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:	**D3.3**
Deliverable title:	**ICT resilience mechanisms and verification**
Work package:	WP3
Due date of deliverable:	M30 – 30/06/2020
Actual submission date:	M30 – 30/06/2020
Start date of project:	01/01/2018
Duration:	42 months
Reviewer(s):	Hans-Peter Schwefel (GD), Nicole Diewald (Fronius)
Editor:	Nicola Nostro (RT)
Authors:	Nicola Nostro (RT), Enrico Schiavone (RT), Gabriele Morgante (RT), Kamal Shahid (AAU), Domagoj Drenjanac (GD), Ivan Mercep (GD)
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
0.0	08/04/2020	Nicola Nostro, Enrico Schiavone	Definition of Table of Contents
0.0	29/04/2020	Enrico Schiavone	Contribution to Sections 3.3.1 and 3.3.2
0.0	11/05/2020	Enrico Schiavone	Contribution to Sections 3.2 and 4
0.0	25/05/2020	Gabriele Morgante	Contribution to GUI section
0.0	29/05/2020	Kamal Shahid	Contribution to section 3.3
0.0	08/06/2020	Domagoj Drenjanac	Contribution to section 3.3 and overall review
0.1	09/06/2020	Nicola Nostro	Implementation of comments, minor modification in the entire deliverable and editing of executive summary and conclusion. Release for internal review.
0.2	16/06/2020	Enrico Schiavone	Modifications in the deliverable to implement comments from internal reviewers
0.3	19/06/2020	Nicola Nostro, Kamal Shahid, Domagoj Drenjanac, Ivan Mercep	Modifications to address comments from internal reviewers.
0.4	26/06/2020	Nicola Nostro	Release to reviewers.
0.5	29/06/2002	Nicola Nostro	Release for final 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This deliverable contains original unpublished work except where clearly indicated otherwise.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

List of Acronyms

Net2DG	Leveraging Networked Data for the Digital electricity Grid
AC	Alternating Current
ADFS	Active Directory Federation Service
AMI	Advanced Metering Infrastructure
API	Application Programming Interface
AVR	Automatic Voltage Regulation
CEP	Complex Event Processing
CPU	Central processing unit
CRUD	Create, Read, Update and Delete
CSS	Cascading Style Sheets
DAO	Data Access Object
DB	Database
DoS	Denial of Service
DSO	Distribution System Operator
EGC	Event Generation & Correlation
EM	Electrical Measurement
GIS	Geographic Information System
GMon	Grid Monitoring (application)
GTM	Grid Topology Mapping
GUI	Graphical User Interface
GW	Gateway
HE	HeadEnd
HTTP	HyperText Transfer Protocol
HW	Hardware
ICT	Information and Communications Technology
ICT GW	ICT Gateway

ID	Identifier
IDE	Integrated Development Environment
INV	Inverter
IP	Internet Protocol
JVM	Java Virtual Machine
LAN	Local Area Network
LC	Loss Calculation (application)
LV	Low Voltage
MQTT	Message Queue Telemetry Transport
ODet	Outage Detection (application)
ODiag	Outage Diagnosis (application)
OGM	Observability Grid Model
ORM	Object-Relational Mapping
OS	Operating System
POI	Point Of Interest
PV	Photo Voltaic
RAM	Random Access Memory
RDBMS	Relational DataBase Management System
REST	REpresentational State Transfer
RTU	Remote Terminal Unit
S&R	Security & Resilience
SM	Smart Meter
SPA	Single-Page Application
SQL	Standardized Query Language
STS	Secure Token Service
SW	Software
UI	User Interface
UTC	Coordinated Universal Time
UUID	Universally Unique Identifier

1 Executive Summary

This report documents the final implementation of the ICT GW including the additional security and resilience functionalities that provide more robustness to the entire Net2DG solution.
The main objective is to describe the undesired events that can occur during the normal operation of the ICT GW, their detection through the Event Generation & Correlation and the automatic reactions the ICT GW is able to trigger in order to contrast and/reduce the effects of such undesired events.
This deliverable also provides the verification results of the additional security and resilience functionalities, while the verification of main basic functionalities is provided in the context of WP5.
Furthermore, refinements have been performed in the already existing modules in order to meet field and laboratory requirements and make the solution more efficient; such refinements are also described in this deliverable.

2 Introduction and Overview

The main focus of this deliverable is to describe the security and resilience additional functionalities that contribute to the robustness of the ICT GW and the overall Net2DG solution.
These functionalities and their specification are the result of the threat and security analysis carried out and developed in the context of WP3 and reported in D3.1 [1].
The analysis in D3.1 [1] highlighted the threat events that potentially constitute a significant risk for the DSO, the whole Net2DG system, the ICT GW, its functions and interfaces.

A summary of threats to be avoided includes:

- Overloading of resources, due to malicious software, viruses, failures of ICT GW modules
- Intrusion both at network and ICT GW level
- Spoofing, 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.
- Corruption, which can affect the integrity of the data (e.g., measurements, events, grid topology information), due to either intentional actions on data transmission or network failures or HEs malfunctions
- Delaying, either of measurements sent from HEs to the ICT GW or of internal elaboration of ICT GW or response to application requests.

The threats for which the risk has been considered significant, have been further investigated in the context of Net2DG in order to identify proper countermeasure both technical and procedural.
Purpose of mitigations is to reduce the probability of occurrence of either a failure or an attack. Nevertheless, these mitigations do not to completely remove the probability of occurrence.
Each of the identified mitigations is assigned to one or more subsystems or components of the ICT GW, for example encryption schema (TLS), as well as Authentication are assigned to the HEs and to the corresponding Adapters in the ICT GW, meaning that they should support them. In order to increase the level of security the detection of anomalies is an additional mitigation assigned to the ICT GW Security and Resilience component aiming at detecting any potential deviation from the expected behavior of both the ICT GW and communication with the HEs. At the same time the monitoring of specific events occurring in the system and their correlation within the context in which they are observed (e.g., monitoring of collected measurands and correlation with reference threshold or previous values) can be seen as the warning signals, meaning that something unexpected is occurring.
Moreover, the deliverable describes further refinements carried out on some specific modules (Section 5) and new modules (Section 4) implemented to provide greater robustness to the ICT GW.

While the verification of main functionalities of ICT GW (interaction with subsystem in the field, collection of measurands and events, as well as grid topology information) has been carried out in the context of WP5 and documented in deliverable D5.1 [2], current deliverable describes the verification

activities carried out during development of the security and resilience functionalities, and in particular the successful generation of events and implementation of the countermeasures for each of the identified undesired events.

Finally, the definition of test procedures to verify the security and resilience measure, as well as the results of their execution, are provided in Section 6.

3 ICT Gateway Security and Resilience

3.1 Overview

The high-level architectural description of the ICT Gateway (ICT GW), including interfaces with external subsystems (e.g., HE subsystems, Application, OGM) is shown in Figure 1, unlike the architecture presented in the Deliverable D3.2 [3], in the current final solution the Security & Resilience module has been implemented as an external and standalone software module with respect to the ICT Gateway, in order to be able to detect also outages regarding the ICT GW itself.

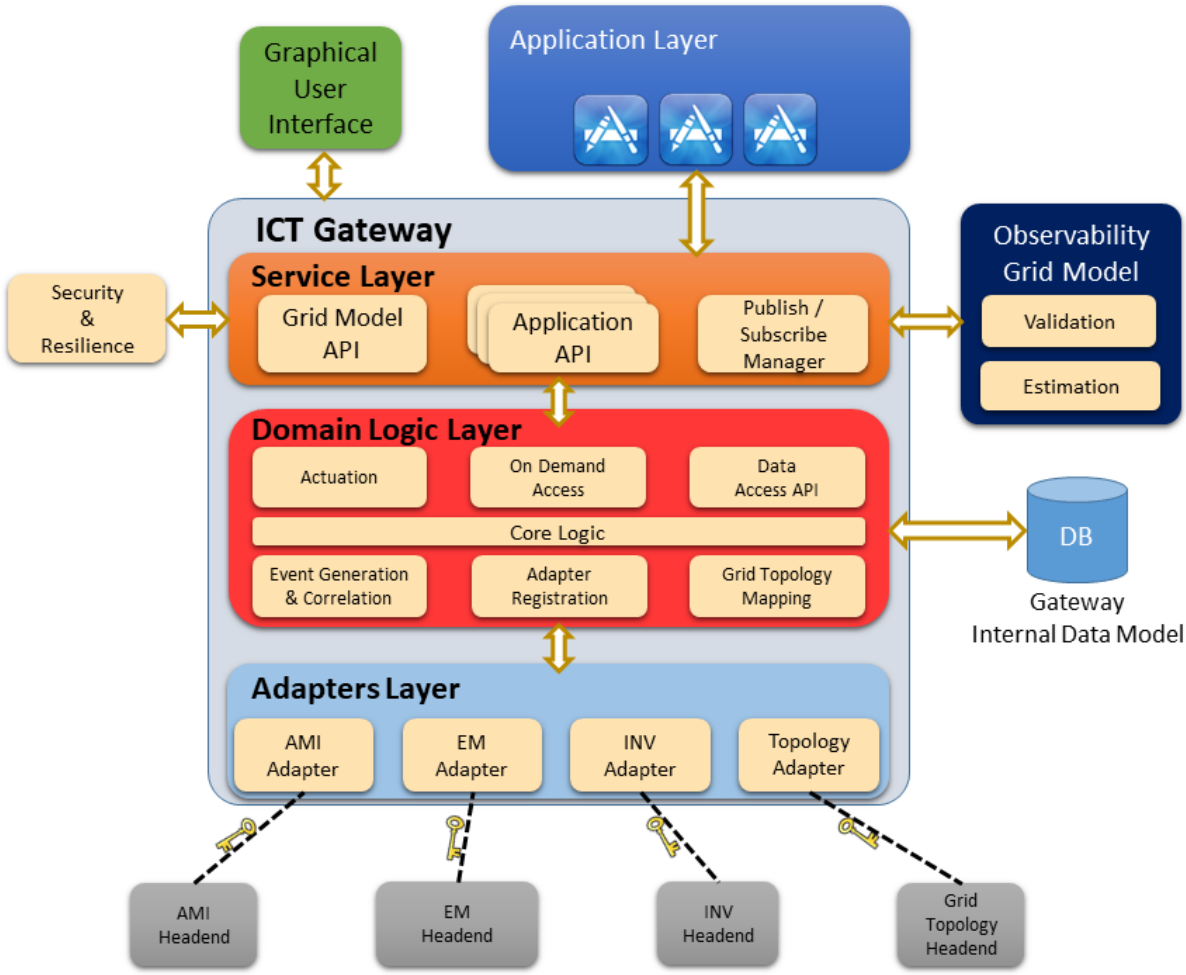

Figure 1 - ICT Gateway Architecture

ICT GW is the first contact point with the field subsystems aiming at collecting both grid topology information and measurements, events and alarms from each of the HE to which it is connected.
All the Information received from the field are collected in a Database (DB) according to the data model defined within the context of the project [3].
Information is then made available, on request, to the applications at the Application Layer and to the Observability Grid Model (OGM) for their elaboration and processing.

On the other hand, the ICT GW allows to provide proper setpoints received from the application layer through the Actuation module to the HeadEnds able to support such kind of control.

Current section aims at describing the new modules, namely “Event Generation and Correlation” and “Security and Resilience”, implemented and integrated in the ICT GW to provide additional security and resilience functionalities.

3.2 Event Generation and Correlation

The role of Event Generation & Correlation (EGC) module consists in the processing of data coming from multiple sources, aggregated into events and representing specific occurrences in the considered environment.
Together with the functionalities provided by Security & Resilience module, the events are analysed based on models and rules (e.g., thresholds, time windows, relationships among entities). When the rules match, a set of predefined actions is triggered: they most often comprise the generation and insertion of the event into the database, as well as, where applicable and available, the invocation of actions and mitigations capable of automatically solving the detected/observed problem or alerting the user of the unwanted event through the GUI, to be noticed that the notification to the user is always presented through the GUI, as described in the next sections and shown in Section 3.2.

The EGC implementation has been previously foreseen to leverage Complex Event Processing (CEP) techniques; however, this idea has been discarded in order to not overload communications involving the ICT GW. In fact, it would have required capturing all the streams arriving to and coming from all ICT GW ports, and then analysing them in real-time searching for complex patterns and dependencies. The EGC, instead, generates events after being invoked by other components. Some of the modules that trigger the generation of an event are: Security & Resilience, Adapters, Application API, Core Logic, Adapter Registration module, Grid Topology Mapping, Observability Grid Model. In some cases, the triggering of EGC is timely performed, in real-time, as soon as some specific condition is met and discovered by any of the above-listed components. In the remaining cases, it is the S&R which periodically performs actions (e.g., ping request), reads the database and analyses the existing or missing information according to the rules and models.
Following sections describe in detail the undesired events (threats and hazards), their high-level description of consequences, their potential causes and the action/mitigation implemented to counteract it. The events identified are grouped based on the following categories:

- Anomaly in measurement
- Grid topology anomalies
- Authentication
- Outage of components
- Shutdown / Restart of the ICT GW
- Timestamp Error
- Not sufficient input
- SW manipulation
- Tampering

- Port scanning
- Anomaly in ICT resource usage

3.2.1 Anomalous or Missing Measurements

Anomalous or Missing Measurements category represents the events when anomalies occurred during the reception of measurements from the field. The anomaly is represented by either a measurement value out of a nominal range, or exceeding a threshold, or unexpectedly missing.

The first three events starting from top of Table 1 named *Voltage value equals to zero, Single phase zero voltage, Voltage imbalance* could theoretically be considered as sub-categories of the fourth one, namely *Anomalous value.* This mostly depends on how the valid range of values or thresholds are set in the configuration of S&R (e.g., whether 0 voltage is valid or not).

It is worth pointing out that detecting voltage imbalance is one of the purposes of applications on top, which use complex algorithms on a significant amounts of data, nevertheless the ICT GW is the first point of contact to collect measurand from the fields, therefore it is able to carry out a first data processing for detecting potential anomalous measures.

Regarding the last two events in Table 1, *missing phase* and *missing measurement*, it is worth to notice that one of the potential causes is the disconnection of the communication network between the ICT GW (in particular the adapter) and the HeadEnd. In fact, it may happen that some requests for measurements conducted by an adapter, or some of the corresponding responses provided by the HeadEnd, get lost because of connection issues. The same stands for phases, in case the requested measurements are of category voltage and the responses are divided by phase.

Table 1 - Events of Category Anomalous Measurements

Name	Description	Potential Cause	Action / Mitigation
Voltage value equals to zero	The ICT GW receives a sequence of measurement messages containing "Value": 0 and the related measuring device does not send any associated service message to report the issue	Disconnection e.g., of a cable from a measurement point	Alert to DSO: faulty device. Measurement from device not reliable.
Single phase zero voltage	ICT GW receives a measurement message containing "Value": 0 on a phase, while concurrent measurements, pertaining to the other phases of the same device, have a value different from zero	A phase imbalance may be caused by unstable utility supply, broken wires, failed fuses, damaged contacts.	Alert to DSO: Potential harm to transformer and/or electric equipment. Measurement from device not reliable.
Voltage imbalance	Inconsistent amplitude of three-phase voltage, amplitude difference surpasses the specified range. ICT GW receives a measurement message containing a value on a phase that compared with the measurements of the other phases of the same device, at the same instant of time, exceed the tolerable limit (e.g., +-5V or +-10V)	A phase unbalance may be caused by unstable utility supply, broken wires, failed fuses, damaged contacts.	Alert to DSO: Potential harm to transformer and/or electric equipment. Measurement from device not reliable.
Anomalous value	Security & Resilience module, monitoring measurements from the HEs, detects a potential anomaly: a measurement value exceeds a threshold or is out of a valid range.	Data Collection System Outage. Wire disconnection e.g., of a cable from a measurement point. Data Corruption. Interference.	Alert to DSO: Measurement from device not reliable.

Name	Description	Potential Cause	Action / Mitigation
Missing phase	Security & Resilience module, monitoring measurements from the HEs, detects a potential anomaly: the number of phases does not correspond to what known in adapter registration	Disconnection of the communication network between ICT GW and HE. Crash of device. Headend fault.	Measurement from device not reliable. Automatic attempt to retrieve the missing value Alert to DSO: Missing voltage phase. Measurement from device not reliable.
Missing measurement	Security & Resilience module, monitoring measurements from the HEs, detects a potential anomaly: one of the expected measurements is not received.	Disconnection of the communication network between ICT GW & HE. Crash of device. Headend fault.	Measurement from device not reliable. Automatic attempt to retrieve the missing value Alert to DSO: Measurement from device not reliable.

3.2.2 Anomalies in Grid Topology Mapping

Anomalies in grid topology mapping represents the events when anomalies occurred during the mapping between measurement devices and grid nodes (e.g., a measurement device sending data is not mapped to a grid node; a grid node marked as measurement device is not present in the HE's capabilities).

Table 2 - Events of Category Anomalous Grid Topology Mapping

Name	Description	Potential Cause	Action / Mitigation
Unmappable measurement device	A new device not present in HE's capability during adapter registration, starts sending measurements and it is not mapped with any grid node or cable.	Corruption of data. Wrong processing of data.	Alert to DSO: grid topology not updated. The new device is flagged as not trustable. Automatic triggering of GTM.

3.2.3 Authentication and Registration Errors

Authentication and Registration events pertain to all the situations where authentication/registration failures occur during authentication/registration with a HE or during the authentication of an Application.

To be noticed that in the current solution the generation of events *Failure in authentication* and *Sequence of Failures in authentication* is only implemented for the Inverter HE, since it is the only case where the authentication is performed on the ICT GW side, while in the other cases the authentication is performed at the HEs, where ICT GW does not have the responsibility.

Table 3 - Events of Category Authentication and Registration

Name	Description	Potential Cause	Action / Mitigation
Failure in authentication	An adapter cannot authenticate with the HE using the right credentials, and receives a response from HE indicating it, i.e. an invalid Access Token	Simultaneous use of the same credentials. It may indicate that some entity, other than ICT GW, is trying to access the HE. Credential theft.	Alert to DSO: simultaneous use of credentials. Automatic attempt to retrieve the missing measurements (if any).

Name	Description	Potential Cause	Action / Mitigation
Sequence of failures in authentication	An adapter cannot authenticate with the HE using the right credentials after multiple attempts, and receives a sequence of responses from HE indicating it, i.e. an invalid Access Token	Credential theft. It may (indirectly) indicate a loss of measurements / events and risk of ongoing attack	Alert to DSO: Credential theft and measurements not collected. Automatic attempt to retrieve the missing measurements (if any).

3.2.4 Outage of Components

Outage events are related to the outage either of the overall HE, or of a single device belonging to a HE, or of internal modules of the ICT GW, or of Net2DG subsystems other than ICT GW (e.g., DataBase, Applications, OGM).

Regarding the *Data collection system outage* event, it may happen (as in the case of the Inverter HeadEnd), that some secondary entity is involved in order to manage the data collected from the devices and to deliver it to the HeadEnd itself; when an outage occurs to that entity, e.g., a loss of AC supply, it can be reflected in the measurement response provided by the HeadEnd to the Adapter as a *"Value": null* message.

Table 4 - Events of Category Outage

Name	Description	Potential Cause	Action / Mitigation
Data collection system outage	ICT GW receives a measurement message containing "Value": null, while no concurrent Event related to this situation, in the same interval, is found	- Data Collection System Outage. - Outage of AC at the measurement device.	Alert to DSO: suspected outage.
Measurement device unreachable	A known device, already available to the HE's during adapter registration, has now stopped sending measurements.	- Disconnection of the communication network between ICT GW and HE. - Device offline	- If device is offline, it could be flagged in the database. - if there is no answer or it is not possible to check the status of the device, retry to retrieve missing measurements. After a number of attempts an alert to the DSO has to be sent and the device has to be flagged as non-responsive.
Not-responsive component	A component is invoked but not responding, either: - internal to the ICT GW, or - external, e.g., OGM, applications, DB, REST API (Http client status request), Web Socket Server	- Network Communication between ICT GW and HE. - Server failure.	Alert to DSO about specific component.

3.2.5 Shutdown or Restart of Components

This category of events pertains to both intentional and unintentional (crash) shutdown of the ICT GW. As shown in Table 5, when an ICT GW *controlled shutdown* occurs, it means that ICT GW has been intentionally shut down by the user. There are procedures planned to be executed just before closing, and one of them is the generation of *a ICT GW controlled shutdown* event and its insertion into the database, so that, as soon as ICT GW is up and running again, this event can be distinguished from unexpected terminations. For the latter, no events are persisted into the database, while a more sophisticated action is required, including also the involvement of Security & Resilience and of a dedicated external component (more details are in Section 3.3).

Table 5 - Events of Category Shutdown or Restart of Components

Name	Description	Potential Cause	Action / Mitigation
ICT GW controlled shutdown	The ICT GW execution is terminated by the user in a controlled way.	Intentional shutdown	Planning of procedures to be executed just before closing, to allow restoring it at restarting.
ICT GW unexpected shutdown	ICT GW API (e.g., REST) is not responding	- Unexpected shutdown - Disconnection from the communication network	External component (Security & Resilience) periodically contacts the ICT GW to timely detect the event. It directly alerts the DSO through the GUI.

3.2.6 Events for Future Developments

In addition to the hazardous events described and addressed in previous section, further events with lower risk have been identified and described in Table 6. In fact, after a prioritization analysis, considering criteria as criticality from points of view of security and DSO needs, they have been considered currently not necessary, but still they may be studied in the future at least as a research topic.

Table 6 - Additional Events with Lower Risk

Name	Description	Potential Cause	Action / Mitigation
Error in registration	For some reason, i.e. payload is not valid: - a HE cannot register itself with an adapter, or - an adapter cannot register with the ICT GW	Data Corruption	Alert to DSO: HE/Adapter not registered. Automatic attempt of new registration.
Unauthorized authentication attempt	Unauthorized authentication attempt by an application	Cyber attack	Alert to DSO: cyber-attack attempt. Application temporary blocked.
Timestamp Error	Suspected timestamp error is detected by monitoring clock accuracies of data subsystems (HEs)	Time zone is misaligned	Alert to DSO: potential misalignment of timestamps
Not Sufficient Input	A component (e.g., OGM) cannot be executed successfully due to incorrect input	Not sufficient amount or erroneous type of input data	Alert to DSO: incomplete amount of data for elaboration
SW code modification	Security & Resilience module detects an intentional software code modification, i.e. at the adapter layer, based on MD5 The detection can be based on the extraction of the code related to the running services from the relative Java Archive (JAR) file and evaluating its MD5 signature.	Malicious code modification.	The signature is compared with a genuine signature stored in a protected area of the Security & Resilience and if necessary, returns the name of the corrupt service allowing an easy software recovery.
Smart meter tampering	Registration of magnetic field detection and meter cover tampering. Any registration can be accompanied by indication in the display. This indication can be configurable to be temporary (i.e. it disappears when the source to tamper disappears), or permanent until a tamper release command is received either from a smart metering system or by activating the sealable push-button.	Intentional tampering	Smart meter flagged as not trustable
Port Scanning	A number of connection requests is carried out on each port to identify the open ones and subsequently carry out an attack e.g., a DoS.	Cyber attack	Alert to DSO: cyber-attack attempt

Name	Description	Potential Cause	Action / Mitigation
Anomaly Detection of ICT Gateway Resources	In case of ICT GW overloaded resources its nominal behaviour can be compromised both in terms of execution times and in terms of correctness of the elaborated data. Relevant resources that can influence the correct behaviour of the ICT GW or that can be a symptom of any SW/HW fault or malicious attack occurring are the CPU and the RAM.	SW Fault HW Fault Cyber attack	Continuous monitoring of resource in order to be able to intervene promptly with maintenance or recovery actions.

3.3 Security & Resilience

Security & Resilience (S&R) directly interacts with Event Generation & Correlation (EGC), implementing fault & attack detection mechanisms to provide security, resilience and robustness. The main functionalities offered by these two modules are the identification of anomalies in the ICT network and in the measurement devices, with the final purpose of detecting potential faults or attacks occurring both in the ICT infrastructure and at HE levels, by analysing the format and the syntax of the messages exchanged. Anyway, a preliminary analysis of the measures with respect to reference thresholds where possible, is also performed by the S&R module in order to provide a quick alert to DSO through the GUI.

As shown in Figure 2, S&R has been implemented as an external and standalone software module with respect to the ICT Gateway, this solution allows to monitor the ICT GW and detect whether it is not working anymore. For example, in case of an unexpected shutdown of the ICT Gateway (event briefly described in Table 5), all its components would be terminated as well, and having the S&R as an external component would allow to detect such an event and trigger the proper mitigation action. The S&R interacts and monitors the ICT GW through the Service Layer being the interface with external modules.

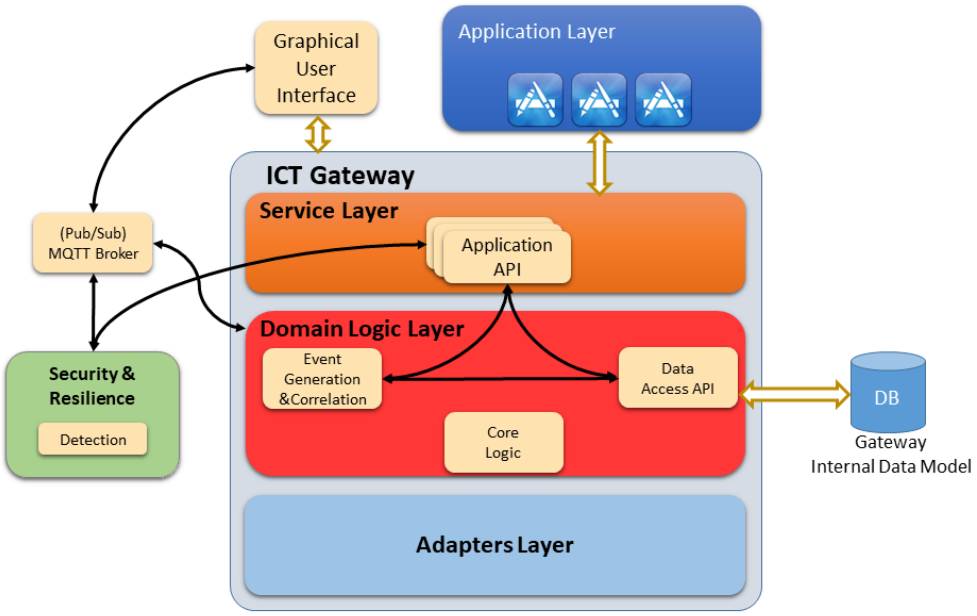

Figure 2 - Architecture and Data Workflow between Security & Resilience, ICT Gateway and the User (GUI)

Security & Resilience periodically communicates with ICT GW over the REST Application API exposed by the Service Layer. Through this channel, it interacts with EGC and Data Access API in order to retrieve the information necessary for anomaly detection and real time fault and attack analysis.

3.3.1 ICT GW Unexpected Shutdown

In case of occurrence of *ICT GW unexpected shutdown*, the ICT GW has been terminated unexpectedly, hence it is not responding to any request, and it is refusing all the connection attempts. Thus, the S&R needs to alert the user and in order to do so, a different path is necessary. As indicated in Figure 2 and Figure 3, an MQTT [4] broker has been selected for this purpose: using a publish/subscribe paradigm, S&R publishes on a dedicated topic[1] a message reporting the *offline* status of ICT GW. The GUI, or in general any authenticated subscriber of the topic, is timely informed of the occurrence and an alert is shown to the user. In case of regular behaviour, the S&R module periodically pings[2] the ICT GW, receives a response and publishes *online* on the *ict-gateway* MQTT topic.

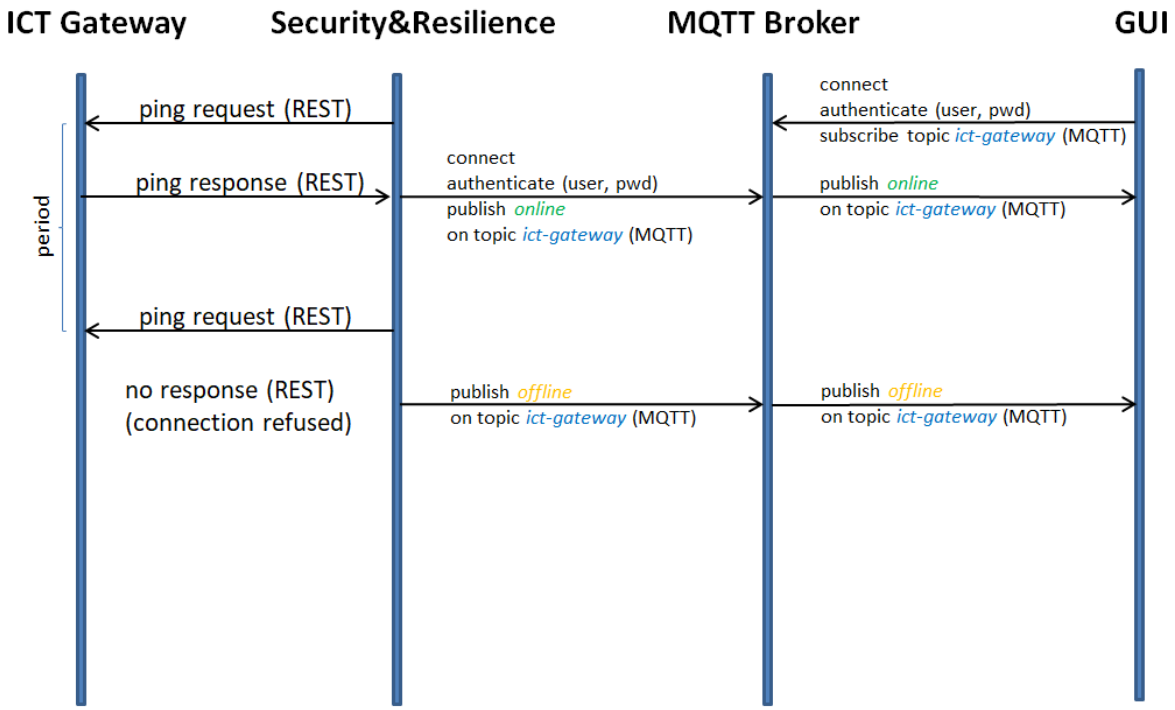

Figure 3 - Interactions when ICT GW is running (top) or in occurrence of *Unexpected Shutdown (bottom)*

As explained in Section 3.2, this event can be easily distinguished from a *ICT GW controlled shutdown*: the latter is persisted into the database, while the ICT GW *unexpected shutdown* does not cause the insertion of any event. Anyway, for both *ICT GW controlled shutdown* and *ICT GW unexpected shutdown* the *offline* message could be published on the MQTT topic: for the *ICT GW controlled*

[1] *ict-gateway*, as shown in Figure 3.

[2] The ping is currently implemented as a request/response service provided by the REST Application API on the Service Layer.

shutdown, it may occur if the S&R pings the ICT GW during an intentional reboot of the ICT Gateway, and thus when it is temporarily unable to send the response.

It is important to notice that both the *ICT GW controlled shutdown* and *ICT GW unexpected shutdown* events have been introduced because of their usefulness in understanding when there is a potential need to retrieve possibly missing measurements and events. They provide, with a slight difference, information regarding the precise moment starting from which the retrieval has to be attempted. As soon as the ICT GW is restarted, it verifies the existence of an *ICT GW controlled shutdown* in the DB:

- if it is present, ICT GW starts retrieving measurements/events from the *ICT GW controlled shutdown* event timestamp (information stored into the database)
- if it is not present, an *ICT GW unexpected shutdown* is supposed to be happened; thus, the ICT GW attempts retrieving measurements from the timestamp of the last measurement existing in the DB (where appropriate, incremented by an interval depending on current configuration, e.g., 15 minutes, that corresponds to the time difference of two consecutive retrieval attempts normally performed by the ICT GW). If no measurement exists in the DB, the current run is the first run of ICT GW, thus the retrieval starts from current timestamp (as in the default setting).

4 Description of New Modules

This section describes in detail the set of modules that have been designed, integrated into the ICT GW and added to the overall Net2DG solution, as continuation of Task T3.2 and main contribution of Tasks T3.3 and T3.4. A brief introduction to those components has been already given in D3.2 [3], although their status was under design or development at the time of delivering the document.

Fault and Attack detection mechanisms to provide security, resilience and robustness (with respect to, e.g., failure of devices, lack of communication, cyber-attacks) are implemented in the Net2DG ICT Gateway mainly through the Security & Resilience module and the Event Generation and Correlation module. The functionalities of these two modules aim at identifying anomalies in the ICT network or in the electric grid and to detect faults/attacks correlating such anomalies through the knowledge of the underlying subsystems. In order to support these modules and to make the entire solution more robust, further modules not foreseen in the scope of the Work Package 3 have been integrated with the ICT GW, requiring also additional activities of code implementation accordingly to the design from WP2, namely the Observability Grid Model, which provides an estimation and a validation of data when they are not available from the field and the Graphical User Interface through which the user can interact with the entire Net2DG solution (ICT GW and Applications) and also be notified of any problems that are occurring.

4.1.1 Observability Grid Model

Observability Grid Model (OGM), is used to calculate electrical parameters for the grid observability applications (e.g., calculate voltage values for all grid nodes in the LV topology) as well as to estimate and complement missing data (cable lengths and types, loads, etc.) as described in D2.1 [5] and D.2.2 [6]. When an application sends a request for voltage/current value for a specific 15 min. time interval to the ICT Gateway and the ICT Gateway does not have the requested values, it triggers OGM. Thus, the ICT Gateway (client) calls the OGM (server) to obtain electrical values for the LV grid.

It is worth mention that the OGM has been designed in the context of WP2, while in the context of WP3 it has been integrated in the overall SW framework, also requiring additional code implementation.

The input from ICT Gateway includes: **(a)** impendence matrix Z, **(b)** voltage vectors – one per phase, **(c)** current matrices – one per phase, **(d)** power measurement vectors – one per phase and vector of contractual power limits. Based on this input, OGM calculates operational parameters (e.g., voltages, currents) and detect faulty measurements and incorrect grid topology data. Consequently, as a response to ICT Gateway, OGM forwards: **(a)** voltages without missing values, **(b)** currents without missing values as well as **(c)** power measurements for all consumer and generator nodes.

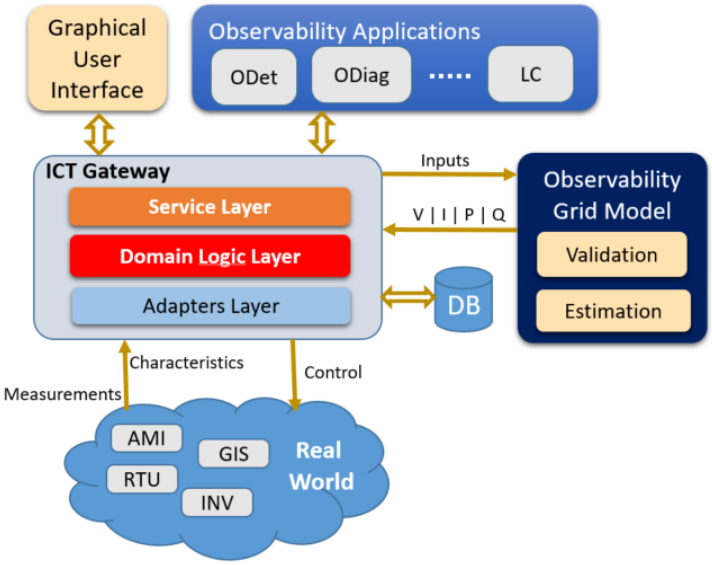

Figure 4 - Architecture and Data Workflow between Observability Grid Model and ICT Gateway

It is worth to mention that OGM is built based on various information sources available at DSO level. Typically, the information available to characterize a given distribution grid is available in various formats and databases that is collected by the ICT Gateway via data fusion. This model is the basis for supporting the observability applications taking into account the information available but also considering some feasible technical assumptions when information is missing (for details, see D2.1 [5]).

4.1.2 Grid Model API

Grid Model API, in contrast to the Observability Grid Model which is a standalone service, is a part of ICT Gateway service layer and thus it provides an access to the OGM for the external clients, e.g., various applications that utilize ICT Gateway.

Moreover, Grid Model API encompasses two modules inside ICT Gateway:

- An interface towards the external clients, e.g., GMon application that is interested in calling OGM Server, and
- OGM Client that communicates directly with OGM Server.

Interface toward the external clients is required because the clients, e.g., GMon application, cannot call OGM Server directly because they are lacking information contained in ICT GW. Moreover., this interface is implemented as HTTP REST Service that interacts with OGM Client which then triggers OGM execution. REST Service is parameterized GET service that expects the following parameters from a client:

- fromDate – denotes start interval for grid calculations performed by OGM Server,
- toDate – denotes end interval for grid calculations performed by OGM Server and
- topologyId – specifies a topology that will be fed to OGM Server.

The above listed parameters are required for an application, e.g., GMon, that calls the API. Received parameters are utilized when communicating with OGM Client which does the following:

- retrieves from ICT GW database all measurements for the specified topology and within provided time intervals,
- retrieves all the nodes and cables for the specified topology,
- processes existing measurements and maps them to extracted time intervals and topology nodes – voltage, active and reactive power, active and reactive energy,
- it packages processed data into a JSON message and sends it to OGM Server,
- receives result, a JSON message, from OGM Server and
- returns aggregated result to the external client that sent a request to HTTP REST API.

The above described workflow implies extensive database querying which is circumvented by implementing complex queries that do both, reduce database interaction and increase OGM Client performances. In future release, OGM Client will be enhanced to persist data received from OGM Server.

4.1.3 Actuation

The Actuation module is in charge to handle the interactions with coordination control design undertaken in WP4, which takes place in the Automated Voltage Regulation (AVR) application (at Application Layer) in order to exploit actuation capabilities (where existing in the field) to achieve better voltage quality in the electrical grid.
Figure 5 shows the high-level sequence diagram that involves both the AVR application and the ICT GW (its Actuation module), as well as all the other components and sub-systems involved in the actuation process.

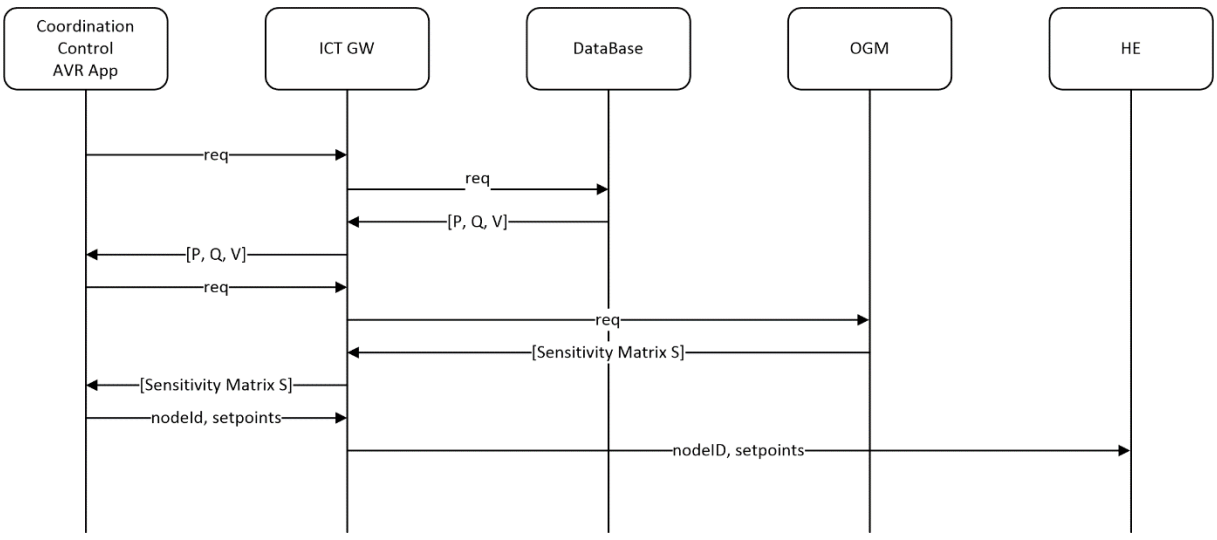

Figure 5 - Sequence Diagram of Actuation

In order to realize this last major feature to be provided by ICT GW to support for actuation capabilities, it is required to extend the following:

- OGM Server, and
- ICT GW.

In particular, the OGM Server has to be extended with the following functionalities:

- Make a sensitivity matrix available to OGM Client in ICT GW,
- Adapt the sensitivity matrix in a way that it holds information about grid node Id received from OGM Client,
- Package the sensitivity matrix in a Json message, and
- Extend the REST API with GET method to support OGM Client in obtaining the matrix.

Moreover, the ICT GW has to provide the following functionalities:

- Extend the existing REST API with the following two methods:
    - A method for getting the sensitivity matrix for a specified topology Id, and
    - A method for receiving setpoints.
- Actuation model that is responsible for the following:
    - Receiving setpoints,
    - Based on grid node Id in setpoints look up for a device,
    - Check if device supports RW mode,
    - Look up for a headend and an adapter that server the device,
    - Forward the setpoints to the adapter and
    - Adapter forwards the setpoints to the responsible headend.

As part of interaction and integration with WP4 activities, this module, which is supposed to handle the interactions with actuation subsystems (through Headend), will be implemented and integrated, in the overall solution, in the context of WP4 activities and tested within WP5 in order to fully meet field trial requirements.

4.1.4 On Demand Data Request

This module allows any application to directly access data (on demand) from any of the HEs through the ICT GW. An Application (e.g., ODet, ODiag) sends a data request to ICT GW through the Application API by providing its ID, the topology ID, a specific ID for a Grid Element as well as the relevant data type. The Application API forwards the request to Core Logic, which is then forwarded to the relevant Adapter. The requested information, which is used by the application for further elaboration is not stored in the database, while they are immediately sent to the involved application.

4.1.5 Graphical User Interface

Graphical User Interface (GUI) allows the DSO operators to interact with the Net2DG system by providing input and output for both the Applications and the ICT GW functionalities. Following sections describe the main features of the GUI with some examples and the description of related architecture.

4.1.6 Load topology map

The DSO topology map is automatically loaded when the user accesses to the GUI application using the browser, as shown in Figure 6. In particular, all grid Nodes and Cables are rendered on a base map layer without other POIs (Point Of Interest).

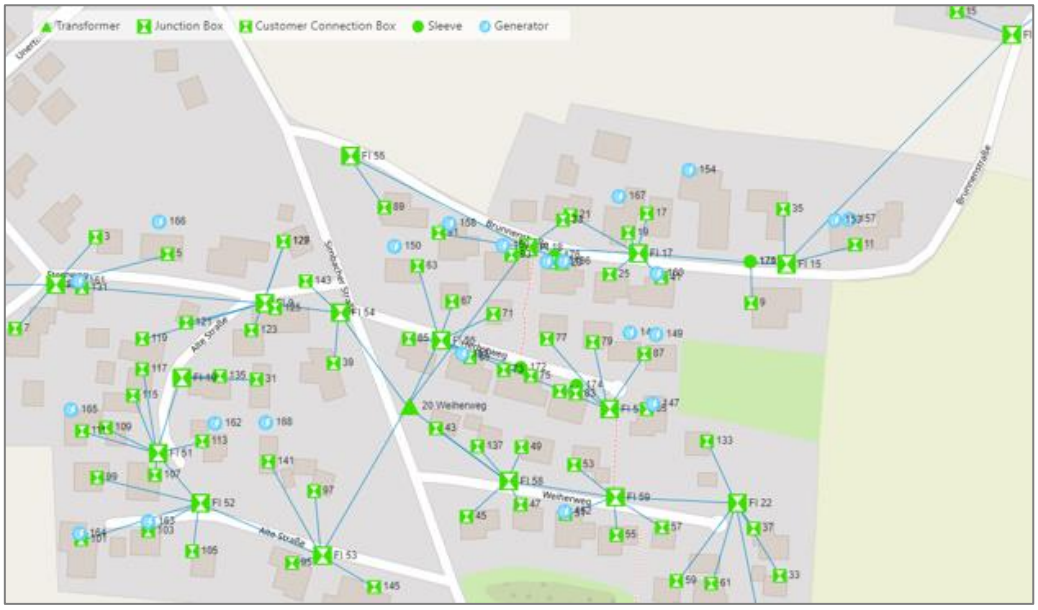

Figure 6 - DSO Topology Map

4.1.7 Show/Hide cables

The Show/Hide cables feature (see Figure 7) allows the user to show or hide the topology cables clicking on the button in the upper right corner of the screen, with the results shown in Figure 8 and Figure 9.

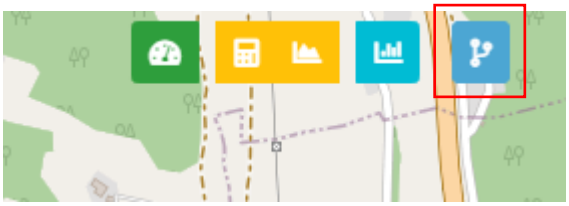

Figure 7 - Show/Hide Cables

Figure 8 - Topology Map with Cables

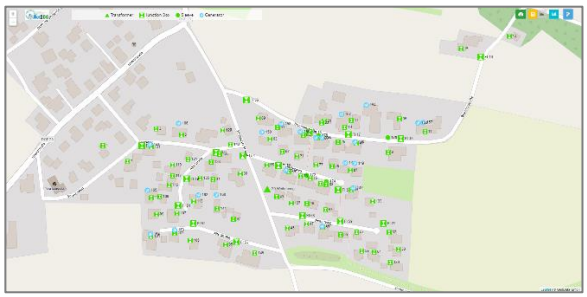

Figure 9 - Topology Map with Hidden Cables

4.1.8 Grid Monitoring (GMon)

The GMon application is executed by the DSO, who specifies through the GUI interface a LV grid area (by a trafo ID) and a time interval [t1, t2] in the past (e.g., one past month) and then uses measured or OGM-calculated average voltage values over 15min intervals (lumped 3-phase value for each grid node and time interval) in order to provide outputs [6].

Figure 10 represents actual sequence diagram involving the GMon application, the ICT GW and the GUI in order to describe the GMon workflow.

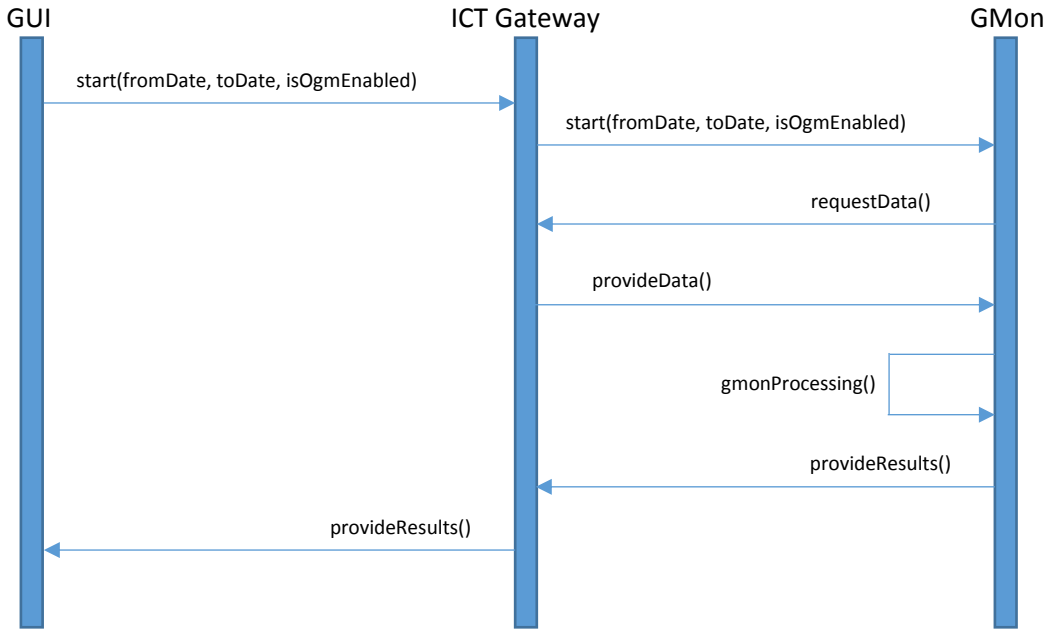

Figure 10 - GMon Workflow

In order to start the Grid Monitoring application, the user has to open the Grid Monitoring dialog by clicking on the green button on the upper right corner (Figure 11).

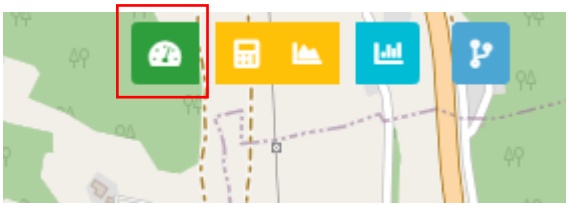

Figure 11 - GMon Execution

When the dialog is shown, the user has to specify a date range in the past on which the GMon application will run, and if the OGM calculation has to be enabled or disabled (see Figure 12).

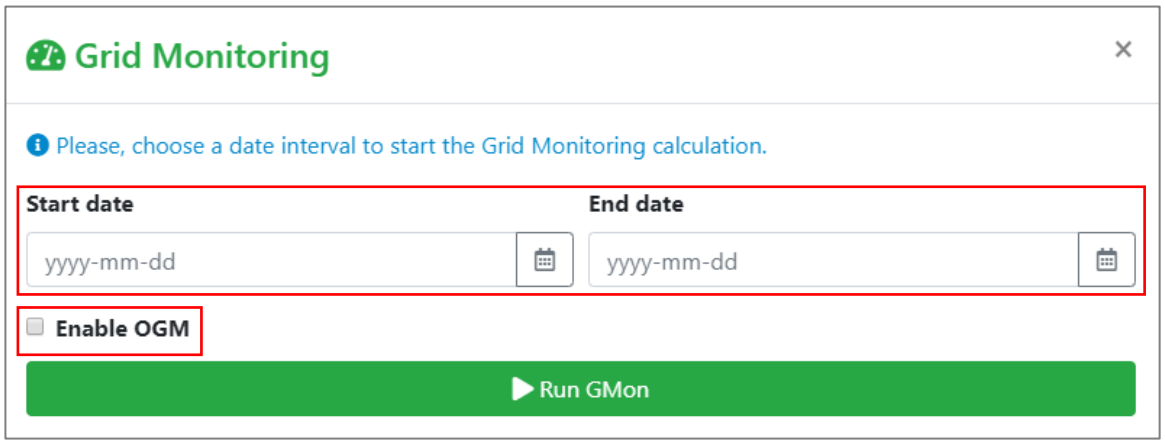

Figure 12 - GMon Execution Dialog

After the GMon successful running, Nodes and Cables on the map are coloured in red or yellow to identify warning (yellow) or critical (red) situations (if any), as show for example in Figure 13.

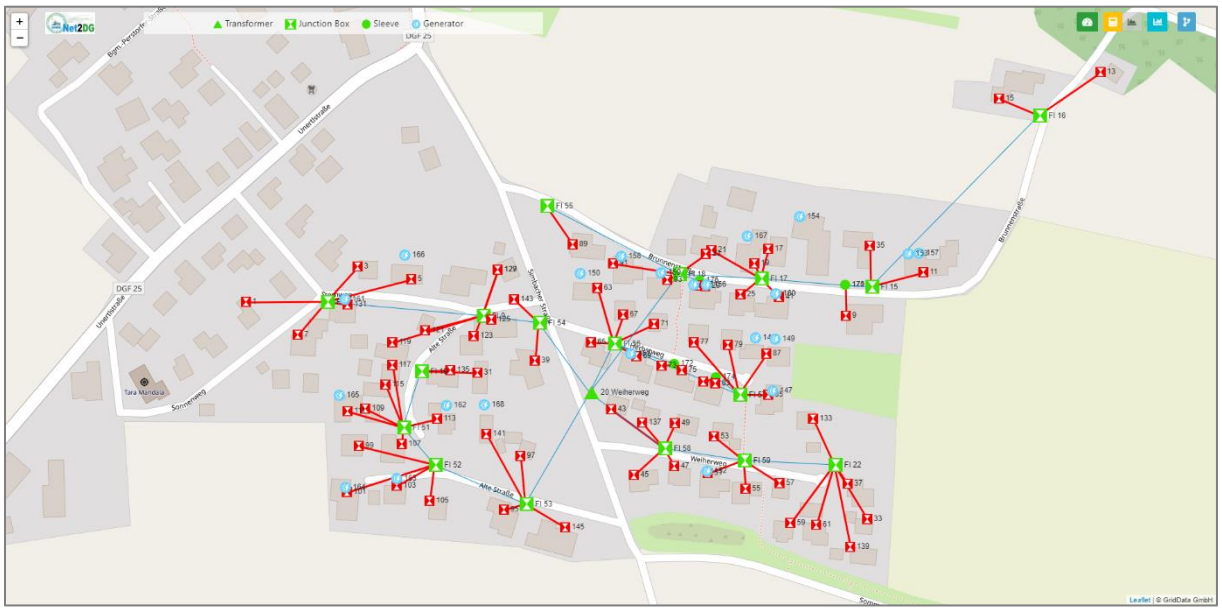

Figure 13 - GMon Violations

The User can see detailed GMon results by clicking on a specific node or cable on the map.
Figure 14 shows an example of Node Voltage view in the selected date range, when the user clicks on a node (in this case node 3), the Lower 10% quantiles, the Upper 10% quantiles and the Voltages are show in the graph.

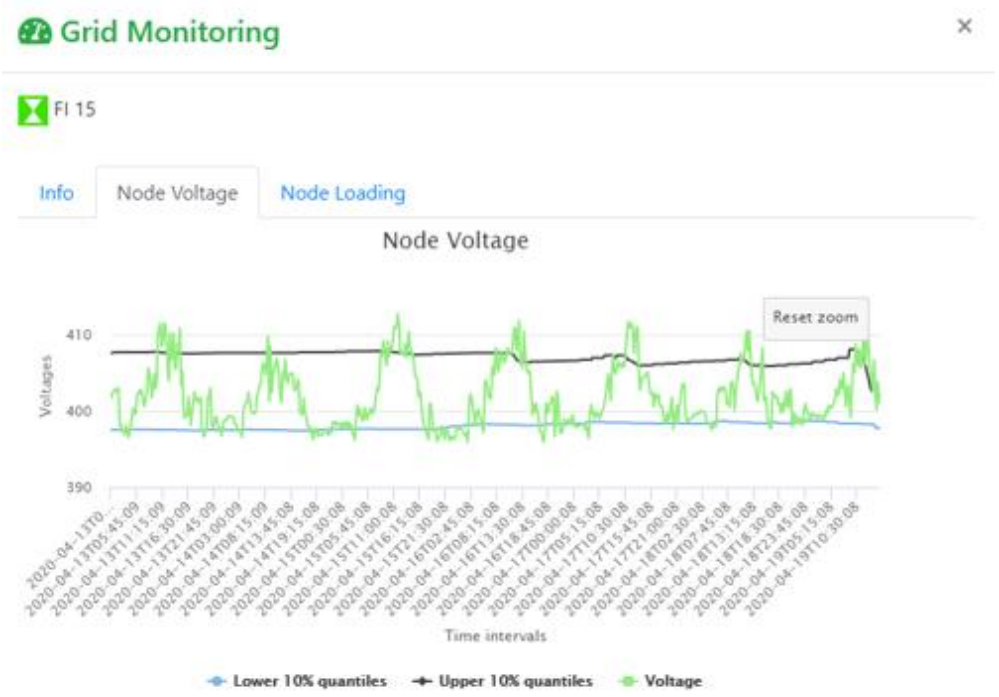

Figure 14 - GMon Node Voltage Results

Figure 15 shows an example of cable Feeder Voltage, when the user clicks on cable, the source and destination node are shown together with all the nodes from that cable to the feeder; for all the nodes in the left Y axis are reported the Max upper quantile, the Min lower quantile and the Average in Voltages, while in the right Y axis are reported the number of violations.

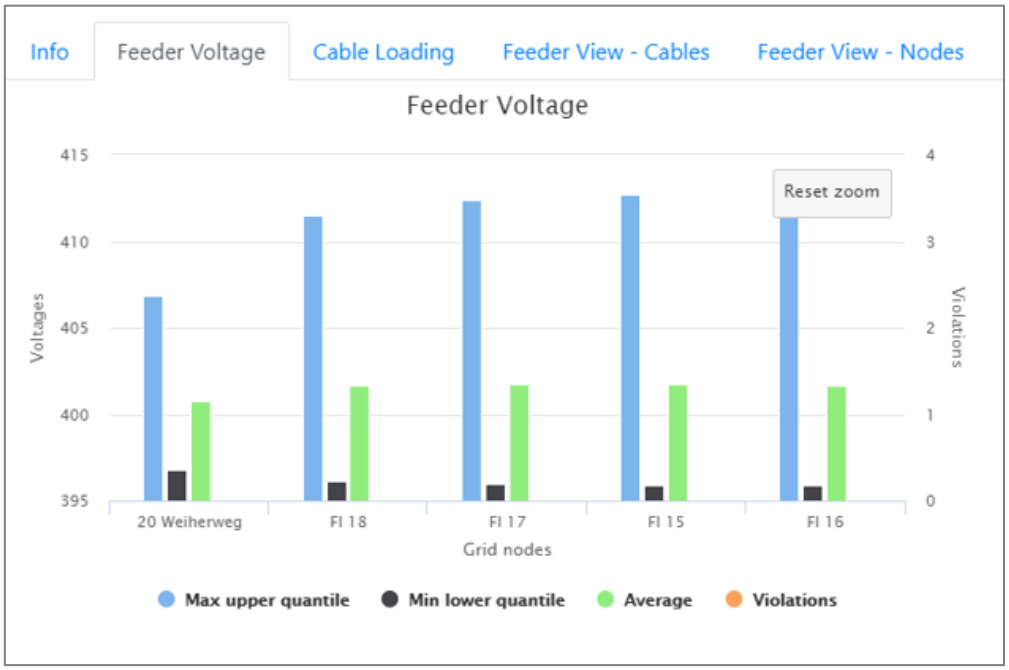

Figure 15 - GMon Cable Feeder Voltage Results

4.1.9 Losses Calculation (LC)

The Losses Calculation (LC) application is executed by the DSO, who specifies a LV grid area (by a trafo ID) and a time interval [t1, t2[in the past (e.g., 'last month') and then uses measured or OGM-calculated average power values over 15min intervals (lumped 3-phase value for each grid node and time interval) in order to provide output [6]. Figure 16 shows the workflow of LC application involving GUI, ICT GW and LC.

Figure 16 represents actual sequence diagram involving the Losses Calculation application, the ICT GW and the GUI in order to describe the LC workflow.

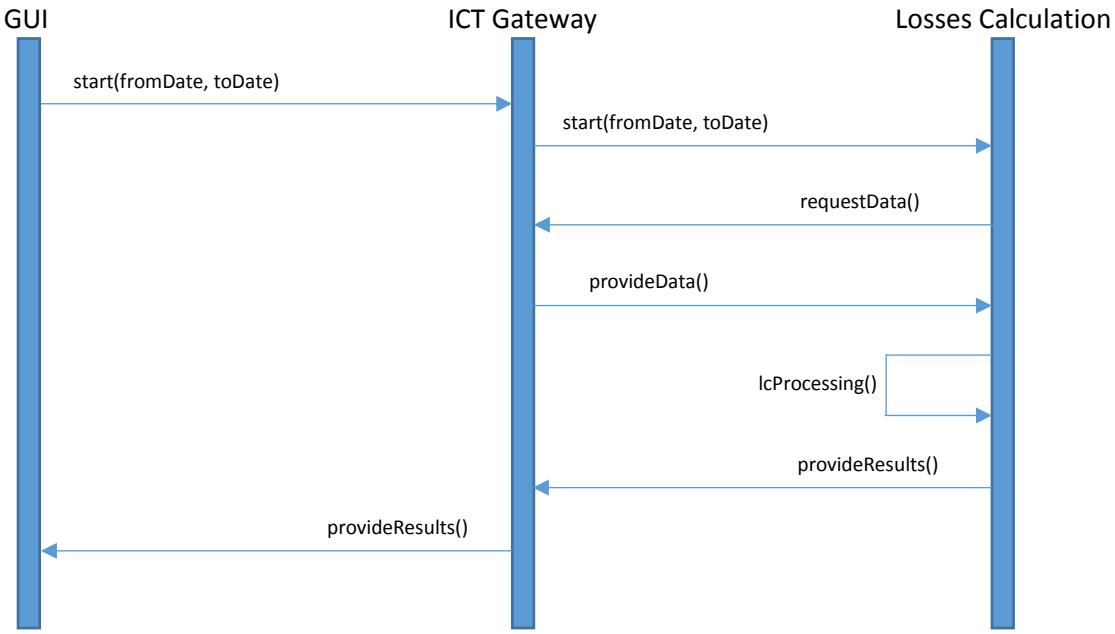

Figure 16 - Losses Calculation Workflow

In order to start the Losses Calculation application, the user has to open the Loss Calculation dialog by clicking on the orange button on the upper right corner (see Figure 17).

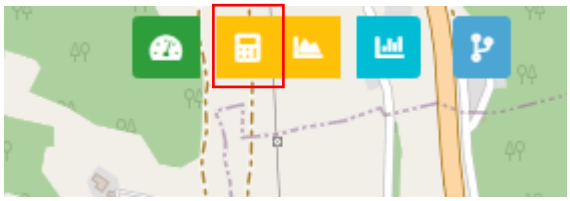

Figure 17 - Loss Calculation Execution

When the dialog is shown, the user has to specify a date range in the past on which the Losses Calculation application will be executed (see Figure 18).

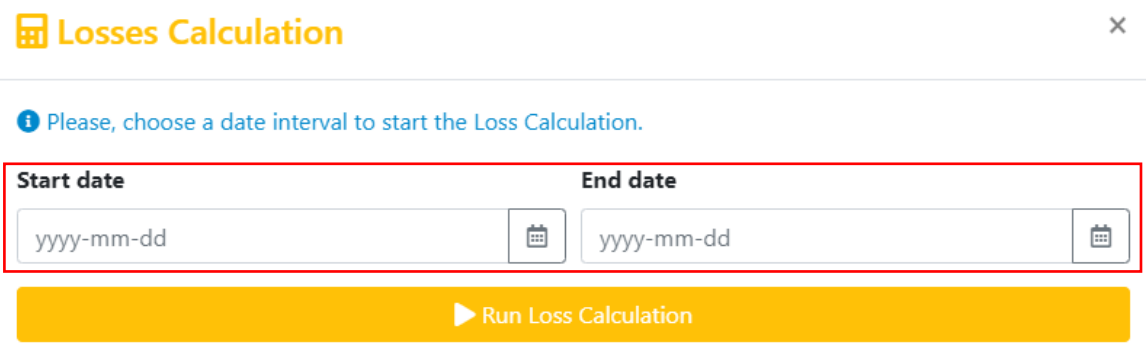

Figure 18 - Losses Calculation Execution Dialog

At the end of the Loss Calculation processing, the results will be available by clicking on the orange button on the upper right corner of the screen (see Figure 19).

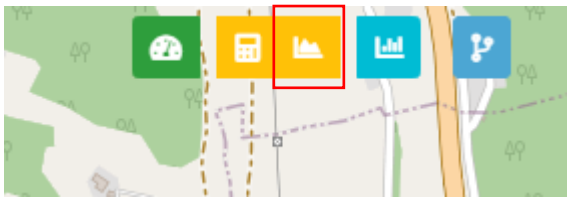

Figure 19 - Losses Calculation Results

Figure 20 shows both the Active and Reactive energy losses as result of the LC application run in the selected date range.

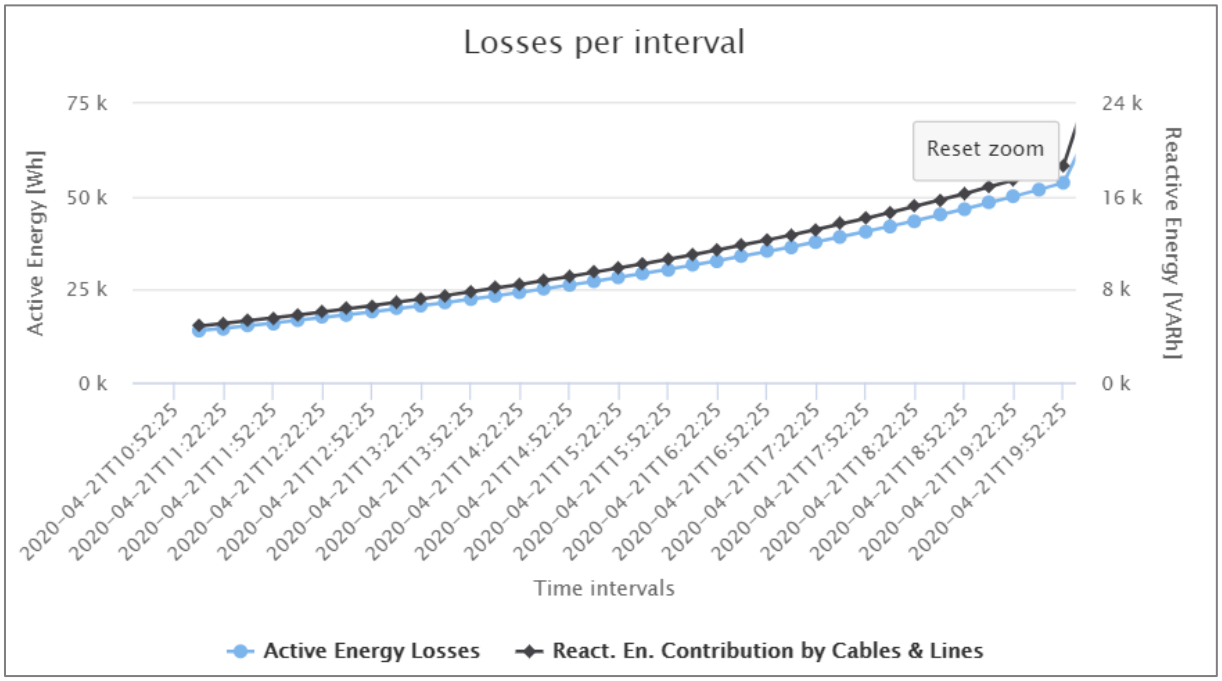

Figure 20 - Losses per Interval

Figure 21 shows both the Active and Reactive energy as result of the LC application run in the selected date range.

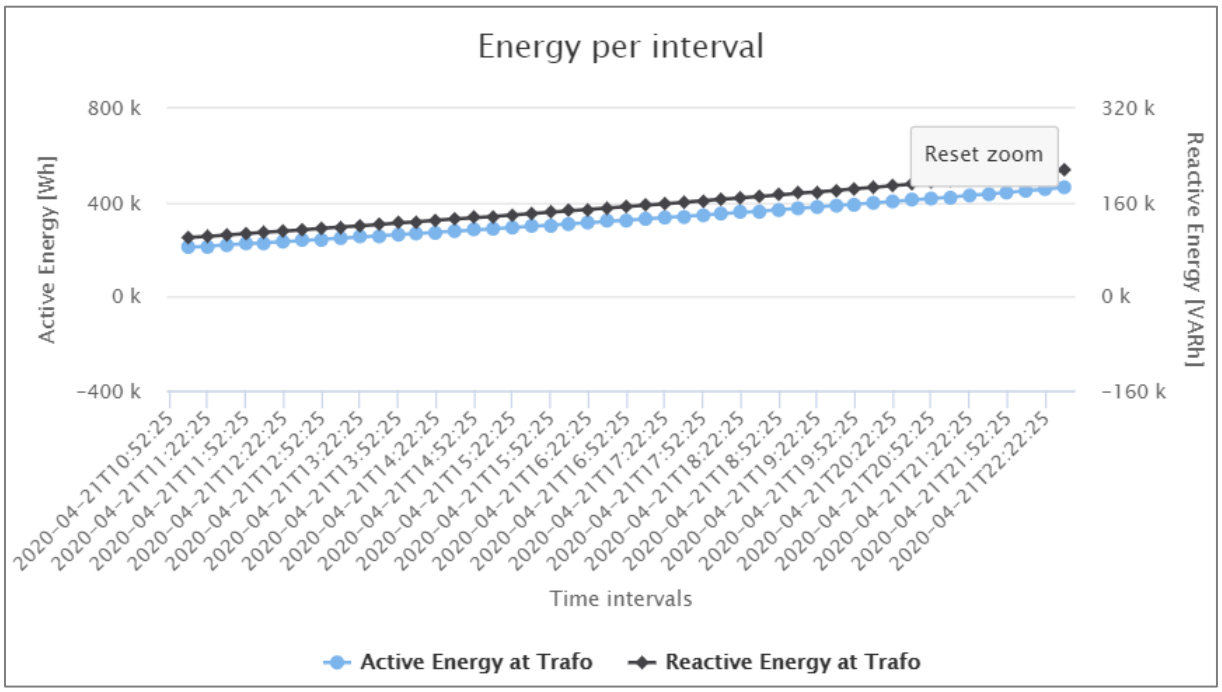

Figure 21 - Energy per Interval

Figure 22 shows both the Active and Reactive energy relative losses as result of the LC application run in the selected date range.

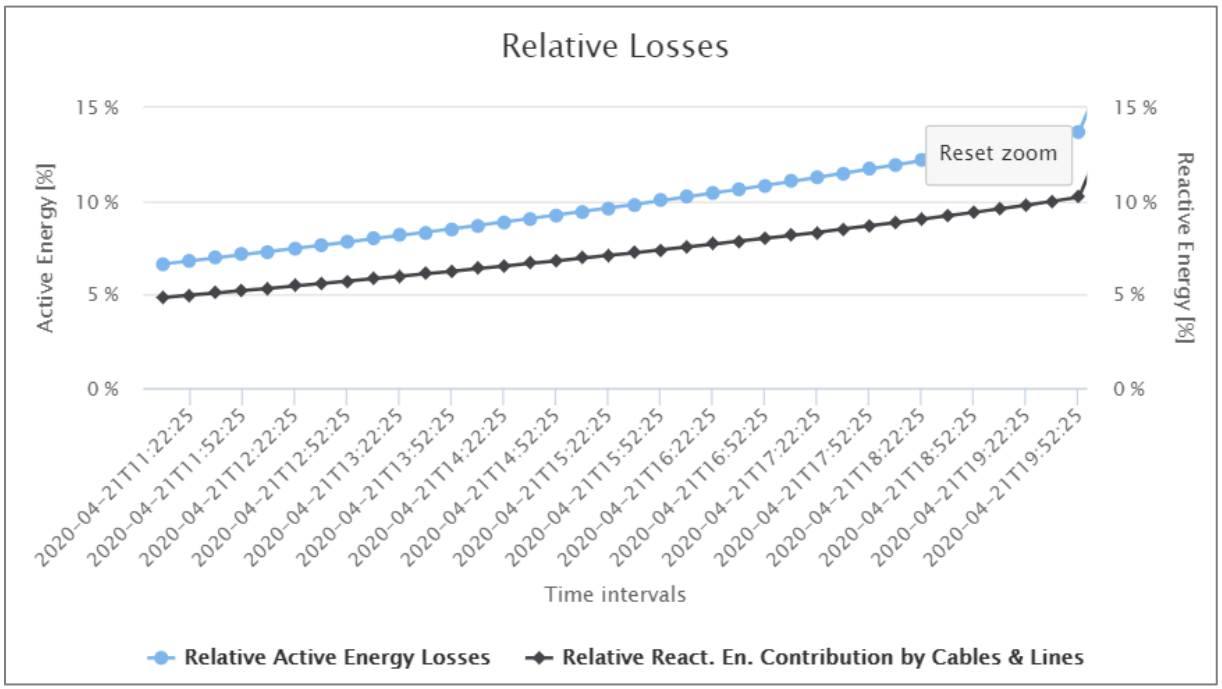

Figure 22 - Relative Losses

Figure 23 shows both the Accumulated Active and Reactive energy losses, respectively in the left Y axis and right Y axis, as result of the LC application run in the selected date range.

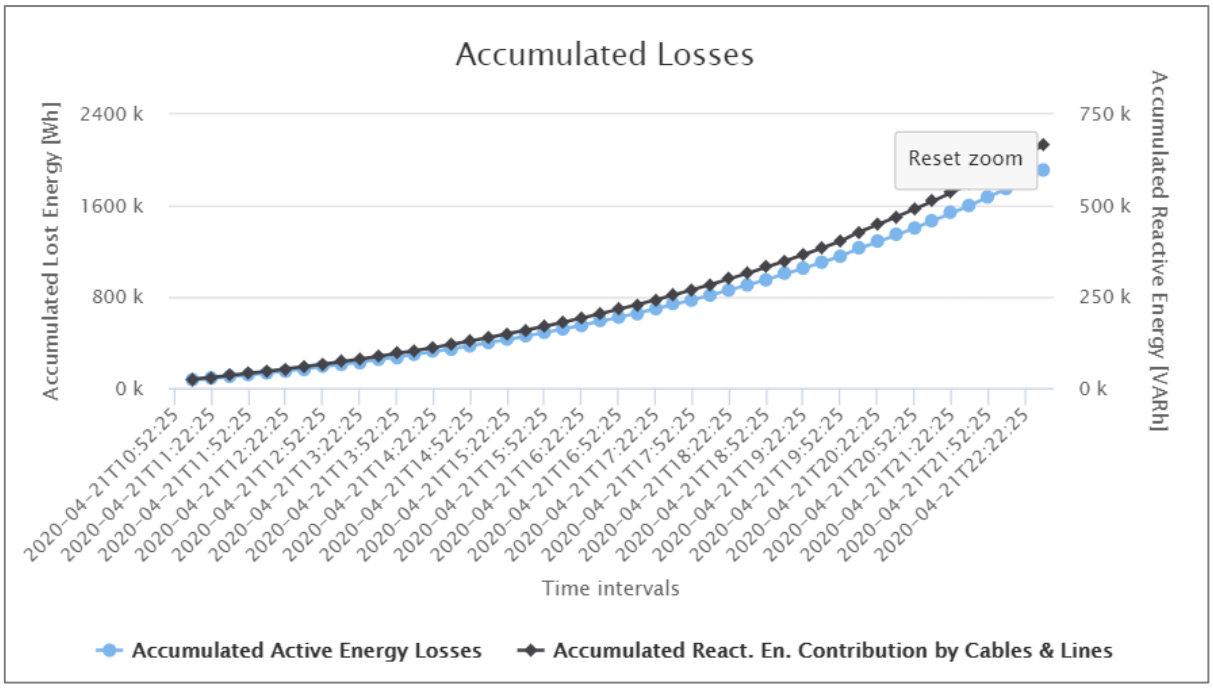

Figure 23 - Accumulated Losses

Figure 24 shows both the Accumulated Active and Reactive energy at Trafo, respectively in the left Y axis and right Y axis, as result of the LC application run in the selected date range.

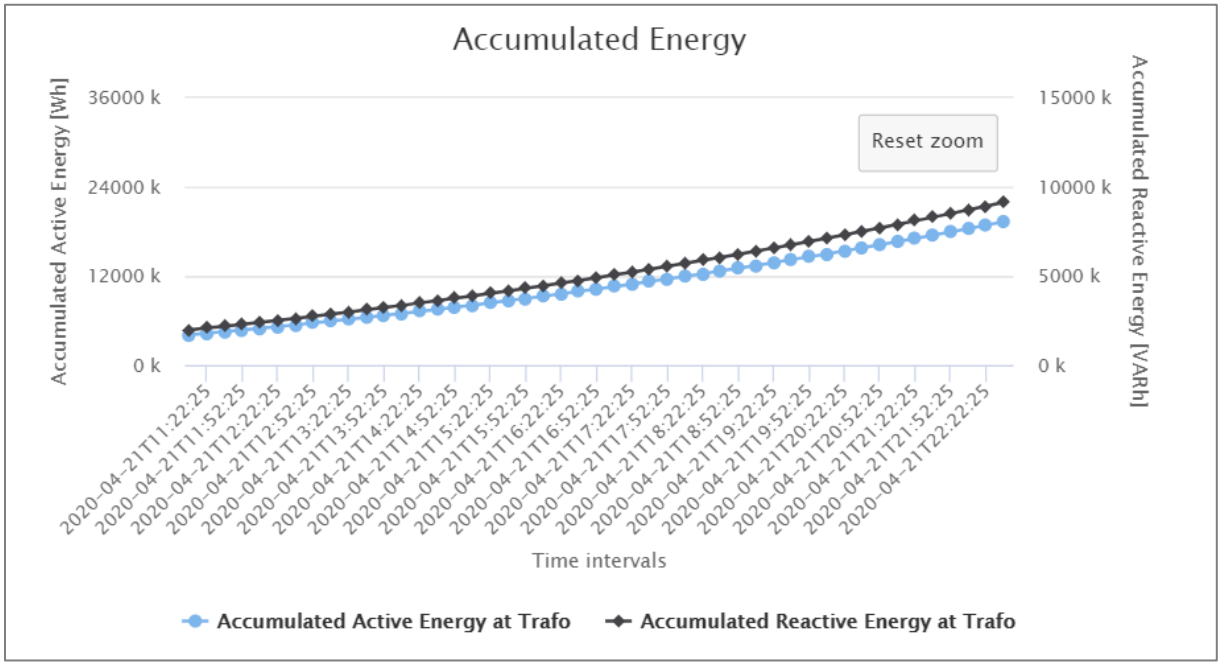

Figure 24 - Accumulated Energy

Figure 25 shows both the Accumulated Relative Active and Reactive energy losses, respectively in the left Y axis and right Y axis, as result of the LC application run in the selected date range.

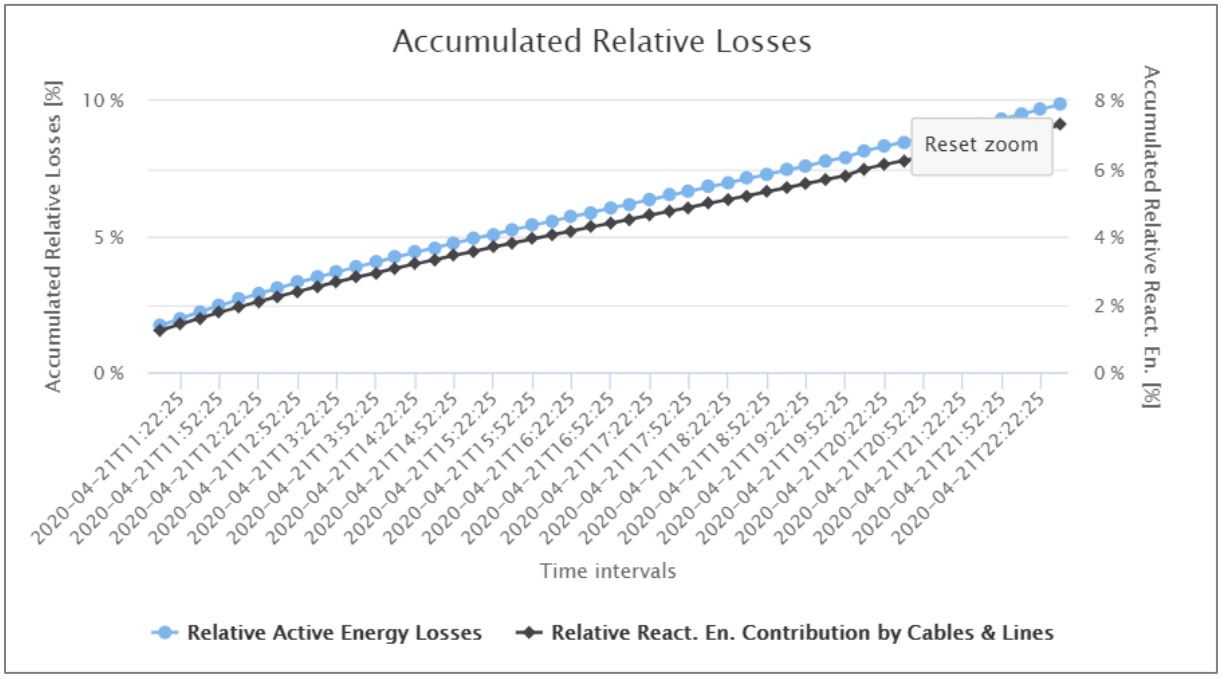

Figure 25 - Accumulated Relative Losses

4.1.10 Event Alarm Notifications

The GUI is able to provide alarm notifications to the user about abnormal events happening on the topology grid as well as at the ICT GW level, as described in previous Section 3.2. The events are detected, processed and stored by the "Security and Resilience" module that also notifies the GUI through the ICT Gateway.

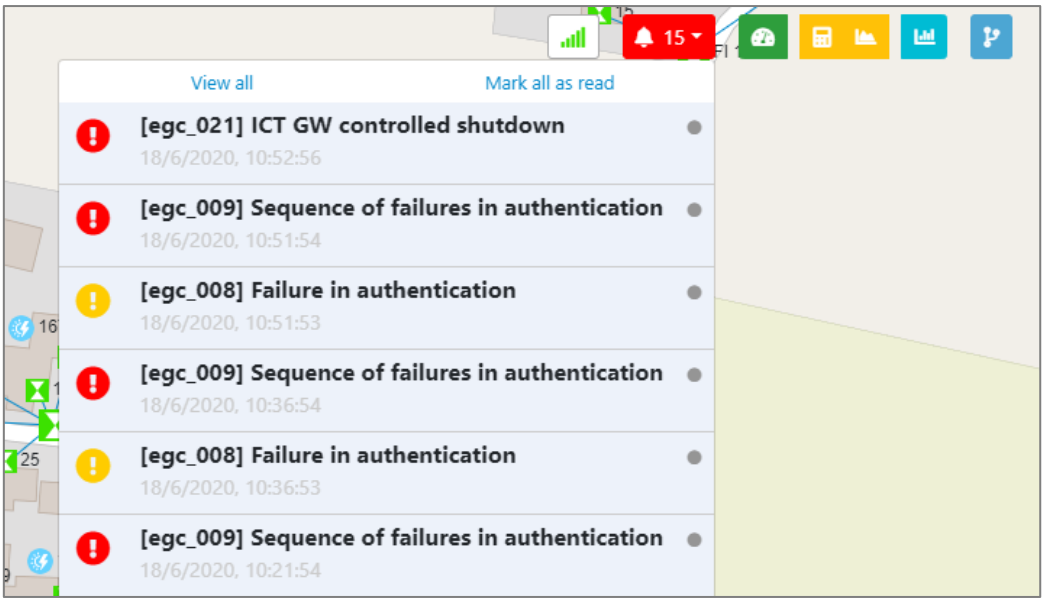

Figure 26 - Event alarm notifications

The User is able to visualize all notifications by clicking on the link “View all” as shown in Figure 26. A new modal dialog is opened showing the whole list of event alarm notifications with further details, as shown in Figure 27 and Figure 28.

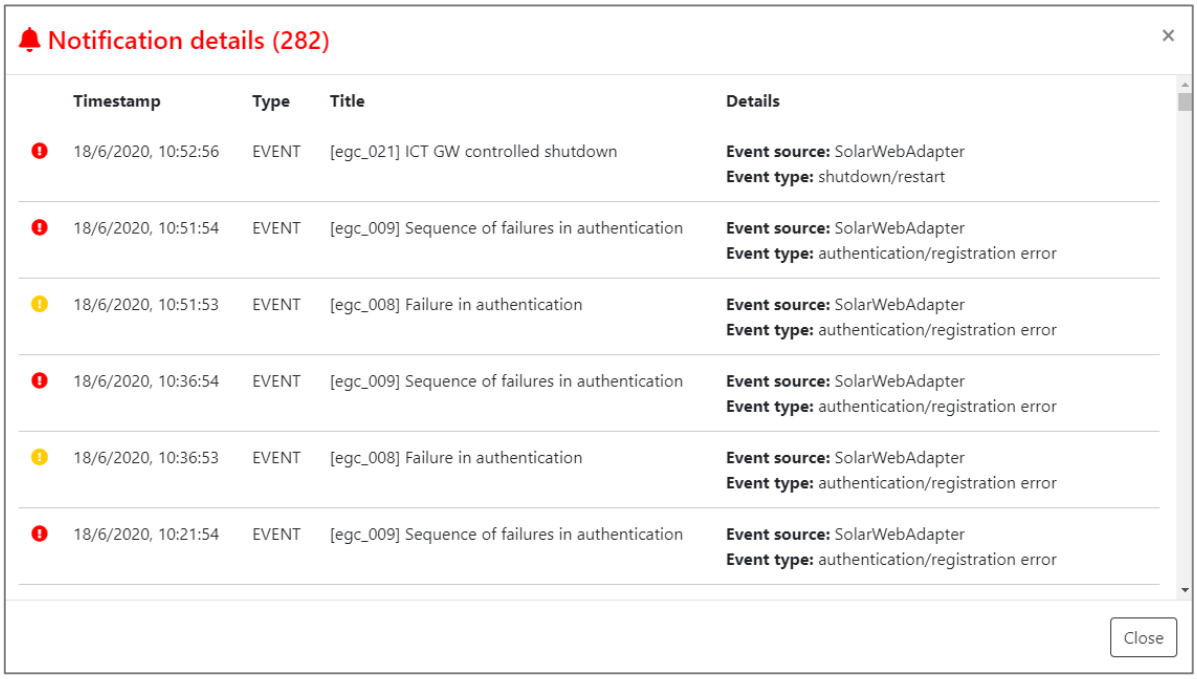

Figure 27 - Event Alarm Notifications Details

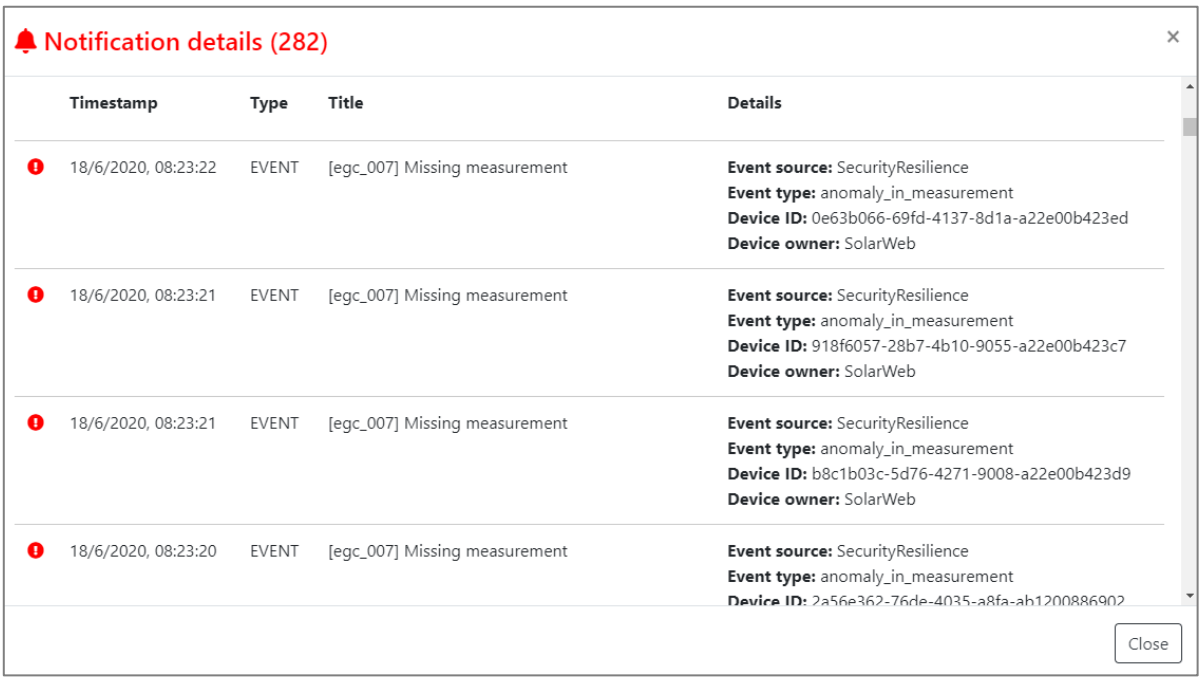

Figure 28 - Event Alarm Notifications Details

4.1.11 Graphical User Interface Architecture

The GUI application is based on a typical three-layers architecture, as described in Figure 29 [3]:

- Presentation layer
- Business layer
- Data layer

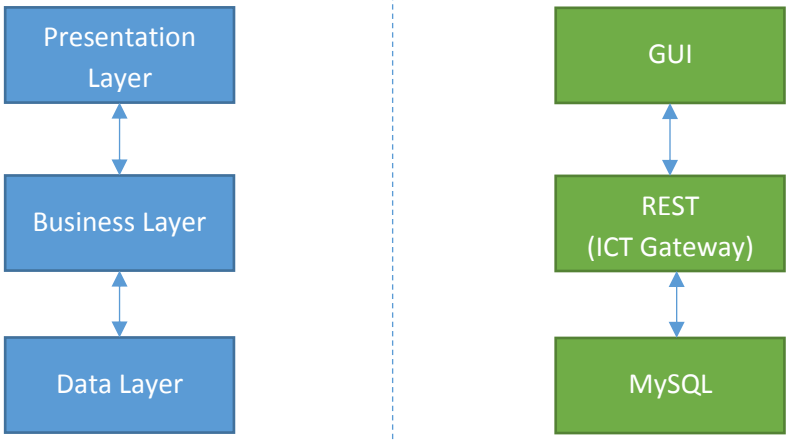

Figure 29 - GUI Architecture

4.1.12 Presentation Layer

It is responsible for presenting the information to the User, provided by the Business Layer. In particular, the approach "Single-Page Application" (SPA) using the framework Angular 8[3] that allows to develop the interface through separated components (separation of concerns).

The GUI is optimized in terms of display resolution and different devices thanks to the adoption of the framework Bootstrap 4[4] that offers a set of ready-to-use UI components and CSS styles.

The map is developed using OpenStreetMap libraries[5], which are free, open source and offer a good level of reliability. Furthermore, the data necessary for map rendering are cached into the browser Local Storage after the first time the UI is loaded, thus improving the performance by reducing the response times.

4.1.13 Business Layer

It is responsible for the business logic computation, hence implements the core algorithms. The computational results are provided to the Presentation Layer through REST services approach because it represents a simple and linear architectural style in which data are exchanged between layers using Json messages. In particular, the Business Layer is represented by the ICT Gateway middleware that implements all core Net2DG algorithms and provides them to the GUI through the REST services.

[3] https://angular.io/

[4] https://getbootstrap.com/

[5] https://switch2osm.org/

4.1.14 Data Layer

It is responsible for the persistence of the data and it is integrated with the Business Layer (ICT Gateway). In particular, the data are managed through a MySQL RDBMS that interacts with the Application Layer through the MySQL Connector bridge and the ORM (Object-Relational Mapping) Hibernate framework.

5 Description of Refined Modules

Following sections provide the list of modules that have been refined within the first half of third year of the project to meet DSOs and laboratory requirements and to allow the integration with “Security & Resilience” and “Event Generation & Correlation” Modules.

5.1.1 Core Logic

5.1.1.1 Time Synchronization

All the timestamps managed by the ICT Gateway and by its components have been aligned to the Coordinated Universal Time (UTC) which has been chosen because is the primary time standard all over the world. In practice, all the adapters and especially the ones capable of retrieving measurements and events, are in charge of aligning the time information; this can happen either by specifying UTC as a setting at the time of requesting data to HeadEnds or by converting to UTC the timestamp in the response message whenever it arrives in different time zone.
Modifications to time information do not only involve the time zone, but also the format that has been uniformed as well.
Not only internal modules as adapters or database are synchronized to the chosen time zone and format, but also external components as the Security & Resilience.

5.1.2 Gateway Internal Data Model

The data model defines common terms, symbols and formats used in the Net2DG project and representing the entire DSO system or sub-systems. As shown in the overview of Figure 30, it is now logically divided into multiple complementary sub-models: Topology (Figure 31), Measurements and Events (Figure 32), Adapter Registration (Figure 35), and Applications (Figure 36). Naming conventions and details regarding the meaning of relations do not differ from what was already specified in the Deliverable D3.2 [3].
This section highlights the updates of the data model with respect to what has been described in [3] and [1].

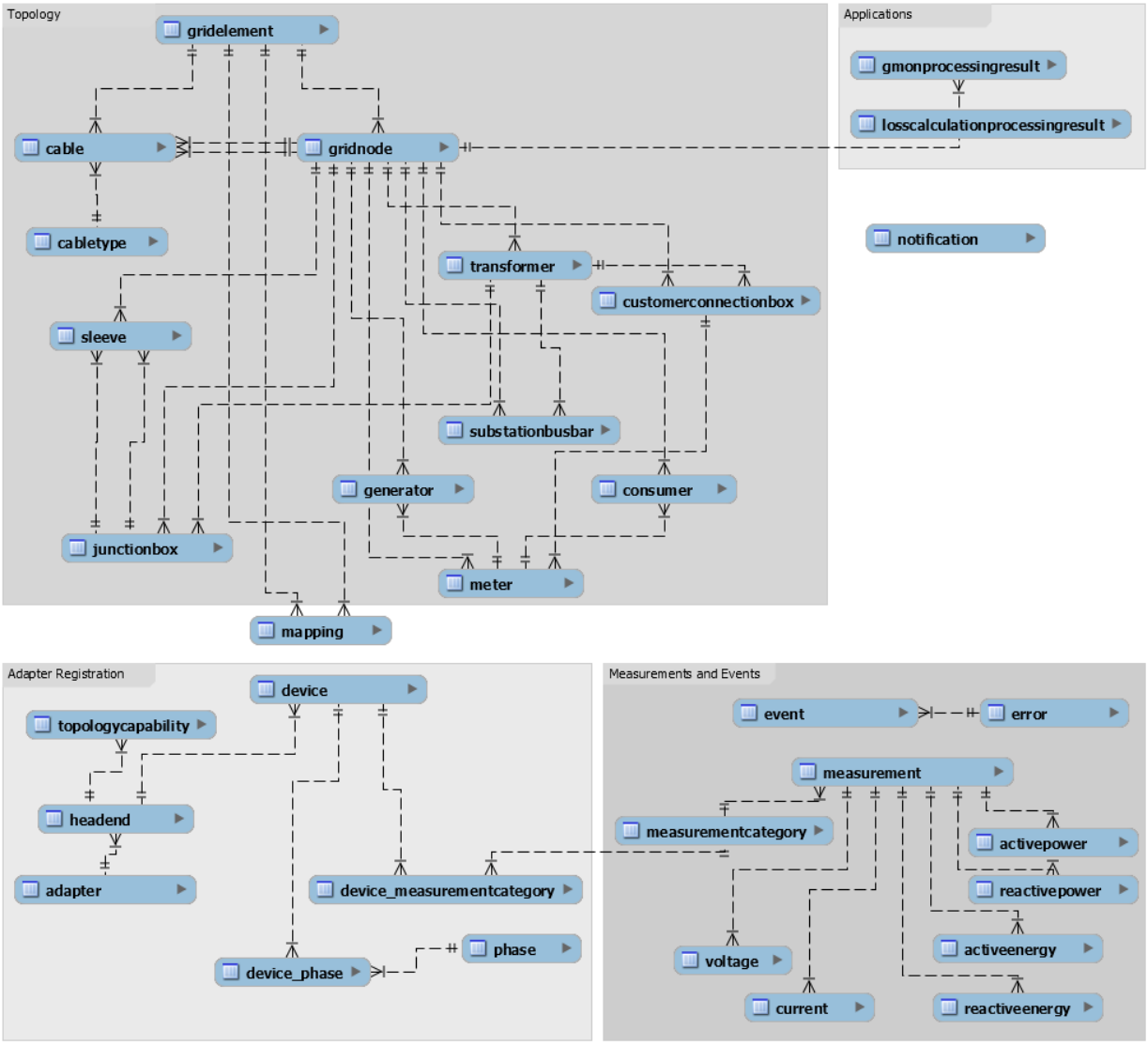

Figure 30 - Overview of ICT Gateway Internal Data Model

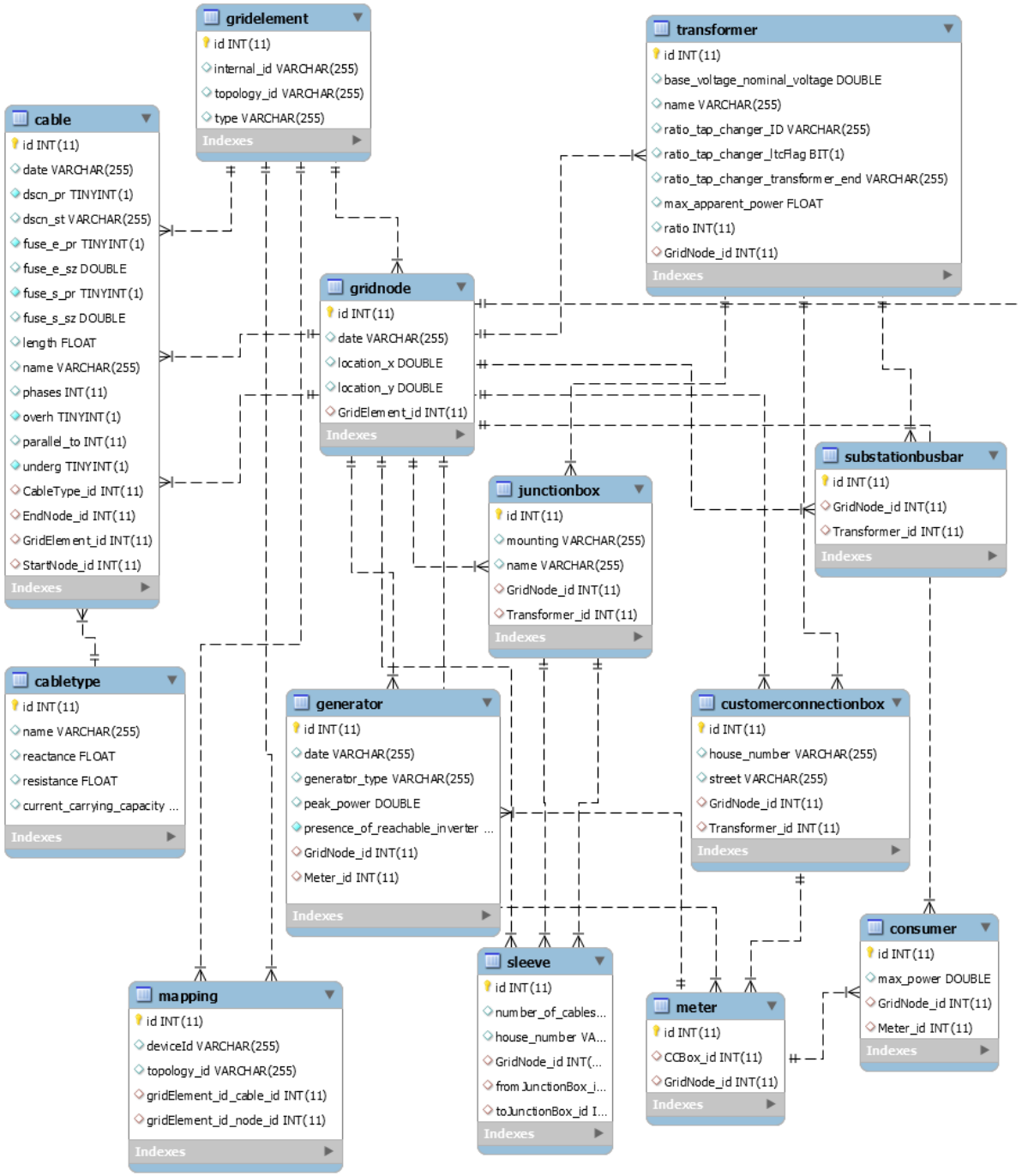

Figure 31 - Data Model Part showing Grid Topology Entities and Mapping Table

Figure 31 reports the current status of the grid topology sub-model. As can be noticed after a careful comparison with [3], the main difference is the addition of the table called `mapping`, which contains the information produced by the Grid Topology Mapping module and hence allows the relation between topology sub-model and measurements and events sub-model. As a consequence, there are not anymore outgoing relations from `gridelement` directed towards `event` and `measurement` tables (Figure 32), where the fields `gridElement_id_cable_id`, `gridElement_id_node_id` have been

removed: the relation is provided by joining the table (`event` or `measurement`) with the `mapping` table through the field `deviceId`.

Another modification regarding topology sub-model involves the table `cabletype`, where the `current_carrying_capacity` field has been added.

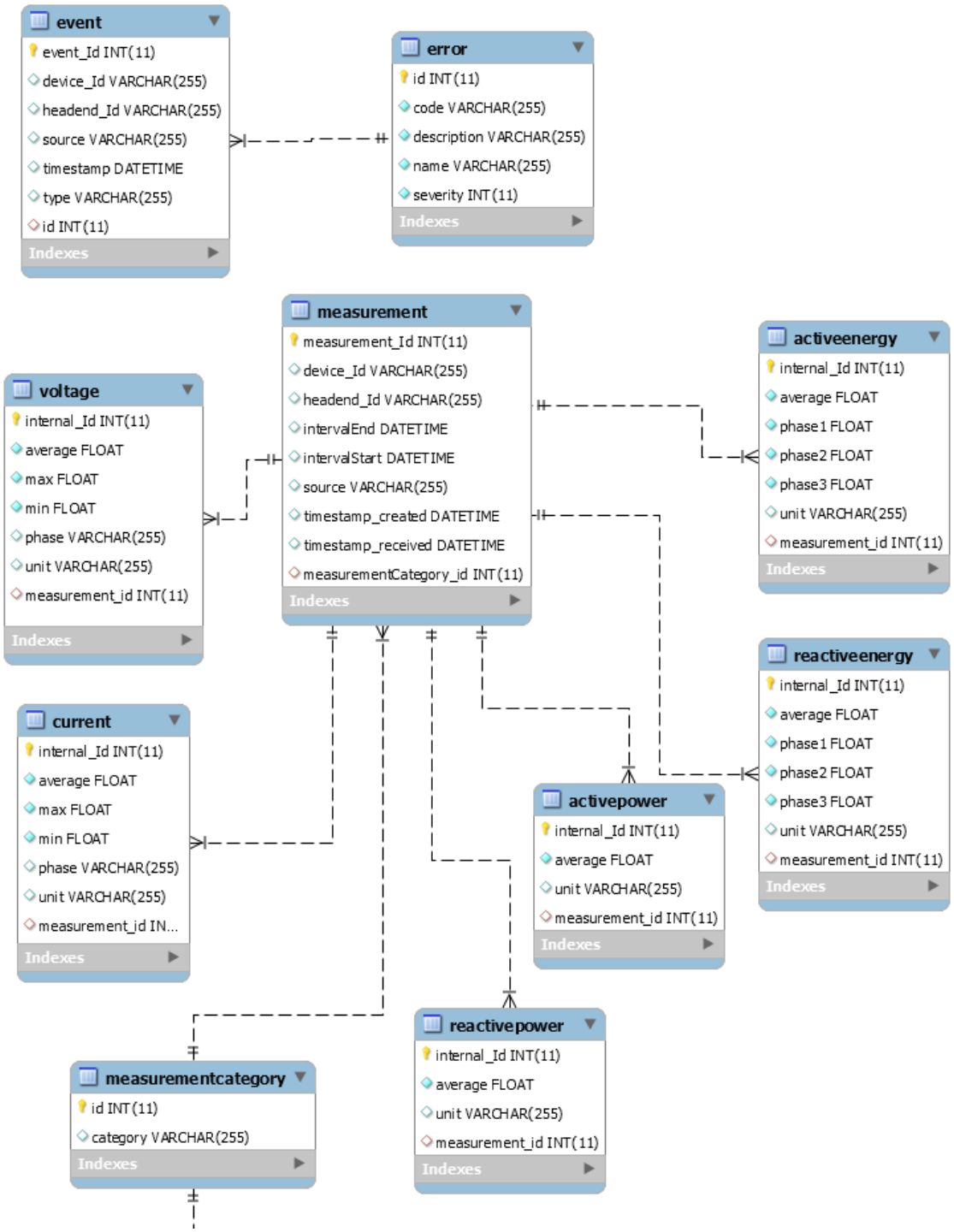

Figure 32 - Data Model Part Showing Measurements, Events and Related Entities

An important update in Measurements and Events sub-model involves time information storage: field `timestamp` in `event` table, and fields `timestamp_created`, `timestamp_received`, `intervalStart`, `intervalEnd` in `measurement` table, have been refactored and they now are an attribute of type `DATETIME`. The same stands for other time information in the entire data model (e.g., in `device.lastReading` field, or in `headend.registration` attribute, both of which are shown in Figure 35).

With respect to deliverable D3.2 [3], new fields have been introduced into `error` table (Figure 32): `code`, `description` and `severity`. The `error.code` is an identifier of the category of the error, the `error.description` provides a brief explanation, and the `error.severity` is a label expressing the assigned level of severity. These attributes are particularly useful for showing alerts on the Graphical User Interface (GUI), enriched with colour information corresponding to their severity, as detailed in section 4.1.10. Another field in the table is `error.name`, which basically corresponds to Name in Table 1 - Table 4.

Then, another addition to the data model is the table `measurementcategory`, where the information about the category of measurement is stored: possible values of the field `category` are shown in Figure 33. It has to be noticed that a measurement of category `MEASUREMENT_VOLTAGE` corresponds to up to three entries in `voltage` table, since voltages are stored per-phase; however, this does not have any influence on `measurementcategory` entity.

id	category
1	MEASUREMENT_ACTIVEENERGY
2	MEASUREMENT_VOLTAGE
3	MEASUREMENT_CURRENT
4	MEASUREMENT_REACTIVEENERGY
5	MEASUREMENT_ACTIVEPOWER
6	MEASUREMENT_REACTIVEPOWER

Figure 33 - Example of values in table `measurementcategory`

An important update regarding the data model is the addition of a set of tables generated during adapter registration process, which are logically grouped into the sub-model shown in Figure 35. The `Adapter` table stores information about each adapter of the ICT GW. The auto-generated `id` column is a foreign key for the `headend` table which references it as `adapter_id` with a many-to-one relation. Similarly, `headend` table is created as soon as a HeadEnd registers itself with ICT GW. Both, `headend` and `device` tables, have an additional column named `mode`, which can hold one of the two values: 1) R (Read) or 2) RW (Read and Write). The first one represents a device/headed from which it is only possible to read out data, i.e., measurements or events, while, the second one refers to a device/headed where ICT GW can send some data to, e.g., AVR application writes setpoints to a particular inverter. ICT GW utilizes the value of this table to distinguish devices where it can send data to.

When a topology headend is persisted, the corresponding table is referenced by `topologycapability` and `device` tables. The `topologycapability` table stores metadata about a topology pertaining to a HeadEnd as e.g., total number of cables or nodes, DSO name or geographical

area. Each headend of type topology has at least one related entry in topologycapability table and the relation is enabled by the headend_id column. As shown in Figure 34, the type of a HeadEnd can be either Topology or Measurements_Events, in this latter case, a relation with device table is expressed.

id	name	registration	type	adapter_id
1	SolarWeb	2020-05-08 13:14:39	Measurements_Events_Headend	3
2	AMIMediator	2020-05-11 12:29:39	Measurements_Events_Headend	2
3	Lan_Topology_HE	2020-05-08 10:59:43	Topology_Headend	4
4	Janitza_HE	2020-05-08 13:13:39	Measurements_Events_Headend	1
5	TME_Topology_HE	2020-05-11 12:28:15	Topology_Headend	4

Figure 34 - Example of values in table headend

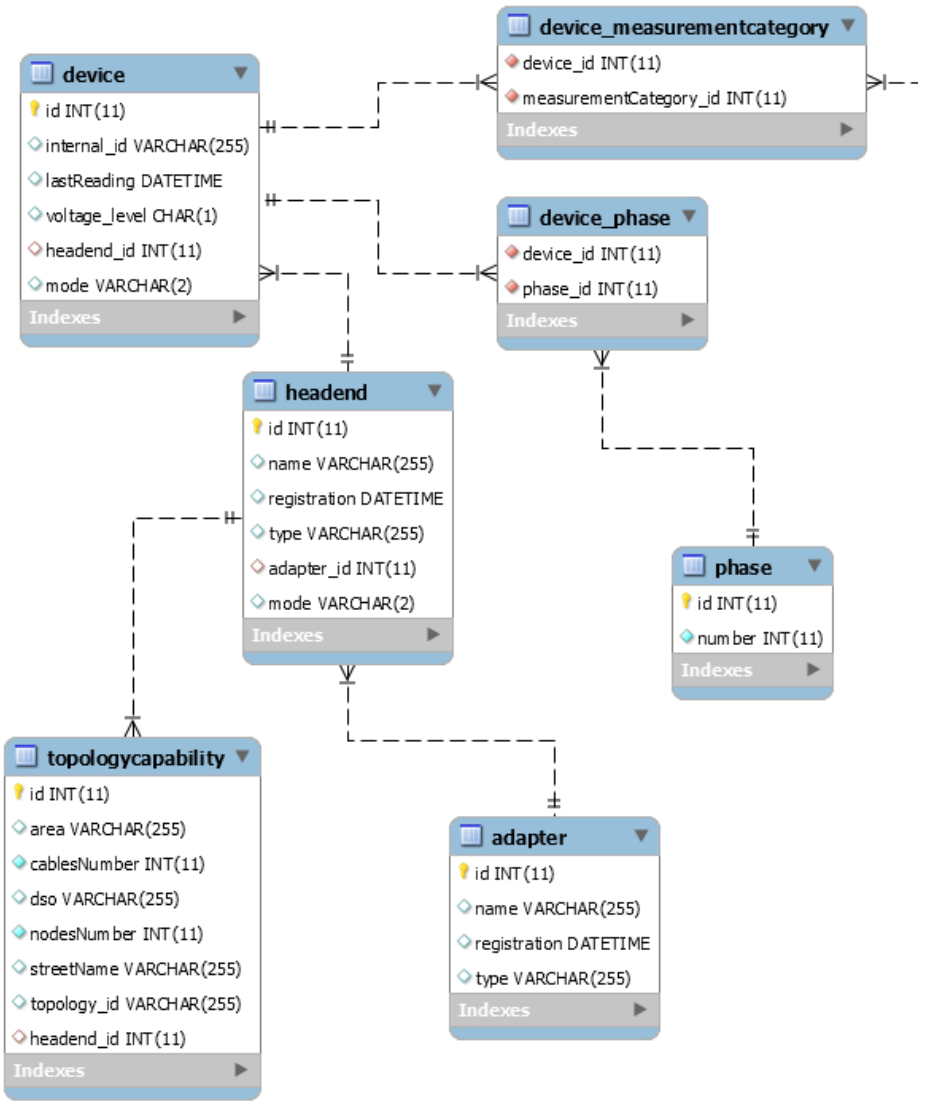

Figure 35 - Data Model Part Showing Adapter Registration, HeadEnd and Device Related Entities

`Device` table (and in particular the `device_id` field) plays a central role in the data model because it connects multiple sub-models: Topology (via `mapping` table), Measurements and Events, and Adapter Registration. The column `lastReading` is also very important for obtaining a status of active devices and for letting other components as S&R and EGC detect inactive devices and generate corresponding events (see Section 3.2). Other tables as `device_phase` and `device_measurementcategory` have been introduced to store metadata about a device and the kind of measurement it can provide, also for the purpose of detecting anomalous or missing measurements and phases, as described in Section 3.2.

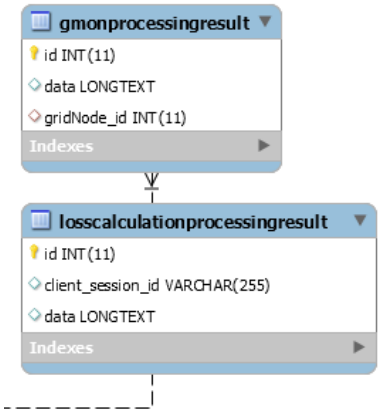

Figure 36 - Data Model Part Showing Applications Results Entities

There are also some additional tables logically grouped in the Applications sub-model (shown in Figure 36), which are used for persisting `data` generated during applications processing and to connect them with grid topology as it happens for grid monitoring application via the `gridnode_id` field in `gmonprocessingresult` table.

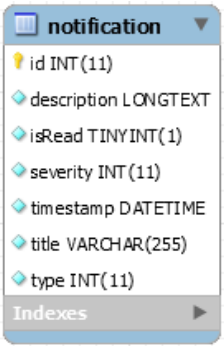

Figure 37 - Notification Table

Finally, the `notification` table, shown in Figure 37, is introduced in order to persist data sent to the GUI from other modules, e.g. the S&R. The table contains: a detailed **`description`**, a flag called **`isRead`** -useful to trace the notification status-, the **`severity`** level (Low, Medium, High), the **`timestamp`** of notification generation, a **`title`**, and the notification **`type`** (e.g. EVENT).

5.1.3 AMI Adapter

The meter data from the AMI system in Denmark is challenged by that the data flow is under strict regulation to ensure that its primary objective i.e. to provide data for billing purpose, is at all-time 100% covered. Further, it is by law required also to push data to an entity called the Data-Hub every single day, with the latest consumption measurements. If this data flow is interrupted or the AMI system fails to deliver 100% data coverage, even by a mistake, this will lead to contract breaches among the partners and possible legal actions. Therefore, it is of uttermost important not to disturb the AMI if at all possible.

Typically, the data from the measurements go through the AMI infrastructure to the HES, and is further being pushed to a third party database. From here, it is possible to extract data (historical data) every 6 hours that can be accessed via the Net2DG components in the server cloud hosted by KAMSTRUP. This approach has passed all hosting policies and legal checks and shown to be a robust approach for a steady information flow. Thus, a Historical data HE has been implemented on Kamstrup's server cloud that parses/reads the measurements and forwards those to AMI adapter in ICT GW.

Moreover, in order to meet specific on-demand data requests from an application, the proper refinements have been implemented at this level of integration.

5.1.4 Data Access API

Regarding the data access API, there are no many substantial differences with respect to what has been already described in the deliverable D3.2 [3]: all the entities existing in the database and their relations are specified by pair classes, namely the Model and the Data Access Object. So, the Data Access API leverages Hibernate framework and Java annotations to provide access to the database, in compliance with the DAO (Data Access Object) pattern, and for enabling the CRUD (Create, Read, Update and Delete) operations.
An obvious difference is constituted by the number of tables, which is increased as shown in Section 5.1.2.
An important update, instead, concerns the performance improvements: a significant effort has been spent aiming at reducing the number of database interactions.
Data Access APIs performance was not optimal on the large data sets. By constructing DTOs directly from a query result, a large performance improvement was made. This optimization also removed logic from the Measurement API component. Database indexes are added on intervals, device id and measurement category to provide additional query optimization. Results of optimization and related improvements are shown in both Table 7 and Table 8, respectively for Voltage and Energy measurement API.

Table 7 - Voltage measurements API performance before and after the optimization

	Query (s)	Loop (s)	Total (s)	#Measurements
Before	38,617	570,172	608,789	24300
After	1,188	0	1,188	24300

Table 8 - Energy measurements API performance before and after the optimization

	Query (s)	Loop (s)	Total (s)	#Measurements
Before	13,043	125,747	139,790	6048
After	1,228	0	1,228	6048

On the Grid Model API, for example, extensive querying has been replaced with fewer complex queries. In addition, the persistence and update of measurement-related entities (e.g., device, phase, etc.) is being handled on Core Logic side with a "caching" approach, thanks to which the updates are kept in memory and periodically inserted into the database instead of once per measurement. Performance evaluation regarding the *Caching* approach is shown in Table 9, where we compare it with the previous implementation, referenced as *Default.* As can be noticed, there is not any improvement if the number of measurements is very limited (e.g., 4), and this is probably due to the introduction of new data structures needed for the caching approach, but when it grows (e.g., from 40 to 40 thousand), the time saved becomes significant. The improvement is motivated by a clear reduction in the number of queries.

Table 9 - Performance comparison for the persistence of measurements before (Default) and after (Caching) the improvements

# **Messages**	**#Measurements**	**Default** Elapsed time (s)	**Caching** Elapsed time (s)	**Default** Elapsed time hh:mm:ss	**Caching** Elapsed time hh:mm:ss	**Time saved (s)**	**Time Saved** (%)	**Time saved** hh:mm:ss
1	4	2,44	2,88	00:00:02	00:00:03	-0,44	-18,03%	00:00:00
10	40	10,27	6,55	00:00:10	00:00:07	3,72	36,22%	00:00:04
100	400	60,15	46,13	00:01:00	00:00:46	14,02	23,31%	00:00:14
1000	4000	545,81	426,70	00:09:06	00:07:07	119,11	21,82%	00:01:59
10000	40000	4869,62	4188,87	01:21:10	01:09:49	680,75	13,98%	00:11:20

5.1.5 Adapter Registration

The Adapter Registration Module has been refined with respect to what was described in the deliverable D3.2 [3]: in the updated version, it does not simply maintain in memory the information about the registration process of the adapters, HeadEnds and available devices, but persists it into the database. This choice has been made in order to maintain the information even if the ICT GW is intentionally restarted or its execution is terminated for some reason. Moreover, thanks to the storage in the database, other components as external from the ICT Gateway as the Security & Resilience module can perform analytics. One example is the `lastReading` information, now available in `Device` table and usable by the S&R to take trace of inactivity or outage of equipment.

5.1.6 Application API

The Application API has been enriched and refined to satisfy requirements of applications and new or existing modules that have emerged during the recent development. Regarding the request/response APIs, the number of REST services has increased and they are structured to reflect entities from the

data model, e.g., REST API for active energy, reactive energy, voltage, currents, etc. In addition, what pertains the publish/subscribe paradigm, has been substituted with an MQTT (Message Queue Telemetry Transport) broker. MQTT [4] is a lightweight publish/subscribe network protocol that currently has been introduced alongside existing APIs implemented using WebSocket. However, in a future version of ICT GW it may completely substitute WebSocket, because of its properties such as the possibility to have multiple publishers and subscribers (instead of point to point communication), the lower bandwidth needs, the higher assurance of delivery and minor overhead.

6 Verification of ICT GW Security and Resilience functionalities

This section describes the tests carried out during development of the security and resilience functionalities, and in particular the successful generation of events and implementation of the countermeasures for each of the events listed in Section 3.2.

For the verification of other basic functionalities of the ICT Gateway, e.g., the correct obtainment and storage of grid topology information, the reception of periodic measurements or events, the mapping of measurements to grid topology, and so on, a detailed report of the test cases and related results is available in [2]. Moreover, further integration tests are going to be conducted in the context of WP5.

Starting from a predefined initial configuration, and upon execution of a set of operations, all the conditions are created for which an event is supposed to be generated and persisted into the database. The notation used for the test includes:

- **Test ID:** it represents the identifier name of the test
- **Test Title:** it associates to the test a meaningful title
- **Test Purpose:** it describes the aim(s) of the test
- **Preconditions:** it describes the initial configuration
- **Input:** it describes the triggering condition/operation which initiates the test, with an extract of the example input where existing
- **Output:** it describes the sequence of actions/conditions to be verified in order to prove the test outcome
- **Result:** the test outcome
- **Coverage:** it lists the event(s) covered by the test

Test ID	**Test Title**
Data collection system outage test	Injection of null measurements
Test Purpose	
This test verifies that, upon reception by the ICT Gateway of a MEASUREMENT_DETAILS_RESPONSE JSON message containing a null “Value” Object where measurement unit is missing, the Security & Resilience module timely detects the anomaly (during its next iteration) and the EGC demands the insertion into the database of a *Data collection system outage* event.	
Preconditions	
1. ICT Gateway running 2. S&R running	
Input	

MEASUREMENT_DETAILS_RESPONSE containing null “Value”.
The following is an extract of the message, where the null value is reflected as missing measurement “`Unit`” inside the “`Value`” object.
`{`
`"measurementType": "MEASUREMENT_VOLTAGE",`
`"ChannelType": "UACMeanL1",`
`"measurement": {`	

```
    "DeviceType": 232,
    "DeviceId": "27b1dba2-c742-40ee-92c3-aafb00a46a00",
    "NodeType": 97,
    "DaloId": "240.874201",
    "Value": {
      "Value": 0,
      "Min": 0,
      "Max": 0
    }
  }
}
```


Output

- *Data collection system* outage event persisted into the database (Event and Error tables)
- alert to DSO "suspected outage" visible on the GUI

Result

Test successfully executed: correct persistence of *Data collection system outage* event in DB; event alarm notified to the GUI.

Coverage

Data collection system outage

Test ID	Test Title
Voltage value equals to zero test	Injection of zero measurements sequence

Test Purpose

This test verifies that, upon reception by the ICT Gateway of 2 MEASUREMENT_DETAILS_RESPONSE JSON messages containing measurement values equal to zero, the Security & Resilience module timely detects the anomaly (during its next iteration) and the EGC demands the insertion into the database of an *Voltage value equals to zero* event.

Preconditions

1. ICT Gateway running
2. S&R running

Input

A sequence of two MEASUREMENT_DETAILS_RESPONSE pertaining to the same device and containing only 0 values (average, min, and max)

The following is an extract of one of the two messages.


```
{
  "measurementType": "MEASUREMENT_VOLTAGE",
  "ChannelType": "UACMeanL3",
  "measurement": {
    "DeviceType": 232,
    "DeviceId": "27b1dba2-c742-40ee-92c3-aafb00a46a00",
    "NodeType": 97,
    "DaloId": "240.874201",
    "Value": {
      "Value": 0.0,
      "Min": 0.0,
      "Max": 0.0,
      "Unit": "V"
    }
```

```
    }
}
```


Output
• *Voltage* value equals to zero persisted into the database (Event and Error tables) • alert to DSO “suspected faulty device” visible on the GUI
Result
Test successfully executed: correct persistence of *Voltage value equals to zero* event in DB; event alarm notified to the GUI.
Coverage
Voltage value equals to zero

Test ID	Test Title
Single phase zero voltage test	Injection of single phase zero voltage
Test Purpose	
This test verifies that, upon reception by the ICT Gateway of a MEASUREMENT_DETAILS_RESPONSE JSON message containing, on a single phase only, a voltage measurement equal to zero, while values on other phase(s) are different from zero and inside a valid range, the Security & Resilience module timely detects the anomaly (during its next iteration), and the EGC demands the insertion into the database of a *Single phase zero voltage* event. A *Voltage imbalance* should be generated as well, because a single phase zero voltage is a special case of voltage imbalance.	
Preconditions	
1. ICT Gateway running 2. S&R running	
Input	
MEASUREMENT_DETAILS_RESPONSE containing 0 voltage value on a phase and plausible values on the other phase(s) The following is an extract of the message showing the phase with zero voltage values:	


```
{
  "measurementType": "MEASUREMENT_VOLTAGE",
  "ChannelType": "UACMeanL1",
  "measurement": {
    "DeviceType": 232,
    "DeviceId": "27b1dba2-c742-40ee-92c3-aafb00a46a00",
    "NodeType": 97,
    "DaloId": "240.874201",
    "Value": {
      "Value": 0.0,
      "Min": 0.0,
      "Max": 0.0,
      "Unit": "V"
    }
  }
}
```

Output
• *Single phase zero* voltage persisted into the database (Event and Error tables) • *Voltage imbalance* persisted into the database (Event and Error tables) • alert to DSO “potential harm to transformer/electric equipment” visible on the GUI
Result
Test successfully executed: correct persistence of both *Single phase zero voltage* and *Voltage imbalance* events in DB; event alarm notified to the GUI.
Coverage
Single phase zero voltage; Voltage imbalance

Test ID	**Test Title**
Voltage imbalance test	Injection of voltage imbalance
Test Purpose	
This test verifies that, upon reception by the ICT Gateway of a MEASUREMENT_DETAILS_RESPONSE JSON message containing a value on a phase that compared with the measurements of the other phases exceeds the tolerable limit of +-10V, the Security & Resilience module timely detects the anomaly (during its next iteration), and the EGC demands the insertion into the database of a *Voltage imbalance* event.	
Preconditions	
1. ICT Gateway running 2. S&R running	
Input	
MEASUREMENT_DETAILS_RESPONSE containing voltage values unbalanced by +-10V. The following is an extract of the message injected, a phase with voltage values not balanced (+-10V difference) with respect to the other two phases:	


```
{
  "measurementType": "MEASUREMENT_VOLTAGE",
  "ChannelType": "UACMeanL2",
  "measurement": {
    "DeviceType": 72,
    "unit": "V",
    "LogDateTime": "2020-03-10T07:05:00",
    "DeviceId": "96bd9e4f-ebab-405c-9435-a44200e5469a",
    "NodeType": 97,
    "DaloId": "240.79197",
    "Value": {
      "Value": 133.30234,
      "Min": 132.307,
      "Max": 134.2,
      "Unit": "V"
    }
  }
}
```


Output
• *Voltage imbalance* persisted into the database (Event and Error tables) • alert to DSO “potential harm to transformer/electric equipment” visible on the GUI

Result
Test successfully executed: correct persistence of *Voltage imbalance* event in DB; event alarm notified to the GUI.
Coverage
Voltage imbalance

Test ID	Test Title
Anomalous value test	Injection of anomalous value
Test Purpose	
This test verifies that, upon reception by the ICT Gateway of a MEASUREMENT_DETAILS_RESPONSE JSON message that exceeds a threshold (e.g., 250V), the Security & Resilience module timely detects the anomaly (during its next iteration), and the EGC demands the insertion into the database of an *Anomalous value* event. [A *Voltage imbalance* should be generated as well if the measurement is of category voltage: most likely there would be an imbalance between phases].	
Preconditions	
1. ICT Gateway running 2. S&R running	
Input	
MEASUREMENT_DETAILS_RESPONSE containing measurement value over a threshold (e.g., 250V). The following is an extract of the message injected, a phase with one of voltage values over the threshold:	


```
{
 "measurementType": "MEASUREMENT_VOLTAGE",
 "ChannelType": "UACMeanL2",
 "measurement": {
   "DeviceType": 72,
   "unit": "V",
   "LogDateTime": "2020-03-10T07:05:00",
   "DeviceId": "96bd9e4f-ebab-405c-9435-a44200e5469a",
   "NodeType": 97,
   "DaloId": "240.79197",
   "Value": {
     "Value": 233.307,
     "Min": 233.302,
     "Max": 270.202,
     "Unit": "V"
   }
 }
}
```


Output
• *Anomalous value* persisted into the database (Event and Error tables) • [*Voltage imbalance* persisted into the database (Event and Error tables)] • alert to DSO “Measurement from device not reliable” visible on the GUI • [alert to DSO “potential harm to transformer/electric equipment” visible on the GUI]
Result

Test successfully executed: correct persistence of *Anomalous value* and *Voltage imbalance* events in DB; events alarms notified to the GUI.
Coverage
Anomalous value, [Voltage imbalance]

Test ID	**Test Title**
Missing phase test	Injection of missing phase
Test Purpose	
This test verifies that, upon reception by the ICT Gateway of a MEASUREMENT_DETAILS_RESPONSE JSON message where the number of voltage phases is not correct (is not corresponding to what known during adapter registration and stored into device_phase table), the Security & Resilience module timely detects the anomaly (during its next iteration), and the EGC demands the insertion into the database of a *Missing phase* event.	
Preconditions	
1. ICT Gateway running 2. S&R running 3. Device_phase table populated	
Input	

MEASUREMENT_DETAILS_RESPONSE containing two (out-of-three) voltage phases.
The following is an extract of the message injected, showing one of the two phases present in the JSON message, while the third one is completely missing:
{
"measurementType": "MEASUREMENT_VOLTAGE",
"ChannelType": "UACMeanL1",
"measurement": {
"DeviceType": 232,
"DeviceId": "27b1dba2-c742-40ee-92c3-aafb00a46a00",
"NodeType": 97,
"DaloId": "240.874201",
"Value": {
"Value": 233.30234,
"Min": 232.307,
"Max": 234.2
}
}
}	

Output	
• *Missing phase* persisted into the database (Event and Error tables) • alert to DSO “Measurement from device not reliable” visible on the GUI	
Result	
Test successfully executed: correct persistence of *Missing phase* event in DB; event alarm notified to the GUI.	
Coverage	
Missing phase	

Test ID	Test Title
Missing measurement test	Deletion of measurement and related entry
Test Purpose	
This test verifies that, upon deletion of an entry from measurement table (and of the related entry from corresponding child table, e.g., activeenergy), the Security & Resilience module timely detects the anomaly (during its next iteration), and the EGC demands the insertion into the database of a *Missing measurement* event.	
Preconditions	
1. ICT Gateway running 2. S&R running 3. Existing measurement entries in the database	
Input	

Execution of DELETE query to remove an entry from measurement table and the related one from child table (e.g., activeEnergy).
The following are the queries used to delete the entries:
`DELETE FROM activeenergy`
`WHERE activeenergy.measurement_id = 1;`
`DELETE FROM measurement`
`WHERE measurement.measurement_Id = 1;`	

Output	
• entries in measurement and child table (activeEnergy) deleted • *Missing measurement* persisted into the database (Event and Error tables) • alert to DSO “Measurement from device not reliable” visible on the GUI	
Result	
Test successfully executed: successful deletion of the entries, correct persistence of *Missing measurement* event in DB; event alarm notified to the GUI.	
Coverage	
Missing measurement	

Test ID	Test Title
Failure in authentication test	Injection of Authentication Error
Test Purpose	
This test verifies that, upon reception by an Adapter of an authentication error message from a HE (i.e., “AccesToken invalid” JSON message), the Adapter automatically retries authentication and notifies the issue to the EGC, which demands the insertion into the database of a *Failure in authentication* event.	
Preconditions	
1. ICT Gateway running	

2. HE running
Input
Authentication error message injected to ICT GW. The following is an example of message injected: `{ "statusCode": 401, "result": "AccessToken invalid" }`
Output
• *Failure in authentication* persisted into the database (Event and Error tables) • alert to DSO “Simultaneous use of credentials” visible on the GUI
Result
Test successfully executed: correct persistence of *Failure in authentication* event in DB; event alarm notified to the GUI.
Coverage
Failure in authentication

Test ID	**Test Title**
Sequence of failures in authentication test	Injection of Sequence of Authentication Errors
Test Purpose	
This test verifies that, upon reception by an Adapter of a sequence of at least two authentication error messages from a HE (i.e., “AccesToken invalid”), the Adapter automatically notifies the issue to the EGC, which demands the insertion into the database of a *Sequence of failures in authentication* event. A *Failure in authentication* should be generated as well.	
Preconditions	
1. ICT Gateway running 2. HE running	
Input	
Sequence of authentication error messages injected to ICT GW The following is one of the injected messages in the sequence: `{ "statusCode": 401, "result": "AccessToken invalid" }`	
Output	
• *Failure in authentication* persisted into the database (Event and Error tables) • Sequence of failures in authentication persisted into the database (Event and Error tables) • alert to DSO “Possible credential Theft” visible on the GUI	
Result	

Test successfully executed: correct persistence of *Failure in authentication*, and *Sequence of failures in authentication* events in DB; events alarms notified to the GUI.
Coverage
Failure in authentication, Sequence of failures in authentication

Test ID	**Test Title**
Unmappable measurement device test	Injection of unmappable measurement

Test Purpose

This test verifies that, upon reception by the ICT Gateway of a MEASUREMENT_DETAILS_RESPONSE JSON message containing a deviceId that is not present in HE's capability (thus not persisted into device table of the database), the Adapter Registration module detects the occurrence, and the EGC demands the insertion into the database of a *Unmappable measurement device* event.

Preconditions

1. ICT Gateway running

Input

MEASUREMENT_DETAILS_RESPONSE containing an unknown deviceId.

The following is the entire message injected, where the deviceId (in bold) is artificial.


```
{
  "payload": [
    {
      "measurementType": "MEASUREMENT_VOLTAGE",
      "ChannelType": "UACMeanL1",
      "measurement": {
        "DeviceType": 72,
        "DeviceId": "12ab3c4d-efgh-567i-8901-123456m7890n",
        "NodeType": 97,
        "DaloId": "240.79198",
        "Value": {
          "Value": 233.30234,
          "Min": 232.307,
          "Max": 234.2,
          "Unit": "V"
        }
      }
    }
  ],
  "headendId": "SolarWeb",
  "rtuId": "98ab7c6d-efgh-543i-2101-198765m0987b",
  "category": "DATA",
  "type": "MEASUREMENT_DETAILS_RESPONSE",
  "timestampCreated": "2020-03-10T07:05:00",
  "timestampReceived": "2020-03-10T09:05:17",
  "measurementIntervalStart": "2020-03-10T06:50:00",
  "measurementIntervalEnd": "2020-03-10T07:05:00"
}
```


Output

- *Unmappable measurement* device persisted into the database (Event and Error tables)
- alert to DSO "Grid Topology not updated" visible on the GUI

• Device is flagged as not trustable • Automatic triggering of GTM
Result
Test successfully executed: correct persistence of *Unmappable measurement device* event in DB; event alarm notified to the GUI.
Coverage
Unmappable measurement device

Test ID	**Test Title**
Measurement device unreachable test	Update of device lastReading with old date
Test Purpose	
This test verifies that, upon updating lastReading field in Device table with a value that is null or older than 24 hours with respect to current UTC time, the Security & Resilience module timely detects the outage (during its next iteration), and the EGC demands the insertion into the database of a *Measurement device unreachable* event.	
Preconditions	
1. ICT Gateway running 2. S&R running 3. Existing entry in device table	
Input	

Execution of UPDATE query to set the lastReading field of a Device to a value that is older than 24 hours. The following is the query executed for this test.
`UPDATE device`
`SET lastreading = '2020-03-18 09:00:00'`
`WHERE device.id = 1;`	

Output	
• *Measurement device unreachable* persisted into the database (Event and Error tables) • alert to DSO “Device offline / not responsive” visible on the GUI • Device is flagged as offline / not responsive • Automatic attempt to retrieve missing measurements	
Result	
Test successfully executed: successful update of `device.lastReading`; correct persistence of *Measurement device unreachable* event in DB; event alarm notified to the GUI.	
Coverage	
Measurement device unreachable	

Test ID	**Test Title**
Non-responsive component test	Injection of “under maintenance” response
Test Purpose	

This test verifies that, upon reception of an html page reporting an “under maintenance” status of an external component (e.g., a HE) instead of a JSON response message, the corresponding adapter detects the outage, and the EGC demands the insertion into the database of a *Non-responsive component* event.
Preconditions
1. ICT Gateway running
Input

Injection of “under maintenance” html page
The following is an extract (top and bottom) of the injected document, corresponding to the real “under maintenance” page of the Inverter Headend (Solarweb):
 	
`<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">`
`<html>`
`<head>`
`<title>Fronius International GmbH</title>`
`<meta http-equiv="Content-Type" content="text/html; charset=utf-8">`
`<style type="text/css"> body { background-image:`
`url('`
 	
[…]
 	
`l3hPrUFTGzMzDmh5UpZVmYxma4FKC6YiIimbgHvVJB//Z'); background-repeat: no-repeat; background-attachment: fixed; background-position: center center; }`
`</style></head> <body></body> </html>`

Output
• *Non-responsive component* persisted into the database (Event and Error tables) • alert to DSO “Component offline / not responsive” visible on the GUI
Result
Test successfully executed: correct persistence of *Non-responsive component* event in DB; event alarm notified to the GUI.
Coverage
Non-responsive component

Test ID	**Test Title**
ICT GW Controlled Shutdown test	ICT GW controlled shutdown
Test Purpose	
This test verifies that, upon shutdown of the ICT GW by the user, before exiting the Core Logic commands to the EGC the insertion into the database of an *ICT GW Controlled Shutdown* event.	
Preconditions	
1. ICT Gateway running	
Input	
Execution of Ctrl+C on the keyboard in a command prompt where the executable jar of the system was launched. Alternatively (equivalent test) pressing the “Exit” button on the IDE’s console.	

Output
• *ICT GW Controlled Shutdown* persisted into the database (Event and Error tables) • [If S&R and MQTT broker are running, S&R will also publish the "offline" message over the ict-gateway channel]
Result
Test successfully executed: correct persistence of *ICT GW Controlled Shutdown* event in DB; event alarm notified to the GUI; "offline" message published to MQTT broker over the ict-gateway channel
Coverage
ICT GW Controlled Shutdown

Test ID	Test Title
ICT GW unexpected shutdown test	ICT GW unexpected shutdown
Test Purpose	
This test verifies that, when the ICT GW is not running, the S&R timely (during its next iteration) publishes the "offline" message to the MQTT broker on the channel *ict-gateway*.	
Preconditions	
1. ICT Gateway running 2. S&R running 3. MQTT broker running	
Input	
ICT is shutdown (e.g. by immediately stopping the thread)	
Output	
• S&R publishes the "offline" message on the MQTT broker over the ict-gateway channel • alert to DSO "ICT GW offline / not responsive" visible on the GUI	
Result	
Test successfully executed: event alarm notified to the GUI; "offline" message published to MQTT broker over the ict-gateway channel	
Coverage	
ICT GW unexpected shutdown	

7 Conclusions

The activities carried out in the context of WP3 during the last six months, which led to the conclusion of the work package, are described in this deliverable.

This deliverable describes in principle all the refinements performed in the already existing modules composing the ICT GW, in order to fully meet lab and field trial requirement raised during last period thanks to the intensive cooperation within WP5 and relevant feedback obtained within WP6 by the reference groups.
Furthermore, the deliverable describes the results of activities carried out in tasks T3.3 and T3.4 aimed at providing the ICT GW with additional functionalities of security and resilience, therefore allowing for a more robust overall Net2DG solution. Exploiting the results of the security and threat analysis in T3.3 was devoted to further describe the already identified undesired events and to provide a means for detection of such events, through the new module Event Generation & Correlation identified; while T3.4 was devoted to the identification of reaction to be triggered as soon as one of the undesired events was detected, e.g., alert the DSO about the events, try to collect missed or malformed measurands form the field, restore the connection with non-responding components/sub-systems, mark some devices as not trustable when their measurands or their grid topology mapping do not seem to be consistent to what expected.

The work carried out in both the tasks allows to identify and define further undesired events that could be addressed in future if considered relevant, anyway the definition of solutions to monitor and detect these additional anomalies occurring in the ICT GW have been studied and shortly described in the deliverable, even if they are not integrated in the current release.

Finally, the described additional functionalities implemented in current solution have been verified through the test specification described in Section 6 to prove the correct implementation.

This deliverable also reports, in ANNEX A, all the requirements extracted from Deliverable D1.2 [7] and corresponding and the corresponding implementation satisfaction.

8 References

[1] Net2DG, *Deliverable D3.1 - ICT Analysis and Gateway Design,* 2018.

[2] Net2DG, "Deliverable D5.1 - First integrated deployment at Lab and Testbed and preliminary results," 2019.

[3] Net2DG, *Deliverable D3.2 - Data Gateway Realization,* 2019.

[4] U. Hunkeler, H. L. Truong and A. Stanford-Clark, "MQTT-S-A publish/subscribe protocol for Wireless Sensor Networks.," in *In 2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE'08)*, 2008, January.

[5] Net2DG, *Deliverable D2.1 - Algorithms for grid estimation and observability applications,* 2018.

[6] Net2DG, *Deliverable D2.2 - Final realization of grid state estimation and observability applications,* 2019.

[7] Net2DG, *Deliverable D1.2 - Initial Baseline Architecture,* 2018.

[8] O. E. a. P. Niblett, Event Processing in Action, MANNING Greenwich, 2011, pp. 68-73.

ANNEX A. Status of requirements

This annex reports all the requirements extracted from Deliverable D1.2 [7] with the purpose of confirm whether they have been satisfied by current ICT GW implementation, where in scope for the ICT GW itself, and to provide in case a rational behind.
Each table reports the Requirement ID, the requirement description, the nature of the requirement either mandatory or optional, the fulfilment of the requirement, and a comment if necessary, only when mandatories requirements have not been met.
In general, when optional requirements have not been satisfied it is because we mainly focus on the relevant functionalities of the ICT GW.

System Requirements

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
SYS-01	The Net2DG solution must be able to support the processing of grids with up to 50.000 measurement points and up to 2000 secondary substations.	M	No	There is the risk that current prototype cannot efficiently handle such kind of numbers.
SYS-02	The actual prototype deployment in Net2DG must support the handling of grids with up to 5000 measurement points and 200 secondary substations.	M	YES	-
SYS-03	The Net2DG control coordination should work in such a way that unavailability of the Net2DG system does not create safety-critical grid behavior or large-scale blackouts.	O	YES	-
SYS-04	The Net2DG solution should have a maximum downtime of 100 hours per year (98,85%).	O	YES	There is no a quantitative evaluation of this requirement, which is planned during the last 12 months of the project.

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
SYS-05	Authenticity, Integrity, and confidentiality: Requirements for ensuring authenticity, confidentiality and protecting messages integrity shall be identified, and appropriate controls identified and implemented.	M	YES	-
SYS-06	The Net2DG solution must be able to run on a standard Microsoft Windows platform (both virtualized and physical). Support for server 2016 is mandatory, while server 2012 R2 is optional.	M	YES	-
SYS-07	For small installations and test purposes, it must be possible to execute on a single server instance.	M	YES	-
SYS-08	For larger installations, it must be possible to install individual parts on separate servers. Support for multiple instances of high-load services for load balancing purposes is optional.	M	YES	-
SYS-09	It must be possible to install and upgrade the Net2DG solution.	M	YES	-
SYS-10	It must be possible to install Software updates and addition of new adapters in the Net2DG prototype locally by direct physical access to the executing machines as well as remotely.	M	YES	In the current development environment
SYS-11	Software maintenance should only be possible with the right credentials.	O	YES	-
SYS-12	All Net2DG components must support debug logging; As default, log level should be “warning”. Log files should be stored locally.	M	YES	-
SYS-13	It shall be possible to activate a detailed tracing of actions by a local configuration.	M	YES	-
SYS-14	Log files for debug purposes must not contain privacy sensitive information.	M	YES	-
SYS-15	The system must make a separate audit trail for any action done by the operator.	M	No	At the moment these are logged together with other data

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
SYS-16	The Net2DG solution must assure that stored data is persistently removed after a configurable time period.	M	No	At the moment this feature is not yet implemented, in favour of other relevant features, but it can be easily implemented.

Interface to Grid Topology Sub-System

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
GTS-1	GTS must register at the ICT Gateway and provide the following basic information • Type of Topologies contained: LV, MV • Number of Secondary Substations covered	M	YES	-
GTS-2	When requested by the ICT Gateway, the GTS must be able to provide information regarding the following capabilities • Number of Grid Nodes contained • 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	M	YES	-

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
GTS-3	The Grid Topology Subsystem must be able to provide the following information about the CURRENT LV Grid topology upon request from the ICT Gateway: • For Secondary Substations: Substation ID, GPS Coordinate, number of transformers, numbers of feeders per transformer, additional parameters per transformer (to be specified later in WP2), metering device IDs. • For Junction Boxes: Junction Box ID, GPS Coordinate, numbers of outgoing cables, additional parameters for junction box (to be specified later in WP2), metering device IDs (if any) • For Prosumer Connections: Internal Connection Point ID; Smart Meter ID; number of phases of prosumer connection; number, IDs and types of connected loads and generators (detailed parameters to be specified later in WP2), metering device IDs. • For Cables/Lines: Cable ID, number of phases, Cable Length, Cable Parameters (Resistance, Impedance, etc.), Types and IDs of entities connected by start and end of the cable; optionally also GPS coordinates of start and end of cable.	M	YES	-
GTS-4	The Grid Topology Subsystem should also be able to provide basic MV grid topology information – to be specified later by WP2 what is needed.	O	NO	-
GTS-5	The Grid Topology Subsystem should be able to publish changes of the LV grid topology to the ICT Gateway.	O	YES	-
GTS-6	The Grid Topology Subsystem (GTS) should be able to provide information about the accuracy of LV topology information (e.g. ranges for actual cable lengths) to the ICT Gateway if available. The GTS should provide and appropriately label default values for missing information (e.g. often the case for cable lengths to the households) or derive estimates for such information from e.g. GPS coordinates.	O	NO	-

Interface to Measurement and Actuation Subsystem (MAS)

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
MAS-1	The ICT Gateway must support two different registration processes: MAS-initiated and Gateway-initiated. During the registration, the following information must be communicated by the MAS to the ICT Gateway: • Type of MAS: e.g. AMI, Inverter Web, Inverter RTU, Substation RTU, mobile PQ RTU, SCADA • Number of measurement devices managed by the MAS • Number of actuation devices managed by the MAS	M	YES	-

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
MAS-2	When requested by the ICT Gateway, the MAS must provide the following information for all measurement and actuation device (only those in 'scope' for the requesting DSO) • IDs of all measurement and actuation devices • Measurement capabilities: Voltages, Currents, Power, Energy, per-phase or aggregated/averaged over phases, instantaneous or time averaged measures, min and max averaging intervals, measurement precision, measurement timestamp precision • Capabilities to adjust measurements: precision ranges, averaging interval ranges, clock synchronisation ranges, others to be defined in WP3/WP2 • Supported event notifications: threshold crossings, device unreachability, device shutdown, device start-up, others to be specified in WP2. • Actuation capabilities: None, Q(U), P(U), curtailment capabilities, change of state (e.g. open/close, tap level), (others to be specified in WP2/WP4)	M	YES	-

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
MAS-3	The IDs and additional information provided by the MAS must enable the ICT Gateway to uniquely link the measurement/actuation point to the grid topology. One or more of the following solutions must therefore be supported by the MAS • The MAS provides an ID that can be linked to the grid topology directly, e.g. the Metering Point D of a connection point or the substation ID. How this ID is obtained in the MAS is out of scope for Net2DG. • The MAS provides the geographic coordinates of the measurement/actuation point. • The MAS provides a reference measurement that the ICT Gateway can compare to different measurements from other subsystems (e.g. inverter SM measurement compared to AMI SM measurement) and thereby identify the measurement point in correspondence to another subsystem.	M	YES	Except for lats bullet, which currently is not implemented.
MAS-4	The MAS must provide the ICT Gateway the possibility to send requests for readings of one or more measurement device IDs and then provide the corresponding measurement data.	M	YES	-
MAS-5	The MAS should be able to actively publish new measurement data to the ICT gateway.	O	YES	-
MAS-6	The MAS should be able to detect events of different type and to publish these events to the ICT Gateway.	O	YES	-

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
MAS-7	MAS and ICT Gateway must mutually authenticate each other. They should use integrity and confidentiality protection for their communication, if supported by the MAS capabilities. If no protection mechanism is supported, an additional security analysis must be made to assess viability of additional security mechanism (VPNs or similar).	M	YES	-
MAS-8	The MAS should inform the ICT Gateway whether it uses authentication and integrity protection mechanisms to connect to the individual measurement and actuation devices so that the ICT Gateway can derive a 'trustworthiness' meta attribute to the data from the measurement/actuation devices.	O	NO	-
MAS-9	Data collection on the MAS and data exchange with the ICT Gateway must be conform to GDPR, this implies that required documentation for usage, flows and security measures must be made.	M	YES	-

Interface to Actuation

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
ACT-1	The Actuation Subsystem must be able to receive requests to modify setpoints from the ICT Gateway and communicate back a status to the ICT Gateway whether this setpoint was completely, partially or not at all implemented.	M	NO	It is planned to be completed and integrated within WP4 and tested in WP5.

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
ACT-2	The Actuation subsystem must be able to receive request to reset setpoints to default values from the ICT Gateway and communicate back a status to the ICT Gateway whether this setpoint was completely, partially or not at all implemented.	M	NO	It is planned to be completed and integrated within WP4 and tested in WP5.

Interface to AMI

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
AMI-1	The AMI system must support interval-based data collection from all relevant meter points in the AMI system.	M	YES	Currently the data Collection is based on historical data as described in Section 5.1.3
AMI-2	The AMI headend should provide the data to the ICT Gateway using the CIM standard.	O	NO	-
AMI-3	The AMI interface should support identity-based authentication and data-in-transport protection based on industry standard encryption mechanism.	O	YES	-
AMI-4	The data collection must be configurable in terms of which data should be collected. The AMI system must be able to validate a specified set of data collection requests in terms of data communication capacity prior to accepting a new configuration request in order to avoid congestion in the network.	M	NO	Currently the data Collection is based on historical data as described in Section 5.1.3
AMI-5	The AMI system must support configuration of interval loggers (logger interval, data types) for grid surveillance.	M	NO	Currently the data Collection is based on historical

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
				data as described in Section 5.1.3
AMI-6	The AMI system should be able to prioritize data collection to facilitate different use-cases and their associated needs. The prioritization should as a minimum support high-priority data types (billing data, for example) and background data collection for grid data processing purposes	O	NO	-
AMI-7	The AMI data collection should support data collection with different reliability characteristics, as a minimum the following types should be supported: Reliable: All data of a certain types must be collected, the AMI system must continue retrying until all data are collected (required for billing data). Best effort: It should be possible to configure collection of certain datatypes as best effort. Best effort data collection is characterized by having a finite number of retries and limited data collection window. If a certain datalogger is missed for a specific time window, the AMI system will not attempt to fetch it later, instead it should move forward to the next time window (could be 6hour intervals).	O	NO	-
AMI-8	It should be possible to configure the AMI system to initiate data collection based on configurable events (could be an overvoltage). When the trigger event happens, the AMI system should automatically collect a predefined dataset for the affected meter(s)	O	NO	-
AMI-9	The AMI system must support data collection from multiple types of usage points and multiple types of metering equipment. Types should at least include: • Households • Industries • Production sites (windmills/PVs) • Substations. Types of metering equipment should include:	M	YES	Currently the data Collection is based on historical data as described in Section 5.1.3

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
	• DC types of household meters • CT types of industry meters (SME / small production sites) • High precision meters for large scale industries and production • CT meters for substation monitoring • Multi-instruments for substation monitoring. Data collected from all kinds of metering equipment should be exposed to attached systems via a harmonized interface (ex. CIM based).			

Interface to Inverter Subsystem

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
Inv-1	The Inverter Web or RTU Headend must provide upon request by the ICT Gateway for each installation o The Metering Point ID belonging to this installation. o The number and type (PV, peak Power) of generation units connected at the installation- o The number and type of storage units connected at the installation (if any). o The ID of the additional Smart Meter that is part of the installation (if any). o A reference to the alternative access via the inverter WEB/RTU headend, allowing the ICT gateway to identify the installation to be the same for the different access paths.	M	YES	-
Inv-2	The Inverter Web or RTU Headend should be able to provide a test measurement trace of voltages and/or Power/Energy Readings from the Smart Meter belonging to the inverter installation to the ICT Gateway. This test measurement trace should be of a form that allows the ICT Gateway to identify the equivalent AMI Smart Meter and hence to identify or verify the Smart Meter ID. Afterwards the ICT gateway send the correct metering point ID to the WEB/RTU Headend	O	NO	-

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
	so that it may stores it for future communication.			

RTU Subsystems

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
RTU-1	The ICT Gateway should be able to ask the RTU headend to 'ping' a specified set of RTUs. The Headend will then respond with the reachability information about these head-ends and optionally also provide other parameters: round-trip time of ping to RTU, packet loss rate of communication to RTU, status of connected measurement and actuation device.	O	NO	It has been implemente d a script on the RTU HE that pings a set IP address and if it fails for 3 consecutive times (done every 30 sec) it reboots the device.

Security

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
Sec-01	Any subsystem Head-End Server must mutually authenticate with the ICT Gateway before being able to exchange data with ICT Gateway.	M	YES	-
Sec-02	Cryptographic schemes must be enforced for external communication (i.e. communication between ICT Gateway and Head-End Servers that are not placed at the DSO domain) and support both integrity and confidentially protection.	M	YES	-
Sec-03	ICT Gateway should protect internal communication using authentication and encryption.	O	YES	-

Req ID	Req Description	Mandatory/ Optional	Satisfied (Yes/No)	Comment
Sec-04	Net2DG must be able to authenticate and authorise remote maintenance access before allowing interacting with the system. Sec-03-2: Local maintenance access via the GUI shall be limited to users that re logged-in with root credentials.	M	YES	-
Sec-05	ICT Gateway must record any subsystem connected ad user logged to the system.	M	YES	-
Sec-06	ICT Gateway should terminate a remote session at the end of the session or after a pre-defined time of inactivity.	O	NO	-
Sec-07	ICT Gateway should deploy Intrusion prevention system on the network to prevent unauthorised intrusion on the network.	O	NO	-
Sec-08	ICT Gateway should implement malicious code protection mechanisms to avoid installing of malicious code.	O	NO	-
Sec-09	ICT Gateway should implement anomaly detection on measurement data to detect attacks on data integrity.	O	YES	-
Sec-10	ICT Gateway should implement anomaly detection on timestamps to detect attacks on time synchronization.	O	NO	-