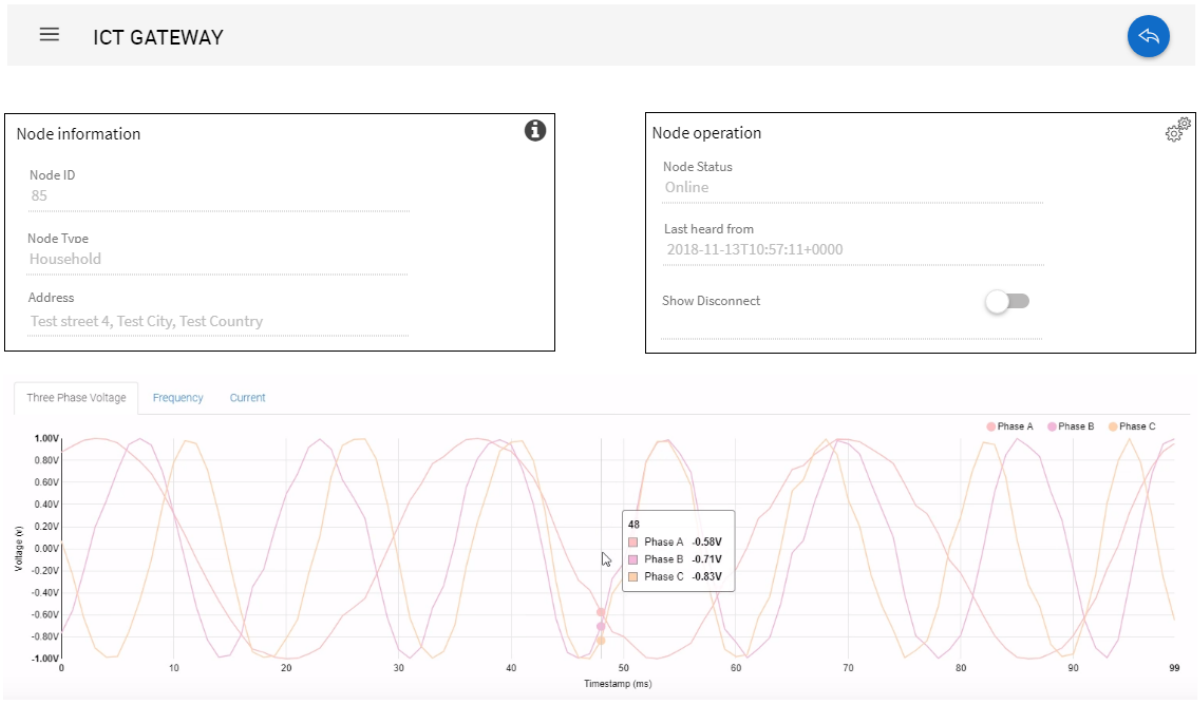

Figure 10: ICT Gateway UI - Node View

When the operator selects Alert tab in the main view, it is presented with the new view illustrated in Figure 11. There is a list of different types of alerts/events which can be filtered by event type and event location, i.e., the grid topology where the event emerged. Each list item, i.e., an event, is clickable. With each click, the operator sees additional information: grid topology on which the event occurred, a node associated with the event, and a short description of event.

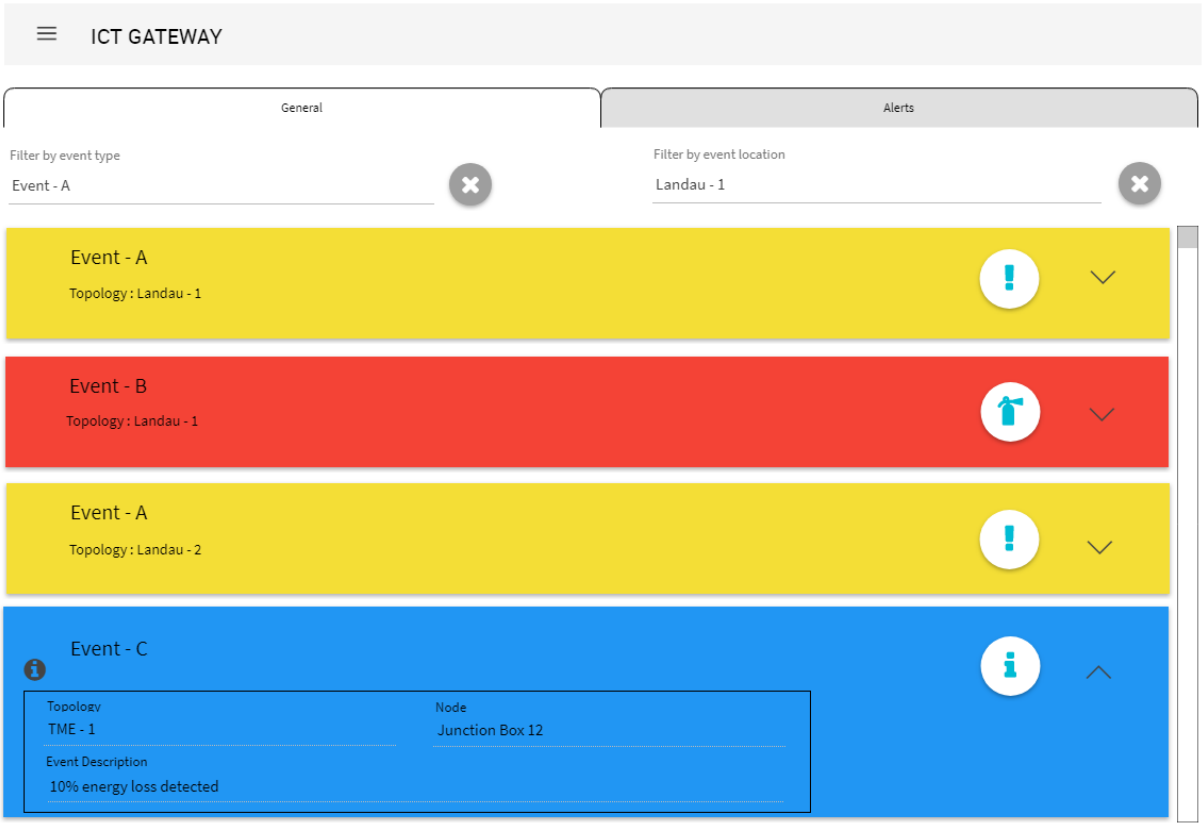

Figure 11: ICT Gateway UI - Alert View

In addition to the above mock-ups and information they present, there will be a visualization element that holds information about registered subsystems as well as deployed and active applications, e.g., either an additional tab or a separate element in Main View. Moreover, it has be possible to trigger an application for supports, e.g., the Loss Calculation application. A user can be notified about the execution results either through alarms or nodes on a map, e.g., the Node View.

When the project and ICT Gateway will become more mature, there will arise the need for extending the user interface. The extension can be addressed by adding new tabs in the main view.

6 Initial Design/Solution Approaches of Other Required Components

6.1 Substation/junction box (Janitza) RTU HeadEnd Server

During the first development iteration, the RTU HeadEnd Server for the Janitza measurement devices will be designed and implemented. RTU HeadEnd Servers for mobile PQ systems, streetlight control, and possibly other actuation devices will be rediscussed during Year 2. This section therefore focuses on the HeadEnd Server for the Janitza measurement device.

An RTU HeadEnd Server is a server application running in a Virtual Machine (VM) at a DSO site. It communicates with an RTU Adapter residing in the same network and also with numerous remote RTUs which communicate with the RTU HeadEnd Server over Internet (3G or any other cellular network technology). One the one side, an RTU HeadEnd Server communicates with an RTU Adapter and on the other side with remote RTUs. Consequently, these two communication paths will be separately addressed in this section.

RTU HeadEnd Server towards RTU Adapter

As already described RTU Adapter, Section 5.4.4, an RTU HeadEnd Server is an initiator of authentication and registration with an RTU Adapter deployed on an ICT Gateway. Since it maintains a local register of remote RTUs, it provides this to the RTU Adapter during the registration and also sends a notification to the RTU Adapter when the local register is updated, e.g., new RTU connected to RTU HeadEnd Server or an existing one disconnected.

Moreover, it has to provide infrastructure for subscriptions by RTU Adapters. It needs to locally maintain information to which RTUs (end devices) an adapter has subscribed. In addition, it has to have also a mechanism to handle control/request messages issued by an RTU Adapter. Such a message has to be transformed, in order to conform to the protocol running on the WebSocket connection to a remote RTU and forwarded to the remote RTU.

It is worth to point out that the connection established between an RTU HeadEnd Server and an RTU Adapter is based on WebSocket and thus it is required to define messages and specify protocols to support the above listed workflows.

RTU HeadEnd Server towards RTU

An RTU HeadEnd Server is a publicly available access point for remote RTUs and thus it has to be secured. Therefore, it is required that remote clients have to authenticate themselves prior to proceeding with communication. Authentication can be either username/password based or certificates can be utilized instead.

In addition to authentication, it is also required that each remote RTU register itself by providing metadata, e.g., its Id, type of end device, or type of measurements it will provide. After these two steps are successfully completed, an RTU HeadEnd Server is ready to receive measurements from remote RTUs and to forward control/request messages to remote RTUs.

It is worth to point out that the connection established between an RTU HeadEnd Server and RTU is based on WebSocket and thus it is required to define messages and specify protocols to support the above listed workflows.

6.2 Topology HeadEnd Server

This section covers the design of a HeadEnd server tailored for processing grid topology data. Due to the participation of two DSOs in the project, it is required to have two separate HeadEnd servers since each DSO has a different legacy system for storing and maintaining grid topology data.
On the one hand, both HeadEnd systems will conform to the common design directions which are listed in the next section. On the other hand, each will implement a proprietary module for accessing and parsing data from DSO specific underlying legacy systems, i.e., GIS.

6.2.1 Common Design Directions

Following are the main design aspects that have to be addressed in both HeadEnd server implementations:

- A HeadEnd server is an initiator of communication with the ICT Gateway over the corresponding adapter deployed on the ICT Gateway.
- The HeadEnd server thus performs authentication and registration with the Adapter during which it sends a message with capabilities, i.e., information about maintained topologies.
- Interface that is capable of providing the following data
    - Detailed information about each topology,
    - List of nodes and lines in a specified topology,
    - Detailed information for a specified node or a line,
    - Capabilities that are already sent during the registration process.
- Interface to trigger topology reprocessing, i.e., read, parse and process GIS data, from the Adapter.
- Infrastructure for subscriptions created/deleted by the Adapter.

It is worth to point out that the connection established between an RTU HE Server and an RTU Adapter is based on WebSocket, thus the tables below define messages to provide the above listed functionalities.

Table 54: Grid topology HE to ICT Gateway interface options

Grid Topology HE to ICT Gateway Interface	Grid Topology HE to ICT Gateway	ICT Gateway to Grid Topology HE
Request-Reply()	Message with capabilities	Request capabilities
	Message with node information	Request information for particular node ID
		Create/delete subscription
		Trigger grid topology reprocessing
Publish	Registration request message	Status message with HTTP code
	Publish changes in topology	No response

Table 55: Data models and representation

Message Type	Specification	Meta data
Registration request	•HE pushes message to ICT Gateway •Authentication method specified: username/password, PKI, certificates	•Authorization data •Number and types of topologies with IDs •Number of covered secondary substations
Request capabilities	•Get topology data for specific topology ID	
Message with capabilities	•Number of Grid Nodes contained in topology •Types of grid nodes that are supported •Prosumer types that are supported •Capability to actively push topology information changes to the ICT-GW •Type of cable or aerial line attributes that are supported	
Request information for particular node	•Get information for a particular node in topology	•Topology ID •Node ID
Node information	•Returned data are specified in Section 8.1.1 in D1.2	
Publish changes in topology	•Grid Topology HE detects changes in topology files published by GIS •It pushes changes to ICT Gateway	•List that contains changed/updated nodes in all maintained topologies

6.2.2 StwLan Grid Topology HeadEnd Server

The Grid Topology HeadEnd heavily relies on processing multiple files generated by GIS at Landau. The structure of those files is presented in Annex A in this document. The GIS system periodically writes files to the file system of the HeadEnd server, every few months or manually upon change. The HeadEnd server detects the presence of new files, reads and processes them. To detect whether a current topology has been updated, it checks each line if there is a modification to the current topology. If yes, then updates are made for the internal model at the HeadEnd server and a notification about the topology update is sent to the ICT GW.

From the processed files, it has been extracted a list of entities already introduced in D1.2 Section 8.4 [1]. The following sections describe each entity in detail.

Entity of type *cable* is responsible for making connections between all other entities. Top-level entity is of type *substation* and it is an entry point from the medium voltage grid to the low voltage grid. Such an entity is connected to the medium voltage grid on the one side and to the low voltage grid on the other side. Moreover, a *junction box* entity has one cable as input, but multiple cables as outputs. It splits one cable into multiple cables. A junction box can be connected with either another junction box or with a prosumer. *Sleeve* represents just a simple connection point of two cables.

Households and street light systems are connected to junction boxes, while photovoltaic systems are connected to households.

In order to model the details of a household connection and associate it with a metering device that acts as a data source, it was necessary to introduce an additional logical entity named *MeteringPoint* which is associated with a house connection. Consequently, it was required to introduce an additional cable that spans between a *MeteringPoint* and a house connection. In addition, since the GIS system does not provide a file with information about fuses in the grid topology, the HeadEnd server implements the rules for mapping fuses on the extracted cables. Therefore, some cables are enriched with attributes that pertain to information about fuses. Circuit breakers are included in the processed topology as well.

Due to the lack of explicit mapping between a cable and a household that connects it to the grid, the main challenge was to find a way to perform that mapping. A cable has a name of a junction box where it originates and only a house number where it ends, but not a street. Consequently, it cannot be mapped to a household uniquely identified by junction box, street and house number. Therefore, it is necessary to scan all households for each cable and compare junction box and house number to those provided in entries representing households. When a match is found, the cable can be assigned to the particular household. It is important to note that one junction box does not serve households from two different streets. Otherwise, the match would not be unique.

To establish a relation between a cable and an entity, in particular when the entity is a household, the grid topology HeadEnd has to be carefully designed and implemented. Figure 12 below illustrates the workflow that the Grid Topology HeadEnd has to conform with.

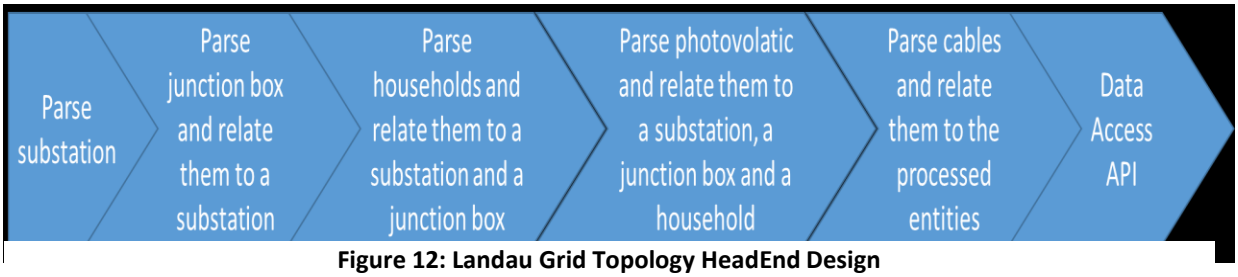

Figure 12: Landau Grid Topology HeadEnd Design

The Grid Topology HeadEnd starts by extracting and parsing substation data which is later referenced by other entities. Then, it parses junction boxes and relates them to the already processed substations.

After that, households are parsed and related to the already processed substation and a junction box. The same is performed on photovoltaic data. Finally, each cable entry is processed in a way that it can be uniquely identified with two already processed entities it connects to: junction boxes and households. The outcome of the Grid Topology HeadEnd comprises of different tables that reflect different node types and a table with the list of all cables where for each cable is defined a starting entity and an ending entity.

The following issues appeared during the automatic extraction and processing of grid topology by utilizing the Grid Topology HeadEnd:

- When observing cable entities, it can be seen whether a cable connects a streetlight to the grid or some other entity. Since there is no information about cables in street light entities, it is impossible to find out the exact cable that connects a streetlight to the grid. Thus, it can only be inferred that a particular cable connects a streetlight to the grid, but not which one. Consequently, the whole streetlight system will be observed as one consumer with a predefined average electricity consumption derived from experiments that Landau internally conducted in the past.

- Due to the lack of exact reference to a cable, a similar problem appears in sleeve entities where it is not trivial to find out on which cable a particular sleeve is installed. Consequently, a subset of sleeves will be manually processed, i.e., following the manually defined rules in code.

6.2.3 TME Grid Topology HeadEnd Server

At TME, the Grid Topology HeadEnd heavily relies on processing a single “humongous” CIM based file generated by GIS, and therefore terminology for the TME HE grid topology server reflects also the CIM terminology. The details and structure of that file is presented in Annex B in this document. The GIS system periodically updates the file system of the HeadEnd server, every few months or manually upon change, while the HeadEnd server detects the change, reads and processes it. To detect whether a current topology has been updated, it checks each line if there is a modification to the current topology. If yes, then updates are made for the internal model at the HeadEnd server (in terms of a complete new file or even in the form of differences from the already available file) and a notification about the topology update is sent to the ICT GW.
From the processed file, a list of entities is extracted. The entities are briefly described in the following section.

The top-level entity in an LV grid is of type *Substation*, which is an entry point from the medium voltage grid to the LV grid. This entity is connected to the MV grid on one side and to the LV grid on the other side. The *BusbarSection* entity plays the same role as *junction box* (as in StwLan grid topology*)* that has one cable as an input, but multiple cables as outputs. It splits one cable into multiple cables. An entity of type *ACLineSegment* (cable) is responsible for making connections between all other entities. *ConnectivityNode* (also termed as *GridNode*) represents points where terminals of AC conducting equipment are connected with zero impedance.

In order to model the details of a household connection and associate it with a metering device that acts as a data source, two entities are introduced i.e. *EnergyConsumer* and *UsagePoint*. Here, *EnergyConsumer* is a point in the network e.g. an end of house connection cable, while *UsagePoint* is a logical or physical point in the network to which readings or events may be attributed. It is used at the place where a physical or virtual meter may be located. The EnergyConsumer entity is connected to the *BusbarSection* via *ACLineSegment*. Since the CIM file does not provide any information about the streetlights and photovoltaic (PV) systems, it is assumed that the streetlights are connected to the *BusbarSection*, while PV systems are connected to *EnergyConsumers*. Moreover, although the GIS system provides information about fuses and other cable attributes (such as circuit breakers, disconnectors etc.) in grid topology, this information is not sufficient to map those to the extracted cables. Therefore, the HeadEnd server implements the rules for mapping fuses to the extracted cables.

As in the StwLan grid topology, due to the lack of an explicit mapping between an *ACLineSegment* and an *EnergyConsumer* which is connected to the grid by *ACLineSegment*, the main challenge was to find out a way to perform that mapping. An *ACLineSegment* only refers to the Substation where it originates. There is no information regarding house number or even the street and consequently, it cannot be uniquely mapped to a household. Therefore, it is necessary to scan all *EnergyConsumers* as well as the *UsagePoints* for each *ACLineSegment* (cable), and then compare Substation and *BusbarSection* to those provided in entries representing *EnergyConsumers*. When a match is found, the cable can be assigned to the particular *EnergyConsumer*.

To establish a relation between an *ACLineSegment* and an entity, in particular when the entity is a household, the grid topology HeadEnd has to be carefully designed and implemented. Figure 13 illustrates the workflow that the Grid Topology HeadEnd has to conform with.

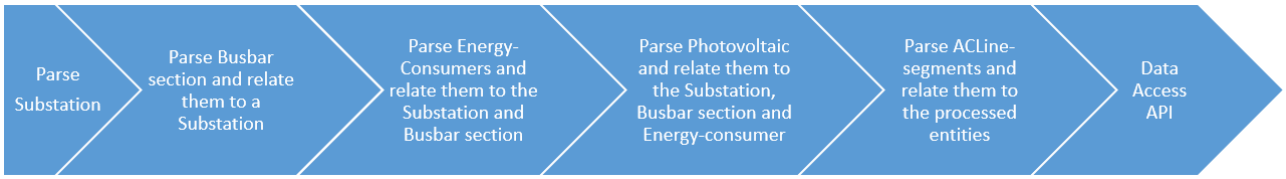

Figure 13: TME Grid Topology HeadEnd Design

The Grid Topology HeadEnd starts by extracting and parsing substation data, which is then later referenced by other entities. Then, it parses the Busbar section (junction boxes) and relates them to the already processed substations. After that, Energy Consumers are parsed and related to the already processed substation and a Busbar. The same should be performed on photovoltaic data (if available). Finally, each cable (AC line segment) entry is processed in a way that it can be uniquely identified using two already processed entities it connects: Busbars and energy consumers. The outcome from the Grid Topology HeadEnd comprises of different tables that reflect different node types and of a table with the list of all cables where for each cable a starting entity and an ending entity are defined.

The following issues appeared during the automatic extraction and processing of grid topology by utilizing Grid Topology HeadEnd:

- There is no information about cable in the EnergyConsumer entity. Similarly, the ACLineSegment only refers to a location, which in turn refers to a coordinate system without any information about the node it is connected to. It therefore seems impossible to find out an exact cable that connects an EnergyConsumer to the grid. It can only be inferred that a particular cable connects an EnergyConsumer to the grid, but the exact EnergyConsumer cannot be identified.
- Due to the lack of exact reference to a cable, similar problem appears in fuses and disconnector entities where it is not trivial to find out on which cable they are installed.

6.3 RTU Design

During the first development cycle, only the RTUs for the Janitza devices is designed in detail. Some of the considerations below will later be generalized to other RTUs during Year 2. Figure 14 shows the design of AMI system, in particular its communication with smart meters, and thus it serves as a guideline for design of RTU.

An RTU is based on Raspberry Pi and it has a wired connection towards the Janitza device and a wireless connection to Internet (3G). Moreover, it can be deployed either in a substation, a junction box or at a household. On the one side, an RTU communicates with an RTU HeadEnd Server and on the other side with a Janitza device. Consequently, these two communication paths will be separately addressed in this section.

RTU towards RTU HeadEnd Server

An RTU HeadEnd Server has publicly available access points which shall be utilized by remote RTUs to establish a connection with the centralized system. Since an access point is publicly available, it has to be protected in a way that each client that tries to connect first has to authenticate itself. Authentication can be performed either by providing username/password or a client should provide a valid certificate. After successful authentication, an RTU has to register itself with the RTU HeadEnd Server which will eventually propagate that information to the RTU Adapter.

After successful authentication and registration, an RTU can start interaction with an RTU HeadEnd Server in the following ways:

- It will periodically read specified values from a Janitza device and send them to the RTU HeadEnd Server,
- It reads values from Janitza every 5 s and aggregates received data to 15 min intervals (configurable interval)
- It sends aggregated data to HeadEnd every 15 min
- It does simple data processing and generates alarms as well
- It can receive the following messages/commands from the RTU HeadEnd Server
    - Change sampling rate

- Synchronize internal clock with the server (ICT Gateway)
- Is Alive message
- Request for immediate reading of values

It is worth to note that the connection established between RTU and RTU HeadEnd Server is based on WebSocket and thus it is required to define messages and specify a protocol to support the above listed workflows.

RTU towards Janitza device

The communication between RTU and the Janitza device is based on the ModBusTCP protocol. In our case, the Janitza device acts as a server and the Java-based client application running on Raspberry Pi acts as a ModBus client. Therefore, the client application has to assemble messages which contain registry addresses for reading out the values on the Janitza device. Messages are periodically sent to the Janitza device in order to get the readings, i.e. measurements. The communication between Java client and Janitza server is based on the request/response paradigm. Section 3.6 has already introduced what kind of measures can be fetched from Janitza devices.

Messages received from Janitza devices, i.e. responses, will be formatted as it will be specified in Task 3.2, timestamped and enriched with device Id, and finally sent to the RTU HeadEnd Server over a Web Socket connection.

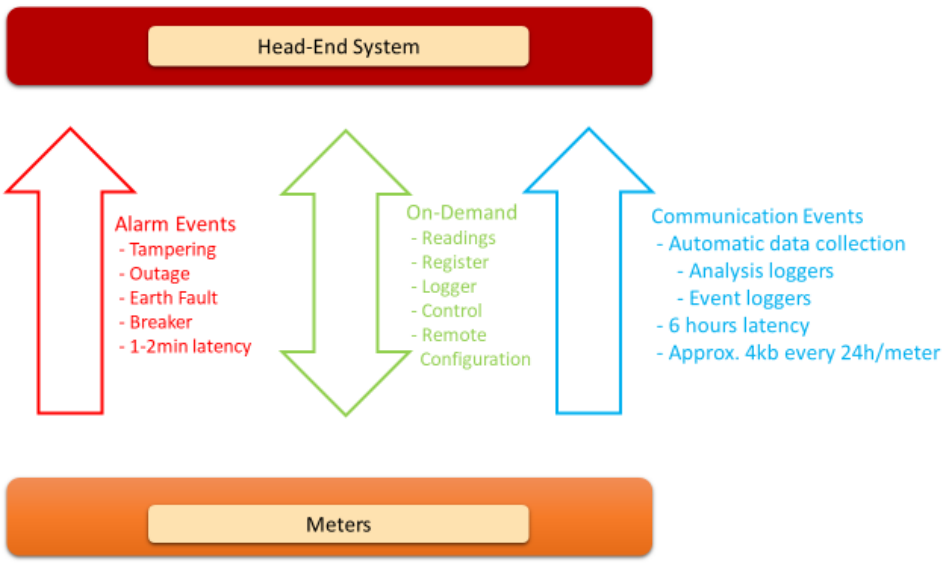

Figure 14: Communication AMI Meter to HeadEnd

6.4 Net2DG Remote Operation and Management Domain

The Net2DG system will evolve during the run-time of the project and system updates, testing and validation will be necessary. In order to ensure cost and time efficiency, the technology partners in

Net2DG shall be able to perform the basic operation and management tasks remotely for the field and lab trial during the Net2DG system development.

The Net2DG technology partners may perform the following operations remotely

- Start and stop software components of the Net2DG system at the remote test site
- Remotely view the Net2DG system dashboard
- Upload software components and configuration files to the remote test site
- Inspect logging data of the Net2DG system at the remote site

This will be provided with a remote-control software *TeamViewer* running on the machine hosting the ICT Gateway (Windows 10 OS).
Then, SSH will be used to assure the security of network connections between ICT Gateway and other application servers or HeadEnd servers at the DSO domain, which are running Linux OS in VMs. In particular, the SSH network protocol support will be obtained with *PuTTY*, a software which consists of several components and permits user control e.g., over the SSH encryption key, protocol version, and so on.

7 Threat and Fault Analysis

The purpose of this section is to provide a Threat and Fault Analysis of the ICT Gateway. The Analysis aims at identifying and analysing the main functionalities of the ICT Gateway in order to evaluate the potential threats which need to be addressed through design, installation and operation of this system. It is worth noting that the analysis focuses on the ICT Gateway and its communication to HeadEnd servers. Therefore, only:

- functions executed by the ICT GW are in scope of the analysis; and
- communications with other systems (e.g., HeadEnds, Applications, Grid Model) are in scope of the analysis.

The analysis has been performed by applying a systematic approach described in Section 7.1.

7.1 Methodology

This section describes the methodology adopted to carry out the threat analysis of the ICT GW.
The analysis is based on two specific aspects characterizing the ICT GW:

- Its main functions,
- The interfaces with other systems, considering the exchanged information.

Therefore, the high level communication architecture provided in the Deliverable D1.2 [1] and main functionalities described both in D1.1 [32] and D1.2 [1], represent the relevant input for such an activity.

The following sections provide more details of individual steps of the applied methodology.

7.1.1 Threat and Hazard Identification

As starting point for the identification of scenarios or causes with a potential impact on security and or on nominal operation of the system, the analysis considers:

- The list of subsystems and related functions described in Table 56,
- The interfaces of the ICT GW with the external systems, thus to consider the different data-flows related to the functions accomplished by the system under analysis; the list of the dataflows is reported in Table 57.

Table 56: Functions description

Subsystem	Function	Function Description
ICT GW	Request data logger	On-demand data collection is used when applications require additional or different information to complete its processing, therefore ICT GW is in charge of requesting such information to the proper HE.
ICT GW	Event generation and correlation	ICT GW creates events based on correlating multiple measurements.
ICT GW	Grid topology mapping	Identifies the generator of an event/data and associates it with node ID defined in grid topology; enriches data with metadata available from a grid topology.

Subsystem	Function	Function Description
ICT GW	Request capabilities from Grid Topology HE	ICT GW requests grid capabilities such as: - Number of Grid Nodes contained in topology - Types of grid nodes that are supported - Prosumer types that are supported - Type of cable or aerial lines attributes that are supported
ICT GW	Request information for particular node from Grid Topology HE	ICT GW requests grid capabilities such as: - Number of Grid Nodes contained in topology - Types of grid nodes that are supported - Prosumer types that are supported - Type of cable or aerial lines attributes that are supported
ICT GW	Actuation	Send setpoints modification/reset to actuation subsystems.
ICT GW	Request validation and estimation	Triggers a request of validation and estimation to the Grid Observability Model
AMI HE	Reply data logger	AMI HE reply event loggers according to request from ICT GW (originated by Applications)
Mobile PQ HE	Long time recordings	Where the instrument is set to use periodic measurements only (this setting is used for long-term statistical studies and benchmarking field-based equipment testing and evaluation)
Mobile PQ HeadEnd	Continuous Data Logging	Where the instrument is set to log RMS and power values once per “x” seconds until memory is filled or for a specified time period.
Stationary grid measurement (Janitza) HE	Reading and writing values	Reading and writing values from a client software communicating with the Janitza device, where the communication between the two is performed by utilizing the Modbus TCP protocol
Inverter Web HE	Publish Data and Events	Provides monitoring data, status information and alarms to ICT GW
Inverter Web HE	Event detection	Detects any relevant event to be published to ICT GW
Inverter Web HE	Data collection	The subsystem should collect all data of certain types according to the specific request from ICT GW
Grid Topology HE	Detect changes in the topology files published by GIS	Detection and publishing of any changes in the grid topology.
Master Time	Clock Synchronization	Synchronisation of independent clocks.
Grid Observability Model (WP2)	Validation	Validation check of measured data (e.g., before pushing the information to applications which subscribed for it).

Subsystem	Function	Function Description
Grid Observability Model (WP2)	Estimation	Calculates missing information (e.g., estimating measurement values before pushing information to applications which subscribed for it).

Table 57: Interface Data Flows

Source	Destination	Data flow/information	Description
ICT GW	AMI HE	Reply and request messages Subscription Unsubscription	Reply to registration Request Capabilities, Data and Event Subscribe Data Unsubscribe Data
ICT GW	RTU Mobile PQ HE	Request and reply messages Subscription Unsubscription	Request capabilities and data Reply to registration Subscribe / Unsubscribe (for continuous data logs, as short time interval measurements, or long time recordings)
ICT GW	RTU Stationary grid measurement (Janitza) HE	Request and reply messages Subscription Unsubscription	Reply to registration Request Capabilities, Data and Event Subscribe Data Unsubscribe Data
ICT GW	Inverter Web HE	Request messages Subscription Unsubscription	Request data, capabilities (Async and where applicable also Sync) Request(registration)
ICT GW	Inverter Web HE	Control commands	DER control values, start and stop time, x-y curve
ICT GW	Inverter Web HE	Additional Information	- Changes in End Device List - Changes in group memberships
ICT GW	Grid Topology HE	Request messages Reply(status(ok))	Request capabilities Request information for particular node ID Request(topology) Request(data) Reply(status(ok)) to registration request
ICT GW	Application Layer	Reply (Registration, Topology Subscription, Unsubscription, Unregistration, Status(accepted), Status(partial), Data, Status(finish), Data, Status, Data)	Subscription ID status for event Subscription status and ID for data channel

Source	Destination	Data flow/information	Description
ICT GW	Application Layer	Event notification	Notification of data and events according to application subscription.
ICT GW	Grid Observability Model (WP2)	Request(data validation/estimation) Publication(data update)	Data to be validated or estimated
AMI HE	ICT GW	Request and reply messages	request(Registration) reply(Capabilities, Data, Event) Publish(Event) Reply(Order) Notify(data)
RTU HE (Janitza)	ICT GW	Request and Reply messages	request(Registration) reply(Capabilities, Data, Event)
RTU HE (Mobile PQ)	ICT GW	Request and Reply messages	request(Registration) reply(Capabilities, Data, Event)
Inverter Web HE	ICT GW	Request and Reply messages	request(Registration) reply(Capabilities, status(ok), "publish" Data, "publish" Event)
Grid Topology HE	ICT GW	Registration and Request messages	Registration(Authorization data; Number and types of topologies with Ids; Number of covered secondary substations) Request(Number of Grid Nodes contained in topology; Types of grid nodes that are supported; Prosumer types that are supported; Capability to actively push topology information changes to the ICT-GW; Type of cable or aerial lines attributes that are supported) Request for Node(Topology ID; Node ID) Response(topology) Reply(data) Publish(event)
Master Time	ALL	Clock Synchronisation	Synchronisation of independent clocks.
Application Layer	ICT GW	Request messages updates publication	request(Registration, Topology, subscription event, unsubscription event, unregistration, on-demand data, visualization) publish(reports, stats)
Grid Observability Model (WP2)	ICT GW	Estimation and Validation response Publication Notification	Provides estimated or validated data publish(data, reports, stats) notify(event, alarms)

The threat identification has been based on a HAZOP approach [33] conducted through the application of specific selected guidewords for both functions and data flow. The application of guidewords allows identifying, in a systematic way, potential deviations from nominal behaviour of the system under analysis.
All the selected guidewords and related descriptions are provided in Table 58 and Table 59 respectively for functions and interfaces.

Table 58: Functional Threat Analysis Guidewords

Guideword	Description
NOT	The function does not execute when it should
OTHER THAN	Something quite different happens
REPETITION	Typically, applicable to communication functions and messaging whereby, due to a failure, the system repeats a function or an old message, thus leading to flooding or overloading

Table 59: Interface Threat Analysis Guidewords

Guide Word	Description
NOT	Messages are not sent
CORRUPTION	Change the content or characteristics of a message
DELAY	Messages are delayed
MISROUTE	Typically, applicable to communication messaging whereby a message is misrouted, therefore directed to the wrong destination
READ/EAVESDROP	Obtain the content of data in a storage device, or other data medium / capturing packets from the network transmitted between two nodes of the network and reading the data content
SCAN	Access a set of targets sequentially in order to identify which targets have a specific characteristic
SPOOF	Masquerade by assuming the appearance of a different entity in network communications. Typically applicable to communication functions and messaging where two systems communicate with each other, but a third system pretends to be one of the other two in order to communicate or gain access.

7.1.2 Threat and Hazard Classification and Risk Evaluation

Once the threats have been identified and consequences have been detailed, the Risk analysis is performed.
In order to check the acceptability of a dangerous situation, the approach is based on the connection between the severity of the potential threat with its probability. The occurrence of a threat having serious consequences but whose probability of occurrence is very weak can be accepted, whereas a less serious but more frequent accident considered cannot be accepted. This comparison is presented in the form of a matrix “Probability - Severity”.

Table 60 provides the categories of probability of occurrence of a hazard/threat and a description of each category.

Table 60: Qualitative Likelihood of Attack Occurrence

Probability	Characterisation	Example
Highly Probable	Can be done by readily available off-the-shelf equipment, without any constraints on physical presence or special software.	Attack can be performed from standard PC connected to the Internet with standard SW
Probable	Can be performed using easily accessible hardware and software (tools from the Internet), requiring some physical presence in the wider neighbourhood.	Sniffing on a non-protected household WLAN
Unlikely	Requires physical access to the building (which is not strongly protected) or some more complicated SW tools to overcome ICT barriers, e.g. via correlation of different information in order to perform an attack.	Physically attaching to a Household Ethernet that is not protected otherwise; sniffing on a weakly protected (e.g. using former WEP) WLAN with known-plaintext attacks via sending email
Remote	Requires physical access to a building that is access protected via locks, alarm systems and access procedures; requires special hardware support that is not available on markets; requires very complicated SW tools to perform attack; can only be done with insider information or multiple traffic traces.	Access to a substation that is locked and has an alarm system (so that the lock cannot be easily broken); sniffing of data traffic by breaking into a protected ISP network first

Table 61 describes the severity levels and the consequences associated with each level.

Table 61: Consequence severity categories

Severity Level	Consequence (one of the columns is enough to justify the severity level)		
	Number of impacted grid/ICT elements	Service impact	Reputation impact
S4 - Disastrous	Impact on Grid/ICT operation	Material damage (of at least 5k€) due to wrong services or endangering of human beings	Formal investigation against DSO with related publicity

Severity Level	Consequence (one of the columns is enough to justify the severity level)		
	Number of impacted grid/ICT elements	Service impact	Reputation impact
S3 - Catastrophic	Full LV grid (served by DSO substation)	Wrong setpoints/values communicated by critical information services	Potential newspaper article circulation about DSO security problem
S2 - Critical	Neighbourhood / (part of) LV feeder	Coordinated wrong outcome of non-critical information services for larger number of customers for several days; continuous unavailability of critical services for periods of at least several hours	Multiple customers lose trust in DSO solution
S1 - Serious	One household	Wrong outcome of non-critical information services; continuous unavailability of non-critical information services for periods of at least several hours; shorter (up to 60min) unavailability of critical services	Single customer believes that problem is due to DSO
S0 - Minor	Single ICT/grid node	Shorter unavailability (up to 2 hours) or slightly outdated (up to 60 minutes) result of non-critical information services to individual customers	Annoyed person that is not customer

For each identified threat, its estimated probability and severity have been combined to obtain the threat's 'rank'.

Table 62 represents the reference risk matrix, as results of hazard/threat identification and ranking. The risk criticality matrix considers the risk criticality regarding the system under analysis.

The probability and severity are assigned based on expert judgment. Both probability and severity are assigned in a conservative and protective way in this preliminary phase of the project, while they will be re-assigned after implementation of proper countermeasure(s) in order to reduce the risk to an acceptable level.

Table 62: Risk Criticality Matrix

RISK CLASSIFICATION		SEVERITY				
		MINOR	SERIOUS	CRITICAL	CATASTROPHIC	DISASTROUS
PROBABIL	Highly Probable	Tolerable	Tolerable	Intolerable	Intolerable	Intolerable
	Probable	Tolerable	Tolerable	Tolerable	Intolerable	Intolerable

	Unlikely	Negligible	Tolerable	Tolerable	Tolerable	Intolerable
	Remote	Negligible	Negligible	Tolerable	Tolerable	Tolerable

Table 63 provides the list of quantitative risk categories and actions requested against each category.

Table 63: Qualitative Risk Categories

Risk Category	Actions to be applied against each category
Intolerable	Shall be eliminated
Tolerable	Acceptable only if the reduction of the risk to negligible is not possible or if cost for reducing the risk would exceed the improvement gained
Negligible	Acceptable

7.1.3 Countermeasures Identification

Once the threats have been identified and according to the results of the Risk analysis, the methodology follows two different ways:

- If the threat's risk is evaluated as "Negligible" or "Tolerable", then no other actions are required for the identified threat and its status can be set at "DELETED".
- If the threat's risk evaluated as "Intolerable" then it is important to identify the proper countermeasure(s) useful to prevent the occurrence of the threat or to reduce its probability of occurrence. The result is represented by the threat countermeasure(s), which identify long-term strategies that may include planning, procedures, maintenance activities, utilization of specific components, equipment, and other activities, as well as how to implement them.

7.1.4 Analysis Results

This section provides a brief summary of final results of the performed analysis. Table 64 and Table 65 summarize the results of the accomplished analysis respectively for functions and Interfaces.

Following list provides a description of possible hazard/threats status:

- SOLVED: it has been identified an appropriate countermeasure
- DELETED: the hazard has been cancelled if:
  - another hazard fully incorporates the first one or
  - the hazard is judged not dangerous or
  - the hazard is judged impossible
- TRANSFERRED: the hazard identifier is not the main system/subsystem triggering the hazard and then it is not responsible for the hazard resolution. Therefore, the hazard is transferred to another system
- CLOSED: the identified mitigations have been implemented, tested and it is given the proper documentary evidence

Table 64: Functional Hazard/Threat Analysis summary

Hazard/Threat Status	Number

Open	26
Solved	0
Deleted	29
Transferred	0
Closed	0
Total	55

Table 65: Interface Hazard/Threat Analysis summary

Hazard/Threat Status	Number
Open	104
Solved	0
Deleted	7
Transferred	0
Closed	0
Total	111

The complete Threat and Hazard Analysis is provided in Annex C and Annex D, for both functional and interface analysis respectively.

It is worth noting that, in this initial phase of the project, any identified hazard and threat cannot be closed. Evidence of implementation of one or more countermeasures aiming at mitigating the threat/hazard will be given in the next phases of the project, through results of tasks: T3.2, T3.3 and T3.4.

8 Conclusions and Outlook

This deliverable collects the results obtained from the activity carried out in task T3.1 aiming to analyse the communication technologies between the data sources and the ICT Gateway, as well as to identify and describe the interfaces of the subsystems that will have to interact with the ICT GW. The analysis developed and described in this deliverable takes as input the WP1 outputs, in particular the Deliverables D1.1 [32] and D1.2 [1].

The deliverable initially provides a brief overview of the state of the art and after that, in Section 3, the analysis of the existing interfaces is approached. This analysis provides the possible options that each subsystem is able to provide interacting with ICT GW; the information, such as measures, events and alarms, as well as topological grid information, are also identified to make the ICT GW able to perform its functionalities.

The identification of the information available from the field has allowed a first more in-depth analysis of the volume of data that Net2DG, and in particular the ICT GW, must be able to handle to efficiently perform its functions. This analysis, based on the information made available by the two DSOs involved in the project, allowed to identify potential issues that could be found during the project, as well as to provide general design guidelines, both for the ICT GW and for the overall Net2DG system, in order to ensure an appropriate dimensioning of software and hardware, also including the capabilities of the network. This analysis, based on different configurations at the involved DSOs, allowed identifying, with a certain confidence, the absence of problems regarding the current communication technologies. The recommended design and technologies will be able to manage huge volumes of data if these are not sent in bursts. On the other hand, it has highlighted potential issues that must be addressed, such as the planning for the storage of large amounts of data that is made available by the field in the course of days, as well as for the ability to post-process such amounts of data.

The deliverable also collects and describes the first results of the activities carried out in task T3.2 related to the ICT Gateway Development. In particular, Section 5 describes the ICT GW architecture, the components and the main functionalities; the section also introduces general design directions that will be addressed by all adapters running inside the ICT Gateway.
A first representation of the data model is also provided both for the grid topology and for the events and measurements of the field. This data model will be refined in Year 2 of the project.

The APIs are also defined at high-level without specifying all parameters and functions since the project is in an initial phase. They will be refined and extended in the course of Task 3.2 based on the outcome and the needs of selected application designs in deliverable D2.1 [31].

Section 6 provides a description of necessary but not yet existing components, which are useful for interfacing with some of the grid subsystems, such as RTU HE for Janitza measurement devices or the Topology HE. Other components such as RTU HeadEnd Servers for mobile PQ systems, streetlight

control, and possibly other actuation devices will be discussed during Year 2 activities in tasks T3.2, T3.3 and T3.4.

Finally, Section 7 provides an initial analysis of faults and security threats. The analysis has been carried out following a systematic approach based on HAZOP methodologies, usually applied in the context of safety critical systems. The HAZOP approach foresees the application of specific guidewords to the functions of the ICT GW and the messages exchanged by the ICT GW with other systems. This leads to the identification of potential threat and hazard scenarios. For each of these scenarios possible countermeasures have been identified which aim at mitigating or reducing the probability of occurrence of the identified hazards. A classification of the dangers and a refinement of countermeasures will be performed during the second year of the project and properly documented through tasks T3.2, T3.3 and T3.4.

9 References

[1] Net2DG, "Deliverable D1.2 - Initial Baseline Architecture," 2018.

[2] Y. W. (ed.), "BigIoT Deliverable D2.1, 'Analysis of Technology Readiness', BigIoT consortium," BigIoT, March 2016.

[3] A. Bröring, S. Schmid, C. K. Schindhelm, A. Khelil, S. Käbisch, D. Kramer, D. L. Phuoc, J. Mitic, D. Anicic and a. E. Teniente, "Enabling IoT ecosystems through platform interoperability," *IEEE Software,* vol. 34, no. 1, pp. 54-61, Jan. 2017.

[4] "eSmart Systems," [Online]. Available: https://www.esmartsystems.com/ .

[5] "Coordination of Transmission and Distribution data eXchanges for renewables integration in the European marketplace through Advanced, Scalable and Secure ICT Systems and Tools, State of the Art - TSO-DSO Interoperability," TDX-ASSIST, 2017.

[6] "NextGen SCADA Europe," ENTSO-E, 2018. [Online]. Available: https://www.entsoe.eu/events/2018/01/30/nextgen-scada-europe-2018/ .

[7] "'Nyt SCADA system – IT sikkerhed og smartgrid', Fredericia, Denmark: Net-Sam SCADA A/S," Nov. 2013. [Online]. Available: https://docplayer.dk/22685307-Nyt-scada-system-it-sikkerhed-og-smartgrid-net-temadag-om-fremtidens-elsystem-trinity-fredericia-26-november-2013.html.

[8] "Finalist til prestisjefylt IT-pris," 29 11 2018. [Online]. Available: https://www.aenett.no/presse-og-aktuelt/finalist-til-prestisjefylt-it-pris/. [Accessed 18 12 2018].

[9] Y. Zhang and T. H. a. E. F. Bompard, "Big data analytics in smart grids: a review.," *Energy Informatics,* vol. 1, no. 1, 2018.

[10] A. Alimardani, F. Therrien, D. Atanackovic and J. a. V. E. Jatskevich, "Distribution system state estimation based on nonsynchronized smart meters," *IEEE Transactions on Smart Grid,* vol. 6, no. 6, pp. 2919-2928, 2015.

[11] M. Stefan, J. G. Lopez, M. H. Andreasen and R. S. a. R. L. Olsen, "Data Analytics for Low Voltage Electrical Grids.," in *IoTBDS*, 2018.

[12] M. Seijo, G. López and J. J. Matanza, "Planning and performance challenges in power line communications networks for smart grids.," *International Journal of Distributed Sensor Networks,* vol. 28, 2016.

[13] IEEE Smart Grid Big Data Analytics, Machine Learning and Artificial Intelligence in the Smart Grid Working , *Big Data Analytics in the Smart Grid. White Paper Draft.*

[14] Illinois Institute of Technology, "Public/Private Partnership Creates Opportunity to Fundamentally Address Local Energy Crises,," [Online]. Available: https://web.iit.edu/mediaroom/press-releases/2008/nov/20/publicprivate-partnership-creates-opportunity-fundamentally.

[15] "PingThings, "Predictive Grid,"," [Online]. Available: http://www.pingthings.io/ .

[16] IBM, “Strategic Asset Management to Improve Electricity Network Planning and Maintenance,” [Online]. Available: https://www-935.ibm.com/industries/energy/solutions/asset-workforce-management.html.

[17] S. Vyasa, R. Kumara and R. Kavasserib, “Data Analytics and Computational Methods for Anti islanding of Renewable Energy Based Distributed Generators in Power Grids,” *Renewable and Sustainable Energy Reviews,* vol. 69, pp. 493-502, March 2017.

[18] “Scottish & Southern Electricity Networks, “Thames Valley Vision,”,” [Online]. Available: https://www.ssepd.co.uk/thamesvalleyvision/.

[19] “UPGRID Project,” 2015-2017. [Online]. Available: http://upgrid.eu/.

[20] S. Kadam, B. Bletterie and W. Gawlik, “A Large Scale Grid Data Analysis Platform for DSOs.,” *Energies,,* vol. 10, no. 8, p. 1099, 2017.

[21] H. Xiaosheng, T. Kai, D. Xuzhu, Z. Datong and X. Xiaoliang, “Research and implementation of outage analysis key technology based on information integration of power distribution and utilization,” in *International Conference on Electricity Distribution (CICED)*, China, 2016.

[22] F. Hohn and L. Nordström, “Data Models and Protocol Mapping for Reduced Communication Load in Substation Automation with High Sampling Rate Protection Applications,” in *Proceedings of IEEE SmartGridComm*, Aalborg, Denmark, 2018.

[23] B. Khaleghi, A. Khamis, F. O. Karray and S. N.Razavib, “Multisensor data fusion: A review of the state-of-the-art,” *ELSEVIER,* vol. 14, no. 1, pp. 28-44, 2013.

[24] F. Fusco, S. Tirupathi and R. Gormally, “Power Systems Data Fusion based on Belief Propagation,” in *IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, Turin, Italy, 2017.

[25] M. Kordestani and M. Saif, “Data Fusion for Fault Diagnosis in Smart Grid Power Systems,” in *IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*, 2017.

[26] California Public Utilities Comission, *Common Smart Inverter Profile; IEEE 2030.5 Implementation Guide for Smart Inverters,* USA, 2018.

[27] “MAVOWATT 230, 240, 270 & 270-400, Power Quality Analyzer”.

[28] “Janitza electronics GmbH: Power Analyser UMG96RM Basic device – User manual and technical data.”.

[29] “Janitza electronics GmbH: Power Analyser UMG 96 RM, Basic unit, Extension UMG 96RM-PN Extension UMG 96RM-P, Extension UMG 96RM-CBM - Modbus-address list and Formulary”.

[30] A. Bondavalli, F. Brancati and A. Ceccarelli, “Safe Estimation of Time Uncertainty of Local Clocks,” *International Symposium on Precision Clock Synchronization for Measurement, Control and Communication, ISPCS ,* pp. 1-6 , 2009.

[31] Net2DG, “Deliverable D2.1 - Algorithms for grid estimation and observability applications,” 2018.

[32] Net2DG, “Deliverable D1.1 - Case Study Specifications & Application Requirements,” 2018.

[33] R. Winther, O.-A. Johnsen and B. Axel Gran, “Security Assessments of Safety Critical Systems Using HAZOPs,” in *Computer Safety, Reliability and Security*, Berlin, Heidelberg, 2001.

[34] “Bringing Our Electric Grid into the 21st Century,” 2014. [Online]. Available: https://www.engerati.com/resources/bringing-our-electric-grid-21st-century. .

[35] UPGRID, “D.2.1 - Report on the Implementation of the CIM as a Reference Data Model for the Project,” 2016.

10 Annex A

The following tables show how the corresponding files look like in the Landau GIS system, in particular which information items are present in the header of each single file.
For increased readability of this deliverable version, only one example is provided in this shorter version of the Annex.

Table 66: Substation in GIS

File type	Substation
Headers	**Description**
TrafostationNr	Identification of a substation consisting of a street name and a number
Stationstyp	Type of a station
BaujahrStation	Year of substation production
Bemerkung	Additional information about a substation
HotLink	Path on which an image is stored
Datum	Installation date
Rechtswert	Coordinate in GIS system
Hochwert	Coordinate in GIS system
Some headers are not important for our analysis and thus are omitted.	
Example	
20 Weiherweg; ;0; ; ; ;26.09.2001;4551949,411999999500000;5389990,472000000100000;0,0;20 Weiherweg;;;;20; **Substation is named *20 Weiherweg* and is it built in 2001 and has two coordinates in GIS system.**	

11 Annex B

The following table lists the different nodes and the related attributes as available in the corresponding TME CIM based file obtained from the GIS system.
For increased readability of this deliverable version, only one example entry is provided in this shorter version of the Annex.

- **Note:** Master resource identifier (mRID) is a globally unique identifier issued by a model authority. It must semantically be a UUID as specified in RFC 4122.

Table 67: List of Nodes and their description - shortened

Node	Attributes	Description

Location	<mRID> <CoordinateSystem>	The place, scene, or point of something where someone or something is, and/or will be at a given moment in time. Can be defined with one or more PostitionPoints (coordinates) in a given coordinate system. - In Net2DG, this is an attribute to trafo, cable ends, etc.

12 Annex C

This annex reports on the threat and hazard analysis identified on the ICT Gateway functions through the application of a HAZOP approach. For each threat and hazard, caused by malicious intentional acts or by faults, an initial risk classification has been performed prior the identification of potential Mitigations or Countermeasures.

For increased readability of this deliverable version, only one example entry is provided in this shorter version of the Annex.

Threat ID	Block	Function	Function description	Guideword	Threat/Hazard Description	Status	Rationale (if DELETED)	Consequence	Cause	Probability	Severity	Risk Classification	Mitigation/ Countermeasure
TF_001	ICT GW	Request data logger	On-demand data collection is used when applications require additional or different information to complete its processing, therefore ICT GW is in charge of requesting such information to proper HE.	NOT	ICT GW does not trigger the request of data to the HE server.	OPEN		Applications do not receive requested information.	- HW fault - SW fault - Intentional/Accidental Misconfiguration -Malicious code - Worm and Virus - Power disconnection - Wrong input - Overloaded resources	Highly Probable	Catastrophic	Intolerable	- Maintenance procedures - Security policies - Antivirus - Use of UPS - Anomaly detection

13 Annex D

This annex reports on the threat and hazard analysis identified on the dataflows between the ICT Gateway and the other systems, through the application of a HAZOP approach. For each threat and hazard, caused by malicious intentional acts or by faults, an initial risk classification has been performed prior the identification of potential Mitigations or Countermeasures.

For increased readability of this deliverable version, only one example entry is provided in this shorter version of the Annex.

Threat ID	Source	Destination	Data flow/Information	Description	Guideword	Threat/Hazard Description	Status	Rationale (if DELETED)	Consequence	Cause	Probability	Severity	Risk Classification	Mitigation/ Countermeasure
TI_001	ICT GW	AMI HE	Reply and Request messages Subscription Unsubscription	Reply to registration Request Capabilities, Data and Event Subscribe Data Unsubscribe Data	NOT	The message is not sent to the AMI HE	OPEN		- AMI HE does not receive a request, therefore does not reply with data, events and capabilities.	- Environmental condition - Interference - Power disconnection - Cable disconnection - SW bugs - Network congestion - Malicious code installed - HW fault - Router misconfiguration	Highly Probable	Catastrophic	Intolerable	- Timeout - Use of a UPS - Protection against interference - Maintenance procedures - Security policies

14 Annex E

The following tables list entities representing measurements and events, as introduced in Section 5.2, showing a preliminary version of the data model structure, attributes, and data types. The tables also report on source of the measurement/event, and potential application which may use the data (where available). Generally, measurements can be connected to `GridNode` or `Cable` or also to both entities, as follows:

- Voltage measurements (and events related to voltages) are only linked to a single `GridNode`. Thus, the measurands involving voltage only contain a single `GridElement_id` attribute.
- Current measurements are linked to a `Cable` AND to a `GridNode` (which is at the end of the cable, where the measurement is taken).
- Power measurements (active or reactive or apparent) must be linked to a `Cable` and to a `GridNode`.

Therefore, the measurands involving current and power contain `GridElement_id_1` and `GridElement_id_2` attributes.

The same also holds for events regarding voltage (or other measurements), current and power values.
For increased readability of this deliverable version, only one example entry is provided in this shorter version of the Annex.

Table 68: Measurands for AMI

Measurand Name	Description	Attributes	Data Type	Unit	Source	Applicability
`ActivePositivePower`	Active positive power consists of active power from quadrants 1 and 4.	`GridElement_id_1`	`INT`		AMI	Loss Calculation (LC)
		`GridElement_id_2`	`INT`			
		`measurement_id`	`INT`			
		`measurement`		kW		
		`display_OBIS_code`				
		`designation_1`				
		`designation_2`				
		`timestamp_begin`				
		`timestamp_end`				
		`clock_accuracy`				
		`error_characterization`				