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:	**D1.2**
Deliverable title:	**Initial Baseline Architecture**
Work package:	WP1
Due date of deliverable:	31/08/2018
Actual submission date:	M8 - 31/08/2018
Start date of project:	01/01/2018
Duration:	42 months
Reviewer(s):	Nuno Silva (GD), Jan Dimon Bendtsen (AAU-AC)
Editor:	Erik B. Pedersen (KAM)
Author:	Hans Peter Schwefel (GD), Nuno Silva (GD), Domagoj Drenjanac (GD), Rasmus Løvenstein Olsen (AAU-WCN), Jan Dimon Bendsten (AAU-AC), Nicola Nostro (RT), Lorenzo Vinerbi (RT), Lorenzo Falai (RT), Rosaria Esposito (RT), Christoph Winter (Fronius), Nicole Diewald (Fronius), Hannes Heigl (Fronius), Erik B. Pedersen (KAM)
Contributing partners:	Resiltech, GridData, AAU-AT, AAU-WCN, Kamstrup, Fronius

Dissemination Level of this Deliverable:	**PU**
Public	*PU*
Confidential, only for members of the consortium (including the Commission Services)	*CO*

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

Document history

Version nr.	Date	Authors	Changed chapters
1.0	31/08/2018	Erik B. Pedersen	First version for submission to EC

Statement of Originality

This deliverable contains original unpublished work except where clearly indicated otherwise.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

Table of Contents

List of Figures

List of Tables

1 Executive Summary

This deliverable introduces the overall system architecture of the Net2DG solution and its system context for execution. Starting off from the use-cases and application requirements that have been derived earlier in D1.1, this document defines overall system requirements on scalability, maintainability, and security. It then introduces further use-cases for system management and maintenance of the Net2DG system.

The central entity for the architecture of Net2DG is the ICT Gateway connecting to data and actuation subsystems, for each of which there are subsystem head-ends as point of contact. Some of these head-end servers are already existing devices, most notably for AMI and inverter web systems, while the head-end servers will need to be developed in Net2DG for the grid topology subsystem and for data sources and actuation units that are connected via remote terminal units. Utilizing basic interaction patterns for publish-subscribe and for request-reply, message flows for the interaction between applications, ICT Gateway, and data and actuation subsystems are introduced for the main types of application use-cases of Net2DG.

The overall ICT architecture for Net2DG is described, in which the Net2DG ICT Gateway and applications servers are deployed at the DSO domain, while head-end servers and data source placement varies across different subsystem types. From the message flows and the derived ICT architecture, requirements on the interfaces to of the ICT gateway to different subsystems are derived, and a high-level description of the sub-systems is provided. Finally, first solution directions for the interface between applications and ICT Gateway are highlighted and the security aspects of the Net2DG architecture are discussed based on an initial threat analysis.

This document will be the basis for application development in WPs2 and 4, and for ICT Gateway and interface development in WP3. The architecture will be updated during Year 2 of the project based on feedback from these work-packages.

2 Introduction

The Net2DG System Architecture Description acts as a blueprint for the project execution by identifying major building blocks and their tasks and responsibilities.

It will take outset in the functional requirements identified in the Net2DG D1.1 document (D1.1[1]). In addition to these requirements, this document will specify functional requirements related to system administration as well as important non-functional requirements, which should be handled on a system architecture level.

The architecture will be described from different angles or views covering structural aspects (major building blocks and interfaces in between), dynamic behaviour (as sequence diagrams) and deployment-oriented aspects, such as the communication architecture, the security architecture and the IT deployment architecture. The latter will focus on the specific deployments at the two DSO partners.

It is not intended to be a full-coverage design description, but a guidance to the implementation done in various Net2DG work packages. As such it focuses on the most important and design driving use-cases, while others, which resembles these, will be detailed later in WP2, WP3 and WP4.

[1] Case Study Specifications & Application Requirements, Net2DG deliverable D1.1

3 Architectural Principles

A principle is a fundamental statement of belief, approach, or intent that helps drive answers to important decisions. It may refer to current circumstances or a desired future state. A good principle is constructive, reasoned, well-articulated, testable and significant.
Architectural principles can be used to link stakeholder concerns (through its rationale) to architectural decisions (through its implications):

Table 1 Using principles to link concerns and decisions

Architectural decisions applies to building blocks. Building blocks refers to blocks at different levels of abstractions that can put together to build something. At the system level, a building block may be a component and at the component level, a building block may be a service, module, or software package. In the design phase, a building block may be a pattern or style.

Use open standards

Statement	Use open standards that promote interoperability for data, applications, and technology.
Rational	Interoperability is important for integration and re-use of building blocks. Interoperability is achieved with robust implementations of documented, free and maintained open standards.
Implication	1. Interoperability and industry standards will be followed unless there is a compelling business reason to implement a non-standard solution.

Separation of concerns

Statement	Use separation of concerns to promote changeability of building blocks.
Rational	Changeability is important to improve development time and cost with regard to future changes. Changeability is achieved through low coupling and high cohesion. Low coupling *between* building blocks promote reusability and variance points. High cohesion *within* building blocks promote clear responsibilities and isolation of change.
Implication	1. Data will be self-descriptive unless there is a compelling business reason not to. 2. Interfaces will be stateless and version controlled. 3. Applications will use abstractions of communication technologies. 4. Clear variance points will be identified when designing and implementing new features.

	5. Circular references will be avoided between building blocks. 6. Building blocks will not know about internal details of other building blocks. 7. Building blocks will be semantically self-contained. 8. Building blocks will internally handle errors that cannot be mitigated by other building blocks. 9. Building blocks will be testable in isolation. 10. The robustness principle of RFC1122 will be followed when implementing interfaces: “Be liberal in what you accept and conservative in what you send”. 11. All inputs from other building blocks will be validated.

Keep it simple

Statement	Keep features and solutions simple and open for iterative improvements.
Rational	Simplicity is important for development efficiency and quality. Simple features are easier to understand and implement which will make them less error prone. They will also fit better into an agile development cycle where more room can be made for emergent design and less time can be spent on architecture details.
Implication	1. Features will be kept to a minimum in terms of functionality and new technologies as well as important architectural changes are implemented in platform projects. 2. Bells and whistles will be avoided unless they *are* the business case. 3. Features will be designed for iterative improvements, such may require re-factoring.

Security by design

Statement	Consider security when designing and implementing new features.
Rational	Security is important for correct operations and privacy concerns but can be cumbersome and negatively affect user-friendliness. Thinking about security during the design phase will minimize the impact on other functionality, prevent security by obscurity, and help reach the right level of security based on a security risk assessment.
Implication	1. Security initiatives will be based on a security risk assessment. 2. The out-of-the-box user experience will be based on secure default settings. 3. Role based access control and audit logging will be enforced on all external interfaces and considered on all internal interfaces. 4. Defense in depth will be used to mitigate the impact of vulnerabilities and make it difficult to exploit these. 5. Users will be granted the least amount of privileges required to perform their business processes. 6. Separation of duties (more than one person is needed to complete a task) will be considered on critical functionality to prevent fraud or errors.

Design for operations

Statement	Consider daily operation when designing features to ensure efficient and cost effective operation based on availability of relevant data and system insight.
Rational	Operations is part of the total cost of ownership and many hours can be spent during tedious tasks or operating a misbehaving system without visibility into its workings.
Implication	1. Automate operational tasks to make them repeatable and less prone to human errors. 2. Logging is enabled in production so insights are available when they are needed the most. 3. Logging formats and metrics are unified through common schemas. 4. Instruments for root cause analysis are employed so the underlying cause of failures can be found after the failure happened.

System efficiency

Statement	Design for cost-efficient deployments for small to medium sized DSOs
Rational	Sufficient scalability and performance is important to deliver core business functions cost-efficiently and meet required service level agreements (SLA). The application nature of Net2DG might increase data throughput significantly making small/medium sized DSO resemble larger DSO in terms of computational requirements.
Implication	1. Scale horizontal by partitioning data storage and providing parallelism in data processing when applicable. 2. Consider caching to minimize I/O overhead and avoid complex re-computations. 3. Consider distribution of load to avoid peaks and efficient utilization of resources. 4. Embrace eventual consistency, which gives higher availability in the presence of network partitioning (CAP theorem). 5. Asynchronous instead of synchronous communication. Only provide as fresh data as needed and limit the use of synchronous operations. 6. Always consider bulk operations before single operations.

4 System Requirements

The section presents the non-functional system requirements for the Net2DG project.

Requirement	**Scalability:** 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. SYS-02: The actual prototype deployment in Net2DG must support the handling of grids with up to 5000 measurement points and 200 secondary substations.
Rational	The main target for Net2DG is small to medium-size DSO in Europe; this puts the scalability range from few thousands to 50-60.000 measurement points.

Requirement	**Availability:** 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. SYS-04: The Net2DG solution should have a maximum downtime of 100 hours per year (98,85%).
Rational	The Net2DG solution provides new innovative data processing and control coordination solutions for the LV grids and relies on data from existing systems. However, the implementation of the Net2DG solution will not affect other DSO systems (such as MV SCADA or Billing systems) and affect the availability of those. Therefore, the rationale for the availability requirement for the Net2DG solution is set to a level that the usefulness of the provided services to the DSO is not affected.

Requirement	**Security:** SYS-05: Authenticity, Integrity, and confidentiality: Requirements for ensuring authenticity, confidentiality and protecting messages integrity shall be identified, and appropriate controls identified and implemented.
Rational	GDPR and ordinary operational security concerns mandates that the solution is based on a security-by-design approach. The framework for the derivation of more detailed security requirements is developed in Section 9.

Requirement	**System platform:** 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. SYS-07: For small installations and test purposes, it must be possible to execute on a single server instance.

	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.
Rational	Most DSO environments are today based on Microsoft Windows, to avoid introducing non-standard technologies into their datacenter; the Net2DG should be based on the same technology stack. Furthermore, there is an ongoing trend towards virtualized environments and even cloud based solutions. In order to reduce both IT CAPEX and OPEX spendings.

Requirement	**System maintenance:** SYS-09: It must be possible to install and upgrade the Net2DG solution. 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. SYS-11: Software maintenance should only be possible with the right credentials.
Rational	To accommodate a continuous evolution of the Net2DG solution, it is crucial that SW maintenance is efficiently supported by the software and system deployment. In the long run, SW maintenance should support automatization using standard tools.

Requirement	**System troubleshooting:** SYS-12: All Net2DG components must support debug logging; As default, log level should be “warning”. Log files should be stored locally. SYS-13: It shall be possible to activate a detailed tracing of actions by a local configuration. SYS-14: Log files for debug purposes must not contain privacy sensitive information. SYS-15: The system must make a separate audit trail for any action done by the operator.
Rational	Efficient means to troubleshoot during prototyping and later production rollout is crucial in order to achieve a high quality product and maintain low response times for system support.

Requirement	**System clean-up:** SYS-16: The Net2DG solution must assure that stored data is persistently removed after a configurable time period.
Rational	Data is not allowed to be stored infinitely for reasons of resource efficiency and data protection.

5 System Administration and Masterdata Management Use-cases

This section contains the derived system level use-cases from the system administration user-stories in D1.1[2]. These use-cases will be considered according to their given prioritization in the development work in WP3.

5.1 System Administration Usecases

ID and name:	Admin-1: *Registration and authentication of data and actuation subsystems*
Parent user story	*System Administration and Masterdata Management*
Overview and goal	Registration and authentication of data and actuation subsystems at Net2DG system start
System applicability	*Whole Net2DG system*
Business rationale	*Making it easy to work with the Net2DG system. Saving cost for IT specialist to support use of the gateway. The burden on IT specialist regarding editing configuration files, system configuration, etc shall be kept to a minimum. Minimizing integration effort.*
Precondition	*DSO and subsystem operator have made an agreement that data will be provided to the DSO. The subsystem operator has configured an identification and proper (pre-shared) set of credentials for registration of its subsystem at the Net2DG system. For data owned by the DSO and required by the subsystem operator, a similar agreement should be in place.*
Actors:	*DSO operator, Subsystem operator, Net2DG system*
External stimulus	*DSO operator has (re)installed gateway and needs to configure the system. Connectivity to subsystem Head End is ensured.*
Main flow	1. DSO operator configures eligible subsystems in the Net2DG solution and starts the Net2DG system, which then initializes and starts the corresponding adaptors. 2. Net2DG system is in wait state for incoming registration requests 3. A subsystem sends a registration request to the Net2DG system 4. Net2DG system authenticates the request and registers the connection 5. Net2DG system obtains interaction capabilities and configures itself internally with located interaction capabilities 6. DSO receives a confirmation on the GUI, that the relevant actuator/sensor subsystems have been connected.

[2] Case Study Specifications & Application Requirements, Net2DG deliverable D1.1

Alternate flow	*For inverter web subsystems, also an inverse registration procedure is possible, i.e. the Gateway registers at the subsystem headend.* *Subsystem cannot contact the Net2DG System:* • *Failure messages needs to be displayed to the Subsystem operator* *Malicious or unauthorized connection is tried established* • *Net2DG cannot authenticate and/or authorized connection registration request. Net2DG logs event and may notify DSO operator of attempt to register unauthorized subsystem.*
Characteristics	*Time spent on this task by the DSO operator/subsystem operator to setup subsystem interaction (should ideally be equal to the time it takes to click discovery ~zero)*
Security impact	*Authentication of subsystem sources is critical: DSO does not want impersonated subsystems in the operational loop.* *Integrity of registration is important to avoid e.g. MiM attacks (e.g. change of IP addresses from original source, to a malicious source) or important information having changed, e.g. source information (credential, IP, port etc.)*

ID and name:	Admin-2: *Adding/removing data sources or actuation units*
Parent user story	*System Administration and Masterdata Management*
Overview and goal	To be able to add or remove data sources or actuation units while the system is running
System applicability	*Net2DG system functionality*
Business rationale	*Some units (actuators and sensors or even full data/actuation subsystems) may need to be replaced at run time, or for other reasons be taken out of service for a time period. This should not trigger unnecessary alarms that might distract the DSO operator, who has to waste time searching for non-existing faults.*
Precondition	*A Net2DG system in normal operation with no faults occurring.* *A need to add/remove a specific data source or actuation unit or subsystem for some time period.* *Net2DG system has setup a subscription from the subsystem on changes in data source or actuation unit availability.*
Actors:	*DSO operator* *Subsystem operator* *Net2DG system* *Applications that depend on units being added/removed* *Units to be added/removed and its related interface*
External stimulus	*A need occurs to add/remove a specific entity*

Main flow	1. *Subsystem pushes an update to Net2DG system indicating that an entity (sensor or actuator) has been added or removed.* 2. *Net2DG system adds/removes entries in internal database and sends software signals to dependent (subscribed) applications that a change has happened* 3. *If added – Net2DG system may make a check if source is also available* 4. *If removed – Net2DG system may send a confirmation of the processed removal to the subsystem headend.* 5. *Net2DG system reconfigures itself to having more or less information or control options available* 6. *DSO operator receives an update message* 7. *Net2DG logs the event*
Alternate flow	*Entity added/removed is not existing* - *Net2DG system should inform DSO operator with an error message* *Entity is not responding (when added)* - *Net2DG system should warn DSO operator*
Characteristics	*Time it takes to confirm operation (from DSO operator clicks add/remove until an OK message is shown)*
Security impact	*Authentication of added sources is critical (by the subsystem headend).* *Integrity of removing messages it critical.*

ID and name:	Admin-3: *Software Component Maintenance*
Parent user story	*System Administration and Masterdata Management*
Overview and goal	Adding or removing Software Components to the Net2DG system while in operation; updating them during operation This use case is related to the long-term life cycle of the Net2DG system.
System applicability	*System level*
Business rationale	*The Net2DG system should enable easy deployment of new smart grid applications by relieving the complexity of worrying about discovery and interfacing to data sources and actuator units. Being able to install/remove applications easily, would allow DSO operators to effectively configure their system to their needs without having the need for many IT specialists.*
Precondition	*Net2DG system is in operation and running and has a known set of information source interfaces as well as actuation interfaces.*
Actors:	*DSO operator, Net2DG system*

External stimulus	*DSO Operator has a need to use some application (e.g. voltage control) or remove an existing application (it may not be useful anymore or an application provider offers a better application)*
Main flow	1. DSO Operator clicks on install new application (or remove) 2. If install - Net2DG system checks available sources if requirements (licences and more) are met for this application. Net2DG system downloads and installs application. Application is initiated, reads needed configuration and setups subscription to needed information sources, and negotiates authentication with actuation units. 3. If uninstall - Net2DG system removes any subscription to information relevant to the application and informs any potential other applications that this application has been removed (the application may provide information to other apps). 4. DSO operator receives an OK or failure message
Alternate flow	*New installed application does not have access to relevant sources/actuators:* • *Net2DG system must send signals to the application if some requirements are not met. Application must either adapt and/or visually warn the DSO operator* *Removing an application leads other applications to not properly work* • *Before uninstalling any applications, a list of dependent applications shall be shown to the DSO operator.* *During the Net2DG development and assessment activities, this operation may also be done by other actors remotely, see Use-Case Admin-7.*
Characteristics	*Time spent on this task by the DSO operator for starting an installation, until the application is in a running condition.* *Alternatively, time spent for an IT specialist to manually install and get an application running*
Security impact	*Authentication of application sources is critical: DSO does not want malware to be installed.* *Integrity of application code is critical, as malware is not desired in the system.* *Availability less critical as this procedure is not to be executed very often.*

ID and name:	Admin-4: *Graceful shutdown*
Parent user story	*System Administration and Masterdata Management*
Overview and goal	*Graceful shutdown of the Net2DG system enabling later resume/restart without loss of data or work processes*
System applicability	*System level*

Business rationale	*A shutdown of Net2DG system could be required due to both scheduled and unforeseen events. The shutdown should be carried out in a reliable and safe way thus preventing data loss and giving the possibility to resume any interrupted processes.*
Precondition	*Net2DG system is properly in operation and running.*
Actors:	*DSO operator, Net2DG system*
External stimulus	*DSO Operator has a need to execute the shutdown of the system or an unexpected event requires the system to shutdown*
Main flow	1. In case of scheduled activity - DSO Operator clicks on shutdown or automatic shut down is triggered 2. The Net2DG system saves data, process status and other important information before shutdown is started 3. In case of an unexpected event requiring the shutdown – system should be able to automatically save all data and processes in order to (automatically) resume them after restarting process 4. In both previous cases events should be recorded in a log.
Alternate flow	*After restarting activity, the system is not able to properly recover the data or resume the process.* • *The system shall warn the DSO Operator/IT Operator, which shall be able to manually select one out of several valid starting condition: new system initialization, partial removal of data that creates inconsistencies, etc.* *This use-case may also be executed remotely by other actors, see Use-Case 7 below.*
Characteristics	*Time spent on this task by the operator for recovering*
Security impact	*Integrity of recovered data and authentication of applications on reboot.*

ID and name:	Admin-5: Net2DG *System Operation Dashboard*
Parent user story	*System Administration and Masterdata Management*
Overview and goal	*The correct operation or the occurrence of ICT faults of the Net2DG systems shall be continuously visualized to the DSO and system operator*
System applicability	*System level*
Business rationale	*The DSO operator must be able to verify that the Net2DG system is operating correctly.*
Precondition	*Net2DG system is in operation.*
Actors:	*DSO operator, Net2DG system*
External stimulus	*None – dashboard is continuously updated.*

Main flow	1. The Net2DG system shows status information about its own status (such as number of active applications, data volumes processed, etc., exact contents will be specified in WP2 and WP3) and about the reachability of data source subsystems and actuation subsystems continuously to the DSO.
Alternate flow	*Additional remote access to the dashboard is desired, see next use-case.*
Characteristics	*Methods shall be included to avoid that freezing of the user-interface (e.g. screen) shows outdated wrong information of the dash-board.*
Security impact	-

ID and name:	Admin-6: Remote Field- and Lab-Trial Operation and Management
Parent user story	*System Administration and Masterdata Management*
Overview and goal	*The technology partners in Net2DG shall be able to perform the basic operation and management tasks remotely for the field and lab trial during the Net2DG system development. This use case relates to the time scope of the Net2DG project lifetime.*
System applicability	*System level*
Business rationale	*The Net2DG system will evolve during the run-time of the project. Net2DG partners having to travel to the local site for each system update and for testing/validation step will not be time and cost efficient for the project.*
Precondition	*This use-case is specific to the prototype development and evaluation within Net2DG (WPs 2-5).*
Actors:	*Net2DG Technology Partners, Net2DG system*
External stimulus	*Net2DG system update, configuration update, validation, or debugging is required in the field or lab tests of WP5 is required.*

Main flow	1. The Net2DG technology partner coordinates the required actions with ALL involved Net2DG partners for the specific test site. 2. The Net2DG technology partner remotely connects to the Net2DG system at the test-site (field or lab). 3. The Net2DG technology partner can perform the following operations remotely • Start and stop software components of the Net2DG system at the remote test site (including support services such as NTP, DNS, etc.) • Remotely view the Net2DG system dashboard (of Use-case Admin-6) • Upload software components and configuration files to the remote test site • Inspect logging data of the Net2DG system at the remote site 4. After performing the actions/changes, the Net2DG technology partner documents the changes in a site-specific log. 5. An automatic logging of the origin, duration, and main actions of the remote connection is stored at the test site.
Alternate flow	-
Characteristics	*This use-case shall increase the efficiency (time, cost) of the Net2DG trials of WP5.*
Security impact	*As this use-case enables the upload of new software components and may also involve business sensitive information, the remote operation has to be done via a secure (authenticated, integrity protected, and encrypted) connection.*

5.2 Use-case Prioritization

UC – ID	Priority (1 highest)	Rational
Admin-1: Registration and authentication of data and actuation subsystems	1 – will be implemented	• A simple way to register and authenticate subsystem is critical as not to expose field tests and partners to security riscs. • More advanced and easy to use registration procedures and functionality is less critical for the life time of the project.
Admin-2: Adding/removing data sources or actuation units	3 – mostly part of headend functionality	• For AMIs and Inverter Web system, the functionality on headend side already exists (and will be used by Net2DG).

		For Headends that will be developed in NetDG, simple solutions will be applied.
Admin-3: SW Component Maintenance	5 – out of scope for Net2DG	• Should be addressed only after the whole system is quite mature and operational for some time (demo and field-tests are running successfully) • Requires a dedicated (in-cloud) infrastructure for repository of applications – also managing available applications in the repository should be supported • Relevant for scalable product
Admin-4: Graceful Shutdown	1 – will be implemented	• Important to have already in prototype development as frequent restarts are expected
Admin-5: System Operation Dashboard	2 – will be implemented	• A simple way of visualization will not take much effort and it will be helpful for testing
Admin-6: Remote trial operation	1 – will be implemented	• Without remote access to the test sites, the 'local' partner would need to perform a lot of specific and detailed actions during the Net2DG WP5 activities. This will not be feasible for our DSO partners (and likely also for AAU-lab).

Table 2 Priority of the various system administration use-cases

The marked high-priority use-cases will be considered for the component design and development within WP3.

6 System Architecture

This section outlines the overall system architecture with identification of subsystems, interfaces and allocation of responsibilities.

6.1 System Context

The proposed system architecture is very similar to a classical middleware-based architecture. The middleware layer provides a uniform application platform for domain-oriented applications by abstracting specific provider subsystem interface details into a normalised/harmonised data model and by taking care of issues related to reliability and security.

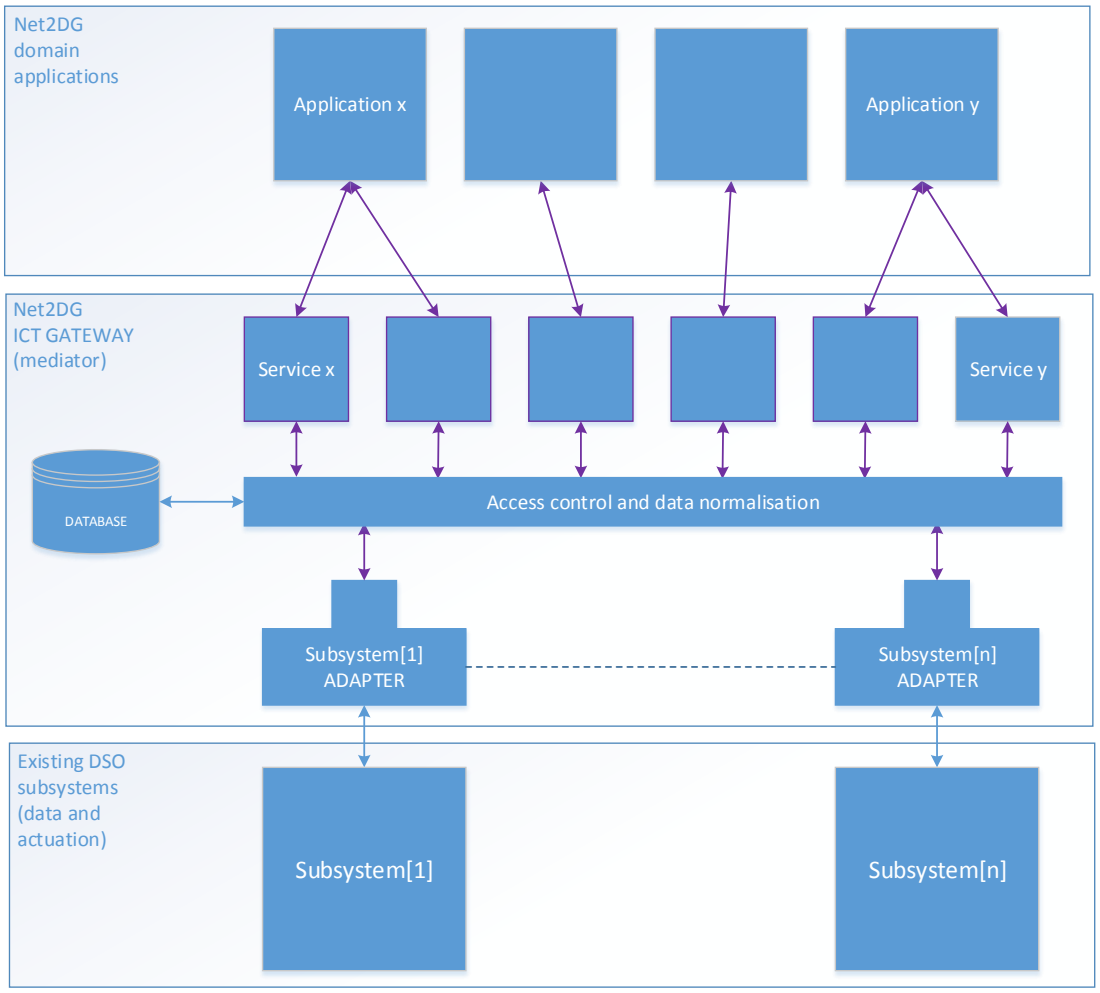

Figure 1 Net2DG System Architecture

The concrete instantiation of the architecture achieved by the Net2DG project will contain a set of specific subsystems and applications as required for implementation of the use-cases identified in D1.1[3].

For now, section 6.2 lists the set of subsystems and application already identified by the Net2DG project. This list will be updated as part of a planned revision of D1.2 (this document) at a later stage (M24).

6.2 Identified subsystem and applications and their naming

This section defines the components and subsystems visible on a system architecture level and defines their naming (for usages throughout the Net2DG project)

[3] Case Study Specifications & Application Requirements, Net2DG deliverable D1.1

Component/subsystem Naming	Architectural Role	Description
ICT Gateway	Mediator	The ICT gateway acts as mediator between data sourcing and actuation subsystems and domain applications. Supports data and configuration/control flows for all application use-cases.
Grid Topology Subsystem	Data subsystem	Provides access to information about the distribution grid topology and the connected consumers, generators, and prosumers. Accessed by ICT Gateway via 'Grid Topology Headend'.
Inverter WEB Subsystem	Data and actuation subsystem	Provides system level access to a set of inverters installed in a particular DSO's grid. Supports data retrieval and configuration/control of individual inverters. Accessed via 'Inverter Web Headend'.
AMI	Data and actuation subsystem	Provides access to the Advanced Metering Infrastructure for data retrieval and configuration/control of individual smart meters. Accessed via 'AMI Headend'
RTU Subsystem(s)	Data and actuation subsystem(s)	Provides access to distributed RTUs for data retrieval and configuration/control of individual RTUs (and attached measurement devices). There can be different RTU subsystems for different measurement and actuation device types, e.g. for inverters, storage, substation measurements, mobile PQ measurements. These are then called 'Inverter RTU Subsystem', 'Substation RTU Subsystem', etc. Each RTU subsystem has one 'RTU Head-End' that connects to the set of RTUs and is the point of contact for the ICT Gateway.

GUI	Graphical User Interface	Interacts with the local staff, which is assumed to be DSO staff. Provides input and output (mostly visualization) for all domain applications and for ICT Gateway functionalities of the Net2DG system.
ODET	Domain application	Provides outage detection capabilities and implements support for the outage detection use-case.
ODiag	Domain application	Provides outage diagnostics capabilities and implements support for the outage diagnostics use-case.
PM, GMon, LC, AVR (low prio: NDet, NDiag, LMRec, LMAct, CalcExch, MinExch)	Domain applications	Provide application functionality for the corresponding use-cases; see Chapters 7 and 8 of D1.1. (Low-prio applications are not expected to be considered in the first implementation cycle until Month 15)
Grid Model	Enabling application providing calculated grid data.	Operates on same level as applications and calculates grid parameters and stores them in the ICT Gateway

6.3 Dataflows between subsystems

6.3.1 Communication Patterns, Semantics and Syntax

Dataflows are described by sequence diagrams. The flows and interactions are based on generic patterns and with the same vocabulary. The following generic patterns are identified:

Publish-Subscribe:

Verb:	Description
Subscribe(type[x])	A request from an application to be notified when a certain criterion is fulfilled (event type X received etc.)
Publish	An announcement of a new data element from a subsystem or application
Notify	A notification sent from the mediator to the subscriber(s) of this specific data element.

These verbs are used to create the standard publish-subscribe pattern, in which a consumer application can subscribe to a set of data elements (events, automatic collected data etc.). The design pattern is built around a mediator function, which allows multiple subscribers to subscribe to various data elements regardless where the data source(s) (publish) are located or whether they support subscription or not. A generic message exchange sequence is shown below.

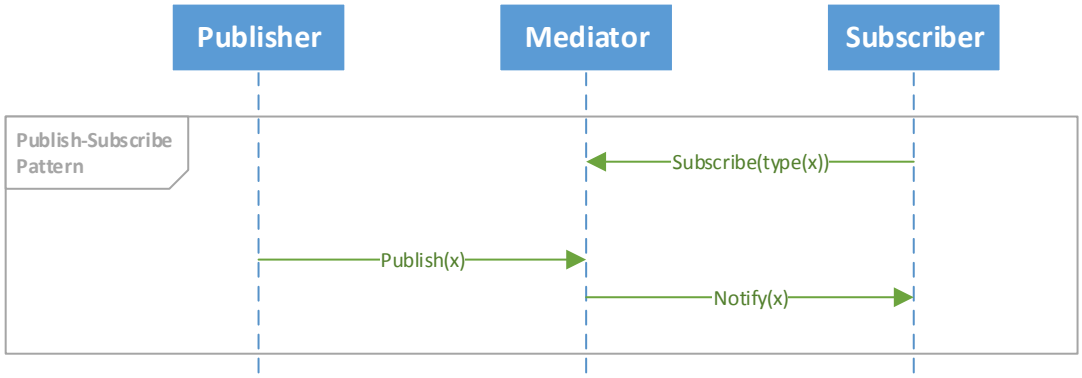

Figure 2 Publish-Subscribe Pattern

A subset of the publish-subscribe pattern could be a static stream API, where the mediator exposes streams with predefined data (could be consumption or voltage data automatically collected) required by multiple applications.

On-demand jobs:

Verb:	Description
AsyncRequest(order(x))	Request for asynchronous execution of order(x)
SyncRequest(order(x))	Request for synchronous execution of order(x)
Get(order(x))	Used to poll for status on an asynchronous order request.
Reply(status, [result])	Reply from order request, in case of asynchronous request, it contains a status on the acceptance of the order request (ok/nok). For the synchronous request, it contains an execution status and optionally order result.

Another important communication pattern is the on-demand job request. This implies that applications request data elements or wants to perform configuration or control actions. This pattern exists in an asynchronous (non-blocking) and synchronous (blocking) variant. The asynchronous pattern is preferable for most actions that requires field-site communication as the execution delay can be considerable. The message exchange for this variant is shown below:

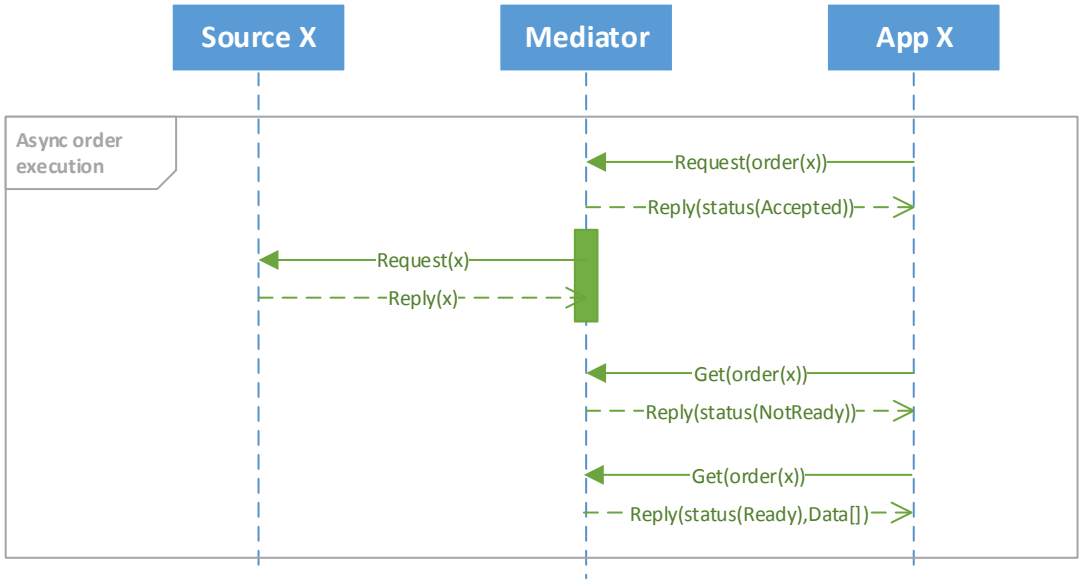

Figure 3 Asynchronous order handling

6.3.2 Basic System Functionalities

6.3.2.1 System Start-up

Before system start-up, the DSO has made legal agreements with any third party subsystem operator, based on which the subsystem operator enables the registration of the subsystem at the Gateway and also the DSO enables the subsystem authorisation at the Net2DG system.

System start-up consist of the following phases:

1. ICT GW initialisation and subsystem registration
2. Subsystem capability registration
3. Application start-up and synchronisation

When the system is up and running, it enters normal operation during which the various applications execute, and background synchronization will keep the whole system in a consistent state. It is a pre-requisite that subsystem contains the necessary capabilities and information to support minimum functionality, as an example, the GIS system is required to contain enough information to support the Net2DG grid analysis.

The three phases are shown in Figure 4, Figure 5 and Figure 7.

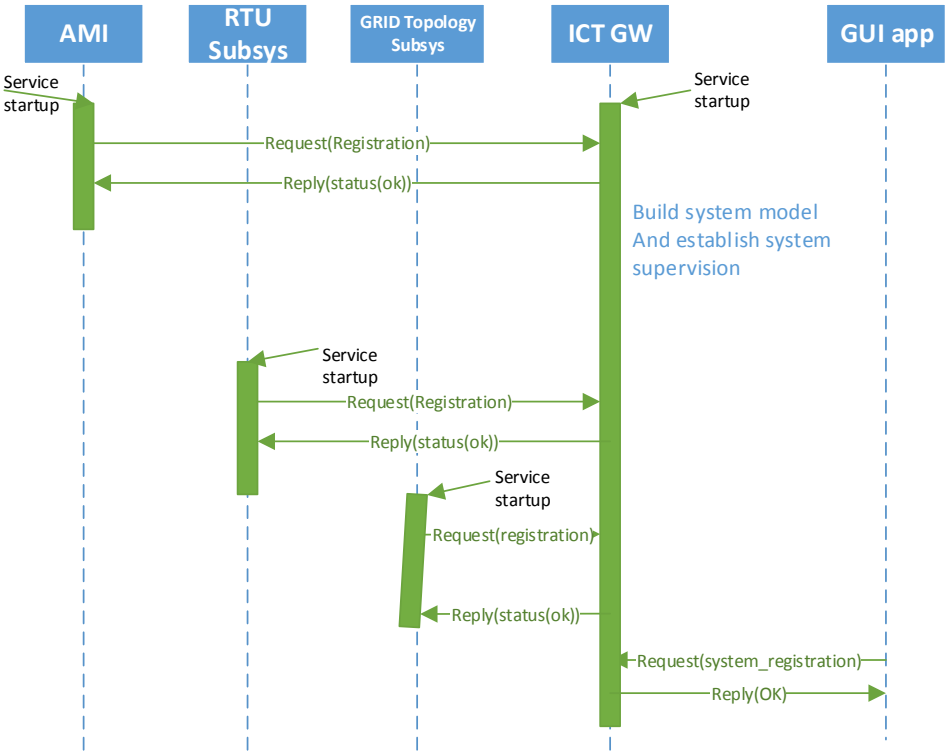

Figure 4 ICT Gateway initialisation and subsystem registration

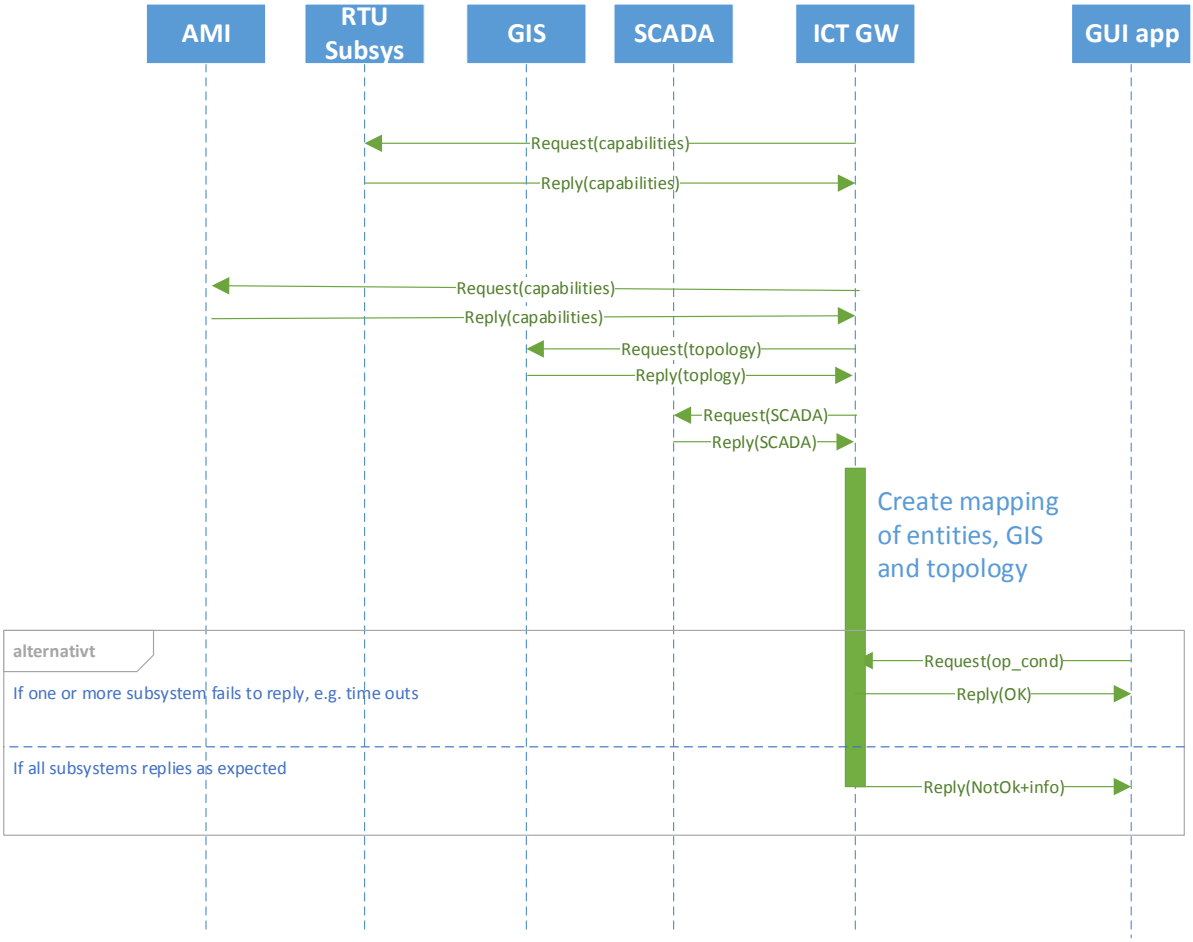

Figure 5 Subsystem capability registration

The main difference of inverter subsystems regarding the initial procedure is that inverter subsystems does not know to which DSO the inverters are connected, and so they do not know at which ICT gateway they have to register. Therefore, there is also a Gateway initiated registration procedure, which is outlined below in Figure 6 and Figure 7. However, even though the initial communication is different, the message exchange during application executions are the same from the perspective of the ICT gateway. The realization of data collection internally in the inverter subsystem is described later in Sect. 8.2.4.

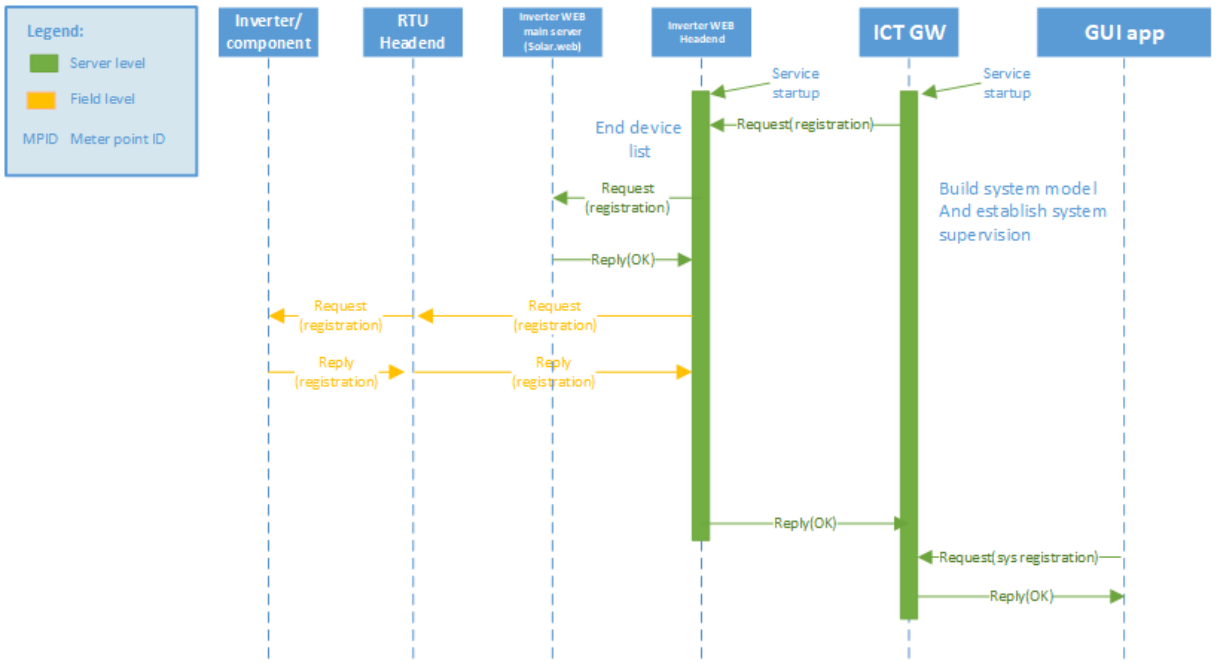

Figure 6 Inverter subsystem registration

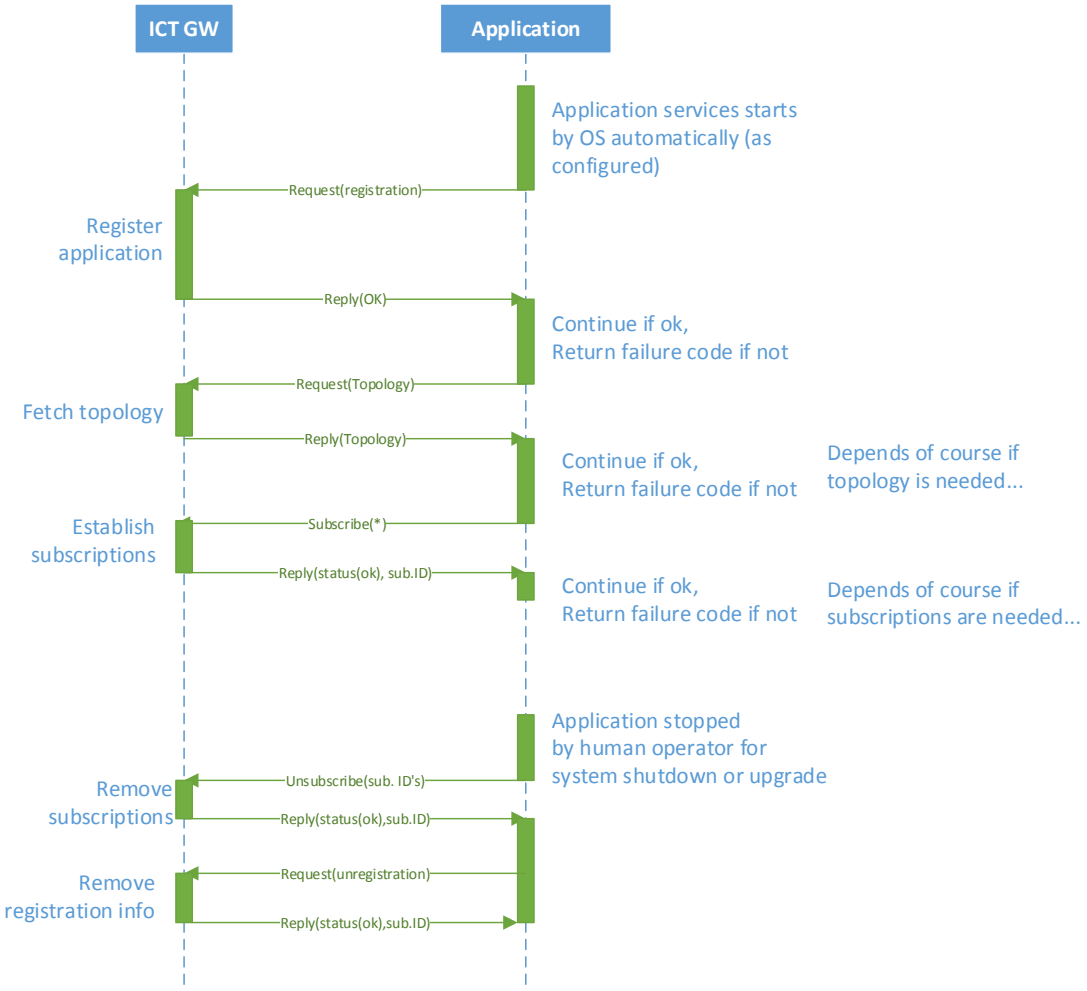

Figure 7 Application registration and de-registration

6.3.2.2 Generic data collection

Data collection consist of two schemes, a predefined/configured push scheme, which is part of the generic publish-subscribe pattern, and an on-demand request scheme, where data is collected based on requests from applications. Note that data can be measurement readings as well as event type data and also ICT reachability data (also called 'Ping' responses).

Push (publish-subscribe) data and event collection:

The ICT GW supports a publish-subscribe pattern towards the domain application, while acting as an end-point for automatic push (publish) of collected data and events from data and actuation subsystems. As there will be multiple applications requiring access to different subset of data and events, then the subscription scheme is not repeated between ICT GW and subsystems. Instead they will have a static end-point and a configuration for what data should be conveyed to the ICT GW (note these subsystems will have other end-points to serve as well). The scheme for events and data are shown below.

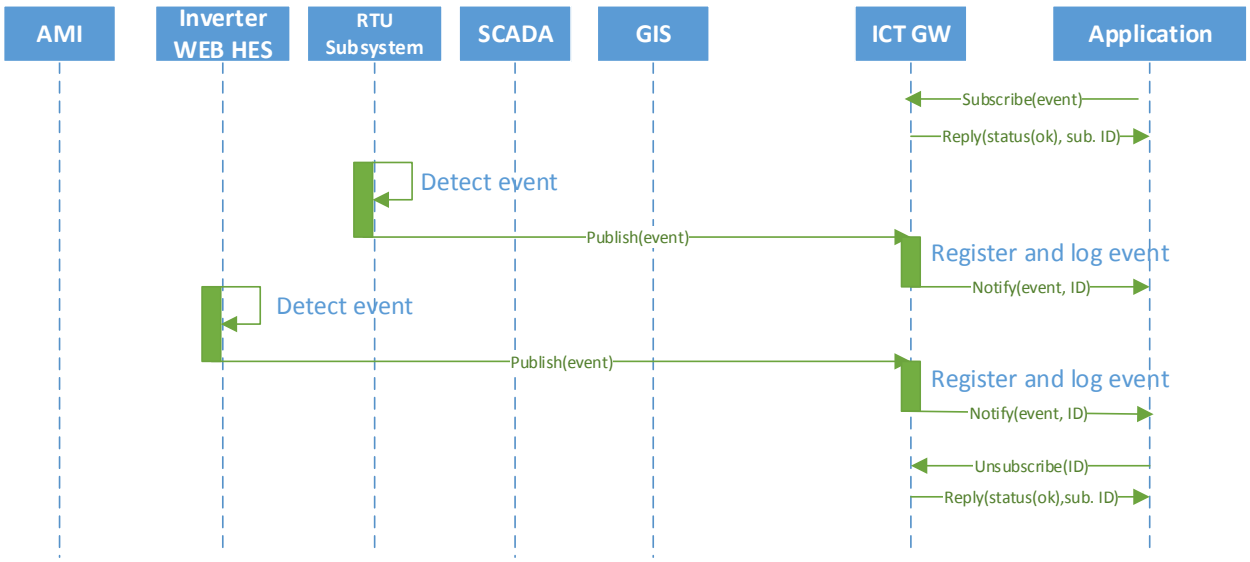

Figure 8 Event collection (Push/publish-subscribe)

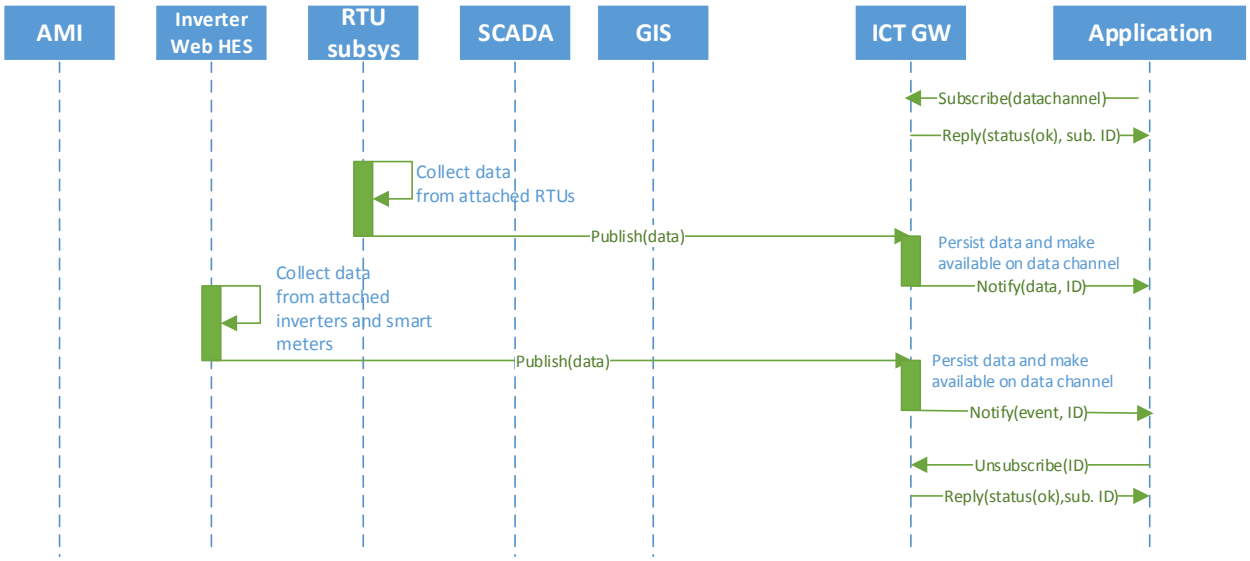

Figure 9 Automatic Data collection

If certain subsystem do not support push of data and events, the ICT GW adapter should implement the functionality on their behalf (not in the core GW functionality).

On-demand data collection:

On-demand data collection is used when applications require additional or different information to complete its processing. It utilizes the asynchronous order pattern (preferable) as shown below:

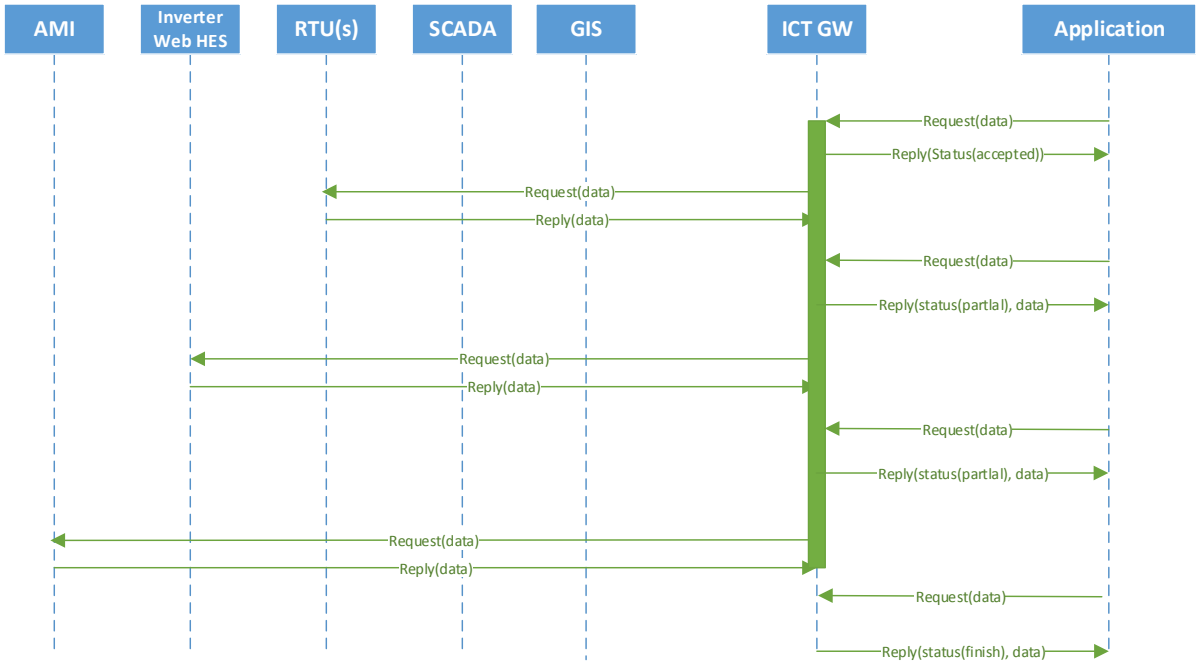

Figure 10 On-demand data collection

Interaction between ICT Gateway and Grid Model

As an important aspect in data normalization, recovery of missing data and/or validation of measured data rely on calculations using a grid model. This requires the ICT Gateway to interact with a grid model that provides estimated values. Figure 11 shows this process, which is executed in parallel with other activities and as the ICT gateway requires use of the grid model functionality.

The process shown is triggered by an application request for data, although it could also be triggered by the ICT Gateway itself as a part of a subscription based notification push to an application. For example, an application may have setup a subscription to specific information and before pushing information to this application, the ICT Gateway may perform a validation check or calculate missing information in similar fashion.

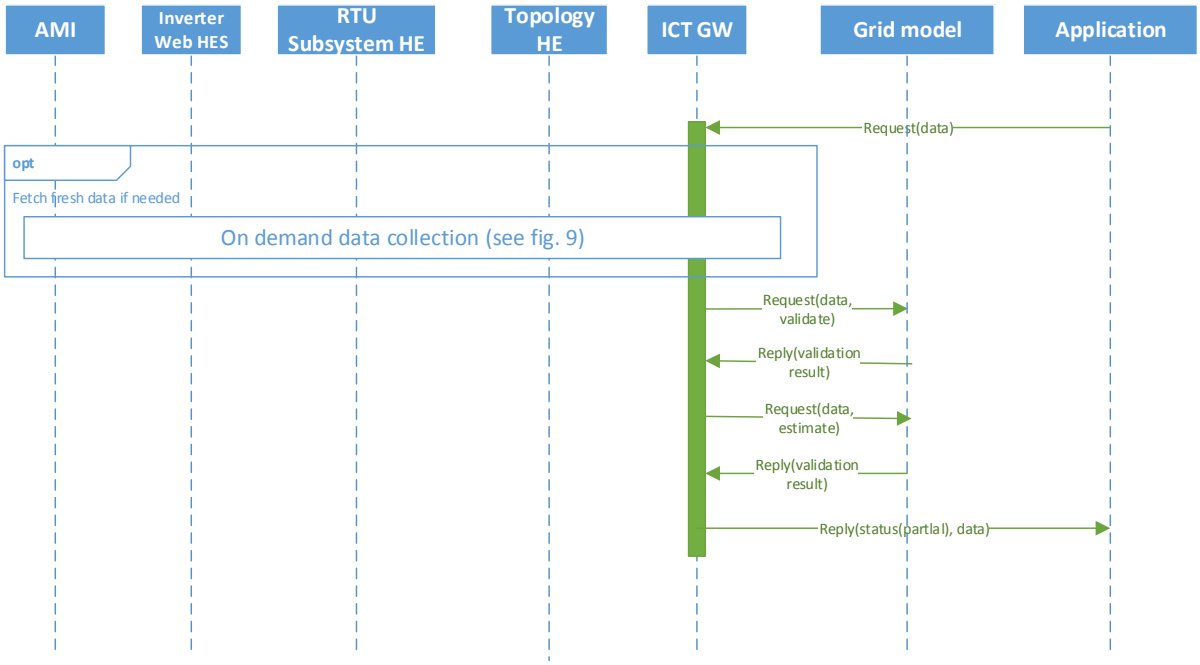

Figure 11: Interaction between ICT GW and Grid Model in order to validate values or calculate missing measurement values obtained by the data access process shown in Figure 9.

6.3.3 Application Use-cases

The application use-case is initiated once the system has passed the system start-up phases, which means that all the following sequence diagrams assume the previous message flows from Sect. 6.3.2.1 have been executed.

6.3.3.1 UC: Outage Detection (Event -scheme)

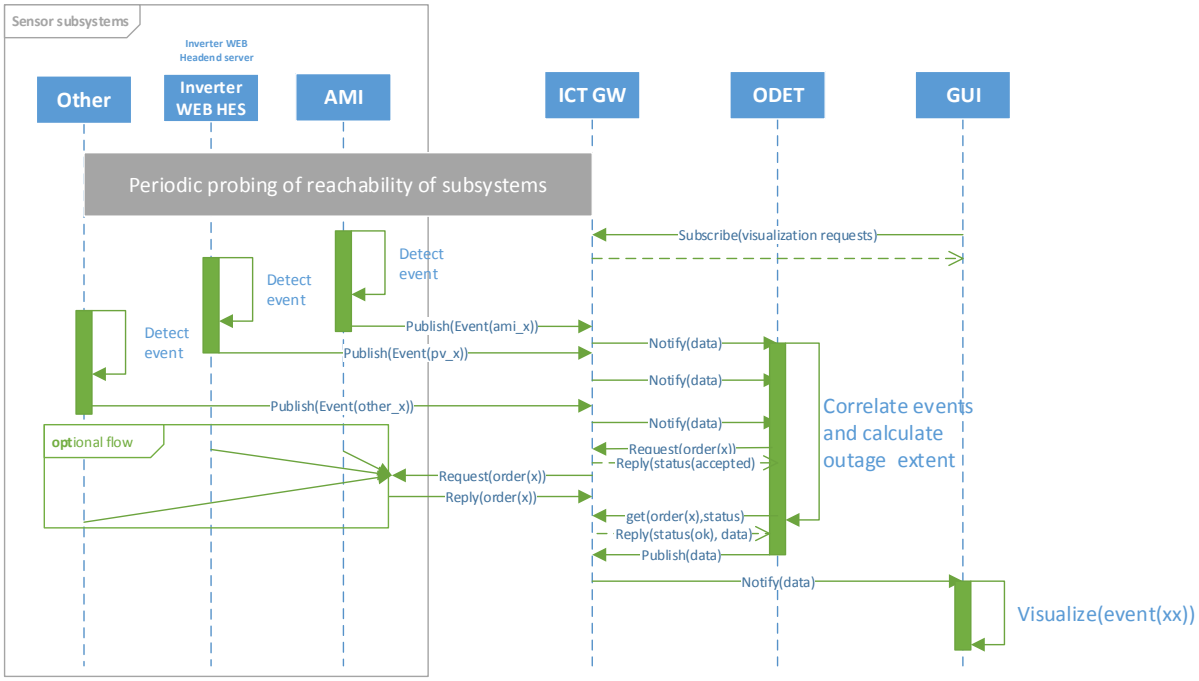

Figure 12 Outage Detection (ODET) use-case

The outage detection use-case relies on the correlation of events and measurement data from the available subsystems. Note that some events, e.g. unreachability of the subsystem, may be directly created by the ICT GW. Also, in case the subsystem's capabilities do not allow to detect required events, e.g. voltage boundary crossings, the corresponding adaptor in the ICT GW may create the corresponding event based on a regular push or active request of measurement data. The result of the outage detection is itself another event that is stored in the ICT Gateway and, based on an existing subscription, then visualized via the GUI application.

6.3.3.2 UC: Outage diagnostics (iterative data collection)

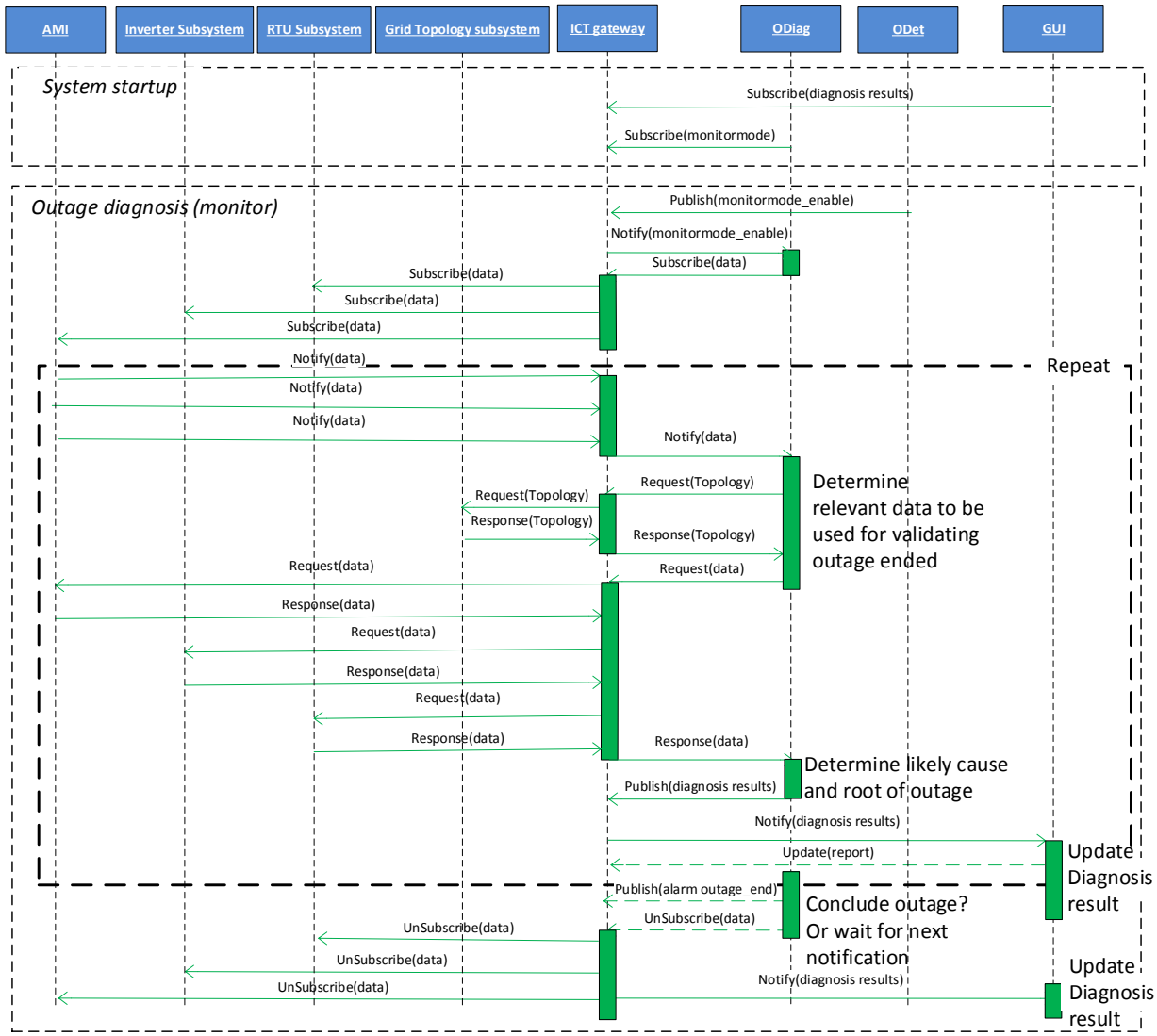

Figure 13 Outage Diagnosis (ODiag) use-case

The ODiag application is triggered by a detection event from the Odet application. It will subsequently iteratively request additional measurements from the affected LV grid until it can determine the likely cause(s) and locations of these causes of this outage, which will be published to the ICT Gateway. The latter event publication will trigger a corresponding visualization at the GUI. After a successful diagnosis and localization, the iterations will continue until the end of the outage can be confirmed, upon which the ODiag application will publish an overall outage report to the Gateway.

6.3.3.3 UC: Loss calculation and recording (data collection)

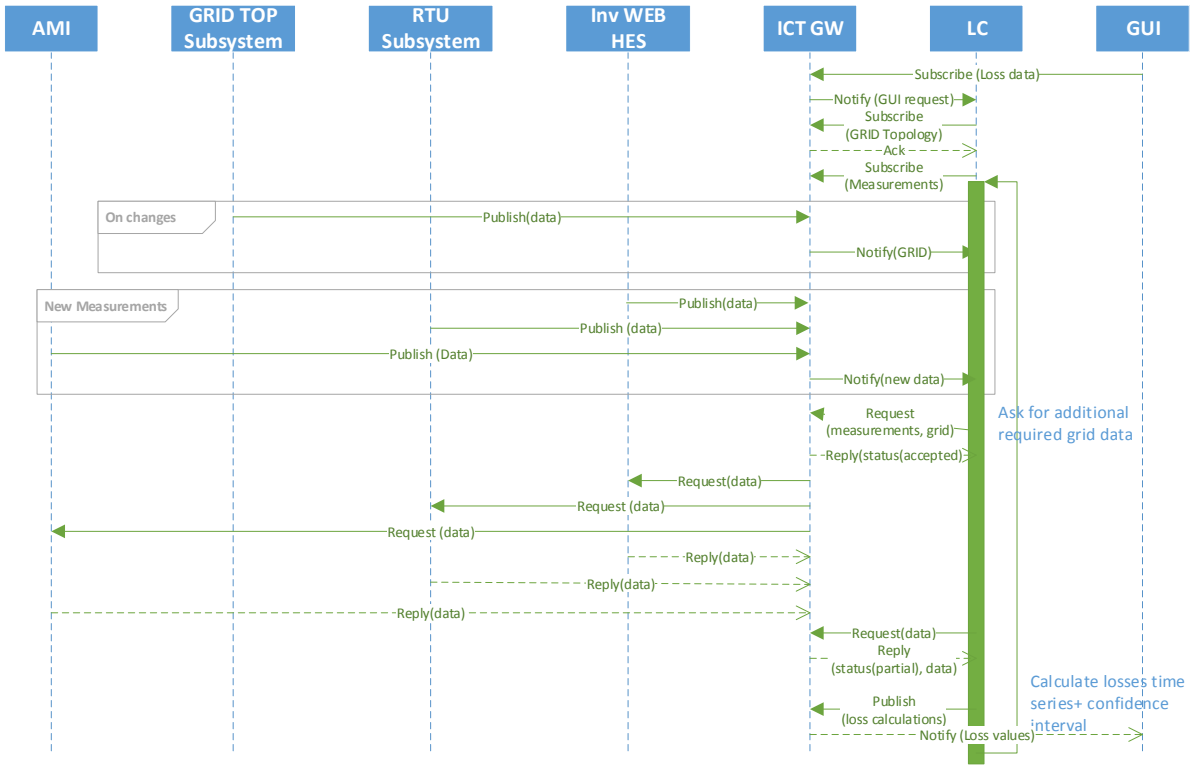

Figure 14 Loss Calculation and Recording (LC) use-case

The LC application is activated by a use command through the GUI. LC application will be executed based on historic topology and measurement data (see Figure 14), therefore, it gets the grid topology and subscribes to topology changes. Subsequently, LC application subscribes to all relevant parameters from the relevant parts of the LV grid (measurements or obtained by grid model). The LC application obtains time intervals of available measurements and calculates from these, for which sub-intervals it wants to perform the loss calculation (e.g. if measurement intervals are all 15 min. or higher, then the LC application will calculate losses for 15 min intervals). Note that for this request, the LC application is not interested in calculated values from the grid model, but only in actual measurement intervals. The ICT Gateway (IG) notifies LC application about new available data, which after receiving the data checks if the data is sufficient to calculate new loss values. If not enough data is available yet, the LC application waits for more or requests actively for additional values. LC application calculates loss values and publishes the loss values in the IG. The IG notifies GUI about new loss values, by which the GUI application is finally triggered for visualization.

6.3.3.4 UC: LV Grid Monitoring

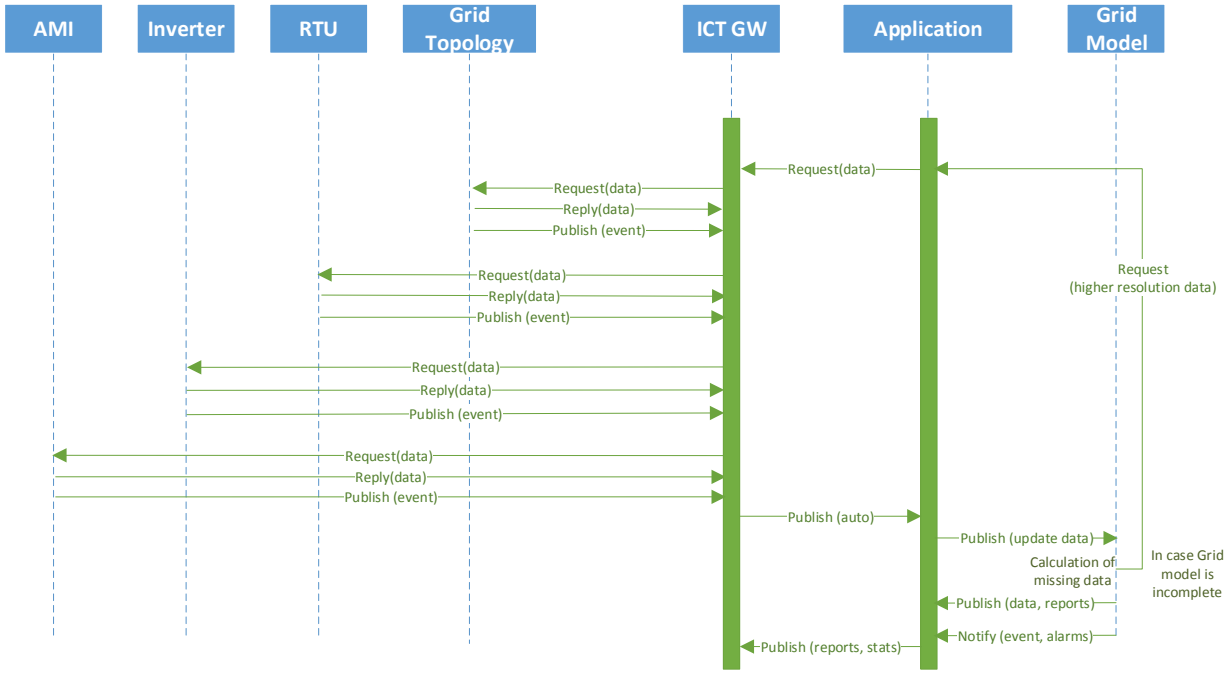

Figure 15 LV Grid Monitoring (GMon) use-case

The GMon application is running periodically whenever there is a change of data from the available sources. It can however be triggered also by the operator, for which case there must be an update on the information polled from the field. This is why both request/reply sequence and also automatic publishing of data from data sources to the ICT gateway are used.

The GMon application initiates the process by reading and/or requesting measurement from the field and assessing whether these complete the Grid Model. When this is not the case, it calculates the missing ones and populates the Grid Model. On this process, data refresh may be requested to increase the granularity of the available data so that the error margin is decreased. This is also the case for operational parameters (calculated or received) that are reaching previously defined thresholds. This may then trigger subsequent applications such as control related (for ex. AVR).

Periodically or when requested by the operator, reports, statistics and alarms are sent to the ICT Gateway so that KPIs can be calculated.

6.3.3.5 UC: Automatic Voltage Regulation (Control scheme)

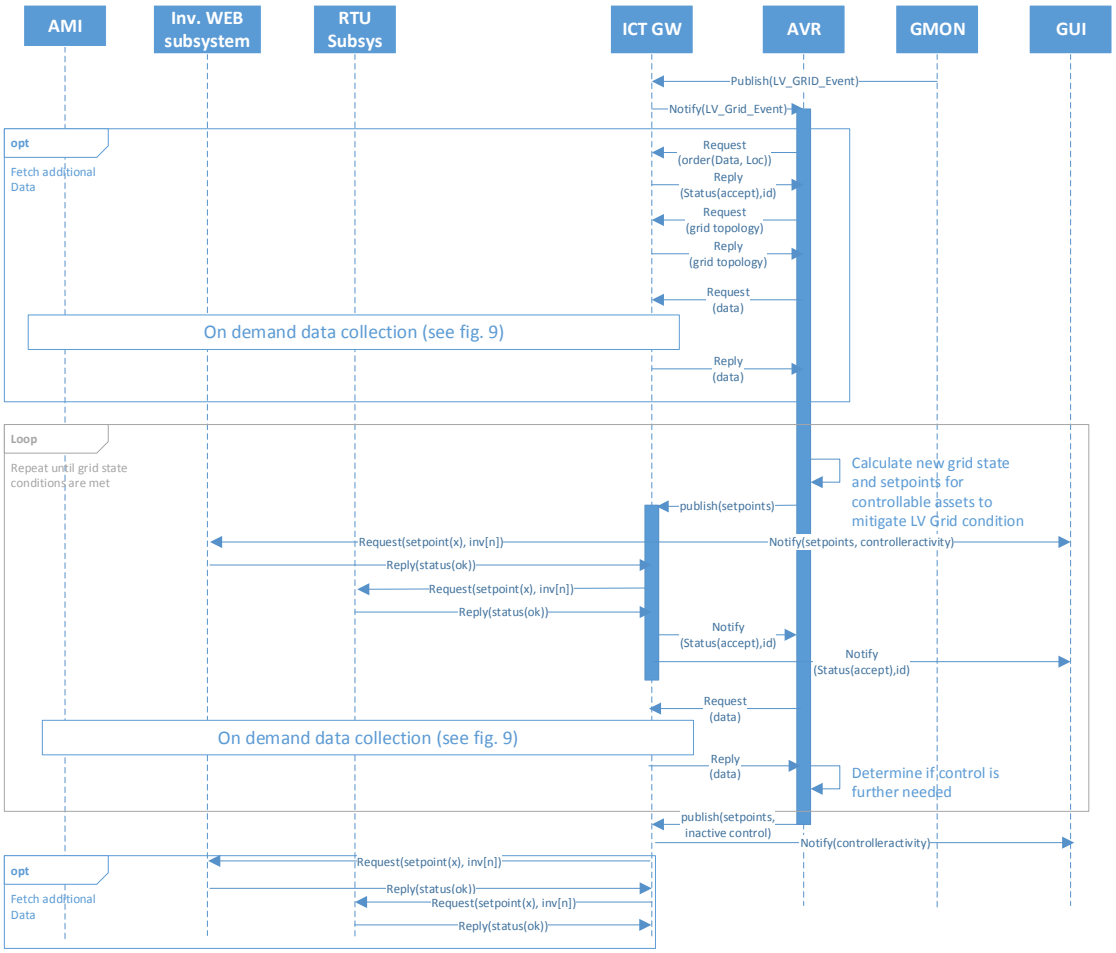

Figure 16 Automatic Voltage Regulation (AVR) Use-case, realized by set-point manipulation

The AVR application is triggered by events that are detected by the GMon application (e.g. by voltage boundary crossings). It then obtains the relevant grid topology and relevant grid values (measured values are prioritized to calculated values from the grid model) from the ICT Gateway and uses this data to calculate setpoints for the inverters and for generation curtailment or load activation (here assumed to be implemented via RTU subsystems). Controller actions are visualized via the GUI application as well. If the conditions that triggered the start of the AVR application are not removed immediately, then the control loop is executed periodically. Otherwise, a default setpoint configuration is written to the controllable assets and the AVR application returns to an inactive state. Details on conditions for entering and exiting alert status and how the AVR handles its internal grid status in this case will be specified in WP4.

7 Communication Network Architecture

7.1 High level description of domains

Communication systems are critical for Net2DG as they provide the service to connect entities distributed in the field together, enabling the various functionality to work properly. Since there are many elements in the communication infrastructure, this chapter aims to provide an overview of the systems and components that allow communication. Terms and concepts are introduced that are relevant and needed for later understanding of system design and deployment are introduced. Further, the overview of communication in this chapter creates the base for the work in Work Package 3 and in particular on the ICT analysis done in WP3.1.

Figure 17 shows a very high-level picture of the different domains that are relevant to the Net2DG project. Later this view is detailed to provide a more elaborate view of the complex network scenarios that arises in the project. The generic views will finally be mapped into specialized deployment scenarios for the two cases, Thy-Mors Energy and Stw. Landau, and will be used as input towards WP 3.

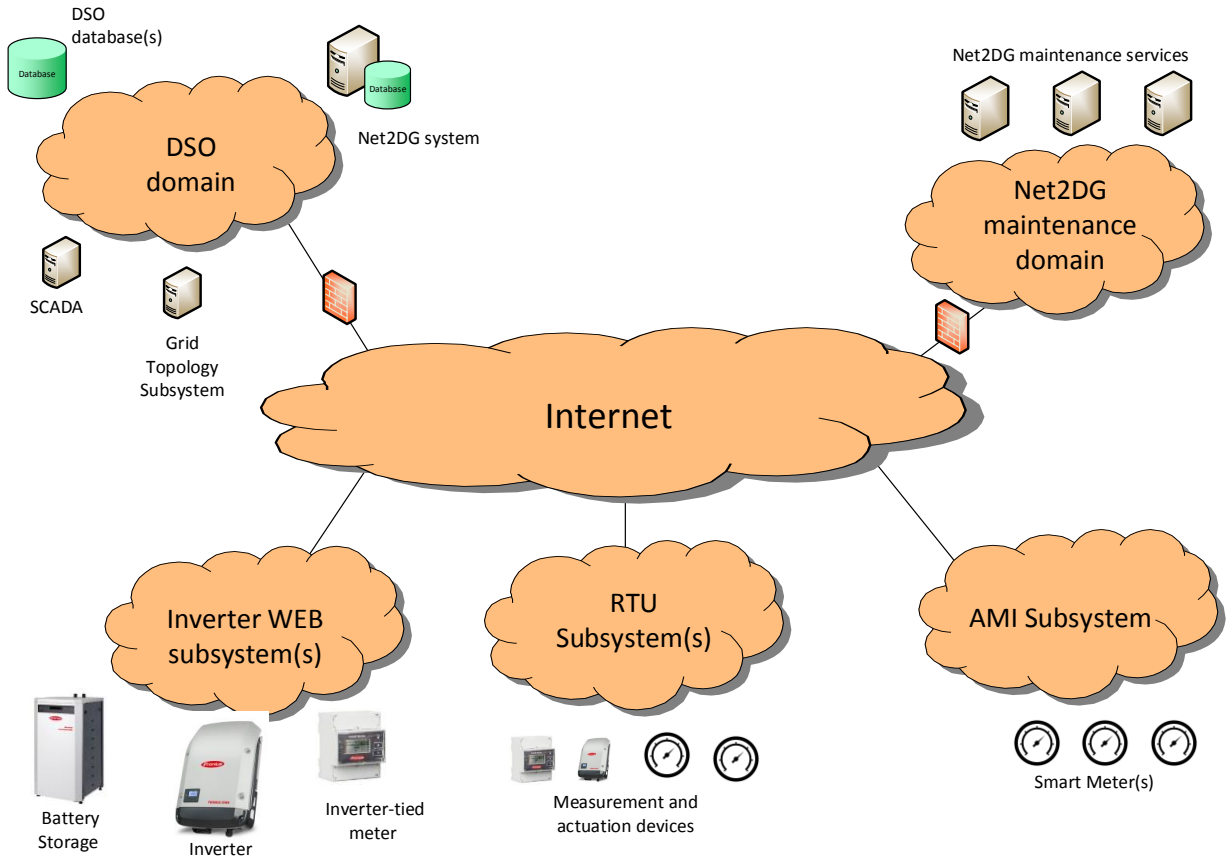

Figure 17: High level division of access domains and subsystems

In the centre of the picture, it is seen that the Internet will play a key role to interconnect the different domains: DSO/Enterprise domain, Net2DG support, inverters, measurement and AMI. In the following, a short overview of the main characteristics of these domains is provided.

The Internet: A huge collection of networks interconnected via routers and managed by a large set of protocols. Provides Layer 3 connectivity at a best effort level. No Quality of Service is guaranteed. Latency may range from 10 ms to hundreds of ms., with packet loss probabilities from 0% to 10%. Access networks to/from the internet will add to these characteristics, e.g. cellular networks or home networks will add specific characteristics to the end-to-end performance that will need to be considered.

DSO domain: Set of local networks physically related to the enterprise (DSO in this case) which may constitute several subnetworks and virtual networks (VLAN). Access may be strictly restricted in some subnetworks or completely separated from others. Typical networks are Ethernet, Fiber and WiFi.

Net2DG maintenance domain: A domain which hosts one or several functionalities to support maintenance of the Net2DG system, e.g. log repository for debugging purposes, application repository, code repository, data repository for analysis etc. The domain may hosted by one or more of the partners in the consortium and will be of a similar kind as a DSO enterprise network.

Inverter WEB subsystem: This is the domain in which PV inverters are being accessed and controlled at server level. Access to inverters is done internally with case specific networks and relevant application layer protocols. It is assumed that interfacing between inverters and the rest of the system is done via a central portal/web interface (except for RTU subsystems, see below). Internal network characteristics are case specific. Inverters are accessed via a Head End service.

RTU Subsystem(s): The domain in which external remote terminal units (RTU's) such as substation measurement devices, mobile devices, Inverter RTUs, etc. are located. Access networks to RTUs are typically cellular technology, but could also be others on a case-by-case basis. RTUs are accessed via a dedicated RTU Head End service.

AMI: Advanced Metering Infrastructure (AMI), this domain covers smart meters distributed in the low voltage grid. Typically, an internal network structure is found in this domain, which often is characterized by a low capacity network, such as radio mesh network or PLC. Thus, capabilities and constraints are case specific.

7.2 Network architecture and entities

Starting with the DSO domain (upper left part of Figure 17), the domain is split into several subnets: One subnet dedicated for hosting locally the hardware related to Net2DG: Net2DG application server(s), ICT Gateway, GUI application and Net2DG database(s). Notice that these may not necessarily be executed on the same physical machine, but can be executed on multiple servers that run on the same Layer 2 network, typically an Ethernet network. In general, the ICT Gateway will interact with any subsystem component, such as smart meters, inverters, SCADA etc., via **Head End** servers (HE) such that discovery, configuration, direct access to individual measurement or actuation devices are decoupled from the ICT Gateway, allowing the interaction to be focused on data access only.

The Telecontrol Network relates to the part of the DSO domain that contains the operational subsystems, i.e. the SCADA system and its operational databases. In Net2DG it is assumed that communication between different domains is done via a demilitarized zone (DMZ). Therefore, a SCADA Head End (SCADA HE) will be installed in the nearby DMZ network, which will grant access to/from data in the Telecontrol Network to the Net2DG subsystem. This means that the ICT Gateway is supposed to contact this HE in order to gain access to data from the SCADA or to send actuation data to the SCADA system.

As a second specific subnet, the DSO domain contains also an Office Network which may contain grid topology information and GIS data, that the ICT gateway will need. Analog to the Telecontrol Network, a Head End service located in a DMZ network is used to provide secure access to the information in the Office Network.

To relieve the ICT Gateway from micro management of individual RTUs, a dedicated RTU Head End server is running in a DMZ between the Net2DG network domain and the external connection of the DSO. This HE will provide access to the RTUs located in the field. In the same DMZ there will be support services as needed to support the Net2DG operation. This could be a private DNS for addressing and naming, NTP for time synchronization or FTP for log access. Some services may already exists at a given DSO, and therefore it is not strictly necessary to have these services running here.

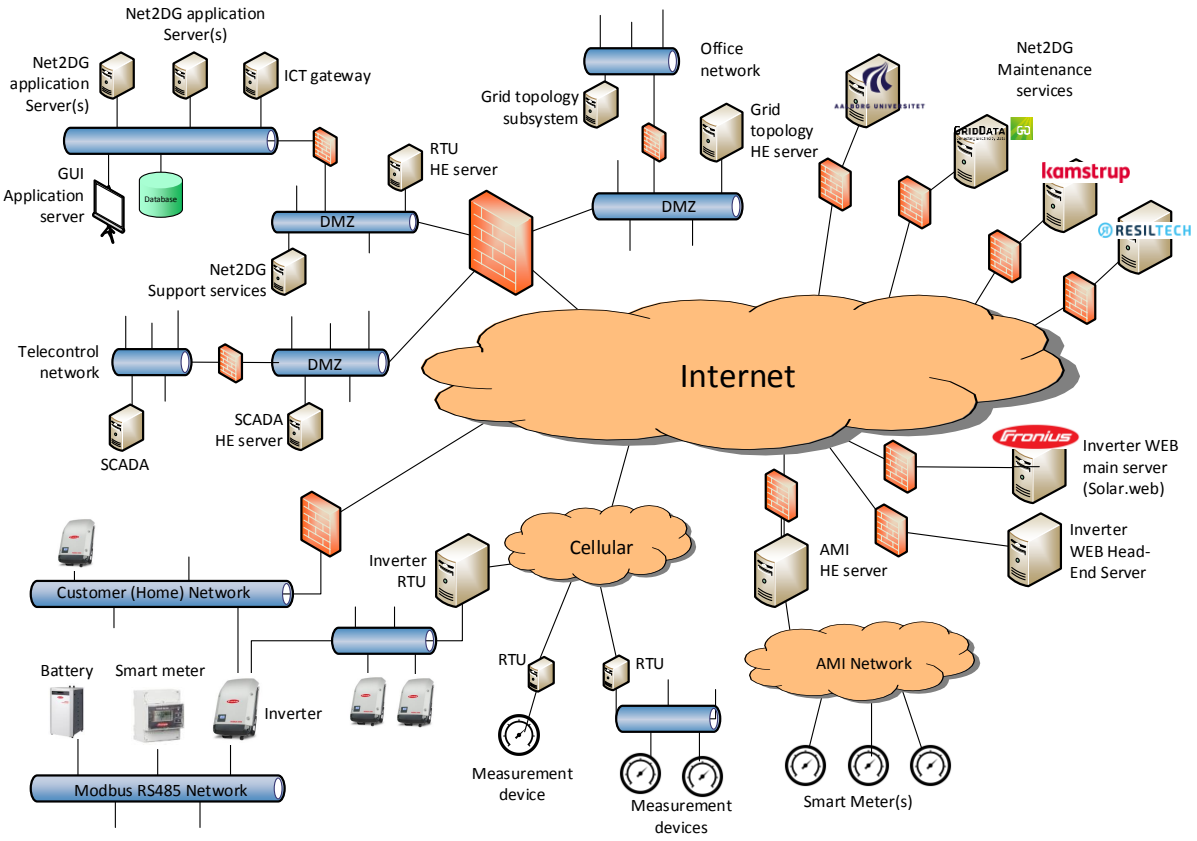

Figure 18 Generic Communication architecture in Net2DG

Figure 18 illustrates a more detailed and generalized view of the communication architecture in Net2DG. In the following, an explanation of this architecture and its components is provided, while later deployment architecture diagrams will reveal specializations and mild variants of this picture.

The Net2DG maintenance domain covers access to various sets of servers that assists and supports the Net2DG deployment, such as software repositories, log repository, etc., which may be hosted by different partners. The main interaction is here with the Net2DG servers located at the DSO.

PV Inverters can be accessed in two different ways:
1) via an interface to an Inverter WEB Headend. This interface simplifies the technical interaction between Net2DG and multiple inverters, which otherwise would not have been easy to discover, authenticate and access. The Inverter WEB Headend will have possibilities to perform active control of active and reactive power flow (Q and P) as well as maintaining a constant power factor. In this context, it will act as an aggregator between the ICT gateway and the PV inverters that are organized in groups.
2) via a field level inverter RTU, which is based on Modbus TCP. The inverter itself communicates with subordinate devices such as batteries or additional smart meters on a proprietary basis. The communication to these subordinate subsystems is not subject to technical developments within Net2DG.
Both ways of communication need an additional Inverter Head-End Server which provides additional data which cannot be provided by Solarweb or by the RTU (metadata: which data is available from which inverter type, which control possibilities, measuring accuracy, etc.)

More RTUs may be utilized for data access (e.g. from substation measurement devices or mobile PQ measurement devices) and for actuation (e.g. for street light activation and control). The RTUs access the local measurement or actuation device over a local network of device specific type.

Finally, the Advanced Metering Infrastructure (AMI) offers a web interface through the AMI Headend that allows interaction with the smart meters as well as fetching data collected automatically in the internal AMI network. The AMI network may constitute a hierarchy of networks of different types and with a large variety of performance.

All of these networks and interfaces will be carefully analyzed in WP 3, but the terminology and architecture will be critical for the later details of the use cases in later chapter of this deliverable.

7.3 Net2DG specific Entities and definitions

In the following section a short description of the various types of entities found in the scope of Net2DG are provided.

Net2DG Application Server: A machine (physical or virtual) that is focused on executing a particular net2dg application service.

GUI Application Server: A machine with a screen and keyboard attached, which focus is to enable the interaction with the human operator on site.

ICT Gateway: The Net2DG solution that allows easy interaction between Net2DG applications and (external) subsystems.

Head End: Not all subsystems can be expected to be accessible directly, e.g. SCADA or topology information, as they are subject to strict security policies at the DSO. To be able to get access to the relevant information, Head End servers are defined and setup to ensure that relevant information can be accessed via a DMZ. In Net2DG the following are considered:

- SCADA HE: allows access to SCADA
- Grid Topology HE: allows access to grid topology
- RTU HE: allows access to RTUs in the field
- AMI HE: allows access to smart meters
- Inverter WEB Headend: allows access to inverters

Net2DG Maintenance Server: Servers that offers specific services used by the Net2DG solution.

Inverter WEB Headend: Inverter WEB Headend: For all cloud, this is the single point of communication for the ICT gateway regarding DER inverters in Net2DG. It also provides additional data which cannot be provided by the Inverter WEB main server (e.g. metadata, data availability for each inverter type, control capabilities, measuring accuracy…).

Inverter WEB main server (i.e. Fronius Solar.web): Within the inverter WEB subsystem, this is the single point of communication for DER inverters. Access to inverters has a proprietary basis with case specific networks and relevant application layer protocols.

Inverter RTU: At field level, this gateway provides a local interface to DER inverters. The communication to the DER inverter is based on Modbus TCP according to the standard specifications of SunSpec Alliance.

8 Sub-system Interfaces

This section outlines the overall system requirements to the various sub-system interfaces and describes the related architectural design to fulfil these.

The terminology for requirements is the following: mandatory requirements use the key word 'must', while optional requirements use 'should'.

8.1 Interface Requirements: ICT Gateway to Data and Actuation Subsystems

The section describes the interfaces in between the ICT gateway and the data and actuation provider subsystem (southbound interfaces).

8.1.1 Interface to Distribution Grid Topology Subsystem

The following are the requirements for the interface between ICT Gateway and Grid Topology Subsystem (GTS), as provided by the Grid Topology Headend:

GTS-1 Registration (see Fig 4): GTS must register at the ICT Gateway and provide the following basic information

- Type of Topologies contained: LV, MV
- Number of Secondary Substations covered

GTS-2 Capabilities (see Fig 5): 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 arial lines attributes that are supported

GTS-3 Request-based LV topology: 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.

GTS-4 – MV topology: The Grid Topology Subsystem should also be able to provide basic MV grid topology information – to be specified later by WP2 what is needed.

GTS-5 – Publish of changes: The Grid Topology Subsystem should be able to publish changes of the LV grid topology to the ICT Gateway.

GTS-6 – Information Quality and Missing information: 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.

8.1.2 Common Requirements on Interface ICT Gateway to Subsystem Headend

The following requirements apply to the interface to any Measurement and Actuation Subsystem (MAS). For any external (non-DSO) MAS, it is assumed that the necessary legal and business agreements to access the data have been established – and that this procedure is not handled via the technical interfaces that are discussed in this section.

MAS-1 Registration: The ICT Gateway must support two different registration processes:

MAS-initiated (see Figure 4) and Gateway-initiated (see Figure 6).

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

MAS-2 Capabilities (see Fig 5): 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)

MAS-3 Correlation of IDs: 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.

MAS-4 Request Data Access (see Figure 10): 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.

MAS-5 proactive access (See Figure 9): The MAS should be able to actively publish new measurement data to the ICT gateway.

MAS-6 Event notification (see Figure 8): The MAS should be able to detect events of different type and to publish these events to the ICT Gateway.

MAS-7 Authentication: 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).

MAS-8 Security Levels of data: 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.

MAS-9: GDPR compliance: 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.

8.1.3 Additional Common Requirements to Actuation Subsystems

Actuation subsystems in Net2DG comprise the following catagories: Inverter-systems (PV and Battery), Load Activation (e.g. Streelights), Generation curtailment, and OLTC. Control of relays via Smart Meter Ports is out of scope for Net2DG.

In addition to the common requirements from the previous section, the interface to subsystems that support actuation are subject to the following requirements:

ACT-1 Setpoint modification: 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.

ACT-2 Setpoint reset to default: 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.

8.1.4 Additional Specific Requirements for Interface to AMI

In addition to the common requirements in Sect. 8.1.2, the following requirements apply to the AMI subsystem interface:

AMI-1: Interval-based data collection: The AMI system must support interval based data collection from all relevant meter points in the AMI system.

AMI-2 Data Format: The AMI headend should provide the data to the ICT Gateway using the CIM standard.

AMI-3 – Security: The AMI interface should support identity based authentication and data-in-transport protection based on industry standard encryption mechanism.

AMI-4: Configuration of Interval-based data collection: 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.

AMI-5 Configuration of loggers: The AMI system must support configuration of interval loggers (logger interval, data types) for grid surveillance.

AM-6 Prioritisation of different data types during data collection: 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

AM-7 Support for multiple reliability classes: 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).

AMI-8 Event based data collection: 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)

.

Ami-9 Support for multiple usage point types: 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:

- 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).

8.1.5 Additional Specific Requirements for Interface to Inverter Subsystem

In addition to the common requirements in Sections 8.1.2 and 8.1.3, the following specific requirements apply to the interface to inverter subsystems:

Inv-1: The Inverter Web or RTU Headend must provide upon request by the ICT Gateway for each installation

- The Metering Point ID belonging to this installation.
- The number and type (PV, peak Power) of generation units connected at the installation-
- The number and type of storage units connected at the installation (if any).
- The ID of the additional Smart Meter that is part of the installation (if any).
- 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.

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 so that it may stores it for future communication.

8.1.6 Additional Specific Requirements to RTU Subsystems

RTU subsystems in Net2DG are envisioned to be used for the following device types:

- Substation measurement devices (if not included in the AMI)
- Junction box measurement devices (mobile PQ or other)
- Inverter RTU access (data access and actuation)
- Street light activation, OLTC, generator curtailment, remote LV breaker operation, etc. (status data access and actuation)

The following requirement applies to RTU subsystems in addition to the ones listed in Sect. 8.1.2 (and in case of actuation subsystems, also Sect 8.1.3):

RTU-1 Ping: 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.

8.1.7 Interface Requirements for Data Access and Actuation via SCADA System

The SCADA system is not expected to be used in the first Net2DG development iteration. If an interface to the SCADA system as a data source turns out to be necessary for any of the two field trials, the common requirements in the earlier section cover this interface as data source already.

Actuation via SCADA related actuation units will be mainly performed in the lab trial, where a simple SCADA mock-up will be used. In the field-trials, all actuation will be done via RTU subsystems, see previous section.

If a more elaborate interface to the SCADA system will be needed in Net2DG, then the update of D1.2 in Month 18 will describe further details.

8.2 Inverter Subsystem

8.2.1 Solarweb API (Inverter Web Headend)

At server level, the ICT gateway can communicate to the Inverter Web Headend of Fronius by using the Solarweb API. This interface allows reading and, in a beta version, writing (remote control) of grid-relevant parameters. The reading interface divides roughly into real-time and archive requests – real-time requests will get data directly from the field devices and can therefore only be used when the field devices are not in standby or down. Archive requests will use the data stored at Solarweb server level. Remote control (beta version) allows the control of a target active power value at the metering point (PCC), and, if there is a battery, the control of an operational battery power envelope (Pbatt,max and Pbatt,min).

8.2.2 IEEE 2030.5 Standard (Inverter Web Headend)

A second path to communicate with Fronius Inverters at server level is the IEEE 2030.5 standard.
The implementation of this communication protocol is mandatory to fulfil the Californian Rule 21 Phase 2 standard and will be ready to use until February 2019. The protocol offers a wide range of possibilities regarding monitoring and control of PV systems, which can be useful in Net2DG.

The main point of Rule 21 is that the utility (DER Server, Inverter WEB Headend in the Net2DG system) must be able to send commands to the aggregator (DER Client = Fronius Solarweb). The aggregator will then send the commands to certain groups of inverters; each inverter must have the capability to be part of 15 independent groups which are defined by the utility. Figure 19 illustrates the path of communication; security standard will be TLS 1.2.

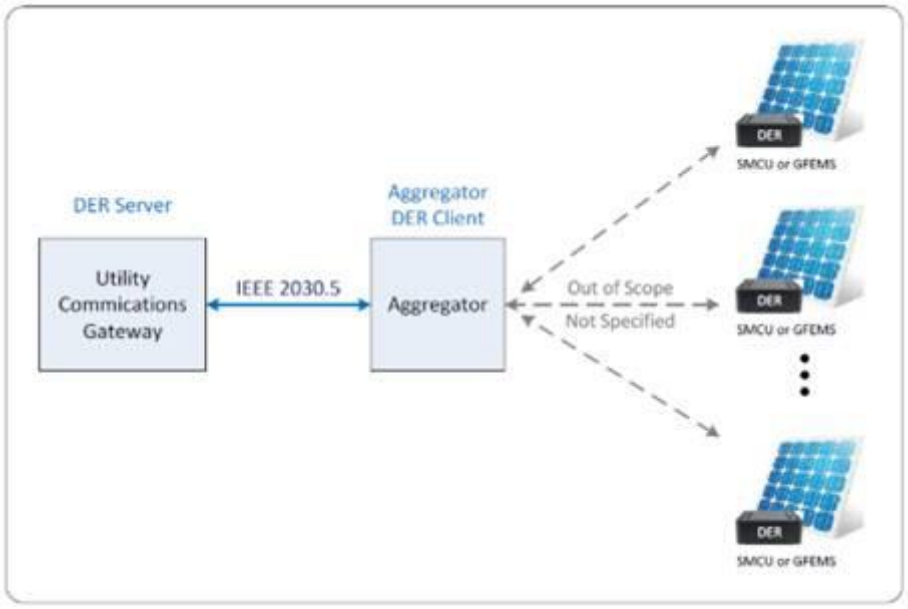

Figure 19 Communication path with inverter groups of Inverter WEB Headend via Fronius Solarweb

The implementation is based on the Common Smart Inverter Profile (CSIP) IEEE 2030.5 Implementation Guide for Smart Inverters from March 2018 (Version 2.1). Thereby default settings for control functions are set by the DER Server, which can later be superseded by scheduled control events. Furthermore, the aggregator will have the capability to report monitoring data, the status of the DER system as well as alarm notifications when anomalies in the AC grid are detected.

8.2.3 Inverter RTU Sub-system

This section shortly summarizes the existing interface that the existing Inverter RTUs provide. This interface will be used by the Inverter RTU Headend, which will be designed in WP3.

The inverter RTU communicates with Fronius inverters via the Fronius local interface. The communication is based on Modbus TCP according to the standard specifications of SunSpec Alliance. The interface allows reading and writing (control) of grid-relevant parameters. The interface divides roughly into real-time and archive requests – real-time requests will obtain the data directly from the field devices and can therefore only be used when the field devices are not in standby mode. Archive requests will use the data stored locally.

8.2.4 Inverter Subsystem internal message flows

The following figures show the behaviour of the inverter subsystem for the different general procedures that have been defined in Sect. 6.3.2. These flows visualize how the different components

within the inverter subsystem will interact with each other and will be the basis for the design and implementation of as yet non existing components such as the Inverter WEB Headend and the inverter RTU Headend within WP3.

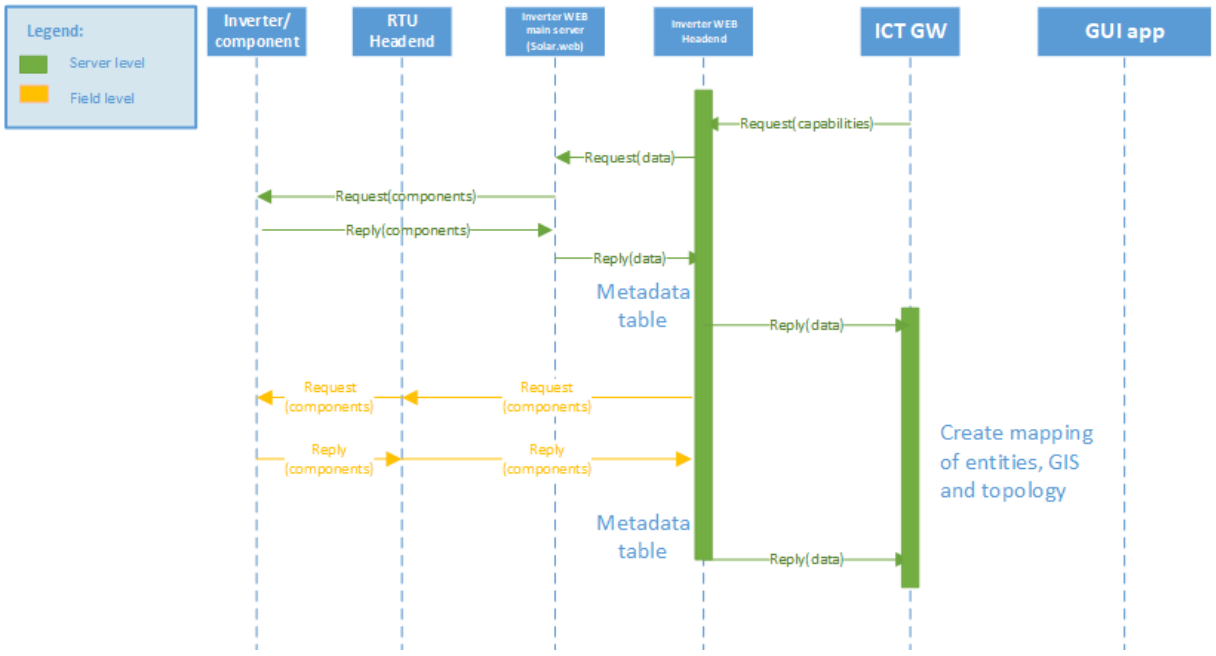

Figure 20 Inverter Subsystem capability registration

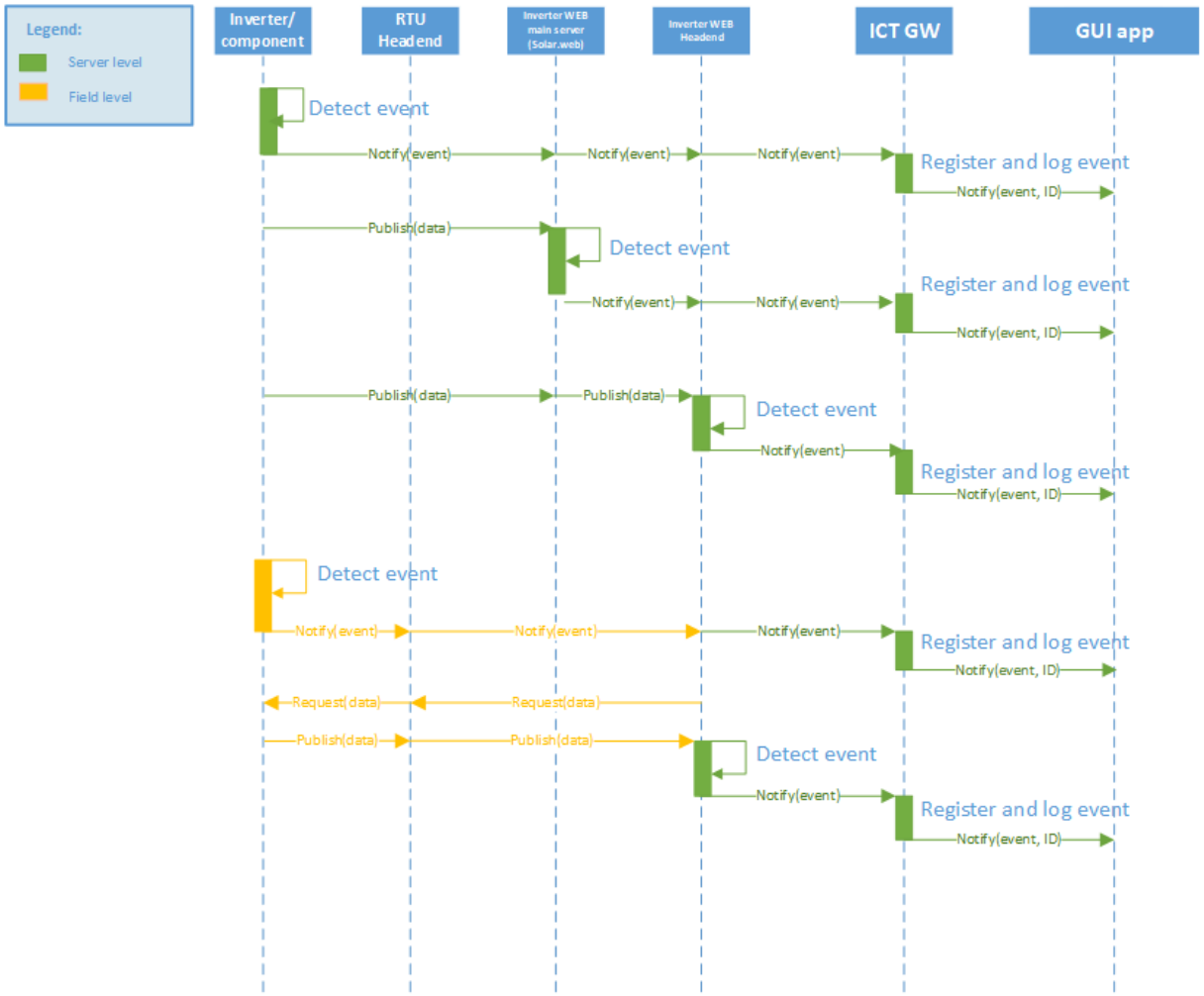

Figure 21 Inverter Subsystem Event collection (Push/publish-subscribe)

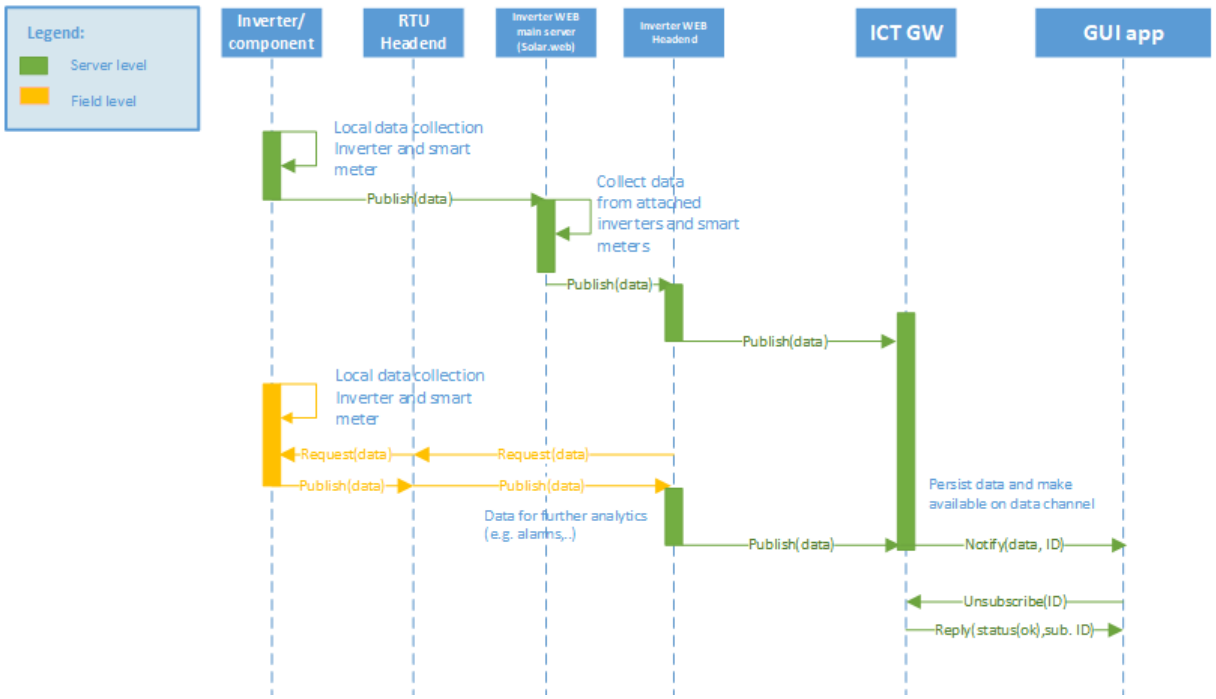

Figure 22 Inverter Subsystem Automatic Data collection

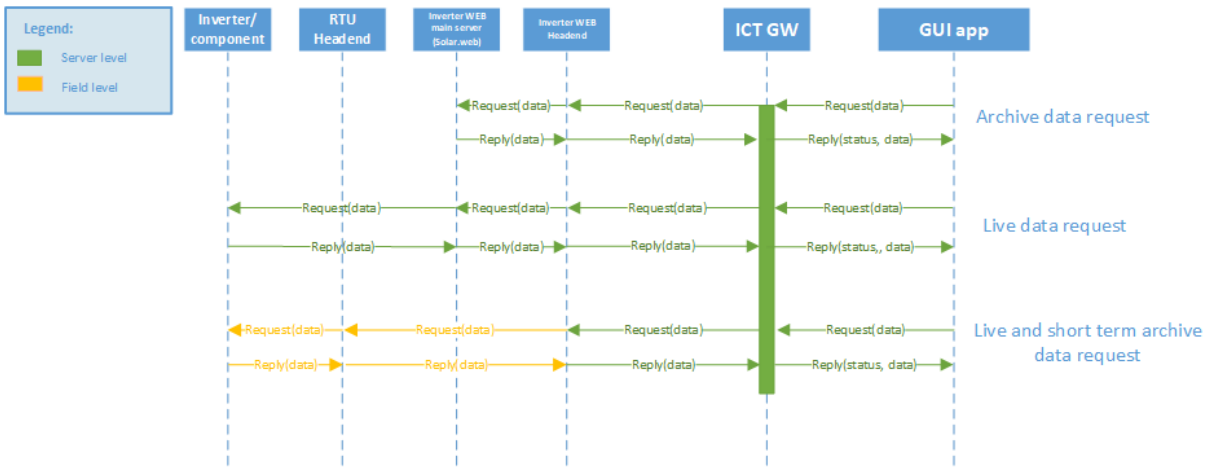

Figure 23: Inverter On-demand data collection

8.3 AMI Sub-System API

The AMI system from Kamstrup (named the OMNIA Suite) provides an industry standard CIM[4] based integration API. This API allows 3rd party systems (MDM, SCADA, CIS and in Net2DG case, the ICT Gateway) to access the AMI system features. This is shown below (with an MDM integration example).

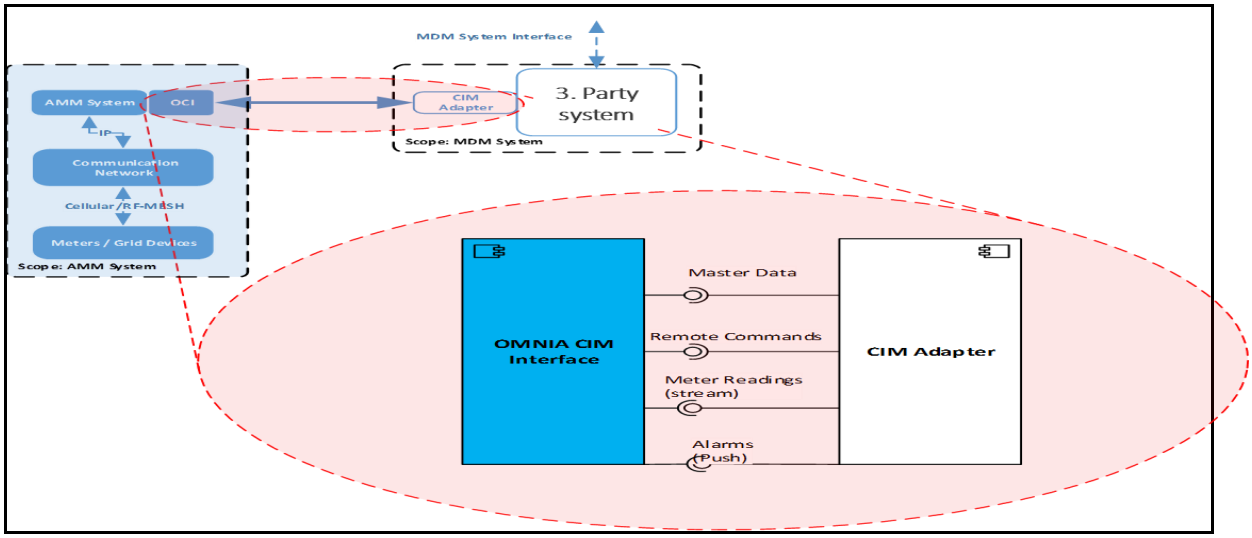

Figure 24 CIM based AMI integration

CIM defines the messaging between various systems in the DSO landscape and has been adapted by Kamstrup to provide a harmonised integration API, which can greatly reduce the effort of integrating AMI with other subsystems at the DSO. The API is implemented as a standard SOAP based interface

The API is rather large as it covers the full functionality of the AMI system. To facilitate different degrees of integration it is divided into 5 parts:

Volume interface	Supports push of automatically collected data from the AMI system (billing data, event loggers, analysis loggers etc.)
Synchronisation interface	The synchronisation interface is used for receiving information from higher-level systems to maintain meters, concentrators, usage points, concentrator points and the connections between them in the AMI system.
Command interface	If the higher-level system wants to perform an action in the AMI system (on-demand readings, breaker etc.), the command interface is used.
Real-time interface	The interface applies to the transmission of alarm messages from meters and other devices in the AMI to the adjacent system.
Information interface	This interface is used to perform changes to the configurations of the meters.

[4] CIM = Common Information Model, defined by IEC61970 and extended by the IEC61968 to cover electrical distribution systems

8.4 Grid Topology Subsystem

This section introduces entities captured in Grid Topology Subsystem utilized in StwLan that reflect and describe the LV grid topology. Moreover, it will be explained how these entities are related to each other and what are they functions in the representative grid. The general data types are very similar at TME, so the principles carryover also to the second field trial. The detailed analysis of both Grid Topology Subsystems will be described in D3.1.

The Grid Topology Subsystem at StwLan uses file exports of data from the GIS system together with additional existing information files from StwLan; these files are processed by the Grid Topology Headend, which then provides the interface to the ICT Gateway. The Grid Topology Headend is a component that will be designed and implemented for the two field trials in Net2DG.

The following table lists the entities in the underlying GIS system.

Table 3 – GIS entities in Grid Topology Subsystem

Entity
Cable
Substation
Junction box
Sleeve
Street light system
Household
Photovoltaic system

In the export from the GIS system, each type of entity is described in an own file, i.e., there are 7 different types of files. Listed entities can be divided into three categories: (1) cables, (2) grid elements and (3) prosumers. Grid elements are substations, junction boxes and sleeves, while households, street light and photovoltaic systems are prosumers.

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

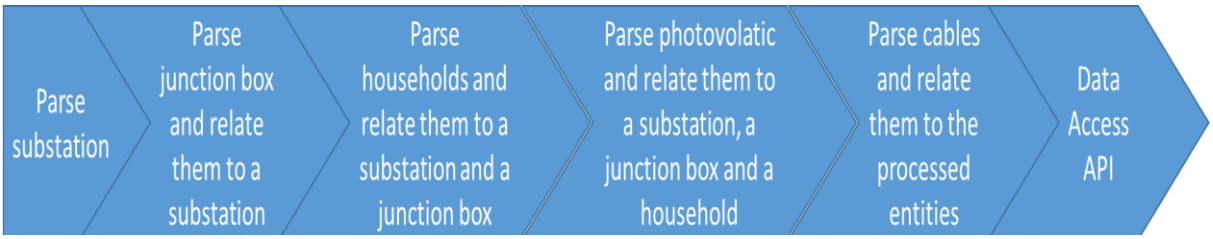

Figure 25 – Grid Topology Headend main functions

The workflow starts with extracting and parsing substation data, which can later be referenced by other entities. Then, junction boxes are parsed and related to the already processed substations. After that, households are parsed and related to the already processed substation and a junction box. The same is performed on photovoltaic data. Finally, each cable entry is processed in such a way that it can be uniquely identified which two entities among, the already processed ones, i.e., junction boxes and households, it connects.

Extracted entities and cables are provided on the interface towards the ICT Gateway. Data can either be pushed on each detected change, i.e., a topology update, in the subsystem or ICT Gateway can request the entities on-demand. Moreover, the subsystem can either provide the whole topology, a subset of nodes and related cables, or just give a detailed information about a particular node.

8.5 Net2DG Interface to Domain Applications

8.5.1 Draft API design for the Interface between Applications and the ICT Gateway

As the communication paradigm for an interaction between different applications and ICT Gateway is uniform across the all applications, i.e., publish/subscribe and request/response, one communication protocol can be utilized. Due to the support for full-duplex communication channels over a single TCP connection, WebSocket can be utilized as a communication paradigm. There two main entities in Websocket communication protocol:

4. A WebSocket server that listens on a predefined port (endpoint) and
5. A WebSocket client that connects to the WebSocket server.

In the scope of Net2DG, ICT Gateway takes the role of WebSocket server, while each application acts as a WebSocket client.

Due to the standing full-duplex TCP connection between a WebSocket client and a server, the WebSocket protocol can be used to realize both the, publish/subscribe and the request/response communication patterns. However, to provide a meaningful communication between the two sides, it is necessary to develop a communication protocol on top of the websockets. In particular, it is required to define a set of messages that will be exchanged between WebSocket client and server. A message can be a simple JSON formatted string with a defined set of key/value pairs.

WebSocket protocol can address the interactions defined in Section 6.3.2 in the following way:

- Application registration
  - Application acting as a WebSocket client establishes a connection with ICT Gateway acting as a WebSocket server
  - ICT Gateway sends back registration request
  - Application responds with registration message containing required data
  - Deregistration is triggered upon closing the connection
- Application requests topology
  - Application sends topology request message over the connection established during registration phase
  - ICT Gateway responds with a message containing topology
- Application subscribes to data (push-based data collection)
  - Application sends a request subscription message with required data, e.g., data source type, interval, etc.
  - ICT Gateway continuously pushes data to the subscribed application over the connection established during registration phase
  - Application can also send remove subscription message with a reference to the previously created subscription
- On-demand data collection
  - Application sends request data message with the defined content, e.g., data source type, interval, etc.
  - ICT Gateway responds with acknowledgment message
  - ICT Gateway pushes data to the application as soon as it arrives from a subsystem

The detailed communication protocol, i.e., the precise definition of the messages introduced aboves, will be designed later in WP 3.

8.5.2 Draft Data Model Provided by the ICT Gateway to the applications

Grid Topology

A data model reflecting a grid topology will be constituted of multiple tables where each table corresponds to an entity in the grid topology. An entity can be a substation, a junction box, a cable, a household, a photovoltaic, etc. An entry in a table is one node in the grid topology and it has a GridNode ID (uniquely marking the grid location), which may have multiple other IDs associated, e.g., measurement device ID, SmartMeter ID, Household ID, Inverter ID, Generator ID, etc.

In addition to GridNode ID, each node has one of the following types:

- Substation (initially assuming single-transformer substation only)

- Junction box
- Prosumer Metering Point
- Building Terminal Box (ex. German 'Hausanschlusskasten')

Other grid nodes, likes sleeves, fuses, or breakers, may be included based on the detailed analysis in WP3. Those could in principle also be represented by cable attributes.

All grid nodes can have sub-nodes as well. Moreover, all grid nodes can have one or more measurement devices as sub-nodes, while prosumer node can have additional sub-nodes:

- Generator nodes (PV, wind, CHP etc.)
- Consumer nodes (Domestic, commercial, industry, EV etc.
- Actuation nodes

Cable entities are different from grid nodes. Cables are described using the following properties: cable ID, start node id (GridNode ID), end node id (GridNode ID), number of phases, length, resistance, reactance (inductance and susceptance may be considered as part of WP2), cable type, etc. It should be pointed out that the sub-node to grid node association is a virtual one (i.e. sub-nodes are not represented in the list of cables).

When an application requests a topology from ICT Gateway, it can specify whether is it interested in 1) obtaining the whole topology, 2) only in one grid node (and implicitly all nodes below that one), or 3) in all nodes within a geographic rectangular region). In any case, a response consists of the following:

- List of tuples <GridNode ID, node type, [optional parameters of node, …]>
- List of Grid Cables/Lines: <cable id, start node id, end node id, length, resistance, reactance (inductance and susceptance may be considered as part of WP2), [optional params: cable type, …]

Finally, an application can also request for details for each grid node. In that case, as an answer it gets the following information in response:

- Measurement device ids, types, capabilities, …
- Generators ids, types, capabilities
- Actuation devices, types, capabilities

Measurement

The main focus of a data model that reflects measurements is to associate measurement with their data source. Consequently, measurements arriving from a given data source will be captured within own table/entity. All entities will have an associated GridNode ID that corresponds to grid topology node and timestamp. Other properties will depend on the type of data source.

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

- List of MeasurementDevice IDs
- Time-interval of interest

For example, a request could be for all available measurements from the measurement devices that have been taken within a specific time-interval. Reply/Notify contains in both cases: List of <Measurement device ID, timestamp of taking measurement, measurand1, unit1, accuracy1, [other metadata], [measurand2, …]]>.

Events

Events introduced in Fig will be captured in the same table in a data model. Each event contains the following elements:

- Event creator
  - ID of Measurement device
  - ID of ICT Gateway (if the Gateway or any subsystem created the event based on correlating multiple measurements)
  - ID of application (like outage detection and GUI)
- Type of event - examples
  - Parameter exceeds thresholds (e.g. voltage measurement exceeds threshold)
  - New measurement data available
  - Non-reachability of measurement device
  - Shut down of component
  - …
- Further event parameters will be identified later in detail based on the event types

Subscriptions

Since the publish/subscribe communication pattern is used both for interaction between ICT Gateway and applications as well as for interaction between ICT Gateway and subsystems, ICT Gateway will have to manage a large number of subscriptions. Therefore, the data model should have an additional table/entity for managing those subscriptions.

Additional Meta-data will be analysed for inclusion in WP3, e.g. Quality data attributes (trust) or candidates from the following list:

- Timestamp accuracies
- Timestamp origins
- Measurement accuracy

9 Preliminary Security Analysis and Requirements

The Net2DG solution will introduce new technological components/subsystems, which will interface with both new and already existing components/subsystems within in the context of the DSO's distribution grid. Even though such new components and interfaces are meant to improve quality, efficiency and maintenance of the grid, they may also add new vulnerabilities to the system where they are deployed. Therefore, additional requirements are necessary in order to address such vulnerabilities and maintain Confidentiality, Integrity and Availability (CIA) concepts.

This section is not intended to provide a real security architecture at this stage; rather it is meant to provide a preliminary threat analysis, derive related security requirements and clearly identify the boundaries of the security architecture.
It is important to highlight that no specific requirements will be derived for all subsystems depicted in Figure 18, but only to the subsystems and communication in scope to Net2DG, therefore this section will focus on the ICT gateway and its communication to Head-End servers.

One main requirement is to avoid introducing vulnerabilities to existing DSO IT subsystems that are interfaced by Net2DG, in particular the telecontrol network and the DSO's office network. In order to account for this requirement, the architecture in Section 7 already introduces the interaction with these networks via Demilitarized Zones (DMZs), which contain the Head-end Servers that provide the point of attachment to the Net2DG system, thus providing secure access.

9.1 Preliminary Threat analysis and Derivation of Security Related Functions

The preliminary threat analysis is carried out based on the high-level architecture shown in Figure 18, aiming at identifying potential scenarios where security attributes (confidentiality, integrity and availability) can be violated.
The following sections discuss the identified scenarios and associated security functions to be implemented as part of the Net2DG system. The analysis assumes any generic subsystem that is interacting with the ICT Gateway; an analysis on specifics regarding different subsystem types is done later in WP3.

9.1.1 Eavesdropping attacks on Head End-ICT Gateway communication

This case considers unauthorized interception of communication between ICT Gateway and any Head End Server without the consent of the communicating parties.
Eavesdropping attacks have impact on confidentiality; these attacks can have twofold impact: violation of customer privacy and collection of relevant information regarding the distribution grid, thus making the attacker able to plan/start a more sophisticated attack to the grid.

This kind of threat is considered difficult to be detected since there is no modification of data. Therefore, the focus should be more in preventing the attack. In addition, security countermeasure can be implemented for detection purposes.

The attack steps for this threat are as follows:

1. During normal operation (that is a precondition for the attack), data is sent and received through the communication network connecting ICT Gateway and the specific Head End Server.
2. The attacker gets access to the communication network connecting ICT Gateway and the specific Head End.
3. The attacker starts eavesdropping on the communication in an attempt to read information exchanges (e.g., in order to receive covert channel communications or perform traffic analysis).

Desired Net2DG functionality (note: the following items are part of security measures, therefore the enumeration continues from the list above):

4. ICT Gateway should be able to detect divergences from normal and expected establishment of secure connection to subsystems thus implementing a system for Network Access Control to check the authenticity of any subsystem before establishing any connection
   Data and events are logged in parallel to determine what has happened at what time, a special granularity level of logging is set during this period.

Moreover, the following preventive countermeasures should be provided:

- The ICT Gateway and firewalls are configured with an access control policies used to provide authorization or to specify privilege for different types of users (including local DSO staff, remote maintainers), subsystems and devices.
- Secure communication between ICT Gateway and HE is established using encryption based on a session-specific key.

9.1.2 Integrity attacks on Head End-ICT Gateway communication

This scenario describes the case where an attacker carries out a Man-in-the-Middle attack, i.e. the attacker makes independent connections with the nodes involved in a communication and relays messages between these two parties, making them believe that they are talking directly to each other, while the communication is in fact controlled by the attacker. This kind of attack aims at compromising the integrity of data exchanged between any Head End and ICT Gateway, in order to weaken grid situation awareness of the DSO or even cause harmful control actions (e.g., load shedding in response to a fake frequency deviation).

1. During normal operation: each subsystem connected to the Net2DG ICT Gateway is working according to specifications.

2. The attacker gets access to the communication network connecting ICT Gateway and the specific Head End.
3. The attacker intercept messages on the communication network.
4. The attacker sends corrupted data to the destination.

Desired Net2DG functionality (reactive functionality, hence continuing the above steps):

5. ICT Gateway should monitor inputs from subsystems and compare received input with other data from other subsystems and with estimated values from the grid model, e.g. data from AMI should roughly match data from Inverter Subsystem at the same or close grid locations.
6. As soon as an anomaly is determined with some high likelihood:
    a. The operator is warned visually via the GUI
    b. Values from the suspicious subsystem/measurement point are device is flagged as untrusted or even discarded
    c. If subsequent data streams continue to be anomalous, the subsystem may be disconnected completely until manually repaired and new registration procedure has been completed successfully. There should be a maximum number of possible retries for the same subsystem.
7. Data and events are logged in parallel to determine what has happened at what time, a special granularity level of logging is set during this period.

Moreover, the following preventive countermeasures should be provided:

- The ICT Gateway and firewalls are configured with an access control policies used to provide authorization or to specify privilege for different types of users (including local DSO staff, remote maintainers), subsystems and devices.
- Secure communication between ICT Gateway and HE is established using encryption based on a session-specific key.

9.1.3 DoS attacks on the Head End-ICT Gateway communication

This case focuses on someone trying to deny access to/from the ICT Gateway:

1. During normal operation: data is sent to and received by configured network interfaces of the ICT Gateway, and data is going out via these interfaces.
2. An attacker can attempt to perform two kinds of DoS attacks:
    a. The attacker launches an attack on relevant ports (or all ports) by flooding the network interface at the ICT Gateway with data packets
    b. The attacker launches the attack at Head End level in order to exhaust resources such as CPU or I/O bandwidth, thus overwhelming the Head End by flooding computationally intensive requests.

Desired Net2DG functionality (reactive functionality, hence continuing the above steps):

3. ICT Gateway notices that actual data is not being properly received, long delays and high packet losses are observed.
4. ICT Gateway notifies applications about the DoS attack in progress and enables a special DoS state:
    a. Each application may reconfigure itself to operate with reduced data availability or reduced data timeliness (to be defined in WP3).
    b. ICT Gateway serves applications according to a priority list/level of criticality.
    c. The ICT Gateway visualizes on its dashboard (see Section 5.1) that connectivity is poor or lost – and visualizes the suspicion that a DoS attack is ongoing.
5. ICT Gateway operates and serves applications in a special DoS- mode:
    a. Limited access to data sources – optimizing reuse of data being read.
    b. Enabling more use of the grid model, e.g. reserving more processing capabilities for grid calculations and reducing effort in reading measurement data from affected subsystems.
    c. Prioritizing actuation signals in communication to subsystems.
6. Data and events are logged in parallel to determine what has happened at what time; a special granularity level of logging is set during this period.
7. DoS attacks ends: ICT gateway determines that the connectivity is good again and returns to normal operation mode after reporting to the applications that normal conditions are back
    a. Computational resources and priorities are rolled back to normal.

9.1.4 Intrusion Attacks/malicious code installation on Head End Servers

This scenario describes the case where an attacker performs unauthorized installation of malicious code at Head End Servers.

There can be several motivation and consequences due to installing malicious code:

- The attacker installs malicious code at Head End Servers in order to gain access to other entities in the subsystem or to gain access to the ICT Gateway.
- The attacker installs malicious code at Head End servers in order to get (potentially confidential) information.
- The attacker installs malicious code at Head End Servers in order to modify/corrupt information.
- The attacker installs worms that can be distributed via the communication network copying themselves to other subsystems and affecting the operation of other subsystems connected to the network.

1. Normal operation.
2. An attacker get access to the Head End Servers.
3. The attacker installs malicious code with one of the above mentioned motivations.

As the Head-End Server is part of the subsystem, it is actually within the scope of Net2DG to add protection to the Head-End Server. However, there is still desired Net2DG functionality in order to

mitigate the impact of such an attack. The continuation of the above sequence describes the reactive measures:

4. The ICT Gateway should monitor events to detect unauthorized activities, changes to information, anomalous patterns of data exchanged with each subsystem.
5. As soon as an anomaly in the communication to the Head-end is detected, the Net2DG system should disconnect the subsystem and check if a new registration of the subsystem removes the problem. If not, then the subsystem should stay disconnected and applications are notified about the disconnection for security reasons.
6. Data and events are logged in parallel to determine what has happened at what time; a special granularity level of logging is set during this period.

9.1.5 Intrusion Attacks/malicious code installation on ICT Gateway

This scenario describes the case where an attacker performs unauthorized installation of malicious code at the ICT Gateway.

There can be several motivations for and consequences of installing malicious code:

- The attacker installs malicious code at the Net2DG ICT GW in order to modify the system, other applications, or data leading to disclosure of (potentially) confidential information, modification of information, Denial of Service.
- The attacker installs malicious code at the ICT GW in order to attack external subsystems.
- The attacker installs worms that can be distributed via the communication network, copying themselves to other subsystems and affecting the operation of other subsystems connected to the network.

1. Normal operation.
2. An attacker gets access to the ICT Gateway.
3. The attacker installs malicious code with one of the above-mentioned motivations.

Desired Net2DG functionalities as reactive counter measure:

4. An intrusion prevention system on the network should be deployed to spot and avert attacks by unauthorized parties.
5. Net2DG should implement malicious code detection and removal mechanisms.
6. Net2DG should monitor events to detect unauthorized activities or changes to software and information.
7. As soon as an anomaly is detected, the ICT GW should go in an intrusion-safe state (to be defined in WP3), in which it generates and disseminates internal security alerts to all applications and possibly connected subsystems.
8. Data and events are logged in parallel to determine what has happened at what time; a special granularity level of logging is set during this period.

Moreover, the ICT Gateway and firewalls should be configured with an access control policies used to provide authorization or to specify privilege for different types of users (e.g., remote maintainers), subsystems and devices.

9.1.6 Time synchronization attack

ICT Gateway and the Net2DG applications perform analysis of measurement data from the grid and, according to the analysis results; the relevant applications may provide control decisions to maintain normal operation. Potential errors in measurements intentionally caused by malicious attackers will have the consequence of causing the applications to make wrong decisions, which in the worst case could lead to a blackout. The attack on subsystem data integrity was already covered in Section 9.1.2; in contrast to that section, the attack considered here is one where the timestamps of the measurements are altered, which can have the same detrimental effect as a modification of the measurement data itself:

1. During normal operation, the measuring devices deployed in the grid are time synchronized through an NTP server to allow the ICT Gateway to align all collected measurements in the time domain.
2. The attacker aims at executing malicious code on the NTP server due to software vulnerabilities, thus leading the measuring devices to be set to intentionally deviating values. Variants of this attack may involve attacking the communication of the NTP server or by Denial of Service attacks on the NTP server, making the time synchronization unavailable.
3. One or more devices send measurements with an incorrect timestamp due to the maliciously modified or lacking NTP server signal.

Desired Net2DG functionality to react to this attack:

4. ICT Gateway receives data from a spoofed device and detects the wrong timestamp.
5. ICT Gateway does not consider the timestamp of the data from the spoofed device in the measurement data analysis. Alternatively, it may obtain an own timestamp (and a correspondingly enlarged timestamp accuracy meta-data) and replace the suspected wrong timestamp.
6. ICT Gateway alerts related applications about potential lack of data from the specific device(s).
7. The applications react appropriately to the missing information situation.
8. Data and events are logged in parallel to determine what has happened at what time; a special granularity level of logging is set during this period.

In case the attack ceases and the NTP server works correctly:

9. Measurement devices synchronize with the correct clock.
10. ICT gateway detects the correct timestamp and informs dependent applications about device reset and the reliability of its measurements.

9.2 Security Requirements

This section outlines the overall security requirements to the various sub-system interfaces:

Sec-01: Any subsystem Head-End Server must mutually authenticate with the ICT Gateway before being able to exchange data with ICT Gateway.

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.

Sec-03: ICT Gateway should protect internal communication using authentication and encryption.

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.

Sec-05: ICT Gateway must record any subsystem connected ad user logged to the system.

Sec-06: ICT Gateway should terminate a remote session at the end of the session or after a pre-defined time of inactivity.

Sec-07: ICT Gateway should deploy Intrusion prevention system on the network to prevent unauthorised intrusion on the network.

Sec-08: ICT Gateway should implement malicious code protection mechanisms to avoid installing of malicious code.

Sec-09: ICT Gateway should implement anomaly detection on measurement data to detect attacks on data integrity.

Sec-10: ICT Gateway should implement anomaly detection on timestamps to detect attacks on time synchronization.

10 Deployment Architecture

This section describes the specific architecture variants that will be used for the two field-trials.

10.1 Deployment at StwLan

The field trial at StwLan will initially use a single LV grid (one secondary substation, presumably Weiherweg 20) and will in a second step be extended to 2-3 neighboring secondary substations. Specifics to the StwLan deployment are:

1. The SCADA system will not be used as any actuation will be done by RTU subsystems.
2. The substation measurements are not included in the AMI system but will be done by a RTU-based solution using Janitza measurement devices. The RTUs will use Raspberry Pis as platform in the prototype and use cellular communication to communicate with the Head-end Server at StwLan.
3. Janitza devices will also be used for measurements on junction boxes; all Janitza measurement devices will be managed by the same Head-end Server, irrespective whether they measure at the substation or at the junction box.
4. Mobile PQ measurement units will not be used in the first deployment (instead Janitza measurement devices will be deployed where needed).
5. A single server installation will be initially done for the Net2DG domain, in which applications, ICT Gateway and GUI run on separate VMs.
6. The DMZ at the DSO domain may be merged into a single DMZ – this is still under investigation therefore not shown like that in the figure below yet.
7. Streetlights are planned to be used as actuation device – those will be connected by RTUs realized also as Raspberry Pis.
8. The German Smart Meter architecture[5] allows for multiple Gateway administrators, hence several AMI Head-ends have to be considered. In the prototype phase, only a single GW administrator will be considered.

The figure below shows the modified deployment scenario for Stadtwerke Landau.

[5] It is not clear at this stage, whether Inverter data also has to be accessed via the Smart Meter Gateway. The figure below shows this scenario, but it is still under investigation.

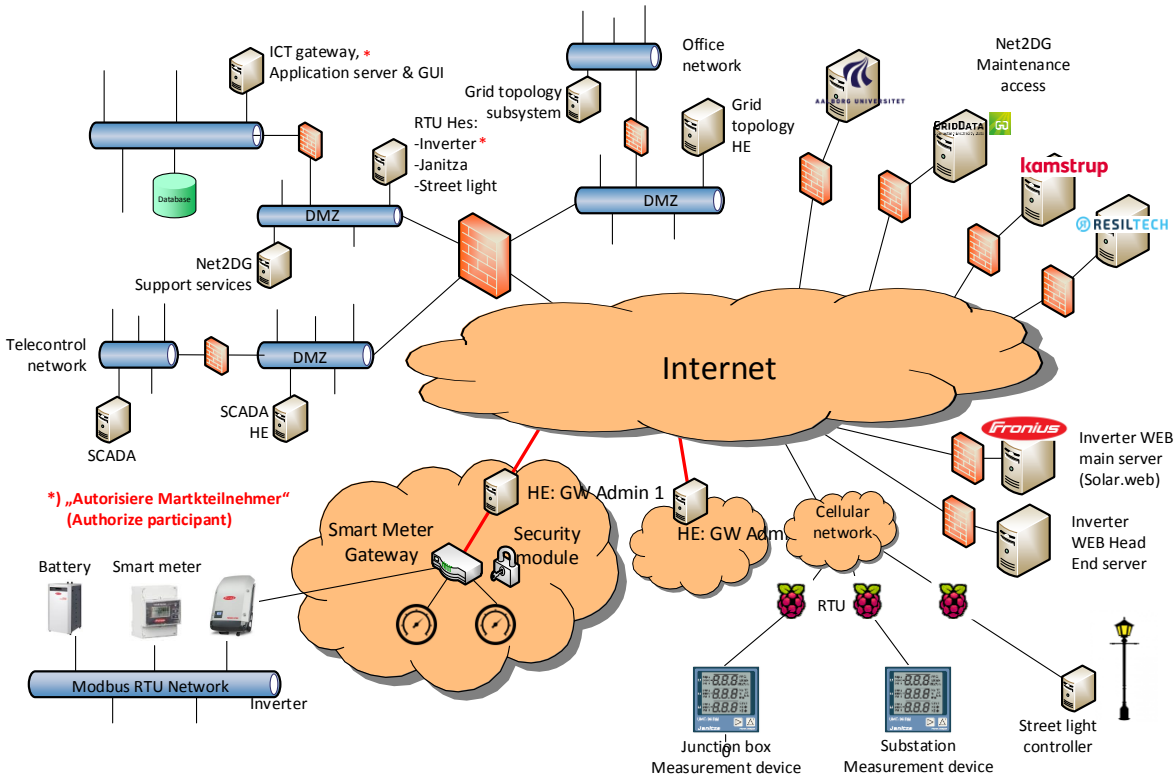

Figure 26 – Deployment variant for Stadtwerke Landau field trial

10.2 Deployment at TME

TME already has a full-scale smart meter rollout in place including CT meters at the substation. The Net2DG field trial will use a small part of the distribution grid (approximately 1000 households). Data from the smart meters in this area will be provided via the AMI HES, which also provides datacollection from substation monitoring devices. Communication to smart meters are via RF Mesh or 2G communication. RF Mesh meters are collected by a concentrator, which in turns is connected via fiber og 3G.

The other parts of the Net2DG field trial setup are expected to resemble the setup for Stadtwerk Landau, see figure Figure 27.

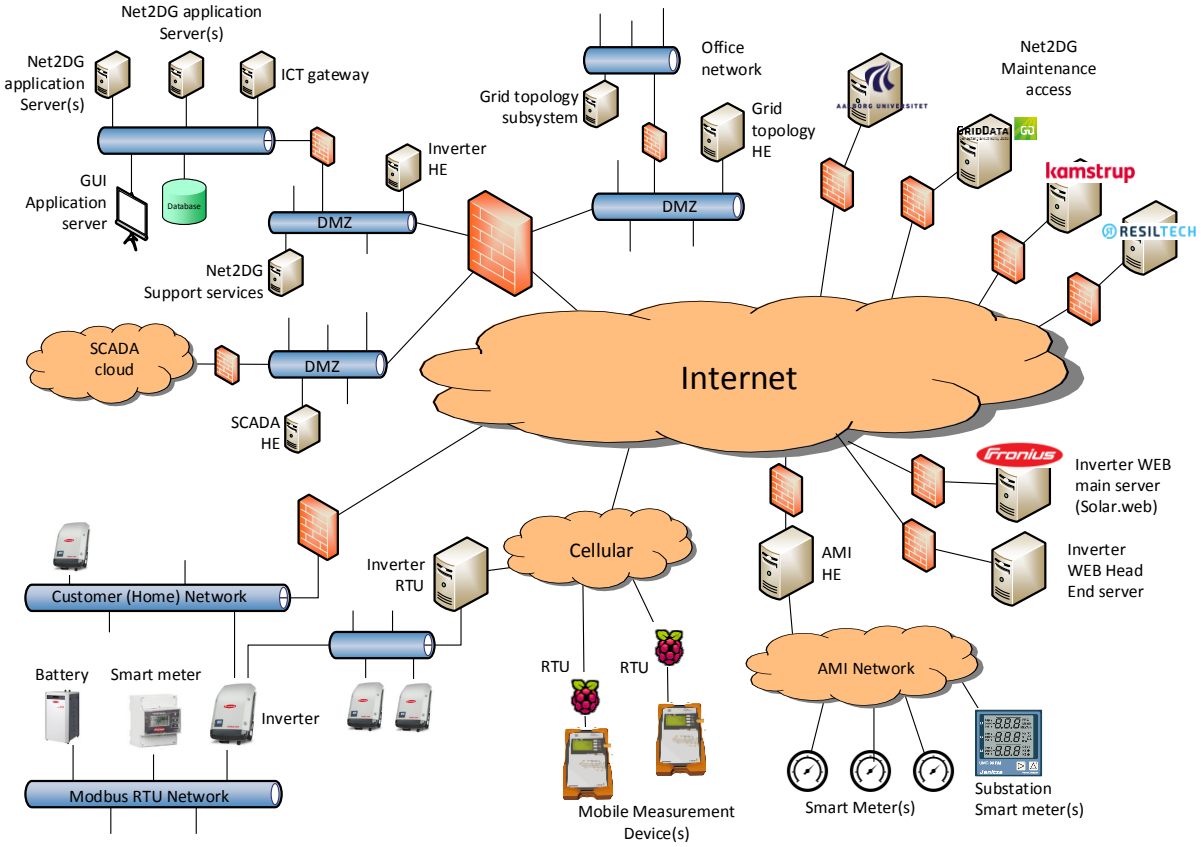

Figure 27 – Deployment variant for TME field trial

11 Conclusions and Outlook

Throughout this document, the anticipated Net2DG system architecture has been described and analysed from various viewpoints.

Section 3 - 5 contains a set of supplementary requirements to the functional requirements captured in the Net2DG deliverable D1.1. Emphasize has been on establishing guiding architectural principles and non-functional requirements which should be used throughout the project to validate design elements and ensure a firm basis for later system validation.

Requirements for system administration have been added as well, these were omitted from D1.1 as they were agnostic to the domain oriented focus for that document, but they are equally valid for the system design going forward and the resulting operational characteristics.

Section 6 outlines the high-level architecture with subsystems and the anticipated information flow between them. Important principles like simplicity and decoupling between parts have been incorporated into the design and it constitute a firm basis for the implementation work in WP2-4.

Section 7 and 8 adds further details to the communication architecture and the interface design for the most important subsystems.

Section 9 provides a preliminary security analysis (which will be further detailed in WP3) and highlights the most important security requirements, which should be followed to ensure GDPR compliance and secure communication network operation.

Section 10 shows the first draft deployment architecture for the field trials; this part will be revised as part of WP5.

The overall conclusion for this document and the work behind it is that the system architecture and its basic constructs for subsystem interaction has been established. It is based on sound principles for system-of-systems and can fit into an existing system landscape for a small or medium sized DSO in the European setup.

As the work in WP2-5 progress, it will be important to revise this document and keep it up-to-date. An update is planned for M20.