Technical Specification WAMS

Version 1.0

01.03.2023

Short Description	This user specification includes the professional and technical requirements for an existing or newly created IT system for the APG Wide Area Measurement System (WAMS) from a user's point of view.	
Author	**Austrian Power Grid AG (APG)**	**Responsible Organizational Unit**
		US (System Standards)
Confidentiality Level	**Public**	**Entitled Recipient Group**
		Tendering Participants

Content

1 Document Information....4
1.1 Goal of the Document....4
2 General Information....5
2.1 About APG....5
2.2 Description of the Areas....5
3 Initial Situation and Objective....7
3.1 Initial Situation (Actual State)....7
3.2 Objectives....7
3.3 Non-objectives....8
4 Technical Overview....9
4.1 Affected Process Groups and Business Processes....9
4.2 System Context....9
4.3 Interfaces and Related Systems....9
4.4 User Roles....12
5 Functional Requirements [1]....13
5.1 #BP-001 – General....13
5.2 #BP-002 – PDC....13
5.3 #BP-003 – WAMS....19
6 Non-functional and Security Requirements....32
6.1 #NFRG-001 – Performance....32
6.2 #NFRG-002 – PDC Communication Protocols and Compatibility....33
6.3 #NFRG-003 – Interfacing with SCADA....34
6.4 #NFRG-004 – Interfacing with MATLAB and Python....34
6.5 Additional Non-functional and Security Requirements (IT Standard Catalogue)....35
7 Glossary....59
8 Directories....60
8.1 List of Figures....60
8.2 List of Tables....60
9 Appendix....61
9.1 References and Applicable Documents....61

9.2 Legal Liability 61

1 Document Information

1.1 Goal of the Document

This user specification includes the professional and technical requirements for an existing or newly created IT system for the APG Wide Area Measurement System (WAMS) from a user's point of view. It defines the totality of the demands on the deliveries and achievements of a contractor within an order determined by the customer. Thus, it differs from a functional specification to be created at a later date, which represents the concrete solution. This document, together with the documents referenced herein, serves as the basis for the tendering of the IT system and services. Thus, it has the character of a specification and is used to check the fulfilment of the requirements for the performance acceptance from the client's point of view.

2 General Information

2.1 About APG

Austrian Power Grid AG (APG) is Austria's independent transmission system operator and is responsible for the domestic transmission system at the high-voltage level.

In close cooperation with the grid operators of its European neighbours, APG monitors, co-ordinates and controls the cross-border flow of electricity and ensures the long-term and sustainable supply of electricity in Europe within the framework of ENTSO-E (European Network of Transmission System Operators for Electricity), the association of European transmission system operators.

Its key tasks include the safe operation and ongoing maintenance of the facilities. Careful and long-term network planning ensures that Austria's electricity supply system will continue to meet the constantly growing challenges of the future.

APG operates the Austrian transmission grid at the 110, 220 and 380 kV voltage levels.

2.2 Description of the Areas

The following organizational units from APG are involved in the process of the system specification:

Organizational unit	Description
US: System Standards	In its function, US specifies the framework conditions for safe and efficient operation of the transmission network. US is also responsible for the development of the APG WAMS.
UAI: IT and Telecommunication	UAI provides all IT-related services to support APG in its operations as: • Hard- and software • Operations of all infrastructure • First level support

Table 1: Organizational units

2.2.1 Primary Contact

The primary contact person in the tendering phase is responsible for any communication. All communication takes place via the tendering platform.

Name	Lukas Weibold
Role in Company	Procurement Project Team Member APG WAMS
Address	IZD Tower, Wagramer Straße 19, A-1220 Wien

Table 2: Primary contact

Queries shall be made in German or English via the electronic procurement portal apg.vemap.com of the Contracting Entity (item “Questions”) and must be received within the deadline for queries. Any questions will be collected, answered after anonymization, and will be available to interested parties for download on the Contracting Entity’s procurement portal. The applicant is obliged to take into account the answers provided as well as any corrections, and to base its request for participation thereon. With a view to equality of treatment, the Contracting Entity requests that any questions are formulated in such a way that the party submitting the questions cannot be concluded therefrom.

Questions that are not submitted electronically are inadmissible, in order to ensure the equal treatment of all applicants, and hence will be disregarded.

2.2.2 Stakeholder

Stakeholders are persons or organizational units that have a direct or indirect influence on the requirements or are directly or indirectly affected by the system to be developed. The following table lists the relevant company areas with the associated contacts and responsibilities.

Organizational unit	Name	Responsibility
US	Martin Lenz	Expert Grid Operation & Standards Project Manager APG WAMS
UAI	Konstantin Trinkl	Application Manager Project Team Member APG WAMS
UAI	Andreas Strasser	IT-Demand Management Project Team Member APG WAMS

Table 3: Stakeholder

3 Initial Situation and Objective

3.1 Initial Situation (Actual State)

APG operates a Wide Area Measurement System (WAMS) since 2016. A WAMS collects high-resolution measurements from GPS-synchronized Phasor Measurement Units (PMUs) and collects them via a Phasor Data Concentrator (PDC). The collected raw measurements from the PDC can be visualized via the existing WAMS. The existing WAMS, however, does only offer limited possibilities for direct online calculation / analysis of the raw PMU measurements and further functionalities, which can deal with increasing complexity in terms of system operation.

3.2 Objectives

The following objectives must be achieved through the launch of a new WAMS:

Objective	Description
Implementation of new functionalities	APG has specified new functionalities in the fields of tendering processes and monitoring. These must be implemented.
Increase of usability for the end-user	The usability of the current system is no longer satisfactory for many users and is perceived as out-of-date. This should be improved in the replacement project. Special emphasis should be put on the automation of processes and the avoidance of manual tasks.
Implementation of new technical requirements	The tendering process must be constantly changed by regulatory requirements and contracts. The existing system is too inflexible in this case, changes can only be made by the system provider and not configured by the department. In addition, many manual tasks have only arisen due to the fact that in the existing system this was not or could not be implemented. The new system should be highly modular and highly configurable.
Fulfilment of the internal security requirements and non-functional requirements (quality and general requirements)	The new system must meet APG's internal security requirements and the quality and other general requirements.
Ensuring availability and support	The contractor must provide and guarantee support for the new system in accordance with the defined SLAs.

Table 4: Objectives for the project

3.3 Non-objectives

The following non-objectives are defined for this project and should be considered at the introduction of the new WAMS:

Non-Objective	Description
Cloud solutions are forbidden	APG does not accept solutions that cannot be operated by APG itself. "Cloud" systems of any kind are not desirable. Thin clients or web applications are desirable.

Table 5: Non-Objectives for the project

4 Technical Overview

4.1 Affected Process Groups and Business Processes

This chapter lists and describes the process groups and business processes that are affected by the introduction of the system.

ID	Title Process Group	Description
#PG-001	WAMS	-

Table 6: Process groups

ID	Title Business Process	Description
#BP-001	General	General requirements.
#BP-002	PDC	PDC requirements.
#BP-003	WAMS	WAMS requirements.

Table 7: Business processes

4.2 System Context

The following chapters define the WAMS and delimits it from the related systems. In the following system context diagram, the system process groups, processes and use cases are presented and supplemented with the related systems and data required for their implementation. Thus, it is clear which related systems or which data are necessary for the realization of the system and which interfaces are necessary for the monitoring program.

4.3 Interfaces and Related Systems

This chapter defines all related systems, which will have interfaces to the new WAMS. Example files for specific interfaces can be requested from APG if necessary.

ID	Interface	Implementation priority
#I-001	APG PMUs (IEEE C37.118)	MUST
#I-002	Third Party PDCs from other TSOs and external partners (IEEE C37.118)	MUST
#I-003	APG ZNFS (IEC 104)	MUST
#I-004	CSV Export (Fileshare)	MUST
#I-005	MATLAB / PYTHON	MUST

Table 8: Interfaces to environmental systems

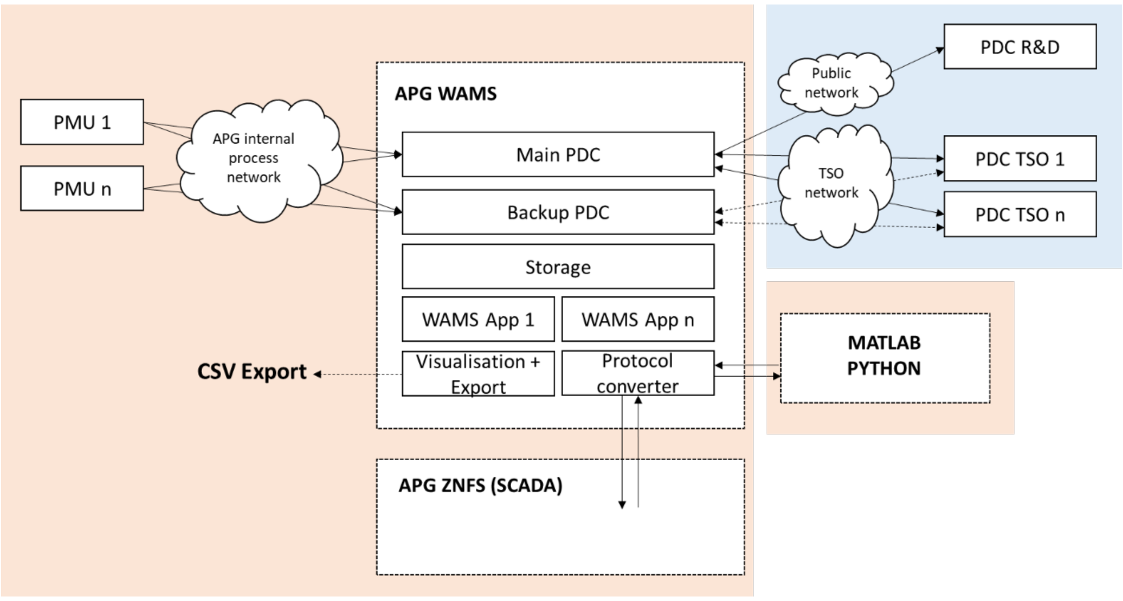

Figure 1: Interfaces to related systems

<table>
<tr><th>ID</th><th>Short</th><th colspan="2">Description</th></tr>
<tr><td><b>#I-001</b></td><td>APG PMUs</td><td colspan="2">APG PMUs (GPS-synchronized devices) measure the relevant phasor quantities from different substation feeders with high-resolution (e.g. 50 samples per second). The measurements are send via APG’s internal process network to the Phasor Data Concentrator (PDC) of the APG WAMS. The protocol being used is IEEE C37.118.</td></tr>
<tr><td><b>Input</b></td><td><b>Output</b></td><td><b>Types</b></td><td><b>Contact</b></td></tr>
<tr><td>-</td><td>Measurements</td><td>IEEE C37.118</td><td>-</td></tr>
</table>

<table>
<tr><th>ID</th><th>Short</th><th colspan="2">Description</th></tr>
<tr><td><b>#I-002</b></td><td>Third Party PDCs from other TSOs or external partners</td><td colspan="2">APG exchanges several PMU measurements with other TSOs. The measurements are exchanged between the different PDCs via a dedicated TSO network. The protocol being used is IEEE C37.118.
APG furthermore sends unidirectional PMU measurement streams to external partners (R&D) via the public internet. The protocol being used is IEEE C37.118.</td></tr>
<tr><td><b>Input</b></td><td><b>Output</b></td><td><b>Types</b></td><td><b>Contact</b></td></tr>
<tr><td>Measurements</td><td>Measurements</td><td>C37.118</td><td>-</td></tr>
</table>

<table>
<tr><th>ID</th><th>Short</th><th colspan="2">Description</th></tr>
<tr><td><b>#I-003</b></td><td>APG ZNFS</td><td colspan="2">The APG ZNFS is a SCADA for the control room operators. The ZNFS can receive real-time information from the WAMS (e.g. generated alarms, warnings, down sampled raw PMU measurements or data streams with calculation results). The ZNFS can also send real-time information to the WAMS (e.g. breaker positions of feeders).</td></tr>
<tr><th>Input</th><th>Output</th><th>Types</th><th>Contact</th></tr>
<tr><td>Measurements
Alarms
Warnings
Calculation results</td><td>Measurements
Alarms
Warnings</td><td>IEC 104</td><td>-</td></tr>
</table>

<table>
<tr><th>ID</th><th>Short</th><th colspan="2">Description</th></tr>
<tr><td><b>#I-004</b></td><td>CSV Export (Fileshare)</td><td colspan="2">The APG WAMS exports CSV files consisting of internal/external PMU measurements, alarms, warnings and relevant calculation results to a dedicated fileshare for ex-post analysis.</td></tr>
<tr><th>Input</th><th>Output</th><th>Types</th><th>Contact</th></tr>
<tr><td>Measurements
Alarms
Warnings
Calculation results</td><td>-</td><td>CSV</td><td>-</td></tr>
</table>

<table>
<tr><th>ID</th><th>Short</th><th colspan="2">Description</th></tr>
<tr><td><b>#I-005</b></td><td>MATLAB / PYTHON</td><td colspan="2">APG has developed real-time capable algorithms (MATLAB and Python scripts) to process PMU measurements. These algorithms usually return new data streams consisting of calculation results, which can serve as a basis for further processing (e.g. generation of alarms or warnings).</td></tr>
<tr><th>Input</th><th>Output</th><th>Types</th><th>Contact</th></tr>
<tr><td>Measurements</td><td>Alarms
Warnings
Calculation results</td><td><To be defined></td><td>-</td></tr>
</table>

4.4 User Roles

The following roles are needed in the IT system at least. The final user role concept has to be evaluated during the implementation phase.

ID	Role	Description
#R-001	Administrator	This role has all authorizations for configuration and administration purposes of the entire APG WAMS. The administrator can also configure the settings of the PDCs. This role is assigned to the employees of the IT (UAI).
#R-002	Standard User	This role is assigned to APG System Operators and other WAMS users within APG. Standard Users can read measurements and calculated
#R-003	WAMS Expert	This role includes all features of a Standard User and is assigned to experts, who have all authorizations to change the configuration of the different WAMS applications. WAMS Experts can also setup and configure dedicated scripts (MATLAB, Python).

Table 9: User roles

5 Functional Requirements [1]

5.1 #BP-001 – General

5.1.1 #UC-001 – General Requirements

5.1.1.1 #A-001 – The system must have a concept for user roles and permissions.

The system must have at least the following roles:

- Administrator
- Standard User
- WAMS Expert

5.1.1.2 #A-002 – The WAMS must be modular and scalable.

The WAMS must be flexible and easily adaptable to APG's needs and requirements. Adding of new functionalities depending on APG’s needs and future developments must be possible.

5.1.1.3 #A-003 – The WAMS and all its related functionalities must be independent from proprietary hardware.

The operation of the WAMS must be independent from proprietary hardware, as the server infrastructure is provided by APG.

5.2 #BP-002 – PDC

5.2.1 #UC-002 – System Architecture and Redundancy and Sizing

5.2.1.1 #A-004 – The WAMS must allow to be designed with a main (primary) and backup PDC.

The measured values are recorded in real time with the WAMS. There must be a parallel system, which additionally collects the measured values.

5.2.1.2 #A-005 – The PDCs and archive servers must be able to be configured on hot-standby mode to provide adequate system redundancy.

Because of the two servers, there must be redundancy in the storage of the data.

5.2.1.3 #A-006 – The PDCs must provide an automatic detection of any function failure.

Automatic detection of any system function failure as well as switching to available resources must be provided. Suppliers are required to describe their integrity check functionalities (e.g. detection of bitflips or storage/data failures) in detail in their offer.

5.2.1.4 #A-007 – The PDCs must provide access to the stored data at any time period.

Users must be able to access the stored data from both servers at any time period. The storage space is provided by APG and must be managed by the PDCs.

5.2.1.5 #A-008 – The PDC must provide a dedicated administrator interface for configuring main aspects of each PDC.

The main aspects of each PDC must be configured in a dedicated administrator interface:

- Connection of PMUs and PDCs
- Data streams (inputs and outputs)
- Alarms and warnings
- Data storage management functions

5.2.2 #UC-003 – PMU Data Processing and Manipulation

5.2.2.1 #A-009 – The PDCs must allow individual data manipulations.

Each PDC must allow as a minimum the following individual data manipulations:

- Data quality check and flagging
- Scaling
- Offset
- Phase to sequence conversions
- Sequence to phase conversion
- Power calculations (real power, reactive power)
- Polarity inversion
- De-trending and basic filtering
- Re-sampling of a received data stream. The re-sampling is defined as changing the data rate of a PMU data stream from one rate to another rate (e.g.: 50 samples per sec to 10 samples per sec).
- PMU and Channel Renaming

5.2.2.2 #A-010 – The PDCs must provide facilities to change the PMU ID or other identifiers of C37.118 data.

Each PDC must provide facilities to change the PMU ID or other identifiers of C37.118 data. Independent renaming facilities must be provided for streams received (i.e. re-named before being presented by the PDCs) and streams sent.

5.2.2.3 #A-011 – The PDCs must provide changes to a IEEE C37.118 stream at the point it is received.

The following changes must be made to a IEEE C37.118 stream at the point it is received:

- Re-number PMU IDs
- Re-number stream IDs
- Rename phasors (Channels)

- Rename analogue values
- Rename digital values

5.2.2.4 #A-012 – The PDCs must provide a change in the IEEE C37.118 labelling of output data as it leaves the PDCs.

The PDCs must provide a change in the IEEE C37.118 labelling of output data as it leaves the PDCs.

5.2.3 #UC-004 – PDC Input and Output Streams

5.2.3.1 #A-013 – The PDCs must display a table showing a dynamic configuration list.

Each PDC must display a table listing all the configured input and output streams, and the configuration for each stream together with their status. The list must be dynamic. If a change is made to the configuration list, it must be visible immediately.

5.2.3.2 #A-014 – The PDCs must provide the options to edit the configuration list.

Options must be available to start, stop, edit, or delete input and output streams, and configure new input and output streams.

5.2.3.3 #A-015 – The PDCs must provide a summary of the recent IEEE C37.118 configuration for each listed stream.

For each listed stream in the input and output streams table, a summary of the recent IEEE C37.118 configuration and data frames for this stream must be displayed. This provides a useful tool for analysing and reviewing the IEEE C37.118 information in its raw form. The IP addresses of any clients that are currently connected and receiving this output stream must be also listed.

5.2.3.4 #A-016 – The PDCs must allow to be configured with redundant input streams from the same PMU or PDC source.

Redundant IEEE C37.118 streams have the advantage that if one source is interrupted, data continues to be processed from the redundant source or sources. Selection of the source to be processed must be performed dynamically, choosing the highest quality data.

5.2.3.5 #A-017 – The PDCs should provide that any IEEE C37.118 stream should have the option of additional data integrity provided by automatic data recovery.

For example, loss of streaming data because of a significant network failure can be recovered automatically from The PDCs transmitting the stream. Each PDC should provide a local data buffering facility that can be used to recover lost stream data. This should operate in parallel to as well as independently of the live stream connections.

5.2.3.6 #A-018 – The PDCs must allow each output data stream to be enabled and disabled independently.

It must be possible to enable and disable each output data stream independently.

5.2.3.7 #A-019 – The PDCs must allow an independent configuration of each output data stream.

It must be possible to configure each output data stream independently. The configuration of each data stream must include, as a minimum, assigning a data stream ID, selecting data elements included for output, data frame structure, waiting times for data arrival (nor-mal and late data arrival), output data rate, and the number of data frames to be transmit-ted in one IP data packet.

5.2.3.8 #A-020 – The PDCs must allow an independent configuration of each input data stream.

It must be possible to configure each input data stream independently. The configuration of each data stream must include, as a minimum, assigning a data stream ID, selecting data elements included for input, data frame structure, waiting times for data arrival (nor-mal and late data arrival), input data rate, and the number of data frames to be transmit-ted in one IP data packet.

5.2.4 #UC-005 – PDC Input and Output Streams with PMU

5.2.4.1 #A-021 – The PDCs must allow a PMU Data Time Alignment.

Each PDC must align the PMU data according to their time stamps, not according to the order of their arrival time. The time alignment function of the PDC must be able to maintain time quality and UTC synchronization and add other data quality information of the aligned data on an individual PMU basis to be included in the output data frames.

5.2.4.2 #A-022 – The PDCs should provide special drivers for Arbiter 1133 A PMUs.

Via special drivers each PDC should allow to capture additional information (power quality, waveforms) from Arbiter 1133A PMUs. Suppliers should provide information regarding possible parameters.

5.2.5 #UC-006 – Reporting and Monitoring

5.2.5.1 #A-023 – The PDCs must provide statistics in table form for each PMU.

Each PDC must display statistics in tabular form for each PMU for the following exemplary categories:

- With poor validity
- With poor GPS lock
- Duplicates being processed
- Duplicates being ignored

5.2.5.2 #A-024 – The PDCs must provide input stream statistics.

The input stream statistics must be provided on consolidated data values from individual streams, for example:

- The current connection status
- Ingress Latency (min, max, average)
- Inter Data Frame (min, max, average)
- Missing Data Frames (total, max consecutive, % missing data)

5.2.5.3 #A-025 – The PDCs must provide output stream statistics.

The output stream statistics must be provided on consolidated data values from individual streams, for example:

- The current connection status
- Through Latency (min, max, average)

5.2.5.4 #A-026 – The PDCs must provide automatic logging of events, alarms and warnings.

The purpose of these logs is to support both the administrators and users of the PDCs in their day to day activities as well as to support troubleshooting activities in the event of problems. All PDC related events must be logged in a global log, as follows:

5.2.6 #UC-007 – Error Handling

5.2.6.1 #A-027 – The PDCs must allow the configuration of different wait time settings.

The output stream statistics must be provided on consolidated data values from individual streams, for example:

- The current connection status
- Through Latency (min, max, average)

5.2.6.2 #A-028 – The PDCs must provide an alarm when data is not received in time from a PMU data stream for more than a defined number of times.

Each PDC must be able to generate an alarm or a warning when “data not received in time” occurred to a PMU data stream for more than a number of times during a specified period. The number of times that “data not received in time” occurs must be configurable.

5.2.6.3 #A-029 – The PDCs must mark data after the maximum system wait time.

Data received after the maximum system wait time will be discarded and must be marked as “data not received”.

5.2.6.4 #A-030 – The PDCs must provide self-monitoring functions.

Each PDC must provide self-monitoring functions to monitor the operating conditions and the performance of The PDCs. Any detected problems must be reported through local display and built-in event logging.

5.2.6.5 #A-031 – The PDCs must be supported by local and remote configuration software.

The configuration software must support both local and remote configuration of each PDC. Local and remote configuration functions must meet all security requirements and procedures.

- Each log entry must be time stamped
- Each log entry must contain details including the applicable thresholds violated
- It must be possible to filter and sort the log on specific criteria

5.2.7 #UC-008 – Online Data Storage Management

5.2.7.1 #A-032 – The PDCs archive must provide continuous, rolling real-time data recording for a specified period.

Each PDC archive must provide continuous, rolling real-time data recording for a specified period. Based on the available storage capacity, data must be maintained in the system for a fixed amount of time, before being automatically deleted to make space for new data. A down sampling after defined time periods must be possible.

5.2.7.2 #A-033 – The PDCs must allow to save user-defined snapshots for an unlimited time with the original sampling rate.

A snapshot is defined manually by a user. This time section from the measured values is not subject to the defined down sampling. Each snapshot is stored with time stamp and measured values. Additionally, a name can be defined and a description can be added. A snapshot is also not deleted after the defined time. Important events or tests, for example, are saved as snapshots.

5.2.7.3 #A-034 – The PDCs must allow to export from its archive.

Each PDC must allow to export from its archive CSV and COMTRADE synchrophasor format for use in standard spreadsheets, third-party packages and COMTRADE standard readers.

5.2.7.4 #A-035 – The PDC must provide an automatic export option.

The PDC must provide an automatic export option after a defined period of time (e.g. every 5 minutes) and defined data points in CSV and COMTRADE.

5.3 #BP-003 – WAMS

5.3.1 #UC-009 – Roles and Rights Concept

5.3.1.1 #A-036 – The WAMS must allow a multi-user local and remote access for real-time data presentation.

Multiple users must be able to access the system locally or remotely at the same time. For simultaneous use, it must be possible to customize views without changing another user's view.

5.3.1.2 #A-037 – The WAMS must allow to manage access permissions for each user.

Access permission must be managed for each user separately.

5.3.1.3 #A-039 – The WAMS must allow an administrator to edit the roles and rights concept and make it globally visible.

The administrator must be able to edit and adjust the roles and rights concept and the associated permissions/authorizations. In addition, this role must be able to assign the roles to the users.

5.3.1.4 #A-039 – The WAMS must allow an administrator to add new roles

The WAMS must allow an administrator to add new roles and assign permissions to them.

5.3.2 #UC-010 – GUI and Visualisation Concept

5.3.2.1 #A-040 – The WAMS must allow to configure presentation views for each user separately.

The WAMS must offer flexible and easily custom-designable views. It must be possible to define different user view presets.

5.3.2.2 #A-041 – The WAMS must have a hierarchical GUI concept.

A hierarchical GUI concept must be possible, e.g.:

- Synchronous area level
- Control area level
- Substation level
- Data details

This serves to ensure that the user is not presented with an overload of information when entering the system. The user must be guided from high-level information to more detailed information.

5.3.3 #UC-011 – Charts and Views

5.3.3.1 #A-042 – The WAMS must provide standard charts and views.

The WAMS must provide at least the following standard charts:

- Time series charts
- Single number charts / textboxes
- Tables
- Alarm / warning boxes (e.g. red box, yellow box)

5.3.3.2 #A-043 – The WAMS should provide advanced charts and views.

The WAMS should provide the following advanced charts/views:

- 2D charts (e.g. scatter plot)
- 3D charts (e.g. spectral analysis)
- Bar charts
- Polar charts
- Gauges
- Geographic / geospatial maps
- Heat maps (frequency, voltage magnitude, angle difference)

Suppliers are required to describe their advanced charts and views capabilities in detail in their offer.

5.3.3.3 #A-044 – The WAMS must provide basic interactions with charts and views.

The WAMS must provide basic interactions for a user (zooming, panning and automatic/manual scaling) to be able to interact with the charts and views.

5.3.3.4 #A-045 – The WAMS should provide specific functions for the interaction with charts and views.

The specific functions should provide the following features:

- User selectable data from presentation
- User selectable data time window
- User selectable reference value (e.g. for representation in pu-values)
- User selectable line colour, markers and gridlines
- User selectable axes scaling (linear, logarithmic, min, max)
- Phase smoothing for phase angles
- Reviewing of data by cursors
- Numerical presentation of the last value in a legend
- Multi-axis presentation

5.3.4 #UC-012 – Real-time and Historical Event Management and Reporting

5.3.4.1 #A-046 – The WAMS must ensure a user-configurable real-time and historical event management and reporting.

In this case, categories must be defined by the user through applications or algorithms, and the reporting or the assignment of events to categories must happen through this.

5.3.4.2 #A-047 – The WAMS must store historical events in a dedicated database.

Historical events based on user-configured alarms and warnings must be stored in a dedicated database and must contain the following properties, for example:

- Severity of event (alarm, warning)
- Type of event (level, oscillatory, voltage stability,…)
- Time of occurrence
- Duration of event
- Trigger status

5.3.4.3 #A-048 – The WAMS must allow a user to search historical events.

A user must be able to search historical events based on query filters.

5.3.4.4 #A-049 – The WAMS must offer an overview of historical events.

An overview of historical events must be presented in a tabular form (event browser).

5.3.4.5 #A-050 – The WAMS should offer an export of the overview of historical events.

The WAMS should provide a manual export of historical overviews. The export of the table should at least be possible in CSV.

5.3.4.6 #A-051 – The WAMS must allow a user to add an individual textual description to events.

A user must be able to add an individual textual description to the relevant event.

5.3.4.7 #A-052 – The WAMS must allow to export automatically and manually user-configurable reports.

The format of the reports must be a user-friendly printable format (e.g. DOCX, HTML, PDF, XLSX).

5.3.4.8 #A-053 – The WAMS must allow to save templates for the exports.

The WAMS must allow a user to create templates for exports and set them as default if necessary.

5.3.4.9 #A-054 – The WAMS should provide a WYSIWYG editor for the creation of reports.

The WAMS should make it possible to compile reports with placeholders by drag and drop or similar.

5.3.4.10 #A-055 – The WAMS must allow to integrate tables, charts/views and other relevant information in the report.

The WAMS should not only be able to display textual content as a report, but must also be able to integrate charts and other graphics.

5.3.5 #UC-013 – Real-time Event Signalling

5.3.5.1 #A-056 – The WAMS must offer a real-time event signalling in the visualisation.

Real-time event signalling must be possible in the visualisation:

- Over/under level and range detection alarm and warning
- Rate of change detection alarm and warning
- Angle difference monitoring alarm and warning
- Oscillation alarm and warning
- Voltage stability alarm and warning
- Islanding detection alarm and warning
- Real-time event list

Active alarms and warnings should be displayed in a list in the main view.

5.3.5.2 #A-057 – The WAMS should offer an audio signalling.

Audio signalling in case of events should be possible. Signalling sounds and duration should be user-configurable. The sound should be different for different alarms and warnings.

5.3.5.3 #A-058 – The WAMS must allow to generate user-configurable notifications.

The system must allow to send these notifications via E-Mail, SMS, acoustic signal and direct interface to SCADA.

The qualified user must be able to configure recipients content. Furthermore, it must be possible to trigger these notifications with an alarm. In this case, the qualified user must be able to set a threshold to the alarm KPI, and only if that threshold is surpassed, the notifications must be send.

5.3.5.4 #A-059 – The WAMS must allow to define the content of the notifications.

The qualified user must be able to define a text with variable blank spaces in advance and define with what content the system fills these blanks before sending the notification.

5.3.5.5 #A-060 – The WAMS must allow to configure the notification receiver list for the different event categories.

This function must be part of the front-end application. The qualified user must be able to see and manipulate the lists of notification recipients. The event category should categorize alarms, based on user-defined thresholds for the alarm KPIs. These KPIs are sometimes measured, and sometimes calculated by the system.

5.3.6 #UC-014 – Real-time Monitoring and Detection Features

5.3.6.1 #A-061 – The WAMS must provide a real-time over/under level and range detector.

The WAMS must provide a real-time over/under level and range detector, which can be configured for each PMU raw or pre-processed data stream:

- Voltage magnitude
- Angle difference
- Frequency
- df/dt
- Active power
- Reactive power

Alarm, warning, threshold configuration and notification must be possible for each raw or pre-processed data stream.

5.3.6.2 #A-062 – The WAMS must provide a rate of change detector.

The WAMS must provide a rate of change detector, which can be configured for each PMU raw or pre-processed data stream:

- Voltage magnitude
- Angle difference
- Frequency
- df/dt
- Active power
- Reactive power

Alarm, warning, threshold configuration and notification must be possible for each raw or pre-processed data stream.

5.3.6.3 #A-063 – The WAMS must be able to calculate angle differences for a defined region (e.g. control area or synchronous area).

The WAMS must provide facilities to define the relevant region for angle difference calculation.

5.3.6.4 #A-064 – The WAMS must be able to calculate angle differences based on a central reference PMU approach and between adjacent PMUs.

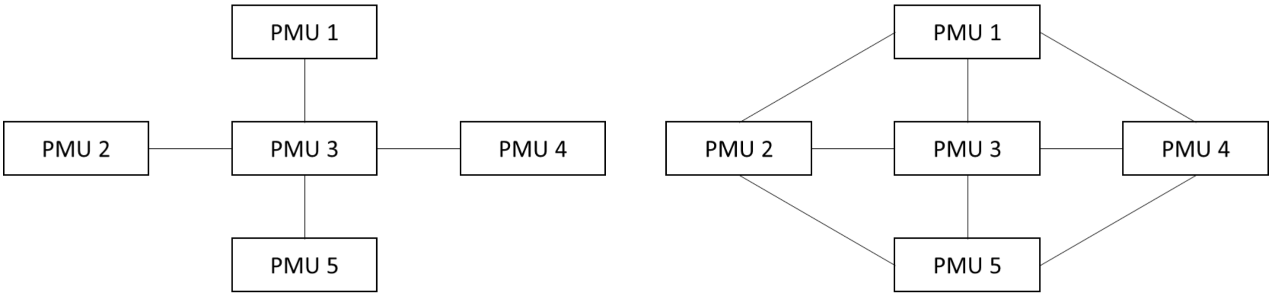

Figure 2: Central reference and adjacent PMU angle difference calculation

In case of a central reference angle calculation, the WAMS must support the definition of a ranked priority list of reference PMUs in a dedicated/given region via configuration. When data is missing or a calculation error occurs for a leading reference PMU, it must be possible to automatically use a 2nd/nth reference PMU to calculate the angle differences.

In case of a system split (island detection), the WAMS must be configured to have 2 or multiple reference areas via an automated process.

Per island a reference point must be defined. The WAMS must help in nominating reference points per island and do this automatically. This can be overridden manually via configuration. Once a system split is resolved the WAMS will return back to its normal state.

5.3.6.5 #A-065 – The WAMS must have a configurable priority list for central reference angle calculation.

If the WAMS calculates angle difference as described in #A-065 using a central reference, then there is a possibility that the reference PMU is not available. In this case, the WAMS must select a replacement PMU that is next in the priority list. The qualified user must be able to configure this list.

5.3.6.6 #A-066 – The WAMS must calculate dynamic angle references.

The WAMS must calculate dynamic angle references to avoid random perturbations and sudden changes in the reference angle, thereby providing a better representation in case of oscillations or disturbance events.

5.3.6.7 #A-067 – The WAMS must be able to handle failures or anomalies of the currently selected reference PMU.

The WAMS must be able to handle failures or anomalies of the currently selected reference PMU by performing a seamless switch to an alternative PMU via a configurable ranked priority list.

5.3.6.8 #A-068 – The WAMS must be able to monitor and detect specific categories of oscillations.

The WAMS must be able to monitor and detect the following categories of oscillations at least in the frequency range 0.01 – 10.00 Hz (Assumption: PMU measurements are provided with 50 samples per second):

- Damped oscillation
- Un-damped oscillation
- Progressive oscillation

5.3.6.9 #A-069 – The WAMS should be able to extend the frequency range of oscillation monitoring and detection.

The WAMS should be able of extending the frequency range of oscillation monitoring and detection. Suppliers are required to describe their system's capabilities in detail in their offer and to fully demonstrate their system's capabilities in FAT.

5.3.6.10 #A-070 – The WAMS must be able monitor oscillations on measured, as well as on calculated values.

The oscillation monitoring and detection must be performed on measured and calculated values:

- Frequency
- Voltage magnitude
- Angle difference
- Active power
- Reactive power

5.3.6.11 #A-071 – The WAMS must be able to calculate the oscillation properties for at least 10 individual modes.

The WAMS must be able to calculate the oscillation properties for at least 10 individual modes in the frequency range 0.01 – 10 Hz. Suppliers are required to describe their system's expandability in detail in their offer and to fully demonstrate their system's expandability in FAT.

5.3.6.12 #A-072 – The WAMS should be able to calculate the oscillation properties for more than 10 individual modes.

The WAMS should be able to calculate the oscillation properties for more than 10 individual modes in the frequency range 0.01 – 10 Hz. Suppliers are required to describe their system's expandability in detail in their response and to fully demonstrate their system's expandability in FAT.

5.3.6.13 #A-073 – The WAMS must perform the detection of the dominant modes automatically.

The detection of the dominant modes must be performed automatically.

5.3.6.14 #A-074 – The WAMS should be able to manually configure modes or mode ranges of interest.

The WAMS should be able to manually configure modes or mode ranges of interest (e.g. well-known inter-area modes).

5.3.6.15 #A-075 – The WAMS must be able to calculate various measures of damping for the different oscillation modes.

The WAMS must be able to calculate various measures of damping for the different oscillation modes, which are commonly used:

- Mode frequency
- Mode amplitude (single-sided and peak-to-peak)
- Decay time (τ)
- Halving time (τR1/2R)
- Damping coefficient (|σ|)
- Damping ratio (ζ)

These KPIs are also used to trigger alarms.

5.3.6.16 #A-076 – In the WAMS the oscillation monitoring and detection should be also based on multi-input values.

In the WAMS the oscillation monitoring and detection should be also based on multi-input values. Furthermore, the WAMS should be able to configure the parameters for the oscillation monitoring and detection.

5.3.6.17 #A-077 – The WAMS should be able to configure the parameters for the oscillation monitoring and detection.

The main parameters for the calculations inside the oscillation monitoring and detection must be configurable, e.g.:

- Time window
- Filter parameters
- List of Inputs

5.3.6.18 #A-078 – The WAMS must offer to configure the warning and alarm functionality for each mode.

The WAMS must offer to configure the warning and alarm functionality (hysteresis, time counter, combination of calculation results,…) for each mode.

A Hysteresis must be configured by requiring the threshold breach to persist for a defined period of time (in seconds) before an alarm or warning is triggered. This will ensure to avoid alerting to very brief excursions of damping values or recurring low amplitude oscillations.

5.3.6.19 #A-079 – The WAMS should offer the oscillation monitoring and detection based on spectral observation functionalities (spectrum and FFT).

The main parameters for the calculations inside the spectral observation functionalities should be configurable, e.g.:

- Time window
- Filter parameters
- Other relevant parameters for the underlying algorithm

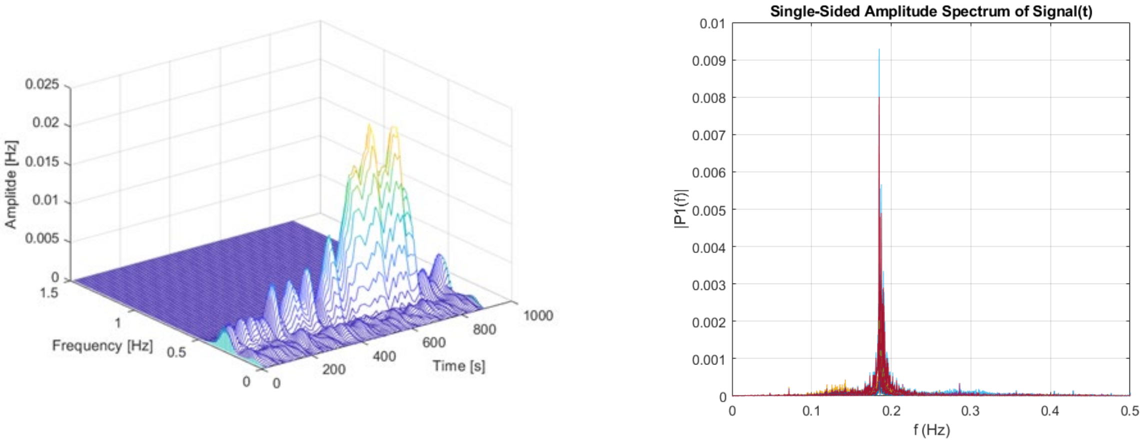

Figure 3: Spectral observation functionalities examples

5.3.6.20 #A-080 – The WAMS must be able to locate the source of oscillations.

The WAMS must be able to locate the source of oscillations (PMUs locations with the highest mode observability). The supplier is required to show a concept of how the source location identification works.

5.3.6.21 #A-081 – The WAMS must be able to identify the different coherent generator groups.

The WAMS must be able to identify the different coherent generator groups (PMU locations), which oscillate against each other. The clustering of the different coherent generator groups must be visually supported (e.g. different colouring of PMU locations).

5.3.6.22 #A-082 – The WAMS must be able to visualize mode shapes.

The mode shapes must be shown on a map and a polar plot when the corresponding mode of interest is selected. The visualization must be available in real-time and also when triggered by events defined by the qualified user.

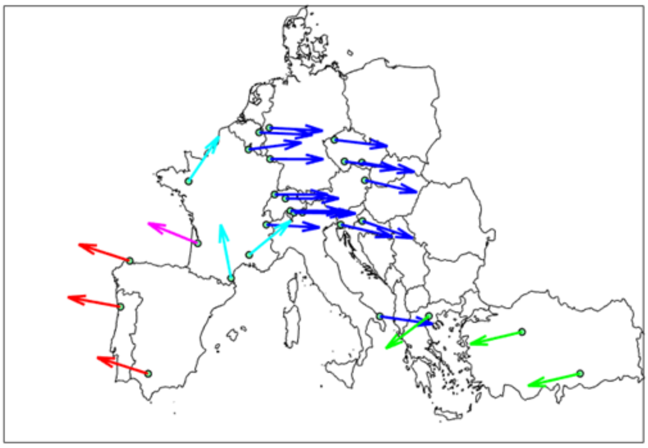

Figure 4: Mode shapes visualisation example

5.3.6.23 #A-083 – The WAMS must be able to monitor the voltage stability of a pre-defined corridor or line.

The WAMS must be able to monitor voltage stability user-configurable corridors or lines.

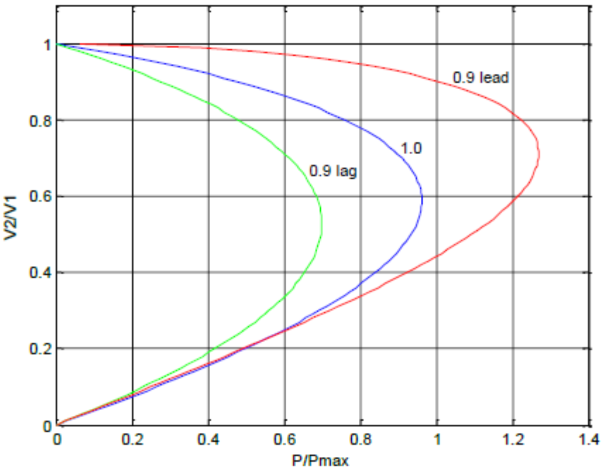

Figure 5: Voltage stability monitoring example with PV curves

5.3.6.24 #A-084 – The WAMS must be able to define various corridors or lines.

The WAMS must be able to define various corridors or lines where voltage stability monitoring is applied. Suppliers are required to describe their system's expandability (number of parallel monitored corridors or lines) in detail in their response and to fully demonstrate their system's expandability in FAT.

5.3.6.25 #A-085 – The WAMS must offer a configuration for each monitored corridor or line.

For each monitored corridor or line the main parameters for the calculation inside the voltage stability monitoring and detection must be configurable.

5.3.6.26 #A-086 – The WAMS must be able to show the calculation results in dynamic PV curves.

The dynamic PV curves should be available to the user, and should help her evaluate grid stability.

5.3.6.27 #A-087 – The WAMS must be able to trigger alarms or warnings if stability indexes are over the tolerated limits.

If a stability threshold on the PV curve is surpassed the WAMS will trigger an alarm.

5.3.6.28 #A-088 – The WAMS must be able to detect in real-time two or more electrical islands.

The WAMS must be able to detect in real-time two or more electrical islands.

The islanding detection may not only rely on frequency measurements. Suppliers are required to describe their system's capabilities in detail in their response and to fully demonstrate their system's capabilities in FAT.

If islanding has occurred, an islanding alarm event must be generated indicating the number of electrically separated islands and an island identifier for each PMU location.

5.3.6.29 #A-089 – The WAMS must offer a configuration for warnings and alarms.

It must be possible to configure the warning and alarm functionality for the islanding detection. If islanding has occurred, an islanding alarm event must be generated indicating the number of electrically separated islands and an island identifier for each PMU location.

5.3.6.30 #A-090 – The WAMS must offer a visualisation of different islands.

It must be possible to visualise the different electrical islands and PMU islanding identifiers in a map.

5.3.6.31 #A-091 – The WAMS must allow to develop user configurable (programmable) functions

The WAMS must allow to develop user configurable (programmable) functions that can be applied in real-time to raw PMU measurements or calculation results.

5.3.6.32 #A-092 – The WAMS must allow to generate real-time calculation results.

The user configurable (programmable) functions must allow to generate new real-time calculation result streams or warning/alarms.

5.3.6.33 #A-093 – The real-time calculations must provide standard functionality for data analysis.

The user configurable (programmable) functions must allow to use at least the following (logical) operations:

- Arithmetic

- Complex arithmetic
- Filtering
- Logical (AND, OR, XOR, INVERSE)
- Comparison (IF)
- Timers
- Counters
- Loops (FOR, WHILE, DO-WHILE)

5.3.6.34 #A-094 – The WAMS must allow the user to develop the configurable (programmable) functions via script based languages.

The WAMS must allow the individual calculation from signal data. The functions must be script based. Suppliers are required to present the concept for this requirement.

5.3.6.35 #A-095 – The WAMS should allow the user to develop the configurable (programmable) functions via graphical blocks.

The WAMS should allow the individual calculation from signal data with visual graphic blocks, similar to Simulink or LabView. Suppliers are required to present the concept for this requirement.

5.3.6.36 #A-096 – The WAMS should be able to perform power quality monitoring.

The WAMS should be able to perform power quality monitoring by EN 50160, IEC 61000-3-6 (Harmonics) and IEC 61000-3-7 (Flicker). Suppliers are required to present the concept for this requirement.

5.3.7 #UC-015 – Ex-post Analysis and Replay Mode

5.3.7.1 #A-097 – The WAMS must provide the user necessary tools to perform detailed ex-post analysis.

The WAMS must allow a user to utilize historical WAMS data captured around an event to conduct an ex-post analysis, that identifies the key PMU measurements that were most impacted by the disturbances as well as an initial assessment of the nature of the disturbance (i.e. generation trip, load loss, or line trip). Suppliers are required to present the concept for this requirement.

5.3.7.2 #A-098 – The WAMS should allow an oscillatory stability analysis study mode.

The WAMS should allow an oscillatory stability analysis study mode (frequency domain analysis functionality) to analyse the power spectrum, cross spectrum & coherency of the historical data to identify the dynamic characteristics observable within the PMU data such as the dominant oscillatory modes and their corresponding mode shape.

5.3.7.3 #A-099 – The WAMS should allow users to play back selected visualisation periods of historical data for enhanced ex-post analysis (replay-mode).

This should allow the qualified user a detailed analysis via stop & play of how the algorithms worked. The user should be able to control the play back speed and analyse "frame-by-frame" if required.

6 Non-functional and Security Requirements [1]

6.1 #NFRG-001 – Performance

6.1.1 PDC

6.1.1.1 #NF-001 – The PDCs must be scalable.

The system sizing for each PDC is only specified for initial sizing. The delivered system must be expandable as the input and output requirements grow.

The following describes the initial sizing:

- Each PDC must be at least able to receive real-time data streams at the highest reporting rate (50 samples per second) from up to 100 PMUs with an average of 10 phasors per PMU.

Suppliers are required to describe their system's expandability in detail in their response and to fully demonstrate their system's expandability in FAT.

6.1.1.2 #NF-002 – The PDC must not introduce more than 0.1% additional total vector error (TVE) due to filtering and data sampling functions for each output message rate.

The filtering and data down-sampling processing functions of each PDC for each output reporting rate must not introduce additional Total Vector Error (TVE) more than 0.1 %.

6.1.1.3 #NF-003 – The system clock of each PDC must be synchronized to UTC within 1 microsecond.

Each PDC system clock must have a time resolution of better than 1 microsecond.

6.1.1.4 #NF-004 – Each PDC must be able to complete all data receiving data processing data alignment, and data repacking for all inputs and outputs within 5 ms.

Each PDC must be able to complete all data receiving data processing data alignment, and data repacking for all inputs and outputs within 5 ms excluding the waiting time for data arrival. This performance requirement must be met under the maximum number of input PMU data streams and maximum number of output data steams with the maximum number of phasor as specified for the delivered as-build or expanded system.

6.1.2 WAMS

6.1.2.1 #NF-005 – The WAMS must allow a simultaneous connection of several users.

Simultaneous connection of several users (at least 5 parallel users) must be possible.

6.1.2.2 #NF-006 – The WAMS must update and refresh the data at least once a second.

Update and refreshing of measurements and relevant calculation results in the currently selected user charts/views must be possible at least once a second.

6.2 #NFRG-002 – PDC Communication Protocols and Compatibility

6.2.1 Protocols

6.2.1.1 #NF-007 – Each PDC must at least support IEEE C37.118-2005, IEEE C37.118.2-2011 and IEEE 1344 standard.

Each PDC must at least support IEEE C37.118-2005, IEEE C37.118.2-2011 and IEEE 1344 standard.

6.2.1.2 #NF-008 – Each PDC must support both UDP/IP (unicast and multicast) and TCP/IP connections. The multicast destination IP address must be configurable.

Each PDC must support UDP/IP (unicast and multicast) as well as TCP/IP connections. The qualified user must be able to configure multicast destination IP address.

6.2.1.3 #NF-009 – Each PDC must support both IPv4 and IPv6 internet protocols.

The PDCs must support all relevant internet protocols, like IPv4 and IPv6.

6.2.1.4 #NF-010 – Each PDC must be expandable and upgradable to support receiving real-time data in other data frame protocols and/or other operating modes.

Each PDC must be expandable and upgradable to support receiving real-time data in other data frame protocols and/or other operating modes.

6.2.2 Compatibility

6.2.2.1 #NF-011 – The PDC must support PMUs from different vendors.

Each PDC must support PMUs from different vendors and must not be related to only one PMU vendor. Suppliers are required to describe their compatibility with different PMU models in detail in their response.

6.2.2.2 #NF-012 – The PDC must provide proper interfaces to facilitate communications with other PDCs.

Each PDC must provide proper interfaces to facilitate necessary communications with other PDCs. Suppliers are required to describe their compatibility with different PDCs in detail in their response.

6.3 #NFRG-003 – Interfacing with SCADA

6.3.1 Protocols

6.3.1.1 #NF-013 – The WAMS must be capable to exchange event information, measured and calculated data by standard IEC 60870-5-101/104 and ICCP/TASE.2 with the SCADA of APG.

The WAMS must be capable to exchange event information, measured and calculated data by standard IEC 60870-5-101/104 and ICCP/TASE.2 with the SCADA of APG.

6.4 #NFRG-004 – Interfacing with MATLAB and Python

6.4.1 Data Exchange

6.4.1.1 #NF-014 – The WAMS must be capable to exchange user-configurable information with MATLAB and Python.

The WAMS must be capable to exchange information with MATLAB and Python (scripts) in real-time or at least close-to-real-time (≤ 30 seconds).

6.4.1.2 #NF-015 – The WAMS must allow to send each raw or calculated data stream.

The WAMS must allow to send each raw or calculated data stream (PMU measurements, calculation results from internal applications,…) to MATLAB and Python (scripts).

6.4.1.3 #NF-016 – The WAMS must allow to receive new data streams, alarms and warnings, which are generated by MATLAB and Python.

The WAMS must allow to receive new data streams, alarms and warnings, which are generated by MATLAB and Python (scripts). It must be possible to visualise these new data streams in the different charts/views and generate alarms or warnings. An incorrect behaviour of the scripts (e.g. due to internal bugs) must not negatively affect the operation of the WAMS.

6.5 Additional Non-functional and Security Requirements (IT Standard Catalogue) [1]

6.5.1 IT-Service Level Management & Compliance Management

6.5.1.1 #NFR-1-01 – A service level agreement must be negotiated with APG.

A service level agreement must be negotiated with APG, specifically for all error classes, availabilities etc.

6.5.1.2 #NFR-1-02 – The system vendor should meet certain service level requirements for class 1 errors.

This service level requirement only refers to errors of class 1 - “critical”:

The definition of class 1 errors (“critical”) is based on the AVB-IT:

Class 1 – “critical”

The practical use of any part of the IT system or of the entire IT system is not possible or unreasonably restricted. The error has a major impact on business processing or security. This refers primarily to errors that rule out further processing.

Function-related examples: System downtime without recovery, data loss/destruction of data, incorrect results in case of time-critical mass processing of data.

- Availability: 99,9 % (benchmark)
- Response time: max. 2 hours after notification by APG
- Recovery time: 6 hours, also on weekends

6.5.1.3 #NFR-1-03 – The system must appropriately consider all listed standards, and must clearly indicate any non-compliance.

The customer handles information security in accordance with the IEC 27000 series (family of standards). The application must comply with all applicable standards of that series (specifically IEC 27032 (“Guideline for cybersecurity”), IEC 27033 (“Network security”) and IEC 27034 (“Application security”)).

Security Engineering must be effected pursuant to IEC 21827 (“Information technology - Security techniques - Systems Security Engineering -- Capability Maturity Model”). Web applications must comply with ÖNORM Standard A 7700 (“Security of Web applications”).

Regarding to authentication, IEC 9798 (“Entry authentication”) must be observed. In case of message exchange and digital signatures, the following standards apply:

- IEC 9797 (“Message Authentication Codes”)
- IEC 15945 (“Specification of trusted third party services to support the application of digital signatures”)
- IEC TR 14516 (“Guidelines for the use and management of trusted third party services”)
- IEC 13888 (“Non-repudiation”)

- Cryptographic algorithms should comply with the following standards:
- IEC 18033 (“Encryption algorithms”)
- IEC 10116 (“Modes of operation for an n-bit block cipher”)
- IEC 19772 (“Authenticated encryption”)
- IEC 29192 (“Lightweight cryptography”)
- IEC 9796 (“Digital signature schemes giving message recovery”)
- IEC 14888 (“Digital signature with appendix”)
- IEC 15946 (“Cryptographic techniques based on elliptic curves”)
- IEC 10118 (“Hash functions”)
- IEC 18031 (“Random bit generation”)
- IEC 18032 (“Prime number generation”)
- IEC 18014 (“Time-stamping services”)

Cryptographic keys must be treated in line with IEC 11770 (“Key management”). Personal data must be treated in line with IEC 29100 (“Privacy framework”) and IEC 29101 (“Privacy architecture framework”)."

6.5.1.4 #NFR-1-04 – The system vendor must provide a system for bug tracking.

For bug tracking, the vendor must provide a system (such as Jira) that APG can use to deliver tickets. If any licence costs are incurred for this, the vendor must take that into account in the tender. For this ticketing system, 5-10 users on the part of APG may be expected.

6.5.2 Document & Knowledge Management

6.5.2.1 #NFR-2-01 – The system vendor must provide a functional documentation.

This functional documentation must contain at least a user manual and a description of all functional configuration parameters. This includes at least:

- Processes and process descriptions
- Masks and messages
- Structures all functions & use cases

The functional documentation must also be retraced after changes. This must also be priced in this area in the Service Level Agreement.

6.5.2.2 #NFR-2-02 – The system vendor must provide a technical documentation.

This technical documentation must include the following as a minimum:

- documentation of the application architecture
- installation manual
- maintenance manual including all routine tasks for system administrators (incl. database maintenance)
- description of all technical configuration options (especially where these settings are found and where they can be modified)

- description of logging functionalities incl. performance logging (especially how the logs are to be interpreted, e.g. error codes)
- description of all roles and privileges within the system incl. technical users and a role/authorisation matrix
- description of the data model / schema
- documentation of all interfaces (each interface must be delivered with a separate interface specification)
- documentation of (security-relevant) configurations of the used middleware and runtime environments
- documentation of all network ports used, in the form of a port matrix

6.5.2.3 #NFR-2-03 – Upon request, the system vendor must be able to provide the source code of the application plus documentation for developers at any time.

The source code may be required, for instance, for security audits and must be available upon request at any time. The documentation must include the following information:

- instructions for compiling
- source code documentation
- system architecture (modules)
- marking of security-relevant code
- technologies used (e.g. programming languages, IDEs, libraries, frameworks)

6.5.3 Service Architecture

6.5.3.1 #NFR-3-01 – The system should have a multi-tier applications architecture.

The applications architecture should be multi-tier capable or modular (at least three tiers), which will be preferred over any monolithic design.

6.5.3.2 #NFR-3-02 – The system should be loosely coupled to other systems.

Any coupling to other systems should be as loose as possible. By this we mean the use of established standards regarding interchange formats (for the exchange of data) and interface technologies (interface design).

6.5.3.3 #NFR-3-03 – The system should support parallel access of multiple application servers to the database.

Multiple application servers should be able to simultaneously access (read), and write in, the database.

6.5.3.4 #NFR-3-04 – The system should use standard interfaces, ports and proven technologies for communication between application tiers.

Interfaces between application tiers should be standardised and should use proven technologies (e.g. HTTPS, ODBC, JDBC, OLE DB, ADO.NET). On network side, IANA registered or de-facto standard ports of protocols must be used (e. g. http port 80, https port 443 etc.).

If no registered or de-facto ports are defined, the standard ports of the application must be used (e. g. Apache Webserver http port 8080). Exceptions must be constituted and approved by UAI IN team.

6.5.3.5 #NFR-3-05 – The system should support multi-core CPUs to achieve the required performance.

If multiple cores are available in the processor, the application should also use them.

6.5.3.6 #NFR-3-06 – The system should separate the functionalities of individual application layers.

The functionalities of individual application layers should be separated. In particular, no business logic should be implemented at database level.

6.5.3.7 #NFR-3-07 – The system should use standardised, proven technologies.

Standardised, proven and established technologies should be used on the server (among other things, for middleware and runtime environments such as JAVA and .NET).

6.5.3.8 #NFR-3-08 – The system should use lightweight application servers.

Lightweight application servers should be used (e.g. Apache Tomcat is preferred over JBoss, unless otherwise required to provide the necessary functionality).

6.5.3.9 #NFR-3-09 – After any unexpected server restart, the system must automatically return to a normal working state.

The system must automatically return to a normal working state, without manual intervention, after any unexpected server restart. There must be no difference to a scheduled, orderly reboot for an administrator.

6.5.3.10 #NFR-3-10 – Software running on client computers must be installable using SCCM.

Applications, plugins, services etc. that are installed on the client system must be installable using SCCM. Installation must be possible in a “silent” fashion (i.e. imperceptible to the user) using MSI packages provided by the system vendor.

6.5.3.11 #NFR-3-11 – The system must be compatible with current virtualisation systems.

All components must be compatible with current virtualisation systems. Current virtualisation systems include VMWare, HyperV and Citrix as a minimum. Any fat clients must be executable via Citrix.

6.5.3.12 #NFR-3-12 – The system should be a web application.

A thin client will be preferred over any fat-client architecture. In case of fat clients, the deployment and updates of the client systems need to be clearly regulated.

6.5.3.13 #NFR-3-13 – The system vendor must ensure that the database of the system is compatible with the listed settings and features.

The following basic conditions must be met (any deviations need to be documented and justified):

- The AUTO_CLOSE feature must NOT be used.
- The application must not use any distributed transactions nor any cross-database transactions.
- Each database must use the full recovery model.
- The compatibility mode of the databases must be 100, 110, 120 or 130, with 130 being preferred.
- The application must support SQL Always-on Availability Groups.
- The database collation must be LATIN1_General_CI_AS.
- The databases must use the contained database feature.
- MultiSubnetFailover must be supported (https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/create-or-configure-an-availability-group-listener-sql-server?view=sql-server-2017#MultiSubnetFailover,
- https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/always-on-client-connectivity-sql-server?view=sql-server-2017)
- The trustworthy bit must not be set

6.5.3.14 #NFR-3-14 – The system vendor must ensure that the database architecture is comprehensively documented.

The following aspects of the database architecture must be documented as a minimum:

- estimation of database size and growth for one year
- all database users, including description and access authorisations
- frequency of recommended index defragmentation
- estimated workload generated by the database – OLTP, OLAP, DWH
- all SQL Agent Jobs must be clearly documented (steps and schedule)
- if applicable: configuration/description of partitioning, file stream, encryption, linked servers & full text

6.5.3.15 #NFR-3-15 – The manufacturer must take into account the listed specifications of APG when modelling the data in the database of the system.

The data management concept must include at least the following:

- Master data should be clearly separated from transactional data (e.g. own tables)
- The increase of data volumes during long-term operation of the application needs to be considered in the data model
- Description which data can be archived and/or deleted manually and which data can be archived and/or deleted automatically; this must be decided in consultation with the customer; specifically, the database design should allow data partitioning.

- The physical data model must include explicitly required database artefacts for performance optimization (e.g. indexes, partitioning, etc.), as well as a plan for scheduled maintenance of the database.
- If a relational database is used, no business data must be used as primary keys; surrogate keys must be used instead.

6.5.3.16 #NFR-3-16 – The system must be able to move data that is no longer required for business operation (archiving).

It must be possible to move any transactional data that is no longer required (e.g. old data) to a separate area where it is subsequently processed or finally archived. This area must not be located within the operational system or, in case of increasing amounts of data, negatively influence its performance. The data is moved when certain thresholds or settings (when, what, how or data size, age of data, etc.) that are determined by an administrator are exceeded.

6.5.3.17 #NFR-3-17 – The system must securely connect to e-mail servers. (only relevant for systems sending or receiving e-mails)

Secure transmission must be ensured via Transport Layer Security. Communication takes place via standard ports of the SMTPS and IMAPS protocols. Authentication must be enabled with OAuth. Details can be found under (https://docs.microsoft.com/en-us/exchange/client-developer/legacy-protocols/how-to-authenticate-an-imap-pop-smtp-application-by-using-oauth).

6.5.3.18 #NFR-3-18 – The system must support the encryption and digital signature of e-mails using the S/MIME standard. (only relevant for systems sending or receiving e-mails)

- The management of certificates (import, invalidation, listing) must be possible in the application
- It must be possible to list all certificates including details (especially incl. expiry date)
- If there are several certificates for the same object, the certificate with the longest validity must be used
- Certificates and private keys must be stored safely (e.g. Keystore).

6.5.3.19 #NFR-3-19 – The system must securely connect to e-mail servers. (only relevant for systems sending or receiving e-mails)

It must be configurable for each e-mail recipient whether a digital signature and/or any encryption must be used. In order to ensure secure communication, the following must be checked prior to dispatch: In case of encryption:

- Check whether the e-mail address of the recipient is consistent with the name of the recipient certificate (subject alternative name)
- Check if the recipient certificate is valid
- If verification fails, the message must not be sent, and a corresponding alert must be displayed and logged.

6.5.3.20 #NFR-3-20 – Upon receipt of e-mails, the system must be able to check the digital signature and to decrypt any encrypted e-mails. (only relevant for systems receiving e-mails)

It must be configurable for each sender whether a digital signature and/or any encryption are expected. In order to ensure secure communication, the following must be verified upon receipt and prior to further processing:

Verification of digital signature:

- Check whether the e-mail address of the sender is consistent with the name of the sender certificate (subject alternative name)
- If several valid certificates exist for the sender's e-mail address, all available certificates of the sender must be used to verify the signature.
- Check whether the sender certificate is valid
- Check the blocking status of any certificate (CRL, OCSP) - it must be possible for the application administrator to enable and disable this check.
- Decryption:
- Check whether the recipient certificate is valid. If so, the relevant private key must be used to decrypt the message.

If verification fails, the message must not be processed, and a corresponding alert must be displayed and logged.

6.5.3.21 #NFR-3-21 – The system must put users in a position to reroute all e-mails to a configurable e-mail address, in order to not trigger any external e-mail dispatch in testing environments. (only relevant for systems sending e-mails)

This serves the purpose of testing the dispatch of e-mails with a transparent mail account in pre-production systems. In this context, encryption needs to be disabled as well. A prefix must be inserted in the subject that reflects the correct recipient, and indicates whether the message would have been encrypted.

6.5.3.22 #NFR-3-22 – The system must be compatible with the usual internet gateways (proxy).

If an internet connection is required, the following methods must be supported:

- HTTP Proxy with authentication (domain, user name and password)
- support of HTTPS Inspection (import of our proxy CA certificates must be possible). Authentication scheme: preferably NTLMSSP (basic authentication, in case of need)
- FTP Proxy with authentication (domain, user name and password). Authentication format: Raptor
- SFTP connections via SOCKS 5 with authentication (domain, user name and password)

6.5.3.23 #NFR-3-23 – The system must observe current standards for name resolution.

The system must support the configuration of all parameters (server, database host) using DNS records (CNAME records and A-records).

6.5.3.24 #NFR-3-24 – The system must be able to process DFS paths.

Access to files must be possible via DFS paths.

6.5.3.25 #NFR-3-25 – The system vendor must document any network communication into and out of the system.

A complete port concept needs to be prepared for any network communication between application components and via interfaces (must include the following for all components of the system for each port: source, destination, port, protocol).

6.5.3.26 #NFR-3-26 – The system must ensure that any communication into and from the system can be disconnected and controlled using firewalls.

The system must be implemented in such a way that the required communication can be managed through firewalls in accordance with the “least privilege” principle.

6.5.3.27 #NFR-3-27 – The system must be able to access file servers via an SMB/CIFS protocol.

If any data from file servers within the network are required, the system must support the use of SMB/CIFS shares. SMB version 2 must be used as a minimum.

6.5.3.28 #NFR-3-28 – The system must support specified technologies used at APG.

For efficient use to be made of the APG infrastructure, the system must support the following technologies:

Server:

- Microsoft Exchange Server 2019
- Windows Server 2022
- Microsoft SQL Server 2019

Container:

- Docker Container (Unix based)

Client:

- Windows 10 64-bit incl. all currently supported semi-annual updates. All future semi-annual updates must be supported upon release.
- Office 365
- IE Edge 108.0.1462.54 and later / Edge Chromium equivalent version to Edge
- Additional platforms/technologies used at APG:
- Citrix (for fat clients)

- VMware
- Citrix NetScaler (WAF)
- BPM: Bosch Inubit
- ETL: Talend Integration Suite
- Automation: Automic Automation Engine

6.5.3.29 #NFR-3-29 – The system vendor must ensure that any licence management is executable on virtualised hardware.

Technical procedures for licence verification (e.g. limitation of number of users) must be mapped virtually. There must not be any hardware dependency (e.g. dongles).

6.5.3.30 #NFR-3-30 – If the system has printing functionality, Microsoft print servers must be supported.

If the system supports the function of printing, Microsoft print server must be supported as printing service. The standard Microsoft print server functionalities must be supported (the reference for printing functions is Microsoft Office).

6.5.3.31 #NFR-3-31 – The system must be browser-independent.

As a minimum, those browsers must be supported that are listed in the APG catalogue of technologies to be supported.

6.5.3.32 #NFR-3-32 – The system should not be Java-based on the client side.

Web technologies should be able to run on APG standard clients, without requiring any additional browser plugins or runtime environments.

6.5.3.33 #NFR-3-33 – The system must use Microsoft SQL Server as database technology.

As database technology, Microsoft SQL Server 2016 must be supported.

6.5.3.34 #NFR-3-34 – The architectural concept and the offer of the system vendor must include and separately state all costs for third-party software licences.

This requirement concerns licence costs, in particular, that are incurred for third-party software required for operation, such as the Java Runtime Environment.

6.5.3.35 #NFR-3-35 – For Java based systems, the APG standard Java distribution must be used, or alternatively the offer of the vendor must identify the Java Environment separately.

Currently, the standard APG Java distribution is the "Red hat Open JDK". In case another Java distribution is used the offer of the vendor must contain all applicable license cost for development and operations of and with the Java distribution.

6.5.3.36 #NFR-3-36 – If LDAP queries are effected in the system, the LDAPS protocol must be used.

In case of LDAP queries, LDAPS must be used.

6.5.3.37 #NFR-3-37 – The system vendor must ensure that all server processes are executed as Windows processes.

Execution via the command line is not desirable.

6.5.3.38 #NFR-3-38 – The system vendor should deliver a modular system.

The software should consist of modules with defined functions that can be started and stopped separately. This serves the following objectives:

- By operating multiple instances of performance-critical modules, bottlenecks should be avoided.
- Functional changes within the application should be limited to individual modules. This is meant to minimise risks in case of new releases as well as the effort required for testing and acceptance.
- By limiting any changes to individual modules, development and release cycles should be reduced.
- In the event of any (or several) module(s) failing, no unjustified functional impact on other modules which are still running should occur.

6.5.3.39 #NFR-3-39 – The system vendor must create an XSD.

If XML is used for data exchange, an XSD (XML Schema Definition) must be created and used.

6.5.3.40 #NFR-3-40 – The system vendor must ensure that the WSDL uses the APG namespace.

If a SOAP interface is implemented (as server), the targetNamespace must begin with http://www.apg.at in WSDL. The namespace must not contain any reference to the vendor of the system under any circumstances.

6.5.3.41 #NFR-3-41 – The application has to support authentication with domain accounts against the database infrastructure.

The application has to support domain accounts for authentication against the database servers and must not support only local SQL accounts.

6.5.3.42 #NFR-3-42 – The application has to support Kerberos for authentication against the database.

If the application uses a database, it has to support authentication over Kerberos. More specifically, NTLM should not be used.

6.5.3.43 #NFR-3-43 – The performance of the application should scale approximately linearly with the available resources.

Example: If the available resources (e.g. computer cores) are doubled, the performance of the application (data throughput and response time) is expected to double.

6.5.3.44 #NFR-3-44 – File exports must prevent access to files during creation/modification.

When creating files, the system must use the postfix .tmp in the filename during the write operation. Only after the write operation is finished shall files be renamed to their target name (according to specifications).

6.5.4 IT Operations

6.5.4.1 #NFR-4-01 – It must be possible to configure and maintain the system via the user interface.

The following functions must be available for the configuration and maintenance via the user interface:

- Administration of the system must be possible with a separate “administrator” role.
- If a database is used, the configuration data must be stored there.
- Technical configuration data must be separated from functional configuration data (e.g. different database tables).
- Environment-specific configuration data (i.e. different configuration in productive and testing environments such as URLs, login data, interface configurations etc.) must be marked as such in order to be able to copy them from testing environments to productive environments.
- In particular, all technical parameters (ports, URLs, paths, etc.) must be configurable.

6.5.4.2 #NFR-4-02 – The system must display up-to-date information about the software status on the user interface.

The version number incl. patch level, the date and time of the software build need to be displayed. This information may be displayed on the help pages, for instance.

6.5.4.3 #NFR-4-03 – The system vendor must ensure that testing environments are visually distinct from productive environments.

This may be realised, for instance, by using different colours on the user interface.

6.5.4.4 #NFR-4-04 – The system must be able to display self-explanatory error messages to the user.

Functional or technical errors must be displayed in the application. The typical user of the system has no detailed technical know-how.

Self-explanatory means that the user is provided with sufficient information to deduce the cause of the error (user error or system error, operating error etc.). Purely technical information is not sufficient. If the error is too complex, error codes must be used. The error codes must be explained in the user manual. Error messages displayed to the user must not contain any security-relevant information (e.g. database details etc.).

6.5.4.5 #NFR-4-05 – Authorised users must be offered a possibility by the system to log out from the system at any time.

System users must be able to log out of the system at any time.

6.5.4.6 #NFR-4-06 – The system vendor must provide a backup and restore concept.

A backup and restore concept must be developed in cooperation with the customer's requirements. A documented restore test will be part of the acceptance process. Any foreseeable expenses incurred by the system vendor must be included in the price quoted.

The backup and restore concept must include at least the following:

- Responsibilities: division of roles & responsibilities between APG and the system vendor?
- Basic conditions: which basic parameters must be met for unrestricted backup and restore functionality?
- Minimum (system) requirements: requirements with respect to the systems (software and hardware) of APG?
- Procedure: what is the time schedule for backups, which steps will APG be responsible for (and when)?
- Sequence: succession of steps of the restore process?
- Risk assessment: quality of the backups? Will any data be lost, and what will be the effect of backup & restore on system functionality?

6.5.4.7 #NFR-4-07 – The system vendor must present a concept for scheduled maintenance that meets the availability requirements of the system.

The maintenance concept must include the roll-out of new releases/patches and also database maintenance.

Additionally, monthly operating system and application maintenance windows must be provided for.

6.5.4.8 #NFR-4-08 – The system must be compatible with current backup systems.

The system must be compatible with current backup systems. As a minimum, current backup systems refers to the systems of the following manufacturers: Symantec, IBM, CommVault or EMC.

6.5.4.9 #NFR-4-09 – The system vendor must be responsible for the configuration of middleware and runtime environments (especially security-related configuration) that are part of the delivered system.

Throughout the entire life cycle of the application, the system vendor is also responsible for the configuration of runtime environments, third-party software components and own middleware components. Examples: configuration of TomCat or JBOSS or IIS.

6.5.4.10 #NFR-4-10 – The system vendor must support version updates (major) of middleware, runtime environments and third-party software in due time before expiry of vendor support.

The vendor is responsible for timely updates of middleware, runtime environments and third-party software prior to their official end of life. End of life means that no further patches will be provided by the vendor.

6.5.4.11 #NFR-4-11 – The system and the vendor must support version updates (minor) and security patches for middleware and runtime environments.

Support means that the updates and patches can be installed by APG without first consulting the system vendor, without prejudice to vendor support or the SLAs. Note: The exact definition of minor updates will be carried out upon determining the implementation technology at the functional specification stage together with the customer.

6.5.5 Identity & Access Management

6.5.5.1 #NFR-5-01 – The system must dispose of a role-based authorisation concept (RBAC).

- It must be possible for system administrators to allocate roles to users.
- Within the application, authenticated users must have restricted privileges as required for their respective tasks (least privilege principle).
- A strict separation of roles between functional operations and administrative tasks must be provided.
- The system vendor must submit a proposal for the initial creation of roles, unless predefined by APG.
- There must be a role with read-only access.
- If applicable to the application, the allocation of privileges/authorisations to roles should also be configurable.

6.5.5.2 #NFR-5-02 – The system must execute application processes on the application server with dedicated active directory users having restricted rights (least privilege).

The system vendor must specify all the privileges required for operation in detail. Specifically, Windows system accounts must not be used.

6.5.5.3 #NFR-5-03 – The system should support single sign-on solutions.

If the system and its clients are within a Kerberos zone (realm), the Kerberos protocol should be used, otherwise the OpenID Connect (preferred) or SAML standard should be used for authentication.

6.5.5.4 #NFR-5-04 – If SAML is used as an SSO protocol, the system must permit alternative user authentication with user name and password.

The fallback must be an alternative user authentication with username and password. This is only the case if SAML is used as the SSO protocol.

6.5.5.5 #NFR-5-05 – The system vendor must take care that all application interfaces are secured in a way that they can only be accessed by authenticated systems.

All interfaces that the system offers to other systems (as server) must be secured by native authentication systems (not necessarily Kerberos or SAML, other authentication methods are possible as well).

6.5.5.6 #NFR-5-06 – The system vendor must ensure that access to all resources occurs only after successful authentication.

Resources such as File shares, e-mail accounts, SMTP servers, databases. If possible, the access to these resources must also be via single sign-on.

6.5.5.7 #NFR-5-07 – The authorisation concept against the database system has to be based on the least privilege principle.

The application has to function with the least privileges possible. Therefore, the following roles can be used for database users:

- db_datareader: For pure read access
- db_datawriter: For users that need to perform read/write operations
- db_ddladmin: In specifically argued cases, where permissions exceeding r/w operations are arguably necessary

Moreover, the db_owner role should not be necessary for the functionality of the application

6.5.6 Event Management & Logging

6.5.6.1 #NFR-6-01 – The system must have automatic logging to be able to monitor the system status and system utilisation and to allow analyses.

Each event must be categorised in the system log by severity.

- ERROR: events that limit the functionality of the application (e.g. incomplete process step), users cannot use certain functionalities any longer.

- WARN: events that cause any unexpected behaviour of the application or the failure of any resources, but which do not affect the functionality of the application (e.g. function is assumed by backup resource)
- INFO: events that describe any major expected process steps within the application (e.g. usage of any resource, data export, start/end/parameter of a complex computation, user interactions that modify the system status etc.)
- DEBUG: events that describe minor expected process steps within the application. Debug logs must present a sufficiently fine level of granularity (e.g. each step of a computation etc.) to allow for the exact determination of an error (identification of the source of the error).

The following applies to all of them:

Each event must include at least a time stamp (date and time), level of severity, application-specific information (e.g. package/namespace/class/etc.), and a description of the log event.

6.5.6.2 #NFR-6-02 – The system must log compliance-relevant actions.

Compliance-relevant actions are for example the following activities:

- successful and failed login/logout of users
- changes of privileges/authorisations
- changes of master data (incl. configurations)
- actions that change the system status (functional, workflow or process-related).
- particularly it must be recorded, which user has carried out the action at what time, and what the changes effected were (old value and new value).
- The logs must be stored in a fraud resistant manner. It must not be possible to delete log files or any referenced data (e.g. user accounts must be disabled rather than deleted).

6.5.6.3 #NFR-6-03 – The system should enable the administrator to configure the logging level during operation.

The logging level should be configurable separately for each component.

6.5.6.4 #NFR-6-04 – The system must write logs as files and store them outside the system (human readable).

- Log events must be written into a text log file that is located in a configurable path on the server.
- Log events must be structured in a way that users can interpret them easily and that automatic parsing is possible.
- Log files must be rolled at least once a day
- It must be possible to forward log events to a central logging infrastructure.
- The application must not produce any excessive logs, e.g. as a guideline, 100 MB are accepted per day for the Log Level Info. If this is exceeded, it must be justified.
- The maximum size of log files must be configurable

- All possible log entries must be documented for the information to be available for automatic extraction from the log. This also includes appropriate parsing rules (regex) that describe the field names in the log.
- Single-line log events are preferred over multi-line log events

6.5.6.5 #NFR-6-05 – The system must be able to generate the listed reports using relevant data of APG.

Reports containing summaries of the following content are desirable:

- listing of all active users (that are enabled for login) including their dedicated roles
- listing of all changes of the allocation of users/privileges over a given time interval
- listing of all changes of master data over a given time interval

6.5.6.6 #NFR-6-06 – The system must be able to log performance data to identify possible performance bottlenecks.

Performance logs must record the runtime of the processing of connected technical or functional process steps (less the waiting time for user interactions).

Performance logs must only use the INFO and DEBUG log levels, with INFO being mandatory for all actions visible at the user interface or other interfaces. DEBUG performance logs must record the performance of subprocedures (at least consumption of resources, database calls, calculation steps, etc.).

6.5.6.7 #NFR-6-07 – The system should use the SNMPv3 protocol for alerts via SNMP Traps.

SNMP Traps with SNMPv3 with appropriate MIBs (Management Information Base) should be used:

- SNMPv3 User-based Security Model with Security Type Privacy (authentication and encryption)
- Authentication protocol: SHA
- Privacy protocol: AES
- Human-readable User-based SNMPv3 Traps

6.5.7 Availability Management

6.5.7.1 #NFR-7-01 – The manufacturer must document the re-setup in the form of a disaster recovery plan.

Re-setup must be documented by the vendor in the form of a disaster recovery plan (including procedures to restore the system to working condition).

6.5.7.2 #NFR-7-02 – The system vendor must ensure that the failure of any surrounding system or interface has no unjustified functional impact on the system.

Unjustified functional impact means that processes requiring functional data may be affected by failure, while the overall system or any parts of the system that do not require such data may not. A corresponding (warning) message must inform the user or application administrator that a certain system or the corresponding data is not available for any specific processing (module). All other processes (in other modules as well) must not be affected. If the failed surrounding system is available again, the application must recognise this and proceed with normal processing.

6.5.7.3 #NFR-7-03 – The system vendor must ensure that in the event of failure of individual systems or of the entire system (including the server), recovery/re-setup is carried out within the time agreed with the customer.

A recovery time of four hours is sought.

6.5.7.4 #NFR-7-04 – The system vendor should ensure that the failover mechanism occurs separately and independently for each application layer.

The failover mechanism should be limited to the systems of the relevant layer. For instance, a failover in the business logic layer should not trigger any (automatic) failover in the database layer.

6.5.7.5 #NFR-7-05 – The system vendor should ensure that active application modules are kept to a minimum.

Active application modules should be limited to the smallest possible number of clearly defined functions (ideally one).

6.5.7.6 #NFR-7-06a – The system vendor must ensure that the following architectural requirements regarding clustering are taken into account.

- The modules that the software consists of must be clearly stated (a module is defined as an application component that can be started and stopped separately).
- It must be possible to operate multiple instances of modules in parallel (using the same database). If the module uses any external resources, the operation of multiple parallel module instances must not cause any problems. For client access, the supplier may expect that APG will provide appropriate load balancers with “sticky session” functionality.
- It must be specified for each application module whether it is reactive or active:
  - reactive: Each action of the software is triggered by a call from outside the module.
  - active: The module will execute actions without external call (e.g. via timer/scheduler, polling mechanisms, etc.)
  - Modules that are both active and reactive will be treated as active modules.
- For active application modules, it must be possible to set the module to “slave mode” (demotion), meaning that the module will respond to user and interface interactions, but will not carry out any actions proactively (scheduler/timer, etc.). For active application modules that are in slave mode, it must be possible to set them to “master mode” (the normal operating mode of active modules) (promotion). The aim is to allow for a hot standby scenario here.

- Switching the status (master, slave) of active modules must be possible via the application's GUI (for administrators) and additionally via a programming interface (REST Call, database stored procedure, or similar).
- The status of an active module must be persistent, i.e. after restarting the module, it must have the same status (master, slave) as before.
- SW that is not highly available: automatic promotion and demotion of active modules is not absolutely required. The vendor must document what the proportion of active modules in master mode to those in slave mode is meant to be (typically precisely one module in master mode, any number in slave mode). APG will then ensure during operation that the proportion is observed. Hence, no automatic failover mechanism is required.
- When starting and stopping the application, the order of the modules must be irrelevant.
- Each module must allow for a "graceful shutdown". It must be possible to trigger this shutdown via a programming interface (the use of features of the operating system is possible). If a graceful shutdown is triggered, the system must pass into slave mode (provided it is an active master module) and must not process any more requests. All requests and computations that were started must be finished, and then the module must be shut down.

6.5.8 Testing & Validation

6.5.8.1 #NFR-8-01 – The system vendor must ensure that acceptance and user tests are performed within a testing environment.

The software deployed within the testing environment must be identical with the productive environment (differences may only exist in terms of configurations). Testing environments must not share any resources with the productive environment.

6.5.8.2 #NFR-8-02 – The system vendor must test the code.

Whitebox testing (e.g. unit tests) and/or blackbox testing must have been performed prior to the transmission. These tests must include automatic source code analyses (static/dynamic) to minimise any weak spots in advance, and to ensure high quality during development.

6.5.8.3 #NFR-8-03 – The system vendor must create a testing protocol for each individual component.

When software is delivered, a testing protocol must be transmitted to the customer for individually developed components.

6.5.8.4 #NFR-8-04 – The system vendor must provide a documentation of the test cases used.

The system vendor must provide the test cases that were used for testing the application. They must cover the functionalities indicated in the specification (incl. faults). The documentation of the test cases should include the following as a minimum:

- reference to the specifications (which part of the specifications is covered by the test case)
- description of the test case
- precondition (e.g. state of the software)

6.5.8.5 #NFR-8-05 – The system vendor must provide an acceptance protocol (incl. testing protocol), when the software is handed over.

The protocol must include all test cases, incl. those from previous releases (for regression testing). Hence, this document must be updated and extended with every new software release.

6.5.9 Security - GRC

6.5.9.1 #S-1-01 – The system vendor must prepare a security concept for the application.

The application architecture, the technologies used and the processing of the data must meet the requirements regarding confidentiality, integrity, availability and privacy. The customer must provide the requirements to the vendor, based on prior risk analysis. For instance, these requirements may require additional encryption of local application data.

6.5.9.2 #S-1-02 – The system must prevent the logging of confidential or sensitive personal data.

One example of sensitive personal data is any user's religious affiliation or health data (see also Article 9 and 10 of the GDPR), whereas passwords are examples of confidential data.

6.5.10 Security - Secure Architecture

6.5.10.1 #S-3-01 – The system vendor must apply defined design principles.

Already during the design and development of the application, the principles 'secure by design', 'secure by default', 'privacy by design' and 'privacy by default' need to be taken into account. A more detailed definition of the principles is available in the GDPR.

6.5.10.2 #S-3-02 – The system vendor must ensure that external network connections are encrypted.

External network communication must be encrypted using state-of-the-art ciphers (cipher suites). In case of symmetrical encryption, at least a 256-bit key must be used, in case of asymmetrical encryption, at least a 2048-bit key. Experimental or self-developed ciphers must not be used.

6.5.10.3 #S-3-03 – The system vendor should ensure that internal network connections are encrypted.

After considering the risks/costs, internal network communication should be encrypted using state-of-the-art ciphers (cipher suites). In case of symmetrical encryption, at least a 256-bit key must be used, in case of asymmetrical encryption, at least a 20248-bit key. Experimental or self-developed ciphers must not be used.

6.5.10.4 #S-3-04 – The system vendor should ensure that the transferred data is in encrypted form and protected against any modifications.

Depending on the classification of the data transmitted, it should be secured using digital signature and/or encryption.

6.5.10.5 #S-3-05 – The system must be compatible with current anti-virus software.

All parts of the systems must be compatible with current anti-virus software.

As a minimum, current anti-virus software means Kaspersky Lab, Symantec, Intel Security (McAfee) or Sophos.

6.5.10.6 #S-3-06 – The system must be compatible with current web application firewall systems.

The system must be compatible with current WAF systems. As a minimum, current WAFs means Citrix NetScaler, Imperva SecureSphere or F5 Big-IP ASM. The required information and parameters as well as a concept regarding technical feasibility and testing procedures for future releases and updates must be provided by the contractor. During development of the system, the special requirements regarding WAF systems must be taken into account. For the avoidance of doubt, the WAF is considered as a supplement to the other security standards required in these specifications, and not as a substitute for them.

6.5.10.7 #S-3-07 – The system vendor must ensure that multi-factor authentication is supported for all systems accessible outside the LAN.

The authentication concept must be developed together with the customer, in order to verify the feasibility and use of existing multi-factor solutions (at least two factors). This requirement applies to both the application and its interfaces.

6.5.10.8 #S-3-08 – The system must transmit any authentication data in encrypted form.

The algorithms used for encryption and/or hash functions must be classified as secure at the time of the release; and it must be possible to update them in a timely fashion upon subsequent releases. Kerberos-based authentications must support AES, where type 18 (aes256-cts-hmac-sha1-96) is prefered. RC4 and other insecure algorithms are not allowed.

6.5.10.9 #S-3-09 – The system must offer options for connection to an SIEM (Security Information and Event Management) system.

In order to integrate the system into the central security system, a standardised option for integration into an SIEM system must be available.

6.5.10.10 #S-3-10 – The system must prevent replay attacks.

Replay attacks must be prevented (e.g. by using “nonces”).

6.5.10.11 #S-3-11 – The system must verify any user input on the server side prior to further processing.

Any data input (including imports/uploads or also at interfaces) must be validated on the server side.

- Whitelisting is preferable over blacklisting (whenever possible).
- In case of whitelisting, the smallest possible character set has to be used at first, which will get extended individually.
- Simple filters must be used, while complex filters must be emulated through sequential use of simple filters.

6.5.10.12 #S-3-12 – Web applications must support Webauthn / FIDO2

Relevant only for web applications, when they process authentication by itself (e. g. not using single sign-on services)

Must be supported on every zone crossing from less secure to more secure network zone (e.g. Internet -> DMZ, DMZ -> Intranet, Intranet -> Core Business Net; as well as Internet -> Cloud Hosting / Housing)

6.5.10.13 #S-3-13 – The system must terminate any inactive, interactive sessions with configurable timeout.

For example: An http session allows a user to remain logged in without repeat authentication for as long as the session is maintained. It must be configurable for each role how long the session will be maintained. The timeout will cause the automatic logout of the user.

6.5.10.14 #S-3-14 – No usage of custom URI schemes.

The vendor must not use custom URI schemes (as addition to well-known URI schemes, e. g. http:, mailto:, ldap:, ftp: etc.)

6.5.10.15 #S-3-15 – APG security services and configurations must not be disabled or changed.

Local security services and security configurations implemented by APG on servers and clients must not be deactivated or changed. This relates, for example, to malware protection, local firewalls, Windows group policies etc.

6.5.10.16 #S-3-16 – Applications must run in service user context.

Server applications must run in context of a service user dedicated for this unique application. Locally stored (runtime) data (e. g. temporary files, configurations, application data) must be stored in file system folders that are only accessable to the dedicated user. Service users must be used for one application or IT service only and must not be used for different applications or IT services. For client applications, this requirement applies analogously - in this case, written, well-founded exceptions can be approved bei UAI IT security team.

6.5.10.17 #S-3-17– Network devices used by the IT service must support 802.1X authentication protocol.

All newly added network devices (field devices, IoT, sensors, network components, hardware appliances etc.) must authenticate via IEEE 802.1X protocol. This requirement ist not relevant for APG-provided servers in APG data centres of business clients (in those cases, APG takes care for necessary compatibility).

6.5.10.18 #S-3-18 – Software must be started in a directory path, where non-administrators do not have writing access.

Execution of software in home directories of logged-in users must be avoided.

6.5.11 Security - Cryptography

6.5.11.1 #S-4-01 – The system must be able to collaborate with APG's certificate management (CA).

Certificates for the encryption of transmitted data will be provided by APG. Within the system, only these certificates can be used. For TLS, the usage of certificates issued by the customers certificate authority is obligatory. Parameters of issued certificates: Hash: SHA-256, Key length: 4096 bit (Leaf certificates: 2048 bit).The system must provide the customer with the option to roll out new certificates and withdraw existing certificates. Invalid certificates and certificates that cannot be verified must be rejected.

6.5.11.2 #S-4-02 – Microsoft Office Addins must be digitally signed.

Installation and activation of Add-Ins is only possible with valid signature.

6.5.11.3 #S-4-03 – Windows apps must be digitally signed.

Installation and activation of Add-Ins is only possible with valid signature.

6.5.12 Security - Identity and Access Management

6.5.12.1 #S-6-01 – If passwords are used in the system, the configuration of password guidelines must be possible.

It must be possible for an administrator to configure the relevant parameters (length, complexity, validity, reuse).

6.5.12.2 #S-6-02 – The system vendor must ensure that authentication data is not stored in plain text.

Moreover, the recovery of authentication data from the information stored must not be possible (e.g. by using one-way functions and/or password hashes should be based on key derivation functions).

6.5.12.3 #S-6-03 – The system vendor must ensure that authentication data is stored in a way it cannot be backcalculated (using correspondingly strong cryptographic hash functions).

Depending on the type of application, future-proof functions and key lengths must be used.

References:

BSI TR-02102 Kryptographische Verfahren (DE) (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=8)

BSI TR-02102-1 Cryptographic Mechanisms (EN) (https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=7)

Key lengths in various recommendations: https://www.keylength.com/

6.5.12.4 #S-6-04 – The software should support Windows (group) managed service accounts.

Software on Windows systems using services without built-in accounts should support Windows (group) managed accounts for simplified password change.

More information: https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview

6.5.13 Security - IT Security Incident Management

6.5.13.1 #S-8-01 – The system vendor must eliminate any problems that are of relevance to IT security as quickly as possible after security audits, and must provide temporary workarounds.

If any security vulnerabilities or weak spots are found within the system during the monthly security audits carried out by the system vendor, they must be eliminated after risk assessment by the system vendor and in consultation with the customer within the scope of the SLAs to be concluded, and/or temporary workarounds must be provided.

6.5.13.2 #S-8-02 – The system vendor must ensure that any security-relevant problems within the application, third-party software or libraries are communicated to the customer without delay and are fixed as quickly as possible.

The time until delivery of any patch / workaround to eliminate any security-relevant problems must be determined using the CVSS 3.0 Base Score, which can be calculated both for standard software and for individually developed systems. The following table provides an overview of acceptable response times:

- **Rating: None**
  CVSS 3.0 Base Score: 0.0
  Report to APG within*): -
  Correction / workaround within*): -

- **Rating: Low**
  CVSS 3.0 Base Score: 0.1 – 3.0
  Report to APG within*): - 96 hours
  Correction / workaround within*): - 4 weeks or within next possible patch cycle

- **Rating: Medium**
  CVSS 3.0 Base Score: 4.0 – 6.9
  Report to APG within*): - 48 hours
  Correction / workaround within*): - 2 weeks, possibly within next patch cycle if compensating measures are possible
- **Rating: High**
  CVSS 3.0 Base Score: 7.0 – 8.9
  Report to APG within*): - 24 hours
  Correction / workaround within*): - 1 week

- **Rating: Critical**
  CVSS 3.0 Base Score: 9.0 - 10-0
  Report to APG within*): - 12 hours
  Correction / workaround within*): - 2 days

Systems critical to the company, reachable via the public Internet, or used as security system, the time for reporting and recovery are reduced by 50%.

*) starting from the time when the vulnerability was known to the system vendor or was published in public, whichever comes first.

7 Glossary

Short	Description
WAMS	Wide Area Measurement System
PMU	Phasor Measurement Unit
PDC	Phasor Data Concentrator
FFT	Fast Fourier Transformation
APG	Austrian Power Grid
SCADA	Supervisory Control and Data Acquisition
ZNFS	Zentrales Netzführungssystem (SCADA of APG)

Table 10: Glossary and terms used

8 Directories

8.1 List of Figures

Figure 1: Interfaces to related systems 10
Figure 2: Central reference and adjacent PMU angle difference calculation 24
Figure 3: Spectral observation functionalities examples 27
Figure 4: Mode shapes visualisation example 28
Figure 5: Voltage stability monitoring example with PV curves 28

8.2 List of Tables

Table 1: Organizational units 5
Table 2: Primary contact 5
Table 3: Stakeholder 6
Table 4: Objectives for the project 7
Table 5: Non-Objectives for the project 8
Table 6: Process groups 9
Table 7: Business processes 9
Table 8: Interfaces to environmental systems 9
Table 9: User roles 12
Table 10: Glossary and terms used 59
Table 11: References and applicable documents 61
Table 12: Implementation priorities 61

9 Appendix

9.1 References and Applicable Documents

Number	Description	Filename / Link	State
[1]	Requirements Catalogue	PART D_Req_Cat_WAMS.xlsx	VALID

Table 11: References and applicable documents

9.2 Legal Liability

The following expressions are used in this document:

Key word	Description
MUST	These requirements/criteria must in any case be implemented by the manufacturer. Non-implementation means a gross restriction for the customer, whereby the customer reserves the right to change the manufacturer and/or cancel the project. The implementation can either be done directly (as requested) or can be covered by alternative solutions in consultation with the client.
SHOULD	The manufacturer SHOULD implement these requirements/criteria, but is not obliged to provide a corresponding solution. These are often use cases that are only relevant for individual stakeholders or whose importance optionally depends on the selected solution of other use cases. If a SHOULD use case is not implemented, the manufacturer must in any case provide a valid reason for this. The fulfilment of SHOULD requirements/criteria is evaluated as described in the award criteria sheet.

Table 12: Implementation priorities

The access dates of all links and online references used corresponds to the creation date of this document (page 1).