



Litgrid

**Energy Balance and Ancillary Services
Management Information System**

Technical Offer



Unicorn © 2021 – Unicorn Systems a. s.
Jankovcova 1037/49, CZ – 170 00 Prague 7

Project: Litgrid
Project – Subject: Energy Balance and Ancillary Services
Management Information System
Document Title: Technical Offer

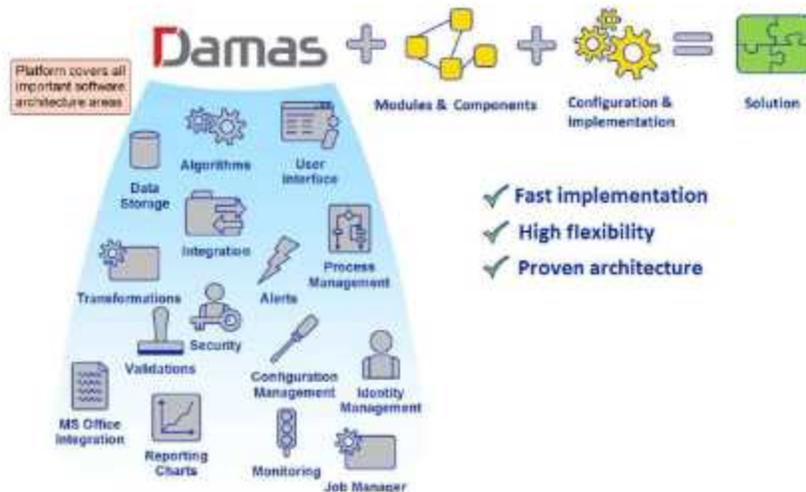
Author: Unicorn colleagues

Contact: E-mail: info@unicorn.com
Tel.: (+420) 221 400 111



1. Executive summary

This document describes the technical offer for the tender **rft 561320** of Unicorn Systems. The proposed solution for Litgrid requirements is based on the Damas MMS – the proven IT platform developed directly for the European TSOs needs. For more details about the Damas MMS please refer to the chapter 11. Damas MMS platform description.



1.1 About Unicorn Systems

Unicorn Systems has been established in 1990 and has over 30 years of experience with delivery of Information Systems and IT related services. During the 1998 Unicorn Systems delivered its first IT system in Energy sector. Until today Unicorn Systems has become well-established IT supplier for organisations and utilities in European energy market.

Unicorn Systems has vast experience in delivery of Market Managements Systems like Balancing Management Information System (followingly as BMIS). The list of the most relevant references is listed below. Please note that this list is not exhaustive, and the details will be provided on Client request as it is stated in the Special Procurement Conditions, Chapter 12, Annex 7.

- ČEPS - MMS – The most complete implementation of Damas MMS, covers the System, Transmission and Settlement Services of Czech TSO.
- EirGrid – Ramping Margin Tool - a solution based on the Damas MMS to allow a n Ireland TSO Grid Controllers to accurately schedule the Ramping Margin reserve services, thereby enabling more effective management of changing demand and generation profiles with increased wind integration.
- SEPS Damas MMS – the system manages key TSO business processes and allows SEPS to fulfill requirements of European and national legislation.
- RTE – LIBRA Platform – Centralised European solution for procurement of Replacement Reserves
- RTE – MARI Platform (ongoing) – Centralised European solution for procurement of Manual Frequency Restoration Reserves
- Fifty (Statnett and Svenska Kraftnät) – Nordic Automation Platform (ongoing) – Centralised solution for Nordic countries for procurement of Manual Frequency Restoration Reserves. This solution should be later replaced by MARI Platform.

- Fifty (Statnett and Svenska Kraftnät) – Nordic Market Management System (ongoing) – The Market Management system built upon Damas MMS to facilitate functions common for Nordic market. First modules are joint aFRR Capacity Market and mFRR Capacity Market
- eSett – Nordic Balance Settlement – The imbalance settlement solution built on Damas MMS product. The solution calculates the imbalance settlement jointly for all 4 Nordic countries – Norway, Sweden, Finland, and Denmark.

1.2 Proposed Solution

In this tender we propose to deliver Balancing Management Information System upon our platform Damas MMS. Damas MMS is a product that is continuously developed within our company for more than 15 years already and has more than 15 installations across Europe mostly for TSOs and HVDC operators.

The decision of delivery the BMIS upon Damas MMS has been taken due to several reasons. Key reasons are summarized below.

1.2.1 Flexibility

The Market Management systems are subject of continuous change as the markets and regulation evolve. The key advantage of Damas MMS is that the specific functionalities are mostly configured right in the platform, rather than specifically developed for the customer. The configuration possibilities include definition of e.g.:

- Data model and its validations
- Data views
- Workflows and processes
- Calculation formulas and aggregation principles
- Dataflows

This allows to quickly implement changes in given functionalities just by changing the metadata configuration right in the editor of the platform. Damas MMS also supports functionalities that are custom developed and integrated into the system rather than configured. In general, custom implemented functionalities are usually used for performance and availability critical modules or functionalities that cannot be handled just via the configuration.

1.2.2 Integrations

BMIS will be integrated to large number of surrounding systems and solutions. These integrations might change in the future. In terms of the technical integrations the Damas MMS support all common standards like ECP, Webservice, FTP etc. In terms of the data formats, we have integrated into the Damas MMS most of the data formats in the market. However, we see the real strength of Damas MMS in a way how new dataflows are implemented into the system. New dataflows are configured in the platform and Damas MMS then generate the XML file prescription with all the configured data. The integration to custom data format is then made just by XSD transformation between the configured generic file and specific standard (e.g. ENTSO-E Balancing Market Document). This allows changes in integrations to be made easily and mostly by configuration of the system.

1.2.3 Security

As a company we put high emphasis of security aspect in all our deliveries. Being well-established supplier for TSOs (especially in Nordics) brings requirements to meet high security standards. We adopted Secured Software Development Lifecycle into our development process. For each of our products we do a security test and involve Security Officer.

We also encourage our customers, including Litgrid, to involve their security experts to make sure the security standard of delivery is high. Also, we recommend execution of penetration tests by independent 3rd party organisation.

The general overview of proposed solution is described in General description of the system.

1.3 Project Approach

We welcome the requirement for agile delivery by LitGrid. The architecture of Damas MMS is well-suited for implementation in sprints that lasts few weeks and delivery of small increments in functionalities. We have several years of experience with this approach mostly for our clients in Nordics – Statnett, Fifty, Oriflame – or in Ireland – EirGrid.

Following the requirements, we are ready to deliver the system in 2 stages, through 164 (116 in Stage 1 and 48 in Stage 2) two-week long sprints. We consider the one calendar month after contract signature, dedicated to the preparation of the System Implementation Plan, to be a general project Start-Up phase, during which project processes will be jointly reviewed and agreed.

1.3.1 Project Start-Up Phase

We plan to start with Start-up Stage. Its main outcome is Initial Study, in which we will agree upon the High-level design of the solution as well as System Implementation Plan with all the details mandated by the requirements: the project objectives, priorities, scope and results of the stages, stakeholders, work schedule, qualitative requirements, risks and their management methods, communication principles, responsibilities, acceptance criteria for intermediate and final results.

1.3.2 Delivery Stages

In both delivery stages, the Dual Track Agile approach will be used. This approach neatly merges design activities that can be quite complex for large projects and might not be too suitable for short sprints, while still allowing for high frequency of delivery and adaptation to changing priorities, requirements, and response to user feedback.

Dual Track Agile Approach

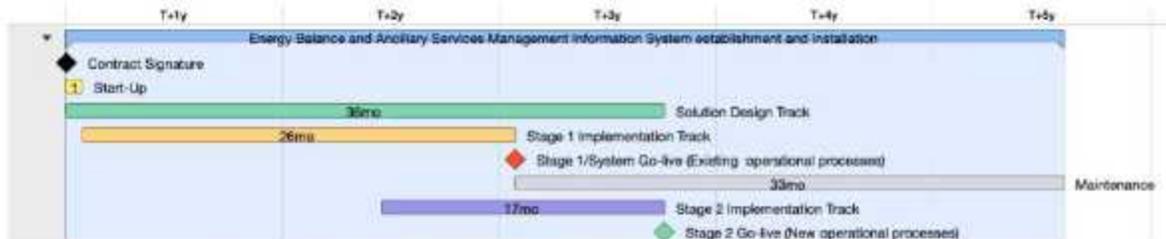
The first track – Solution Design – will continuously analyse and design user stories and add them to Product Backlog, incl. their Test Scenarios. Only items that are agreed as designed between the Supplier and the Customer can be made part of Sprint backlog for particular Sprint. This ensures that the work is well prepared to be delivered in quality by Scrum team(s).

The second track – Implementation – will deliver the user stories that have been designed within the Solution Design in sprints. Our goal is to have stable version after each sprint (so called Potentially Shippable Product Increment) and release it for Customer's testing. The feedback and bugs identified during Customer's testing will be planned for fix in upcoming versions.

Dual Track Agile Approach is great way how to ensure that system is going to be delivered according to Customer's requirements. However, it brings increased requirements for Customer cooperation during the project. The more testing and evaluation of functionalities is done in early stages the easier the user acceptance tests phase is.

Implementation Plan

Project timeline follows requirements: 1st production release (Stage 1 covering existing operational processes) will go live 27 months after contract signature. 2nd major production release (Stage 2 covering new operational processes) will go live 36 months after contract signature.



Solution Design track will start already with the Start-up phase in order to prepare set of user stories for implementation in first sprint.

The detailed project approach and plan are described in chapters **Project plan and Implementation approach**.

1.3.3 Damas MMS license

We will provide to LitGrid the Damas MMS Standard non-exclusive product license. Followingly, there will be provided the Damas MMS Product Support for the BMIS for the 24 months warranty period. Damas MMS Standard Product Support is a mandatory service. Its purpose is to cover the basic costs of ownership to ensure the long-term viability of the product. It mainly covers the maintenance and consultancy services for the Damas MMS standard product. The Damas MMS Basic Product Support does not allow takeover of new major releases of Damas MMS platform without additional license fee. For more details please see the specification of the Damas license conditions in the chapter Annex 1 - Damas License conditions .

1.4 Key assumptions and topics for negotiations

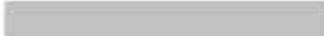
Key assumptions:

- The expected duration of the project is very short in relation to the relatively large scope. Timely delivery is only possible at the cost of a high degree of parallelization, not only on the supplier but also on the customer side.
- We assume that the customer will be able to build up three parallel analytical mini teams which will not share the human resources (except the necessary coordination). The same approach will be applied on the supplier side. These teams must be able to prepare the necessary inputs well in advance (3+ weeks) of the start of the given sprint, in order to have design finalized and test cases prepared for actual start of the sprint. (as not to block actual sprint execution by lack of work or unclear specification with open points).
- The timely delivery would not be possible without very high-level of the configurability of Damas MMS platform which significantly reduces the implementation effort of many functions. On the other hand, each product in the market (including Damas MMS), has also certain limitations. More than 80 % requirements will be solved at least partially by the configuration of Damas platform. The budget and mainly the strict time schedule of the project (which we accept without reservations) is achievable only if both counterparties understand that each requirement can be solved generally by many ways and will also understand that the preferred way is the configuration and not hardcoding. This approach has also significant benefits for the customer because the already implemented functionalities can be changed or reconfigured much more easily than the hardcoded libraries.
- We confirm that if any requirement can be solved by the configuration only at the cost of big compromises (usability, intuitiveness, performance etc.), we will not insist in the solution by configuration. However, we believe that such cases would be rather rare and that the natively

configurable user interface will be in most cases sufficient because it is proven by many existing customers.

- At the same time, we undertake to introduce to the customer, at the beginning of the project, the platform, all its important features, the configuration capabilities and also the limitations, so that the customer understands basic architectural principles of Damas MMS platform.

Topics for negotiations:

- **High number of internal and external systems to be integrated.** Several of them do not exist yet. The interfaces are sometimes not clear. These aspects are significantly increasing the risk of project delay. We suggest splitting the interfaces according to their priorities and at least partially replace some of them by manual input/copy-pasting or other similar approach for some transitional period.
- **The scope of the system itself is relatively high.** We believe that they can be prioritized and the modules with less priority (Grid loss management? Short-term adequacy?) could be delivered in the follow-up phase of the project.
- **The individual requirements can have different priorities.** We would like to indicate example of the requirements which we consider as less important or even non-essential:
 - ENTSO-E transparency: data flows for PDF files
 - REST API interface including VBA library
 - Administration of the user roles
 - Full-text search
 - Inline coding
 - Drag and drop
- **We would like to discuss very strict performance requirements,** especially processing of data flows under 1 second.
- **We would like to discuss possibility of involvement our team from** 

2. Content

1. Executive summary.....	3
1.1 About Unicorn Systems	3
1.2 Proposed Solution	4
1.2.1 Flexibility	4
1.2.2 Integrations	4
1.2.3 Security	4
1.3 Project Approach	5
1.3.1 Project Start-Up Phase.....	5
1.3.2 Delivery Stages.....	5
1.3.3 Damas MMS license.....	6
1.4 Key assumptions and topics for negotiations.....	6
2. Content.....	8
3. General description of the system.....	13
4. Implementation approach	15
4.1 Dual track agile approach.....	16
4.1.1 Implementation sprint overview	19
4.2 Activities outside sprints (Support track).....	20
4.3 Quality Assurance.....	20
4.3.1 QA Strategy.....	20
4.3.2 IT System Testing.....	22
4.4 General methods and processes.....	24
4.4.1 Security processes and standards.....	25
5. Documentation.....	26
6. Project plan.....	28
6.1 Start-up.....	30
6.1.1 Outputs.....	30
6.2 Construction.....	31
6.2.1 Solution description track.....	31
6.2.2 Implementation track.....	32
6.2.3 Defects management.....	33
6.2.4 Outputs.....	33
6.3 Customer testing.....	34
6.3.1 Acceptance tests.....	34
6.4 Warranty Support – Guarantee and Maintenance Services.....	34
6.4.1 Introduction.....	34
6.4.2 Maintenance and Support Services	35
6.4.3 Support issues handling	36
6.4.4 New System Releases / Version control	42
6.4.5 Organization Structure.....	43
6.4.6 Communication Standards.....	44
6.4.7 SLA - Service Level Agreement.....	44
6.4.8 Damas MMS product support	46

6.5	Expected cooperation.....	47
6.5.1	Calculation Formulas and Algorithms.....	47
6.5.2	Cooperation of 3 rd Parties.....	48
6.5.3	Changes in Other Systems.....	48
6.5.4	Infrastructure Preparation.....	48
6.5.5	Working Environment.....	48
6.5.6	Communication and Collaboration.....	48
7.	Project management.....	50
7.1	Roles description.....	50
7.1.1	Project communication and escalation path.....	52
7.2	Project Meetings.....	53
7.2.1	Project management meetings.....	53
7.2.2	Design meetings.....	53
7.2.3	Implementation Phase meetings.....	54
7.3	Project Reporting.....	54
7.4	Risk management.....	55
7.4.1	Risk classification.....	55
7.4.2	Risk Management Process.....	56
7.4.3	Main project risks.....	56
8.	Training.....	58
8.1.1	Damas MMS Platform Introduction Training.....	58
8.1.2	Project Organisation Training.....	58
8.1.3	Test team training.....	58
8.1.4	User training – Admins, System Users.....	59
9.	System architecture.....	60
9.1	Solution overview.....	60
9.2	Logical view.....	60
9.3	Main architectural principles.....	61
9.4	Base technologies and standards.....	62
9.5	Environments.....	63
9.6	Infrastructure.....	64
9.6.1	Deployment view.....	64
9.6.2	Disaster and recovery.....	66
	Hardware 67	
9.6.3	Virtual servers.....	68
9.6.4	Licences.....	68
9.7	Data backup, restore, high availability.....	69
9.7.1	Backup.....	69
9.7.2	Database restore.....	70
9.7.3	Database disaster recovery.....	70
9.7.4	Database high availability.....	71
9.8	Monitoring.....	71
9.8.1	Batch / asynchronous servers.....	71
	72
9.9	Alignment with Non-Functional Requirements.....	73

9.9.1	Requirements for the Software and Architecture.....	73
9.9.2	Requirements for the System's Environments.....	80
9.9.3	Requirements for User Interface and Ergonomics (Usability)	81
9.9.4	Requirements for the System's Performance.....	86
9.9.5	Requirements for the System's Scalability	88
9.9.6	Requirements for the Security and Logging	90
9.9.7	Requirements for Licences.....	95
9.9.8	Requirements for Integration Interfaces.....	96
9.9.9	Integration Components.....	99
9.9.10	Integration with external systems.....	100
9.9.11	Requirements for Testing	102
9.9.12	Requirements for Technical Documentation	104
9.9.13	Requirements for Guarantee and Maintenance Services	106
10.	Alignment with Functional Requirements	110
11.	High-Level System Design.....	114
11.1	System Configuration and Administration.....	114
11.1.1	Configuration of Market Participants.....	114
11.1.2	Configuration of Processes.....	116
11.1.3	Process Development Tools.....	117
11.1.4	Configuration of Variables.....	117
11.1.5	Configuration of Message Templates	118
11.1.6	Data Transmission Control and Monitoring.....	119
11.1.7	Alignment with Requirements for Administration and Management Tools.....	120
11.1.8	Alignment with Requirements for General Forms.....	122
11.2	Balance Planning.....	128
11.2.1	Long-term balance planning.....	129
11.2.2	Day-ahead balance planning	130
11.2.3	Intraday balance planning.....	133
11.2.4	Grid Model Data Processes.....	134
11.2.5	Alignment with Requirements for Balance Planning.....	135
11.3	Balancing Capacity.....	136
11.3.1	Market configuration	137
11.3.2	Reserve requirements	138
11.3.3	Bidding	139
11.3.4	Clearing.....	141
11.3.5	Results communication.....	142
11.3.6	Secondary market.....	143
11.4	mFRR Balancing.....	144
11.4.1	Balancing Bidding and Merit Order List	145
11.4.2	Balancing Demand.....	150
11.4.3	Activation Orders Management.....	151
11.4.4	mFRR GUI.....	153
11.5	aFRR Balancing.....	154
11.5.1	Balancing bidding and merit order list.....	154
11.5.2	Activation orders management.....	154
11.5.3	aFRR GUI	155

11.6	Settlement.....	155
11.6.1	TSO-TSO actual data electricity settlement.....	156
11.6.2	TSO-TSO Balancing energy settlement.....	158
11.6.3	Balancing services Settlement.....	159
11.6.4	Imbalance Settlement.....	160
11.6.5	Network users (NU) transmission service settlement.....	162
11.7	Financial Guarantees.....	162
11.8	Ancillary Services.....	163
11.9	EIC Codes.....	165
11.10	Data exchange formats and interfaces.....	165
12.	Damas MMS platform description.....	173
12.1	Solution overview.....	173
12.2	Key components.....	174
12.2.1	Time series engine.....	174
12.2.2	FlexiGUI.....	176
12.2.3	Calculation engine.....	177
12.2.4	MS Office integration.....	177
12.2.5	Events engine.....	177
12.2.6	BPM (Business process management).....	177
12.2.7	Enterprise integration.....	178
12.3	Architecture.....	179
12.4	User interface.....	180
12.4.1	Accessibility.....	180
12.4.2	GUI technologies.....	181
12.4.3	Deep linking.....	181
12.4.4	Icons and colors.....	181
12.4.5	Automatic refresh.....	181
12.4.6	Touch control.....	181
12.4.7	Responsive layout.....	181
12.4.8	Screen structure.....	181
12.4.9	Help and context tooltips.....	185
12.4.10	Administration interface.....	187
12.5	Time series engine.....	187
12.5.1	Flexible time dimension.....	190
12.6	Calculation engine.....	191
12.7	FlexiGUI.....	198
12.7.1	Screen filter.....	199
12.7.2	List of values (optional).....	199
12.7.3	Data grid view.....	200
12.7.4	Data submitting.....	203
12.7.5	Highlighting.....	204
12.7.6	Authorization.....	205
12.7.7	Chart view.....	205
12.7.8	Dashboards and complex screens.....	205
12.7.9	View configurator.....	207
12.8	Business process management (BPM).....	210

12.8.1	Process diagram	213
12.8.2	Used icons.....	214
12.8.3	Process instance detail.....	219
12.8.4	Context menu.....	219
12.8.5	Multiple process control window	220
12.8.6	Compact view.....	221
12.8.7	Process bar.....	222
12.8.8	Process button.....	222
12.9	Microsoft Office integration.....	223
12.10	Events engine	224
12.11	Enterprise integration.....	227
12.11.1	Communication channels.....	228
12.11.2	Key features.....	229
12.11.3	Data reception separated from business processing.....	229
12.11.4	Scalability and performance	229
12.11.5	Input processing, validations and acknowledgement.....	229
12.11.6	Separate outgoing communication.....	230
12.11.7	Configurability.....	230
12.11.8	Data flow register and monitoring	231
12.11.9	SOA concept.....	232
12.11.10	Enterprise service bus (ESB).....	233
12.11.11	Process integration patterns.....	233
12.11.12	Dataflow design and configuration	234
12.12	Security.....	240
12.12.1	Authentication.....	240
12.12.2	Authorization.....	240
12.12.3	Other	241
12.13	Reference and master data management	241
12.13.1	Reference data and business rules configuration	242
12.13.2	Master data	243
12.14	Calendar	243
12.15	Reports	244
12.16	Multilingual support	245
12.17	Multi currencies support	246
12.18	11.12.2 Metadata management	248
12.19	Data archiving	250
12.19.1	Typical data archiving process.....	251
12.19.2	Retrieving and reading archived data.....	251
12.20	Infrastructure	251
12.21	Audit.....	253
Annex 1 - Damas License conditions		254
Annex 2 – Negotiations documents.....		261

3. General description of the system

The proposed solution is built on the Damas MMS Platform – a commercial off-the-shelf solution by Unicorn Systems designed to support the business processes of transmission system operators and market operators.

The delivered solution is composed from the following main topological part:



Damas MMS Platform was designed and developed by our architects based on our long-term experience with development of custom information systems, particularly for the power industry and for TSOs. The Platform employs the latest development technologies and is well-proven in large-scale installations running in production environments. The Platform allows for highly productive implementations and offers exceptionally large configuration options. All parts of the Platform are designed to make configuration of business processes as easy as possible, and to minimize hard coding.

The Platform design was driven mainly by the following technological requirements: high flexibility, extensive customizability, high performance, high reliability and availability, transparency and security, and standardized interfaces with the external environment.

To meet the requirements for high flexibility, extensibility, high performance, reliability, and more, the proposed solution is divided into modules corresponding to the required applications (

All of them are built on the Damas MMS Platform and using its general functionalities as described in the following chapters.

Together, all the modules work as a single Energy Balance and Ancillary Services Management Information System (hereafter the System), with unified access for internal as well as external users. Neither its users nor external systems need to be aware of the system modularity – they use a single integrated user interface and a common set of APIs.

Each module built on the Damas MMS platform has the same classic 3-layer architecture consisting of the following:

- User interface implemented as a single page (SPA) web application [REDACTED] modern web browser. Each module provides its own set of screens and there are also several screens provided directly by the Damas MMS Platform itself. All of them are accessible as a single integrated user interface.

User interface uses [REDACTED] of the synchronous business logic to read and modify data. In specific situations, especially for performance purposes, user interface reads data directly from database. However, any modifications are always performed using the services of the synchronous business logic.

There is also a separate management user interface. This is a web-based user interface allowing privileged users (analysts, designers) to define business rules and configure the business logic of the System (this configuration is commonly referred to as metadata).

- External APIs supporting business-to-business communication both with market participants as well as other TSOs' systems.
- Business logic based on the Damas MMS platform off-the-shelf functionalities and configuration with necessary customizations according to requirements. The key idea here is a clear separation of synchronous and asynchronous processing. The asynchronous business logic (e.g. settlement processing or data flows processing) has different requirements on system resources than the synchronous business logic (e.g. processing of data from user interface) and it could cause excessive usage of system resources leading to poor response times. To prevent such problems, the asynchronous business logic is deployed separately. As a result, this separation allows System to perform asynchronous processing in parallel with synchronous processing while keeping the overall SLAs (especially response times of the user interface and external APIs).
- Module data stored typically in the form of time series as well as module metadata, i.e. configuration of the module business logic.

Structure of the other modules is specific and described in more details in the following chapters.

Users of the System are market operators, market participants and special users. The System is also integrated with several external systems.

The user interface is mostly configurable using [REDACTED]. If there are specific requirements that cannot be met using the configuration approach (e.g. complex dashboard screens), custom screens can be developed.

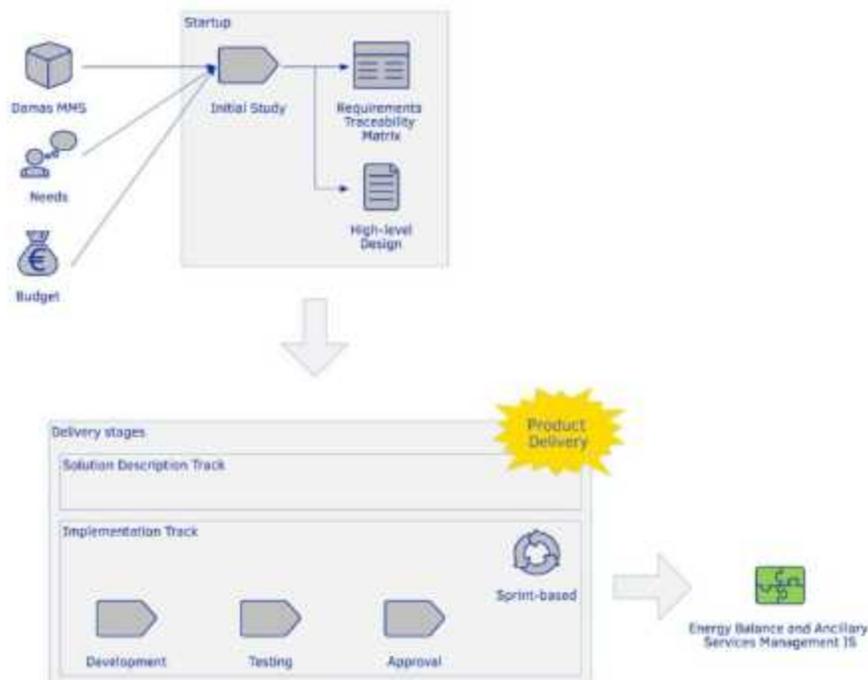
Business logic can be mostly configured by [REDACTED]

The data layer contains the data of the system. The data is divided into two main groups: metadata (configuration created by analysts) and actual business data, also called instance data. [REDACTED]

4. Implementation approach

Unicorn Systems provides modern and complex information systems designed to meet its clients' requirements using well-proven information technologies. Based on requirements and understanding of the way the Energy Balance and Ancillary Services Management Information System should work, we will design and build an information system (IS) integrated into its specific ICT environment. While designing an IS, we bear in mind the principles of best practice for each business area. Apart from standard functional features, a well-designed IS must be able to meet high demands in terms of operation, support, and scalability. The added value of the system must be balanced against its implementation and operational costs.

The project approach reflects and respects the fact that the proposed solution for the Energy Balance and Ancillary Services Management Information System is based on product Damas MMS built by Unicorn for the needs of European energy market, which will have to be configured and customized according to LitGrid's specific needs. I.e. this represents exemplary **Product Delivery** situation.



The project approach emphasizes following principles:

- > We propose to deliver the solution on Fix Time Fix Price basis. Since there is limited space for clarifications during the procurement process, we propose to confirm the total scope in Initial Study during the project start-up.
- > Initial Study shall be executed at the beginning of the project during the project **Start-up** phase. The Initial Study serves as the feasibility study and defines the scope of the whole solution, covering all important aspects (i.e. business, technical, procedural etc.).
- > The first phase of the project will also define the basic framework for the QA Strategy, Test Strategy, and Test Plan, project objectives, priorities, scope and results of the stages, preliminary scope of sprints, stakeholders register, work schedule, qualitative requirements, risks and their management methods, communication principles, responsibilities, acceptance criteria for intermediate and final results resulting in System Implementation Plan.

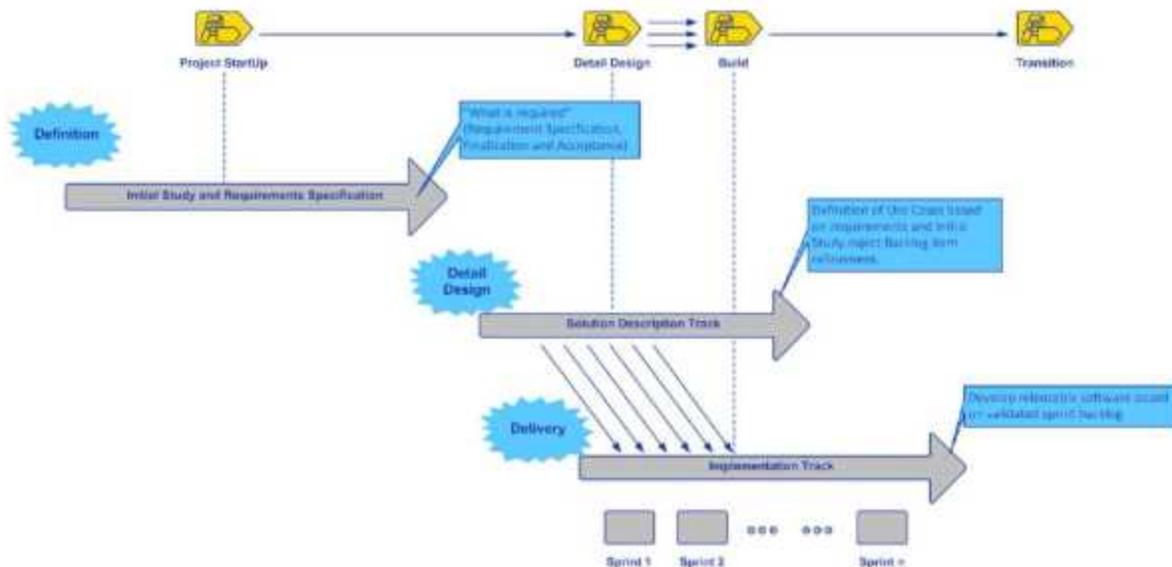
- > The user interface of all visual components will be designed by UX design experts in line with required standards and capabilities of selected products.
- > The iterative approach with Agile techniques will be used in delivery Stages 1 and 2, ensuring that the outputs of the project are presented to the customer as soon as possible. This approach mitigates possible discrepancies between requirement specifications, their design, and their implementation. Please see the Dual Track Agile approach described in the following chapters.
- > System functionality, security, performance, and other non-functional requirements will be tested using manual and automated tests.
- > Information system is documented in detail and on-line documentation is an integral part of project outputs. User Guide and texts in the system will be available in English and Lithuanian. Other project and system documentation will be available in English.
- > Unicorn's Maintenance Team, that will be responsible for provision of Warranty Support, will participate in late sprints to facilitate smooth project transition into operation.

4.1 Dual track agile approach

In line with client's requirements – which correspond well to the approach Unicorn would have suggested for this kind of project – the implementation part of the solution will use agile methodology principles. The **Dual Track Agile** approach will be used as its main framework, including namely the **Solution Design** track and the **Implementation** track. These two tracks are going to run in parallel. For the Implementation track, a Scrum based approach will be used including self-organising team(s) and the products will be delivered in an iterative and incremental manner. There is also dedicated number of hours for bug fixing as a part of each sprint.

We expect that the design will be created separately for each user story identified in the project start-up – User Story represents the main element of system delivery (and this the Product Backlog) and is accompanied by its Test Scenario(s). The accepted Designs and Test Scenarios will be moved to the implementation (i.e. made part of Sprint Backlog), developed and tested as soon as practicable. The Implementation Track will be delivering in Sprints, each sprint will be time-boxed to 2 weeks' duration. The scope for each sprint will be agreed at Sprint planning sessions and will be determined using the ordering of the Product Backlog.

We expect LitGrid to test and accept delivered functionalities after each sprint. This is the preferred way how to fluently transfer the knowledge to LitGrid during the construction phase.



Products delivered will include, but will not be necessarily limited to:

- Product Backlog
 - User Stories, Including Definition of Done
 - Test Scenarios
- Sprint Plan
- Sprint Backlog

The **Solution Description Track** will be a continuous track dedicated to the refinement of requirements and the Product Backlog preparation and prioritisation. Ordering of Product Backlog items reflects their priority. Main inputs to the Solution Description Track include namely the Initial Study, the High-Level Design, and the Requirements Traceability Matrix including the requirements and their basic decomposition. These inputs are created in the Start-up project stage.

The **Implementation Track** will be delivered in Sprints, and these will be time-boxed to 2 weeks' duration. The scope for each sprint will be agreed at Sprint planning sessions and will be determined using the ordering of the Product Backlog, by agreement of Product Owner and respective Scrum team – only designed items can be made part of Sprint backlog.

Each User story will have a Definition of Done; this will provide a detailed description of what is to be completed, along with the plan that will guide the build and the resultant product.

Once the scope within each sprint has been approved, it cannot be changed unless the following exceptions apply:

- The development of a product/user story has been blocked and the issue cannot be resolved within the time allocated for the current Sprint.
- The Implementation Team is not successful in meeting all the requirements necessary to deliver a product/user story. The removal of this must only be approved by the Product Owner(s).
- The Implementation Team has met all the requirements within the time allotted and a further product/user story can be added into the Sprint only with the agreement of the Product Owner(s).

This implementation approach is the best way how to implement and deliver the solution based on the existing platform (product) such as Damas MMS. The Damas MMS platform itself allows to configure most of the features and only some specific/additional features are being implemented by the Implementation team. Therefore, the stability of the platform is ensured during the whole project. The sprint always contains the tasks for the configuration as well as for the implementation. It is expected that the ratio between configuration and specific implementation is 80% to 20%.

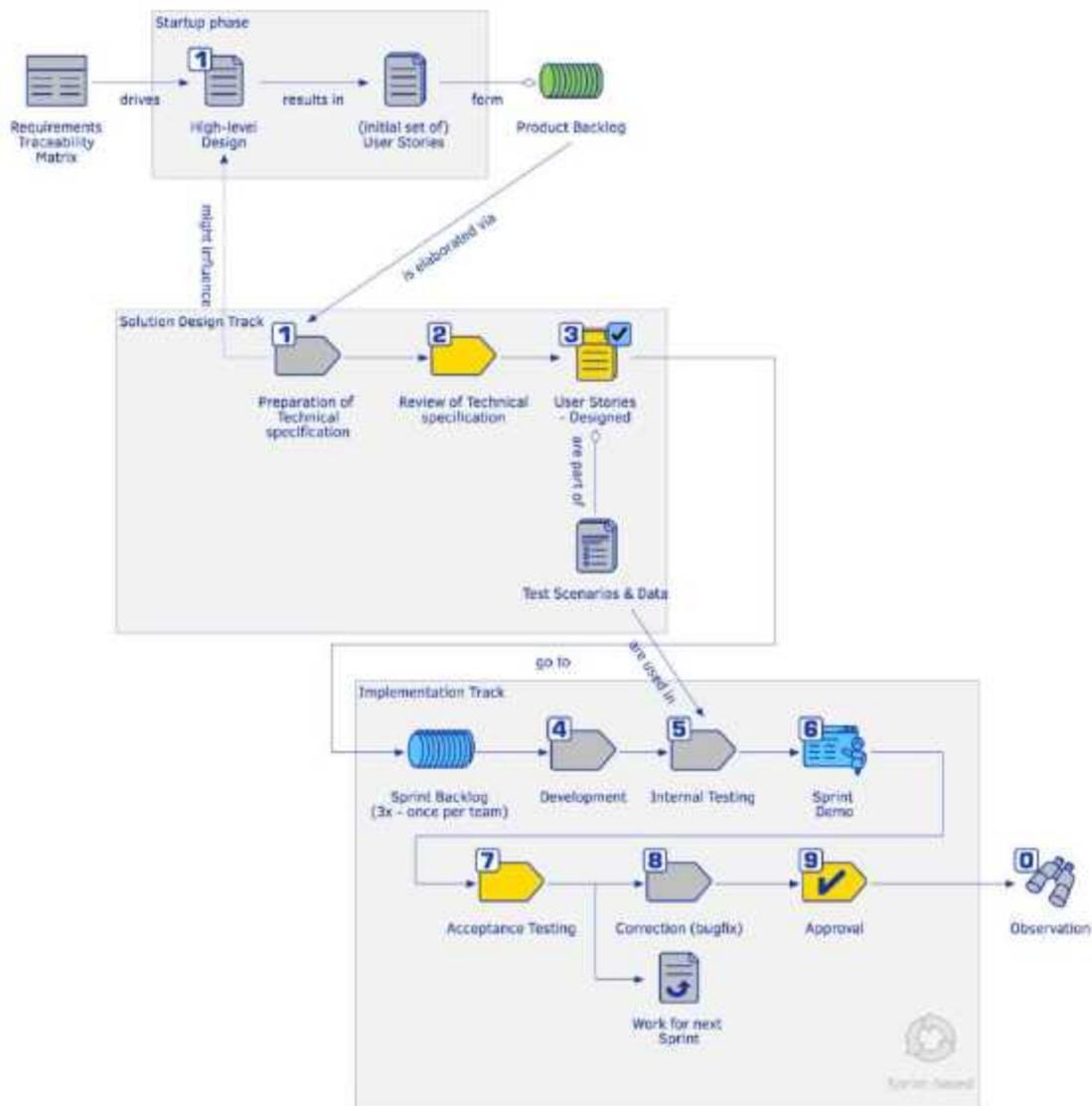
Acceptance Testing is an integral part of every Sprint (another option is to dedicate time for acceptance testing after the sprint – both options are acceptable to Unicorn and will be discussed and agreed during the Start-up phase of the project). Contrary to common delivery models, dedicated integration and acceptance testing phase covering the whole system before it goes live and including non-functional tests is not foreseen in the requested project approach. Mitigation of this risk by means of having non-functional tests period and potential overall acceptance tests round will be discussed during the project start-up phase.

A **Product Backlog** will be produced; this is an ordered list of everything that might be needed in the final solution and is the single source of requirements for any changes to be made to the product. The Product Backlog will cover all agreed requirements. Ownership of the Product Backlog rests with the Product Owner, who is then ultimately responsible for its content, availability, and ordering. It is important to note that the Product Backlog is a living artefact and any changes in business requirements, market conditions, or technology may cause changes in the Product Backlog. It is also important to note that the Scope of the project is fixed.

The project scope is fixed by the Requirements Traceability Matrix. Within the Project Start-up, a requirement list is developed collaboratively by both parties and decomposition to the initial set of User Stories. The requirement list is to be used as the basis for the planning of sprints (all sprints – Preliminary Sprint Plan) and determining the effort required throughout the lifetime of the project as calculated through the awarding of Story Points to each defined User Story.

New User Stories can be defined, provided that one or more User Stories are transferred out with an equal number of points. New User Stories that increase the total number of project Story Points may be considered as Change Requests and will be covered from the available budget for changes (budget-wise) and contingency (timewise).

The logic of the Delivery Process is depicted in the following figure (the numbers denote the steps from LitGrid's Implementation Methodology):



Each functional requirement is met by means of one or more User Stories. During project Start-Up phase, Initial Study activity results – among other things – in High-Level Design (1) and initial set of user stories, forming the Product Backlog. User Stories are elaborated in the Solution Description (= Solution Design) track – User Story definition in level necessary for the implementation (= Technical specification) is prepared (1) and Reviewed (2) by LitGrid. Approved (3) user stories can then be moved to Implementation Track for Development (4) and testing (5) on Unicorn side. During each sprint, a demonstration of new functionality (6) is held, followed by LitGrid's testing (7). Based on the feedback received in from this testing, Correction (8) is performed by Unicorn in order to achieve sprint approval (9). After the sprint, observation follows (10)

4.1.1 Implementation sprint overview

In line with the required approach, we can define the structure of each implementation sprint as follows (assuming 2 weeks per sprint, sprints starting on Wednesday for sake of example):



- **Solution Description Track – Ongoing design:** as described above, User Stories are being prepared continuously
 - Main forum for discussion of draft designs and their approval are **Analytical meetings**, held twice a week. Test Scenarios are discussed here as well.
- At the boundary of sprint, User Stories planned for particular sprint as well as their test cases are agreed. **Sprint Planning** meeting is held and confirms the scope of upcoming sprint – Sprint Backlog.
- Teams coordinate their work through **daily Stand-Up** meeting.
- During **Sprint development**, the scrum team delivers the user stories from Sprint Backlog. The outputs are tested on the supplier side (**Supplier Testing**), using agreed test scenario and in general as per agreed Test Strategy.
- New tested functionality is **released** and presented to the client via **Sprint Demo** meeting. To accommodate the requirements to include **LitGrid tests** of 3 days into the sprint, this Sprint Demo is held mid-sprint (in contrast to Scrum defining this ceremony for the end of sprint)
- At the end of LitGrid tests, **Defect Call** is organized to triage found issues and agree on critical items that need to be fixed within the sprint. After **Bug-fixing Critical** items, sprint is closed via **Sprint Closeout** session where critical fixes are demonstrated and sprint acceptance is issues (in written form, either of protocol, approved meeting minutes, approval by email or similar).
 - At the end of module preparation (last sprint of given module development), approval of the module as a whole might also follow in the same manner.
- Apart from Sprint Closeout, the team organizes **Sprint Retrospective** to discuss what went well during the sprints, what (and how) needs to be fixed in the team and the process. Ideas for further optimizations are shared.

Particular organization of sprints for this project will be agreed during Start-up phase and can be updated as a results of Sprint Retrospectives.

E.g. optimization can be found in moving sprint tests by LitGrid after the end of sprint, thus ensuring higher throughput (more development time in single sprint focused on new functionality). We have found by experience from other projects in Nordics that 3 weeks sprint duration represents suitable balance between focused delivery, frequency of releases and test opportunity on the client side.

4.2 Activities outside sprints (Support track)

Some of the project activities are executed outside Sprint-based approach. These are typically activities outside core analysis & design>development>testing cycle: preparation of infrastructure and environments, user training, go live preparations and similar. These activities are coordinated with Scrum teams by the Project Manager.

Special attention needs to be given to integration-related activities (integration tests with 3rd parties and systems), that usually are not suitable for agile approach (as the counterparts are usually not agile).

4.3 Quality Assurance

Unicorn's methodology defines quality as the ability to be used – to fulfil the intended purpose and the needs of its users.

Unicorn systematically improves the quality of all products, implemented systems and provided services.



This quality-oriented approach is based on:

- Team of experienced specialists understanding LitGrid business thanks to systematic training and certification in the energy domain.
- Emphasis on Unicorn's project management and delivery methodology.
- Systematic evolution of the Damas MMS platform.
- Close supervision and participation of Unicorn's senior managers in key projects.
- Unicorn ISO 9001, ISO 1006, ISO 20000, and ISO 27001 certifications.

The efficiency of this approach is proven by Unicorn's references and solutions in the TSO world.

4.3.1 QA Strategy

Our quality assurance is based on targeted focus on quality challenges in each project stage. The following table summarises the main quality challenges typical for each project phase and shows the quality measures taken by the project team. We do not consider the quality assurance to be just a thing for the testing phase. Ultimately, the quality of the entire solution begins with good specifications and solution design.

A quality assurance plan defining specific actions, tests and their extent (e.g. test types and coverage), outputs, and responsibilities will be elaborated during the Initial Study phase according to contractual requirements.

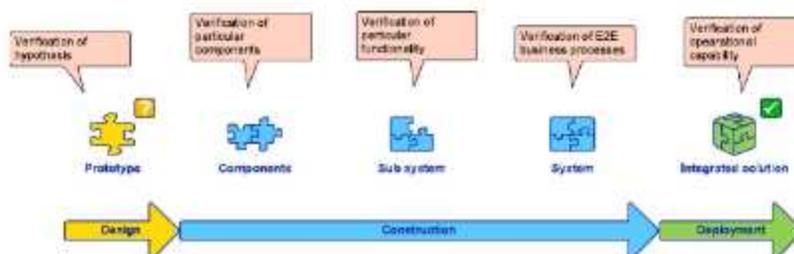
Project phase/track , quality goal	Quality challenge	Quality measures
<ul style="list-style-type: none"> • All phases <ul style="list-style-type: none"> – Project delivery within agreed parameters (Quality, Scope, Time, and Budget) 	<ul style="list-style-type: none"> • Project management • System integration 	<ul style="list-style-type: none"> • Unicorn's proven project methodology based on PRINCE2, Rational Unified Process and Scrum • Proactive approach • Open communication • Clear responsibility split • Senior resources in all key project roles

Project phase/track , quality goal	Quality challenge	Quality measures
<ul style="list-style-type: none"> • Start-up <ul style="list-style-type: none"> – Project setup and start – Elimination of key project risks 	<ul style="list-style-type: none"> • Team ramp-up and engagement • Identification of priorities • Clarity and consistency of requirements • Feasibility of solution architecture • Sufficiency of technology (performance, stability, security) • Efficient testing and deployment 	<ul style="list-style-type: none"> • Project kick-off • Review and confirmation of requirements • Elaboration and acceptance of high-level design concept • High-level Testing and deployment strategy formulation
<ul style="list-style-type: none"> • Solution Description <ul style="list-style-type: none"> – Consistent design properly mapping requirements on Damas MMS product features (minimising the fit gap) – Testable User Stories 	<ul style="list-style-type: none"> • Clarity and consistency of design • Efficient usage of the Damas platform • Consistency of requirements, design and implementation • Requirements traceability • Testability of Solution increments 	<ul style="list-style-type: none"> • Decomposition of the Solution into User Stories • Product Backlog • Detail Design of particular User Stories jointly elaborated by Supplier Business architects and LitGrid experts • Design based on the Damas MMS Platform features and respecting its limitations leveraging on knowledge and experience gained in testing of previously delivered increments • High Level Test Design and Acceptance Criteria defined as part of the User Story • Definition of Test Scenarios, preparation of Test Data

Project phase/track , quality goal	Quality challenge	Quality measures
<ul style="list-style-type: none"> • Implementation Track <ul style="list-style-type: none"> – Smooth development process – Smooth testing process – Integrated and E2E testable solution – Maintenance of production-like quality – User acceptance testing – Integration of other parties 	<ul style="list-style-type: none"> • Functional bugs • Integration bugs • Code quality • Solution stability • Deployment procedures • Solution security • Solution performance • Documentation quality • 	<ul style="list-style-type: none"> • System integration process managed on the project top level • Automated unit testing as part of the build process • Code review and code analysis • Manual functional testing of releases • Automated regression testing • Continuous integration • Solution stability • Automation of deployment procedures • Security hardening • Performance testing • Support provided to other vendors (if needed) • Disaster recovery testing • Documentation review •
<ul style="list-style-type: none"> • Support and Maintenance preparation <ul style="list-style-type: none"> – Production quality – Solution stabilisation – Support and Maintenance readiness 	<ul style="list-style-type: none"> • Solution tuning and stabilisation • Knowledge transfer 	<ul style="list-style-type: none"> • Support and maintenance team involved in later development phase • Setup and testing of support procedures • SLA fine-tuning
<ul style="list-style-type: none"> • Production 	<ul style="list-style-type: none"> • Integration issues 	<ul style="list-style-type: none"> • Support provided to users • Evolutive maintenance resolving future requirements

4.3.2 IT System Testing

Testing is a part of the Quality Control process. When testing quality, we use Unicorn Systems' testing approach, which meets the principles established by the ISTQB. The testing in general proceeds from component parts of the system to complex assemblies to the entire solution deployed into live operation. The Testing Strategy is a key document for test planning and management.



Tests of Damas MMS platform based solutions cover:

- all configurations made specifically for the purpose of particular project,
- all specifically developed functionality,
- integrations with surrounding systems,
- solution deployed to its target infrastructure

Selected tests are automated. A specific testing automation strategy is defined in the Testing Strategy (a part of the Start-up output).

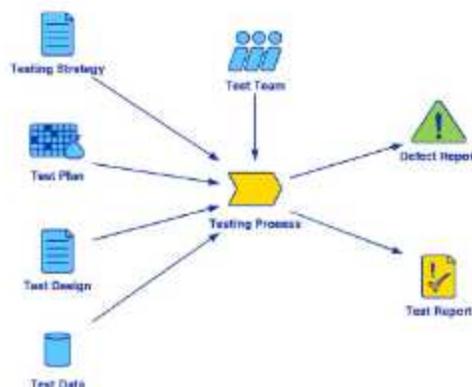
Test scenario structure maps to the Product backlog items (User Stories) to provide transparent view on test coverage and results.

The testing requires, among other things, assistance to be provided by the Customer or by a third party or parties (e.g. other vendors).

4.3.2.1 Testing Process

In order to meet the testing objectives for a project, the testing process is controlled to comply with the approved Testing Strategy. This includes:

- test planning;
- management of the Tests;
- evaluation and reporting of the test progress and results; and
- integration of deviations, if any, in the Plan.



Following chapters describe particular test types in more detail

4.3.2.2 Unit Testing

Unit testing is used to test sections of the code (individual components) in the course of development, in order to verify the functionality of a new or added code unit. The tests can be executed by developers at any time, but they also run automatically with each build.

4.3.2.3 Security Testing

As any other software project delivered by Unicorn, we will develop the System with adherence to Secure Software Development Lifecycle (SSDLC) methodology, which imposes security-related activities, milestones, and outputs, including OWASP-based checks and testing.

4.3.2.4 Functional Testing

Functional testing verifies the proper functioning of the application pursuant to specifications.

A selected set of test scenarios is automated using Selenium or similar browser automation tool (<https://selenium.dev/>). These tests then run on each newly deployed version in test environments. The objective of this automation is to provide quick application testing in order to verify basic system functionalities.

Functional testing includes:

- Atomic testing – Testing of specific functionalities using predefined test scenarios.
- End-to-end testing – Testing of (full) business processes using test scenarios.
- Regression testing – Verifying that functionality of previously tested parts of RMT have remained functional after the deployment of a new version. It is performed both using the automated tests and manually.
- Free testing – Testing of functional requirements without predefined test scenarios.

Based on the technical design outputs, test scenarios are built both for internal and for external users and the scope of testing is determined for each phase. Test scenario designs also include definitions and preparation of testing data. Before the tests are executed, both the test scenarios and the data are consulted with and approved by business guarantors.

4.3.2.5 Integration Testing

This shall test mutual communication between the System modules and systems to which the System is integrated. In the Testing Environment, interface prototypes can be used instead of actual interfaces. Before the integration testing can start, the customer must ensure that test versions of all integrated systems are available in this environment. Integration testing includes the following phases:

- Technical integration testing – verifies that on the infrastructure level, it is possible to call through a given interface and transfer (any) data through it. Therefore, the testing involves especially interface settings, authorization and authentication settings, network element settings, etc.
- Business integration testing – verifies that integrated systems cooperate properly within a given business process, generate output data and process input data correctly, and properly respond to defined alternative scenarios.

Test scenarios and testing data for integration testing are built and maintained in the same way as those for functional testing. Integration testing requires intense assistance from all involved parties, including correct planning and coordination of the assistance.

4.3.2.6 Performance Testing

Objectives of performance testing include the following:

- In the Implementation phase, continuously test the performance of the System in the course of development.
- In the Performance test phase, test the behaviour of the System as a whole (i.e. all of its modules) under load, i.e. measure response times of most frequently used screens and services under workload, using the data matching the actual production operation as closely as possible.

Detailed strategy will be elaborated during the project.

4.3.2.7 High availability and disaster recovery testing

The tests verify whether the system response to a simulated failure matches the system availability and disaster recovery requirements. A detailed test scenario will be prepared during the project.

4.4 General methods and processes

Unicorn's approach of project management is systematic, managed, documented, and certified according to ISO 9001, 14001, 20000, 27001, and others.

Unicorn Approach itself is built on industry best practices, methodologies, and standards – mainly Scrum at the development team level and PRINCE2/PMI PMBOK 6th Ed. at the project management level. For ICT specifics, the sources are Rational Unified Process (SW delivery) and ITIL (for maintenance and support and other services, as well as for IT operations). Unicorn Approach is built in a way to be compliant with ISO certifications.



Standard approaches are adjusted to the situation and condition of each project in details, while basic principles remain the same.

Since Unicorn Approach is used to deliver a very broad portfolio of Unicorn's projects across technological ecosystems and industries, incl. numerous projects delivered in cooperation with other vendors and partners, our best practice is to tailor it specifically to each project.

4.4.1 Security processes and standards

Information Security Management System (ISMS) of Unicorn is based on international standard ISO/IEC 27 0001. Unicorn is certified for this standard by independent authority (TUV SUD). On top of that, Unicorn applies the combination of selected best practices and methodology standards for security.

Unicorn has a broad experience from many projects which place great emphasis on security topics, including the projects for Nordic TSOs.

We use Building Security in Maturity Model (BSIMM) framework as the guidance for the overall security (not only IT systems related areas). BSIMM provides also transparent benchmarking and security scoring mechanisms for the companies. We benefit from this approach via applied mechanisms of continuous assessment and improvements in the security areas defined by the BSIMM. As one of the disciplines under BSIMM, we apply Secure Software Development Lifecycle (SSDLC) principles and practices.

We use Open Web Application Security Project (OWASP) standards to ensure that all relevant requirements are always reflected when building our systems according to the Project security level agreed with our customers.

We expect to engage the Security Officer to the project, who will be in charge of supervising the Security standards on the project.

5. Documentation

Following table summarizes all the documentation that will be provided in related project phases and tracks. More details can be found in related chapter of Project Plan.

User Guide (and texts in the system) will be available in English and Lithuanian. Other project and system documentation will be available in English.

Phase / Track	Documentation
Project Start-up	<ul style="list-style-type: none"> · Pre-Design <ul style="list-style-type: none"> ○ Initial study <ul style="list-style-type: none"> □ incl. High-level Design of solution ○ Requirement traceability matrix · Product Backlog · System Implementation Plan <ul style="list-style-type: none"> ○ Incl. Preliminary Sprint Plan, showing how User Stories are planned to be delivered in allotted sprints · Draft of QA and Test Strategy, preliminary Test Plan, definition of acceptance criteria · Risk list · Definition of customer environment(s) (the envs. are built during this phase) · Templates for documentation produced in delivery Stages 1 and 2
Solution track Design track	<ul style="list-style-type: none"> · Design Documentation (Technical Specification) <ul style="list-style-type: none"> ○ Solution Architecture ○ Detailed Design <ul style="list-style-type: none"> □ Business Process Analysis □ User Stories <ul style="list-style-type: none"> · Incl. the Definition of done (acceptance criteria for each User story). □ Interface definition □ Non-Functional Requirement Analysis □ Data Model · Test Scenarios · Updated Product Backlog
Implementation track	<ul style="list-style-type: none"> · Updated Product Backlog · User Stories (AS-BUILT state documentation) · Administration manual (Application administration and System administration) · User Guide (for end users) · Disaster recovery plan · Integration manual (description of webservices) · Test Results · Sprint, Module, Stage acceptance protocols (acceptance-transfer act)
Whole project - Project Management	<ul style="list-style-type: none"> · Master project schedule · Weekly Status Report, incl. Weekly status call minutes

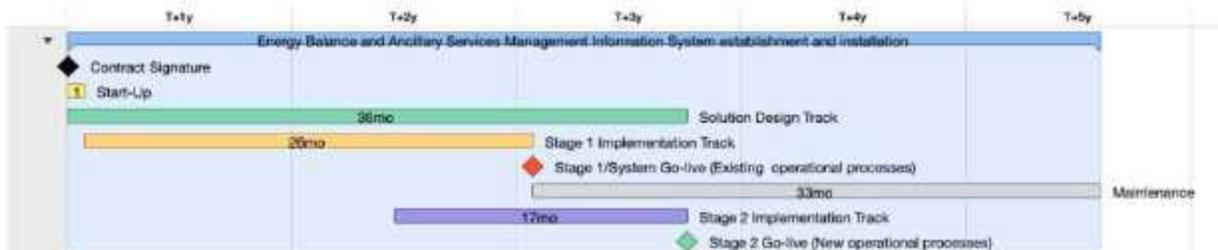


	<ul style="list-style-type: none">· Steering Committee slide deck + meeting minutes· Meeting minutes· Risklog· Changelog
Maintenance phase	<ul style="list-style-type: none">· Weekly Status Report + Weekly status call minutes· Monthly Service Report· Meeting minutes·

6. Project plan

Based on our experience, we propose to split the delivery of the solution into 4 main phases:

- Project Start-up
- Project Construction
- Continuous Customer Testing
- Warranty Support



This project plan reflects and respects expected timeline of the implementation as defined in *Annex 1 BMS Plan*. It will be finetuned during Startup phase of the project.

In order to deliver the System based on the described approach and provided time frame, the following key assumptions have been made:

- There will be no scope changes against the current tender knowledge during the implementation, or the changes will fit into initially allocated change budget and time constraints (I.e. using contingency that will be incorporated in the project schedule) – otherwise the plan will be re-evaluated or overall scope revised.
- Customer has sufficient working capacity to execute acceptance tests for 3 parallel workstreams (3 scrum teams) within 3 working days + retest fixes of Critical issues in 1 working day
- There is not planned any dedicated migration of historical data as it is not requested within the tender inputs
- The Customer is responsible for any cooperation, services, and deliverables provided by third parties (market participants, other suppliers participating in the project, etc.).
- The Customer is responsible for providing all necessary information in the agreed time. Provided information will be complete, consistent, accurate, and current.
- The Customer is expected to make any required decisions concerning the project without unnecessary delay.
- The Customer will allocate sufficient capacity and expertise for active participation. It is expected that the Business and Technical Product roles will be taken on by the Customer.
- The Customer will actively participate in all meetings during both Solution Design (Analytical calls) and Implementation Track (I.e. Sprint Planning, Review, Daily Stand-up).
- The Customer will actively provide feedback on the new version after its release in the implementation Sprint.
- The Customer will accept outputs from the Solution Description Track continuously, throughout the stage. It is expected that the acceptance will be completed for each User Story after its analysis and revision. Only accepted User Stories can be moved from the Product Backlog to the Sprint Backlog and only accepted User Stories will be implemented by the Supplier. All of this will be done based on the priorities defined in the Product Backlog.

- The list of deliverables may be subject of revision and update upon agreement.
- The scope of the project (i.e. requirements) and the coverage is managed in the Requirements Traceability Matrix (RTM). The Supplier implements the solution according to the requirements (based on the RTM).
- The Customer is responsible for consolidation and incorporation of feedback/comments provided by various Customer's representatives to Unicorn's outputs (documents, testing scenarios, etc.) during the acceptance/review procedure.
- The Customer shall provide test data examples in the same structure and containing a representative data sample.
- The Customer is responsible for the deliverables of the 3rd parties, for their cooperation/participation during system integration tests and for creation of the integration environment.
- It is expected that the Project Plan will be evaluated no later than upon the acceptance of the Project Start-up phase.
- The same assumptions apply to the whole project; however, the list of assumptions may be updated and/or extended during the Project Start-up phase or a later project phase.
- The Customer is responsible for reimbursement of travel expenses for business trips. Indicative costs will be submitted for approval prior to each business trip.

Phase	Relative time start	Duration	Note
Project Start-up	T	1 month	Start-up phase will be initiated by Contract signature and Project kick-off meeting.
Solution Design	T	Whole project	Continuous design work in parallel with implementation.
Implementation	Stage 1: T+1 month Stage 2: T+19months	Stage 1: 26 months Stage 2: 17 months	Stages overlap – Stage 2 works can start sooner thanks to availability of 3 rd scrum team
Production Delivery (Go-Live)	Stage 1: T+27 months (existing operational processes) Stage 2: T+36 months (new operational processes)		There is no migration of historical data included
Start of Maintenance	T+27months	Until end of contract	

We state our compliance with the split of modules/goals to Stages, as listed below This plan will be adapted based on detailed analysis of LitGrid requirements during the project start-up.

Stage 1

Modules:

- Main components of the System
- System configuration and administration
- Balance planning module
- Settlement module
- Balancing module

- EIC processes
- Balancing capacity auction
- Configuration and administration of the System
- Guarantee processes
- System go-live

Stage 2

Modules:

- aFRR balancing energy processes
- Integration with MARI platform
- Ancillary service management processes
- Upgrading accounting processes in accordance with grid f Continental Europe requirements
- Data transmission monitoring and control tools
- Integrating the balance capacity market
- Integrating with Picasso platform
- Backlog completion

6.1 Start-up

This project phase prepares groundwork for the rest of the project. The goals of the project are set, requirements are specified in the detail and then decomposed and mapped to the outputs, the concept of the solution and the constraints are set up and agreed with the Customer.

6.1.1 Outputs

The main outputs of start-up phase are:

- **Project kickoff** – teams on both Customer and Supplier get acquainted, communication channels are setup, regular meetings are scheduled and started.
- **Pre-Design: Initial study** – Defines the scope of the project. All functional and non-functional requirements shall be structured, evaluated, and explained between the Customer and Supplier during the project start-up phase. The goal is to have common view on the solution that is going to be delivered. Considers all aspects of the solution (i.e. is a feasibility study) and includes **High-level design** of solution.
- **Requirement traceability matrix (RTM).**
- Prepare initial **Product Backlog** by identifying User Stories covering RTM. Each user story will be given T-Shirt estimate based on assumed complexity of the Implementation
- **System Implementation Plan** – prepare Preliminary Sprint Plan, showing how User Stories are planned to be delivered in allotted sprints,
- **Draft of Test strategy and test plan**, definition of acceptance criteria,
- Initial **Risk log** and **Risk Management Strategy**, with mitigation plan for known risks

- **Agreed deployment strategy**
- Agreement on the Templates for documentation produced in delivery Stages 1 and 2
- **During start-up, design for initial 2 sprints needs to be defined and approved**
- Draft of test strategy and test plan, definition of acceptance criteria

- **Unicorn development and test environments** - Unicorn will prepare internal development environment on their premises during the start-up project phase.
- **Definition of customer environment** – Sizing, configuration, and third-party software. We expect that two main environments will be needed.
- **Customer test environment – Acceptance** – this environment will be used for deployment of already accepted user stories and will be used for acceptance testing. Infrastructure needs to be ready and accessible to Unicorn by 2nd week of the project, to allow for installation for the rest of Start-up + development part of first sprint
- This environment presumably will become the *production environment after successful acceptance tests*

6.2 Construction

Construction will be based on the agile approach describe in chapter 4.1 Dual Track Agile Approach.

6.2.1 Solution description track

6.2.1.1 Outputs

The main output of this phase is design which will contain:

- Business Process Analysis – detailed analyses of business processes.
- User Stories – detailed specifications of all user stories (that shall be implemented) with all parameters (mentioned above).
- Non-Functional Requirement Analysis – the detailed technical design covering non-functional requirements.
- Project Backlog (Refinement) – continuous management of the Project Backlog containing all User Stories with their prioritization.
- Solution Architecture – detailed infrastructure specifications and environments.
- Data Model – a detailed data model of the System.

6.2.1.2 User Stories

Each User Story planned and designed within the Solution Design must contain at least:

- User's activities and the objectives of these activities
- Activities are described step-by-step allowing its realization within a sprint
- User story contains clear criteria for acceptance (Definition of done)
- The User story is as far as possible independent of the other User Stories to smooth start next sprint realization
- It contains Customer's necessary actions for the successful realization of the sprint
- It is possible to demonstrate the result to the Customer and Customer is able to accept the Sprint. I.e. it contains Test Scenarios and test data (where applicable)

6.2.2 Implementation track

The Development phase consists of multiple separate sprints, each targeted to the delivery of a new application version (i.e. Release). The delivery scope within each sprint/version targets first the elimination of any technological risks and then the most important functional features, so that the application is available for functional testing of its core functionality as soon as possible.

6.2.2.1 Sprint planning

Sprint planning flows from priority-order Product Backlog. Priority is set by the Product Owner (LitGrid), nevertheless it should reflect not only business priority (value), but also related risks (due to use case complexity, (un)clarity, having open points) as well as relation of the user story to integration with other systems (in LitGrid or esp. when integrating 3rd party testing), potential impacts to performance or security of the solution.

The implemented solution will be continuously tested and integrated to ensure the high quality of its final version and ensuring that any problem is identified as soon as possible, so an action can be taken. New version of application will be deployed to Test environment for sprint demo in each sprint for LitGrid to be able to test the outputs. New version for the application for Test deployment will be prepared as full set of the software package including all configuration files and components necessary for the system installation.

6.2.2.2 Sprint (acceptance) testing

As part of each sprint, the Customer shall carry out a sprint test against acceptance criteria set out in the User stories included in the sprint. As long as critical errors (priority 1 or 2) have not been prevented, the particular user story shall be considered as not delivered and the delivery and acceptance form shall not be signed. Priority 3 and 4 errors identified during the sprint testing are documented in the backlog and must be corrected until the acceptance test after the last sprint.

Customer's System Test should not take longer than 3 working days. If the Test takes longer, the deadline of the last sprint is prolonged for the number of working days delayed.

6.2.2.3 Sprint acceptance

Sprint acceptance tests will be considered as successful if there are no critical errors (priority 1 and 2, ie. A1 and A2, see below). The remaining errors of priorities 3, 4 shall not affect the acceptance of the basic parts of the system. In the event of such errors, they will be scheduled as future sprint(s) work.

6.2.2.4 Integration Tests

Integration with other system needs to be tested – for LitGrid systems this might or might not be possible during the course of sprint testing. With 3rd party tests we assume this will not be possible and integration tests will have to be scheduled, prepared, and executed outside of sprints. This will be discussed and an approach will be agreed during the project startup phase.

6.2.2.5 Non-functional Tests

Usually after all the sprints are successfully finished, the factory acceptance tests executed covering the whole scope of solution. Main responsibility is on Unicorn side and whole functionality is tested and stabilised for delivery into Acceptance tests.

During this testing sprint all implemented User stories are tested based on their definition of done (functional tests). Other tests such as security or performance (see QA chapter of this Proposal) need to be executed. Since a period of testing for the complete solution (before Stage 1 or 2 go live) is not foreseen by LitGrid, Test Strategy in light of this will be discussed and agreed on during project start-up phase, as not to exclude any of the indispensable testing areas.

6.2.3 Defects management

During the whole testing (during and after sprints), all findings will be reported within the JIRA tool provided by Unicorn. This ticket management system will be used as main tool for reporting, tracking and evaluation.

The priority of the errors is determined by party which has submitted an error ticket (registered ticket in the ticketing system). Error classification priorities are following:

- **Error priority 1 (A1) - Incident**
 - The problem causes a complete production system failure, and / or the work cannot be continued.
- **Error priority 2 (A2) - Error, which cannot be bypassed**
 - The problem in production system is caused by an internal software error or incorrect operation, causing a significant loss of possibilities. A bypass solution is unknown or not acceptable (for the client), but it is possible to proceed in a limited mode.
- **Error priority 3 (B) - Error, which can be bypassed**
 - The problem causes a minimal loss of possibilities. Impact on the system is minor / causes some inconveniences, such as manual work to restore the functioning of the system / to continue the work.
- **Error priority 4 (C) - Error, with low impact and severity (Inaccuracy)**
 - Inaccuracy. The problem does not cause losses of possibilities. Such an application is due to an internal software error or improper activity whose impact on the continuation of the work can be ignored; error / inaccuracy in the product documentation.

Defects detected during sprint tests or acceptance tests (Hardware, Software, Database or Configuration) must be fixed in the Claim management system in a time proportional to the time spent for acceptance testing but no longer than three weeks.

6.2.4 Outputs

The main outputs of construction phase are:

- **Design documentation (Technical design)** – Detail design will be delivered as a set of User Stories for all functional and non-functional requirements. These user stories will be used as a basis for test cases for both Supplier and Customer tests. Part of User Story definition will be the definition of done (acceptance criteria for each User Story). Based on these acceptance criteria the delivery of User story can be approved.
- **Product Backlog** – the list of User Stories stored within the Jira system (provided by Unicorn). Based on refinement of items in the backlog will be prepared the scope for next sprint.
- **Test Cases** - represents test scenarios/cases based on the Detailed Design and on Solution Description outputs
- **Test Data** - represents the data created during sprints
- **Documentation** – we expect following set of documentation
 - Administration manual (Application administration and System administration)
 - User Guide (for application viewer)
 - Disaster recovery plan
 - Integration manual (description of webservices)
 - Installation manual
- **Source codes of the specific part of the solution**
- **Installation package** which includes all necessary components and configuration files
- **Risk list** with mitigation plan

6.3 Customer testing

6.3.1 Acceptance tests

Usually after the factory acceptance tests are finished, the user acceptance tests start. From the principle of the agile approach, customer should get functional and tested solution which should cover the customer expectations. The Acceptance tests period can therefore be relatively short because there is testable version available after each delivered sprint.

Progress of testing is tracked and evaluated within the Jira tool, which is used also for defects management.

A period of testing for the complete solution (before Stage 1 or 2 go live) is not foreseen by LitGrid – test strategy in light of this will be discussed and agreed on during project start-up phase, as not to exclude any of the testing areas above.

6.4 Warranty Support – Guarantee and Maintenance Services

Warranty [Maintenance] support starts with Go-Live. Unicorn maintenance team specialists are involved couple months before Go-Live in actual development and testing of the solution, as part of knowhow transfer.

Following chapter describes Unicorn's provisioning of Guarantee, Maintenance and Support Services. The description is not intended to be a detailed Maintenance Plan. Rather it should give a clear insight to our M&S process.

6.4.1 Introduction

Unicorn successfully delivers dozens of projects every year in many European countries, designed both for their national environments and to support the international cooperation. We provide efficient SLA based IT support and operation services for energy transmission, generation, and trading on liberalized markets as well as in technical solutions for real-time grid control. In the energy industry, our solutions are used by Regional Coordination Centres (RSCs), Transmission System Operators (TSOs), Distribution System Operators (DSOs), Power Exchanges (PXs) and Market Operators (MOs), as well as by all other types of players, all around Europe.

Our Helpdesk operates 24x7 processing calls, e-mails and tickets in English.

We often cooperate with our partners and other vendors, covering the support as the main point of contact for our customer.

Our internal methodology ("Unicorn Approach") is detailed, thorough, well-documented and supported by appropriate IT tools. We apply industry-standard methodologies such as ITIL, PRINCE2, Scrum and IBM RUP, combine them with our own experiences and best practices and take them into much higher level of detail, making Unicorn a real "software factory", capable of delivering dozens of projects simultaneously in an efficient manner with minimum risks.

Our approach has been proven in many international European projects not only in energy and utilities, and its quality was confirmed by ISO certifications 9001:2000, 10006, 14001, 20000, and 27001. All key support personnel also hold ITIL certifications.

IT service management compliant with ITIL principles and recommendations, certified by ISO 20000, will be used for the System support. In the area of system maintenance & support, it comprises namely:

- Separation of development and support teams.
- Providing support to users of the system with guaranteed SLs (Service Levels).
- Regular quality assessment of SLA performance and user satisfaction.
- Effective and fast help when solving incidents and problems.
- A thorough knowledge base about past problems and their solutions.

- Separating knowledge from individuals in order to decrease the personnel-related risks.
- Fast solution of new problems thanks to a direct link to the 2nd- and 3rd-Line Support.

The support team of our specialists has all the knowledge and background necessary for the identification, analysis, and resolution of problems. Besides non-standard tasks, it is also ready to deal with small changes and adjustments which do not have a major impact on the solution architecture any main business processes. As part of the support, we also create many statistics according to the client's requirements and contributing to the constant improvement of the service quality. We also solve any and all non-standard requirements regarding the supported solution, such as migration to a higher database version etc. Number of operational incidents is kept low through proper resolution of incurred problems, thorough root cause analysis, effective prevention, regular check-ups, and optimum usage of existing equipment.

Specific project know-how is stored in our knowledge base, it is shared with our customer, and it will be continuously maintained by and shared among the teams concerned with the delivered system.

Before the support and maintenance phase is initiated, the know-how is transferred in a managed way from the development team to the independent maintenance team, and this process is repeated with each new version. This approach ensures further know-how distribution and further mitigation of know-how loss risk.

All issues identified by users, though reported via any communication channel, are recorded to our issue tracking system (JIRA – jira.unicorn.com). We differentiate the following basic issue types: Incidents, Problems, Service Requests and Change Requests. Until agreed otherwise, the classification of the customer is applied. For each issue type, a specific process is defined. The basic workflows for each type of issue include the following phases: Issue monitoring & review, Issue identification, Issue analysis, Issue evaluation and Action implementation.

We fulfil the requirements described in the non-functional requirements.

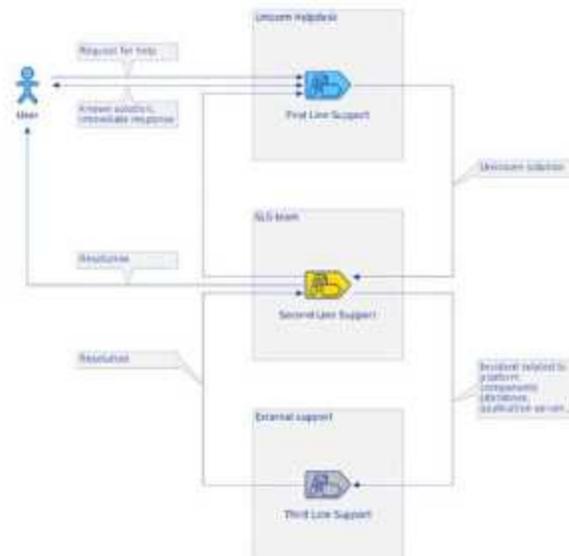
6.4.2 Maintenance and Support Services

The main responsibility of Maintenance and Support team will be to keep the System in operational conditions and up to date.

Unicorn will provide the following post go-live services:

- Unicorn Helpdesk - a service that will be used for issues escalation by LitGrid end users. It will be the SPOC (Single Point Of Contact) for incident reporting to Unicorn.
- System Maintenance and Support (2nd Line Support)
- Damas MMS Maintenance and Support (3rd Line Support)

Given services will be provided under the following scheme:



1. The **1st Line Support** (helpdesk). It receives inputs from users and provides solutions to known problems.
2. If the helpdesk cannot handle given issue (solution is not known, which means that such solution must be analysed, designed, implemented and tested), it is handed over to the **2nd Line Support** - this is a major part of the M&S service from supplier point of view. 2nd level support is usually provided by Unicorn under 24x7x365 mode including the Hotline service (2nd level support has several goals – it prevents the occurrence of the issues (Preventive Maintenance), resolves Incidents (Incident Management) and Problems (Problem Management), and hands over Issues to the 3rd Level Support in case the issues resolution requires the in-depth knowledge of used SW products. Closer description of these processes is available below. 2nd Level Support also provides SPOC for Customer and is responsible for overall alignment of all services provided to Customer.
3. The **3rd Party Support** solves incidents related to the used products (including Damas platform incidents).

6.4.3 Support issues handling

All identified issues should be reported by phone, email or by creating an entry in JIRA (incident management/issue tracking system provided by the Supplier). If the issue is not reported directly to JIRA, our M&S will record the issue by themselves.

As part of the maintenance setup, processes surrounding Customer's incident management system (as per PVR-18) and Supplier's incident management information system (as per PVR-20) will be clarified and mutually agreed. The main point of focus is to eliminate potential for delays or missed reports.

We differentiate the following basic issue types: Incidents / Problems / Service Requests / Change Requests. For each issue type, a specific process is defined. The basic workflows for each type of issue include the following phases: Issue monitoring & review / Issue identification / Issue analysis / Issue evaluation / Action implementation.

For each project, a Maintenance plan is prepared. It is a document which defines the methodology for maintenance activities, project organization, procedures applicable for maintenance of the System and their frequency. Maintenance plan is a part of Maintenance and Support documentation.

6.4.3.1 Incident Management

The goal of the Incident Management process is to restore standard service operation as quickly as possible and minimize the adverse impact of the incident on business operations, without necessarily identifying or resolving the underlying cause of the incidents.

An Incident is defined as an unplanned interruption of normal operation (deviation from expected service levels). Incident Management is the process for dealing with all incidents, including failures reported by users, by technical staff or automatically detected and reported by monitoring tools. Least but not last, Incident Management ensures continuous status or progress reporting in a timely manner, escalation procedure execution and if necessary, evaluation of incident reports. Incident management will be ensured by 2nd line support under responsibility of Unicorn.



Any issue reported by LitGrid or external users which are not an operational incident of the System or not a bug (malfunction) in our delivered solution is outside scope of incident management process (considered as Service Request, Change Request, etc.). The goal for the Second-line support (SLS) is to respond with a defined SLA.



When the correction of the bug is prepared in a release, it is deployed on the test environment first. LitGrid representatives are notified about the fixed problems and change requests via release notes. The corrections will be retested by LitGrid. After successful tests on the test environment, the release is deployed on the production environment and the JIRA ticket is closed. The reporters of the incidents are notified by Unicorn about the release of the correction.

6.4.3.2 Problem Management

The goal of Problem Management Process is to identify and to resolve the root causes of incidents and thus reduce the number of incidents in the future. The problem management process minimizes the number and severity of

incidents and problems and documents the problem to become available for the support as "Known error". The proactive approach identifies and resolves problems before incidents occur.



The term "problem" refers to the unknown underlying cause of one or more incidents. "Known error" is a problem that is successfully diagnosed and for which either a work-around or a permanent resolution has been identified. Resulting changes can be an input for Change & Release Management. Problem management will be ensured by 2nd level support under responsibility of Unicorn.

The Second Line Support identifies through **Preventive maintenance** any recurring issues or suspicious trends in the solution behaviour which may lead to the occurrence of incidents and tracks their problem management lifecycle in the ticketing system. A Problem describes an adverse situation indicating the still unknown cause of one or more existing or potential incidents. There should be a linkage between the problem, related incidents, and requests for change if any. The Second Line Support analyses on regular basis monitoring outputs and suspicious events in the scope of **Problem Identification**. They should do a first basic analysis and quote complexity to continue with **Problem Investigation and Diagnosis**. If incidents occur rarely or have little impact, assigning resources to perform **Root-Cause Analysis** and removal can't be justified. Therefore, further investigation and diagnosis will be performed on Time and Material basis after approval by LitGrid.

The activities in the Problem Management process are divided into two phases. The main objective of Problem Control is to turn problems into Known Problems so that Error Control can propose the relevant solutions:

- **Problem Control:** phase in which the Problem is defined, recorded, classified, and analyzed. This phase is completed by defining a Known Problem as soon as the root cause has been found.
- **Error Control:** phase in which is decided if the cause of the Problem will be taken away, the cause is taken away effectively (applying the Change and Release Management process), the solution is checked with the User and the Problem is closed.

6.4.3.3 Preventive maintenance

Preventive maintenance means services dedicated to the prevention of potential incidents in the operation of the delivered system and its components, in particular through consolidation of incident reporting, investigation of possible connections between incidents, investigation of root causes of incidents, issuance and promotion of best practices towards application end-users.

As a part of the preventive maintenance, Unicorn team also monitors components in the system and immediately inform the Customer about occurrence of any non-standard situations or issues.

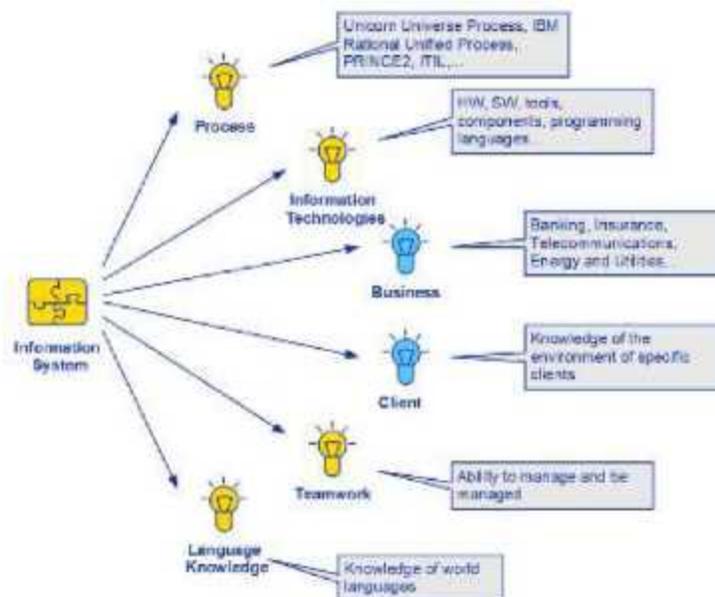
Preventive maintenance comprises also regular updates of the system, its components and underlying infrastructure, cleansing of the system, checking of logs and other regular activities. Deployment of patches and versions is done according to the Patching strategy.

6.4.3.4 Knowledge Management

We do cover the knowledge management typically as part of the problem management to reduce cases when users try to solve the same problem in isolation. The knowledge base is administrated in our online portal and can be accessible for Customer if requested.

Knowledge management is performed according to Unicorn internal methodology (Unicorn approach). It addresses the 5+1 fundamental areas related directly to the team knowledge which are necessary for successful

delivery of IT services. According to this methodology, in order to deliver a high-quality service, teams have to master the following disciplines: implementation process, information and communication technology, business issues, the customer's standards and environment, and teamwork (the ability to manage and be managed), plus language skills.



Unicorn specialists are trained to handle the process, the information technology, the teamwork, and the language skills, but they need to gain also deep knowledge of its business and client areas. This knowledge is actively acquired during take over to the maintenance and then maintained. Specific know-how, which is obtained during takeover, is stored in the project knowledge base and is further maintained by and shared among maintenance, development, and application management.

From the project know-how perspective, it is ensured that the project-specific knowledge is not held by a single project member. This is assured through the following principles:

- The project know-how is well documented and kept up to date, so it can be easily found in project documentation at any time, if needed.
- Tasks in each team is distributed in accordance with the knowledge distribution throughout the project team.
- When new members are added to the team, the already allocated senior resources are responsible for their smooth introduction to the project in order to maximize the efficiency of work and to balance the distribution of know-how
- Implementation projects are separated from maintenance projects, and the same applies to project teams
 - When the maintenance of a system starts, the know-how is transferred from the implementation team to the maintenance team. This, along with other aspects, ensures further know-how distribution and further mitigation of know-how loss risk.

6.4.3.5 Request Management

Within the service requests, Unicorn will handle everything what is mutually agreed and accepted. That usually means:

- **User Support:** A request for a user support, information, consultancy or additional documentation.
- **Standard Service:** predefined procedure (may be part of service catalogue), to be executed by support team without any additional approval. A standard service/change is a pre-authorized action that is low risk, relatively common and follows a procedure or work instruction.

6.4.3.6 Change & Release Management

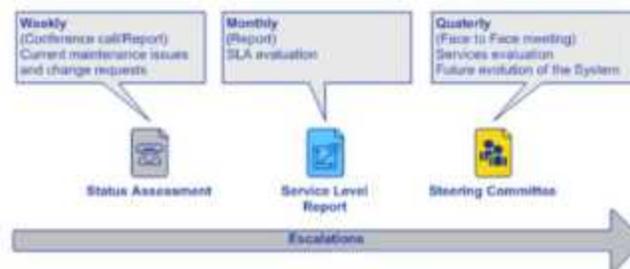
All changes will be registered and handled regardless of their type in the JIRA ticketing system. It provides in a simple way a consolidated information about the nature of each change and the impact assessment of the change, including an indication of all affected (maintenance/project) versions, components, and 3rd party systems. Moreover, it provides the possibility to easily manage workflow and categorize target versions. All relevant information is recorded and traceable anytime. For complex changes, it provides the entire overview of the impacted systems or components including environments. This is a proven collaboration approach, which can be easily adjusted and tailored, based on project requirements. It supports the logical change request decision process by means of automated workflows and via transparent assignment of physical persons into project roles. All activities of users are tracked in the audit log with history evidence. It also supports team collaboration and communication while sending notification about important events related to respective change. Change management will be ensured by 2nd line support under responsibility of Unicorn.

6.4.3.7 Inventory (Configuration Management)

Configuration Management (CM) provides necessary background for Release Management process and product/project governance. CM verifies that a system performs as intended and is identified and documented in sufficient detail to support its projected life cycle. The CM process facilitates orderly management of system information and system changes for such beneficial purposes as to revise capability, improve performance, reliability or maintainability. Configuration items will be stored in CMDB in order to be available and accessible during entire project lifecycle.

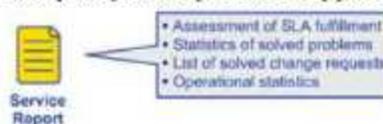
6.4.3.8 Reporting

Regular service meetings and reports will be carried out during the project. Regular service meetings and reports will be provided. We will provide a regular weekly Status Assessment on current maintenance issues, change requests, and incidents according to JIRA. The Status Assessment will be in the form of a conference call or teleconference.



As all incidents and problems are tracked in JIRA, the Customer can monitor the progress of problem solving also in "real time". This is the case also for monitoring, which continuously reports status of the system.

The SLA parameters are monitored throughout the entire life-cycle of the service, and their fulfilment is assessed on regular monthly basis. Customer receives the Maintenance Service Report based on which he can assess the quality and level of the services provided. The Service Report is one of the key outputs of the support service. For the Customer, it serves as the proof of the quality of the provided support.



Structure of the Report will be built using our standard template and reviewed / adjusted to Customer requirements before system is going live. It primarily contains the assessment of the SLA parameters and documents in detail the activities performed within the service during previous period:

- Regular assessment of service execution, it provides all insights related to the service as a whole and to each component of the service.
- SLA fulfilment and breaches including response and resolution times.
- A number of tickets per category, including top categories.
- Major incidents and problems.
- List of improvements.
- Risk list and mitigation actions.
- Continual service improvement and the service trends review.

6.4.3.9 Backup and Restore

Backup and Restore procedure be well-documented and tested as part of the delivery and then maintained by the maintenance team in order to allow restoration with the defined data lost. The procedure is regularly tested and maintained.

6.4.3.10 Disaster Recovery

Disaster Recovery plan and procedure are provided and tested as part of the delivery and will include a feasible plan for Restoring the System for normal use in the event of a serious or critical Incident.

6.4.3.11 System monitoring

To be able to fulfil the goals of the M&S service, we use various monitoring tools such as:

-
-
-
-
-
-

For each project we prepare the monitoring concept. It defines what metrics are monitored / measured and what tools are used for it. Such concept will be elaborated during solution delivery of the project and further detailed during initial phases of software development, when the M&S can get familiar with first project outputs / system previews. Know-how obtained during development and transferred from development to M&S team are also important inputs to the Monitoring concept.

6.4.3.12 Release management

Unicorn develops and maintains the Change calendar for its projects. The Change calendar covers upcoming 3 months in detail and the outlook for additional 9 months. It is updated continually and will be always available to the customer. The change calendar will reflect all the circumstances such as:

- Release plan (upcoming releases)
- Maintenance plan (definition of maintenance window, planned outages...)
- Bank holidays in involved countries
- Vacations of responsible persons etc.
- Other important events (e.g. legislature changes)

Change Calendar is derived from the Maintenance plan, which defines the process of delivery of Maintenance (periodic) releases. It is amended by other types of releases – ad-hoc (hotfixes) and regular ones (minor releases from the maintenance team, major releases coming from the development team).

Change calendar is subject to review and approval by both parties.

Change calendar will be provided in the form of excel spreadsheet, which illustrates the events (delivery of a release, deployment of release to production environment...) as a timeline. Change calendar is maintained together with other documents, such as the release plan, which contains additional information such as content of the releases.

The Customer is directly involved in a definition of the scope of every release. The information about the future releases is continuously shared with in customer in the release plan. This release plan also includes the information about the upcoming versions of underlying applications and finally links them with concrete releases of System itself. The process, defined in the Maintenance plan, will be as follows:

- Release plan contains the calendar of future releases of delivered system as well as underlying applications
- Release cycle starts with a planning session where the M&S team together with the customer agree on a content of the release - Fixes, Changes or Improvements, Upgrades
- Development of the release takes usually 2 weeks, followed by 1 week of testing / bugfixing.
- After, there is 1-week standstill period. During this period, release notes are prepared. Risk assessment is performed, and deployment plan is elaborated. All these outputs are approved by the Customer, who may request its changes.
- Release is deployed to the production at the end of this period, which matches with date of regular maintenance window.
- The whole cycle takes typically one month so it is aligned e.g. with available maintenance windows

This scheme is valid namely for (so-called) Maintenance releases, which contain fixes, small enhancements and similar minor changes to the system. Such releases are the most common for the M&S project. Other types of releases are handled in the following way:

- Patches and hotfixes, which need to be deployed outside the regular release cycle / maintenance window are always produced upon request of the Customer only. Customer initiates the release based on his own decision (e.g. bug found) or based on the information provided by the M&S team e.g. as the output of problem management. Information about the release is therefore readily available to the Customer.
- Major releases, which deliver e.g. whole functional modules to the system or upgrade major system components, are developed by the development team and planned together with the maintenance team. Release cycle is longer in that case (it takes usually several months), however, the logic behind is still the same – scope is defined together with the customer, plan for his delivery and deployment is part of the release plan and is prepared and agreed together with the Customer, so all the information immediately available.

Ongoing communication between the M&S team and the Customer is crucial for the successful operation of the system. We expect to have active (daily) communication with the Customer's team by phone or through other communications channels (issue tracking system, email, video conferences, etc.). That ensures the customer is immediately informed about any circumstances related to provision of the maintenance services (including the need of a new release). The status of preparation of new versions / system releases will be subject of the regular maintenance meetings (weekly basis).

We would like to highlight, that we do not prescribe/force any mandatory releases which the Customer will be forced to install. Maintenance plan rather defines regular process of deployment of new releases, which is aligned with the release plan. Content of every release is negotiated and approved with the customer

6.4.4 New System Releases / Version control

Used development method leverages well-known continuous integration best practices, emphasizing high quality of delivery, reliable and effective deployment, and sustainable development.

In case of unexpected problems after deployment of the version to the target environment, there must exist a way how to roll-back to the previous version. Two approaches are possible in such situation - applying of a previously created backup or running a prepared rollback scripts to revert all deployed changes. The preferred approach is the usage of scripts as their application is typically easier and smoother, requiring less coordination efforts.

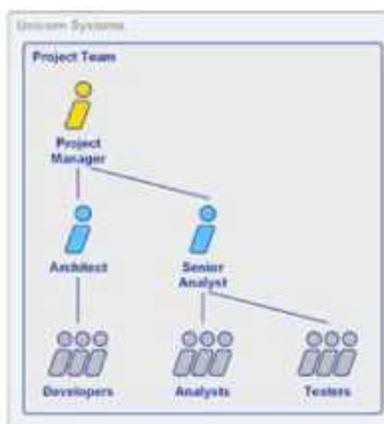
All project tasks are traced in JIRA.

Versioning of releases is described in the guideline which is maintained in project knowledge base.

6.4.5 Organization Structure

Project governance of Maintenance will be ensured by standard organisation structure. According to Unicorn approach, the services are provided by the maintenance and support team, as long-term project. The whole team is led by Project Manager (=Service Manager). Key persons at are also the SW architect and business architect/senior analyst. Next to that, there is the IT Security Manager, a person that ensures security of systems and services at a set of projects.

Project Manager reports on the project status to members of the Steering Committee (=Project Board). If there is anything that cannot be agreed on the project level, it is escalated to the Project Board. Project Manager also shares all the relevant information with project or service team members



Each icon represents a role. The roles have the following responsibilities.

Role	Description
Project Manager	Responsible for the overall quality, quantity, terms, and budget of the project. He or she manages the whole project team, especially the software architect and business architect. Project Manager reports on the project status to the client, the team, and to upper management levels
Architect	A senior developer who is responsible for the technical part of the project, defines the architecture of the software, and leads developers. He or she communicates with technical representatives from the client's side.
Senior Analyst	A senior analyst, who is responsible for the functional part of the projects, guarantees that the software satisfies the business needs, and leads analysts. He or she communicates with Business Users from the client's side
Developers	They write the code, configure the software, or solve issues assigned to them. Results of their work are reviewed by Software Architect and testers.

Role	Description
Analysts	They analyse the business needs of the client and transform them into functionalities of the software. Results of their work are reviewed by Business Architect and passed to Developers to implement
Testers	They execute test scenarios to guarantee the quality of the software. They record any identified issue in the bug tracking system

Besides the above organisation structure, there is a separate team to ensure the continuity and quality of all the services and projects provided to LitGrid- the Core Team. The Core Team consists of Delivery Manager and Cross-Project Architect(s) that participate in (potential other) projects or services provided to LitGrid and Cross-Project Business Architect(s). The team closely cooperates with LitGrid Managers to achieve its purpose. Together, they ensure the compatibility and flexibility of chosen technologies, components, or systems among them.

Project is governed by the Project Board which is represented by Delivery Manager and Account Manager on Unicorn's side. Delivery Manager is responsible for the overall quality of the project. Account Manager deals with the cash flow with the client and represents the customer's needs and requirements internally.

6.4.6 Communication Standards

To achieve good communication at all the levels, it is necessary to set up:

- Teams and cooperation between all sides
- The Core Team of experts to ensure a view and continuity of all the projects as described in Section Organization Structure;
- An organization and communication scheme with representatives from both sides on each level as described in in Section Organization Structure

The following channels are used to ensure smooth communication at all the levels:

- **Meetings** – to report on project status or discuss important business or technical topics.
- **Task and defect tracking tool (e.g. JIRA)** – to track and manage all important activities within the project.
- **Collaboration tool** – to share information and documents during the whole project lifecycle (discuss requirements, review analytic & design documents, etc.)
- **E-mail** – for daily communication and organization of meetings.
- **Ad-hoc phone calls** – to discuss urgent topics.
- **Document Management System (e.g. Plus4U)** – for knowhow sharing.

Communication between Unicorn and LitGrid is carried out by members on the same level or is escalated to the level above. Starting from the top, there are two top management levels that direct members of the Project Board or serve as escalation points in most complex cases.

Special attention is paid to the organization of meetings. Following meetings are organized, starting with the top management.

- **Steering Committee** – Delivery Managers and Account Manager of Unicorn Systems participate in the Steering Committee to monitor the quality of provided services or to solve escalations.
- **Project Physical Meeting** – ad-hoc physical meetings for important milestones e.g. project kick-off. Prepared in advance, including agenda and topics to be discussed
- **Project Status Assessment** – a weekly audio conference on the project level with shared contents. Prepared in advance, including agenda and topics to be discussed. Its output is project status.
- **Internal Project Status Assessment** – a weekly meeting of Unicorn Systems to report on the project status to members of the Project Board.
- Analyst meetings, technical meetings, defect meetings, etc.

6.4.7 SLA - Service Level Agreement

The SLA parameters define the level and scope of the service and the method of meeting the defined parameters. The SLA parameters are monitored throughout the entire time of service, and their realization is recorded and

assessed. The client regularly receives a Service Report, based on which he/she can assess the quality and level of the services provided.

Unicorn differentiates three SLA levels - [REDACTED]

The Customer is entitled to change to different service level (Higher or lower) quarterly, without any implementation costs. It is necessary to Inform Unicorn systems at least one month in advance. E.g. to change the service level for period from April to June, it is necessary to requests this no later than on 10th March.

Based on LitGrid's RFP requirements, we understood the requested services as [REDACTED]. However, we are ready to tailor the service as per specific requirements of LitGrid.

6.4.7.1 SLA specification

In line with LitGrid's non-functional requirements, we offer and commit to the following SLAs

Service parameter	Value
Base service time (BST)	8:00 to 20:00 every day, Lithuanian time Unicorn will provide the service desk function of service operation for designated employees of the Customer (hereinafter "users")
Communication language	English
System availability in BST	98%
Recovery Time Objective (RTO)	6 hours
Recovery Point Objective (RPO)	2 hours
Response time on incidents in BST	Critical: 2 working hours Other: 8 working hours
Workaround of incidents in BST	Critical: 8 working hours Other: 20 working hours for solution without program code change, 1 week otherwise
Response time on change request	1 week
Response time on consultations / training	1 week
Information sharing	<ul style="list-style-type: none"> · Phone - Dedicated phone number for First line support (Helpdesk service available during BST) · E-mail - Dedicated mail address to Unicorn maintenance team (FLS and SLS) · JIRA - will be used also as fault logging system (available 24 x 7 and 365 days in a year).
Monitoring	<ul style="list-style-type: none"> · Tools used: VMware, Zabbix · Infrastructure monitoring - network connection, database management (usage, threads, storage, ...), CPU usage, RAM utilization, storage (HDD) · 7x24 automated monitoring
Meetings	Scheme described above
SW update	Updates without outage anytime, updates which require outage in the maintenance window (planned outage).
Tasks not included in the service / not covered by SLA	Invoiced monthly in addition to the regular fee using manhour rate stated in this proposal.

Warranty support services will be provided off-site; the on-site support can be provided on demand and will be charged on Time and Material Services (TMS) basis.

6.4.7.2 Incident prioritisation

- **Error priority 1 (A1) - Major Incident = CRITICAL**
 - The problem causes a complete production system failure, and / or the work cannot be continued.
- **Error priority 2 (A2) - Error, which cannot be bypassed = CRITICAL**
 - The problem in production system is caused by an internal software error or incorrect operation, causing a significant loss of possibilities. A bypass solution is unknown or not acceptable (for the client), but it is possible to proceed in a limited mode.
- **Error priority 3 (B) - Error, which can be bypassed = OTHER**
 - The problem causes a loss of possibilities. Impact on the system is minor / causes some inconveniences, such as manual work to restore the functioning of the system / to continue the work.
- **Error priority 4 (C) - Error, with low impact and severity (Inaccuracy) = OTHER**
 - Inaccuracy. The problem does not cause losses of possibilities. Such an application is due to an internal software error or improper activity whose impact on the continuation of the work can be ignored; error / inaccuracy in the product documentation.

6.4.7.3 3rd party support

When the problem is caused by the third-party software or component (e.g. bugs in the operating system or database), we fulfil our obligations by providing a workaround which lowers the severity of the problem to Medium or Low category and by communicating with the third party. The Customer shall lead the resolution of such issues.

- The customer will be entitled to use the tools, reuse and adapt the source code for custom needs according to the open-source licensed terms, which also means free of charge.
- Customer has the possibility to engage third parties on development of the system – there is no vendor lock-in
- The Customer is also allowed to replace computation modules by a third-party modules or modify them by involving its own (or third party) resources
- Open-source approach also means that there is no exclusivity for the solution, we may reuse the source code in other projects / customers
- The Customer will not be forced to implement and deploy new versions of the system, unless he decides to

6.4.8 Damas MMS product support

As well, within the post go-live support, the Damas MMS product is continuously developed by Unicorn based both on evolving market rules and our customer's requirements.

From the maintenance perspective, the Damas MMS product support includes the following services:

- Continuous releasing of Damas MMS hot-fixes, patches and upgrades (introducing new general features, functions and configuration capabilities) including the necessary installation procedures, tools and documentation
 - Hot-fixes and patches are released ad-hoc to fix the identified critical problems and/or security issues; the customers are recommended to install them immediately.
 - Upgrades are released according to the Damas MMS product development plan.
 - Customer is obliged to install the upgrade / patch within 6 months after its release; in case of major upgrade that requires the adaptation of the business modules, this period is extended to 24 months. If the customer falls this duty, any service levels of both platform and business support are suspended, unless agreed otherwise.
 - Installation is done by the customer unless the Damas MMS operation service is contracted.

- Possibility to propose new features and improvements for Damas. Unicorn decides in which future Damas MMS release such improvement shall be included. Preferential implementation is also possible, but it requires an extra payment from the customer based on the average daily rate.
- Helpdesk in web-based bug and issue tracking system to report bugs and to propose improvements and other types of issues.
- Individual account to access the Damas platform portal (see <http://damas.unicornsyste.ms.eu>) to be informed about news and upgrades, to download the Damas documentation and new versions, to browse the Damas knowledge base, to ask questions and propose improvements etc.
- Bug fixing and resolution of operational problems of the platform (2nd line support). Product support will start with the problem resolution in time specified for each problem report category (working day means Monday-Friday with the exception of Czech national holidays):
 - Cat. A (disables the operation) – immediately
 - Cat. B (limits the operation) – within 5 working days
 - Cat. C (others) – not applicable, such problems are handled in the next regular platform upgrade
- Right to request additional services (implementation of major upgrades, consultations, development of specific components, on-site support, database optimizations and data archiving etc.)

6.5 Expected cooperation

Unicorn will need to closely cooperate with LitGrid team members to be able to successfully design and deliver the solution. The expected cooperation may differ based on the phase of the project and will be refined during the project start-up. In general, we can already expect a need for following cooperation:

- Product owner – it is necessary for a client representative to coordinate the project with us, at the very least just to ensure that we get the required assistance. Product owner shall attend regular project meetings.
- Attendance of senior management representatives at Strategic forum meetings (Steering Committee and similar).
- Business and technical know-how for the purpose of analytical workshops – business submitter, analysts, system users, etc. We expect approximately involvement of LitGrid business representative and architect at least 2 days per week. Their participation is expected in higher extent during the Initial Study. LitGrid representatives should cooperate mainly on analysis of specific requirements.
- Customer-side testing – new release is deployed to Test environment during each sprint. We expect that client verifies the outputs of every sprint and provides the necessary feedback.
- Reviews of project outputs – this includes analytical, architectural, management, and all other outputs.
- API description for the integration with external systems – LitGrid has to provide the description of all interfaces for the integration as part of design (Solution Design track, before functionality is scheduled for development = made part of Sprint Backlog)
- Access to test instance of internal and external systems – LitGrid should provide/get the access to test or mock instances of internal and external systems which should be integrated with the solution.
- Test data preparation - reasonable data set representing variations of realistic scenarios must be prepared for testing purposes.

6.5.1 Calculation Formulas and Algorithms

LitGrid is responsible for the mathematical specification of all calculation formulas and algorithms used in the System. The definition must allow translation of the rules into system designs and test scenarios.

6.5.2 Cooperation of 3rd Parties

LitGrid will ensure (procure, contract, agree with, escalate) efficient cooperation of all 3rd parties involved in the project including the following:

- Vendors and/or service providers of IT systems integrated with the System or serving as the source of data for it.
- Any other party contributing to the project (legal, accounting, facility services, ..).

Unicorn will provide necessary support to LitGrid regarding cooperation with 3rd parties.

6.5.3 Changes in Other Systems

LitGrid will ensure (procure, contract, manage the delivery) of necessary changes in systems integrated to or affected by the System if such change is required.

6.5.4 Infrastructure Preparation

LitGrid will ensure infrastructure assembling, configuration and availability latest till the Sprint 1 end of development.

6.5.5 Working Environment

LitGrid will ensure appropriate working conditions for all activities performed in LitGrid premises namely:

- Physical access to relevant premises,
- LitGrid laptops if needed to access LitGrid resources,
- sufficient number of equipped work places (chair, desk with drawers) in the same building or in walking distance,
- power supply,
- Internet connectivity allowing access to Unicorn resources and
- drinking water.

6.5.6 Communication and Collaboration

LitGrid will ensure that LitGrid project team will be able to communicate and collaborate remotely with Unicorn project team using video conferencing and other agreed communication devices and remote access to Unicorn resources (documents, data, testing systems, ..) necessary for the project.

• Expected time for cooperation

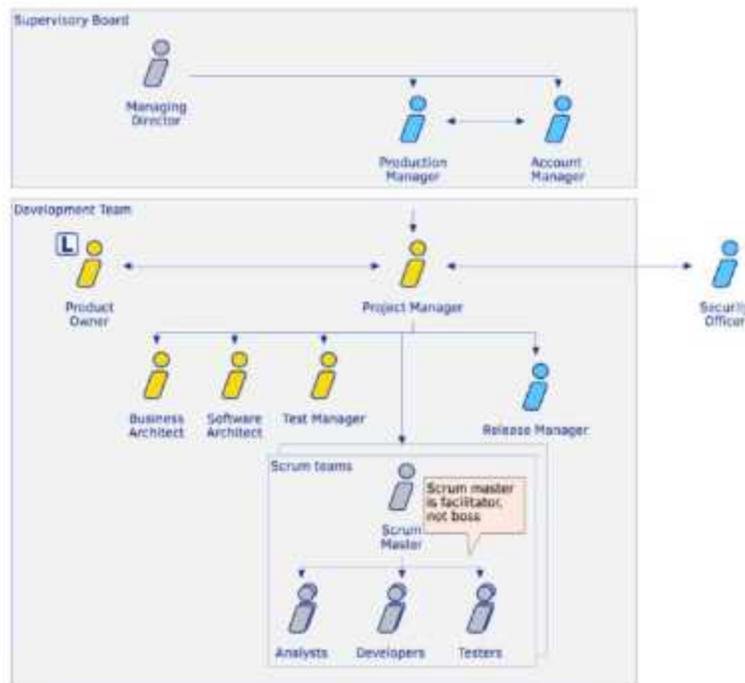
Role	Project Phase	Cooperation	MH / Week
Project Owner	Whole project	Participation on Steering Committee level meetings, decision making	~3
Project manager	Whole project	Review of management outputs Management and allocation of resources on LitGrid side, definition of priorities, coordination of interactions	~20
Product Owner = System and Process Owner	Whole project	Leading of LitGrid functional team and is responsible for the Product Backlog feeding all 3 Scrum teams	~40
Business specialists	Project start-up Construction	Review of project outputs Participation on analytical meetings. Provision of necessary business know-how for specific requirements.	~72

Role	Project Phase	Cooperation	MH / Week
		We see 3 individuals with approx. 24 hours capacity per week	
Technical specialist	Project start-up Construction	Review of project outputs Participation on technical meetings. Provision of necessary know-how for specific requirements (integrations, API, ...). Provision of LitGrid infrastructure	~16
Testers	Project start-up Construction	Preparation of test scenarios Client-side testing of sprint outputs We see 3 individuals with approx. 32 hours capacity per week	~96

7. Project management

Based on our experience we proposed the project organization described below. This structure is derived from the standard Unicorn organization and updated to fully support the agile way of the development. As the project has specific business background, which expects higher knowledge we amend the basic roles defined by the Scrum methodology (Scrum Master and Product Owner) especially by the business architect and software architect. Unicorn is ready to support all the business tasks by the experienced capacities.

We expect to involve experts that were introduced during the pre-qualification phase. However, we reserve the possibility to change them before the start of the project with similarly qualified resources.



7.1 Roles description

Role	Description
Supervisory Board	
Production Manager, Account Manager	Direct the project, supervise the project manager. Counterparts to LitGrid <i>Project Owner</i> . They both report to Managing director.
Development Team	
Product Owner	The Product Owner role is nominated by the Customer. The responsible product owner leads the Customer's functional team and is responsible for the Product Backlog. The product owner also has the responsibility for the functional architecture. The product owner will be spending most time and effort during the Requirements Analysis and Solution description until the user stories are being handed over to the construction phase. This role is held by LitGrid System and Process Owner

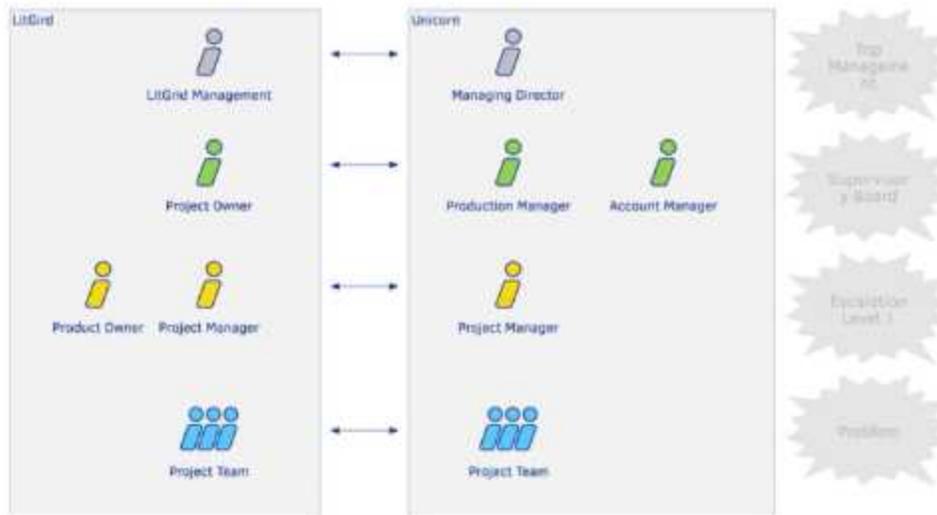
Role	Description
Project Manager	<p>The Project Manager role plans, manages and allocates resources, shapes priorities, coordinates interactions with customers and users, and keeps the project team focused. The Project Manager also establishes a set of practices that ensure the integrity and quality of project documents.</p> <p>The Project Manager role is responsible for managing activities and team leading on the project, acting as a single point of contact for the customer.</p> <p>Counterpart to LitGrid <i>Project Manager</i>.</p>
Business Architect	<p>The Business Architect role leads and coordinates requirements analysis and user stories specification closely with the customer product owner and customer functional team. One of the main responsibilities is to prepare high level estimates and help with the creating of Product Backlog and prioritization process.</p> <p>Partakes mainly in Solution Description stream.</p>
Test Manager	<p>The Test Manager role is tasked with the overall responsibility for the test planning related to each sprint and also for the planning of the overall acceptance tests. The role involves quality and test advocacy, resource planning and management of issues that impede the test effort.</p>
Software Architect	<p>The Software Architect role is responsible for the solution architecture, which includes the key technical decisions that constrain the overall design and implementation for the project.</p>
Release Manager	<p>The Release Manager role is responsible for the overall configuration of the infrastructure and environments for the product development team. The release manager cooperates with the software architect and scrum master to fully support the agile development process.</p>
Security officer	<p>The Security Officer role is responsible for independent project governance from security perspective (project compliance with security process and standards). The security officer is not a member of team and reports to Unicorn Chief Security Officer.</p>
3x Scrum team	
Scrum Master	<p>A scrum master is the facilitator for an agile development team. He is responsible for helping the team to reach consensus for what can be achieved during a specific period of time, helping the team to reach consensus during the daily scrum, helping the team to stay focused and follow the agreed-upon rules for daily scrums, removing obstacles that are impeding the team's progress and protecting the team from outside distractions.</p> <p>Scrum Master is nominated from the scrum team.</p>
Analyst	<p>The Analyst role analyses and designs user stories for defined sprint and participating on the development as metadata developer within our products under the supervision of the BA.</p>
Developer	<p>The Developer role is responsible for developing and testing components, in accordance with the project standards, for integration into larger subsystems. When special testing components, such as drivers or stubs, must be created to support testing, the developer is also responsible for developing and testing the test components and corresponding subsystems.</p>
Tester	<p>The Tester role is responsible for identifying and defining the required tests, performing the tests and monitoring of the testing progress, recording results in each test cycle and evaluating the overall quality as a result of testing activities.</p>

7.1.1 Project communication and escalation path

Tight cooperation and good communication are essential for the success of any project. The communication and escalation rules will be approved during the project kick-off and continuously fine-tuned. These rules shall cover:

- Communication and Escalation rules, including regular hierarchically oriented Strategic forums
- Strategic forum definition (stakeholders, customer representatives, vendors managers)
- Lists of the contact persons and their competencies

Following figure captures proposed communication and escalation scheme.



Highest – Top management level

Not foreseen – only for most critical issues.

Supervisory Board

Regular meetings to check project progress, approve project milestones or changes above project level tolerance. Under normal circumstances, the highest governing body of the project making decisions escalated by project managers. Comprises Project Owner on LitGrid side and Production Manager with Account Manager on Unicorn side.

Project management level

Project management level is represented by the Project Manager with Product Owner on LitGrid side and Project Manager on Unicorn Systems side. Main responsibility is to check on regular basis the project direction, risks, future planning, agile way of working and Customer satisfaction.

Project level

This level represents the daily communication between the specialist during the Solution Design and Implementation track works.

- Solution Design (Solution Description)– communication is arranged mainly between the LitGrid team represented by Product Owner and Unicorn Development Team represented by Business Architect and Software Architect.
- Implementation track – during the sprints Development Team on Unicorn side communicates on daily basis together with Product Owner and Project Team on LitGrid side.

Issues and risks that cannot be resolve on the project level are escalated to Project management level.

7.2 Project Meetings

Following meetings will be scheduled on regular basis to ensure information sharing, management and reporting during the project. Meetings with LitGrid participation are held onsite, using videoconferencing or as combination of both.

7.2.1 Project management meetings

Meeting	Periodicity	Duration	Goal	Supplier Participants	LitGrid Participants
Project kick-off	1 / project	4 hours	Presentation of upcoming Phase goals, plan and organisation Meeting of team members	All team members	All team members
Steering committee	Monthly	2 hours	Progress reporting Phase acceptance Change approval	Steering committee members Other participants if needed	Steering committee members Other participants if needed
Integration meeting / External Status assessment	Weekly	1 hour	System integration and coordination of sub-deliveries Progress assessment Risk and issue management	Integration team members	Product owner PM

7.2.2 Design meetings

Meeting	Periodicity	Duration	Goal	Supplier Participants	LitGrid Participants
Analytical meetings	1 - 2 / week	2 hours	Elaboration of User Stories	Business architects	Product owner Business Experts
Technical meetings	1 - 2 / week in Startup, ad hoc otherwise	2 hours	Solution architecture Elaboration of Technical Stories Technical test architecture	Software architect Hardware architect Security Architect	Technical Experts
Ad-hoc meetings	Ad-hoc	1 hour	Resolution of specific problems or open issues	As needed	As needed

7.2.3 Implementation Phase meetings

Note: For Sprint-related meetings, periodicity is listed per each scrum team (i.e. for 3 teams, there are 3 standups, 3 sprints plannings etc. Per each sprint)

Meeting	Periodicity	Duration	Goal	Supplier Participants	LitGrid Participants
Stand-up	Daily	15 minutes	Last day achievements Actual day plans Dependencies and obstacles to be discussed separately	All team members	N/A
Sprint planning	1 / Sprint	1 hour	Conclusion on the next Sprint backlog	All team members	Product owner
Sprint demo	1 / Sprint	2 hours	Presentation of the Sprint deliverables (increments)	All team members	All team members
Defect call	1 / Sprint	1 hour	Clarification of priority and severity of identified issues, agreement on Critical issues to be fixed (preventing Sprint acceptance)	Test Architect Business Architect Software Architect (Optional)	Product owner Technical Experts (optional)
Sprint retrospective	1 / Sprint	1 hour	Discussion of the cooperation during the last Sprint Improvement plan	All team members	All team members
Sprint Closeout	1 / Sprint	1 hour	Demonstration of fixes of Critical errors, agreement on sprint work remaining, acceptance of the sprint	All team members	All team members
Golive progress meeting	Daily during golive period	1 hours	Check of Golive procedure/checklist steps dure for the day, plan for next day, resolution of any open points and issues	All team members	All team members

7.3 Project Reporting

Project progress will be evaluated continuously.

- > For Solution Design
 - Fever Chart comparing volume of user stories designed and time elapsed
- > For implementation track:
- > Sprint Burndown Chart will be used to monitor the performance during particular sprints.
- > Following KPIs will be measured after every Sprint:
 - Sprint delivery performance (Actual delivery vs. Sprint plan)
 - Systematic lack of performance (scope not delivered) would be escalated, Supplier will present proposed solution to the Steering group.
 - Quality trend
 - Systematic increase of the number of issues above agreed level would be escalated. Supplier will present proposed solution to the Steering group for approval
- > Project Burndown Chart will be used to monitor the performance of whole delivery project.

7.4 Risk management

Unicorn is highly focused on proper management of risks, and we consider the management of risks to be one of the key pre-requisites for the success of the project. The risk management of the project shall be under the responsibility of project manager who shall be responsible for the two key documents:

Risk management plan - defines process of risk management in terms of roles, responsibilities and workflows for risk identification, analysis, and contingency planning. This plan is being setup during the project start-up phase.

Risk log – the list of all project risks and for each risk there is described a set of attributes like: ID, Name, Impact, Probability, Description and for each risk there are defined set of mitigation and contingency strategies.

As a part of project initiation, the draft of risk list is created, it is then continuously assessed and remedial actions are taken accordingly. Unicorn generally divides risks into following categories:

- Project management risks
- Business-related risks
- Technological risks

Management of risks is emphasized among other project management activities. Following principles and procedures will take place to lower the project risks to a manageable level:

- > Start-up phase outputs minimise the key project risks
- > Project governance principles ensuring good risk visibility and efficient mitigation environment
- > Information sharing and cooperation among all parties involved into the project ensure early risk identification
- > Technological risks are proactively mitigated by prototyping key solution components (Proof of Concept)
- > Scope revisions included in each project phase keep the expectations clear and stable
- > Risk mitigation measures shall be decided and approved without unnecessary delays
- > Risk management reporting on regular basis (as part of weekly project status report)

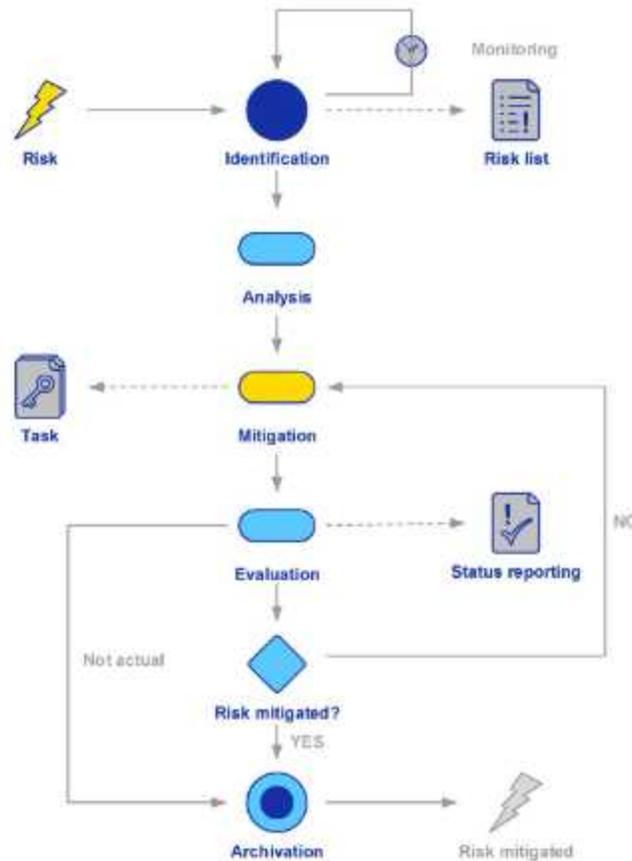
7.4.1 Risk classification

Project risks are classified according to their potential impact and probability. This classification ensures that project team effort is focused on the right things and mitigation measures are relevant to their purpose.



7.4.2 Risk Management Process

The following process ensures good management and reporting capability of actual risks and mitigation measures.



7.4.3 Main project risks

- **Lack of overall client testing and acceptance stage** – the system will be tested in parts, but no time is dedicated to testing the whole solution, esp. in light of integration with other systems (be it other LitGrid or 3rd party systems) and to acceptance (potentially with operational trial). This risk will have to be addresses early in Startup phase, as it can influence overall project approach and Test Strategy.

- **Too many changes and issues** – While the change is inevitable in any IT project and even welcomed, when it comes from users exposed to the system being built, it needs to be accommodated to in systematic manner in project with fixed deadlines and fixed price. For this purposed, contingency (schedule buffer) needs to be incorporated to the project schedule. Unicorn accepts the required split into sprints – we suggest incorporating the contingency via Preliminary Sprint Plan, allocating user stories representing full scope of delivery as of Start-up phase to first 80% of Sprints, keeping remaining 20% of sprints initially empty. Usage of contingency will be monitored - it is one of the project health metrics used by the Project Manager.
- **Tight project schedule** – wide scope of functionalities that needs to be developed. High level of cooperation and pragmatic approach is expected. All functionalities will be implemented using the simplest way fulfilling of the requirements
- **Capacity allocation** – tight project schedule also means, that there will be short time for allocation of proposed team. There is a risk, that some of the proposed specialists will not be able to join the project in expected schedule. In this case Unicorn will propose different resource with same or better experience.
- **Usage of non-standard data formats in communication** – usage of other then ENTSO-E formats will require custom modifications Damas MMS.
- **Getting feedback from users late in the project** – we encourage LitGrid to involve potential users not part of regular project /test team (also from side of market parties) as soon as possible in order to get feedback on the usability as soon as possible.
- **Missing operational trial** – we would like to suggest adding a simulation of the real operation of the system prior golive to verify that the system is ready for live operation

8. Training

Essential part of every Unicorn delivery is to prepare training materials to cover all important aspect of the delivered system. Goal of these materials is to provide necessary set of knowledge to our customer so the users on customer side are able to correctly use new information system.

Training materials are usually compiled from set of user guides as a result of the implementation phase. These user guides with examples and demonstration of the system are presented to the agreed group of users by the end of the construction phase (before the acceptance tests and production use).

Usually, this presentation can be done on-site or remotely by the videoconference system, based esp. on the pandemic situation/policies and mutual agreement.

Unicorn expects to provide trainings listed in the subchapters below. List of expected users will be agreed between customer and supplier during the implementation phase. As a part of these discussion supplier will also provide a summary of required skills for different type of user (System user and System administrator).

8.1.1 Damas MMS Platform Introduction Training

In the very beginning of the project, during the Start-up Phase, LitGrid team members will be given training covering following:

- Damas MMS Platform overview and architecture
 - User interface components and usage principles
 - Relevant shared functionalities of the system
 - User authentication and management
 - Logging
 - Message monitoring
 - ...
- Available Functional components
- Business modules to be used for the System
- Damas Development approach
- Basic Design and Development techniques

Goal of this training is to prepare the team to design, build, test and operate the solution according to the product based development practices. Estimated extent is 4 hours. Training materials are provided in a form of PowerPoint presentation OR demo.

8.1.2 Project Organisation Training

During the Start-up Phase, the LitGrid team members will be given training covering:

- Project organisation
 - Structure and who is who
 - Communication matrices
 - Regular meeting schedule
- Project plan
- Ticketing tool usage including the life cycles of used Ticket types

Summary of the training will be presented in the Delivery phase kick-off . Estimated extent is 2 hours. Training materials are provided in a form of PowerPoint presentation.

8.1.3 Test team training

Before the LitGrid Test team members will take part in the testing the team will be given training covering:

- Damas platform introduction (to a necessary extent given by the number of new team members and their skills)
 - User interface components and usage principles
 - Relevant shared functionalities of the system
 - User authentication and management

- Logging
- Message monitoring
- ...
- Testing Strategy and Plan
- Supportive tools and issue reporting rules

Goal of this training is preparing for smooth testing. Estimated extent is 4 hours. Training materials are provided in a form of PowerPoint presentation accompanying standard Damas MMS documentation.

8.1.4 User training - Admins, System Users

Before the Go-live operation the Operators will be given the System user training covering:

- Damas platform introduction
 - User interface components and usage principles
 - Relevant shared functionalities of the system
 - User authentication and management
 - Logging
 - Message monitoring
 - ...
- System Solution overview
- Particular functional module Business Processes (happy day and alternative scenarios)
 - Input data handling
 - Processing of auctions and predictions
 - Distribution of results
 - Reports
- Error handling

Training focused on System daily operation and usage. Goal of this training is preparing for smooth execution of all business processes. Estimated extent is 1 day. Training materials are provided in a form of PowerPoint presentation accompanying standard Damas MMS documentation, approved User Stories, User Guide.

9. System architecture

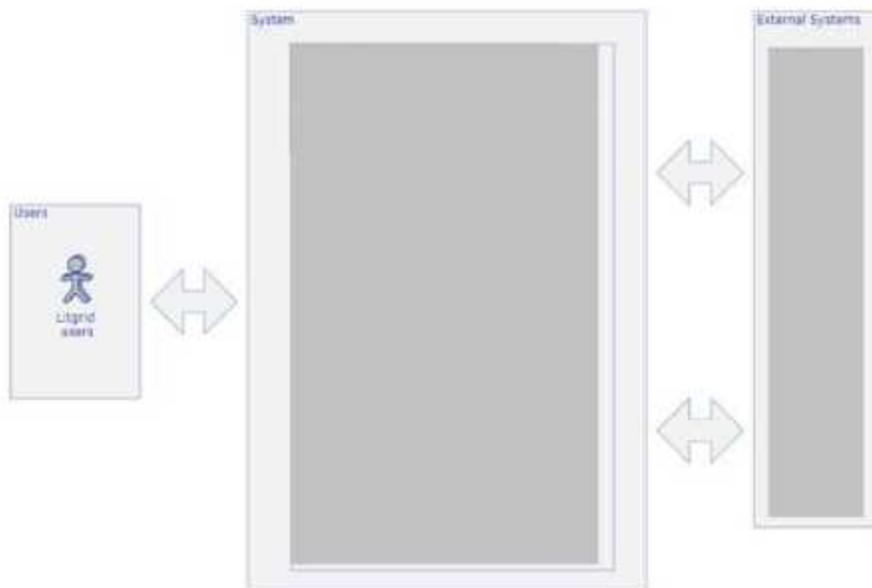
9.1 Solution overview

The proposed solution will be built on the Damas MMS platform – a commercial off-the-shelf product by Unicorn Systems designed to support business processes of transmission system operators and market operators.

Damas MMS platform was designed and developed by Unicorn's architects based on long-term experience with custom information systems development, particularly for the power industry and for TSOs. The platform employs the latest development technologies and is well-proven in large-scale installations running in production environments. The platform allows for highly productive implementations and offers exceptionally large configuration options. All parts of the platform are designed to make configuration of business processes as easy as possible.

The platform design was driven mainly by the following technological requirements: high flexibility, extensive customizability, high performance, high reliability and availability, transparency and security, and standardized interfaces with the external environment.

9.2 Logical view



Integration API

User interface

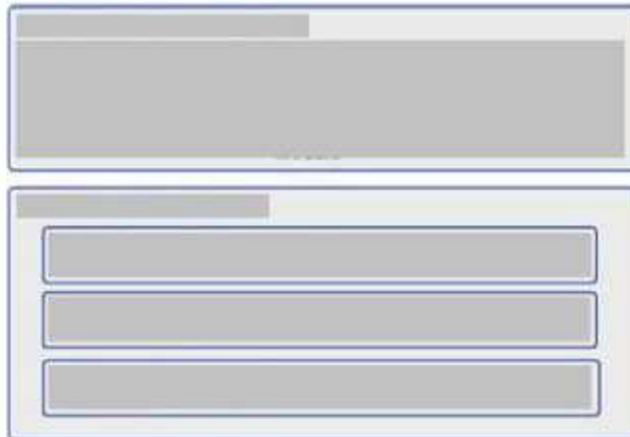
Business logic



Data & metadata



9.3 Main architectural principles



[Redacted text block]

[Redacted text line]

[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

[Redacted text block]

[Redacted text block]

9.4 Base technologies and standards

The Damas Platform is built on the following technologies:

- [Redacted list item]
- [Redacted list item]

The Damas Platform supports, among others, the following standards:

- Security

-

-

-

-

- Communication

-

-

-

- Data representation

-

-

9.5 Environments

Based on requirements and our experience from previous Damas MMS implementations, we assume the following environments will be used during development and operation of the system:

Environment	Purpose	Where deployed
DEV-development	Used by the development team to configure and customize BMS.	Unicorn premises
TST-testing	Used by the test team to perform internal system testing and integration testing.	Unicorn premises
DEMO-demonstration/ PAL-instruction / PRE-PROD-pre-production	Test environment will be used for delivery of the sprint results for customer tests and will be used for demonstrations and learning of system functionalities by Litgrid users. We propose to use this setup of environments, but we could agree on the addition of environments according to the Litgrid needs during the kick-off of the project.	Litgrid premises
PRODUCTION	Environment will be used for deployment of already accepted user stories and will be used for acceptance testing. This environment will become the production environment after successful acceptance tests.	Litgrid premises – deployed in two locations for HA and DR purposes



To minimize the risk of using an incorrect environment, the user interface of each environment uses specific configurable colour scheme. An example of such scheme for 2 environments (Test and Production) from one of the Damas MMS installations is shown in the following figure.



9.6 Infrastructure

Infrastructure is designed with respect to Litgrid non-functional requirements, requirements and typical Damas MMS infrastructure principles described in 12.20 Infrastructure.

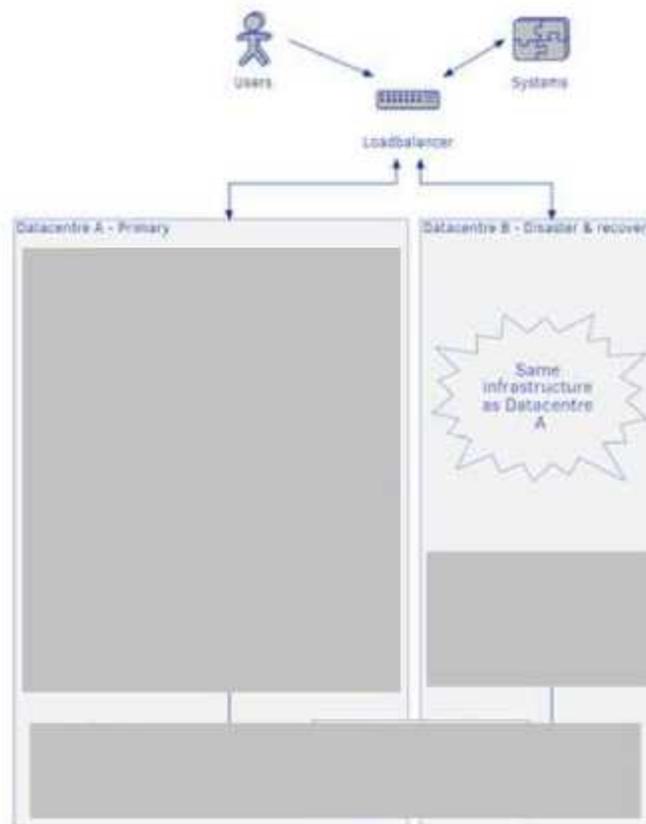
9.6.1 Deployment view

The infrastructure of a solution built over the Damas MMS Platform is designed to guarantee the required response times, availability, performance and security of the whole solution. The design of the hardware infrastructure uses load balancing with no single point of failure (SPOF) and database and application clusters.

The system will be deployed in two datacentres.

Both datacentres will act as active from application point of view, so applications can run on both datacentres simultaneously. From database point of view, primary datacentre will act as active with failover possibility. On secondary datacentre standby database will be deployed for case that primary datacentre disaster.

It is required low latency between all application servers and database. Required latency is 1 – 2 ms.



The deployment structure is based on the following key principles:

- Virtualization** - All servers are virtualized using the VMWare hypervisor technology except database servers. Database servers will be installed on physical servers. Based on our experience with already successfully implemented Damas MMS projects, we recommend usage of VMWare virtualization technology.
- Two environments** - There are 2 main environments provided (Production and Pre-Prod). The structure of all environments is the same, but non-production environment is not as powerful and redundant as the production one. For detailed numbers and server's configurations (number of machines, cores, RAM and Disk capacity), please refer to the next chapter.
- No single point of failure (reliability)** - Each element of the target deployment consists of doubled virtual (or physical - in the case of the production DB) servers to provide high availability and fault tolerance (please refer also to the next chapter). The database servers are operated in active-passive mode, all other elements are operated in active-active mode with load-balancing of incoming requests. In case of a fatal data centre failure, the operation can be switched to a secondary datacentre. For database DR see chapter and subchapters of 9.7 Data backup, restore, high availability.
- Replication of data between data centres** - The replication will be ensured utilizing the Oracle DataGuard by asynchronous redo shipping. Note: The setup of the asynchronous replication influences the RPO.
- Scalability** - The whole solution is both horizontally and vertically scalable, i.e., new virtual and/or physical servers can be added as well as existing servers' configurations can be upgraded resulting in almost linear performance increase. The only exception is the database server, which will not be operated in active-active mode, so this server can only be scaled vertically.

- **Security** – To achieve high security standard, each element is deployed to a separate VLAN so that it is isolated from all other elements by a firewall. [REDACTED]

Windows Server OS – The key technology used to implement the Damas MMS platform is [REDACTED]

Infrastructure contains following server categories:

System Modules

- **GUI portal** – includes frontend for internal Litgrid users and Damas MMS administration use cases for system administration, design with respect to "inline coding principles".
- **Sync logic servers** (backend) - Synchronous business logic servers serving front-end requests. Also includes frontend for Damas MMS administration use cases for system administration, design with respect to "inline coding principles". Responsible for execution of synchronous tasks.
- **Asynchronous business logic** servers of the following types:
 - [REDACTED]
 - [REDACTED]

Database servers – [REDACTED] database is the main system database storing all the data. [REDACTED]

Supporting servers:

- **Jump server** is used as a single-entry point to the infrastructure for administrators. For security purposes, it is not possible to access the infrastructure directly even via VPN or Litgrid internal network. Administrators must first log in to the jump server and then they can access the infrastructure from the jump server.

There is only a single jump server provided in every data centre (i.e., 2 jump servers in total).

- We assume, that each jump server can manage infrastructure of both data centres, so the jump servers are redundant when considering both data centres.
- We assume that the jump server will be configured so all relevant environments are accessible from it.
- **Logging** - Log analysis & storage server is used to gather application logs from all the virtual servers in the data centre using the technologies based on the [REDACTED]. This server is not redundant, because it is not a critical part of the infrastructure. [REDACTED]

- **Monitoring** – [REDACTED]

Storage:

- [REDACTED]
- [REDACTED]
- [REDACTED]

9.6.2 Disaster and recovery

It is general pattern, to build disaster and recovery site in geographically separated location. It solves situations where primary site or entire primary location is in disaster. Trade-off of this solution is high latency. So, the DR site works like backup of entire solution.

According to non-functional requirements, Litgrid requires IS to be operable in HA architecture. In this case, we offer to use two datacentres simultaneously, and active database server will be in primary datacentre. In secondary datacentre standby database will be installed for disaster purposes.

In case, that primary site fails, switch to secondary site in is initiated. Even that activation can be scripted, switch is manually initiated.

Hardware

Three physical servers for virtualization VMware vSphere Enterprise Plus. Two servers for production, one server for Test and supporting services. Required configuration:

Parameter	Description
CPU	
RAM	
HDD	

Two servers for Oracle Database for production active, standby and test:

Parameter	Description
CPU	
RAM	
HDD	



Two High available SAN for database servers (primary and secondary site):

Parameter	Description
CPU	
RAM	
HDD	

Storage for Logging server:

Parameter	Description
CPU	
RAM	
HDD	

Sizing note: sizing is designed according to Litgrid requirements and Unicorn experiences from other already successfully delivered Damas MMS systems. Detailed sizing (CPU, RAM, servers count, storage...), third-party software licences will be finalized during detail design phase when system real volumetrics will be clear.

9.6.3 Virtual servers

The following tables provides information about the resources hosted on the virtual servers:

Production environment – 2x – two sites (two datacentres)

Production virtual servers	Per server					Total		
	Count	Cores	RAM	HDD - OS	HDD - application	Cores	RAM	HDD

Test environment (PAL / PRE-PROD)

Test virtual servers	Per server					Total		
	Count	Cores	RAM	HDD - OS	HDD - application	Cores	RAM	HDD

Supporting servers

Test virtual servers	Per server					Total		
	Count	Cores	RAM	HDD - OS	HDD - application	Cores	RAM	HDD

9.6.4 Licences

Licences for database servers:

- [Redacted]
- [Redacted]

Licences for Application servers:

- VMware

Although the recommended licence for DB servers is

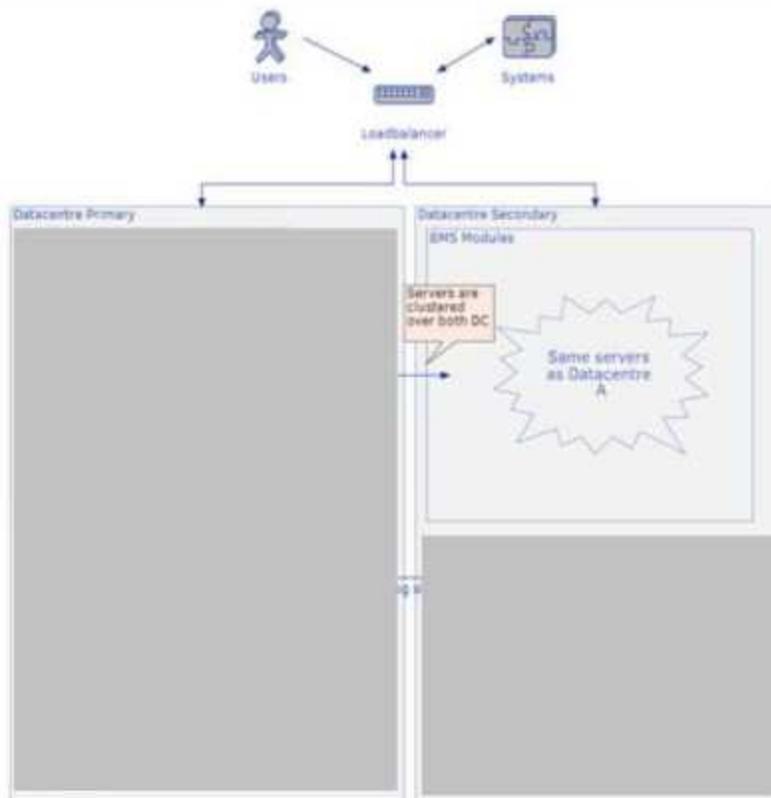
There was confirmed by Litgrid during the negotiations stage that all requested licenses will be provided in advance by Litgrid without any impact to the Unicorn costs. Due to this fact the licenses costs for the infrastructure were removed from the Annex 2 FINAL TENDER document.

9.7 Data backup, restore, high availability

9.7.1 Backup

Database backup

Database backups are performed using



We recommend using two separate backup solutions for each of the datacentres.

It is recommended to perform full database backup once per week, incremental backups daily and archive log backup continuously. This will provide the best time to recover (RTO), minimize data loss (RPO) in case a database restore is necessary, while minimizing impact on performance and required storage space.

Database backups will be kept on long-term storage solutions (such as tapes) for a predetermined period of time. will automatically keep track of backups which are necessary and will mark others as redundant. This can further optimize storage space usage with no negative impact on backup integrity.

9.7.1.1 Database backups and archiving

Additional backups of this data would then be redundant and are automatically skipped if the latest version of this part of the database is already backed up. This is one of key optimizations of backup performance and its storage requirements when the database starts growing larger over time.

9.7.1.2 Application servers

Backup the entire virtual machine. File containing virtual disk of application server can be backed up using standard tools.

- In case of failure, last snapshot of virtual machine is restored, and the virtual machine is restarted.
- No installation is necessary.
- Depending on backup frequency, only the latest logs since the last transfer to logging solution will be lost.
- Time to restore will depend just on the size of the virtual disk and speed of the storage, based on our experience the time of restoration of the snapshot ranges in minutes.

9.7.2 Database restore

The entire database or its individual parts can be restored from backup at any point in time.

Backups can also be restored to other separate databases, if required. This would allow for off-site testing, for example.

It is also recommended to keep portion of the backups locally, on storage easily accessible to the database server. This might highly increase the restore performance and availability of the backup.

Good practice is to perform regular tests of database restore in order to keep track of time-to-recover and certifying the solution's functionality and stability.

9.7.3 Database disaster recovery

The primary database is "active" and as such is used by the application servers, while the standby database is maintained synchronized. Only one of the databases can be active at any point in time, to ensure data integrity.

The role of both databases in this configuration can be switched almost immediately. The standby database would become active, and the former primary database would become standby.

If primary database becomes unavailable for any reason, the standby database becomes aware of this and assumes the role of the primary database. Application servers are then automatically reconnected and start using the former standby database. This entire operation typically takes less than a minute and causes minimal disruption.

Additionally, data changes do not need to be propagated immediately on the standby database but may instead be delayed. This is a good practice to further safeguard the database against logical or human errors. Data changes always arrive at the standby database instantly but are not immediately applied to it. If at any point, portion of data is lost at the primary database (a table is dropped by accident, for example), the replication process can simply be paused and the data safely and easily recovered from the standby database, as it effectively becomes an older copy of the primary database. The synchronization can then be resumed without any disruption to the system. This is typically much more preferable to a full-scale database restore, which would otherwise have to be performed.

The functionality of the standby database also extends to covering any physical data corruption issues. If a transaction log entry is corrupted after it is written to disk, it would have arrived on the standby in this state. The standby database then cannot apply this data change and safely discards it. This is very important as the standby

database affectively also serves the purpose of data corruption prevention. This is typically combined with similar checks on other layers as well.

9.7.4 Database high availability

The database remains highly available using optional active-passive failover and also using the same technique and set of features described in section Database Disaster Recovery cross more datacentres. It does not require any additional hardware support in other layers (such as SAN storage replication). These can however be used in combination or on top of the proposed DataGuard-based configuration to further increase resilience and availability of the system but may not be as cost-effective. Passive node can be also optimized from licences point of view.

Synchronization of both primary and standby databases is done virtually in real-time. Switching to start using the standby database instead of the designated primary typically takes less than a minute. Forward application to switched database (activated standby as primary) depends on infrastructure possibilities. But from application point of view will not exceed one hour.

Switching the roles of databases can also be done in order to perform system maintenance, hardware upgrade or any other similar planned outage on the databases.

9.8 Monitoring

To provide high availability and reliability of the software, it is important to actively prevent possible problems using high-quality infrastructure and application software monitoring.

9.8.1 Batch / asynchronous servers

A very important tool for active monitoring is the management of batch servers, integrated directly into the Damas Platform environment and available to system users with appropriate privileges. This solution provides not only functions for the monitoring of the load of individual batch servers, but also tools for an active control of running processes and for modifications of the batch cluster configuration.

An overview of the state of individual servers (called here by their logical title "execution units") is displayed in the following figure.





The standard configuration of the monitoring solution keeps track of more than 20 indicators, the most important of which are:

- Server availability
- CPU and RAM usage
- Free disk space, tablespaces space usage in DB
- Application availability
- Database availability
- Response time of the application
- Error occurrence in logs

9.9 Alignment with Non-Functional Requirements

9.9.1 Requirements for the Software and Architecture

This section describes the requirements for the System architecture, that include technological equipment and software which must ensure technological independence (may be based on open technologies or standards, i.e., the Supplier may offer equivalent technologies that meet the requirements) and functional according to the principle of 24 hours a day, 7 days a week, 365 days a year.

No.	Requirements	
NFR-1	The System must be implemented according to the architecture model of at least three levels of application (database level, application level, user interface level). The System must be able to configure and extend each of these levels individually, independently of the other levels.	<p>System is designed in 3 level architecture:</p> <ul style="list-style-type: none"> • Database • Application level (synchronous and asynchronous part) • Front End application <p>Scaling and usage of HA architecture at all individual levels of application is possible.</p> <p>Description of High Availability and no single point of failure see chapters:</p> <ul style="list-style-type: none"> • 9.6 Infrastructure • 9.6.1 Deployment view • 12.20 Infrastructure
NFR-2	The System could be based on COTS (commercial off-the-shelf), a standard configurable product. The software could be standard products or modules with elements, i. e. sold as standard licensed software and/or open architecture software with a development plan independent from individual customers, lifecycle, and support, allowing it to be developed, without help from the Supplier, by adding functionality, adapting to new organizational needs and integrating it with an integration platform or other information systems.	<p>Damas platform is a licensed product which is sold as a platform and ready-to use product with defined functionality. Extension and integration is done via usage of API and changing metadata of business logic of target system. API and metadata development is available for any system administrator.</p> <p>Also, please refer 9.1 Solution overview.</p>
NFR-3	The system must be a Web Application.	Dams MMS has web GUI. For more details, please refer chapter 9.2 Logical view.
NFR-4	The System's user interfaces must be compatible with the following browsers: <ul style="list-style-type: none"> • Google Chrome (from 86 to the latest released version prior to the initial stage of the System installation, Microsoft Windows OS); • Microsoft Edge; 	<p>GUI does not need any additional software except web browser.</p> <p>All mentioned browsers will be supported in mentioned versions up to their versions existing at the start of last implementation sprint before UATs. Modifying the solution to support later versions of browsers or</p>

	<ul style="list-style-type: none"> • Mozilla Firefox (from 82 to the latest released version prior to the initial stage of the System installation, Microsoft Windows, Apple Mac OS X, Linux OS). 	<p>other browsers will be subject of evolutive maintenance.</p> <p>For more details, please refer chapter 9.3 Main architectural principles</p>
NFR-5	<p>The System must operate on the most common Windows or LINUX operating platforms or their equivalents:</p> <ul style="list-style-type: none"> • MS Windows Server 2016 and a newer version; • Oracle Enterprise Linux 7.4 and a newer version. 	<p>Application is implemented</p> <p>System uses database, which can be deployed on MS Windows as well on Linux. For more details, please refer chapter 9.6.1 Deployment view</p>
NFR-6	<p>The System must operate on one of the following database platforms or its equivalent:</p> <ul style="list-style-type: none"> • MS SQL Server manufacturer supported version not older than 2016; • Oracle Database Server 12c and newer. 	<p>is used as a primary database by Damas MMS.</p>
NFR-7	<p>The System software must be installed on the server. No components of the System shall be installed on the user's computer (workplace), except for an additional generic software component may be installed on the user's computer if, when connecting to the System, such a software component is offered for installation which does not require the acquisition for Customer to pay usage fees of additional licences or knowledge, and if such a software component has not been previously installed.</p>	<p>Software is installed only at dedicated application and Database servers. User and external systems interact with application using Web-based GUI or application API.</p> <p>For more detailed information, see chapters:</p> <ul style="list-style-type: none"> • 9.2 Logical view • 9.3 Main architectural principles
NFR-8	<p>The logic of the System operation must be implemented on the server, the user's computer must fulfil only a graphical representation task.</p>	<p>Supported. See answer for NFR-7.</p>
NFR-9	<p>The System must have a graphical interface through which it is possible to view and perform actions with the System's functional objects,</p>	<p>Supported. See answer for NFR-7.</p>
NFR-10	<p>The System must have a possibility to implement the data layer in the form of the file system for operating systems, databases, data storages or repositories. At the data level, different data sets need to be integrated into one unified data exchange process using components at the operational logic level.</p>	<p>Supported. All system data is stored in database. Database could operate on Windows or Linux typical file systems. This allows to migrate whole data in database even between different operating systems.</p>
NFR-11	<p>The System operations in the database can only be performed through the System application layer, i.e. direct execution of SQL (Structured Query Language) commands in the database must be disabled.</p>	<p>who has access to system database and appropriate permissions could execute SQL queries.</p>

NFR-12	<p>The System components and the internal and external component integration must be implemented on the basis of the following and other SOA (Service-Oriented Architecture) principles:</p> <ul style="list-style-type: none"> • Standardized service contracts - services must be harmonized according to the same contract-interface design standards. The services must comply with a communication agreement, which must be described in one or more service descriptions and related documents; • Service loose coupling - service contracts (interfaces) must set minimum requirements for interconnection with their users, and the services themselves must be separated from the environment. Services must contain relationships that minimize dependencies and require only that they maintain an understanding of each other; • Service abstraction - service contracts must contain only essential information. Service information must be limited to what is stated in the service agreement. The internal logic of the service must be independent of information that is not described in the service contract; • Service reusability - the logic of service solutions must be independent of business processes or technology. The logic must be divided into services, encouraging their reuse; • Service autonomy - services must perform at least the basic control of their operating environment. Services must control the logic that encapsulates them; • Service statelessness - services must minimize the usage of resources. Services must postpone management of their status information upon need. Services must minimize the specific information stored for the action; • Service discoverability - services must have communication metadata assigned to them, according to which these services are possible to be efficiently located and interpreted. Services must be designed so that they can be detected using the service search tools available in the System; • Service composability - services must be effective participants of a composition, regardless of the size or complexity of that composition. When forming composite services, it must be possible to create and coordinate service sets. 	<p>Supported. Damas MMS uses Web Service API as main communication channel between internal components of the system and as a communication channel with other systems.</p> <p>Web Service module is implemented using [REDACTED]</p> <p>All required principles are supported:</p> <ul style="list-style-type: none"> • Service contracts are standardized and documented • Services are independent • Internal implementation is not available for external users • Services are reusable and discoverable
NFR-13	<p>The System must be able to support the data of several different partners (e.g. company, division, department, unit, etc.) at the same time:</p>	<p>All system data is stored in one single [REDACTED] Database. Availability of this data to all involved parties is configured in Damas MMS based on role permissions. Damas MMS provides ability to assign any number of</p>

	<ul style="list-style-type: none"> It must be possible to share the resources of individual organizational units and the data of databases of individual organizations; It must be possible to see both aggregated data for different organizational units for all organizational units and data for each organizational unit separately. 	<p>roles to given user. It is common that user has more than one role (e.g., Market Operator and System Administrator). Based on those roles, data would be available to this party.</p> <p>All necessary data would be available to users with respective roles.</p>
NFR-14	The System must be able to automatically retrieve data from Microsoft Active Directory Domain Services/Azure AD according to AD structures.	<p>Damas MMS provides the ability to authenticate against Active Directory via entering username and password as well as AD 2FA.</p> <p>For more details, please refer chapter 9.4 Base technologies and standards</p>
NFR-15	The number of data records processed in the system must not be limited, except for those limitations that result from the parameters of the virtual infrastructure and system software used.	Amount of processed data by the system is limited only by used Hardware and performance of system itself.
NFR-16	The System must have means to ensure Single Data Entry, i.e. when entering a certain data value, such as an address, it would not be possible to enter duplicate values for the same IS object, etc.	Data validation is a standard functionality of Damas MMS platform. Validation rules are defined accordingly to specific requirements and need to be negotiated during project phase.
NFR-17	The System must not contain Hard Coded data which would require the services of the Supplier in order to be adjusted and/or changed.	<p style="background-color: #cccccc; padding: 5px;">This data could be modified any time using Damas GUI.</p>
NFR-18	The System must be able to export all non-graphical collected and generated data in the specified format (Excel), or it must be possible for other systems to retrieve them for the analytical tool used.	Data View information could be exported to excel directly from GUI by user using "Export data" functionality. Any received or sent data could be exported in form of xml file. Data could be also exported to other system using Damas MMS API. More complex data export would require specific implementation.
NFR-19	The hardware and software platform specification specified by the Supplier must guarantee that when the Customer purchases the specified hardware and software platform from both the Supplier and third parties in accordance with the specified specification, the System software will meet all technical requirements, including efficiency requirements.	Unicorn offers in its proposal both HW and SW specifications which are considered as sufficient to cover all requirements in performance and reliability of future system.
NFR-20	The internal architecture of the System must be adapted to maintain the availability of the System for at least 98% of the time all year round.	<p>The system will be run 24/7, 365 day per year with availability not less than 98%.</p> <p>Please note that Damas MMS is capable of delivering availability even higher than 99.9%, as proven in existing deployments across European TSOs.</p> <p>Description of High availability and no single point of failure see chapters:</p> <ul style="list-style-type: none"> 9.6 Infrastructure 9.6.1 Deployment view

		<ul style="list-style-type: none"> 12.20 Infrastructure
NFR-21	In the event of an incident that causes the System software to be restarted (e.g., power outage, etc.), the software must run automatically without human intervention, and the data entered into the System and processed during the incident or the software configuration data must not be lost. (The requirement does not apply to data entered in the portal/account filling fields but not yet saved at the time of the incident).	<p>After unexpected restart system will be configured that all services automatically start.</p> <p>All finished transaction are immediately stored into database. System or server reboot will have impact only on currently processing data which are not yet stored into database.</p> <p>Description of High availability and no single point of failure see chapters:</p> <ul style="list-style-type: none"> 9.6 Infrastructure 9.6.1 Deployment view 12.20 Infrastructure
NFR-22	Data backup procedures must meet the requirements for System performance.	Supported. Automatic system backups would be configured to run at dedicated (agreed during project phase) time slots to minimize impact on system's performance. Strategy with full and incremental backups
NFR-23	When creating a backup or archive of the System, the transactions performed on the System must not be lost and data processed, i.e., before the backup or archive is created, all the transactions performed must be completed and the entered data must be saved.	<p>All data of the system are stored within a single [redacted] backup solution [redacted] guarantees full data integrity when performing these operations without system outage.</p> <p>Data archiving is done in bulk and in a consistent manner. Only data marked for archival are switched to read-only mode and this is done in bulk, i.e., all at the same time.</p>
NFR-24	The System's technical infrastructure architecture model, proposed by the Supplier, must be able to use a load balancing service (loadbalancer).	<p>Load balancer is supported at application layer.</p> <p>Description of High availability and no single point of failure see chapters:</p> <ul style="list-style-type: none"> 9.6 Infrastructure 9.6.1 Deployment view 12.20 Infrastructure
NFR-25	The System must be adapted to support proper physical duplication of servers, equipment clustering, and storage in at least two server repositories.	<p>Supported. Physical duplication of system components is possible and HA solution which contains two HW locations is offered.</p> <p>Description of High availability and no single point of failure see chapters:</p> <ul style="list-style-type: none"> 9.6 Infrastructure 9.6.1 Deployment view 12.20 Infrastructure
NFR-26	It must be possible to work with the System while performing other tasks, such as actions of batch tasks, registrations, user actions, except for the actions of the System Administrator, must not block the actions	Web based GUI natively support multi-user environment. Damas architecture is natively designed to support asynchronous way of work for long running and resource-dependent tasks.

	of another user and must not affect the performance of the System, etc.	Long running tasks work in background at dedicated calculation servers and do not effect on performance of other users and tasks.
NFR-27	<p>The Supplier must ensure the operation of the backup System so that the System recovery meets the following requirements:</p> <ul style="list-style-type: none"> • Recovery Time Objective (RTO) shall not exceed 6 hours; • Recovery Point Objective (RPO) shall restore data no older than 2 hours; • Data required for recovery shall be stored for 90 days when the archiving solution is not in use. <p>The Supplier should also provide recommendations on how to restore the integrity of the System data with other related systems during its downtime period.</p>	<p>We are in compliance with this requirement</p> <p>Proposed system is configured in a way that enables to meet required RTO (6 hours) and RPO (2 hours).</p> <p>[REDACTED]</p> <p>The time to recover can be optimized to a couple of minutes, while ensuring zero data loss. This also simplifies recovery of the entire system, as no additional data recovery is needed in order to restore the system's operation.</p> <p>If the disaster recovery cannot utilise the standby database (i.e., both datacenters are inoperational), restore from backups can be used instead. The time to recover would then rely completely on performance of the backup solution and the size of the database.</p> <p>The data restoration from backup is executed according to well-documented procedure.</p> <p>Data required for recovery could be stored for period of 90 days. Exact retention period would be agreed during project phase.</p> <p>[REDACTED]</p> <p>For more details, please refer chapters</p> <ul style="list-style-type: none"> • 9.7 Data backup, restore, high availability • 6.4.7 SLA - Service Level Agreement
NFR-28	The System must be able to make backup copies of all stored data both in the online and offline System, meeting the speed requirements provided by the System and without disturbing the work with the System.	<p>All data of the system are stored within a single database.</p> <p>[REDACTED]</p> <p>solution. To achieve best system performance, is used defined backup and restore strategy, which by default uses daily incremental backups and weekly full backups. Time of backups is also configured to run out of system peak hours. Time slots</p>

		and backup strategy will be clarified during project implementation phase. Such backups could be done when the system is online or offline.
NFR-29	The System must be able to set up automatic backup according to the specified frequency, the specified data storage location (logical drive, remote stations, etc.), categories of records to be copied, records, as well as perform backups of the entire System. The frequency of copying will have to be agreed during the Project implementation stage.	<p>has all necessary configurable settings to automatize backup procedure and perform easy change of configuration in case of need (for example change backups location at disk or network drive)</p> <p>See also answer for NFR-28.</p> <p>For more details, please refer chapter 9.7 Data backup, restore, high availability</p>
NFR-30	The System must be able to set an automatic backup performance schedule and frequency with the option to select (but not be limited to): <ul style="list-style-type: none"> • Backup storage location; • Remote server. 	Supported. supports wide set of configuration settings which covers required backup strategy. See also answer for NFR-29.
NFR-31	The administrators of the System must be able to initiate a procedure to restore System data from a backup. Once the data has been recovered, a solution must be in place to ensure that the integrity of the data is maintained, i.e. The System must implement measures which automatically check that the correctness and integrity of the data has been maintained during data recovery.	All data of the system are stored within a single database. Data are also always consistent upon write – this is ensured by the data are then always consistent and integrity is maintained.
NFR-32	The System must have a backup and recovery log. It must be possible to view, save and export a copy of the log to the repository and, if necessary, print the log.	which is used for backup and restore procedure always produce step-by-step log which could be analysed and printed if necessary.
NFR-33	The System must operate in the virtual infrastructure provided by the Customer. When changing the virtualization platform of the installed System, the licensing and functionality must not change, i.e. It must be possible to move the System's virtual infrastructure to any of the following virtualization platforms, and it must be possible to easily re-migrate to one of the following virtualization platforms after moving to one of the following virtualization platforms: <ul style="list-style-type: none"> • VMware; • Azure Hyper-V. 	Based on our experience with other already implemented Damas MMS systems, preferable virtualization platform is For more details, please see: <ul style="list-style-type: none"> • 9.6 Infrastructure • 9.6.1 Deployment view • 12.20 Infrastructure

NFR-34	The developed System must be harmoniously integrated into the existing information systems infrastructure and must meet high quality requirements, paying special attention to reliability and availability. All essential application operation assurance nodes must be duplicated.	Supported. System corresponds all necessary HA requirements. Please look at chapters: <ul style="list-style-type: none"> • 9.6 Infrastructure • 9.6.1 Deployment view • 12.20 Infrastructure
--------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

9.9.2 Requirements for the System's Environments

This section describes the requirements for System's environments.

No.	Requirements	
NFR-35	The System's environments (DEMO-demonstration, DEV-development, TST-testing, PAL-instruction and PROD-operating environments) must be separate from each other, the transfer of information from one environment to another must be documented and have parameterizable transfer mechanisms.	<p>Based on our experience of other already successfully implemented Damas MMS integrations, we suggest to split environments hosting between Unicorn and Litgrid premises. Dev and internal TST(TEST) we offer to host in Unicorn premises as this will speed up development</p> <p>PAL (Pre-prod) and Production environment will be hosted at Litgrid premises.</p> <p>According to our best-practice experience, at first stages of development TST(TEST) may be also used as DEMO environment. When target infrastructure and environment will be ready at Litgrid premises, PAL (Pre-Prod) environment will be used as DEMO environment. Final configuration of environments could be defined during project phase and could vary depending on actual situation. In the end all environments could be hosted at Unicorn premises or at Litgrid premises if required.</p> <p>All environments could be separated from each other based on usage of different virtual networks. Transfer of any data between environments is always done on demand and documented by release notes.</p> <p>For more detail, please see chapter 9.5 Environments.</p>
NFR-36	The System must offer a possibility for the user with the appropriate rights to set the rules for depersonalization of the System environments (based on the General Data Protection Regulation) and configure the System environment.	<p>GDPR principles are supported. Person info to be depersonalized will be agreed during project implementation stage.</p> <p>For more details, please see chapter 12.12.3 Other.</p>

NFR-37	<p>The System must have an automated process to transfer changes from one System environment to another. It must be possible to move all or part of the changes (without limitation):</p> <ul style="list-style-type: none"> • Processes; • Data; • Configuration; • Parameters. <p>The automated process must be configured with the ability to transfer changes only to the intended processes or modules.</p>	<p>Damas MMS natively designed to migrate business configuration named "Metadata" between environments. This process is automated in form of Wizard. Metadata contains:</p> <ul style="list-style-type: none"> • Processes • Configuration • Parameters • Business logic • Instance configuration <p>Data of instances could be migrated using Damas MMS user interface by export and copy-paste of necessary tabled data between environments using Damas MMS GUI.</p> <p>Full data migration could be done by cloning of database.</p>
NFR-38	<p>The Supplier must prepare all environments according to the rules, at the analysis stage, coordinated with the Customer.</p>	<p>All environments will be created and maintained according to agreement with customer during project phase.</p>
NFR-39	<p>TST and PAL environments must be able to test interfaces with other systems or systems of other participating partners.</p>	<p>Integration with other external systems will be established at all necessary Pre-Prod environments. Set of those environments will be agreed with customer during project phase.</p>

9.9.3 Requirements for User Interface and Ergonomics (Usability)

This paragraph describes the System requirements, which include user interface capabilities and ergonomics/usability. Additional functional requirements are set out in Annex No. 2 "System Configuration and Administration" and Annex No. 9 "Graphical Interfaces of the User. Common forms" of this technical specification.

No.	Requirements	
NFR-40	<p>The System must be implemented in accordance with the principles of good ergonomic practice/usability.</p>	<p>Damas MMS GUI follows proven user experience principles, so it is very easy to understand and navigate for external as well as for internal users.</p> <p>See chapter 12.7 FlexiGUI</p>
NFR-41	<p>The user interface must be informative, intuitive, ergonomic and easy to operate. Wide-spread open technologies must be used to implement the interface. Interfaces must be implemented on the basis of Web-based principles.</p>	<p>Supported. See answer for NFR-40.</p>
NFR-42	<p>The graphical user interface must support floating windows functionality that allows the user to arrange multiple graphical forms on a single screen and to resize the graphical form individually and move selected items on a Drag and Drop basis.</p>	<p>Supported. Damas MMS user interface is designed So it is natively supports different screen size of web browser.</p>

		<p>Damas MMS provides drag and drop functionality for manipulation and arrangement:</p> <ul style="list-style-type: none"> • Timeseries in views in Administration use cases • Process positions in BPM editor <p>Both use cases (Timeseries view and BPM view) are core use cases for data visualization and manipulation in system.</p> <p>See for example chapter 12.7 FlexiGUI</p>
NFR-43	<p>The System user interfaces must be error-proof:</p> <ul style="list-style-type: none"> • The System user interfaces must check the correctness of the input data logic; • The System user interfaces must help to avoid error situations and errors during data entry (for example, explanations of the data entry format shall be indicated next to data entry fields); • Error messages in the System user interfaces must be presented in such a way and with such content that they contribute qualitatively to the correction of the error (for example, the error message must indicate where the error is and how to correct it); • In the System user interfaces, an indication of errors must be provided next to the element that caused the error (for example, the fields with incorrectly entered data must be marked); • If the System can correct the errors itself, the System user interfaces should provide the following information and allow a decision to be made as to whether to use such assistance (e.g. suggestions should be provided for automatic completion of fields); • The number of actions required to correct errors recorded in the System user interfaces must be kept to a minimum. 	<p>Damas MMS provides rich functionality for automatically filling fields where possible. This is e.g., applied in forms (fields existing in database are prefilled) or filters (existing values are filled and available for choosing e.g., via whisper select).</p> <p>In case that data cannot be saved (for example due to validations) the form is by default repopulated with not-saved values. The user can then choose to return to original values if needed or manually change data and repeat the operation.</p> <p>Invalid values are highlighted in the GUI and validation errors are provided in detail.</p> <p>Validation results can be printed.</p> <p>See chapter 12.7.4 Data submitting.</p>
NFR-44	<p>The System shall ensure the correct management of errors caused by incorrect user actions. If the system user executes an incorrect (disabled) command or enters data incorrectly, the System must display the relevant messages to the user and then return to the working state.</p>	<p>The error messages and alerts always clearly describe the problem and give user sufficient information to enable him/her continuing the work.</p> <p>The validation error messages are configurable by administrator, which enables them to be further tailored to the needs of Customer.</p> <p>In case that data cannot be saved (for example due to validations) the form is by default repopulated with not-saved values. The user can then choose to return to original values if needed or manually change data and repeat the operation.</p>

		See chapter 12.7.4 Data submitting.
NFR-45	The System must support UTF8 and Lithuanian alphabet characters. The graphical interface of the System must be prepared for multilingualism - in Lithuanian and English.	<p>Damas MMS support localization and has already been localized to 6 different languages.</p> <p>English language is used in user interface by default. Lithuanian language will be prepared during project implementation phase. UTF8 and Lithuanian alphabet characters are supported.</p> <p>We strongly recommend the Customer being responsible for translation system interface texts from English to Lithuanian - this will bring two very positive outcomes: 1) the texts will be in detail reviewed by Customer 2) the Lithuanian version will be validated by a native Lithuanian speaker with deep knowledge of Litgrid business processes and therefore this will result in higher quality compared to a "common" translation by a translator with no business knowledge.</p>
NFR-46	The System must be able to change the intended user interface language without reinstalling or rebooting the System.	Supported. Language of interface for each individual user is defined in user settings and could be changed without restart of the system.
NFR-47	The System must be compatible with office package spreadsheet and text editor programmes (such as MS Excel, MS Word, or their equivalents), i.e., it must be possible to move tables provided in the user interface to spreadsheet and text editor programs.	<p>Supported. Tabled data from user interface could be copy-pasted to Excel or Word and also could be copied back if structure of rows\columns in Excel table matches structure in Damas MMS GUI table. Damas GUI is also able to export currently displayed tabled data to Excel file.</p> <p>For more details, please see chapter 12.9 Microsoft Office integration</p>
NFR-48	The System must ensure the authenticity, irreplaceability and integrity of the data entered and stored, for example, so that the same information is not entered more than once.	<p>Edited/imported data are validated according to data types and their validation rules.</p> <p>Validation rules are configurable and will be designed and configured during the system analysis stages.</p> <p>See chapter 12.7.4 Data submitting.</p>
NFR-49	The System must be able to export all non-graphical collected and generated data in the specified format	Export to BI systems of any of system data is possible via Data Flow functionality. Data for analysis could be prepared, organized and manually downloaded by users of Damas

	(Excel), or it must be possible for other systems to retrieve the analytical tool used.	MMS GUI or could be send to external systems via API. But as scope of such export is not defined, it needs to be agreed during project phase of implementation. Data exchange could be also done on database level.
NFR-50	Operations in the database layer must be performed only through the System application layer, i. e. direct execution of commands in the database must be prohibited, and the System, in order to perform these operations, must be able to automatically record the required data of the executing user and automatically fill in the fields of information related to the user (e.g. company, personal data, etc.).	Execution of SQL queries is not possible anyhow using Damas MMS application. Any action performed by user is audited and written to logs.
NFR-51	All user functions must be performed using a GUI (a graphical user interface).	Supported. Users are able to change own information. Administrators are able to manage other users via GUI.
NFR-52	The System must be able to ensure the receipt and storage of user input without losing any data of user input.	All data from user is saved to DB in transaction. This ensures integrity of user data input. In case that data cannot be saved (for example due to validations) the form is by default repopulated with not-saved values. The user can then choose to return to original values if needed or manually change data and repeat the operation. See chapter 12.7.4 Data submitting.
NFR-53	The System must be able to filter, sort, search for data in all areas of the System installation according to the selected parameters, according to the selected keywords, their fragments, keywords of individual fields and combinations of their fragments, detailing features.	Data in system are logically organized. Data views are accessible via menu. Searching in menu acts as full text search with search word completion. Own data are organized by its dimensions and by date. Searching by date is also empowered by time filter. This approach enables ability to effectively find requested data. See Damas MMS platform whitepaper, chapters: <ul style="list-style-type: none"> • 12.7 FlexiGUI • 12.4.8 Screen structure
NFR-54	The system must be able to shrink or expand the data according to hierarchical groups, e.g. the type.	Data views supports grouping, sorting, filtering by criteria and many other data manipulations. See Damas MMS platform whitepaper, chapter 12.7 FlexiGUI.
NFR-55	In the System's on-screen forms, the total data must be drilled down to their constituent values. The specific forms and fields to which this requirement	Supported. Drill down links are available in Damas MMS GUI.

	applies will be identified and agreed upon by the Supplier during the Project.	
NFR-56	The System must check that the format of the entered/imported data (e.g. date, number format) complies with the established rules and that the classifier value selected is correct. The Provider must define and validate the input fields and their verification rules at the stage of the functional requirements analysis. The System must check that the format of the entered/imported data (e.g. date, number format) complies with the established rules and that the correct classifier value is selected. The Provider must define and validate the input fields and their verification rules at the stage of their functional requirements analysis.	<p>Edited/imported data are validated according to data types and their validation rules.</p> <p>Validation rules are configurable and will be designed and configured during the system analysis stages.</p> <p>See chapter 12.7.4 Data submitting.</p>
NFR-57	The System must check the correctness of the data format at the level of data fields (e.g. the person's name must not contain numbers, etc.) and at the level of groups of data fields (e.g. the start date of the search must be earlier than the end date of the search, etc.). Prior to saving the entered data, a thorough check of the correctness of the data must be performed (e.g. checking that the data is entered in all the necessary data fields, etc.). The data fields to be checked for correctness will have to be coordinated during the implementation of the Project.	<p>The error messages and alerts always clearly describe the problem and give user sufficient information to enable him/her continuing the work.</p> <p>The validation of input data is configurable by administrator, which enables them to be further tailored to the needs of Customer.</p> <p>See chapter 12.7.4 Data submitting.</p>
NFR-58	The System must ensure that the layout of windows and fields ensures the visibility and accessibility of all relevant information on a single screen.	<p>GUI is implemented in modern technologies. GUI is flexible and responsive.</p> <p>GUI works in requested resolution in normal window as well in full screen.</p>
NFR-59	The System must ensure that any access to the functionality of the System does not require more than 4 clicks.	Supported. Data in system are logically organized and easily available in few clicks.
NFR-60	The graphical user interface and the elements of its control must be unified throughout the System.	All Damas MMS UI components are designed in same Material design and has unified logical behaviour.
NFR-61	The System users must not be able to perform the operations of creation, modification or deletion of recordings directly in the database, i. e. with the means not belonging to the System.	Execution of SQL queries is not possible anyhow using Damas MMS GUI or API. Manual data manipulation is performed via Web GUI or API.
NFR-62	The user interfaces must be personalized depending on the type of user and access rights. Functionality that is not necessary or not allowed for the user's work must not be visible. The user must be provided with the most relevant functions, messages or tasks sent to him.	Based on set of personal roles users will have access to menu and screens available just for that set of roles. E.g., Administrators will see all screens, not power users will see only subset of screens. In case of access of unauthorized resource, user will be notified by error.

NFR-63	The System must be allowed to initiate different functions by opening different windows simultaneously and without interrupting the ongoing system operations.	System / application can be opened in more browser windows simultaneously. Windows are independent so parallel work is fully supported.
NFR-64	The functionality of the automated processes in the System must be accessible to the system user through a graphical user interface. In other cases, when the data of automated processes have to be transferred to external systems, their submission must be realized using Web Services.	Damas MMS GUI provides interface to manage and monitor automatic processes in the system. Communication with external systems is performed via Web Services. Process business logic could be transferred between environments as metadata. See chapter 12.2.6 BPM (Business process management).
NFR-65	The System must be able to enlarge, reduce, change the window width/level settings and zoom the image by enlarging or reducing it at least 5 times.	GUI is implemented in modern technologies. GUI is flexible and responsive. GUI works in requested resolution in normal window as well in full screen. Zoom of images is possible by abilities of web browser.
NFR-66	The user's graphical interfaces must be designed in accordance with modern ergonomic requirements specified in the LST EN ISO 9241-210: 2019 standard, and must ensure convenient access to the main functions and operations performed by the functional parts of the System.	GUI is implemented in modern technologies. GUI is flexible and responsive.  Administrative GUI does not support in all scope because Administrative GUI is targeted to specific set of Admin users. See chapter 12.4.1 Accessibility.
NFR-67	The System must have a functioning information help function to provide help to users of the functional parts.	The context-sensitive help is provided within the application. For example, see chapter: 12.4.9 Help and context tooltips.
NFR-68	When creating the System user interfaces and processes, it must be possible to work with the help of electronic wizards (not mandatory requirement).	Administrative GUI is wizard based. For common User GUI, please refer NFR-67.
NFR-69	The graphical interface must memorize the individual user settings for the graphical interface parameters, which must be agreed during the implementation stage of the Project.	Permanent common user settings are stored in DB (e.g., user language settings). Store of some user specific interface settings (e.g., filters at views) are also supported.

9.9.4 Requirements for the System's Performance

No.	Requirements	
NFR-70	The System performance requirements for user operation: <ul style="list-style-type: none"> • The System performance must be at least: - The opening of the detailed window (with all desired objects) must not exceed 1 second; 	Supported. For requirements we guarantee required performance in 90% cases because performance measurements are highly dependent on many external dependencies:

	<ul style="list-style-type: none"> - The data storage operation after the change must not last longer than 1 second; - The presentation of the menu list to users must take no longer than 1 second; - Navigation between different windows of the System user Interface must not exceed 1 second (except when generating a report); - Navigation between different data entry fields must not exceed 1 second (except when generating a report); - The list values must not be displayed for more than 1 second. • Data search in the system, display of the search result - up to 5 (five) seconds; • Data import and assignment (e.g. the received TSO data or other information) - The System must process at least 1 MB per 1 second (all intermediate data processing, data writing to intermediate tables, etc. must be performed at the same time) ; • Generating reports - No more than 1 second to generate one simple report page and no more than 10 seconds to generate one summary report page. During the System installation project, all reports will have to be divided into simple and summary and it will be agreed which reports will be subject to this requirement. 	<ul style="list-style-type: none"> • Web browser (rendering time differs significantly on various web browsers) • Performance of client workstations • Network infrastructure (e.g. latency between DB, web server and client station) • Complexity and structure of data table. <p>We expect that the response time whenever possible is measured on server side and the measurements are gathered for the period of one week.</p> <p>Required responses for information selection (i.e. not reports) will be fulfilled for responses with up to 10000 records and no bigger than 1MB in total for all records.</p> <p>All reports will be generated asynchronously and will be available as soon as possible.</p>
NFR-71	Automatic (background, batch) tasks and actions performed by other users shall not affect the work of the System users and shall not affect the performance of the System (except in cases when, for reasons of data integrity, access to the currently processed data is blocked).	<p>The infrastructure is designed and sized in a way which covers the potential peaks in workload.</p> <p>However, to avoid such peaks, functional requirements would need to be deeply analysed to minimize potential performance downgrade situations during project phase.</p> <p>See chapters:</p> <ul style="list-style-type: none"> • 9.6 Infrastructure • 9.6.1 Deployment view • 9.6.2 Disaster and recovery
NFR-72	The System must operate in line with the performance requirements when 200 directly connected users (open sessions) will work with it at the same time.	<p>Supported.</p> <p>System can handle 200 simultaneous users. In case of performance issues solution can be scaled horizontally as well as vertically.</p> <p>Please note that for the sake of precise measurements, we expect that user makes request on average every 20s.</p>
NFR-73	The System must ensure the performance of the System specified in the requirements of this document by processing data for at least 10 years working with statistical data and at least one year working with	Supported. Offered HW and SW solution should be enough to cover required performance.

	operative, ongoing data. An example scope of the number of operations/recordings on the basis of which performance efficiency testing is to be performed is given in Clause 5.11 of this technical specification.	
NFR-74	The architecture model proposed by the Supplier must include a mechanism for the balance/load distribution between the servers.	Supported. See chapters: <ul style="list-style-type: none"> • 9.6 Infrastructure • 9.6.1 Deployment view • 9.6.2 Disaster and recovery

9.9.5 Requirements for the System's Scalability

This section describes the requirements for the System scalability, which must support the expansion of the capacity by connecting additional equipment, and the architecture must provide the possibility for the distribution of the balance/load between servers, and it must operate on the basis of a multi-layer architecture.

No.	Requirements	
NFR-75	The architecture of the System and its solution implementation must support the expansion of the technical capacity by connecting additional hardware.	In general, the system is horizontally and vertically scalable. On application layer, the horizontal scaling can be done without stopping the system by adding additional instances of given component. Vertical scaling depends on infrastructure possibilities. On database layer, vertical scaling is expected to be applied. Damas MMS however supports using separated databases for different business modules, which enables practically unlimited scalability in the future.
NFR-76	The connection of additional features to the System must be possible by installing extensions created by the Supplier or third parties.	System is divided into modules. Also, system may be extended by 3 rd party components. Such integrations must use standard Damas MMS API. In case existing set of APIs would need to be extended, it may be developed during project phase, but such work is not included into original scope of a project and need to be negotiated during implementation phase of the project.
NFR-77	The System must be designed and implemented in such a way that it is flexible for modification - after implementing changes in functionality in one or more functional areas, the changes must not be a reason for redesigning the entire System.	Supported. System design respects general principles of Low Coupling and High Cohesion on all architectural levels. The basic principles of functional architecture are described in chapter 3 General description of the system.
NFR-78	The System must be implemented in such a way that when upgrading the System to a higher version (changing/supplementing the functionality of the System) and/or changing the database, no additional work is required (except those recommended by the System Manufacturer when switching from one version of the System to another).	Regular deployment of new versions is fully automated process and require just single click action for deployment of all components of the system. Deployment package prepared by automated builds of CI-CD systems and delivered to target servers where they

		would be installed. No additional actions are needed for regular upgrades.
NFR-79	The software of the System shall not be a limiting factor in increasing the performance efficiency of the System, i.e., to increase the performance efficiency of the System, it is sufficient to add the necessary hardware without changing the source code of the System software.	Supported. Vertical increase of HW resources does not require software re-installation. Horizontal scaling will require Damas MMS component to be installed to new servers.
NFR-80	The System must encompass measures to ensure that upon introducing changes and/or upgrades to the System and/or its individual components, there is a possibility to maintain the changes and configurations made at the database level.	Supported. DB patches of application are incremental and affect only part of data\business logic they should. It means that no other data will be modified.
NFR-81	The System must be implemented in such a way that during updates related to architectural components and/or changes to the database, it is possible to migrate all data without purchasing additional services and licences from the Supplier/System Manufacturer.	Supported. No additional licences, besides listed in chapter 9.6.4 Licences would be required. System updates would include also data migration scripts, in case those would be required by new system version.
NFR-82	When a change and/or upgrade is introduced into the system, it must be possible to ensure that: <ul style="list-style-type: none"> • All stored data will be transferred to the new database structure; • Data consistency and integrity will be maintained; • No stored data will be lost; • The functionality implemented in the System will not be disturbed. 	When deploying new versions, the database structure changes and data migrations are pre-requisites of actual installation and are done via carefully tested procedure with possibility to roll-back in the case of any problems. The installation procedure is always prepared in a way which prevents any disruptions to data integrity – this is enabled by database-level constraints and extensive post-installation validations. We guarantee that no data is lost when installing or upgrading the system. Any application upgrades are first tested in production-like conditions in acceptance environment, which helps to make sure that no functionality is hindered after the upgrade.
NFR-83	Modifications, improvements and error corrections introduced into the system hardware and/or software shall not affect the integrity of previously entered data.	Supported. The system itself verifies data integrity and correctness of data by advanced validation engine, which is the integral part in input data processing. Even if e.g. screens, processes or calculation are changed, the resulting data are still the subject of validations, this safe-guarding the data consistency and integrity. Software updates does not affect on data in Damas MMS database.

NFR-84	The System must have measures to ensure that during the periodic updating of the System according to the vulnerability lists issued by the System Manufacturer, it is not necessary to install a new infrastructure, technological platform.	<p>Supported.</p> <p>The job of maintenance team just to apply security patches right after their release by manufacturer. No additional infrastructure installation should be needed for this action.</p> <p>Any found vulnerabilities are then processed by the maintenance team within standard software maintenance processes. The high-priority critical vulnerabilities are treated as incidents are applied within agreed SLAs.</p> <p>The vulnerability mitigation strategy is part of our Secure Software Development Lifecycle (SSDLC) and is automatically applied by all projects.</p>
NFR-85	Software must not be a limiting factor in increasing the performance efficiency of the System, and the increase in hardware capacity must be carried out without interrupting the operation of the System, as far as possible.	<p>System is vertically and horizontally scalable. HA architecture allows to increase performance of the system by adding new HW resources to existing servers or adding new servers into the cluster without outage of the system.</p> <p>On database layer, vertical scaling is expected to be applied. Upgrade of HW of DB cluster is possible with almost zero outage because of usage of failover cluster.</p>
NFR-86	The System balance planning process is strictly limited in time, so the extensibility of the System must ensure reliable operation of the System in line with the change in the periodicity terms (for example, by moving from 1 hour to 15 minutes or 1 minute of data exchange).	System is designed and calculated to support 15 minutes resolution. Switch to shorter periods would require re-estimation of HW resources based on new inputs and vertical or horizontal scaling of the system. Such scale will require none or close to zero outage based on which part of the system would need to be scaled.

9.9.6 Requirements for the Security and Logging

This section describes the System security requirements to enable technological measures that ensure data security, authenticity and confidentiality of stored or transmitted information and its traceability, monitoring.

No.	Requirements	
NFR-87	In the System, the communication of the users, as well as of the levels of the System architecture model, must take place only through the encrypted data transmission protocols (e.g. standard SSL/TLS, supporting not less than 2048 bytes length of key.).	Supported.

NFR-88	The System must not be able to automatically fill in sensitive and/or confidential information fields according to the beginning of the entered text, e.g. after entering the first three characters of the password the System cannot automatically fill in the remaining characters of the password.	Supported. Autocomplete sensitive information is not possible. It needs to be entered manually.
NFR-89	Passwords and other sensitive and/or confidential information cannot be stored in clear text in the System. If such information is stored, it must not be possible to decrypt it.	Passwords [redacted] and not stored in database as clear text.
NFR-90	The administrator must be able to delete the selected sensitive and/or confidential data in the System, which is not obligatory to collect/which is not necessary for further successful operation of the System (e.g. personal user information).	Not mandatory system user data of any user could be deleted by users with System Administrator user role.
NFR-91	The System must compile and store audit information on data transactions (logs) for at least 6 months. Information about data actions, users who performed data actions, dates, time records must be stored. During the Project implementation stage, the Supplier will need to coordinate what data audit information needs to be collected.	<p>Damas MMS has wide range of auditing capabilities and keeps necessary details for every logged event.</p> <p>Among information which is kept in audit log belongs:</p> <ul style="list-style-type: none"> • Date, time • User who executed the functionality • Action status • ID • Functionality/action executed • Data provided to the functionality (e.g., full XML message with data received/send via data flow) • Error code and details if relevant • Workstation IP <p>See chapter 12.21 Audit .</p> <p>Data retention period for such information could be agreed during project implementation.</p>
NFR-92	<p>The System must be able to store and save information about connections to the System:</p> <ul style="list-style-type: none"> • User names; • Login times; • Information about the computer from which you are connecting (such as the IP address); • Successful and unsuccessful access statuses; • System events (including time and date); • Session ID. <p>Detailed data fields will have to be coordinated during the Project implementation stage.</p>	Supported. Please see NFR-91.

NFR-93	<p>The System must offer a possibility to store the history of actions/audit of all actions specified in this requirement performed by a user logged in as an administrator (in the role of):</p> <ul style="list-style-type: none"> • When and which administrator logged; • Login times; • Information about the computer from which it was logged; • What administrative actions were performed; • What system configuration changes were made; • Session ID. <p>Detailed data fields will have to be agreed during the Project implementation stage.</p>	<p>Damas MMS comes with auditing component. All significant application events are automatically stored in audit log with information about the date and time when the event occurred, user who triggered it, ID of functionality which is being executed, data which is being written and more.</p> <p>The contents of audit can be viewed by user with sufficient permissions.</p> <p>Data modification history is available via historization component of Damas MMS.</p> <p>Please also see NFR-91.</p>
NFR-94	<p>The System must register and store all the information about actions with users:</p> <ul style="list-style-type: none"> • What new users were created, who created; • To which user, when and what rights were granted/revoked, which administrator/user did so; • Which users were deleted (deprived of rights); • Which users were blocked; • Session ID. <p>The detailed data fields will have to be coordinated during the Project implementation stage.</p>	<p>Damas MMS supports so called historization of data – entered values are never deleted, but rather placed in the data history. It is then possible to display value of data, which was valid at the give point of time.</p> <p>Please note, that this feature is data storage intensive and can lead to excessively large data stores. We recommend applying it only on carefully selected time series.</p> <p>See chapter 12.5 Time series engine .</p> <p>Please also see NFR-91 and NFR-93</p>
NFR-95	<p>Process auditing must be performed using a file system. Audit records can be twofold and divided into the following types:</p> <ul style="list-style-type: none"> • Event logs - logs for tracking ESB activities. Records are kept of actions taken or other events that affect the operation of the system (e.g. event "message received from system X", various error messages). Event logs are stored for 90 days. • data flow logs - where incoming, intermediate and outgoing messages are stored (e.g. request parameters, SOAP requests/responses, incoming and outgoing files, etc.). 	<p>System audit logs can be via configured adapters stored on file system in structured format.</p> <p>Logs retention period should be agreed during project implementation phase.</p> <p>Each part of the system has its own logs and also logs are grouped by logical categories (but not only below):</p> <ul style="list-style-type: none"> • Fatal • Data Bridge • Process • Algorithms • All
NFR-96	<p>The following data on the flow data must be recorded in the log records:</p> <ul style="list-style-type: none"> • System from/to which the message is received; • Date and time; • Name of the operation (action/event). <p>The essential attributes defined in the parts of the process analysis must also be recorded.</p>	<p>Supported. Required data attributes are part of every log record:</p> <ul style="list-style-type: none"> • System from/to which the message is received. • Date and time. • Name of the operation (action/event). • Detail of event

NFR-97	<p>Data flow event logs are stored in directories on the server. The common and integration module events are stored.</p> <p>All errors are logged in the event logs. System errors are recorded at the FATAL level, together with the stacktrace, and any errors are recorded at the ERROR level.</p> <p>Traffic logs must be stored on a server and cataloged according to agreed rules. It is preferred that the traffic logs for each module should be kept in a separate directory. The folder name should match the module name.</p> <p>The following information must be found in the log entries:</p> <ul style="list-style-type: none"> • Message ID; • Enquiry code; • Encoding; • Message format; • Headers; • Content of the enquiry. 	<p>Supported.</p> <p>Logs are grouped by categories to speed up investigation.</p> <p>Fatal and Data Bridge (Data flow) logs are stored at separate subfolders.</p> <p>All errors contain stack trace.</p> <p>Every message received from trusted sender will be stored into the system.</p> <p style="background-color: #cccccc; height: 20px; margin: 5px 0;"></p> <p>Please, also see answer for NFR-96.</p>
NFR-98	<p>The System user must be able to easily view the information for specific audit records (both on screen and in the report). During the System installation, the Supplier will need to agree on what information will have to be provided.</p>	<p>History logs and system even messages are available via Damas MMS GUI.</p> <p>Rest of audit information is stored in text logs which could be presented using external systems </p>
NFR-99	<p>The System must be able to protect audit records from unauthorized or unintentional modification.</p>	<p>Audit information is accessible in read-only mode so the audit trail cannot be accidentally changed.</p>
NFR-100	<p>The System administrators must be deprived of the possibility to delete or edit administrator activity logs.</p>	<p>Audit information is accessible in read-only mode so no one could change audit information, even administrators.</p>
NFR-101	<p>Each component of the System must have a separate logging configuration. Logging levels will need to be coordinated during the Project implementation stage.</p>	<p>Supported. </p> <p style="background-color: #cccccc; height: 40px; margin: 5px 0;"></p> <p>See chapter 12.21 Audit</p>
NFR-102	<p>In the System, it shall be possible for administrators to change the logging level without interrupting or otherwise affecting the uninterrupted operation of the System.</p>	<p>Historization detail level is possible to change via Damas MMS GUI by Administrator. Other parameters could be changed via modification of xml configurations.</p>
NFR-103	<p>The systemic time of all levels of the System Architecture model shall be synchronized.</p>	<p>This would be achieved using automatic time synchronization of Operating System.</p>

NFR-104	Access to the ESB must be implemented with SSL protocol with authentication using a client system certificate to ensure a high level of security (communication channel is encrypted with SSL protocol, and authentication is provided with system certificate (with public key) and private key (part of SSL protocol) .	Web service communication channel is protected by using [REDACTED] and usage [REDACTED].
NFR-105	The Supplier undertakes to provide the System with no hidden features that weaken the security, including: malware, viruses, worms, time mines, unauthorized access or features (Trojans, backdoors, easter eggs).	Delivered system features will be well documented which left no space for hidden or unwanted functionality.
NFR-106	The System must realize the possibility to automatically transfer the log records stored by the System to the information and event management solution operating in the existing Customer's infrastructure at a configurable periodicity. The decision will have to be coordinated during the Project implementation stage.	System is integrated with [REDACTED]. See chapter 9.8.2 System produces structured logs in file [REDACTED] See chapter 12.21 Audit Integration with other monitoring systems could be negotiated during the Project implementation stage.
NFR-107	The Supplier must ensure the possibility for the Customer to perform the control and inspection of the Supplier at least once a year in order to assess the organizational and technical measures of the information security applied by the Supplier.	Unicorn is working according to the highest standard of work and security. We are open to provide details per Client request.
NFR-108	The System's database must be stored in encrypted storage and it must be possible for the Customer to use its own cryptographic keys.	System database could normally run on encrypted storage in case it is required by customer security policies. However deeper analysis would be required during project phase as it is not clearly specified which technology would be used for such storage. Would it be Hardware or Software based, etc... Customer could use its own cryptographic keys.
NFR-109	Information security shall be managed in accordance with ISO 27001 and ISO 27002 (or their equivalents) information security management standards.	Supported. System is compliant with standards ISO 27001 and ISO 27002 . Please see chapter 4.4 General methods and processes. Damas MMS is state-of-the-art platform with highest focus on security. The Damas MMS platform is designed with respect to OWASP ASVS version 4.1 requirements, which are also regularly tested.

NFR-110	<p>Web applications (System) and web services must be checked by security measures without a user login:</p> <ol style="list-style-type: none"> 1. identification of the technologies used (platform, programming methods and tools); 2. Web service configuration check (change of working directory, escalation of web service rights, disclosure of information through error messages); 3. vulnerability scanning (user authentication mechanism check, session integrity check, input information processing check, program code integrity check, error message processing, system information disclosure, service configuration errors, etc.) with at least three most popular automated web vulnerability scanners; 4. manual checking of automated search results; 5. Manual vulnerability testing in accordance with all sections of the OWASP Testing Guide v4.1 methodology, not limited to OWASP Top 10 vulnerabilities. 	<p>As the OWASP Top 10 is a subset of OWASP ASVS, the high security level of the application is ensured.</p>
NFR-111	<p>Knowledge verification applications (System) and knowledge verification services must be logged in as users of legal systems:</p> <ol style="list-style-type: none"> 1. check the service configuration (change of working directory, escalation of service rights, disclosure of information through error messages, etc.); 2. verify that all types of users of information System (including remote users) are unable to extend their rights in the System, perform actions and / or obtain data unrelated to the performance of their direct duties; 3. breach detection (user authentication mechanism check, session integrity check, input information processing check, program code integrity check, error message processing, system information disclosure, service configuration errors) with at least three of the most popular automated knowledge breach scanners; 4. manual checking of automated search results; 5. OWASP Testing Guide v4.1 methodology points, not limited to OWASP Top 10 vulnerabilities. 	<p>Only authenticated and authorized users could access any functionality of the system. Extend of rights of users is available only to system administrators.</p> <p>Damas MMS is state-of-the-art platform with highest focus on security. The Damas MMS platform is designed with respect to OWASP ASVS version 4.1 requirements, which are also regularly tested.</p> <p>As the OWASP Top 10 is a subset of OWASP ASVS, the high security level of the application is ensured.</p> <p>We are prepared to share Unicorn's SSLDC guidelines with customer for further details.</p>

9.9.7 Requirements for Licences

No.	Requirements
-----	--------------

NFR-112	The software licences for the System to be purchased must be valid on a perpetual basis and their cost must be calculated from the end of full installation of the System.	All additional 3 rd party software licences are included in the financial proposal. Refer chapter 9.6.4 Licences for more details.
NFR-113	The software for System to be purchased may be licenced and have a development plan and life cycle independent of specific individual Contracting Authorities.	Licence for Damas MMS system is delivered together with the installation of Damas MMS platform. 3 rd party system components (e.g., Oracle Database) have publicly available planned development life circles which could be analysed.
NFR-114	The scope of information processed by the System shall not be limited by licences.	None of the licences limits anyhow scope of processed data.
NFR-115	The Supplier must offer a licence volume that meets all functional, non-functional and other requirements of the Customer. If in the course of the Project implementation it becomes apparent that a larger volume of licences is required to implement certain requirements, the Supplier will have to provide all the missing required licences at its own expense.	Full set of required 3 rd party licences is described in chapter 9.6.4 Licences. No other licences would be required to cover current project scope of functional and non-functional requirements. In case of significant changes in requirements in project stage which would require purchasing of additional licences, such licences should be purchased by customer.
NFR-116	The price of the proposed licences and their support must be clear for the functional scope specified at the time of submission of the proposal. The validity of the System licences must be perpetual and indefinite, without taking into account whether the software maintenance services are purchased or not.	All Damas MMS and 3 rd party licences has unlimited validity, except licences for support.
NFR-117	The application and system software licence for the System shall not contain any licencing restrictions for the integration and/or use of such software with other systems.	All Damas MMS and 3 rd party licences does not contain any restrictions which limit integration with other systems.
NFR-118	The software licences ensuring the operation of functional components of the System may not be limited to the number of users.	All 3 rd party licences does not contain any restrictions which limit system in number of users. Damas MMS license has its own conditions and limitation of users.
NFR-119	The Supplier shall assign to the Customer all proprietary rights to all software solutions offered by it and developed during the provision of the development of installation services.	All 3 rd party licences will be taken over to customer during the project implementation. Details of such take over will be negotiated between appropriate departments of Unicorn and Litgrid during implementation stage of the project. The Damas MMS non-exclusive licence will be delivered natively with the platform. For complete list of 3 rd party licences, please refer chapter: 9.6.4 Licences

9.9.8 Requirements for Integration Interfaces

No.	Requirements	
NFR-120	The data exchange presented in the other sections of this document must be implemented in the System (see Integration Components and Message Transmission).	Damas MMS Enterprise Integration component has build-in [redacted] It is possible to switch endpoints for given data flow just by configuration (matter of minutes). Endpoint support is based on plugins so new types of endpoints can be easily added.
NFR-121	The System must have a customized tool (API Gateway/orchestrator) for data import control, which allows to monitor the data import process, provide error messages and warnings, indicating the causes and locations of the error. An application programming interface (API) must be used for data transfer.	Damas MMS has well standardized API and instruments to manage data exchange and perform monitoring of possible errors.
NFR-122	The System must be able to handle import control rules, i.e., the System must support the development of API management rules, usage monitoring.	Damas MMS messaging has very wide range of data message functionalities, from simple up to very complex validations [redacted] also routing can be done with connection of data in Damas MMS database, etc.
NFR-123	The System must have solutions, protocols and interfaces for data exchange with other systems.	Damas MMS Enterprise Integration component has build-in [redacted]
NFR-124	The System must have an API-based REST or SOAP Web service architecture for integration with the information systems operated by the Customer.	Primary integration channel is [redacted] Such API is used as a common standard for exchange of the information between systems.
NFR-125	The System must implement integration functionality, which allows easy switching of data exchange channels (ECP/ EDX, WS, IMAP, etc.).	Supported. Please see NFR-120. Communication channel switch is possible to do via Damas MMS Admin GUI.
NFR-126	The System must be compatible and support hybrid interfaces between system integrations (On Cloud and On Site).	Supported. Integration with any system could be achieved using wide variety of communication channels available in Damas MMS. It does not matter where partner or current system is deployed.
NFR-127	All parts and modules of the System must be integrated with each other and reflected in the related modules without additional actions of the user (i.e. the changes introduced to classifiers or other information in one module must be reflected in other modules). The exchanges of classifiers or other data used in all parts of the System must take place in real time and inform the user about the detected changes.	All modules of delivered system respects general principles of Low Coupling and High Cohesion on all architectural levels. However, they are designed to use standing data which has a purpose to be the primary source of whole system configuration. Change of such critical information is audited and could be restored from historical values any time. Also, all critical system configuration

		changes are logged as events which could be visible for system administrators.
NFR-128	The interfaces developed and the ongoing data exchanges between the systems must be described using XML schemas, while the processes – using an UML or an equivalent standard.	Damas MMS Enterprise Integration uses Processes will be described in the project documentation
NFR-129	The System shall support secure real-time access to the process of integration events and requests (authentication, certification and other restrictions).	System provide access to all incoming and outgoing data flow messages via Damas MMS GUI. Events about data flow sending\receiving could be configured and received all interested parties based on user roles. Events are available for users with appropriate rights.
NFR-130	The System must ensure the integrity of the imported data: <ul style="list-style-type: none"> • If errors are detected in the imported data, all the data submitted not incorrectly must be imported; • If errors are detected in the imported data, no data is imported; • If errors are detected in the imported data, the correct and separately submitted erroneous data must be imported and their errors identified. Detailed data import rules will have to be agreed during the Project implementation stage.	Technical and business validations and also acceptance rules is possible to configure for each individual data flow. Rules should be agreed during project implementation phase.
NFR-131	The System must automatically check the logical correctness of the entered and imported data according to the established rules (e.g. when entering/importing information, the System must check whether such information already exists, and if it does not find it, must inform the System user about it, etc.). The rules of logical fairness will have to be coordinated and configured by the Supplier during the Project implementation stage.	Supported. Please see NFR-130.
NFR-132	The System must be compatible and support micro-service technologies and their security.	Supported. System supports integration with micro-services.
NFR-133	The System must have functionality to convert message formats between different standard formats (e.g. XLST and XPath, SOAP and REST, etc.)	Damas MMS Enterprise Integration uses
NFR-134	The Supplier must ensure that the System implements the functionality that allows the data transmission, reception and processing functions to be performed in non-consistent parallel sequences.	Supported, Damas MMS Enterprise Integration component architecture allows parallel processing.

		<p>Not all channels do not allow parallel processing by its nature. For example,</p> <p>See chapter in Enterprise integration: 12.11.2 Key features</p>
NFR-135	All the components developed or installed in the System must have documented software interfaces for integrating these components with other components.	All API interfaces has a documentation and also self-descriptive auto-generated swagger documentation.
NFR-136	The addition of new components of the API or the replacement of the existing components without changing the architecture of the components must be ensured.	Supported. In case of adding of any new API backward compatibility and architectural consistency of the system is ensured.
NFR-137	The system must be able to set the daylight saving time and change the applicable time automatically without affecting the operation of the System. The System processes and data exchange must be adapted to the smooth operation of the transition from winter time to summer time and vice versa.	Daylight saving time functionality is a part of Damas MMS system.
NFR-138	All of developed or installed components of the System shall comply with security requirements listed in clause 5.6.	Supported. Please see answers for non-functional requirements section 9.9.6 Requirements for the Security and Logging

9.9.9 Integration Components

For detail overview of interfaces, please reference chapter 11.10 Data exchange formats and interfaces.

Standards applicable to the System data exchange:

No.	Requirements	
DMR-1	Market Data Exchange Standard (MADES) [IEC 62325-503]; <ul style="list-style-type: none"> CIM IEC 62325-451 standard and all message standards in it 	Damas MMS system could exchange CIM data messages according to standard CIM IEC 62325-451.
DMR-2	ENTSO-E standards available on the ENTSO-E website (https://www.entsoe.eu/publications/edilibrary): <ul style="list-style-type: none"> ECAN standard with different versions V5R0, V6R0 and others, Settlement Process (ESP); Scheduling System (ESS); Acknowledgement Document standard with different versions V2R3, V5R1 and others; Common Grid Model Alignment (CGMA); ENTSO-E General Code Lists for Data Interchange. 	Damas MMS system could exchange data messages according to required standards.
DMR-3	Web Service Description Language.	Damas MMS webservices provide WSDL of all web service endpoints.

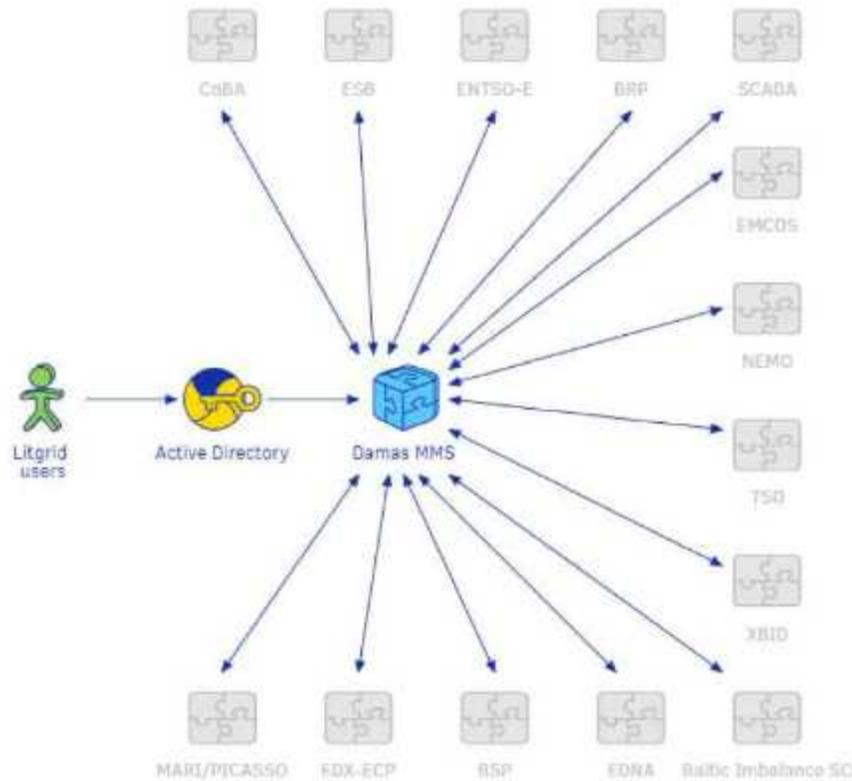
DMR-4	Open Database Connectivity (ODBC), a standardized application programming interface (API) for connecting to databases	Usage of ODBC driver is one of options to connect to DB used by the system. Damas MMS provides API to use system functionalities. Direct execution of SQL scripts is not possible via Damas MMS API.
DMR-5	Simple Mail Transfer Protocol (SMTP)	SMTP is one of the available communication channels in Damas MMS.
DMR-6	Extensible Messaging and Presence Protocol (XMPP) is an open instant messaging protocol standard	Damas MMS communication channels are implemented as plugins. XMPP protocol could be added if necessary to the list of supported protocols. Such need would be analysed during project implementation stage.
DMR-7	Business Process Execution Language (BPEL)	BPEL language is used by ESB system. Damas MMS system could be easily integrated with ESB. Damas MMS has instruments to configure data exchange based on XSLT transformations and data view presentation.

9.9.10 Integration with external systems

Future system would communicate with a lot of internal and external systems.

Damas MMS user's authentication would be done through Litgrid Active Directory. Communication between Damas MMS and other systems would be done via API using dedicated communication channels.

General overview of integrations between Damas MMS and other systems could be found below:



External IS	Details of communication	Suggested way of communication
Litgrid Active Directory	User authentication would be done via Litgrid Active directory.	
ESB	The flow of the System incoming and outgoing web services is managed through ESB.	
SCADA (optional)	Only outgoing communication.	
EMCOS	Electricity Commercial Accounting System (EMCOS). Incoming and outgoing integration.	
EDNA	Only outgoing communication.	
XBID	Incoming and outgoing communication.	
NEMO	Incoming and outgoing communication.	

TSO	Incoming and outgoing communication. By TSO is assumed communication with AST, SVK, PSE, ELERING, etc	
BRP	Incoming and outgoing communication.	
BSP	Incoming and outgoing communication.	
ENTSO-E EDX-ECP	Incoming and outgoing communication.	
Baltic COBA	Incoming and outgoing communication.	
MARI/PICASSO	Incoming and outgoing communication.	
Baltic Imbalance SC	Incoming and outgoing communication.	

9.9.11 Requirements for Testing

The following tests (trials) will have to be performed during the installation stage of the System:

1. Testing of individual modules and functions of the System.
2. Testing of IS web-service and integration with other IS or registers.
3. Functional testing of the System.
4. Regression testing of the System.

We are in compliance with this requirement – details will be agreed as part of Test Strategy preparation during project Startup phase, along with project plan elaboration.

The following reliability tests must be performed and the reports on test results must be submitted to the Customer.

No.	Test title	
PTI-1	Verifying that the backup integration server is taking over the works from the master server.	We are in compliance with this requirement – this in scope of tests described in chapter 4.3.2.7 <i>High availability and disaster recovery testing of this Proposal</i>
PTI-2	Verifying that the main server does not malfunction when the backup server is turned off.	We are in compliance with this requirement – this in scope of tests described in chapter 4.3.2.7 <i>High availability and disaster recovery testing of this Proposal</i>
PTI-3	Verifying that processes are successfully restored after disabling and restoring the System application.	We are in compliance with this requirement – this in scope of tests described in chapter 4.3.2.7 <i>High availability and disaster recovery testing of this Proposal</i>

PTI-4	When ESB is disabled on both servers, data is no longer transferred. Work will continue once the ESB is activated.	We are in compliance with this requirement – this in scope of tests described in chapter 4.3.2.7 <i>High availability and disaster recovery testing of this Proposal</i>
PTW-1	Verifying whether the System processes are running without a GUI.	We are in compliance with this requirement – this in scope of tests described in chapter 4.3.2.7 <i>High availability and disaster recovery testing of this Proposal</i>
PTW-2	Verifying that GUI request balancing works without including idle servers.	We are in compliance with this requirement – this in scope of tests described in chapter 4.3.2.7 <i>High availability and disaster recovery testing of this Proposal</i> , as well as in chapter 4.3.2.6 <i>Performance Testing</i>
PTD-1	Verifying the system performance in case of DB restart.	We are in compliance with this requirement – this in scope of tests described in chapter 4.3.2.7 <i>High availability and disaster recovery testing of this Proposal</i>
PTD-2	Verifying the System operation in case of DB failure.	We are in compliance with this requirement – this in scope of tests described in chapter 4.3.2.7 <i>High availability and disaster recovery testing of this Proposal</i>
PTR-1	Testing DB recovery from backup.	We are in compliance with this requirement – this in scope of tests described in chapter 4.3.2.7 <i>High availability and disaster recovery testing of this Proposal</i>
PTR-2	Testing INT server recovery from backup.	We are in compliance with this requirement – this in scope of tests described in chapter 4.3.2.7 <i>High availability and disaster recovery testing of this Proposal</i>
PTR-3	Testing WEB server recovery from backup.	We are in compliance with this requirement – this in scope of tests described in chapter 4.3.2.7 <i>High availability and disaster recovery testing of this Proposal</i>
AT-1	Processing of large numbers of received messages.	We are in compliance with this requirement – this in scope of tests described in chapter 4.3.2.6 <i>Performance Testing of this Proposal</i>
AT-2	Processing of large-scale messages.	We are in compliance with this requirement – this in scope of tests described in chapter 4.3.2.6 <i>Performance Testing of this Proposal</i>
AT-3	Testing the performance of several selected processes with increasing volume.	We are in compliance with this requirement – this in scope of tests described in chapter 4.3.2.6 <i>Performance Testing of this Proposal</i>

AT-4	Verifying the performance of the Internal System calculations.	We are in compliance with this requirement – this in scope of tests described in chapter 4.3.2.6 <i>Performance Testing</i> of this Proposal
AT-5	Verifying the performance of the selected GUI forms of the System.	We are in compliance with this requirement – this in scope of tests described in chapter 4.3.2.6 <i>Performance Testing</i> of this Proposal

There must be at least two types of testing carried out to verify the System, I. e. The Internal testing and The Acceptance Testing.

We are in compliance with the requirements outlined in the table below. For more information see chapters 4.3 Quality Assurance, in general chapter 4. Implementation approach, as well as chapter 6. Project plan of this Proposal.

Type of testing	Responsibilities	
	The Supplier's responsibilities	The Customer's responsibilities
Internal testing	<ol style="list-style-type: none"> 1. Prepares testing scenarios and the testing plan. 2. Configures the environment required for testing. 3. Prepares the testing data. 4. Performs testing. 5. Eliminates errors identified during testing. 6. Prepares testing reports. 	<ol style="list-style-type: none"> 1. Approves the testing scenarios and the plan. 2. Determines a sample of testing data according to the scenario proposed by the Supplier. 3. Reviews and approves the test results report.
Acceptance testing	<ol style="list-style-type: none"> 1. Configures the environment required for testing and provides other technical conditions for carrying out the testing. 2. Prepares the testing data. 3. Participates in testing. 4. Maintains an error register. 5. Eliminates errors identified during testing. 6. Maintains a register of changes and documents the changes. 	<ol style="list-style-type: none"> 1. Performs the System acceptance testing. 2. Records and describes errors. 3. Accepts the tested IS parts.

9.9.12 Requirements for Technical Documentation

This section provides requirements for technical documentation.

No.	Requirements	
PVR-1	<p>According to the plan previously coordinated with the Customer, the Supplier must submit for coordination the following documentation in the formats and scope agreed with the Customer:</p> <ol style="list-style-type: none"> a) Pre-design proposals. b) Design documentation (including software functional description, software class description, software database description): <ul style="list-style-type: none"> • explanatory note; • technical specifications; • diagrams and drawings; 	<p>We are in compliance with this requirement. Documentation templates will be prepared during project Startup phase.</p> <p>Documentation produced is listed in chapter 5 Documentation and 6. Project plan</p>

	<ul style="list-style-type: none"> • logical and schematic diagrams of technical architecture (including program code); • System functional and interface diagrams with management tools; • lists of software used; • instructions for development and installation; • code development and implementation requirements, instructions; • software performance descriptions. <p>c) Instructions and manuals for administrators and users.</p> <p>d) System development.</p> <p>e) Executable documentation (including a copy of the operational [PRD] environment server with the OS, supporting programmes, source code, and other related documents).</p>	
PVR-2	At least version 2.5 of the UML standard (Unified Modeling Language) must be used in the System analysis, design or technical documents, operational process diagrams, models, database diagrams, software component interface diagrams and other entity interface diagrams prepared by the Supplier.	We are in compliance with this requirement.
PVR-3	Before providing the results, the Supplier must agree with the Customer on the templates of all the provided documents on the Project results with the essential descriptions of how and what results must be achieved.	We are in compliance with this requirement. Documentation templates will be prepared during project Startup phase.
PVR-4	The result template must be compatible with one iteration – The Customer within 5 working days (unless the parties agree on another deadline) evaluates the result template and comments or confirms its appropriateness. If there are comments, the Supplier within 5 working days (unless the parties agree on a different deadline) revises the result template according to the comments and provides the final version of the result template.	We are in compliance with this requirement.
PVR-5	The Customer submits comments on the documentary results within 5 working days, unless the Supplier agrees with the Customer on another term.	We are in compliance with this requirement – proposed project approach suits the 5 working days imposed by Customer on themselves.
PVR-6	All the Project documents must be coordinated within the scope of 2 iterations. The Customer may provide clarifications/comments to the observations and a larger number of iterations if the comments and observations are submitted to the same or dependent parts of the document to which the comments were submitted within the scope of the first 2 iterations, i.e., during iterative 3, shall not contain any entirely new comments that are not related to previous comments or dependent changes to the document. The results are considered accepted if a confirmation is received from the Customer that the results are correct or if the Customer does not provide any response regarding the suitability of the result within the set deadline.	We are in compliance with this requirement. Most of the documents are prepared as part of Solution Description track – more information on how Solution Description and Implementation Track are linked together is available in chapter 4.1 Dual Track agile approach of this Proposal.
PVR-7	The Supplier according to the Project documentation previously agreed with the Customer (including software	We are in compliance with this requirement – compliance of software

	functional description, software class description, software database description).	produced is considered against approved documentation.
PVR-8	The prepared new document has version 0.1. If comments are submitted to a document, a new version of the document, prepared after the comments, shall be established by increasing the second digit of the existing version of the document by one. Version 1.0 is available for the harmonized document. If a new version of the approved document is being prepared and needs to be harmonized, the second number is changed to 1, i.e., 1.1, after a harmonized new version of the document.	We are in compliance with this requirement - the versioning scheme requested works well with proposed project approach.
PVR-9	All the results provided by the Supplier must be compatible with Microsoft Office software formats (XLS (X), DOC (X), PPT (X), MPP). If the Supplier provides the results in another format that requires separate software, the Supplier is responsible for the modification and installation of the required software in the Company, instructions, licences and all other works and costs related to the software.	We are in compliance with this requirement - we will use standard Microsoft Office formats.
PVR-10	All the results and services provided by the Supplier must be provided in the Lithuanian language. Specific terminology must be specified in brackets in English.	User Guide (and texts in the system) will be available in English and Lithuanian. Other project and system documentation will be available in English.
PVR-11	The final results must be presented in an editable format (including documented diagrams).	We are in compliance with this requirement - editable document files will be provided to the Client.
PVR-12	A full, correct source code must be provided to the Customer to compile ready-to-use software using standard tools to perform the functions specified for it.	To be discussed over Contract. There are multiple options to cover this requirement, incl. Escrow provision of the source codes.

9.9.13 Requirements for Guarantee and Maintenance Services

This section describes the requirements for guarantee (PVR-13 – PVR-16) and maintenance services (PVR-17 – PVR-27).

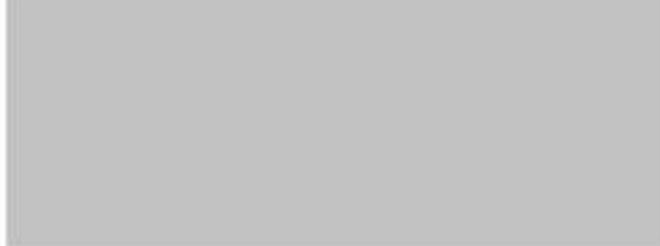
No.	Requirements	
PVR-13	The object of guarantee maintenance is the System developed and installed in accordance with the requirements of this technical specification.	We are in compliance with this requirement
PVR-14	After the Customer approves the acceptance-transfer act of the work performed in the first phase, the System is put into operation. After performing works of the Phase I of the System, the Supplier must ensure the smooth operation of the developed software. The warranty service of the System (of the first and second phase services) must be provided by the Supplier for 24 months then the System (the first and second phase) Transfer -Acceptance- Act is signed by both parties. The system warranty service must be provided during the Customer's business hours.	We are in compliance with this requirement
PVR-15	The guarantee service includes: <ul style="list-style-type: none"> • Elimination of System non-compliance with the established requirements and errors at the expense of the Supplier; • Restoration of the operability of the Existing System, for example, in case of malfunctions of the database or its individual components; 	We are in compliance with this requirement – for more information see chapter 6.4 Warranty Support – Guarantee and Maintenance Services of this Proposal.

	<ul style="list-style-type: none"> • Recovery of corrupted/damaged data when the cause of the failure is the malfunction of the software provided by the Supplier or improperly performed development/support/maintenance works; • Elimination of discrepancies and errors when the System does not work or functions incorrectly not due to improper implementation of the functional requirement or operating logic, but due to other components of the solution provided by the Supplier. Examples of such failures: The provided System functionality improperly affects (e.g., incomplete or incorrectly stored data) the results of functional requirements. 	
PVR-16	The system guarantee services must be provided during the Customer's business hours.	We are in compliance with this requirement – see chapter 6.4.7.1 <i>SLA specification</i> of this Proposal.
PVR-17	The system must operate reliably, meet information technology security requirements, and be quickly restored in the event of a failure. All actions of the Supplier related to the support service must be performed in accordance with the procedures agreed with the Customer.	We are in compliance with this requirement – for more information see chapter 6.4 <i>Warranty Support – Guarantee and Maintenance Services</i> of this Proposal.
PVR-18	Support services are available from 08:00 until 20:00. If the incident was registered after 20:00, the incident is considered received at 8:00 the next day. Errors and malfunctions identified by users are registered in the Customer's service management system. The service provider manages incidents through a system provided by the Customer.	We are in compliance with this requirement – see chapter 6.4.7.1 <i>SLA specification</i> of this Proposal.
PVR-19	<p>The system provided by the customer (incident registration system) would register the errors and disturbances identified by the TSO users. The maintenance service include:</p> <p>Operational System recovery, data recovery (incident resolution) according to incident response and resolution times.</p> <p>Provision of consultations by telephone and e-mail or other electronic means to the System Users with Key Rights, the list of which will be provided by the Customer after signing the service provision agreement. It is envisaged that the consultations will be provided to up to 10 Key Users of the System. Consultations are provided in accordance with the requirements of this technical specification and of the the System developed and installed in accordance with the requirements of the commissioned Supportive Development Services for the issues of guarantee development (System errors, malfunctions, etc.).</p> <p>Counseling services must be provided in real time, live;</p> <ul style="list-style-type: none"> • Monitoring of technical vulnerabilities of the System software by the System Manufacturer, notification of the detected vulnerabilities and provision of updated versions after the correction of vulnerabilities; 	We are in compliance with this requirement – for more information see chapter 6.4 <i>Warranty Support – Guarantee and Maintenance Services</i> of this Proposal.
PVR-20	All malfunctions of the System must be recorded in the incident management information system provided by the Supplier.	We are in compliance with this requirement – for more information see chapter 6.4 <i>Warranty Support – Guarantee and Maintenance Services</i> of this Proposal.

PVR-21	<p>All the System malfunctions, i.e. incidents are classified as follows:</p> <ul style="list-style-type: none"> • Critical error - The System does not work, is inaccessible, essential business logic is incorrect, data loss, major performance disruptions. The definition of critical error is not complete and will need to be agreed upon during the Project; • Other errors - The System (or its most frequently used part/function) is unstable, e.g. error messages are shown requiring reconnection to the System, frequently used operations are incorrectly performed, data is incorrectly saved, data (part of it) is not received/transmitted to other systems and other similar cases, as well as non-compliance of the System with functional and non-functional requirements is detected. Also, other errors are considered to be minor errors that do not limit functionality performance efficiency, do not damage, and do not provide erroneous data. <p>The decision on what type of incident is detected, shall be made by the responsible persons appointed by the Customer, who inform the responsible persons appointed by the Supplier.</p>	<p>We are in compliance with this requirement – for more information see chapter 6.4 Warranty Support – Guarantee and Maintenance Services of this Proposal.</p>
PVR-22	<p>Time limits for incidents responses and solutions:</p> <ul style="list-style-type: none"> • Critical error: <ul style="list-style-type: none"> - The duration of the response shall not exceed 2 working hours of the Customer from the moment of submission of the Customer's notification; - The duration of the solution shall not exceed 8 working hours of the Customer from the moment of submission of the notification of the System error. • Other errors: <ul style="list-style-type: none"> - Response time shall not exceed 8 working hours of the Customer from the moment of submission of the Customer's notification; - Duration of the solution: <ul style="list-style-type: none"> - No longer than 20 working hours from the receipt of the notification of the System error from the Customer, in case the analysis of the error reveals that it is not necessary to change the program code to correct the error; - No later than within 1 week from the receipt of the notification of the System error from the Customer in case the error analysis reveals that it is necessary to change the program code to correct the error. 	<p>We are in compliance with this requirement – see chapter 6.4.7.1 SLA specification of this Proposal.</p>
PVR-23	<p>The Supplier may agree with the Customer (in writing) upon other terms for elimination of errors acceptable to the Customer.</p>	<p>We are in compliance with this requirement – for more information see chapter 6.4 Warranty Support – Guarantee and Maintenance Services of this Proposal.</p>
PVR-24	<p>Any changes to the production environment, including error correction, manufacturer's global system upgrades and other upgrades, may only be implemented with Customer's written permission.</p>	<p>We are in compliance with this requirement – for more information see chapter 6.4 Warranty Support – Guarantee and Maintenance Services of this Proposal.</p>

PVR-25	Preventive maintenance of the System must be ensured (scheduled inspection and adjustment of the System to help prevent or correct errors in the System before they become defective).	We are in compliance with this requirement – for more information see chapter 6.4 Warranty Support – Guarantee and Maintenance Services of this Proposal.
PVR-26	The Maintenance services shall be provided in English or Lithuanian.	We are in compliance with this requirement – for more information see chapter 6.4 Warranty Support – Guarantee and Maintenance Services of this Proposal. English is the language of choice.
PVR-27	After the Customer approves the acceptance-transfer act of the work performed in the first phase, the System is put into operation. After performing works of the Phase I of the System, the Supplier must ensure the smooth operation of the developed software. The maintenance services of the System (of the first and second phase services) must be provided by the Supplier for 24 months after System (of the first and second phase services) Transfer -Acceptance- Act is signed by both parties.	We are in compliance with this requirement – for more information see chapter 6.4 Warranty Support – Guarantee and Maintenance Services of this Proposal as well as chapter 6. Project plan

10. Alignment with Functional Requirements

No.	Questions	Response
FR-1	The System must provide Two-Factor Authentication (2FA). Only authenticated users can see the information provided in the System and perform operations.	<p>Two-factor authentication is fully supported by Damas.</p> <p>The users access the system using their credentials - user name and password. Logging into the system may be further secured by using a client certificate used to confirm the user's identity.</p> <p>SMS could also be used as a part of 2FA method. The requirement of using a client certificate may be set globally or individually. The same authentication principles</p> 
FR-2	The system authorization mechanism must be implemented on the basis of a role-based model and be managed centrally throughout the System.	<p>This requirement is fully supported by Damas.</p> <p>Damas provides several levels of rights settings. In general, a user needs to authenticate first before accessing any of the Damas functionalities.</p> 
FR-3	The System must be able to manage user roles, including users of all partner networks.	<p>This requirement is fully supported by Damas.</p> <p>The administration of users and access rights is a part of system configuration and is fully managed by designers. In addition to detailed permission design, it is possible to group permissions to simplify assigning the business objects to roles. A set of visual functionalities is provided to design and check permission settings, which allows to efficiently manage permissions and verify their functioning.</p>

FR-4	The System must be able to assign, change and remove roles for users and to assign, change and remove access rights lists assigned to roles.	<p>This requirement is fully supported by Damas.</p> <p>The roles can be assigned or removed from users by the users, who are granted permissions to assign or remove roles.</p> <p>Role permission set could be modified by Damas administrator using GUI.</p>
FR-5	The System must be able to manage roles and their access rights, a preliminary list of roles of future System users is provided in the annexes (see Annex 2 of this technical specification). When changing the rights of the existing roles, these must be applied in real time to the users to whom the role associated with the change is assigned. A detailed list of user roles will need to be coordinated and configured during the Project implementation stage.	<p>This requirement is fully supported by Damas.</p> <p>The roles can be managed in Damas MMS by users with administrator privileges. The access rights for the given role can be set for each individual business object (view, time series, process, data flow etc.) The changes are immediately applied to the users, which have the relevant role.</p>
FR-6	The System must be able to create new roles and ensure their dynamic management.	New roles with a unique set of permissions could be created by users with administrator rights.
FR-7	The System must be able to assign more than one role to the user.	<p>This requirement is fully supported by Damas.</p> <p>Damas MMS provides the ability to assign any number of roles to a given user. It is common that the user has more than one role (e.g., Market Operator and System Administrator).</p>
FR-8	The System User must be able to view only such information and use only such functions as are specified in the access rights, for example, if the System User wants to view information that is not assigned to his role, the System must show the user that he does not have access to the information and otherwise restrict the review of information.	<p>This requirement is fully supported by Damas.</p> <p>Damas MMS ensures that the user can access only functionalities for which he/she has permissions (as given by roles the user is assigned to). The message is displayed to the user if the user tries to display/execute the function to which he/she does not have access.</p>

FR-9	The System must be able to specify an expiration date for the selected roles, after which the functions and access rights associated with the role are automatically suspended (i.e., invalidated) to the users who are holders of that role.	The requirements to: <ul style="list-style-type: none"> • suspend and activate role; • suspend and activate permissions; • scheduled suspension of role; • scheduled suspension of permission. will be implemented during the project after a detailed analysis of requirements with Litgrid.
FR-10	The System must be able to export a list of users with their roles and rights.	This requirement is fully supported by Damas. It is possible to export the list into XLSX format.
FR-11	The System user groups must be managed through Active Directory groups, which include user accounts.	Information about user groups sent from Active Directory (followingly as "AD") could be mapped to Damas MMS user groups. This requires sending such information inside the user AD authentication token. Alternative methods need to be analyzed during the project implementation phase.
FR-12	It must be possible to connect to the System without re-entering the user's data via Single Sign-On if the user has authenticated with the organization's Microsoft Active Directory Domain Services/Azure AD profile.	This requirement is fully supported by Damas. 
FR-13	After a user is suspended from an organization's Microsoft Active Directory Domain Services/Azure AD service, the user must be suspended from the System.	This requirement is fully supported by Damas. It is necessary to mention that the user token needs to be also revoked by the AD provider immediately. Such functionality depends on AD configuration and needs to be configured by the owner of the AD service.
FR-14	The System must provide safeguards against unauthorized access, taking into account the users' affiliation with an organization or network of partners, which must ensure that, by default, a particular user can only access his or her own information.	This requirement is fully supported by Damas. Damas MMS users can be divided into internal and external. An internal user belongs to the entity that owns the Damas system. The other (external) users are linked to external entities and are "guests" from the system's point of view. The system provides these entities with their own data space. Within the framework of user rights, external users may be configured to only access the values of the time series owned by their entity. In this context, "entity" means an organization whose employees have access to the system. An entity has its own data in the system, not accessible to other entities. For example: power plants can be entities; their employees may view only the data of production units belonging to their employer.

FR-15	The System administrator must have a possibility to block all actions of one or more other users by providing information in the user interface.	The actions of one or multiple users can be blocked by revoking roles and permissions from given users - this can be done in runtime by the system administrator. Another way to block an user in the system is to set its state to "Inactive". Such functionality is available in GUI. In such a case the user would not be able to log in into the system.
FR-16	The system must be able to set the duration of user work sessions and ensure that sessions close when the session is busy and the System is not used for the fixed time. The duration of the downtime will have to be agreed during the Project.	This requirement is fully supported by Damas. Session timeout is part of standard system configuration. The default value is 30 minutes for the Idle session. Value can be changed in the configuration.

11. High-Level System Design

11.1 System Configuration and Administration

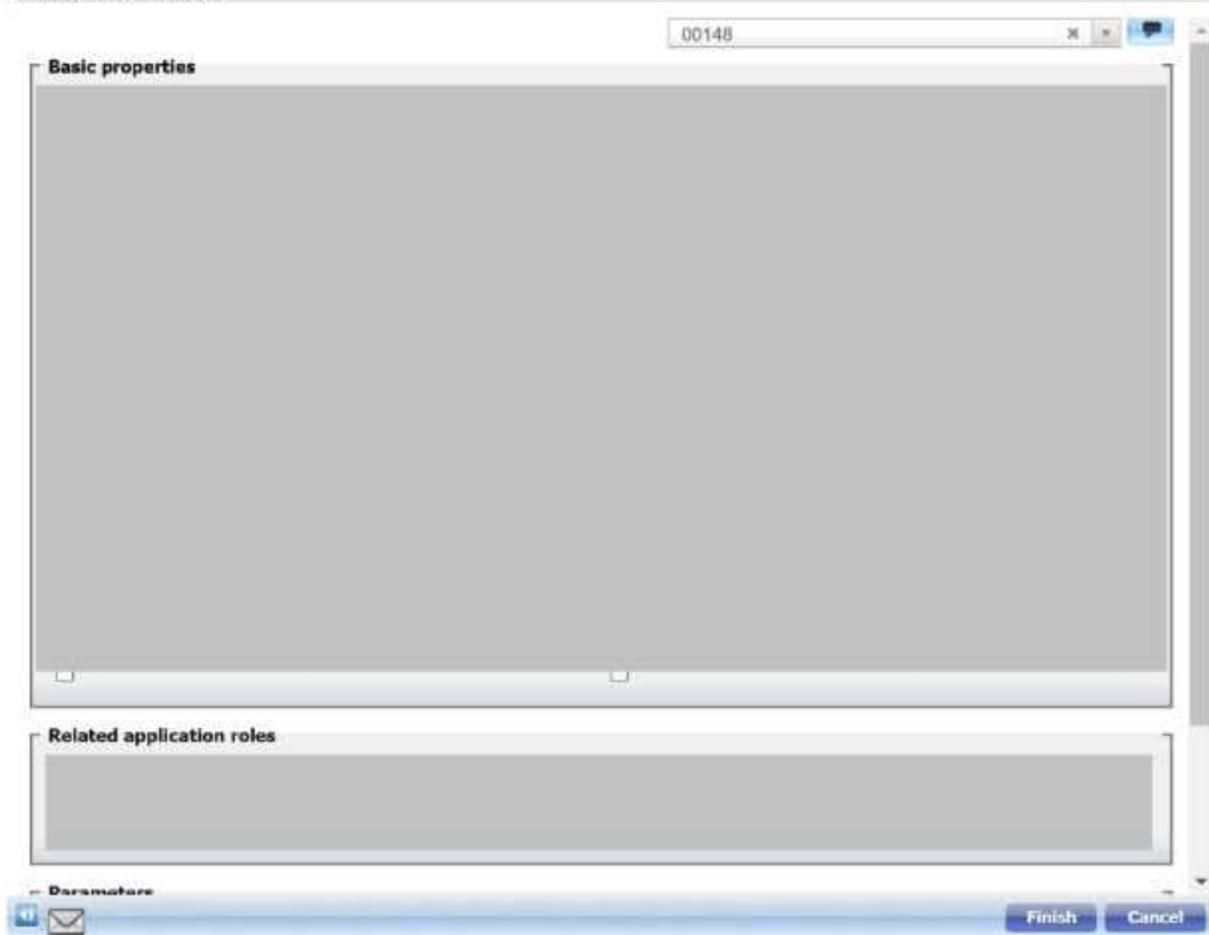
11.1.1 Configuration of Market Participants



Users

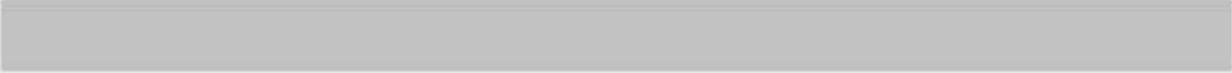
[Redacted content]	
--------------------	--

Create business role



11.1.2 Configuration of Processes





11.1.3 Process Development Tools



11.1.4 Configuration of Variables



Basic properties

Dimensions

Description

Value determination

A screenshot of a software interface showing four stacked, empty form fields. Each field has a title bar at the top: "Basic properties", "Dimensions", "Description", and "Value determination". The fields are currently empty and have a light gray background. There are small blue icons in the top right corner of each field, possibly for expand/collapse or refresh.

11.1.5 Configuration of Message Templates

A large, empty gray rectangular area, likely representing a configuration screen for message templates. The content is completely obscured by a gray block.

Edit data flow type 2 DE05 Send accepted bids to BSP - page 2 of 8



11.1.6 Data Transmission Control and Monitoring

[Redacted text block]

- [Redacted list item]
- [Redacted list item]
- [Redacted list item]

The tool already supports almost all requirements, such as:

- [Redacted list item]

o

11.1.7 Alignment with Requirements for Administration and Management Tools

No.	Requirement	Response
AVR-1	The system must have a multi-parameter search function	
AVR-2	Must be able to operate on database objects: delete, add, add new, assign classifier, and so on.	
AVR-3	The components must allow, without major programming work, to establish and apply business rules, and have the functionalities that implement them.	
AVR-4	The system must be able to include and define additional descriptive fields without major programming work.	
AVR-5	Determine and apply file retention duration and retention requirements rules based on related events and the application of encryption mechanisms.	
AVR-6	Create and apply various object classifications, both received or developed in System modules and external, including at the database level.	
AVR-7	Define and apply lifecycle management rules for existing data, files, and metadata by establishing the use of temporary storage, operational, extended storage, and other storage spaces.	

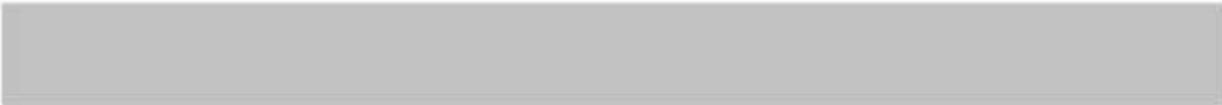
No.	Requirement	Response
AVR-8	The possibility of establishing and applying semantic verification rules must be realized	
AVR-9	The system must be able to specify the numbering of the identifiers to be started and the rules for assigning the next identifier	
AVR-10	Establish and apply rules for varying degrees of depersonalization.	
AVR-11	The system must implement a function for the administration, control and management of related events in order to assess the cases of proper use.	
AVR-12	A mechanism must be implemented to transmit encrypted data and to determine or change encryption methods.	
AVR-13	Define and apply data transfer parameters/components to other System modules or other internal or external systems.	
AVR-14	It must be ensured that new components of the API are added or that existing components are replaced without changing the architecture of the components.	
AVR-15	The system must be able to create and define different rules or processes for different recipients.	
AVR-16	The system must be able to set, manage, monitor the communication rules of the messages by specifying their validity terms and periods.	
AVR-17	For data storage, the system must be able to store files regardless of the file format and have the ability to apply file cataloging.	

No.	Requirement	Response
AVR-18	It must be possible to define and apply the functions of mathematical expression of the different components when compiling or modifying the reports or forms generated by the System.	
AVR-19	The system must be able to change the grouping and sorting rules in the reports.	
AVR-20	It should be user-friendly for reporting from existing data, including both metadata, system data, and file specifications.	
AVR-21	The system must implement electronic helpers for administration (electronic wizard, the basis for creating templates in a specific case, etc.).	
AVR-22	A convenient mechanism for defining, assigning and activating user roles must be implemented, which is linked to access rights sets and different validity periods.	
AVR-23	The different components of the system (forms, reports, interfaces, messages, etc.) must be able to be assigned roles and actions that can be performed with the data available in them, i. e. create (C), read (R), edit (U), delete (D)).	
AVR-24	The system must implement a mechanism for applying user rights management and service authorization rules.	
AVR-25	The system must provide for the possibility to change the descriptions of variables in Lithuanian and English.	
AVR-26	Software licences, that ensures System's administration and control components operation can not be limited by number of users.	

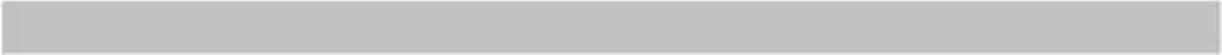
11.1.8 Alignment with Requirements for General Forms

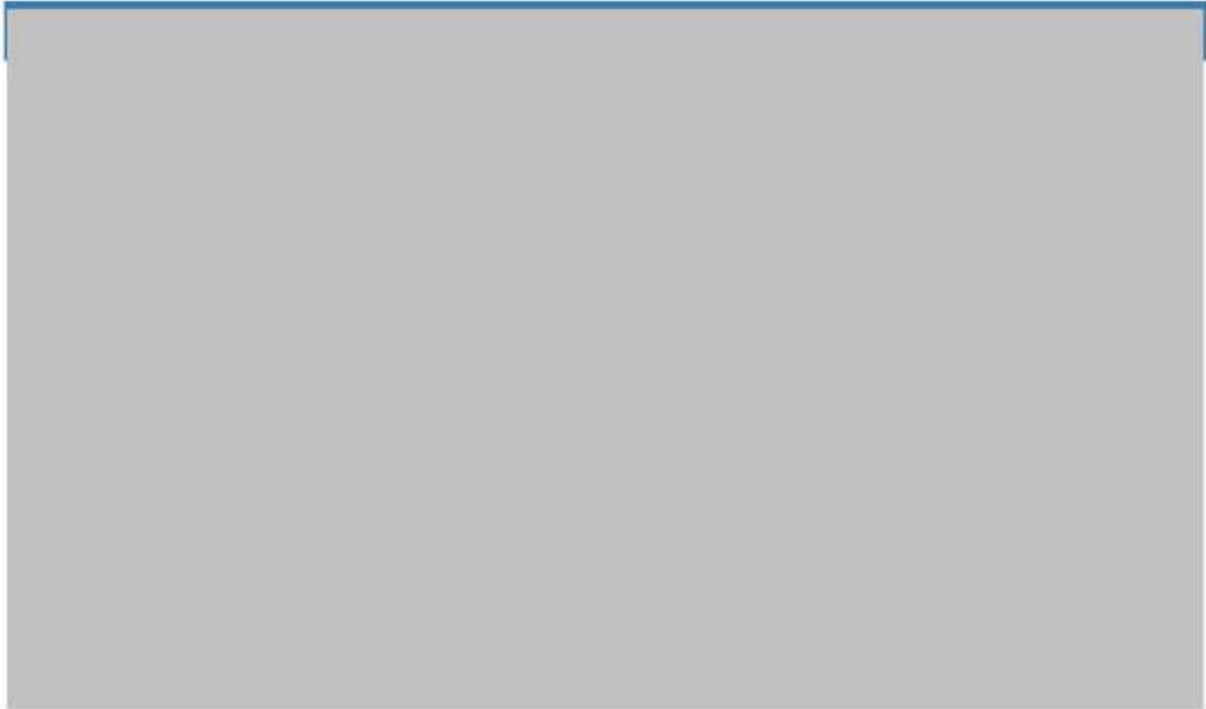






11.1.8.3 Data Editing

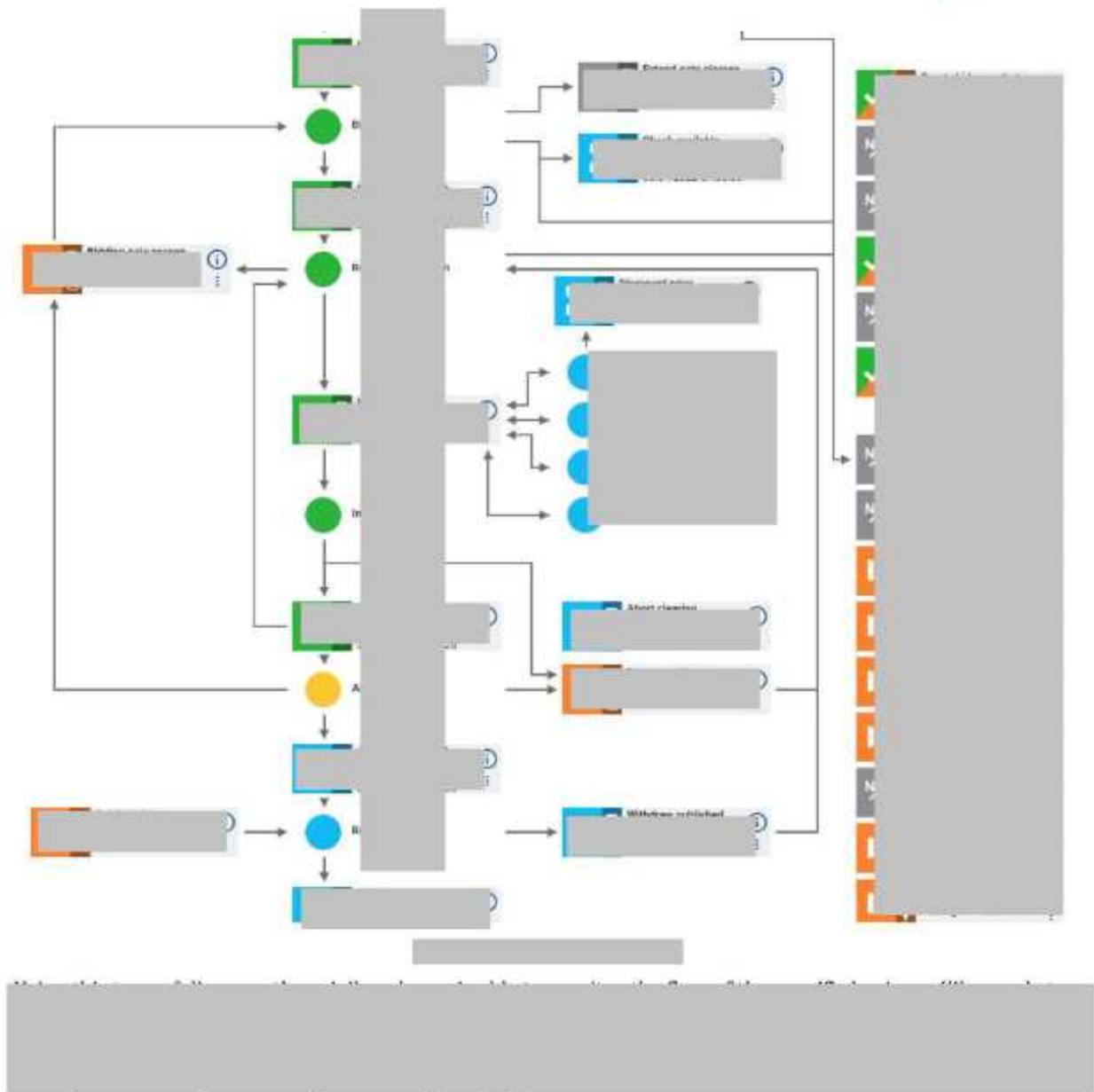


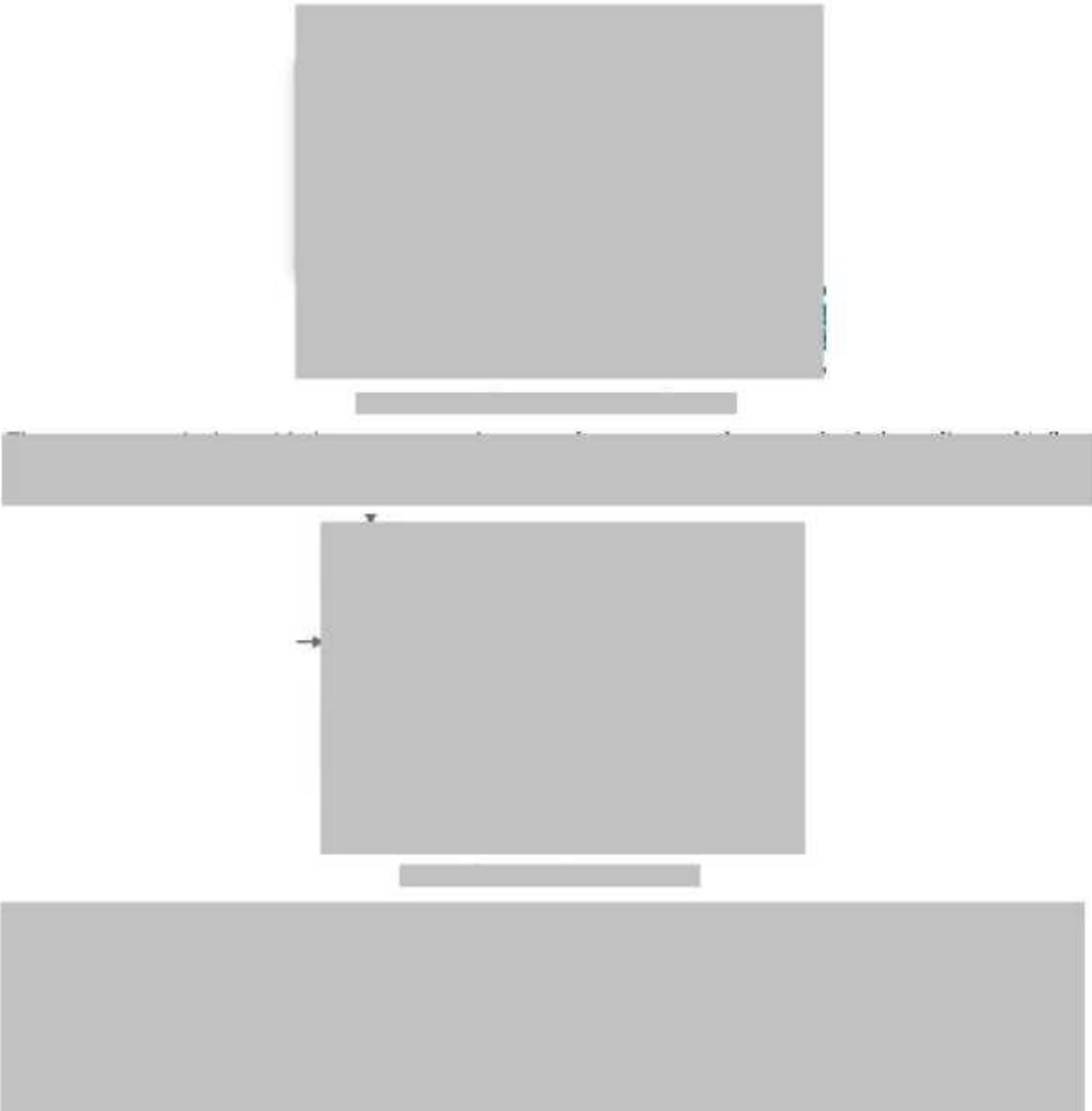


Close

11.1.8.4 Process Management Tools GUI







11.2 Balance Planning





11.2.1 Long-term balance planning



- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

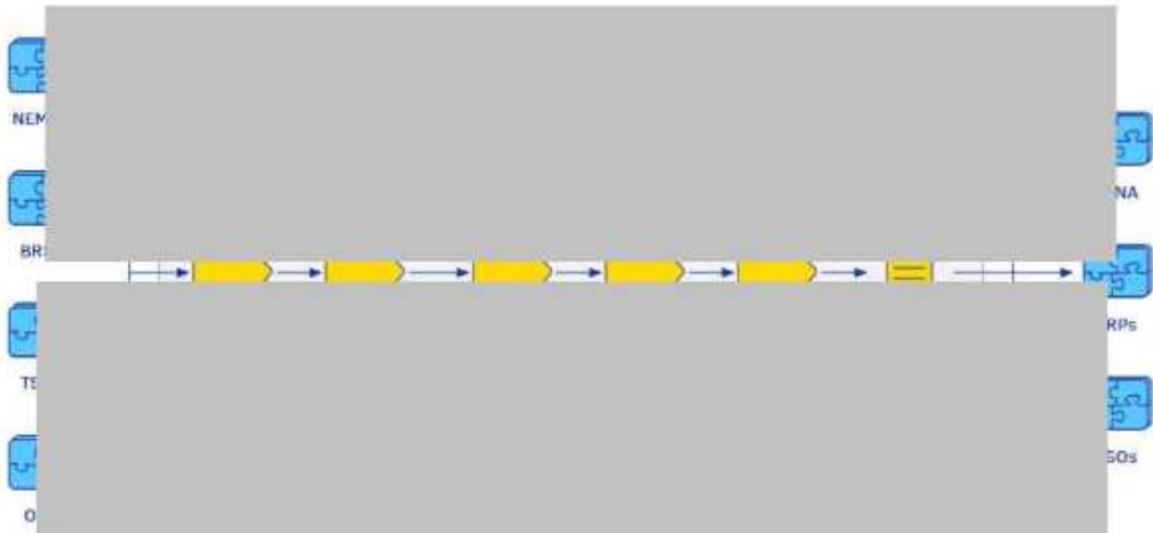
[Redacted]

-
-
-
-
-

[Redacted]

11.2.2 Day-ahead balance planning

[Redacted]



[Redacted]

[Redacted]

[Redacted text block]

[Redacted text block]

[Redacted text block]



[Redacted text block]

[Redacted text block]

- [Redacted list item]
- [Redacted list item]
- [Redacted list item]

[Redacted text block]

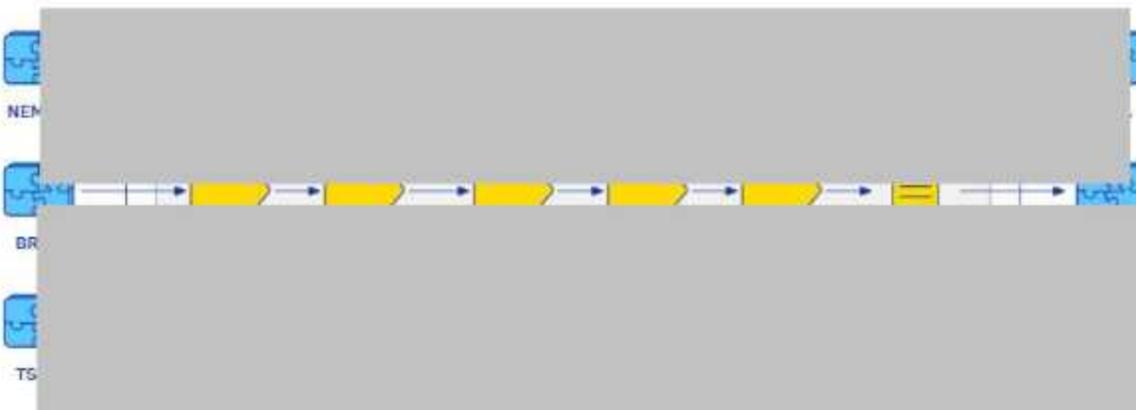
[Redacted text block]



[Redacted text]

11.2.3 Intraday balance planning

[Redacted text]



Input Data	Data Source	Input Channel
[Redacted]	[Redacted]	[Redacted]

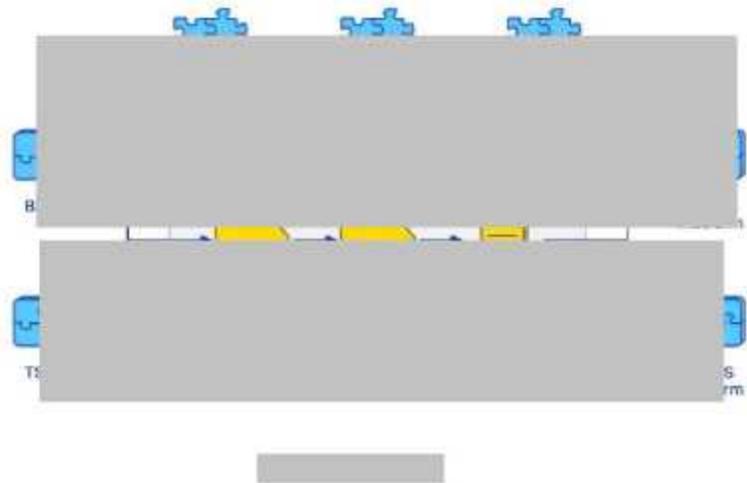
	Data Source	Input Channel
	N	c interface
	N	c interface
	N	c interface
	E	c interface

[Redacted text block]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

11.2.4 Grid Model Data Processes

[Redacted text block]



[Redacted text block]

[Redacted text block]



- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]



member of the chapter 11.2.2.10 for more information.

11.2.5 Alignment with Requirements for Balance Planning

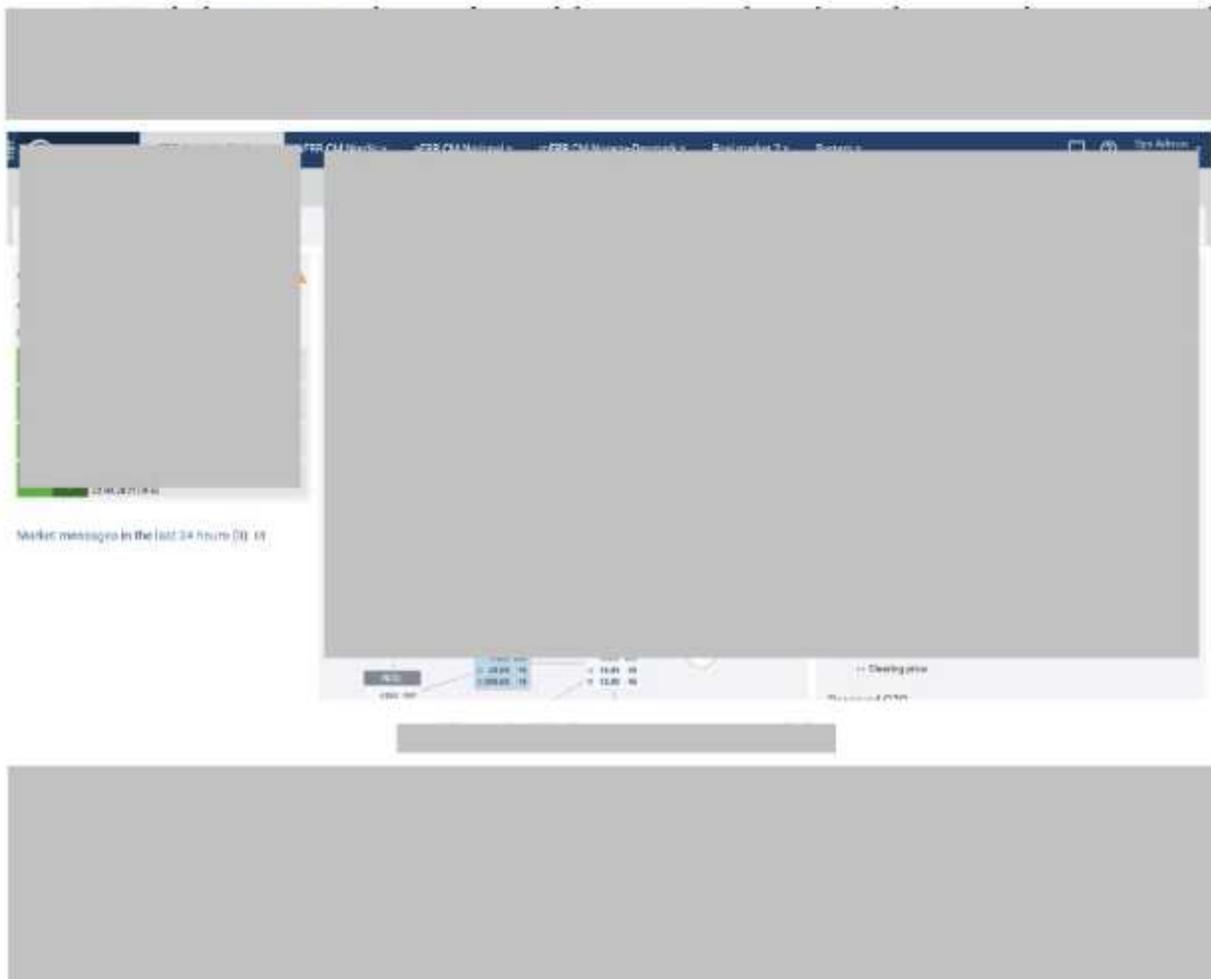
Requirement	Response
1. IGM reports are generated automatically according to the set standard parameters and initiation conditions.	
2. Each report can be generated manually via the GUI with the possibility to view it in the application.	
3. The user can create and configure a report data view in the system GUI.	
4. The generated report can be exported to .xlsx format via the GUI.	
5. Brell reports must be in Russian time, which is not turned ahead or back. Due to the time difference, the first (Summer time) or the first two (Winter time) hours are taken according to the D-1 plan, as we already have this data at the time of report generation. The remaining hours are taken according to the date of the data used to generate the report.	
6. The generated report in .xlsx format is sent to the specified e-mail address.	
6.1.1. The user is shown process monitoring according to the date and time set by the user	
6.1.2. Different colours indicate the status of the step of the process	

6.1.3. After hovering the mouse on the field, information about the number of messages by status or other necessary information is displayed

6.2.1. The user is shown the status of the messages according to the user-defined process type (D-2; D-1; INTRADAY) and the date and time

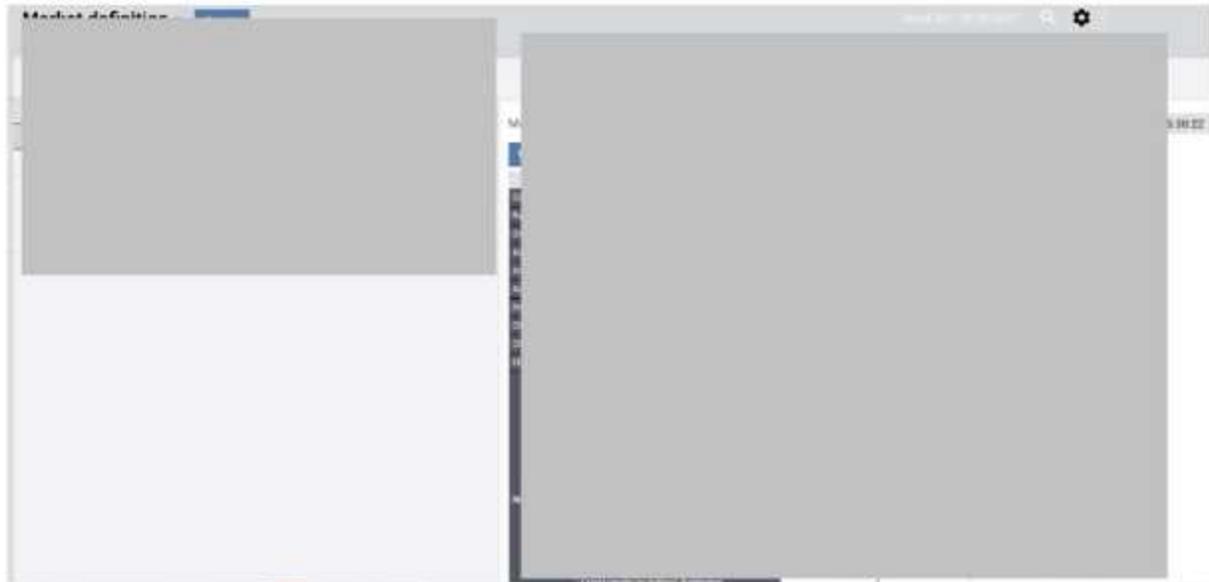
6.2.2. If data are only available for a shorter period than expected in the process, it is indicated how much data is missing.

11.3 Balancing Capacity



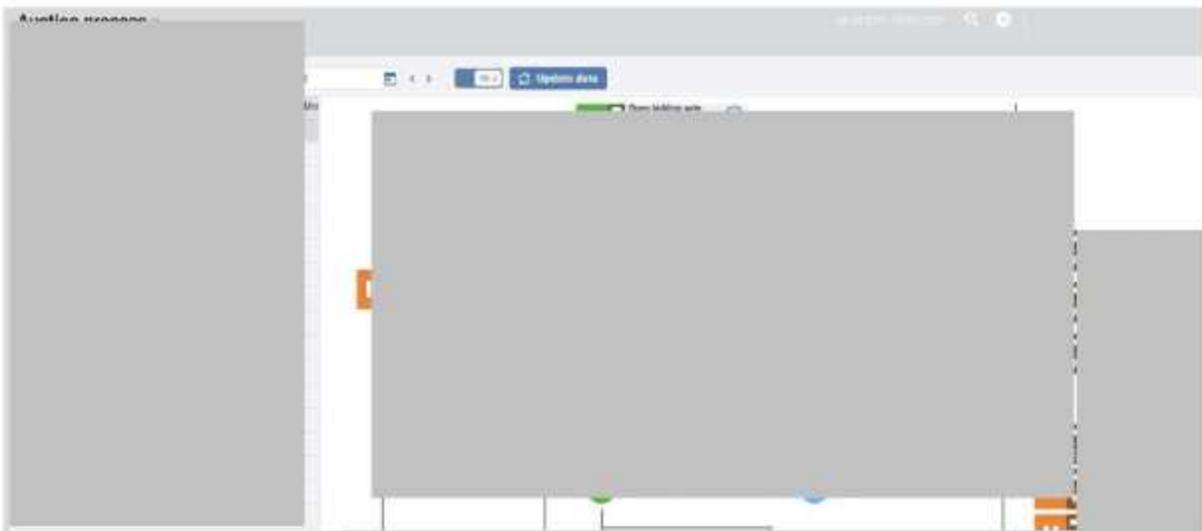


11.3.1 Market configuration



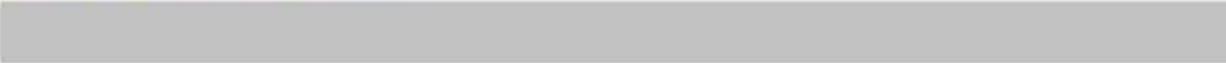


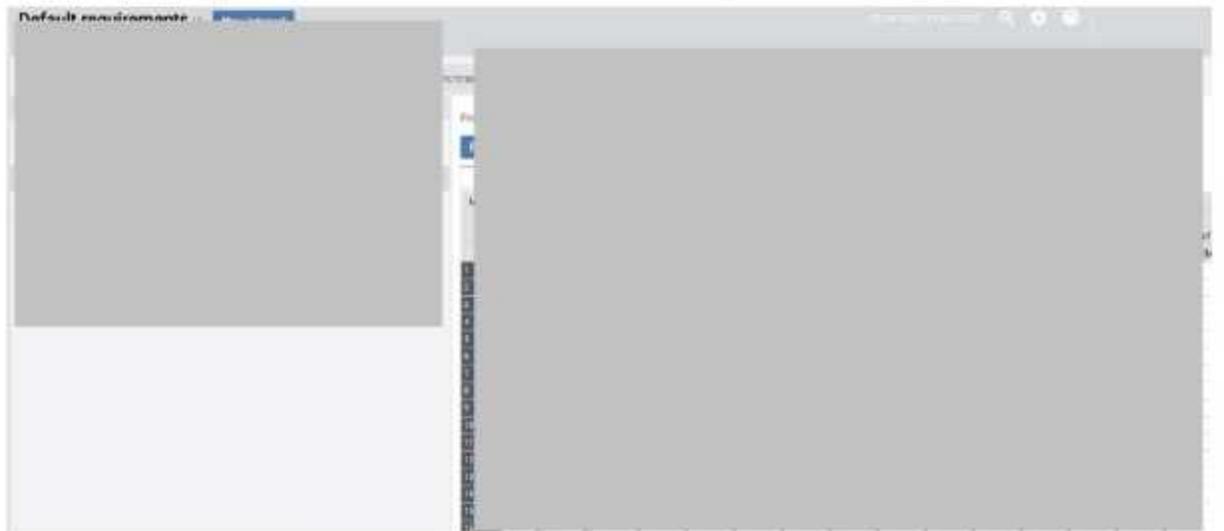
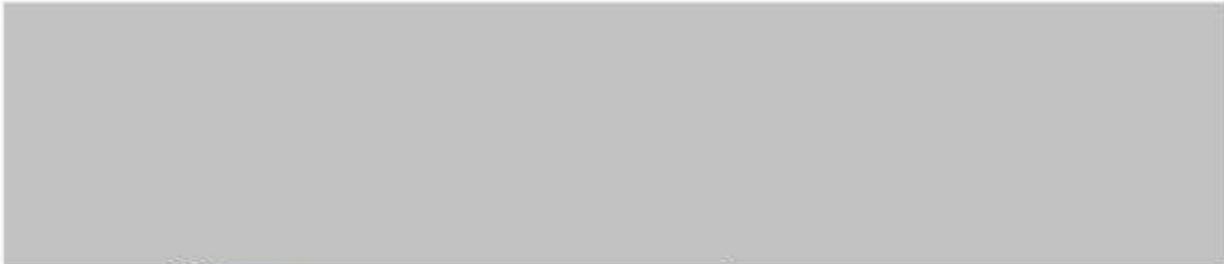
Clearing configuration



Auction workflow

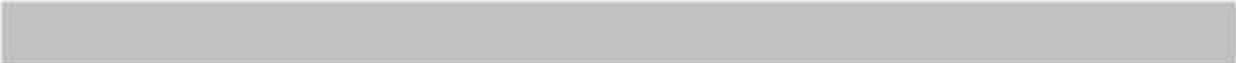
11.3.2 Reserve requirements





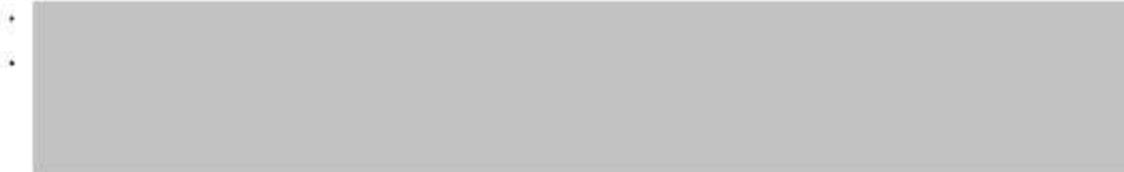
Reserve requirements

11.3.3 Bidding

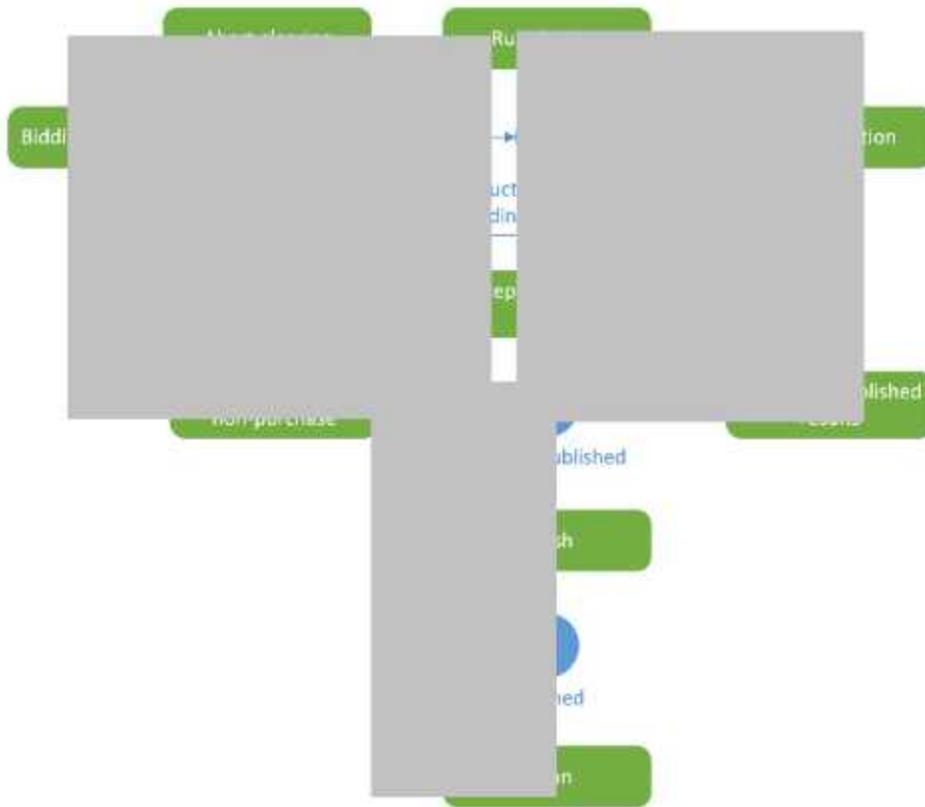




Bid entry form



11.3.4 Clearing



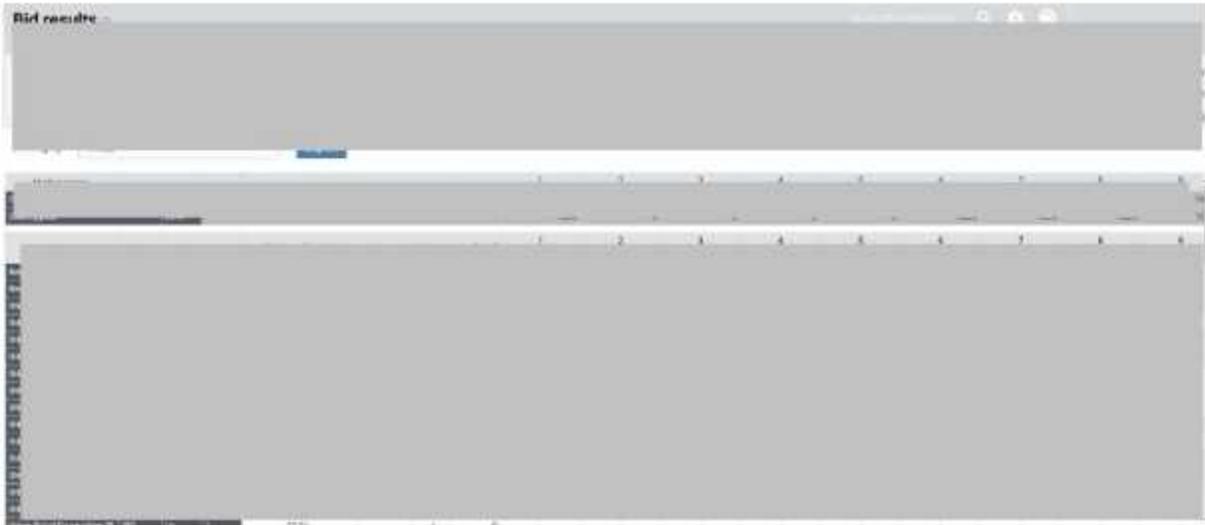
Clearing workflow



- [Redacted]

11.3.5 Results communication

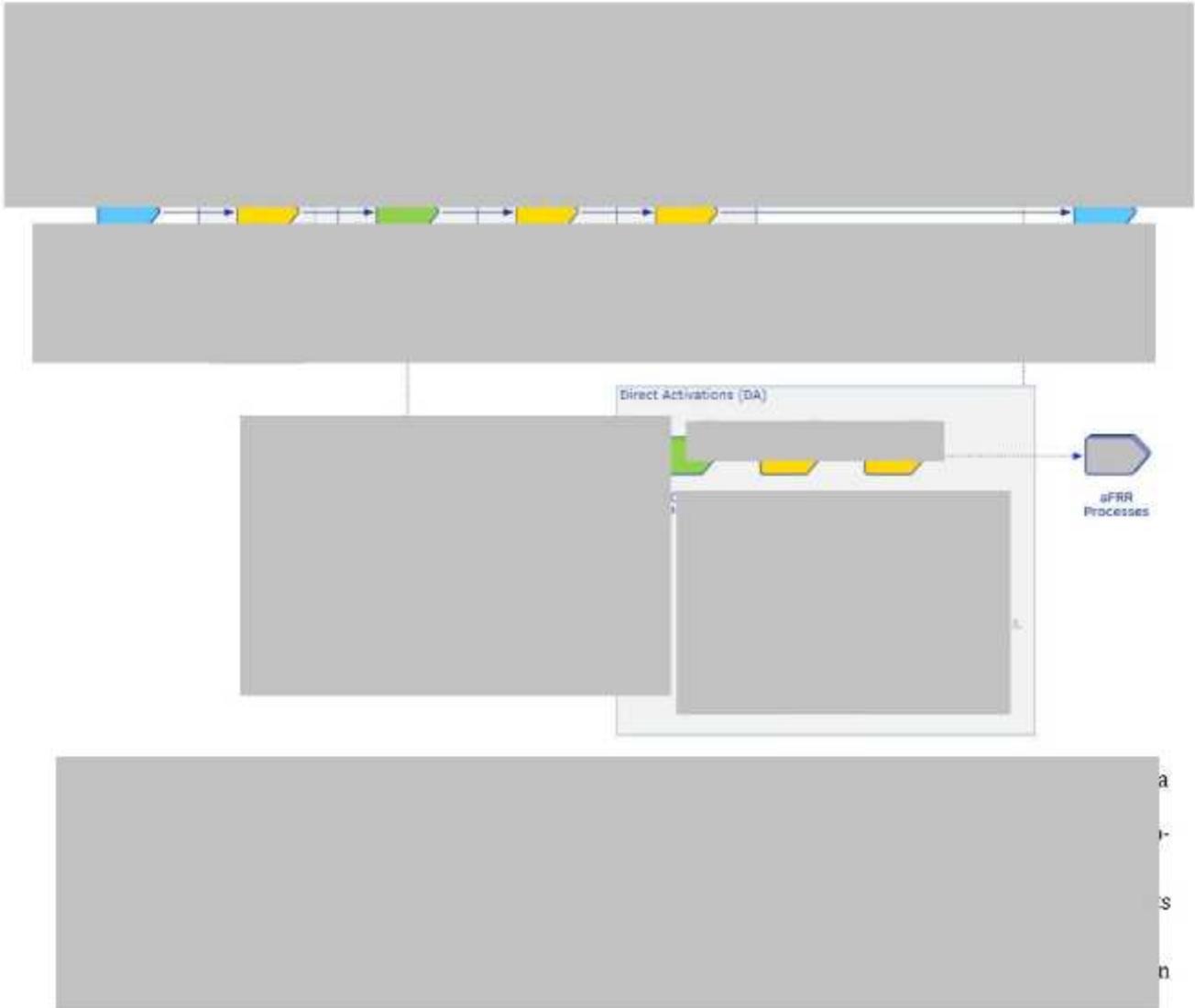
[Redacted]



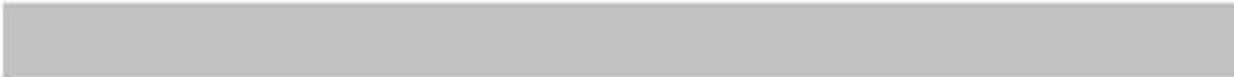
Bid results form

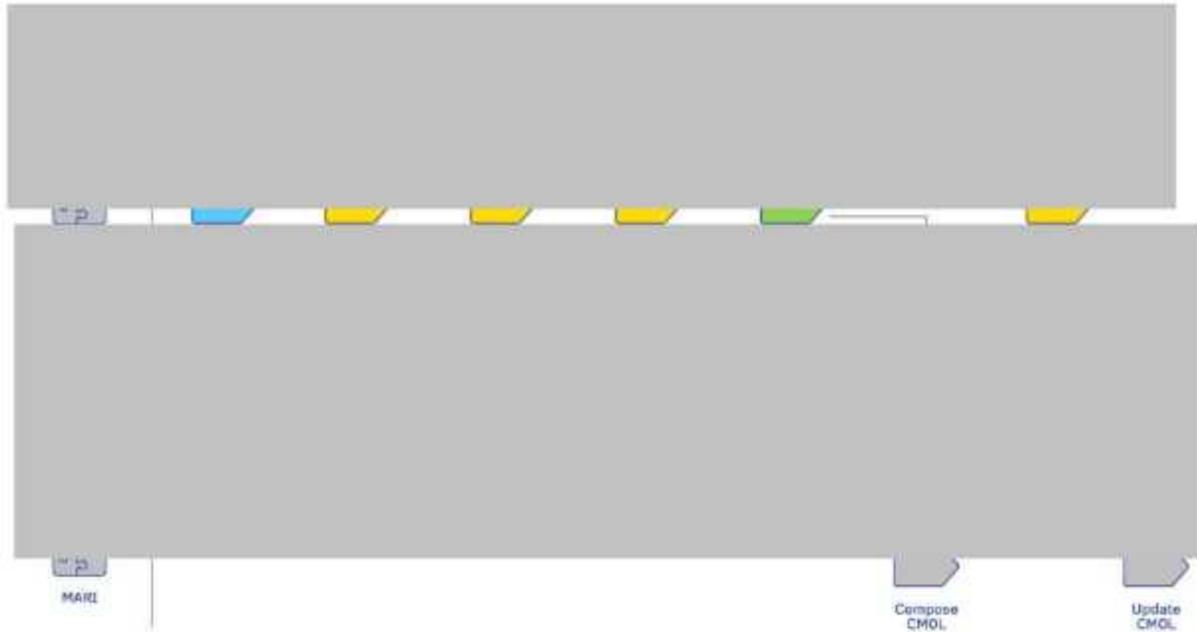
11.3.6 Secondary market





11.4.1 Balancing Bidding and Merit Order List





A screenshot of a software interface. The top portion is a large greyed-out rectangular area. Below it is a horizontal toolbar with several colored buttons: a grey button with a document icon, a blue button, a yellow button, a yellow button, a yellow button, a green button, and a yellow button. Below the toolbar is another large greyed-out rectangular area. At the bottom of this area, there are three buttons: a grey button with a document icon labeled "MAIL", a grey button labeled "Compose CMOL", and a grey button labeled "Update CMOL".



A screenshot of a software interface. The top portion is a large greyed-out rectangular area. Below it is a table with a light blue header and a white body. The table has two columns: "Area Results" and "Prices". There are four rows of data, each with a yellow square in the "Area Results" column and a yellow square in the "Prices" column. A greyed-out rectangular area is overlaid on the table, covering the middle two rows.

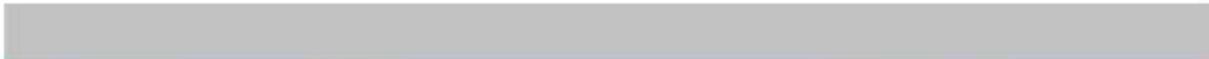
Balancing Data Entities



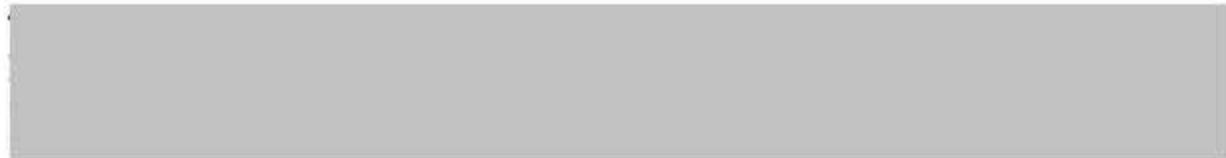
A large greyed-out rectangular area, likely representing a redacted section of the document.



← Offer 1/1 → ← Offer 2/1 → ← Offer 3/1 → ← Offer 4/1 → ← Offer 5/1 → ← Offer 6/1 →



Characteristics	Value	Technical Limit
Offered volume	Var	
Divisibility	Div	
Minimum offered volume	Var	
Direction	Up	
Price	Var	
Activation Type	Sch Dir	
Time Resolution	MT	
Balancing Area	EIC	



-
-
-
-
-
-
-





[Redacted text block]



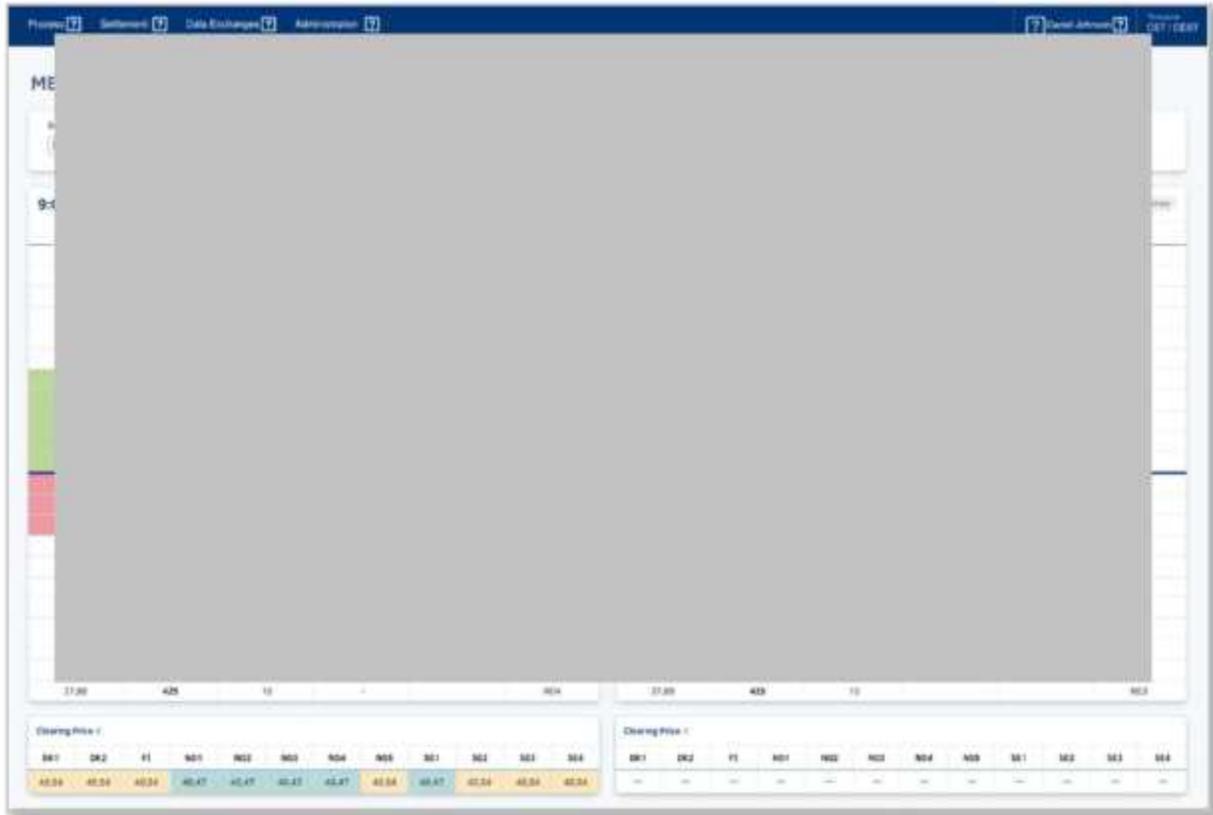
[Redacted text block]

[Redacted text block]

- A. [Redacted text]
- B. [Redacted text]
- C. [Redacted text]
- D. [Redacted text]

[Redacted text block]

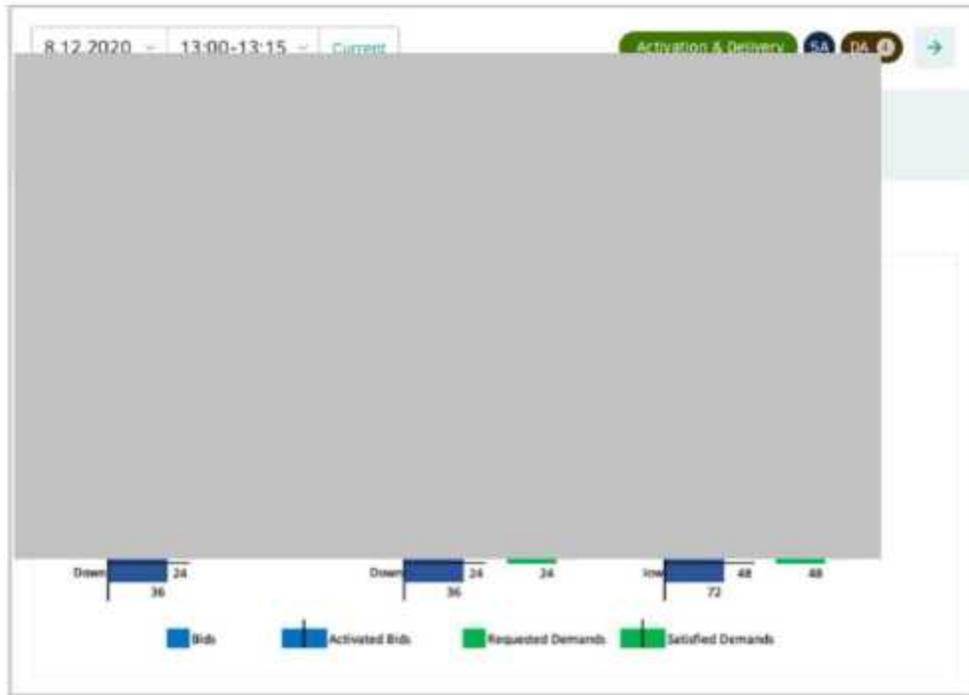




Merit Order List

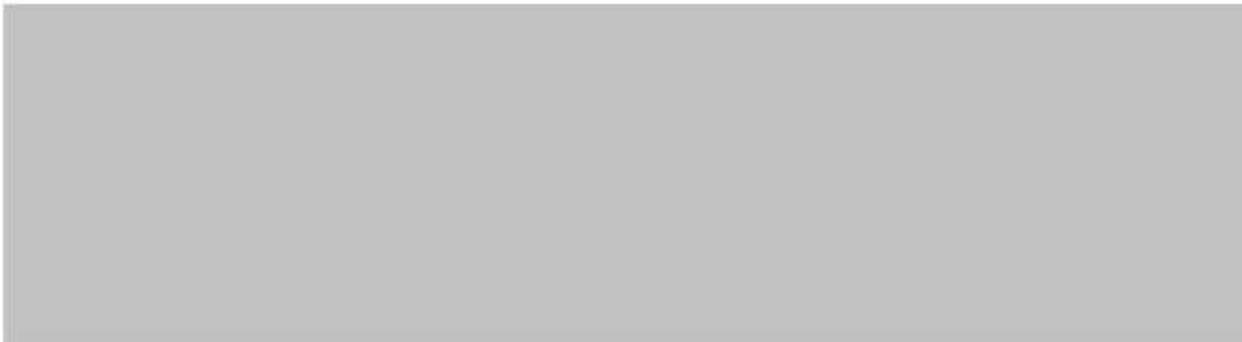
11.4.2 Balancing Demand



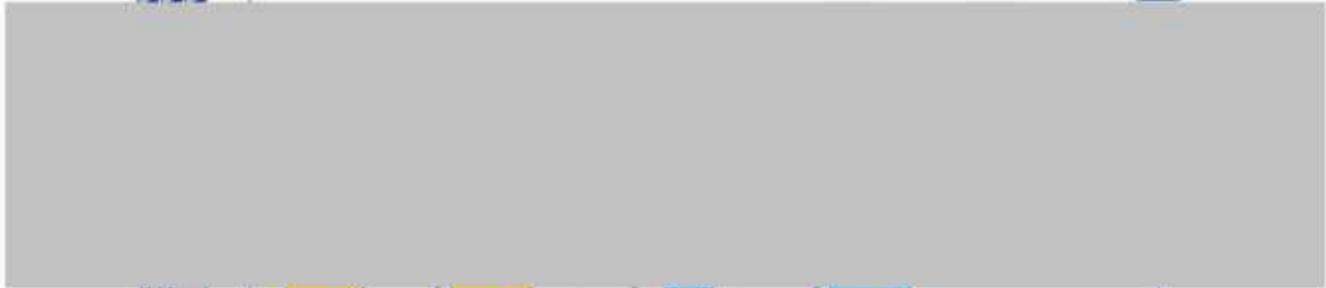


An example of SA and DA Demands / Needs screen

11.4.3 Activation Orders Management



Process sequence for one delivery period 15min



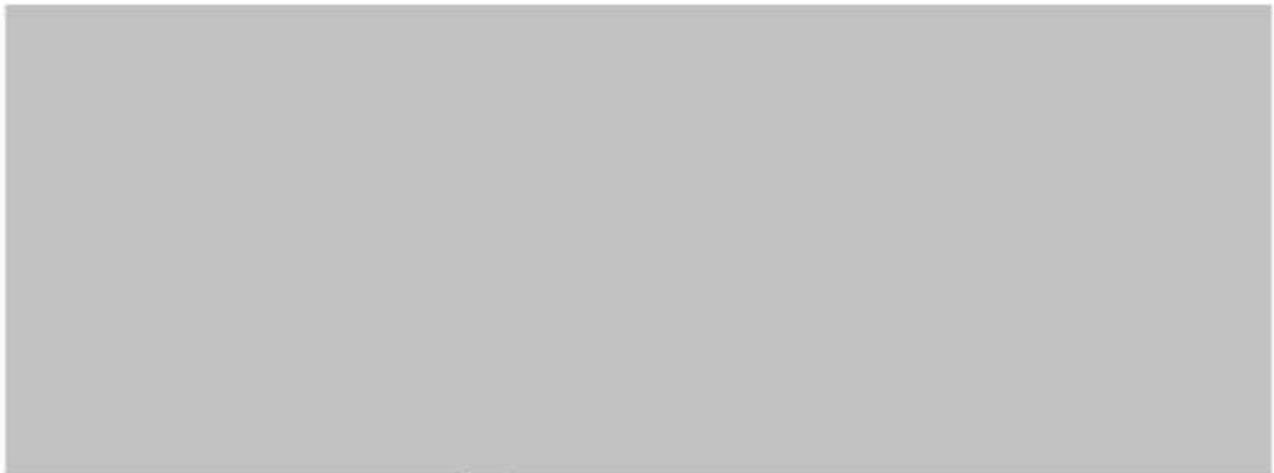
CoBA



CoBA (5A)



Receive ADR





11.4.4 mFRR GUI

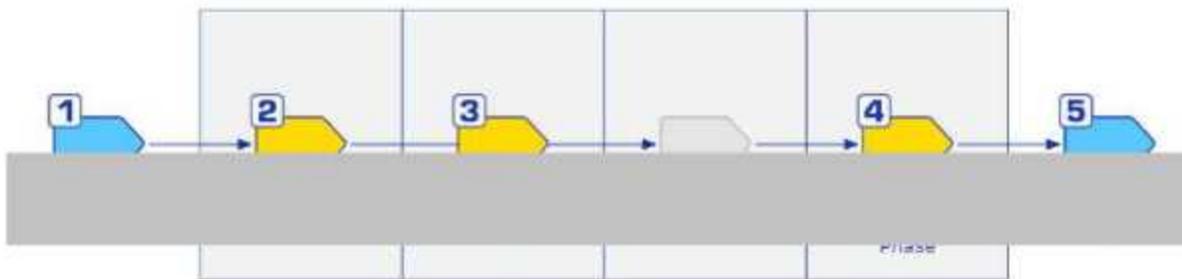
The default Damas MMS product implementation contains the following views:

View	Description
Dashb	
Dashb	
mFRR	
mFRR	

mFRR B

mFRR S

11.5 aFRR Balancing



11.5.1 Balancing bidding and merit order list

11.5.2 Activation orders management

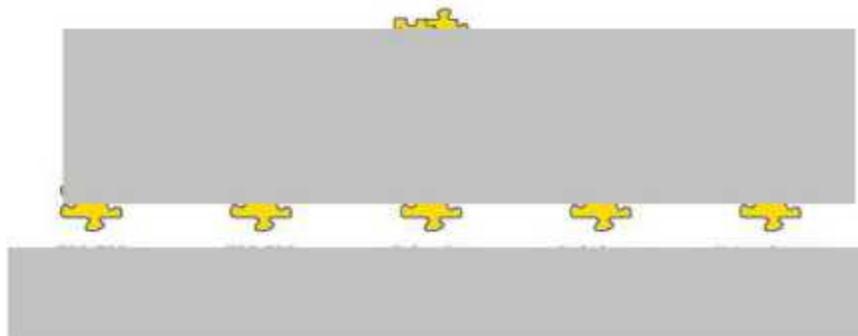
-
-
-
-
-
-
-

11.5.3 aFRR GUI

The default Damas MMS product implementation contains the following views:

View	Description
Dashboa	
Dashboa	
aFRR Bic	
aFRR Bic	

11.6 Settlement



Settlement Calculation Times

Date is displayed in CET (UTC+1) / CEST (UTC+2)

10/11/2019

Refresh View Settings



11.6.1 TSO-TSO actual data electricity settlement





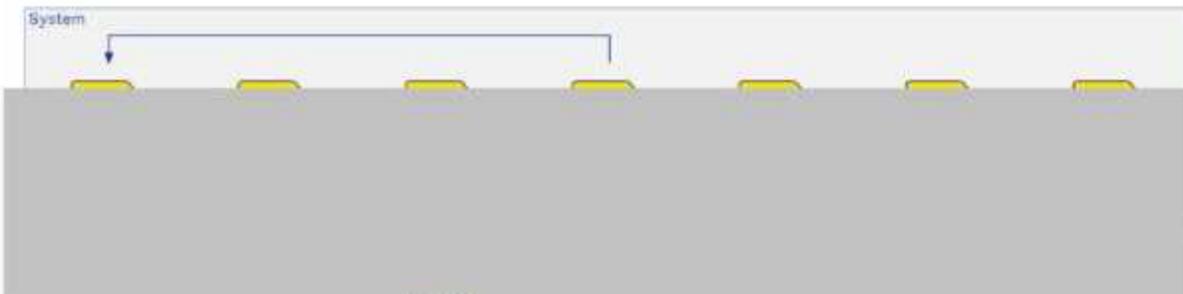
Example of settlement results monitoring screen

11.6.2 TSO-TSO Balancing energy settlement





11.6.3 Balancing services Settlement

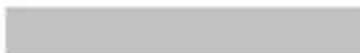
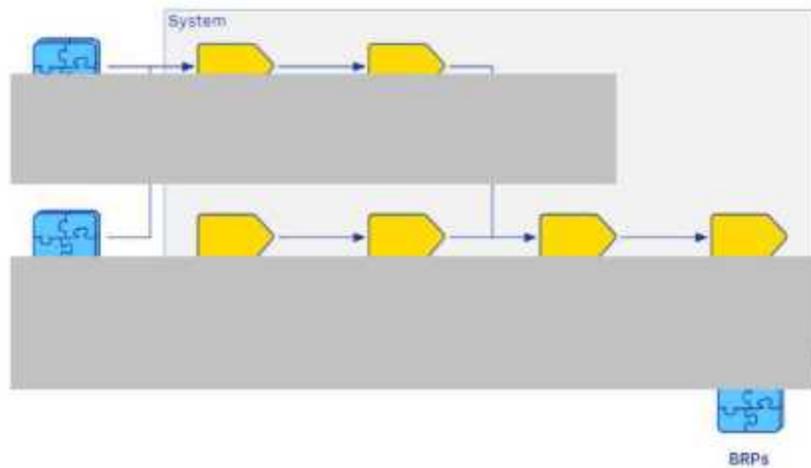
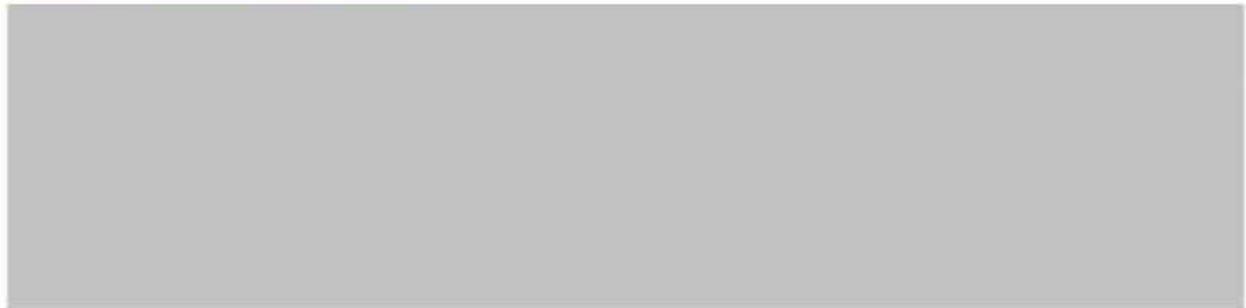


BSP

Balancing services settlement



11.6.4 Imbalance Settlement





BRP Consumption Imbalance

GET (UTC+0) GET (UTC+2)



Consumption imbalance per MBA

GET @RC+@RCESF @RC+@S



[Redacted text block]

11.6.5 Network users (NU) transmission service settlement

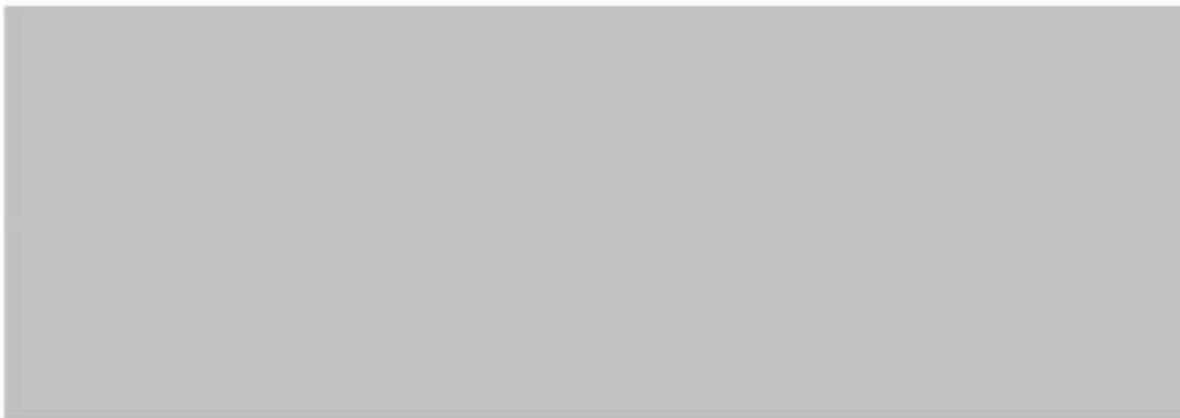
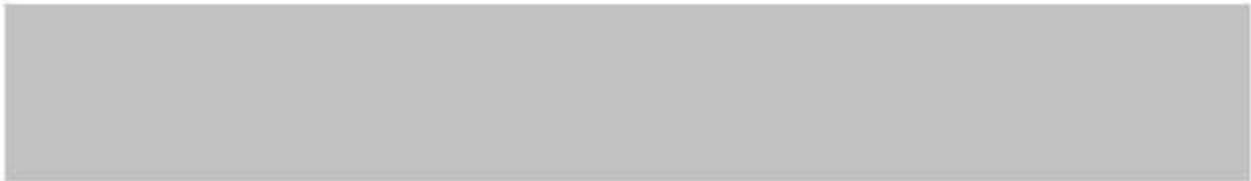
[Redacted text block]

[Redacted text block]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

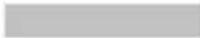
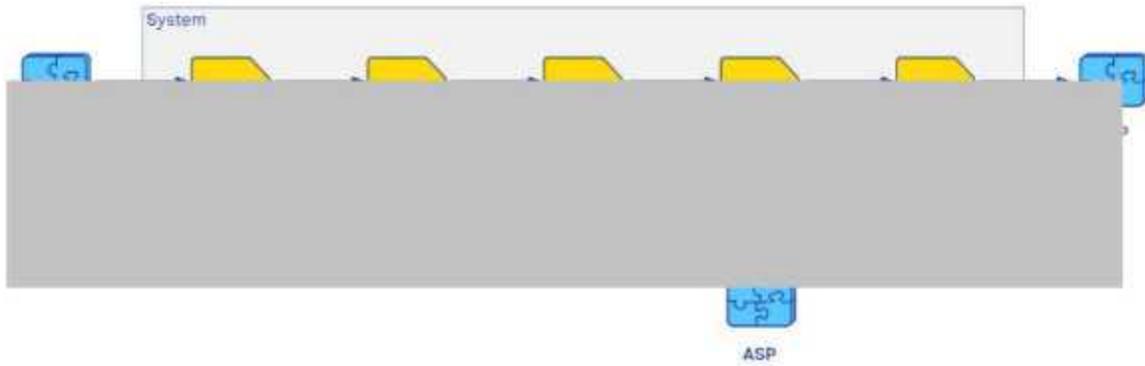
11.7 Financial Guarantees

[Redacted text block]

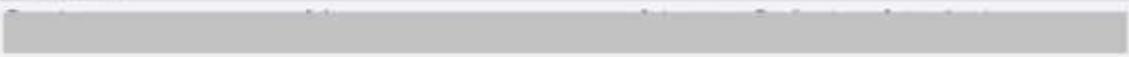


11.8 Ancillary Services

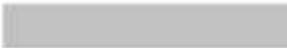




Rule definition

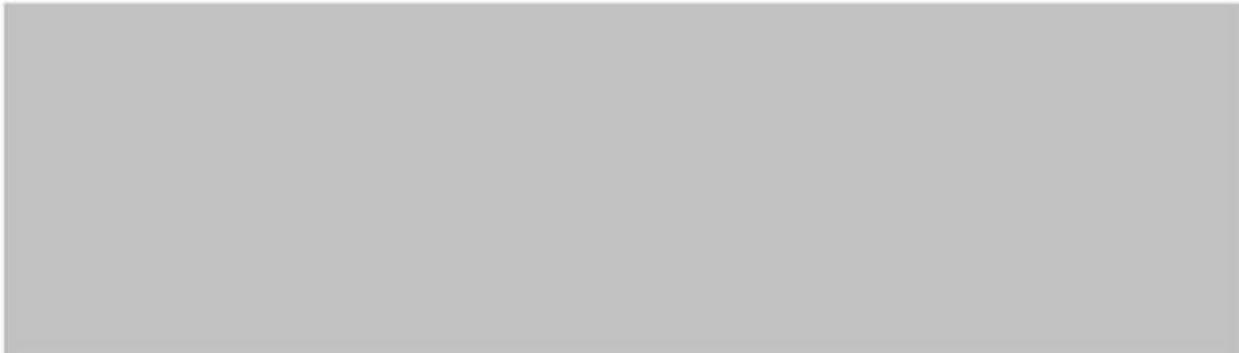


1. Formula





11.9 EIC Codes



11.10 Data exchange formats and interfaces

Data Flow	Module	External System	Direction	Expected Communication Channel	Expected Message Format	Expected Frequency
Recei sched						
Recei from						

Re fro	
Re fro	
Re sch nel	
Re cot fro	
Se cot in an sch	
Se sch TS	
Se the (el	
Se me	
Re ver	
Re age	
Re da	
Re sys (At	
Re	
Se flo	
Re ma	
Re rej	
Re rej bal	

Rec fro		
Rec pro		5
Sen MA		5
Sen CoI		5
Rec		5
Rec (CM		5
Sen		5
Rec res		5
Sen CoI		5
Sen MA		
Rec fro		5
Sen res		5
Rec AOI		5
Sen CoI		
Sen ord		
Rec sig acti		5

Re ne re		5
Re ne lo		5
Re ne		
Se ne		
Se SC		
Re		5
Se PI		5
Se Oj		5
Re fr		5
Re IS		
Se de fo		
Se de fo		
Se de fo		
Re TS hc th		
Re TS hc th		

R	
T	
h	
th	
R	
b:	
b:	
rc	
p)	
R	
in	
in	
rc	
p)	
R	
A	
rc	
h	
h	
R	
C	
T	
Sc	
d:	
R	
P:	
m	
R	
q)	
R	
S	
m	
R	
q)	
Sc	
p)	
Sc	
q)	
Sc	
p)	
Sc	
q)	
Sc	
R	
R	

S	
f	
R	
a	
R	
U	
n	
s	
S	
r	
T	
h	
R	
L	
S	
r	
R	
d	
e	
s	
R	
u	
f	
s	
S	
G	
i	
R	
S	
s	
R	
S	
ú	
s	
R	
S	
ú	
r	
S	
S	
o	
S	

12. Damas MMS platform description

12.1 Solution overview





12.2 Key components

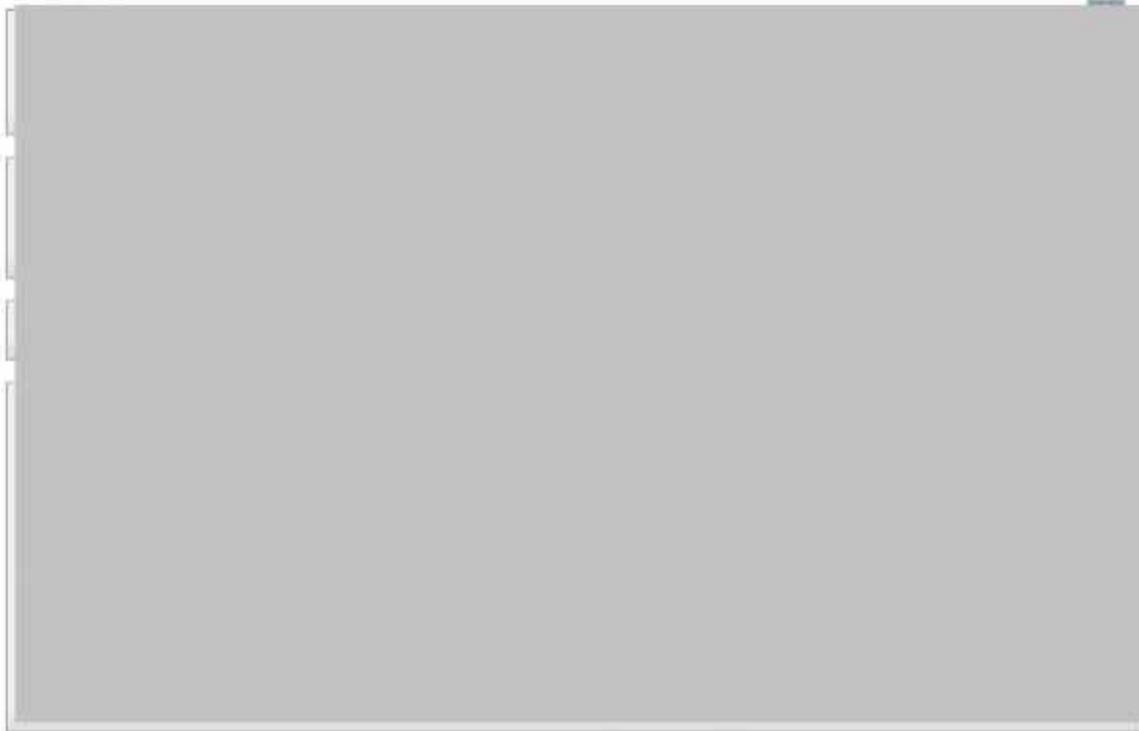


12.2.1 Time series engine

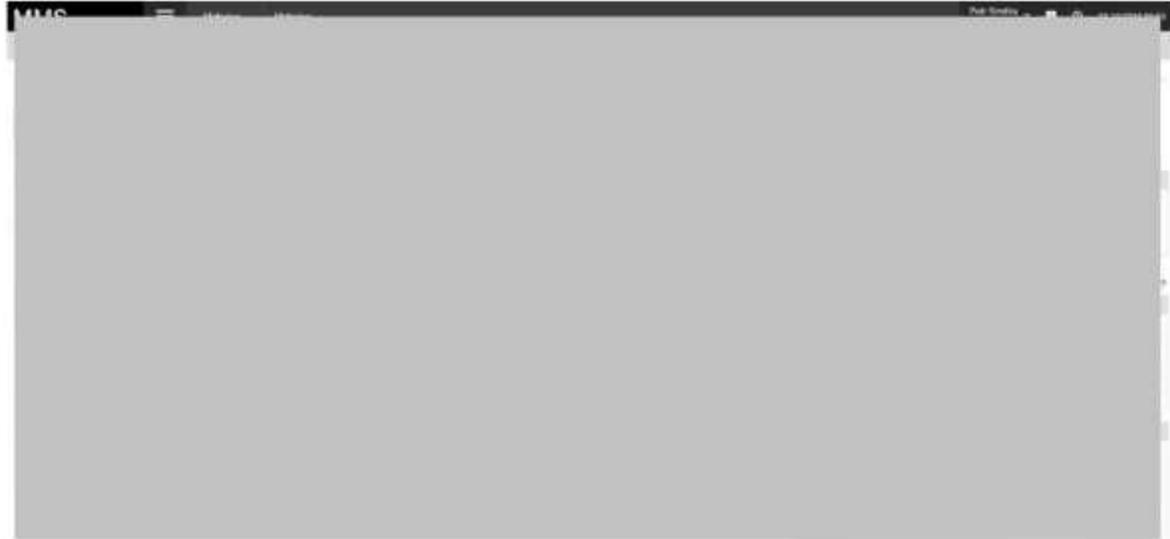
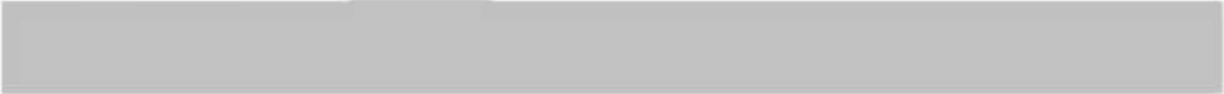


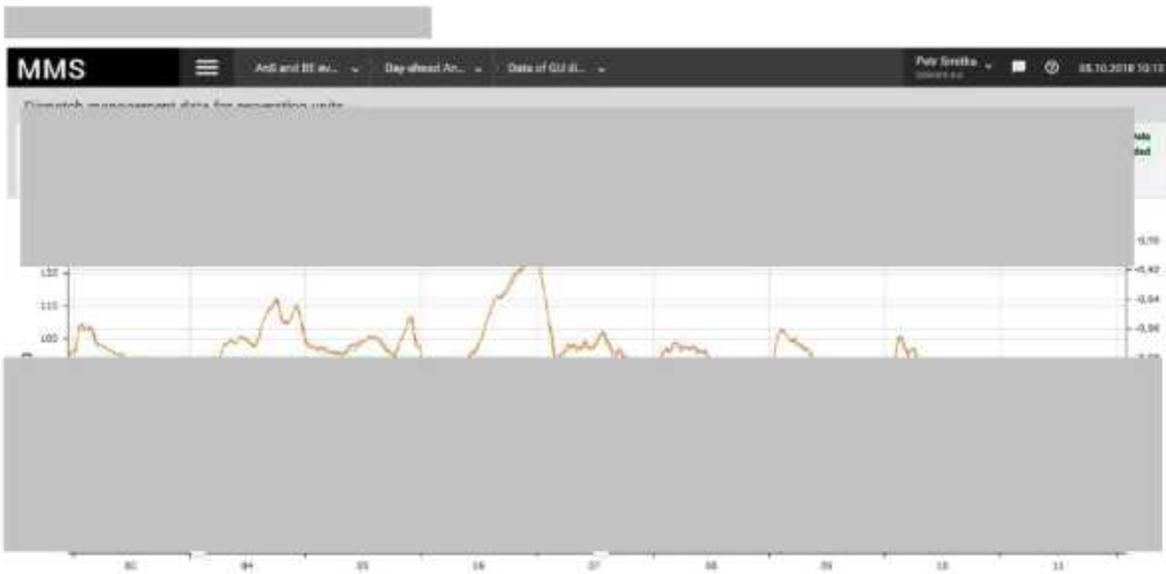


Time series Implicit auction unit price



12.2.2 FlexiGUI





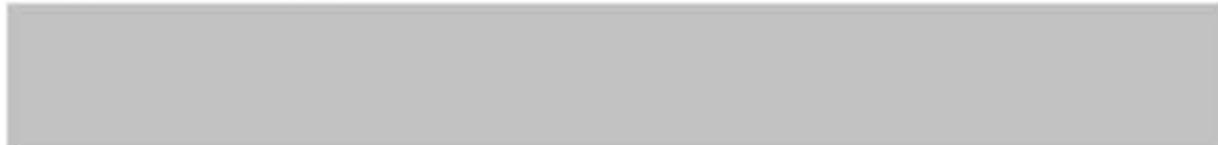
12.2.3 Calculation engine



12.2.4 MS Office integration



12.2.5 Events engine



12.2.6 BPM (Business process management)

With the visual workflow of the Damas Platform, you may define process schedules using inbuilt configuration



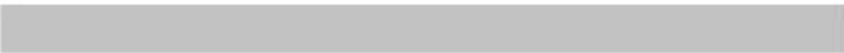
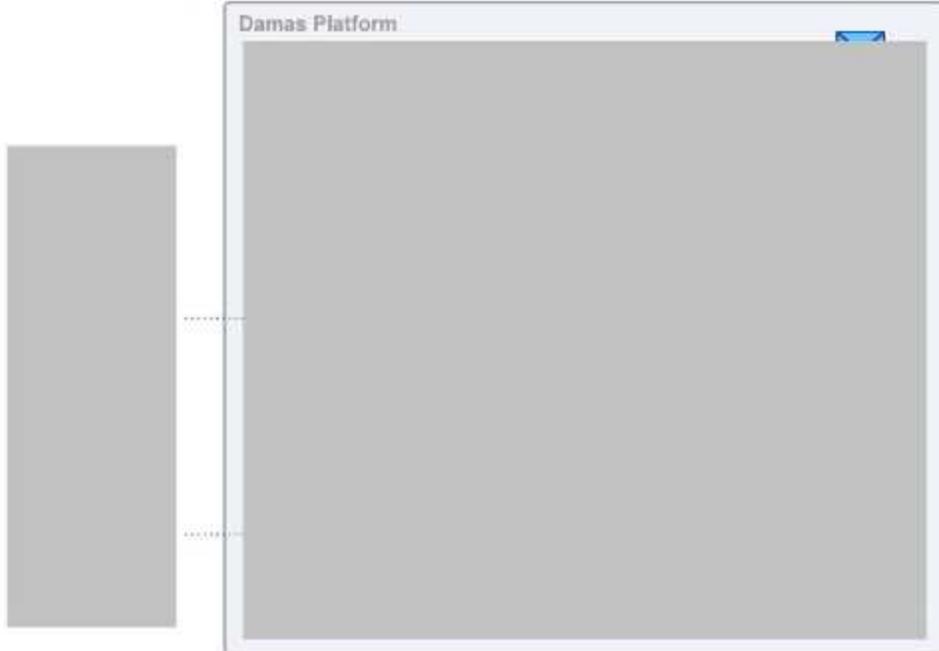
Sample screen for monitoring and control of process execution:



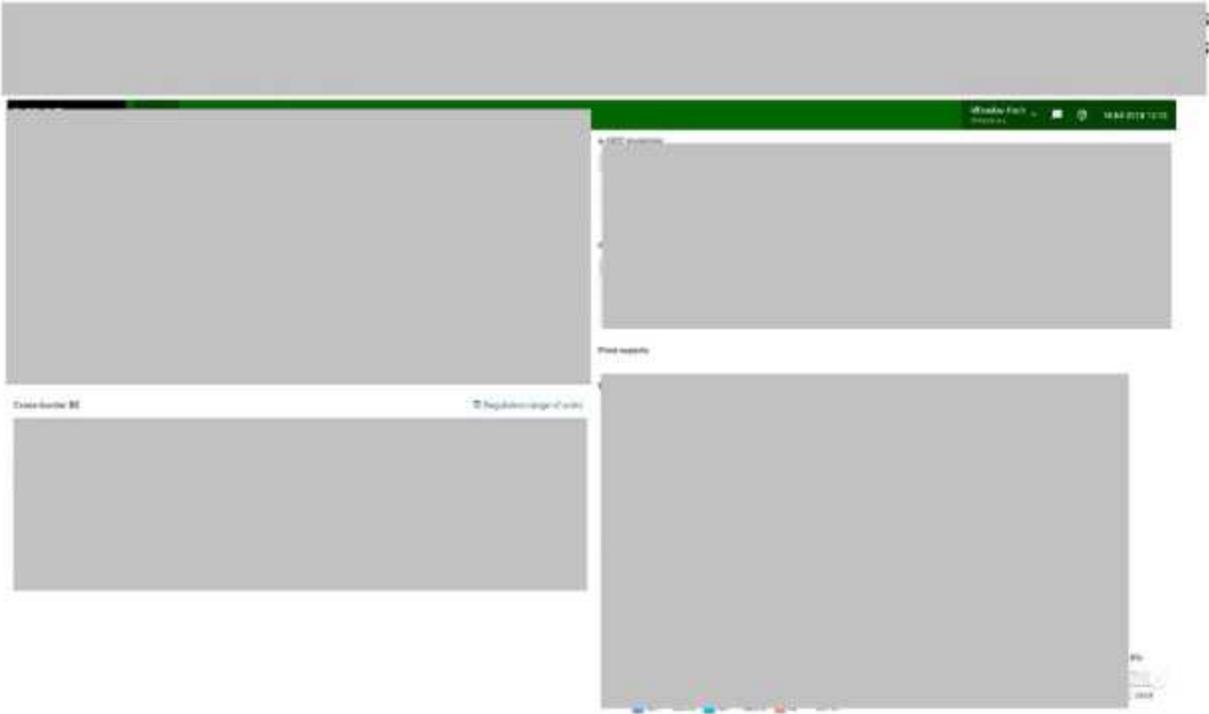
12.2.7 Enterprise integration

[Redacted content]

12.3 Architecture

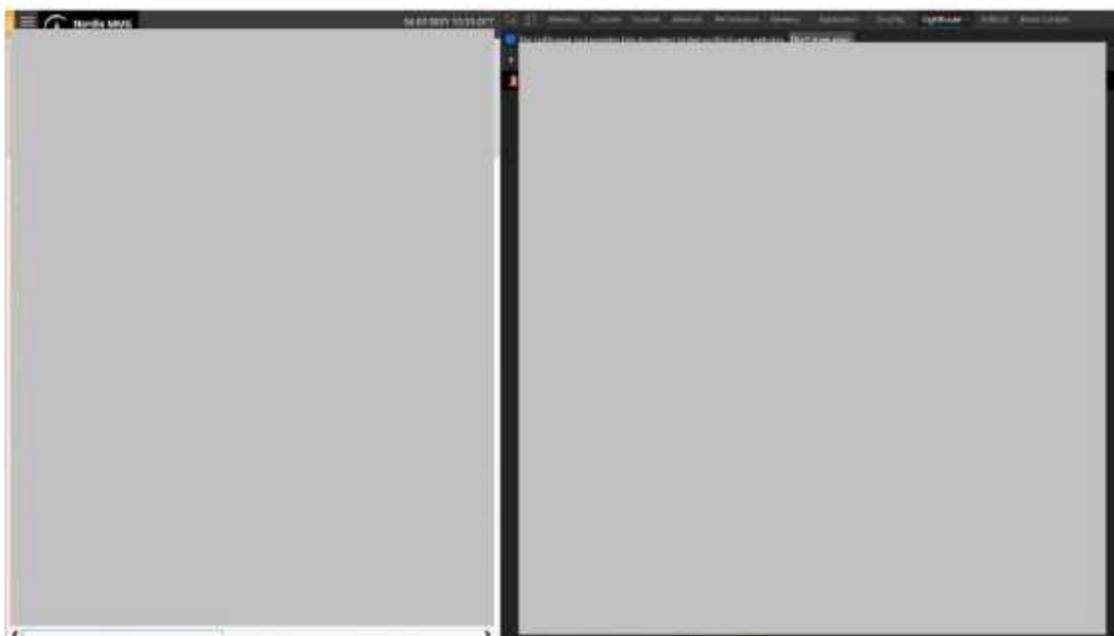


12.4 User interface



12.4.1 Accessibility

The application is designed to be used by users with visual disabilities based on WCAG2 - Guidelines for Information...



12.4.2 GUI technologies

[Redacted content]

12.4.3 Deep linking

[Redacted content]

12.4.4 Icons and colors

[Redacted content]

12.4.5 Automatic refresh

[Redacted content]

12.4.6 Touch control

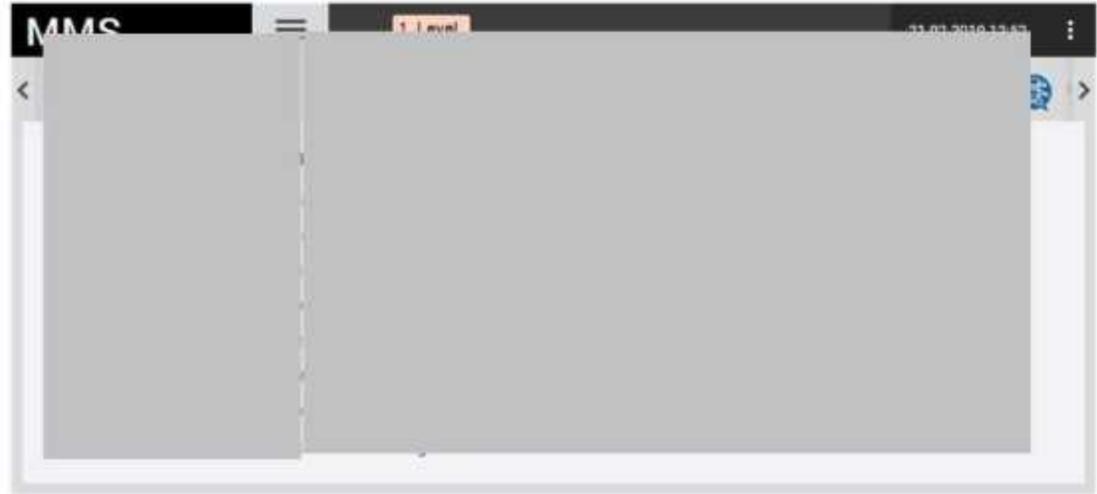
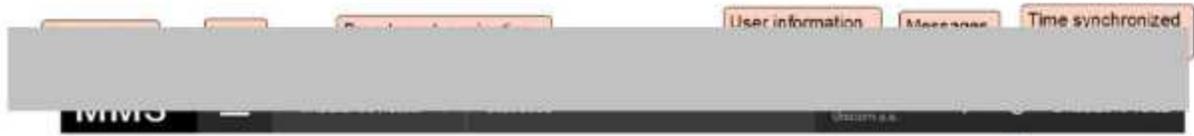
[Redacted content]

12.4.7 Responsive layout

[Redacted content]

12.4.8 Screen structure

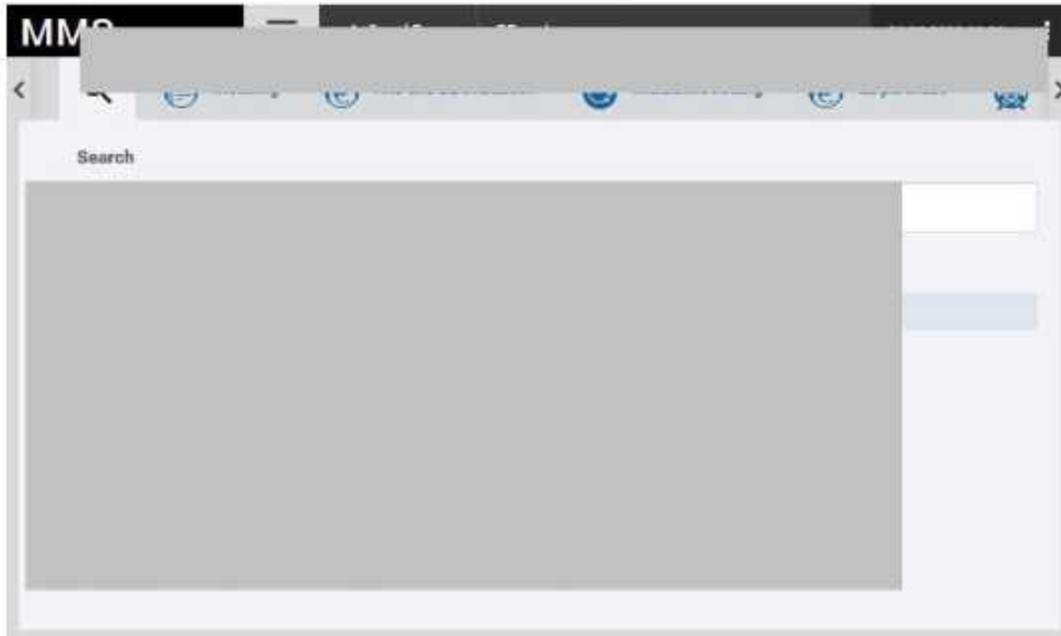
[Redacted content]



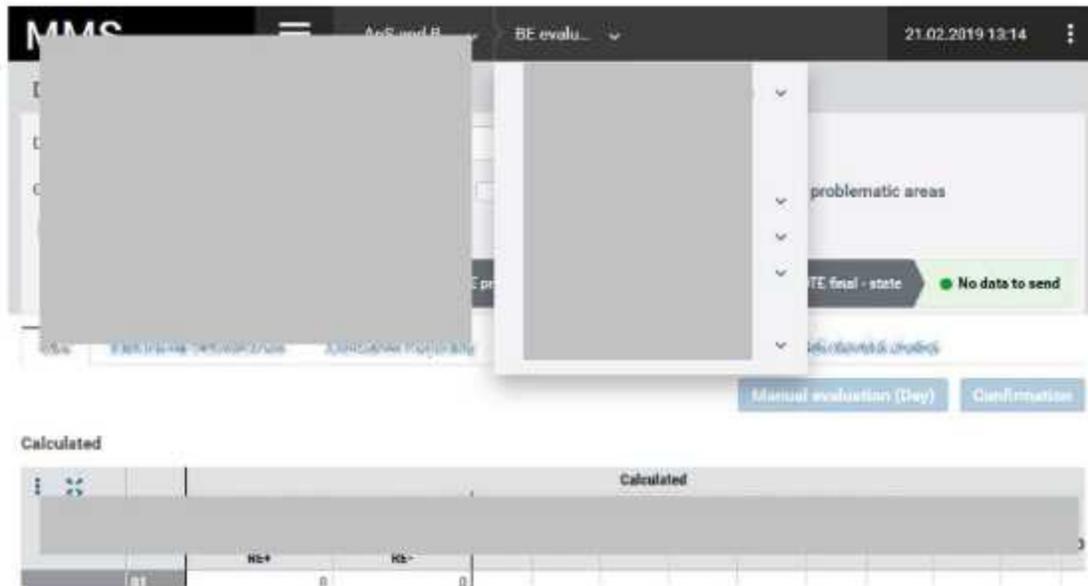
[Redacted text block]

- [Redacted text]
- [Redacted text]

[Redacted text line]



[Redacted text block]

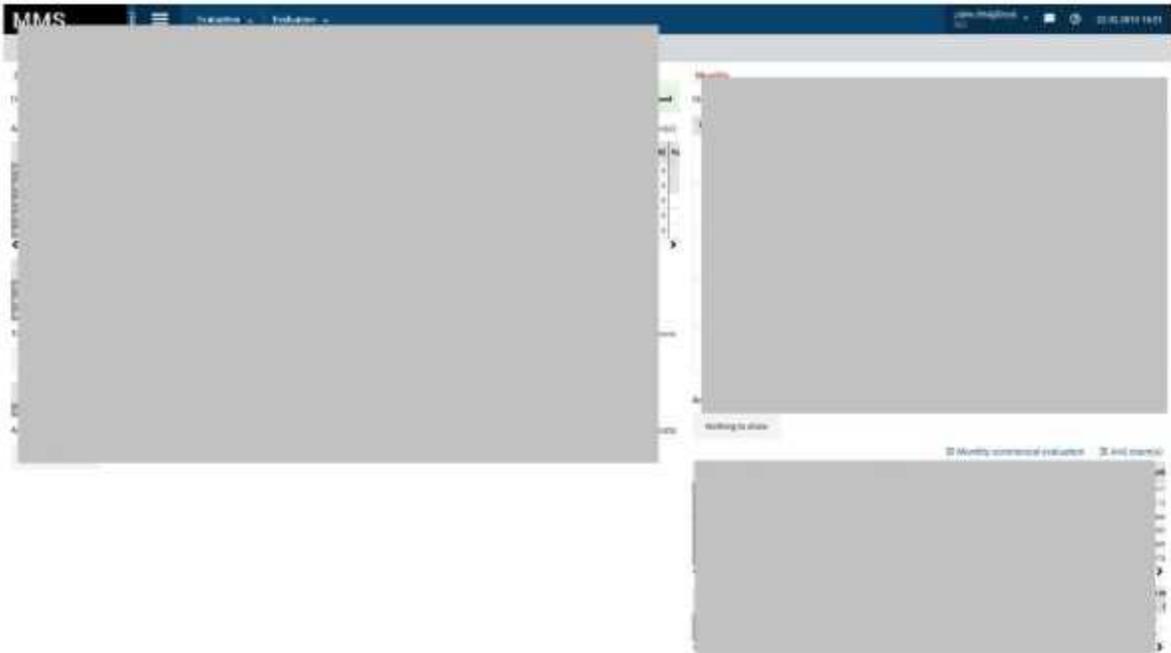
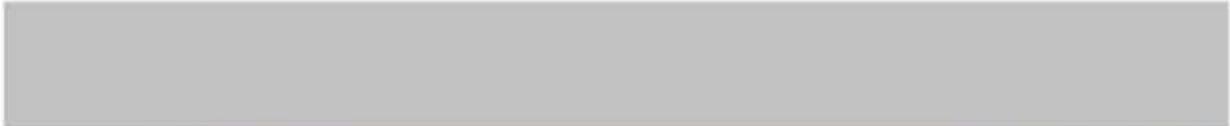


12.4.8.4.1 Data grid screen

Basic screen type for working with data stored in time series.



12.4.8.4.2 Dashboard



12.4.8.4.3 Special and administration screens



12.4.9 Help and context tooltips



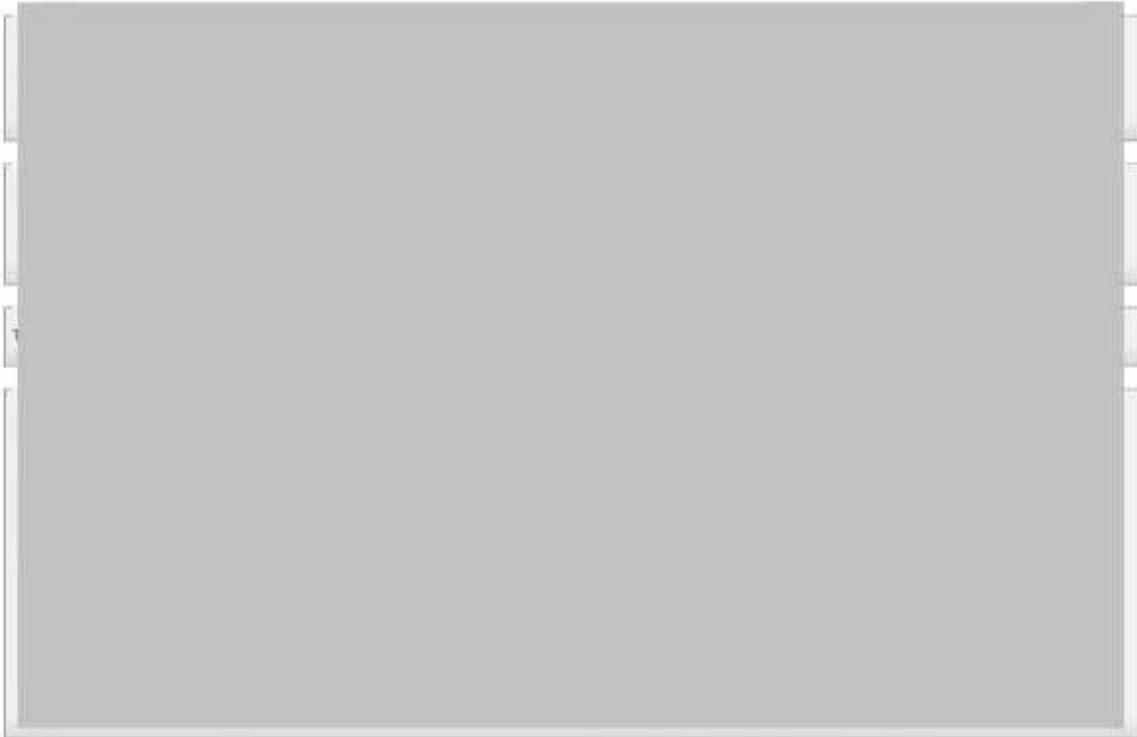
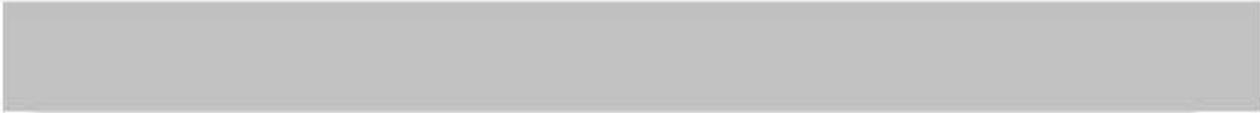
12.4.10 Administration interface



12.5 Time series engine



This section of the page is almost entirely redacted with large grey blocks. A vertical sidebar on the right side contains several orange rectangular buttons with white text, which are partially visible. From top to bottom, the text on these buttons includes: "es", "si", "al", "O", "inc", and "s".



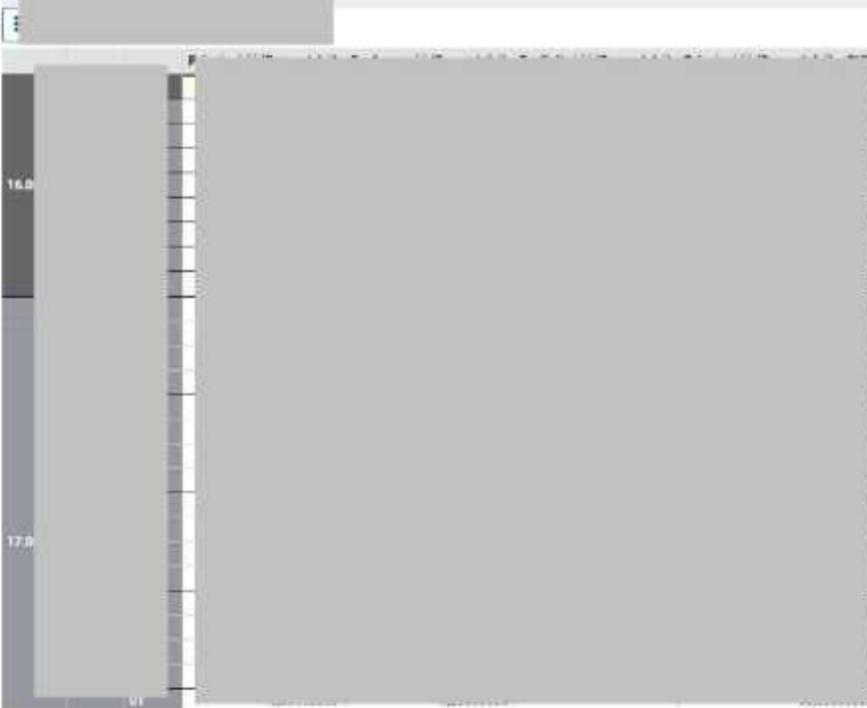
Pohled na časové řady

Období: 01.05.2020 - 31.05.2020

UI elements including a dropdown menu, a table with columns 'PVD', 'Uřadící časová řada bez věcných dimenzí', 'Domas', and 'Unicorn a.s.', and a search input field.

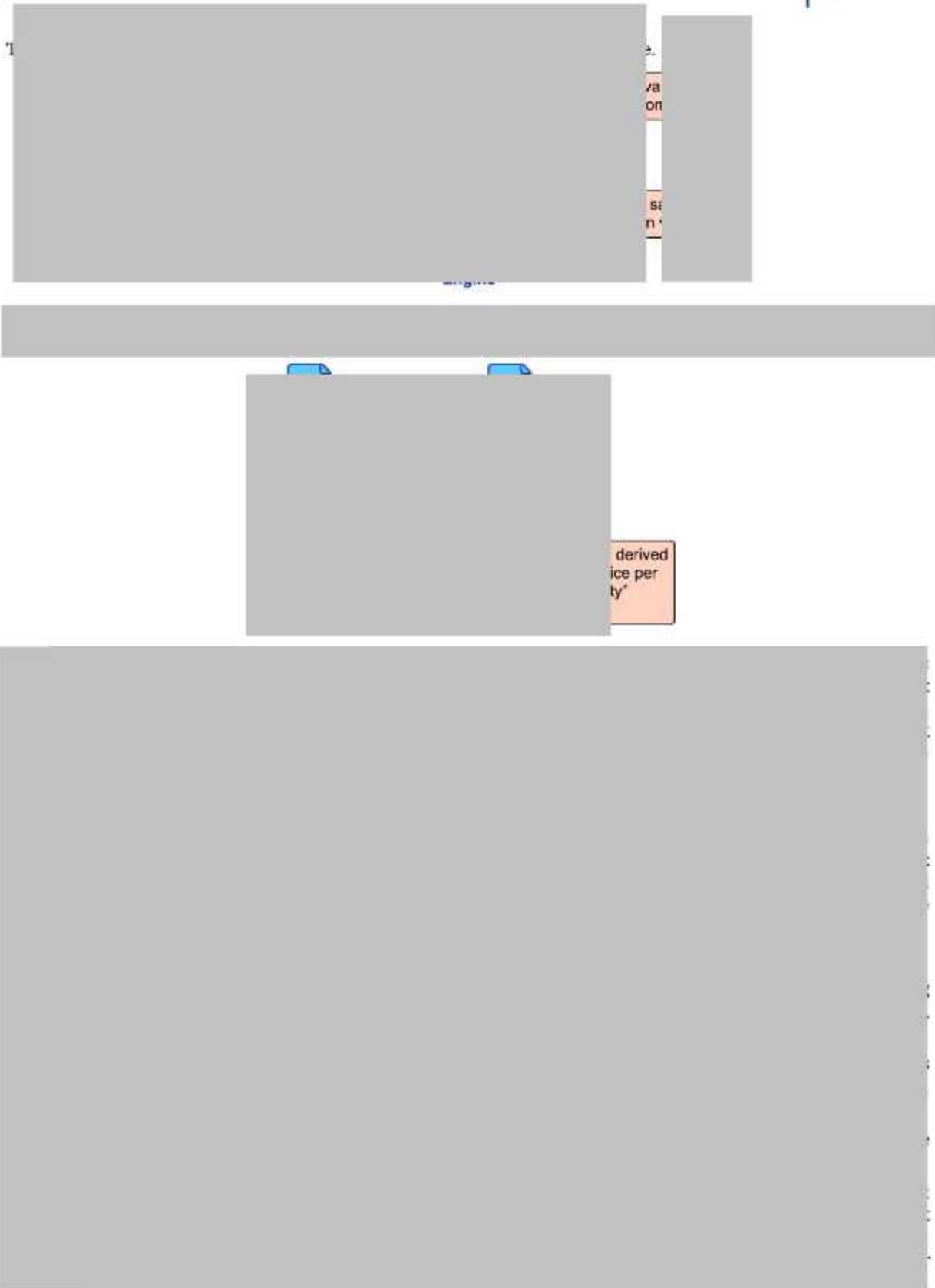
Pouze čí s dynamickou čí bez VD

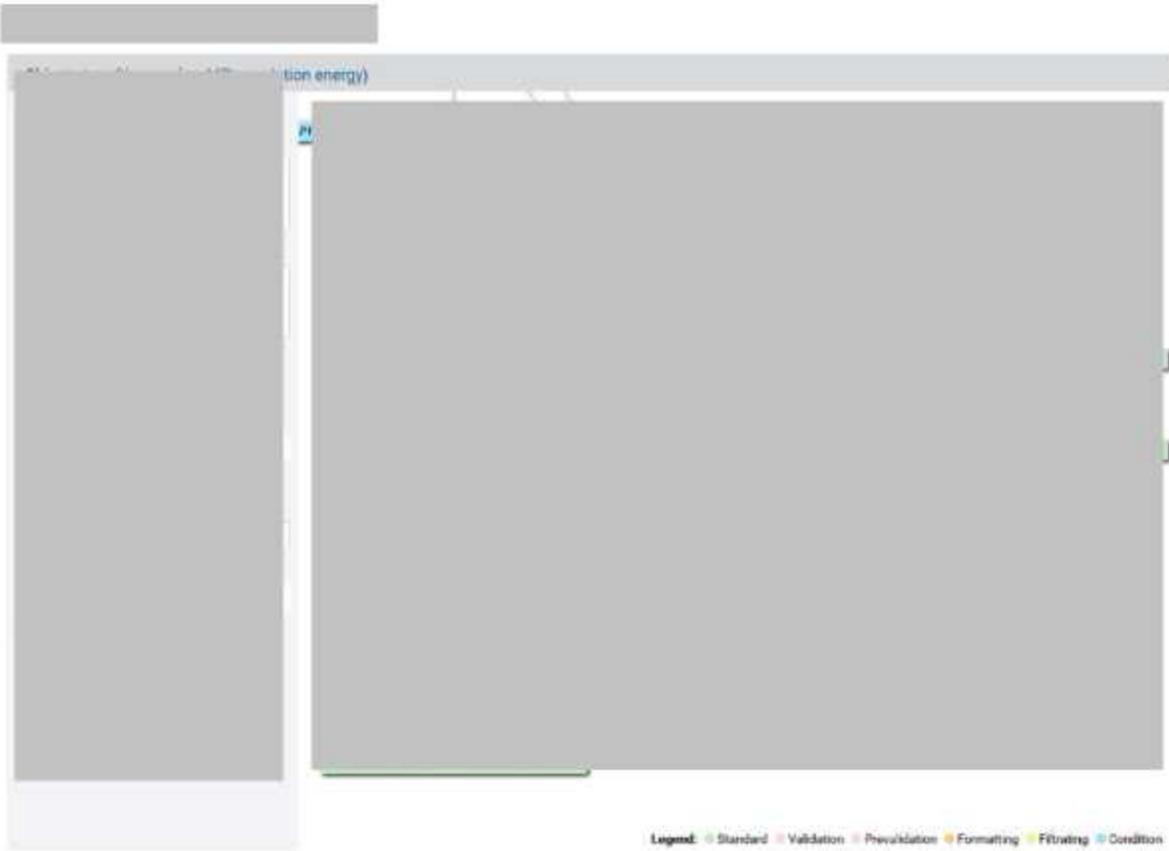
Období: 16.05.2020 - 17.05.2020



12.6 Calculation engine







ion energy)

Legend: Standard Validation Prevalidation Formatting Filtering Condition



Formula Editor

1. Formula

Reset mode Formula is valid

Edit formula Validation Load formula Show differences with original formula Load original formula

2. Parameters

Id	Flow number	Min	Max
Re			
Re			
Dr			
Re			
Pr			
Pr			
M			
En			
En			

Manual generation
 Generation adjustment
 ...ing data

[Redacted content]

Id	Flow number	Generation	Flow number	Min	Max
01					True, False
02					True, False, ...]

Log

[Redacted log content]

[Redacted content]

Function	Description
BASIC UNICORN	
... L-DIV MOD	Basic authentication

Function	Description
CONT(E1, P2)	A A A M M c V (2) A u tto) F s T t I K(TS) T a v L u
REPEAT(E1, TS)	hours. A particular FTO may be a band unit.

Logical functions

--	--

Derived functions

	E1 rounded to the nearest multiple of 10 A P2
--	-----------------------------------------------

Function	Description
Decision functions	
1	E
C	1:E A an
S	c
T	
M	C
E	F en
E	s en
E	b he
E	e ne
E	i
E	F ne
	c
	E is
F	c nt,
	c
	E ys
	f ng
	c
	F
	E be
V) U he
	F he
	f he
	F
C	F
C	F
	F e.
	E
D	> er
	>
	T
I) U he
	f ne
	s
I	T es
C	r er.
I	T
I	T e.
I	t on
C	C
Y	T
F	with an

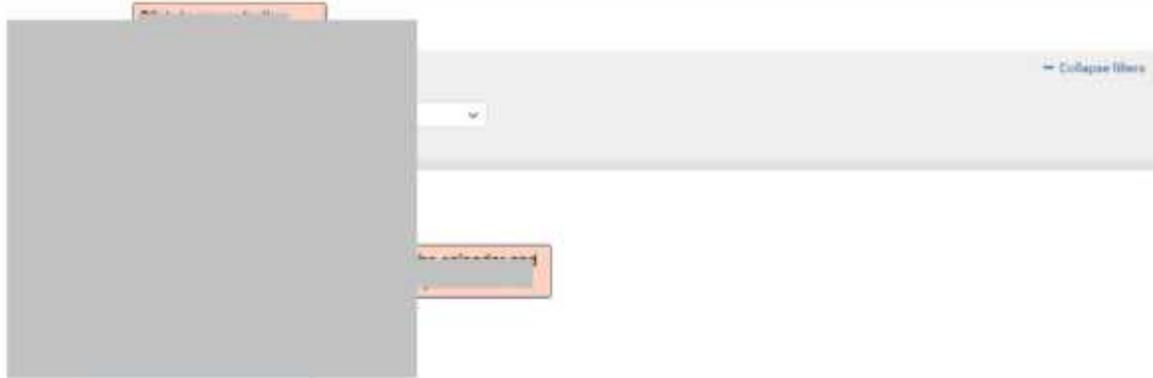
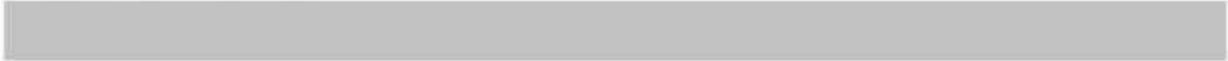
12.7 FlexiGUI



- >
-
- >
-
- >
- >
-
-
-
-

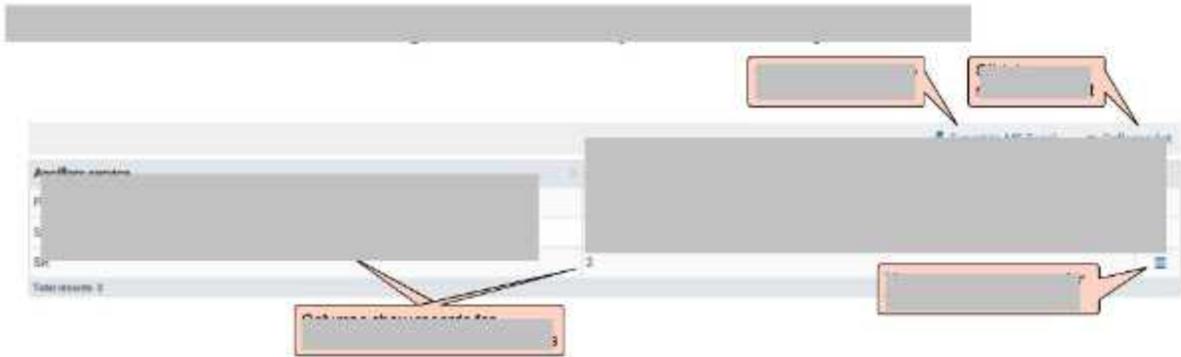
- >
- El
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >
- >

12.7.1 Screen filter

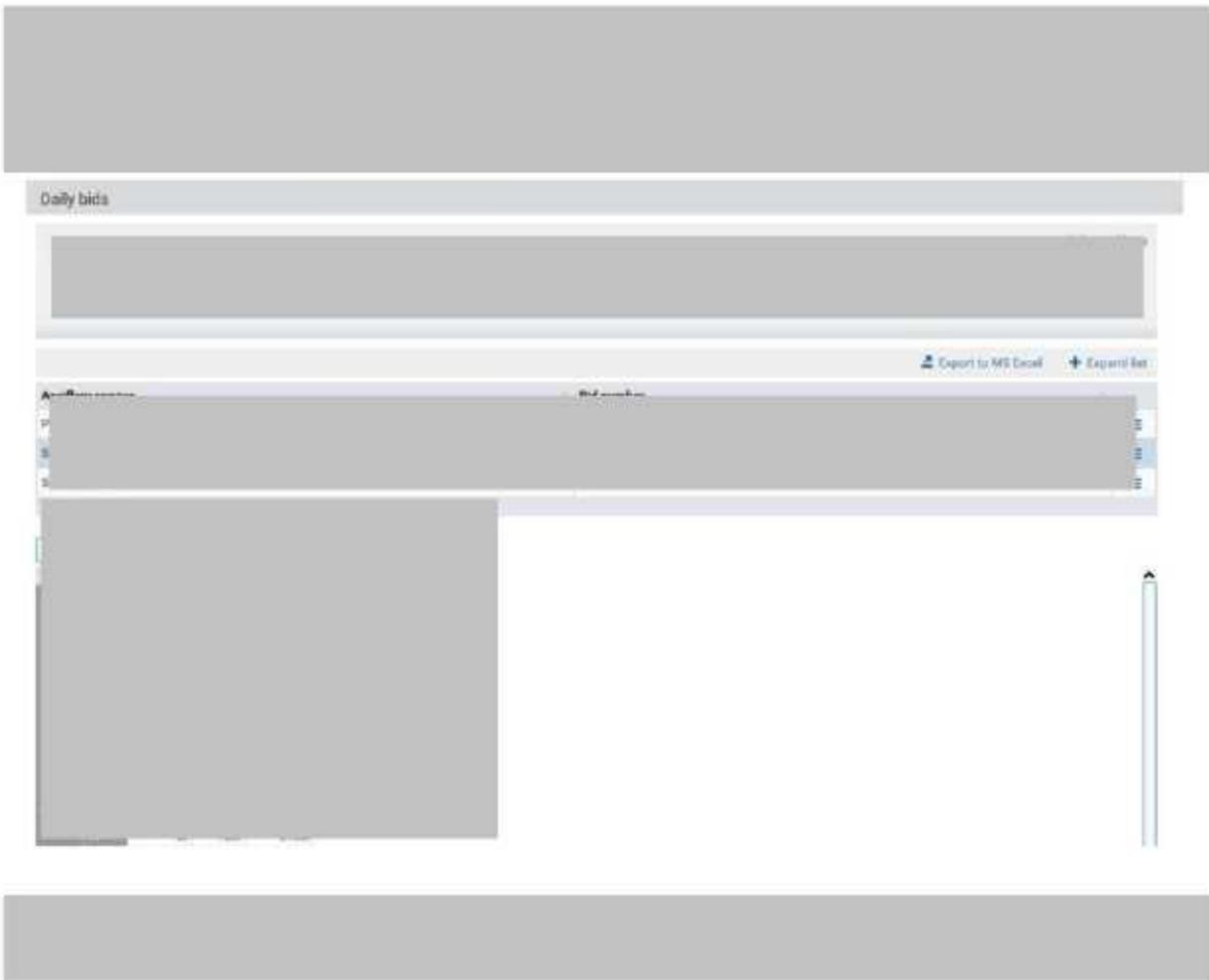


12.7.2 List of values (optional)

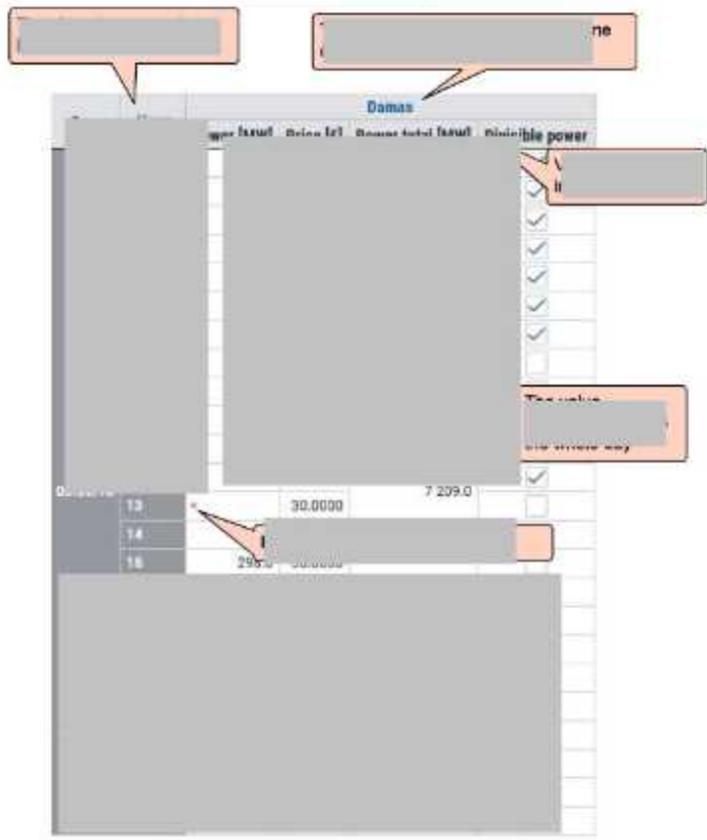




12.7.3 Data grid view



[Redacted]

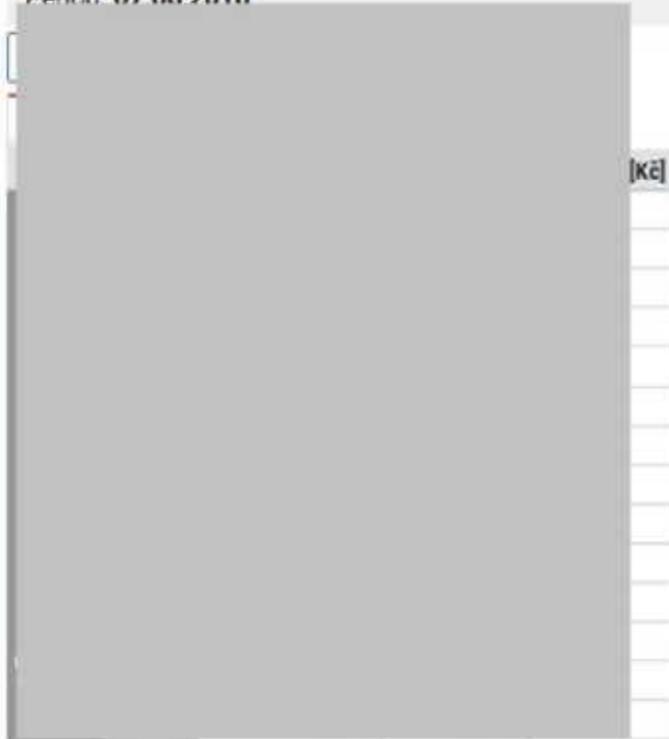


The screenshot shows a software interface for 'Damas'. It features a table with columns: 'upper limit', 'Damas bid', 'Damas total', 'Damas', and 'Damas power'. The table has several rows, with the last three rows (13, 14, 18) highlighted in grey. A pencil icon is positioned over the value '30.0000' in row 14. To the right of the table is a vertical list of checkboxes, with the top one checked. Several callout boxes with orange borders point to specific elements: one points to a redacted box at the top left, another to a redacted box at the top right, a third to a redacted box on the right side, a fourth to a redacted box below the table, and a fifth to a redacted box at the bottom of the table. The interface is surrounded by large grey redaction blocks at the top, bottom, and left.

[Redacted]



Period: 07 06 2018



W
Th
mc
su
the

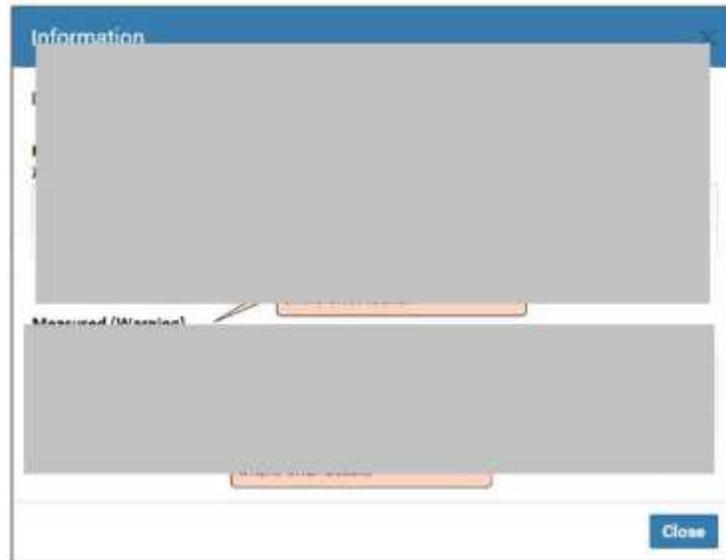


cek,
(for
see



12.7.4 Data submitting

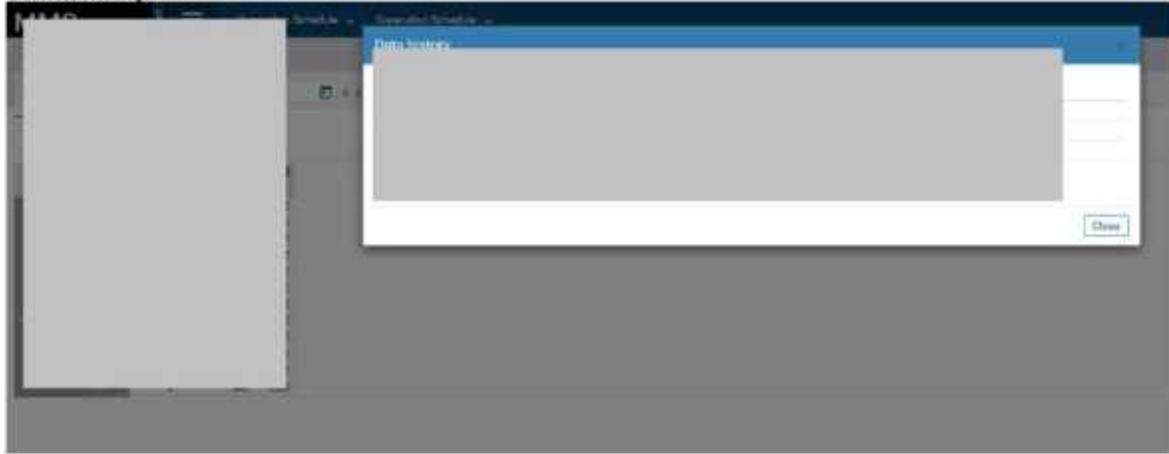
Da
th
Er
If
as



Re	
Wa	
So	a acceptance. Use the nce.
Ha	



Value history:



12.7.5 Highlighting

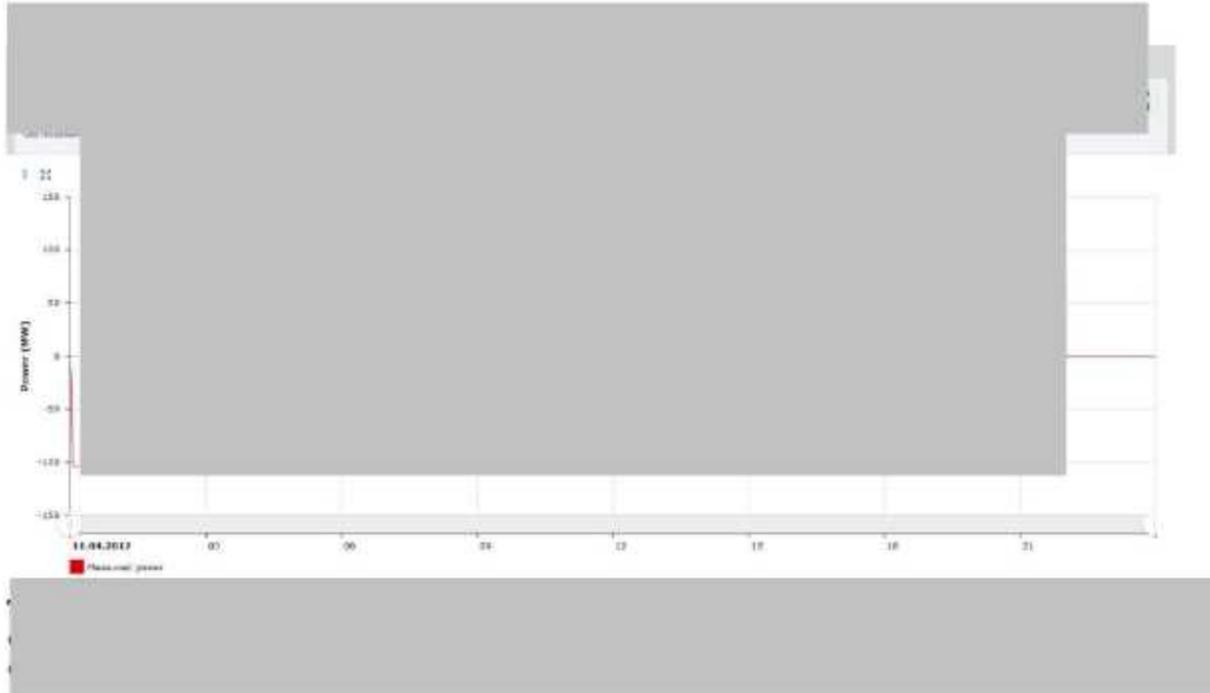
Highlighting	Description	Example
Val rec		00
Inc		,00
Ma		0
Cor		9,00
Cor tha		99,00
Sig		0,00
Cor hig		
Val		
Rec		
Agg		10
Sur		0
Mir		
Ma		
Ave		5



12.7.6 Authorization



12.7.7 Chart view



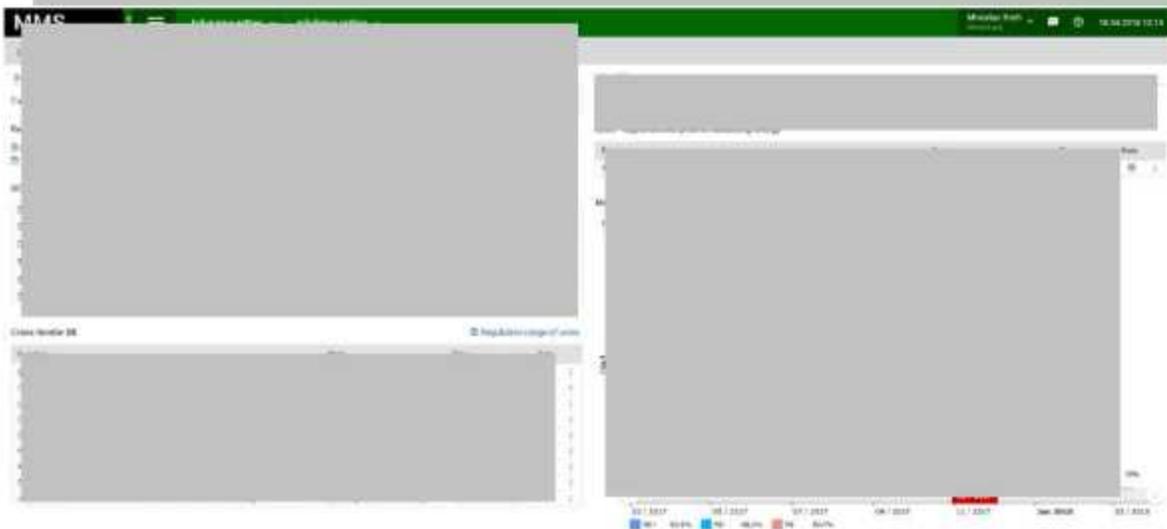
12.7.8 Dashboards and complex screens



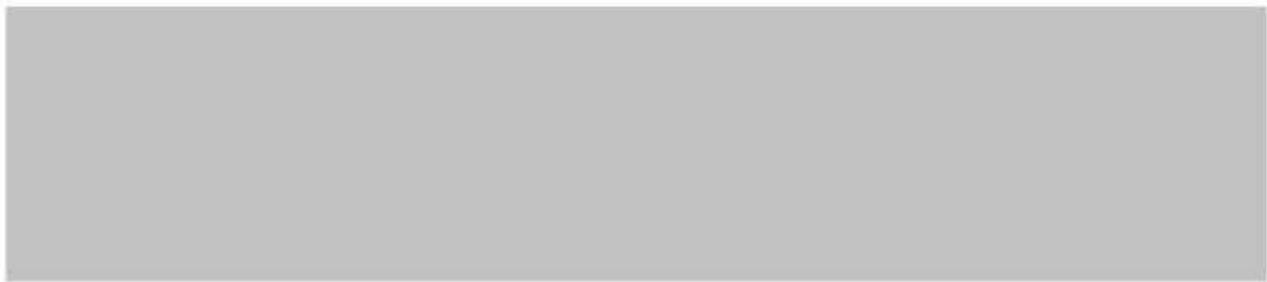
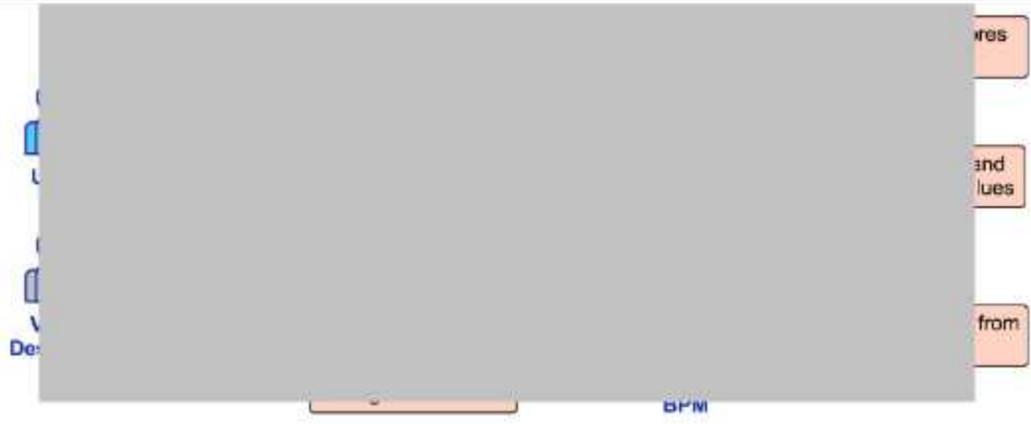


Screen components:

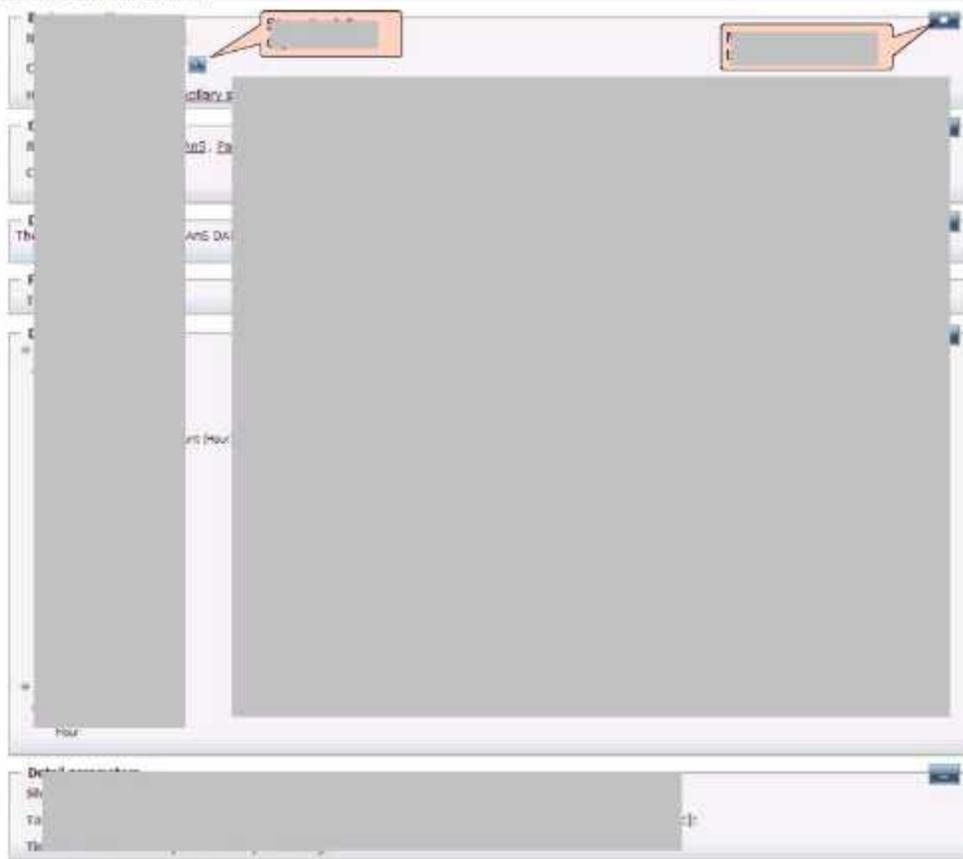
- [Redacted]
- [Redacted]
- [Redacted]
- > [Redacted]



12.7.9 View configurator

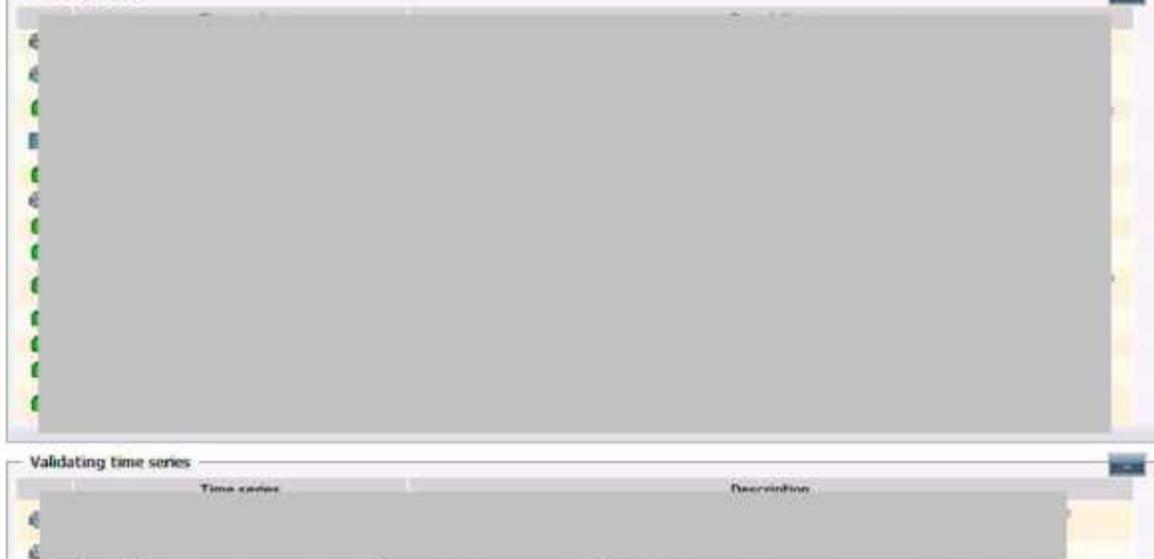


AnS DM1 bid list view definition



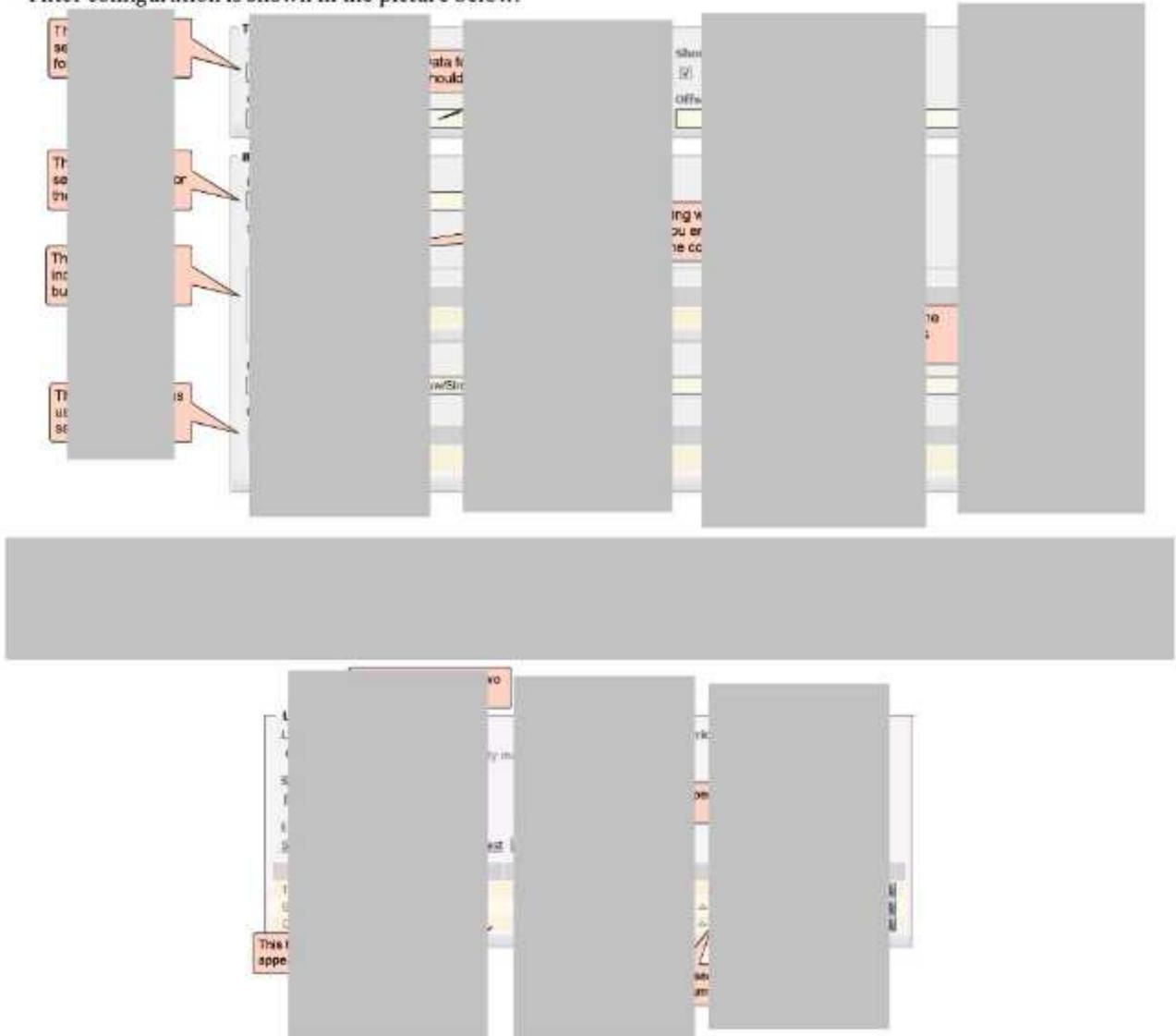
The screenshot shows a software interface for defining a bid list view. It features a central table area that is currently greyed out. To the left of the table is a vertical list of fields, including 'Hour', 'Bidder', 'Bid', 'Bid Type', 'Bid Status', 'Bid Date', 'Bid Time', 'Bid Price', and 'Bid Unit'. Two orange callout boxes are present: one pointing to a 'Filter' button and another pointing to a 'Refresh' button in the top right corner of the table area. Below the table is a 'Definition' section with a 'Description' field.

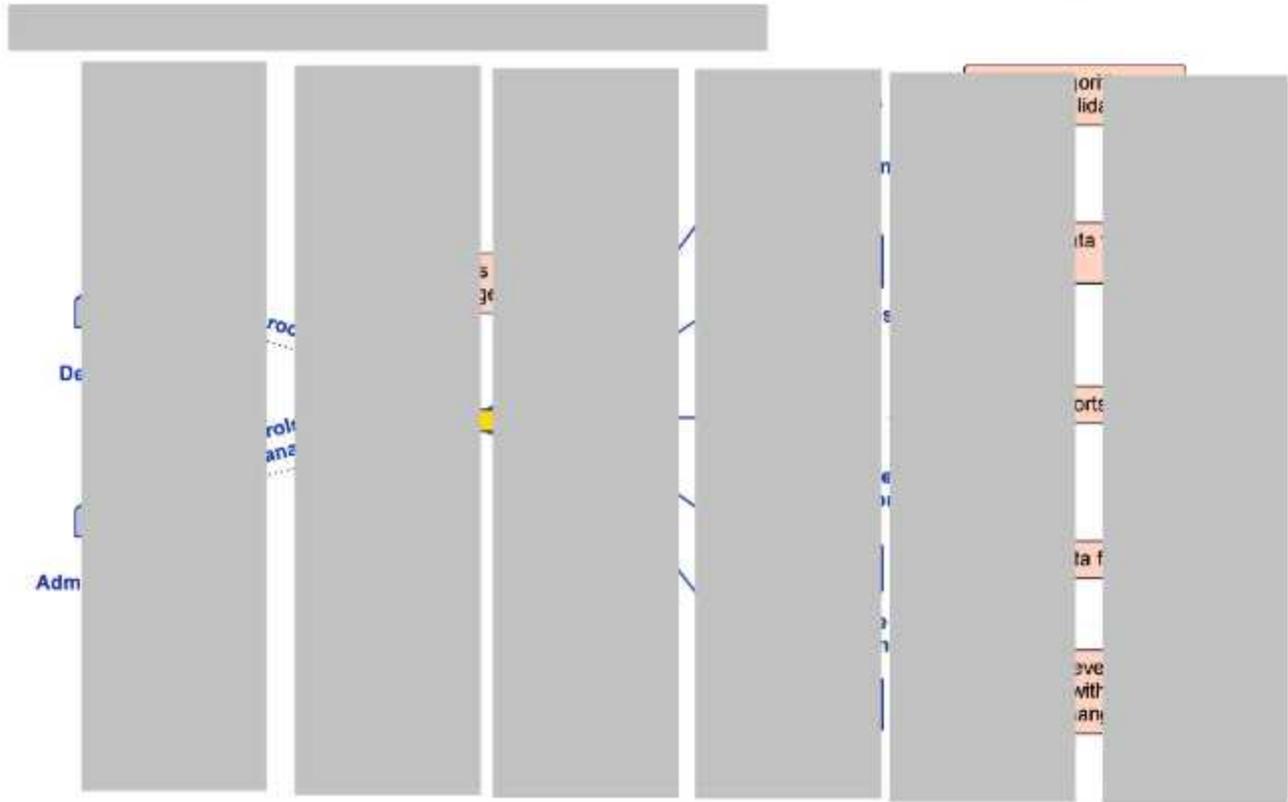
Time series set

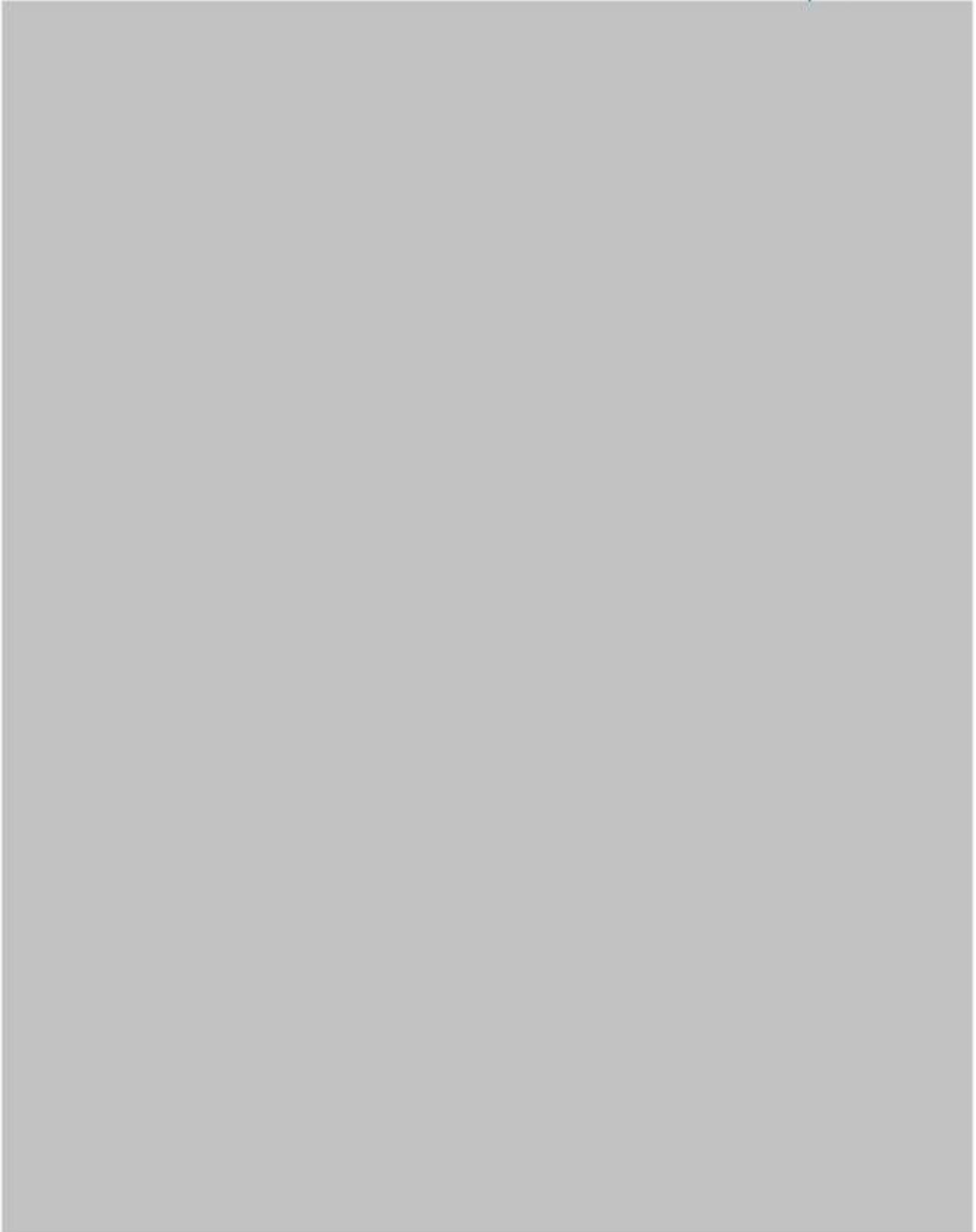


The screenshot displays two stacked interface sections. The top section, 'Time series set', shows a large table with a greyed-out main area and a vertical list of items on the left side. The bottom section, 'Validating time series', shows a table with two columns: 'Time series' and 'Description'. The table content is greyed out.

Filter configuration is shown in the picture below.









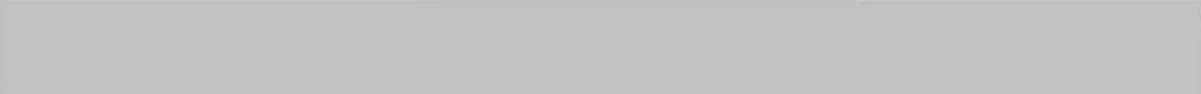
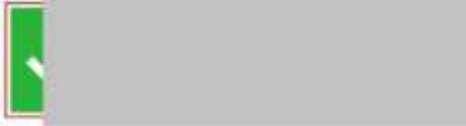
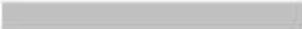
12.8.1 Process diagram





12.8.2 Used icons





Icon **State description** **Type*** **Process Bar** **Compact View**



Icon	State description	Type*	Process Bar	Compact View
				
				
				
				
				
				
				
				

* B - basic phase, A - advanced phase for indication of non-normal operating situation

[Redacted]

[Redacted]

[Redacted]

Icon	Description
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]
	[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

• 

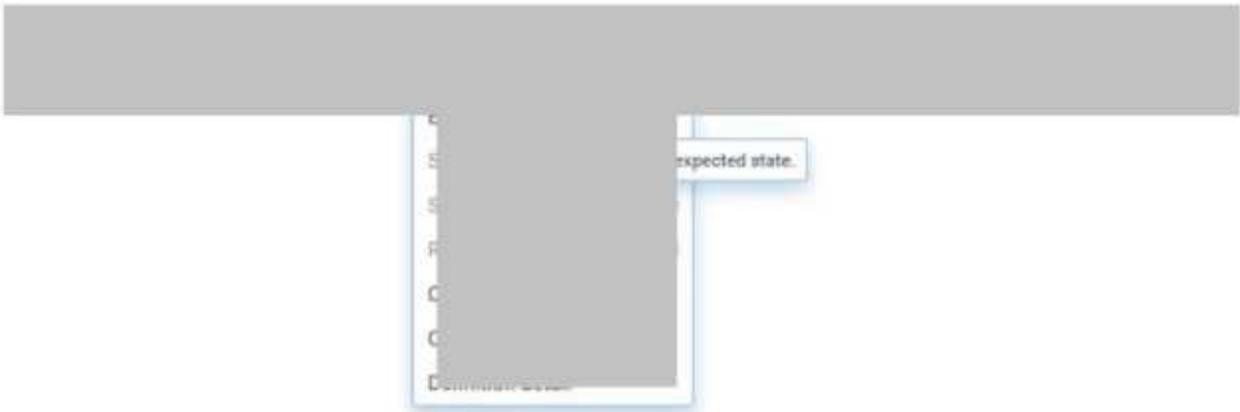


12.8.3 Process instance detail

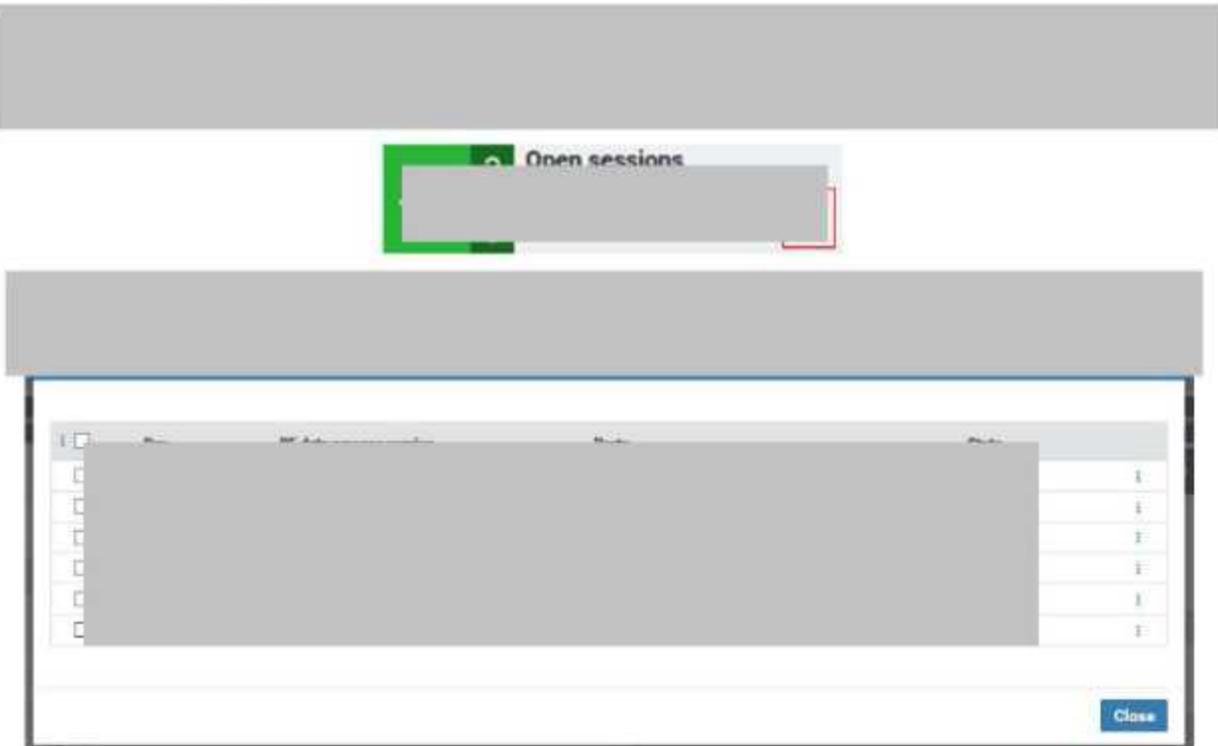


12.8.4 Context menu

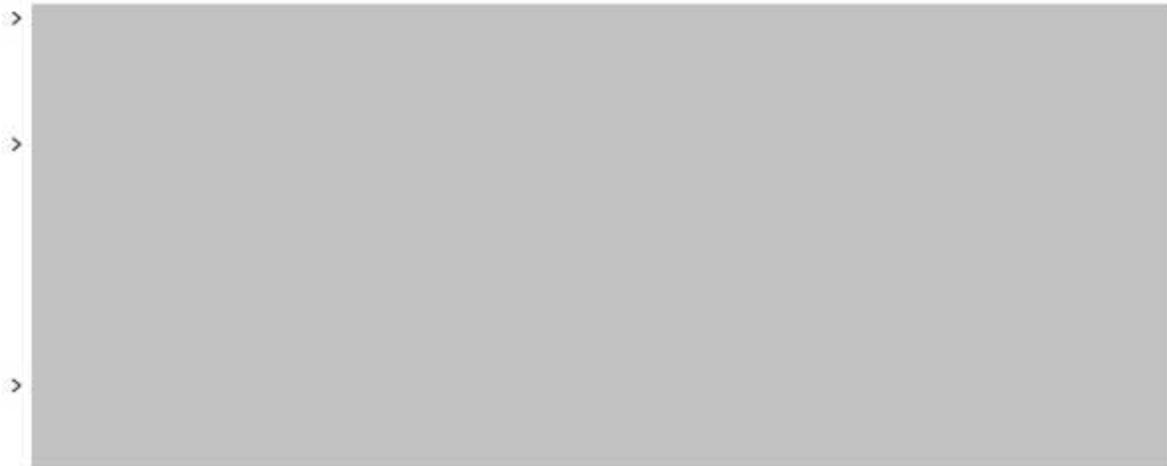




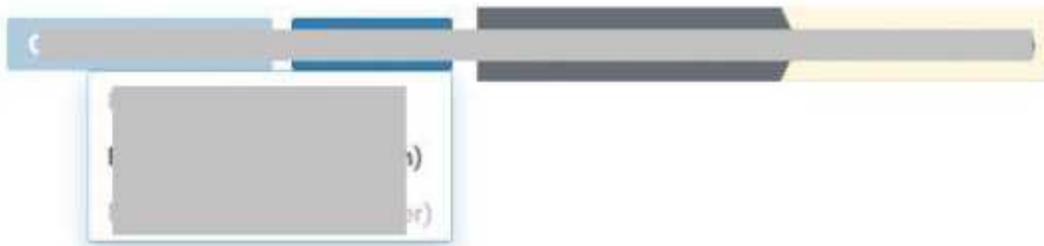
12.8.5 Multiple process control window



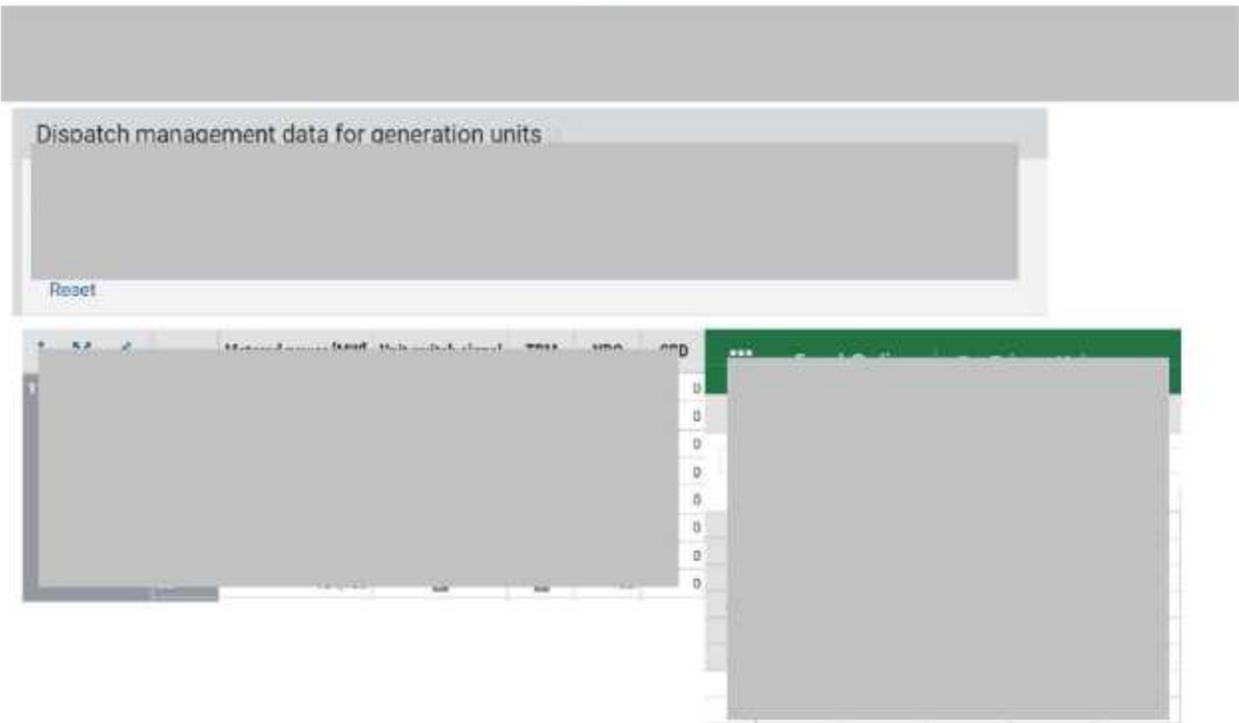
12.8.7 Process bar



12.8.8 Process button



12.9 Microsoft Office integration



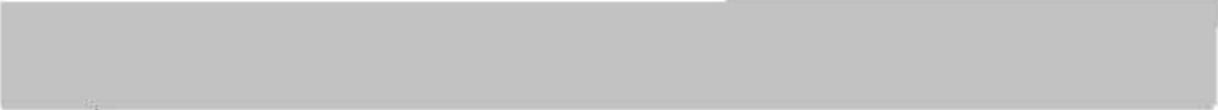
The screenshot shows a web application interface. At the top, there is a grey header bar. Below it, a section titled "Dispatch management data for generation units" contains a large greyed-out area. A "Reset" button is located below this section. At the bottom, there is a table with a green header and a greyed-out body. The table has several columns, with the last column containing the number "0".

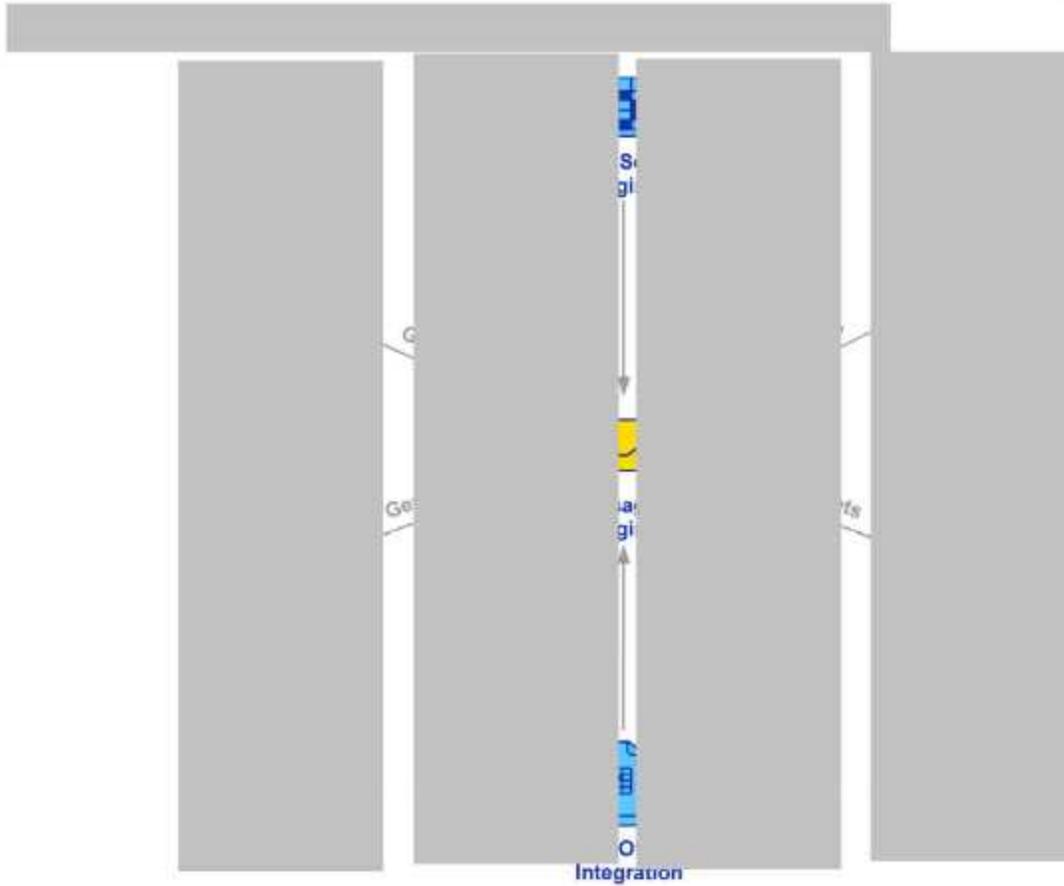


	A	B	C	D	E	F	G	H
1		Data		Energy Mark			Energy Mark	
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
25								
26								

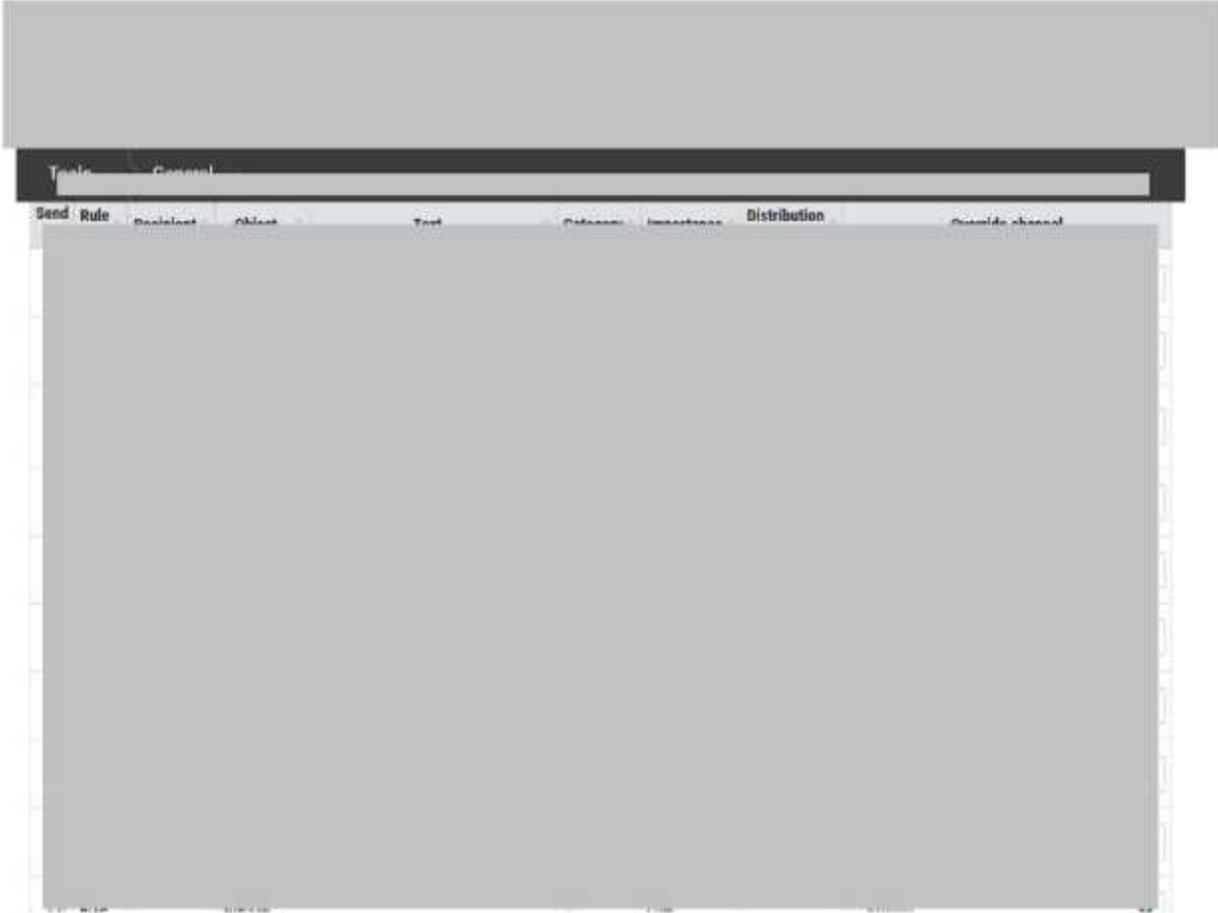


12.10 Events engine

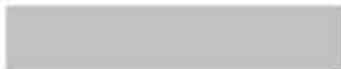








12.11 Enterprise integration



- [Redacted]
- [Redacted]

[Redacted]

- [Redacted]
- [Redacted]

[Redacted]

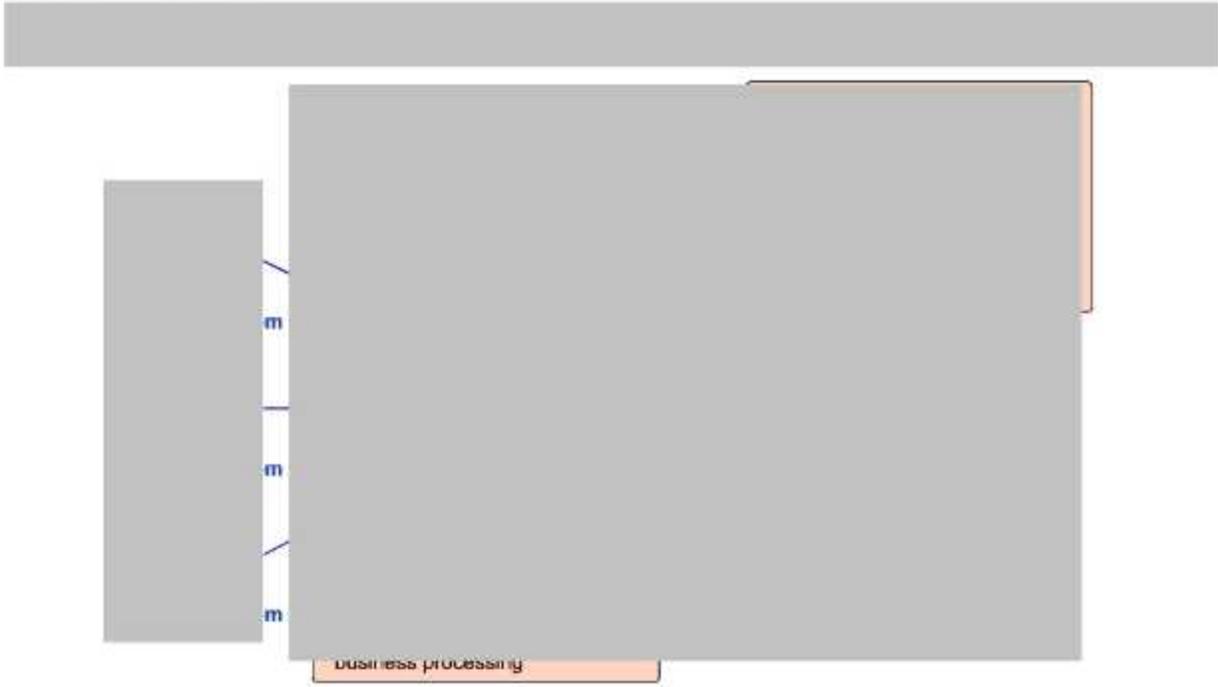
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

12.11.1 Communication channels

[Redacted]

[Redacted]

12.11.2 Key features



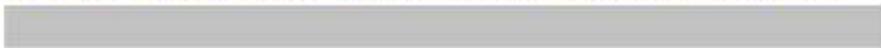
12.11.3 Data reception separated from business processing



12.11.4 Scalability and performance



12.11.5 Input processing, validations and acknowledgement

- 
1. 
 2. 

- 3. S
- 4. I
- 5. S
- 6. A
- 7. I
- 8. C
- 9. C
- 10. I



12.11.6 Separate outgoing communication



12.11.7 Configurability

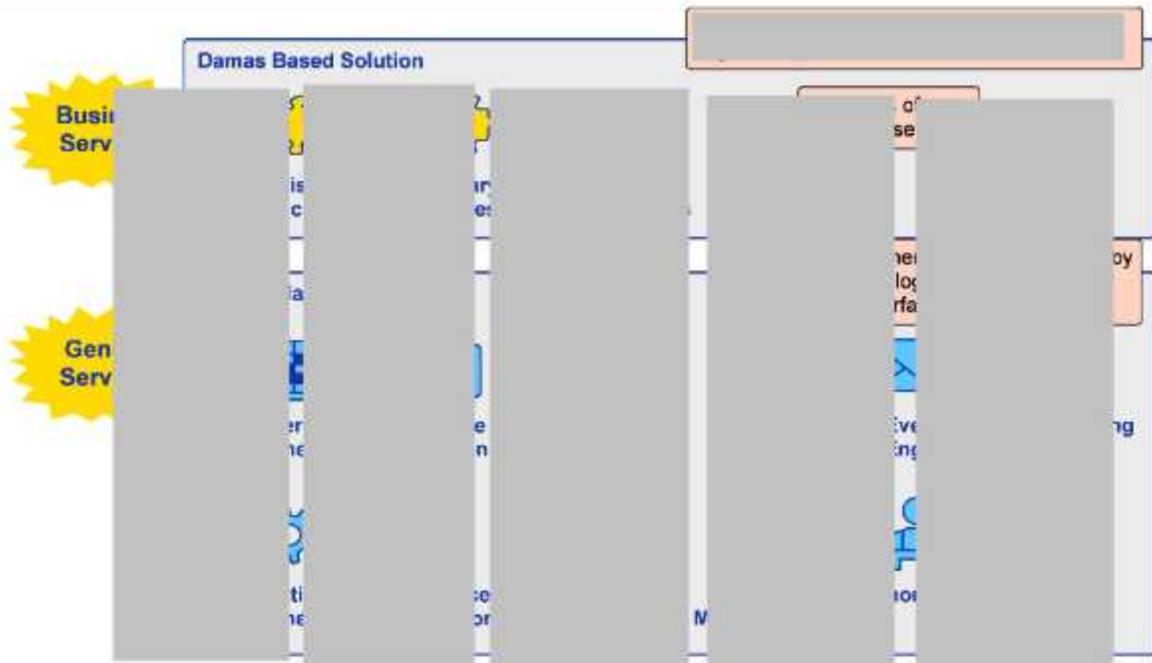


12.11.8 Data flow register and monitoring





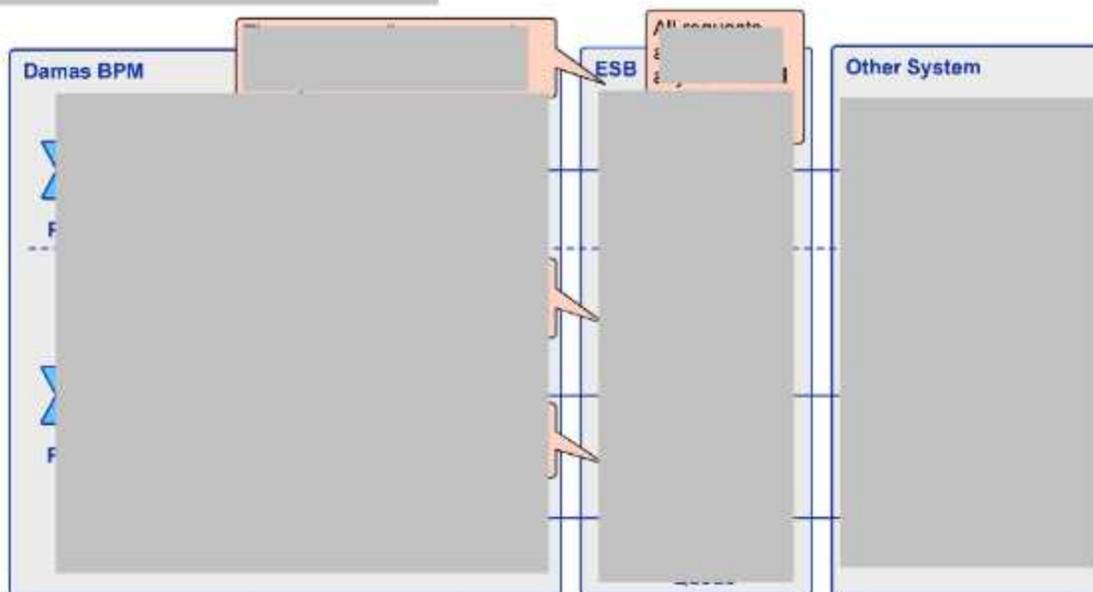
12.11.9 SOA concept

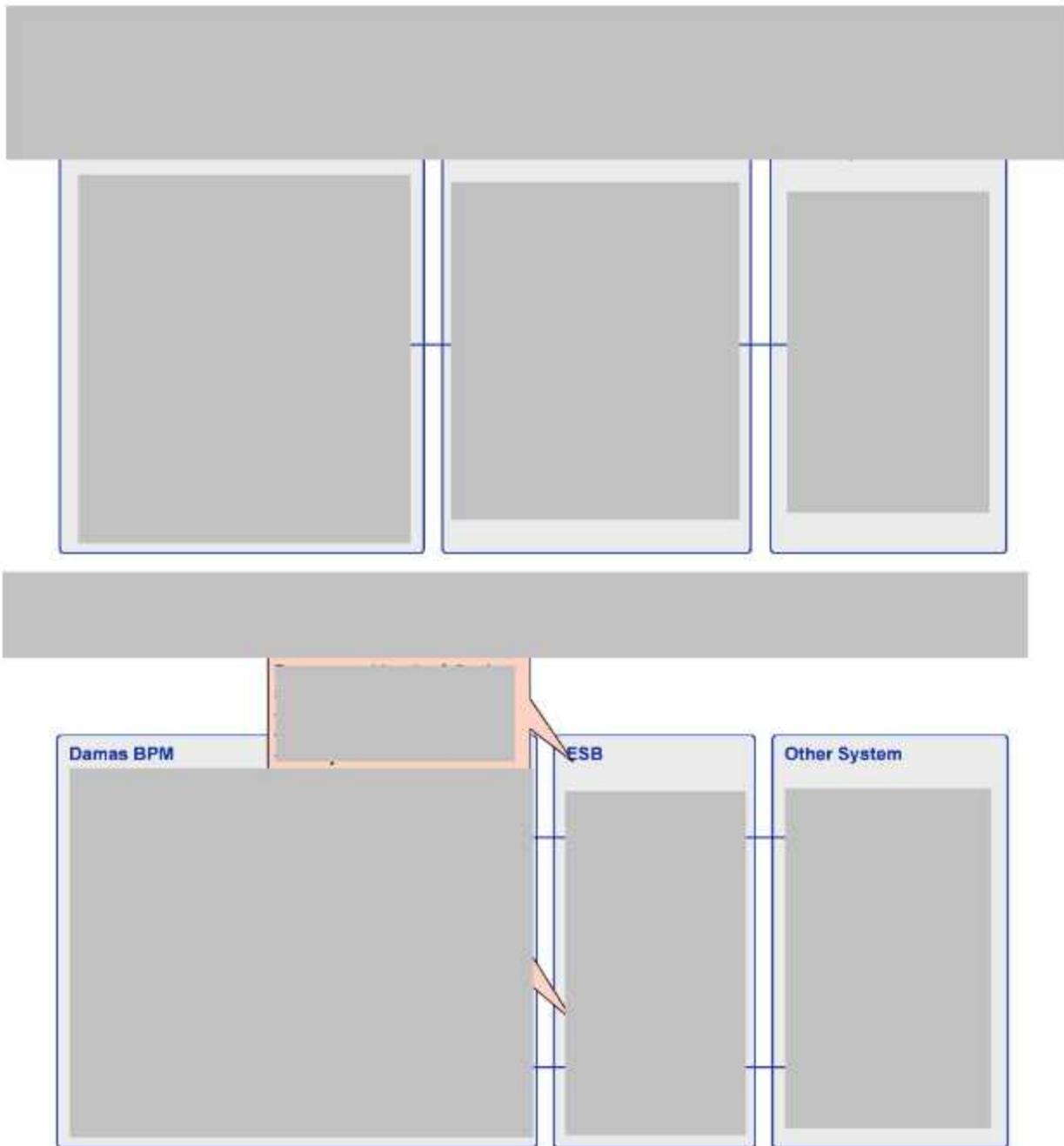


12.11.10 Enterprise service bus (ESB)



12.11.11 Process integration patterns





12.11.12 Dataflow design and configuration



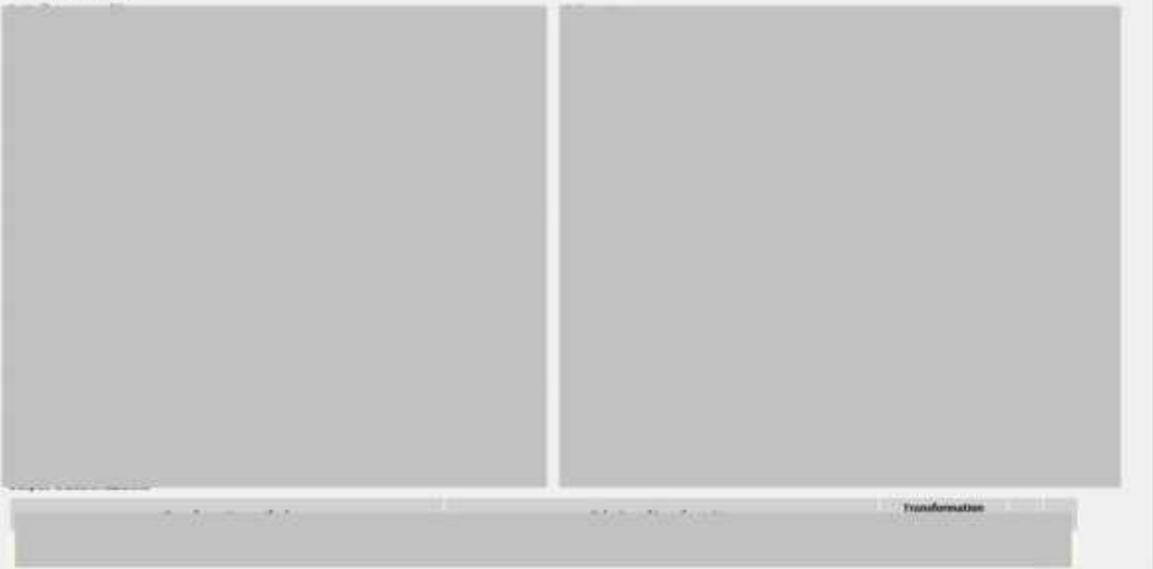




Specific properties



Data flow configuration



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

Output transformations

Transformation method	Selection of transformation
[Redacted]	[Redacted]

[Redacted text block]

12.12 Security

12.12.1 Authentication

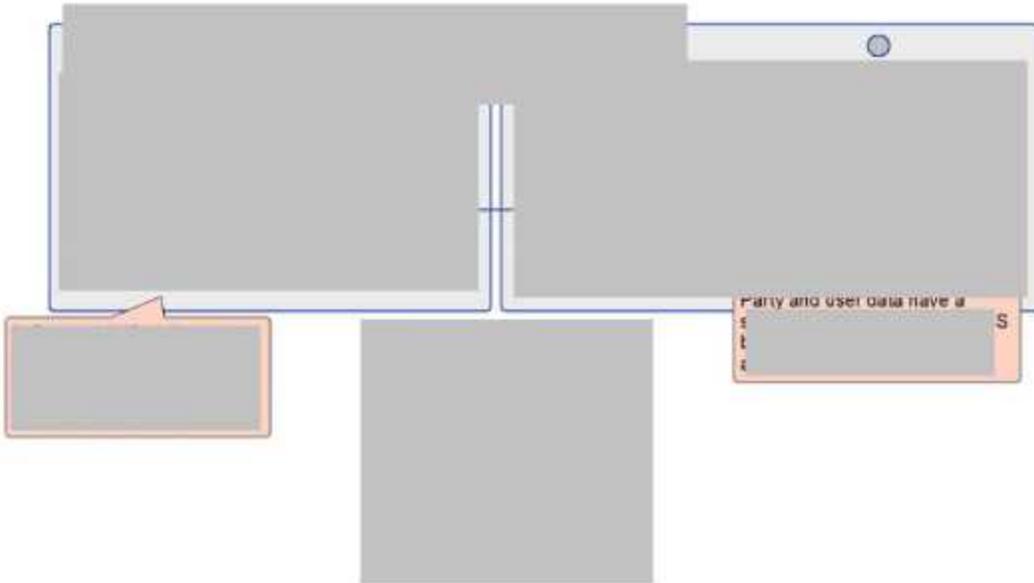
[Redacted content]

12.12.2 Authorization

[Redacted content]

12.12.3 Other

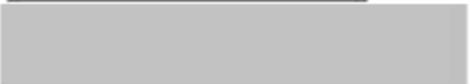
12.13 Reference and master data management





- [Redacted]
- [Redacted]

12.13.1 Reference data and business rules configuration

A table with three columns labeled "Code", "Name", and "Variable". The table content is redacted with a solid grey color. To the right of the table is a button labeled "Nothing to show".



12.13.2 Master data



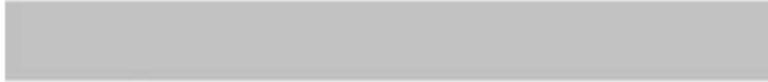
12.14 Calendar



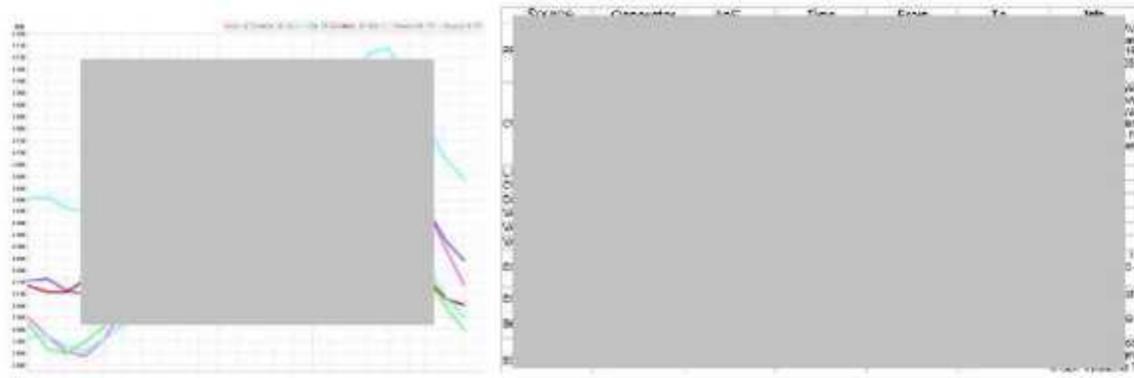


12.15 Reports



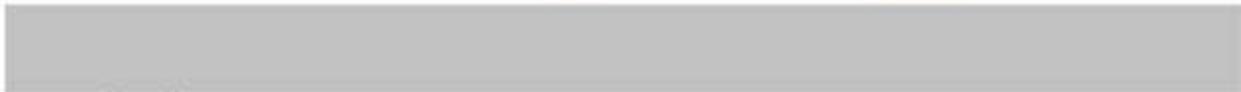
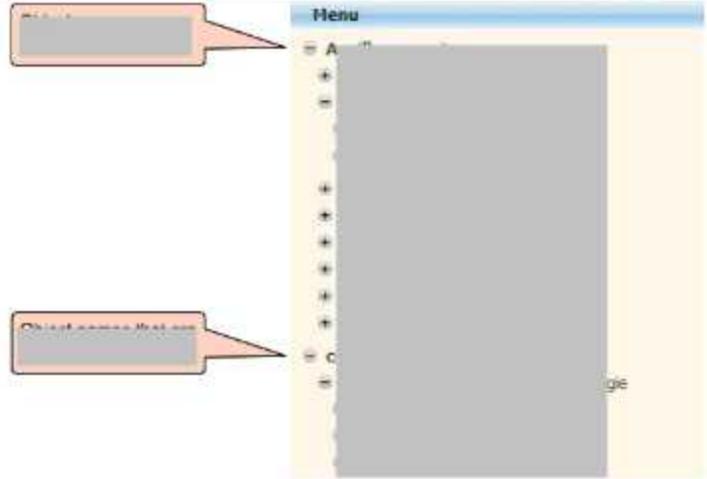


Date: 23.03.10



12.16 Multilingual support





12.17 Multi currencies support





	Validty	Code	Name	Short name	Order
NO					



	Currencies					
	CZK	EUR	SEK	DKK	NOK	GBP
NO13						
NO14						
NO15						
NO16						
NO17						
NO18						
NO19						

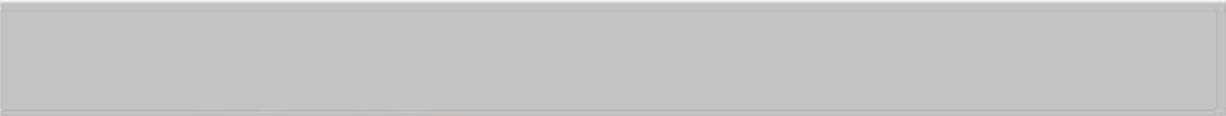




12.18 12.12.2 Metadata management

metadata as standard source codes.





Selection of objects for export

Selected object classes: BUL

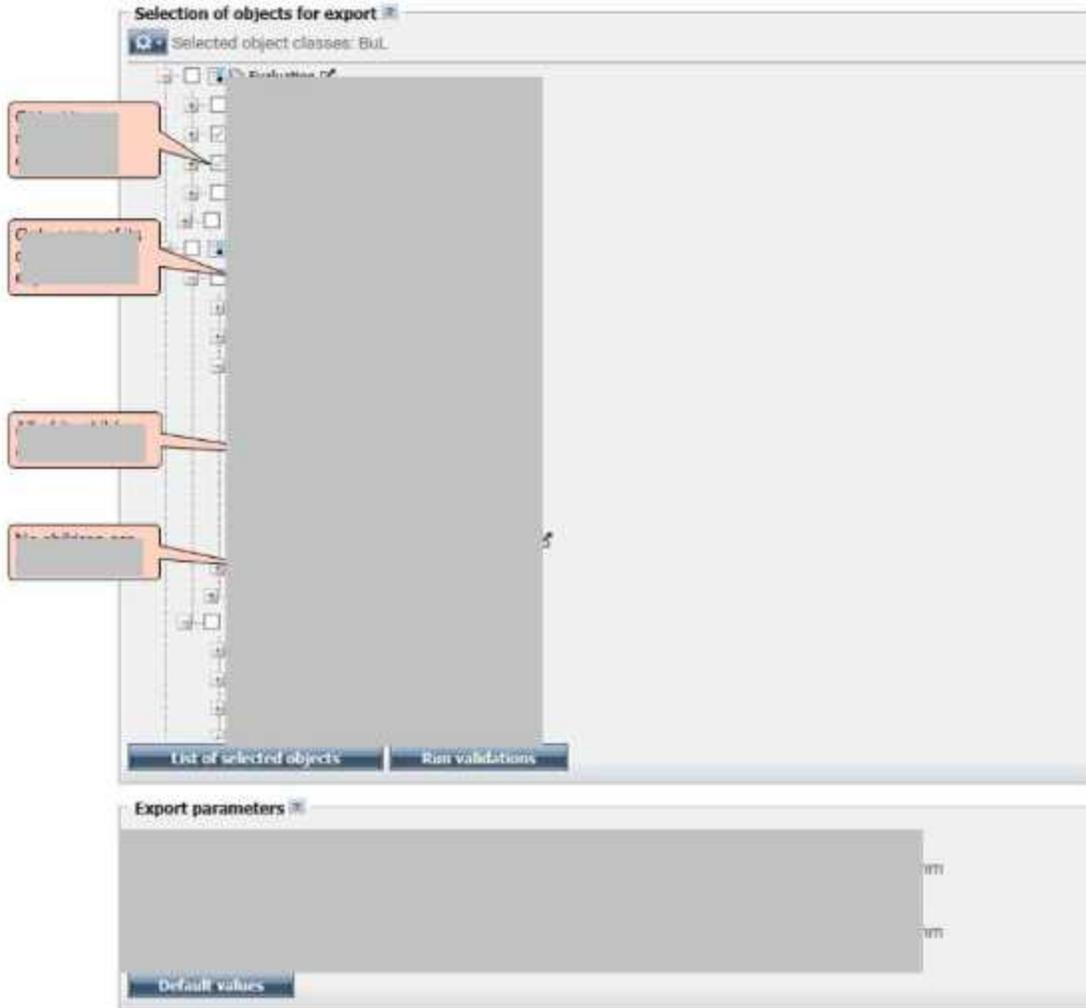
Evolution of

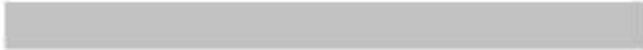
List of selected objects

Run validations

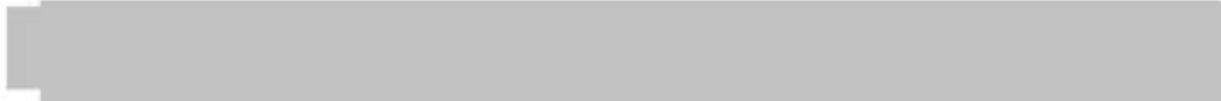
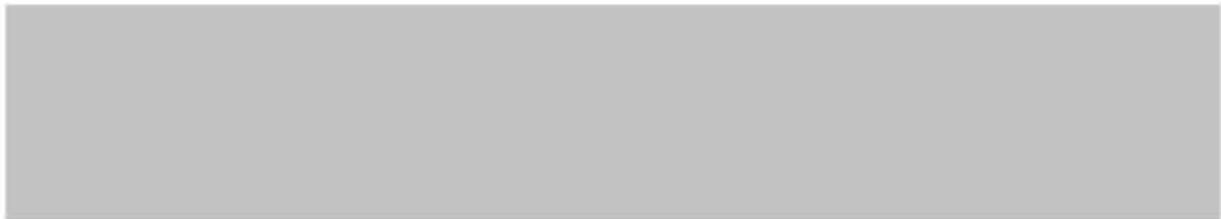
Export parameters

Default values





12.19 Data archiving



[Redacted]

12.19.1 Typical data archiving process

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

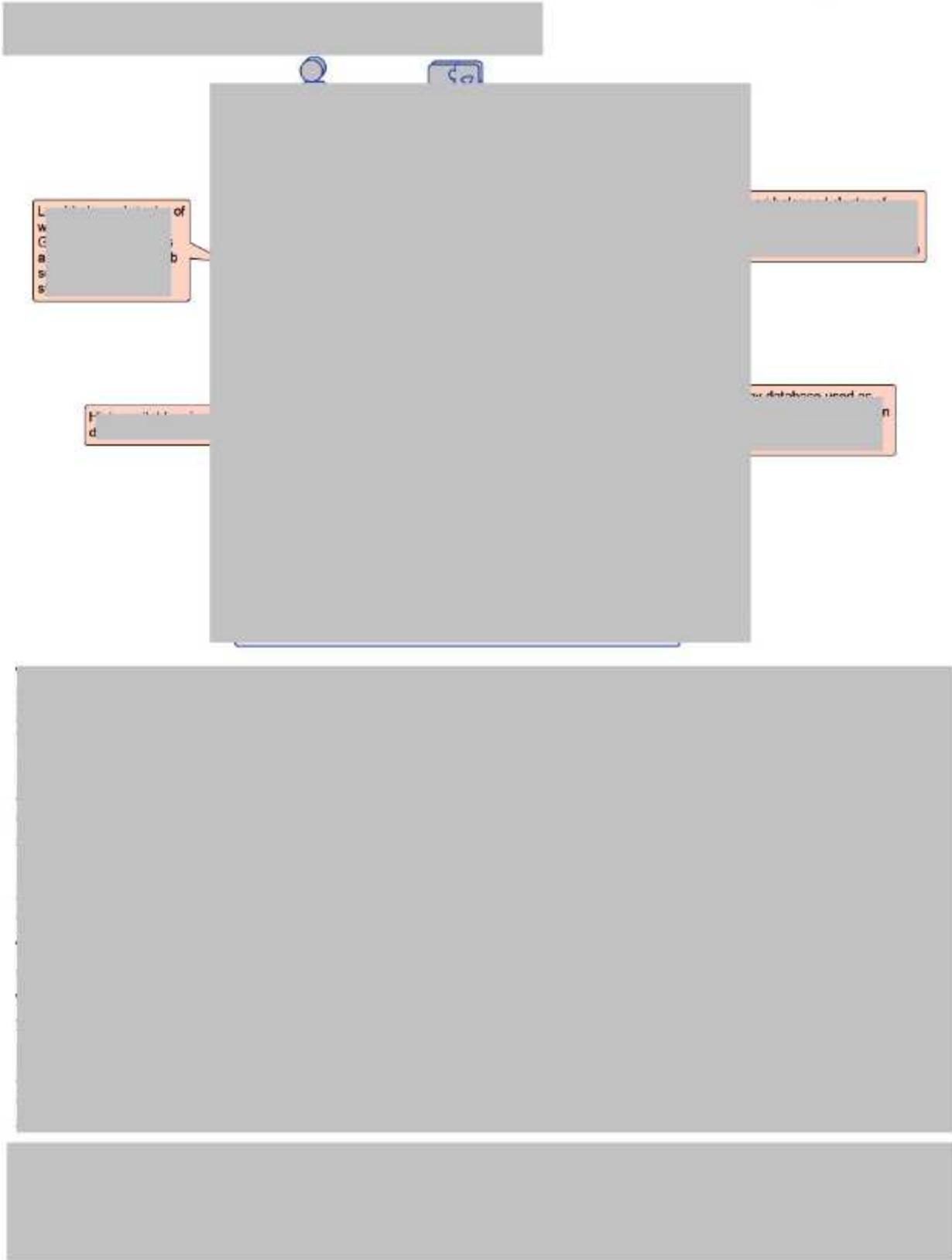
[Redacted]

12.19.2 Retrieving and reading archived data

[Redacted]

12.20 Infrastructure

[Redacted]





12.21 Audit



...to be available to users with the appropriate privileges.

Annex 1 - Damas License conditions

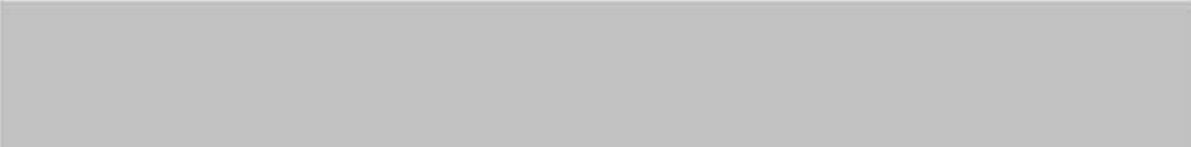
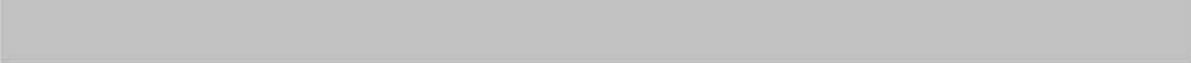
Unicorn Systems commercial Terms and Conditions for Damas MMS Standard Software

(Hereinafter the "Commercial Terms and Conditions")

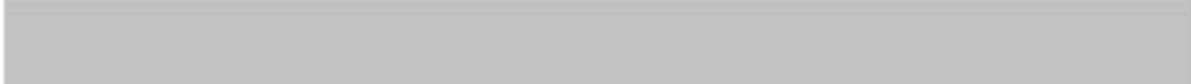
Scope of Commercial Terms and Conditions

1. 
2. 

Pre-Contractual Obligations, Agreement Signing, Written Form

1. 
2. 
3. 

Scope of Delivery

1. 
2. 
3. 
4. 

Rights of USY

1.

2.



Use of Software by Customer

1.

2.

3.

4.

5.

6.

7.

8.

9.

10.



11.



Assignment of Software

1.



Customer's Duty to Cooperate

1.

2.

3.

4.

5.

6.

7.



Terms of the Software Delivery

1.

2.



Price, Terms of Payment, Reservation of Rights

1.

2.

3.



4.



Duty to Check and Notification of Defects

1.

2.



Defects

1.

2.

3.

4.

5.

6.

7.

8.



Liability for Damage; Penalties

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.



Confidentiality and Data Protection

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.



License Termination

- 1.



2.

3.

4.



Product Support Services

1.
2.



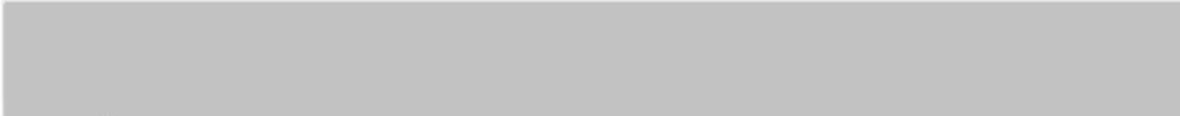
Third Party Software

1.



Final Provisions

1.
2.



Attachment 1 – List of Third-Party SW Programs

The following third-party software programs are included in different versions Damas MMS or may be required by some versions of Damas MMS to run:

/	
L	



.
acco
servi
.
User
exec
expli
of the
parts
has r
.
Back
some



2. *1.1. The description of the solution is insufficiently detailed and no conclusions can be drawn regarding compliance with the safety requirements set out in the technical specification. Missing security information -the text mentions a focus on safety but not enough data to assess.*

Unicorn Answer:

Application API layer

Communication with external systems is performed via communication channels requested by client and finally agreed during project design phase. It is always preferable to exchange data using most secure and commonly wide communication channels used by market participants:

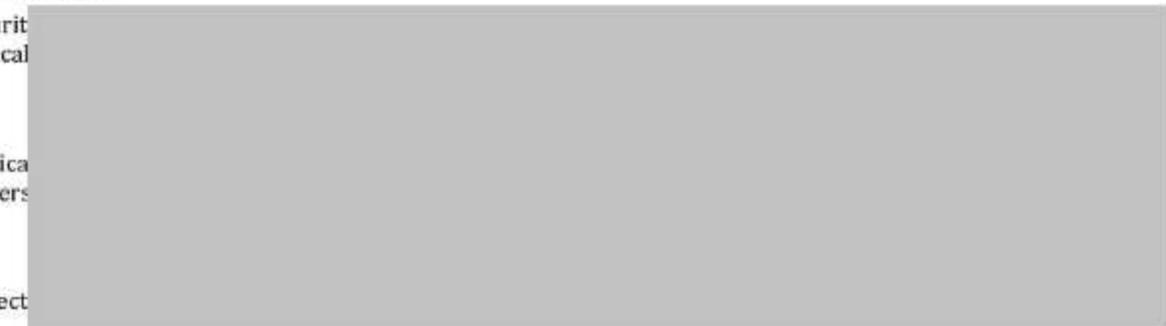
- Web-Services are commonly used to exchange data between systems in energy domain. Damas MMS communication with external systems is built using modern ASP.NET WCF framework which guarantees compliance with latest security requirements and vendor support. Such communication needs to be secured. Security features used by Damas MMS platform:

o
o
o
does.
o
o
.
is use
comm
devel



Database layer

Securit
Typical
.
.
applica
servers
.
.
project



3. 1.2.FR-9, FR-16 - no information is provided on the implementation of the requirements, therefore compliance with the requirements cannot be determined

Unicorn Answer:

The whole chapter of the Functional Requirement were added. For more details about FR, please see chapter Alignment with Functional Requirements.

4. 1.3.TS Requirement NFR-102 - It is not clear from the information provided whether the change of logging parameters can be performed without disrupting the system operation.

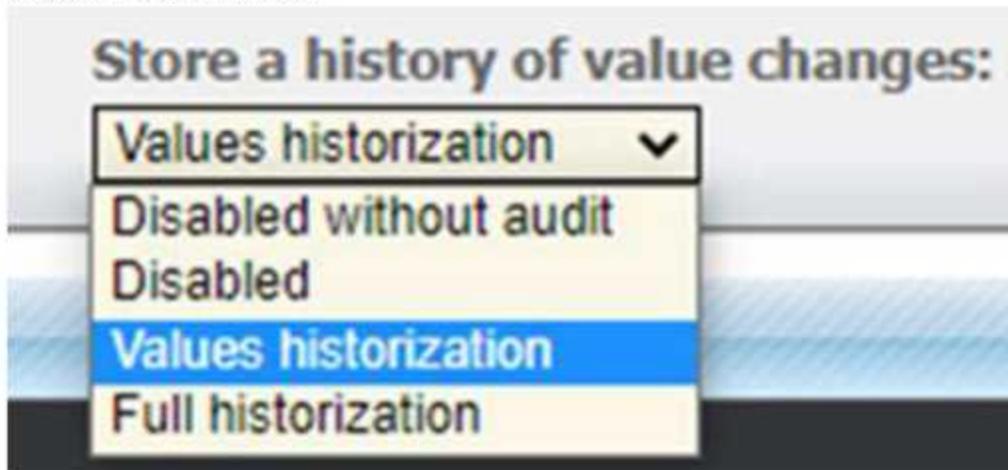
Unicorn Answer:

Damas platform audit is focused at two crucial aspects: data consistency audit and application functionality audit. Data audit is responsible for tracking of any data change made in the system. This ability is called historization of data and it allows to see all changes made over one virtual data column of data.



Date	Changed by	Value	Job	JobId	Serial	Request ID
20 07 2021 15:07:00.000	Damas Administrator	460,504			8077034221	40902642700-40902642700-40902642700
20 08 2021 16:07:26.000	S. ...	460,500	1207040217	1207040227	8077034221	51477044-40902642700-40902642700

Different data change audit log levels could be separately configured per time serie column by administrator of system using administrative WEB GUI.



Data change audit levels could be updated without any interruption of system operation at any time.

5. 2.1. Clarification required: NFR-35 for environmental performance (i.e., TEST / DEV environments provided by Unicorn). PVR-18 - Supplier System (JIRA). The decision states that part of the integration management can be implemented in the proposed solution using BPM and Events Engine. Only first part of question answered here

Unicorn Answer:

Based on our experience of already implemented Damas projects, benefit of having DEV and TEST (internal FAT) environments inside Unicorn premises lies in a field of already defined and well tested development procedures used many times before for other Damas implementation.

Key benefits are:

- initial preparation of DEV and TEST (internal FAT) environments takes just few days. It means fast start of implementation stage of project as there are no delays with environment preparation
- integration with Unicorn internal CI-CD infrastructure which allows to speed up development and testing of deliveries to internal environments
- environments are available only to Unicorn staff as they are located at premises available only via corporate network or corporate VPN secured by 2 factor authentication and individual access rules
- for demo purposes, it could always be granted temporary or permanent public access to Front End part of application to product owner or any other customer staff

Typical configuration of any DEV or TEST environment hosted at Unicorn premises is the following:

Server	CPU (Cores)	RAM (GB)	HDD (GB)	OS
DF				
se				
Fr				
En				
G				
Be				
d				
Be				
d Async				

DEV and TEST environments are used internally by Unicorn team to perform development and internal testing. Such environments are part of development and services workflow. Usage of such environments would not bring any additional cost for Litgrid.

Detailed purpose of every environment and overall layout of environments is described in answer for question ID-10 below.

6. 2.2. It is also necessary to clarify the architectural solution and the layout of the environments.

Unicorn Answer:

Based on requirements and our experience from previous Damas MMS implementations, we assume the following environments will be used during development and operation of the system:

Environment	Purpose	Where deployed
DEV	Used by the development team to develop new features of the system.	Unicorn premises.
TST(TEST)	Used by the development and internal test team to perform internal system testing and integration testing. At the first stages of the project (before Pre-Prod environment would be ready at Litgrid premises) this environment could perform function of DEMO environment where product owner could verify results of development at the end of each sprint.	Unicorn premises.
DEMO/ PAL- instruction / PRE-PROD	Pre-Prod environment will be used for delivery of the sprint results for customer tests and will be used for demonstrations and learning of system functionalities by Litgrid users. Also, this environment would be used for real integration tests with all required external systems. Such environment would have configuration as close as possible to Production environment. After Go-Live this environment will be used for DEMO and user stories acceptance.	Litgrid premises. Not HA.
PRODUCTION	Environment will be used for deployment of already accepted user stories and will be used for acceptance testing before Go Live date. This environment will become the production environment after successful UAT phase of the project.	Litgrid premises – deployed in two locations for HA and DR purposes



All environments should operate at own isolated subnets behind firewall. This approach will allow to clearly separate system configuration and will limit access to dedicated environment to only authorized users.

Based on our experience of already successfully implemented Damas MMS systems, we suggest following schedule of environments life cycle:

- DEV environment will be prepared and used exactly at the beginning of development phase start. It could also be prepared during last weeks of design phase to be able to start development immediately.
- TEST (internal FAT) environment will be prepared before the first DEMO to be able to present results of the development to product owner. Before Pre-Prod would be ready – TEST environment could perform role of DEMO environment.
- Pre-Prod (PAL-instruction, DEMO) environment is usually prepared in parallel during life cycle of the project. Usually, it takes some amount of time, as customer needs to prepare dedicated hardware first. When environment is ready, dev team performs installation and configuration of application there. All next deployments are scheduled based on sprint timelines and internal agreements during project phase. After this moment Pre-Prod environment would be used for all demonstrations.
- Production environment is prepared after Pre-Production environment or in parallel with it. Usually, it is prepared at the end of the development stage and at the beginning of UAT phase of the project. Before Go-Live, when environment is ready and operational, Disaster Recovery (DR) test should be performed to ensure that environment is failure tolerant. This test is better to perform not far to Go-Live date, to be sure that configuration is proper and working as expected. Such DR tests are performed by Litgrid IT specialists with support of Unicorn development team.

Application is built based on 3 tier architecture:

1. From [REDACTED]
by all autho
2. Back [REDACTED]
This back-C [REDACTED]
- At this layer [REDACTED]
3. Data [REDACTED]
can be used [REDACTED]

Detailed architectural description of future system to be deployed to Litgrid premises could be found in chapters "9.6.1 Deployment view", "9.6.2 Disaster and recovery" and "9.6.3 Virtual servers". They contain description of deployment architecture and requirements to Hardware for environments which suggested to be hosted at Litgrid premises (Pre-Prod and Production).

Chapter "9.6.4 Licences" contains list of licences required to run Damas MMS at Litgrid premises.

7. 2.3. *The proposal includes licenses for infrastructure components, which in this case are redundant or need to be clarified due to the layout of the architecture of future environments. Items 2-3-4 of the submitted proposal.*

Unicorn Answer:

All licences were calculated based on proposed specification of HW which are suggested to be hosted at Litgrid premises (Production and Pre-Production environments) only. Unicorn is taking care about licencing of all internal environments which would be hosted at Unicorn premises and would be used for development. No additional licences are required for such environments.

Based on Unicorn's experience with other already successfully implemented Damas MMS based projects, proposal was prepared based on assumption that all application servers would be hosted in virtualized environment which would be deployed at data centres with physical server infrastructure owned by Litgrid. Licence calculations were made for software required to run Damas MMS application and to build HA virtual infrastructure for application servers.

Any other solution architecture needs to be deeply analysed and agreed by both parties additionally during project design phase. As proper licencing of environment requires precise knowledge of infrastructure which must be licenced. This procedure requires deep analyse for finding of compromise between efficient performance and licence cost.

Unicorn assumes that by agreement with customer, target infrastructure design may change, and this would effect on final license cost. That's why all licenses were pre-calculated for proposed infrastructure and provided separately with explicit pricing. In case some of licenses would not be needed, they would be simply deducted from proposal price. Same time additional licenses on top of offered amount would have to be purchased additionally by Litgrid. Unicorn would support Litgrid and would try to provide additional licences using corporate discounts which Unicorn has with [REDACTED]

For more details about initially proposed solution, please refer to chapters below:

- Deployment view and HW specifications for Production and Pre-Production environments could be found at "9.6.1 Deployment view", "9.6.2 Disaster and recovery" and "9.6.3 Virtual servers" chapters of proposal document.
- Chapter "9.6.4 Licences" contains list of licences required to run Damas MMS at Litgrid premises. Number of licences was calculated based on proposed infrastructure requirements for Production and Pre-Production environments.



ID	Type of the Procurement Document, to which the suggestion is dedicated (Technical Specification, Tender form, Draft Procurement Contract or other)	Reference to Tender Document (TS, DPC, TF or other), Clause number and precise text thereof to be negotiated on	Unicorn Systems a.s. questions / suggestions	LITGRID AB response
1	Technical Specification	PVR-18 - Supplier System (JIRA). The decision states that part of the integration management can be implemented in the proposed solution using BPM and Events Engine.	For support, Unicorn typically uses JIRA as ticket management system, JIRA is available 24x7, as we have described in original Proposal, We are however ready to integrate to Litgrid solution. We are not proposing to use JIRA to provide any functional aspects (no part of the actual Solution is using JIRA)	The proposed amendments for the requirement PVR-18 is provided (attached xls document "Changes of the Procurement documents").



2	Draft Procurement Contract	<p>2.3.1. The services of development and installation of the Information System will be paid for the sprints executed in the last quarter, 85 % of their price paid no later than within 30 calendar days from the date of signing of the delivery and acceptance certificate of the executed sprints and receipt of the duly submitted invoice. The invoice and the delivery and acceptance certificate of the executed sprints for the last quarter must be submitted no later than the 10th working day of the current month. If the delivery and acceptance of completed sprints coincides with the delivery and acceptance of module (s), the completed sprints and module (s) shall be the delivered and accepted by the same the delivery and acceptance certificate.</p>	<p>We prefer to keep payment after each sprint delivered to client, or for cumulated sprints delivered in the past quarter.</p>	<p>Given that the development of the Information System consists of 164 sprints, there may be an additional administrative burden for each party of the Contract to pay for each sprint delivered.</p>
3	Draft Procurement Contract	<p>6.2. Intellectual property, third-party licenses</p>	<p>We are delivering the platform based on the Damas solution which has its own license conditions. It was described in the proposal. Following, this chapter must be adapted accordingly to the license which will be preferred by Litgrid.</p>	<p>The proposed amendments for the requirements NFR-119, PVR-1, PVR-12 and SPC Annex 5 "Draft contract", section 6.2 are provided (attached xls document "Changes of the Procurement documents").</p>



4	Draft Procurement Contract	<p>6.2.5. The Seller must transfer to the Buyer the software developed during the project and its source code after the delivery and acceptance certificate of Phase 1 Services of development and installation of the Information System and the Final delivery and acceptance certificate of the Information system respectively is signed.</p>	<p>As it was stated in the previous comment, the Damas has its own licenses conditions. We do not provide the source code to our clients.</p>	<p>Suggestion: The Supplier shall assign to the Customer all proprietary rights to software solutions developed by the Supplier during the provision of the development of installation services.</p>
5	Draft Procurement Contract	<p>6.3.4. During the period of warranty support, the Seller alters the developed results of Services, considering the comments submitted by the Buyer, or informs the Buyer in a reasoned written or other manner agreed between the Seller and the Buyer about the refusal to revise the developed results of the Services, stating the reasons for the refusal. In such a case, the comments submitted by the Buyer shall be dealt with separately by mutual agreement between the Parties.</p>	<p>Please advise about this statement, we found it as not understandable.</p>	<p>This condition means that in case of disagreement between the Supplier and the Buyer whether the developed results of Services requested by the Buyer to be revised by the Buyer is subject of warranty support or not, this condition is not the subject of negotiations. In such a case, the comments submitted by the Buyer shall be dealt with separately by mutual agreement between the Parties, are those comments object of warranty support or not.</p>



6	Draft Procurement Contract	6.4. Securing the performance of the contract.	<p>In this article is set 0.04% penalties in case of the project delay. The penalties must also have a cap, article must be adapted.</p>	<p>It was mentioned during the negotiations that there is a clause in the contract Contract that defines the cap for the penalties. Here The Contracting Entity wants to inform that the cap of 20 per cent from the Contract price for penalties is defined in Clause 3.2.3 of the General Conditions of the Contract.</p>
7			<p>The expected duration of the project is very short in relation to the relatively large scope. Timely delivery is only possible at the cost of a high degree of parallelization, not only on the supplier but also on the customer side</p>	<p>Remark was reviewed and discussed during the negotiations and mentioned assumptions will be evaluated internally and taken into account by the Contracting Entity. No actions were agreed.</p>
8			<p>We assume that the customer will be able to build up three parallel analytical mini teams which will not share the human resources (except the necessary coordination). The same approach will be applied on the supplier side. These teams must be able to prepare the necessary inputs well in advance (3+ weeks) of the start of the given sprint, in order to have design finalized and test cases prepared for actual start of the sprint. (as not to block actual sprint execution by lack of</p>	<p>Remark was reviewed and discussed during the negotiations and mentioned assumptions will be evaluated internally and taken into account by the Contracting Entity. No actions were agreed.</p>



9			<p>work or unclear specification with open points).</p>	
			<p>The timely delivery would not be possible without very high-level of the configurability of Damas MMS platform which significantly reduces the implementation effort of many functions. On the other hand, each product in the market (including Damas MMS), has also certain limitations. More than 80 % requirements will be solved at least partially by the configuration of Damas platform. The budget and mainly the strict time schedule of the project (which we accept without reservations) is achievable only if both counterparties understand that each requirement can be solved generally by many ways and will also understand that the preferred way is the configuration and not hardcoding. This approach has also significant benefits for the customer because the already implemented functionalities can be changed or reconfigured much more easily than the hardcoded libraries.</p>	<p>Remark was reviewed and discussed during the negotiations and mentioned assumptions will be evaluated internally and taken into account by the Contracting Entity. No actions were agreed.</p>



10			<p>We confirm that if any requirement can be solved by the configuration only at the cost of big compromises (usability, intuitiveness, performance etc.), we will not insist in the solution by configuration. However, we believe that such cases would be rather rare and that the natively configurable user interface will be in most cases sufficient because it is proven by many existing customers.</p>	<p>Remark was reviewed and discussed during the negotiations and mentioned assumptions will be evaluated internally and taken into account by the Contracting Entity. No actions were agreed.</p>
11			<p>At the same time, we undertake to introduce to the customer, at the beginning of the project, the platform, all its important features, the configuration capabilities and also the limitations, so that the customer understands basic architectural principles of Damas MMS platform.</p>	<p>Remark was reviewed and discussed during the negotiations and mentioned assumptions will be evaluated internally and taken into account by the Contracting Entity. No actions were agreed.</p>
12			<p>High number of internal and external systems to be integrated. Several of them do not exist yet. The interfaces are sometimes not clear. These aspects are significantly increasing the risk of project delay. We suggest splitting the interfaces according to their priorities and at least partially replace some of them by manual input/copy-pasting or other similar approach for some transitional period.</p>	<p>A more detailed project schedule and other details will be provided during the project implementation phase.</p>
13			<p>The scope of the system itself is relatively high. We believe that they can be prioritized and the modules with less priority (Grid loss management? Short-term adequacy?) could be delivered in the follow-up phase of the project.</p>	<p>During of the project implementation phase the proposal will be evaluated and prioritization is possible without reducing the scope of the project.</p>



14			<p>The individual requirements can have different priorities. We would like to indicate an example of the requirements which we consider as less important or even non-essential:</p> <ul style="list-style-type: none"> o ENTSO-E transparency: data flows for PDF files o REST API interface including VBA library o Administration of the user roles o Full-text search o Inline coding o Drag and drop 	<p>During the negotiation it was noted, that the Contracting Entity do not have defined VBA library. The priorities will be defined during the project implementation.</p>
15			<p>We would like to discuss very strict performance requirements, especially processing of data flows under 1 second</p>	<p>The Contracting Entity Authority, taking into account the remark on very strict performance requirements, propose amendments for the requirement NFR-70. Please review the proposed change (attached xls document "Changes to the Procurement documents").</p>



16			<p>We would like to discuss possibility of involvement our team from [REDACTED]</p>	<p>Given that the Contracting Entity Authority operates in an area important for national security and manages critical information infrastructure, the question requires a more detailed analysis of legislation and circumstances as to whether a possible future public procurement cContract would not pose a threat to national security. The Contracting Entity entity will provide a response as soon as it has the necessary final information to provide this response.</p>
----	--	--	-------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

