ANNEX no. 2 to THE TERMS OF REFERENCE:

LOT 2

Technical specifications for the implementation of the Head end System (HES) and Meter Data Management System (MDMS) platform in 1+1 configuration for the North Electricity Distribution Operator (RED-NORD S.A.)

Contents

LIST OF ABBREVIATIONS AND ACRONYMS

Abbreviation/Acronym	Full Description
AD	Active Directory
ADMS	Advanced Distribution Management System
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AMI	Advanced Metering Infrastructure
AMQP	Advanced Message Queuing Protocol
AMR	Automatic Meter Reading
ANRE	Agenția Națională pentru Reglementare în Energetică (National Energy Regulatory Agency)
API	Application Programming Interface
APT	Advanced Persistent Threat
ASVS	Application Security Verification Standard
AWS	Amazon Web Services
BCR	Binding Corporate Rules
BCP	Business Continuity Planning
BI	Business Intelligence
CIM	Common Information Model
CIP	Critical Infrastructure Protection
CIS	Customer Information System
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CMS	Customer Management System
COSEM	Companion Specification for Energy Metering
CPU	Central Processing Unit
CRM	Customer Relationship Management
CSS	Cascading Style Sheets
CSV	Comma-Separated Values
CT	Current Transformer
CVSS	Common Vulnerability Scoring System
DAST	Dynamic Application Security Testing
DB	Database
DBA	Database Administrator
DBMS	Database Management System
DC	Data Center
DDoS	Distributed Denial of Service
DER	Distributed Energy Resource
DLMS	Device Language Message Specification
DNP3	Distributed Network Protocol 3
DPA	Data Processing Agreement
DR	Disaster Recovery
DSO	Distribution System Operator
DTR	Distribution Transformer
EEA	European Economic Area
EMS	Energy Management System
ERP	Enterprise Resource Planning
ESB	Enterprise Service Bus
EU	European Union
EV	Electric Vehicle
FAQ	Frequently Asked Questions
FIPS	Federal Information Processing Standards

Abbreviation/Acronym	Full Description
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
GIS	Geographic Information System
GOOSE	Generic Object Oriented Substation Event
GPRS	General Packet Radio Service
GraphQL	Graph Query Language
GSM	Global System for Mobile Communications
HES	Head-End System
HMI	Human-Machine Interface
HSM	Hardware Security Module
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
HV	High Voltage
Hz	Hertz
IAM	Identity and Access Management
ICT	Information and Communications Technology
ICS	Industrial Control Systems
IDPS	Intrusion Detection and Prevention Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ILT	Instructor-Led Training
IoT	Internet of Things
IP	Internet Protocol
IRP	Incident Response Plan
ISO	International Organization for Standardization
IT	Information Technology
JSON	JavaScript Object Notation
JWT	JSON Web Token
KMS	Key Management System
KPI	Key Performance Indicator
KT	Knowledge Transfer
kV	Kilovolt
kVA	Kilovolt-Ampere
kW	Kilowatt
kWh	Kilowatt-hour
LDAP	Lightweight Directory Access Protocol
LMS	Learning Management System
LTE	Long-Term Evolution
LV	Low Voltage
M2M	Machine-to-Machine
MD	Moldova
MDM	Meter Data Management
MDMS	Meter Data Management System
MFA	Multi-Factor Authentication
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
MS	Microsoft
MV	Medium Voltage
MVA	Megavolt-Ampere
MW	Megawatt
MWh	Megawatt-hour

Abbreviation/Acronym	Full Description
NERC	North American Electric Reliability Corporation
NFR	Non-Functional Requirements
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NPV	Net Present Value
OAS	OpenAPI Specification
OAuth	Open Authorization
OLTP	Online Transaction Processing
OPC UA	Open Platform Communications Unified Architecture
OS	Operating System
OT	Operational Technology
OWASP	Open Web Application Security Project
P1	Priority 1 (Critical)
P2	Priority 2 (High)
P3	Priority 3 (Medium)
P4	Priority 4 (Low)
PDF	Portable Document Format
PLC	Power Line Communication
PM	Project Manager
PMP	Project Management Professional
POC	Proof of Concept
PRINCE2	Projects IN Controlled Environments 2
PUE	Power Usage Effectiveness
QA	Quality Assurance
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-Based Access Control
RCA	Root Cause Analysis
REST	Representational State Transfer
RESTful	Representational State Transfer compliant
RF	Radio Frequency
RFI	Request for Information
RFP	Request for Proposal
RO	Romania
ROPA	Record of Processing Activities
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RU	Russian
SAP	Systems, Applications & Products
SAST	Static Application Security Testing
SCADA	Supervisory Control and Data Acquisition
SCC	Standard Contractual Clauses
SDLC	Software Development Life Cycle
SEP	Smart Energy Profile
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SLR	Service Level Requirements
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol

Abbreviation/Acronym	Full Description
SP	Special Publication
SQL	Structured Query Language
SSO	Single Sign-On
T&M	Time and Materials
TACACS	Terminal Access Controller Access-Control System
TBD	To Be Determined
TCO	Total Cost of Ownership
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TOGAF	The Open Group Architecture Framework
TOU	Time of Use
TPS	Transactions Per Second
TSO	Transmission System Operator
UAT	User Acceptance Testing
UI	User Interface
UML	Unified Modeling Language
UNDP	United Nations Development Programme
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
USD	United States Dollar
UX	User Experience
VEE	Validation, Estimation and Editing
VM	Virtual Machine
VPN	Virtual Private Network
VT	Voltage Transformer
WAN	Wide Area Network
WBS	Work Breakdown Structure
WCAG	Web Content Accessibility Guidelines
WORM	Write Once Read Many
XML	eXtensible Markup Language

TERMS OF REFERENCE - PART I

GENERAL OVERVIEW

1. INTRODUCTION AND BACKGROUND

1.1 Background

The Republic of Moldova is undertaking a comprehensive modernization of its electricity distribution infrastructure through the implementation of smart metering systems through the "Accelerating a Just Energy Transition in the Republic of Moldova" UNDP project support. This initiative aims to enhance operational efficiency, improve billing accuracy, enable real-time

monitoring of energy consumption, and support the country's digital transformation agenda in the energy sector.

S.A.„RED-Nord" operating as the Distribution System Operator (DSO) in the North regions of Moldova, manages approximately 500,000 meters.

1.2 Contract context

This project is funded by UNDP and aims to implement a comprehensive Advanced Metering Infrastructure (AMI) solution comprising:

Requirement	General description	Verification method
HES Capability	"A robust Head End System (HES) for real-time communication and data collection"	**Evidence required at Offer evaluation stage:** Technical datasheets, architecture documents
MDMS Capability	"A comprehensive Meter Data Management System (MDMS) for data storage, validation, analysis, and reporting"	**Evidence required at Offer evaluation stage**: Product specifications, feature matrix
ADMS Integration	"Full integration with the existing Advanced Distribution Management System (ADMS)"	**Evidence required at Offer evaluation stage**: Integration architecture; Acceptance (handover): Integration testing
Interoperability	"Interoperability with third-party systems, owned and operated by Beneficiary, through standardized interfaces"	**Evidence required at Offer evaluation stage**: API documentation; Acceptance (handover): Interface testing
Scalability	"Must accommodate both existing operational meters and future deployments"	**Evidence required at Offer evaluation stage** Scalability design documents, reference implementations

The solution must accommodate both existing operational meters and future deployments, ensuring scalability and flexibility to meet growing demands.

2. OBJECTIVES

2.1 General objective

To implement an integrated HES and MDMS platform in a 1+1 (active-active or active-standby) configuration that ensures high availability, data integrity, and seamless integration with existing DSO infrastructure while supporting current and future smart metering requirements.

Following commissioning, the Contractor shall provide a **minimum 12-month warranty period** at no additional cost. The warranty shall cover the **correction of defects, errors, or deficiencies**

in the supplied hardware and software components and shall ensure that the system operates fully in accordance with the agreed specifications.

In addition, the Contractor shall include and price **support and maintenance services** in the financial offer for a **minimum of 12 months after commissioning**. These services should cover **regular system monitoring, preventive maintenance, performance optimization, software updates, and user support**, ensuring continuous operational performance beyond defect correction.

The Contractor shall guarantee sustainability and ensure the extended operational continuity of the system by providing support and maintenance for a minimum of 60 months after roll-out (implementation) under the same general terms, confirming that the proposed universal HES and MDM software release version — including all national customizations — will remain fully supported and will not reach **End of Support (EOS) or End of Life (EOL) for a minimum period of five (5) years (60 months)** following the commissioning of the solution in the Beneficiary's production environment.

Under Phase I of the Smart Metering Pilot Initiative, RED NORD with the support of UNDP successfully deployed 18,716 smart meters across its service territory. These pilot meters are already installed, operational, and ready for integration with a centralized Head-End System (HES) and Meter Data Management System (MDMS).

Building on this foundation, the programme is now expanding its smart metering infrastructure to reach a total of 45,000 smart meters by 2027 in the area of distribution of RED NORD.

This procurement requires the selected vendor to provide a comprehensive HES/MDMS solution capable of:

1. **Integrating and providing full licensing coverage[1] (where applicable under the vendor's licensing model) for a total of 45,000 smart metering points, of which 18,716 existing pilot smart meters are already deployed in the field and require immediate integration.**
2. **Ensuring that the system capacity and all necessary licenses are provisioned for the full target of 45,000 metering points from contract commencement, regardless of the actual deployment timeline of physical meters.**

The Contractor shall integrate all smart meter models and types specified in *"Annex 2 LOT 2 - Technical Specifications for the implementation of the Head end System (HES) and Meter Data Management System (MDMS) platform in 1+1 configuration for the North Electricity Distribution Operator (RED-NORD S.A)"*, specifically Section 7.7 "Meter brand compatibility". Integration costs shall be structured per meter model/technology stack, not per individual unit. Additionally, the Contractor shall provide reference pricing for integration of alternative smart meter models not specified in Section 7.7, which may be utilized through contract amendments should budget allow for expansion or should deployment plans require alternative equipment models.

NOTE: This specification outlines the requirements and verification criteria applicable at both the "Evidence required at Offer evaluation stage" and "Acceptance (handover)" of

[1] The term "licenses" in this context refers to system capacity provisioning as well as operational entitlements for managing the specified number of integrated and connected smart meters within the HES+MDMS platform. This is absolutely distinct from traditional software licensing based on user access or software usage rights.
Vendors may apply different commercial models, including capacity-based licensing (if any) tied to the number of meters managed by the system.
Bidders must clearly disclose their licensing/capacity provisioning model(if any) and ensure that all costs—whether termed as licenses, capacity or otherwise countable items —necessary to support the full operational capacity for 45,000 metering points are transparently itemized in their financial proposal from contract commencement.

the assignment stages, ensuring that bidders clearly understand what evidence, documentation, and performance demonstrations are expected during tendering evaluation, and what functional tests and validation metrics will be applied upon assignment delivery, as follows:

- **Evidence required at Offer evaluation stage:** Verification of the 1+1 configuration design through architecture documents.
- **Acceptance stage (handover)**: Test failover and availability metrics.

2.2 Specific objectives

Objective 1: Deployment of a scalable HES platform

Sub-requirement	Evidence required at Offer evaluation stage	Acceptance (handover) testing
Real-time bi-directional communication	Protocol support documentation	Communication tests with actual meters
Multiple communication technologies	Technology compatibility matrix	-
98% data collection reliability	Historical performance data from references	Performance testing over 30 days
Minimum 500K messages/hour	Load test results from other deployments	Stress testing in production environment

Objective 2: Implement a comprehensive MDMS

Sub-requirement	Evidence required at Offer evaluation stage	Acceptance (handover) testing
VEE algorithms	Algorithm documentation, rule sets	VEE accuracy testing with sample data
Hourly/sub-hourly intervals	Product specifications	-
Advanced analytics	Analytics module documentation	Analytics functionality testing
99.9% availability	Architecture for HA, reference Service-level requirements	90-day availability monitoring

Objective 3: Ensure system integration

Sub-requirement	Evidence required at Offer evaluation stage	Acceptance (handover) testing
ADMS integration	Integration of architecture, API specs	End-to-end integration testing
CIM/IEC 61968 support	Standards compliance certificates	-
API support	API documentation	API functional testing
GIS visualization	GIS integration examples	GIS integration testing

Objective 4: Enhance operational capabilities

Sub-requirement	Evidence required at Offer evaluation stage	Acceptance (handover) testing
Automated meter reading	-	Automated collection testing
Outage detection	Feature documentation	Real-time outage simulation
Loss detection	Algorithm documentation	Loss calculation accuracy testing
Demand response	DR module specifications	DR scenario testing

Objective 5: Ensure compliance and security

Sub-requirement	Evidence required at Offer evaluation stage	Acceptance (handover) testing
GDPR compliance	Compliance certificates, privacy design	-
Cybersecurity measures	Security architecture, certifications	Penetration testing
Audit trails	Audit functionality documentation	Audit trail verification
Regulatory reporting	Report templates	Report generation testing

3. SCOPE OF WORK

3.1 General scope - classification

The selected Contractor shall provide a turnkey solution encompassing:

3.1.1 Software provisioning

Item	Evidence required at Offer evaluation stage	Acceptance (handover) testing
HES/MDMS inclusive licenses (if applicable) for minimum 45,000 meters, which will be gradually implemented during the development, roll-out and support stages according to the future agreement	License (if applicable) model documentation	License(if applicable) activation verification
Necessary modules	Module list and descriptions	Module functionality testing
Development tools	Tool documentation	-
Integration middleware and APIs	Middleware and APIs specifications	Integration testing

3.1.2 Professional services

Item	Evidence required at Offer evaluation stage	Acceptance (handover) testing
Requirements analysis, preliminary available BPMN (Annex no.2.1) validation through the re-mapping of the business processes by implementation team and customized solution design	Methodology documentation	-
Installation & configuration	Installation procedures	Successful installation
System integration	Integration plan	Integration test results
Testing & commissioning	Test plan documentation	Test execution results
Training	Training curriculum	Training effectiveness assessment
Documentation	Documentation samples	Complete documentation delivery
Support & maintenance	Service-level requirements documentation	-

3.1.3 Infrastructure design

Item	Evidence required at Offer evaluation stage	Acceptance (handover) testing
Hardware sizing	Sizing methodology and tools, and required specifications for proper computing performance (CPU/RAM/Storage)	-
Network architecture	Architecture diagrams	-
Database design	Database architecture	-
DR/BCP planning	DR/BCP plan template	DR drill execution

3.2 Technical scope – classification

The solution must address the following technical aspects:

Requirement	Evidence required at Offer evaluation stage	Acceptance (handover) testing
Multi-vendor meter support	Compatibility matrix	Testing with actual meter types
Multi-protocol communication	Protocol support documentation	-
Multi-technology communication	Technology support matrix	-
Scalability to 0.5M meters	Scalability architecture	-

Requirement	Evidence required at Offer evaluation stage	Acceptance (handover) testing
Minimum 96 interval reads/meter/day	Performance specifications	Performance testing
99.9% uptime	HA architecture	Availability monitoring

3.3 Functional scope – classification

The integrated HES and MDMS platform shall provide the following key functionalities:

3.3.1 HES functions:

Function	Evidence required at Offer evaluation stage	Acceptance (handover) testing
Device management	Feature documentation	Functional testing
Communication management	Management interface docs	Communication testing
Data acquisition	-	Collection testing
Command execution	-	Command testing
Event management	Event handling documentation	Event simulation testing
Security key management	Security documentation	Security testing
FOTA updates	FOTA capability docs	Firmware update testing

3.3.2 MDMS functions:

Function	Evidence required at Offer evaluation stage	Acceptance Testing
VEE	VEE rule documentation	VEE accuracy testing
Data aggregation	Calculation methods	Calculation verification
Load profiling	Profiling algorithms	Profile accuracy testing
Loss calculations	Calculation methodology	Calculation testing
Billing determinants	Billing interface docs	Billing data testing
Reporting/analytics	Report samples	Report testing
Data archival	Archival strategy	Archival/retrieval testing

4. CONTRACT IMPLEMENTATION APPROACH AND METHODOLOGY

4.1 Implementation approach - classification

The implementation of contract shall follow an iterative, phased approach with clear milestones and deliverables:

Phase	Evidence required at Offer evaluation stage	Acceptance (handover) testing items
Phase 1: Inception and Design	• Requirements gathering methodology; • Solution architecture approach; • Design templates and tools; • Integration strategy.	• Approved requirements document; • Final architecture design; • Validated BPMN (Annex no.2.1) workflows; • Integration specifications.

Detailed Phase 1 requirements:

Activity	Evidence required at Offer evaluation stage	Acceptance (handover) criteria
Requirements gathering methodology	• Methodology documentation; • BPMN tools and samples; • Requirements templates	-
Solution architecture	• Reference architectures; • Design principles; • Technology stack	• Approved architecture for Moldova; • Performance calculations; • Security assessment
Infrastructure planning	• Sizing methodology; • Planning tools; • Reference implementations	-
Integration specifications	• Integration patterns; • API frameworks; • Sample specifications	• Completed specs for all systems components; • Data mapping documents; • Error handling procedures • Integration testing strategy

Phase 2: Development and configuration

Activity	Evidence required at Offer evaluation stage	Acceptance (handover) criteria
System installation procedures	• Installation guides; • Deployment tools; • Automation scripts	-
Base configuration	-	• System operational • Base parameters set • Initial performance baseline
Customization capability	• Customization framework; • Examples from other projects; • Development tools	• Moldova-specific customizations; • Business rules implemented; • Local regulations compliance
Integration development	-	• All interfaces operational; • Data flows verified; • Error handling tested
Data migration approach	• Migration methodology;	• Migration completed;

Activity	Evidence required at Offer evaluation stage	Acceptance (handover) criteria
	• Tools and scripts; • Success stories	• Data integrity verified; • Reconciliation reports

Phase 3: Testing and validation

Test Type	Evidence required at Offer evaluation stage	Acceptance (handover) criteria
Test methodology	• Test strategy documents; • Test case templates; • Automation framework	-
Unit testing	-	• 100% code coverage; • All defects resolved
Integration testing	-	• All interfaces tested; • End-to-end scenarios passed
Performance testing	• Performance test tools; • Benchmark results from similar projects	• Meet all NFR metrics; • Stress test results; • Optimization implemented
UAT approach	• UAT methodology; • Training plans for testers	• User sign-off achieved; • All UAT scenarios passed
Security testing	• Security test methodology; • Penetration test examples	• Vulnerability assessment passed; • Security controls verified

Phase 4: Deployment and commissioning

Activity	Evidence required at Offer evaluation stage	Acceptance (handover) criteria
Deployment methodology	• Deployment procedures; • Rollback plans; • Go-live(commissioning) checklists	-
Pilot/testing approach	• Pilot/testing methodology; • Selection criteria; • Success metrics	• 1,000 meters operational; • 98% communication success; • Performance targets met
Full-scale rollout	-	• All meters integrated; • System stability proven; • Operational procedures working
Commissioning process	• Commissioning checklists; • Handover procedures	• All systems accepted; • Documentation complete; • Knowledge transfer done

Phase 5: Post-implementation support and maintenance (after commissioning + lifespan = minimum 60 months after roll-out / implementation)

Support Period	Duration	Evidence required at Offer evaluation stage
Warranty, support and maintenance period	Minimum 12 months after deployment to the Beneficiary production environment to be included in the offer)	• Service-level requirements documentation; • Support and maintenance(both preventive and maintenance) procedures; • Team structure; • Escalation matrix
Extended lifespan operational continuity	Months starting with 1st after roll-out (implementation) up to minimum 60 in total	• Maintenance (preventive and corrective) pricing; • Maintenance (adaptive and future developments / integrations) pricing estimates; • Support options; • Update/upgrade policy; • Technology refresh plan

4.2 Contract project management methodology - classification

Requirement	Evidence required at Offer evaluation stage	Acceptance (handover) criteria
PM methodology (PMBOK/PRINCE2)	• PM certification of key team members; • Methodology documentation; • Template samples	-
Agile/Scrum approach	• Agile experience evidence for key team members; • Sprint planning examples; • Tools used	• Sprint reviews conducted; • Backlog properly managed; • Velocity tracking
Progress reporting	• Report templates; • Dashboard examples; • Communication plan	• Weekly reports delivered; • Stakeholder satisfaction; • Issues tracked and resolved
Risk management	• Risk methodology; • Risk register template; • Mitigation strategies	• Risks identified and managed; • No major issues materialized; • Proactive mitigation done
Quality assurance	• QA procedures; • Quality metrics; • Review processes	• Quality targets met; • Defect rates acceptable; • Process compliance verified

5. DELIVERABLES AND TIMELINE

5.1. List of required deliverables

Bidders can find below the list of required deliverables and the indicative implementation timeframe, counted from the date of contract signature.

Phase 1: Inception and design (month 1-3)

Deliverable	Phase	Acceptance (handover) criteria
Deliverable 1	Phase 1: Inception and Design	• Approved requirements document; • Final architecture design; • Validated BPMN (Annex no.2.1) workflows; • Integration specifications.

Detailed Phase 1 requirements:

Sub-Deliverables	Acceptance (handover) criteria
Solution architecture	• Approved architecture for Moldova; • Performance calculations; • Security assessment
Integration specifications	• Completed specs for all systems components; • Data mapping documents; • Error handling procedures • Integration testing strategy

Phase 2: Development and configuration (months 4-8)

Deliverable	Activity	Acceptance (handover) criteria
Deliverable 2	Base configuration	• System operational • Base parameters set • Initial performance baseline
	Customization capability	• Moldova-specific customizations; • Business rules implemented; • Local regulations compliance
	Integration development	• All interfaces operational; • Data flows verified; • Error handling tested
	Data migration approach	• Migration completed; • Data integrity verified; • Reconciliation reports
	Source code delivery[2]	• Complete source code for all customizations;

[2] *The Contractor shall deliver complete source code for all customizations, adjustments, and integrations developed under this Contract. This includes all custom modules, integration components, business rules implementations, and country-specific adaptations. The source code shall be well-documented, include all dependencies, build scripts, and deployment procedures. The Contractor grants to UNDP a perpetual license to use such intellectual property or other proprietary right solely for the purposes of and in accordance with the requirements of the Contract and the nonrevocable right to sublicense such use to the*

Deliverable	Activity	Acceptance (handover) criteria
		• Complete source code for all integrations; • Complete source code for Moldova-specific developments; • Code documentation and comments; • Build and deployment scripts; • Version control repository access

Phase 3: Testing and validation (months 9-10)

Deliverable	Test Type	Acceptance (handover) criteria
Deliverable 3	Unit testing	• 100% code coverage; • All defects resolved
	Integration testing	• All interfaces tested; • End-to-end scenarios passed
	Performance testing	• Meet all NFR metrics; • Stress test results; • Optimization implemented
	UAT approach	• User sign-off achieved; • All UAT scenarios passed
	Security testing	• Vulnerability assessment passed; • Security controls verified

Phase 4: Deployment and commissioning (months 11-12)

Deliverable	Activity	Acceptance (handover) criteria
Deliverable 4	Pilot/Testing approach	• 1,000 meters operational; • 98% communication success; • Performance targets met
	Full-scale rollout	• All meters integrated within limits of dispatched number of licenses; • System stability proven; • Operational procedures working
	Commissioning process	• All systems accepted; • Documentation complete; • Knowledge transfer done/training • Source code repository transferred; • IP rights transfer documentation signed

Phase 5: Post-implementation support and maintenance (months 13-24 + lifespan = minimum 60 months after roll-out / implementation)

End-Users (PED and RED-Nord). To the extent that any such intellectual property or other proprietary rights consist of any intellectual property or other proprietary rights of the Contractor: (i) that pre-existed the performance by the Contractor of its obligations under the Contract, or (ii) that the Contractor may develop or acquire, or may have developed or acquired, independently of the performance of its obligations under the Contract, UNDP does not and shall not claim any ownership interest thereto.

	Support Period	Duration	Acceptance (handover) criteria
Deliverable 5	**Support and maintenance period after roll-out included in the offer**	**Months 13-24 (minimum 12 months after deployment in to the Beneficiary production environment to be included in the offer)**	**• Service-level requirements documentation;** **• Support and maintenance(both preventive and maintenance) procedures;** **• Team structure;** **• Escalation matrix**

5.2 Additional information and management arrangements

5.2.1 Technical deliverables validation

Deliverable	Acceptance (handover) criteria
Solution architecture	• Final approved architecture; • All components documented
Design specifications	• Complete specifications; • BPMN(Annex no.2.1) workflows validated
Integration specs	• All interfaces documented; • Test cases defined
Test plans / cases	• Comprehensive test coverage; • All scenarios documented
Test reports	• All tests executed; • Results documented

5.2.2 System deliverables validation

Deliverable	Acceptance (handover) criteria
HES/MDMS platform	• Fully configured; • All modules operational
Integration components	• All integrations working; • Performance verified
Custom reports	• All required reports; • User acceptance
Migration tools	• Migration completed; • Data integrity verified
Monitoring tools	• Monitoring operational; • Alerts configured
Source code repository	• Complete source code for customizations; • Complete source code for integrations; • Version control system accessible; • All build dependencies included; • IP rights documentation complete

5.2.3 Documentation deliverables validation

Deliverable	Acceptance (handover) criteria
Documentation standards	-
Admin guides	• Complete guides delivered; • Technical accuracy verified
User manuals	• All functions documented; • User-friendly format
API documentation	• Complete API reference; • Code examples included
Troubleshooting guides	• Common issues covered; • Solutions verified

! Important: Documentation language requirements

- Technical documentation: minimum English,
- User documentation: minimum Romanian and English,
- Training materials: minimum Romanian and English,
- Administrative interfaces: Multi-language support - minimum Romanian and English.

5.2.4 Training deliverables validation

Deliverable	Acceptance (handover) criteria
Needs assessment	• Completed assessment; • Training plan approved
Training materials	• All materials delivered; • Localized content
Training delivery	• All sessions conducted; • Attendance tracked
Training evaluation	• Competency achieved; • Feedback incorporated

5.2.5 Intellectual property and source code deliverables validation

Deliverable	Acceptance (handover) criteria
Source code for customizations	• Complete, compilable source code delivered; • Code repository access provided; • All dependencies documented and included; • Code meets quality standards (clean code, commenting, naming conventions)
Source code for integrations	• Complete source code for all integration components; • API implementations documented; • Integration middleware code included; • Test harnesses and mock services provided
Source code for Moldova-specific developments	• All country-specific business logic; • Regulatory compliance modules; • Localization components; • Custom reporting modules

Deliverable	Acceptance (handover) criteria
Technical documentation for source code	• Architecture documentation; • Code structure explanation; • Development environment setup guide; • Deployment and build procedures; • Database schema modifications
Build and deployment artifacts	• Build scripts and configuration files; • Automated deployment procedures; • Environment configuration templates; • CI/CD pipeline definitions (if applicable)
IP Rights Transfer Documentation	• Signed IP transfer agreement; • Listing of all custom components with IP ownership clarification; • Documentation of pre-existing components (if any) with license terms; • Sub-licensing authorization to End-User Utility

TERMS OF REFERENCE - PART II

FUNCTIONAL REQUIREMENTS AND TECHNICAL SPECIFICATIONS

6. GENERAL PLATFORM REQUIREMENTS

6.1 Solution architecture requirements

In order to ensure long-term scalability, flexibility, security, and operational efficiency, the following requirements are mandatory and non-negotiable for any proposed HES/MDMS solution. These criteria reflect industry best practices and are aligned with current and future needs of the Beneficiary for a modern smart metering infrastructure.

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Verification method
GR-001	**Unified web-based interface**: Single, integrated web interface for both HES and MDMS to streamline end-to-end operations and provide consistent user experience	• UI/UX design documentation; • Screenshots of unified interface; • User workflow demonstrations; • Training cost analysis	• User acceptance testing; • Interface consistency validation; • Workflow efficiency testing; • Multi-role user testing	Two-stage verification

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Verification method
GR-002	**End-to-End (E2E) integrated system**: Seamless data flow from meter acquisition through validation to export to third-party systems without fragmented architectures	• System integration architecture; • Data flow diagrams; • Integration points documentation; • No subsystem dependencies proof	• End-to-end data flow testing; • Integration continuity verification; • Third-party export validation; • Data integrity across all stages	Two-stage verification
GR-003	**Deployment-Agnostic Architecture**: Support for on-premise, cloud-based, or hybrid environments without architectural redesign	• Multi-deployment architecture diagrams; • Environment compatibility matrix; • Migration methodology; • Configuration management approach	• Multi-environment deployment testing; • Migration scenario validation; • Performance consistency verification across environments	Two-stage verification
GR-004	**Hyperscaler Cloud Support**: Deployable on AWS, Microsoft Azure, or Google Cloud Platform with modern IT and cybersecurity standards compliance	• Cloud provider certification; • Deployment guides for each platform; • Security compliance documentation; • Cloud-native architecture proof	• Cloud deployment testing on 2+ platforms; • Security assessment validation; • Cloud scalability demonstration; • Compliance verification	Two-stage verification
GR-005	**Proven Scalability**: Demonstrated horizontal and vertical scalability for 1+ million smart meters in live operation with performance references	• Scalability architecture documentation; • Performance references >1M meters; • Customer testimonials with contact details; • Live deployment evidence; • Scaling methodology	• Load testing at 1M+ meter simulation; • Horizontal scaling demonstration; • Vertical scaling validation; • Performance benchmarking; • Resource optimization testing	Two-stage verification

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Verification method
GR-006	**Unified Inventory Management**: Centralized, real-time synchronized inventory covering both HES and MDMS domains with all device-related attributes	• Inventory management architecture; • Real-time synchronization design; • Device attribute schema; • Integration with HES/MDMS workflows	• Real-time sync testing; • Inventory accuracy validation; • Cross-domain consistency verification; • Device lifecycle management testing	Two-stage verification
GR-007	**High Availability (1+1 Configuration)**: Redundant architecture with automated failover capabilities to ensure continuous operation	• HA architecture diagrams; • Redundancy design documentation; • Failover mechanisms; • Recovery procedures	• Failover testing; • Switchover time measurement (<30 seconds); • Data integrity verification; • Disaster recovery validation	Two-stage verification
GR-008	**Open Architecture with APIs**: Comprehensive API framework supporting third-party integrations and future extensibility	• Complete API documentation; • Integration framework specifications; • SDK/sample code provision; • API versioning strategy	• API functional testing; • Third-party integration demonstration; • Performance benchmarking; • Backward compatibility testing	Two-stage verification
GR-009	**Mature Commercial Platform**: Proven market presence with 3+ years commercial availability and 3+ deployments >100k meters	• Product release history (3+ years); • Reference deployments >100k meters; • Customer reference letters with contacts; • Market presence documentation	Not applicable	Documentation review only
GR-010	**Advanced Security Framework**: Enterprise-grade security with role-based access, audit trails, and cybersecurity compliance for smart grid environments	• Security architecture documentation; • Compliance certifications; • Role-based access design;	• Security penetration testing; • Access control validation; • Audit trail verification;	Two-stage verification

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Verification method
		• Audit trail specifications	• Compliance assessment	

6.2 Vendor neutrality and interoperability

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Notes
GR-011	Vendor-neutral platform	• Multi-vendor support documentation; • Protocol abstraction layer design; • Integration examples	• Test with 3+ meter vendors; • Verify no vendor lock-in; • Performance consistency	Critical for evaluation
GR-012	Meter brands integration	• Compatibility matrix; • Integration guides per brand; • Certification letters	• Test each meter type; • Verification of the full functionality; • No additional or hidden licenses	Must test all 11 brands
GR-013	Third-party HES integration	• Integration framework; • API specifications; • Past integration examples	Not required initially--	Future-proofing check
GR-014	Standard interfaces	• Interface specifications; • Integration patterns; • Protocol support	• Integration testing with stubs; • End-to-end testing in production	Phased testing approach

6.3 Standards compliance

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
GR-015	Protocol support (DLMS, OSGP, DSMR, MODBUS, M-BUS etc.)	• Protocol implementation docs; • Compliance certificates;	• Protocol analyzer testing;

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Test results from labs	• Interoperability testing; • Compliance verification
GR-016	CIM IEC 61968-9	• CIM compliance certificate; • Data model documentation; • Implementation guide	Not required
GR-017	IEC 61850 support	• Technical documentation; • Integration examples	Not required (Optional)
GR-018	GDPR compliance	• Privacy by design documentation; • Data flow diagrams; • Compliance assessment	• Privacy audit; • Data handling verification; • Access control testing

6.4 Performance and scalability

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Critical notes
GR-019	Minimum 100 k meters with 15-min intervals	• Architecture for scale; • Sizing calculations; • Reference deployments	• Progressive load testing; • 30-day stability test; • Resource monitoring	Phased testing approach
GR-020	On-demand read <30 sec	• Performance design; • Network optimization	• Response time testing; • 95th percentile verification; • Various load conditions	Production only
GR-021	1.25M messages/hour	• Performance benchmarks; • Architecture design; • Queueing strategy	• Stress testing; • Message throughput test; • Queue performance	Lab + production
GR-022	5-year storage, sub-second query	• Database design; • Partitioning strategy; • Index optimization	• Query performance testing; • Data aging simulation; • Archive/retrieve testing	Critical for operations

6.5 Availability and reliability

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
GR-023	99.9% availability	• HA architecture; • Service-level reqiurements commitments; • Reference metrics	• 90-day monitoring; • Availability calculation; • Incident tracking
GR-024	RPO ≤ 15 minutes	• Backup architecture; • Replication design	• Backup/restore testing; • Data loss simulation; • Recovery verification
GR-025	RTO ≤ 1 hour	• DR procedures; • Recovery automation	• DR drill execution; • Timed recovery test; • Service restoration
GR-026	Automatic failover	• Failover design; • Cluster configuration	• Failover testing; • Various failure scenarios; • Data consistency check

7. HES FUNCTIONAL REQUIREMENTS

7.1 Data collection and management

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Notes
HES-FR-001	Scheduled reading with intervals	• Scheduler design; • Configuration options; • Performance impact	• Configure all intervals; • Verify collection accuracy; • Performance under load	Could be added specific interval options
HES-FR-002	Push/pull modes	• Architecture for both modes; • Protocol support; • Use case examples	• Test both modes; • Switch between modes; • Performance comparison	Could be defined when each mode is used
HES-FR-003	On-demand reading <30s	• Communication optimization; • Priority handling	• Response time testing; • Load impact testing; • Various meter types	Production environment only
HES-FR-004	Data concentrator support	• DC integration architecture; • Supported models; • Management features	• DC installation; • Data aggregation testing; • Hierarchy validation	Could be listed specific DC models
HES-FR-005	Missing data handling	• Retry logic design; • Gap detection; • Recovery procedures	• Simulate data gaps; • Verify retry mechanism;	Could be defined retry parameters

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Notes
			• Recovery success rate	
HES-FR-006	Multiple data types	• Data model documentation; • Storage design; • Processing logic	• Collect all data types; • Verify data integrity; • Processing accuracy	Could be listed all data types
HES-FR-007	Bi-directional data	• Prosumer support design; • Net metering logic; • Data flows	• Prosumer meter testing; • Import/export accuracy; • Settlement calculations	Critical for renewables
HES-FR-008	Manual import	• Import formats; • Validation rules; • UI design	• Import various formats; • Validation testing; • Error handling	Could be specified formats

7.2 Remote management and control

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
HES-FR-009	Remote disconnect	• Security procedures; • Command flow; • Audit mechanism	• Execute disconnect; • Verify security; • Audit trail check
HES-FR-010	Load limitation	• Load control design; • DR integration; • Priority logic	• Set load limits; • Verify enforcement; • DR scenario test
HES-FR-011	Prepayment (Optional)	• Prepayment logic; • Credit management; • Integration design	Not required initially
HES-FR-012	Tariff/TOU config	• Tariff structures; • Configuration UI; • Validation rules	• Configure tariffs; • Apply to meters; • Verify billing
HES-FR-013	Command queuing	• Queue management; • Priority algorithm; • Status tracking	• Queue multiple commands; • Verify priority; • Track execution
HES-FR-014	Command retry	• Retry logic; • Status updates; • Failure handling	• Simulate failures; • Verify retries; • Success tracking

7.3 Device configuration and management

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
HES-FR-015	Remote configuration of communication parameters	• Configuration interface documentation; • Parameter types supported; • Security mechanisms for remote config; • Example configuration templates; • Reference implementation evidence	• Configure 100 meters remotely; • Change communication parameters; • Verify parameter persistence; • Test rollback capability; • Measure configuration time
HES-FR-016	Time synchronization for meters and data concentrators with < 1 second accuracy	• Time sync protocol documentation; • NTP/SNTP implementation details; • Accuracy calculation methodology; • Time zone handling approach; • DST transition procedures	• Synchronize 1000 meters; • Measure time drift over 30 days; • Test DST transitions; • Verify <1 second accuracy; • Test sync failure recovery
HES-FR-017	Remote firmware upgrade capability (FOTA) with rollback option	• FOTA architecture documentation; • Rollback mechanism design; • Security measures for firmware; • Batch update procedures; • Success rate from deployments	• Upgrade 100 meters firmware; • Test rollback on 10% failure; • Verify meter functionality post-upgrade; • Measure bandwidth impact; • Test various meter models
HES-FR-018	Device lifecycle management (commissioning, decommissioning, replacement)	• Lifecycle workflow diagrams; • State transition documentation; • Integration with asset management; • Audit trail mechanisms; • Bulk operation support	• Commission 500 new meters; • Decommission 100 meters; • Replace 50 meters; • Verify data continuity; • Test audit trail completeness
HES-FR-019	Automated device provisioning and discovery	• Auto-discovery protocol details; • Provisioning workflow automation;	• Auto-discover 100 new meters;

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Security during provisioning; • Bulk provisioning capabilities; • Network scanning approach	• Test various communication types; • Measure provisioning time; • Verify security compliance; • Test error scenarios
HES-FR-020	Device health monitoring and diagnostics	• Health metrics collected; • Diagnostic capabilities list; • Alert threshold configuration; • Dashboard mockups; • Historical trend analysis	• Monitor 1000 meters for 30 days; • Test diagnostic commands; • Verify alert generation; • Measure detection accuracy; • Test predictive diagnostics

7.4 Communication management

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
HES-FR-021	Support for multiple communication technologies: PLC (PRIME, G3-PLC, OSGP), PLC HYBRID, Serial RS485, RF Mesh, Cellular (2G/3G/4G/5G), Ethernet	• Communication architecture diagrams; • Protocol stack documentation; • Performance data per technology; • Simultaneous handling design; • Reference deployments per type	• Deploy mixed technology network; • Test 200 meters per technology; • Verify simultaneous operation; • Measure performance per type; • Test technology switching
HES-FR-022	Communication path optimization and automatic rerouting	• Path optimization algorithms; • Rerouting trigger conditions; • Mesh network capabilities; • Failover time specifications; • Network topology adaptation	• Simulate path failures; • Measure rerouting time; • Test optimization logic; • Verify data continuity; • Load test rerouting

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
HES-FR-023	Bandwidth management and traffic prioritization	• Bandwidth allocation design; • QoS implementation details; • Priority queue mechanisms; • Traffic shaping capabilities; • Congestion handling	• Test under bandwidth constraints; • Verify priority enforcement; • Measure latency per priority; • Test congestion scenarios; • Monitor bandwidth usage
HES-FR-024	Support for IPv4 and IPv6 addressing	• Dual-stack implementation; • Address management design; • Migration path documentation; • NAT/firewall considerations; • Security implications	• Configure IPv4 and IPv6 meters; • Test dual-stack operation; • Verify address management; • Test migration procedures; • Check security controls
HES-FR-025	VPN support for secure communications	• VPN architecture design; • Supported VPN protocols; • Key management approach; • Performance impact analysis; • Scalability considerations	• Configure VPN tunnels; • Test encryption effectiveness; • Measure performance overhead; • Verify key rotation; • Test failover scenarios

7.5 Security management

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
HES-FR-026	DLMS/COSEM security suite implementation (authentication, encryption)	• Security suite documentation; • Cipher suite specifications; • Authentication mechanisms; • Key exchange protocols; • Compliance certificates	• Test authentication scenarios; • Verify encryption strength; • Attempt security breaches; • Measure crypto overhead;

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
			• Test with all meter types
HES-FR-027	Key management system for security keys and certificates	• Key lifecycle management design; • Certificate authority integration; • Key storage architecture; • Rotation procedures; • Recovery mechanisms	• Generate and distribute keys; • Test key rotation; • Verify secure storage; • Test certificate renewal; • Simulate key compromise
HES-FR-028	Role-based access control (RBAC) with audit trails	• RBAC model documentation; • Role definitions and permissions; • Audit trail architecture; • Compliance mapping; • Integration with enterprise IAM	• Configure 20 different roles; • Test permission enforcement; • Verify audit completeness; • Test privilege escalation; • Review audit reports
HES-FR-029	Support for Hardware Security Modules (HSM)	• HSM integration architecture; • Supported HSM models; • Performance considerations; • Key operations supported; • Failover design	Not required for initial acceptance
HES-FR-030	Encrypted data storage and transmission	• Encryption architecture; • Algorithm specifications; • Key management integration; • Performance impact data; • Compliance documentation	• Verify storage encryption; • Test transmission security; • Attempt data recovery; • Measure performance impact; • Audit encryption coverage

7.6 Event and alarm management

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
HES-FR-031	Real-time event processing and notification (including exceeding the generation resulting from the contracted power	• Event processing architecture; • Notification mechanisms; • Latency specifications; • Scalability design; • Event categorization	• Generate 10,000 events/hour; • Measure processing latency; • Verify notification delivery; • Test event prioritization; • Check event integrity
HES-FR-032	Configurable alarm thresholds and escalation rules	• Alarm configuration interface; • Threshold types supported; • Escalation workflow engine; • Rule definition examples; • Override mechanisms	• Configure 50 alarm rules; • Test threshold triggers; • Verify escalation paths; • Test rule conflicts; • Measure response times
HES-FR-033	Event correlation and root cause analysis	• Correlation engine design; • Analysis algorithms; • Pattern recognition capabilities; • Machine learning integration; • Visualization approach	Not required for initial acceptance
HES-FR-034	Integration with SCADA/DMS/OMS for outage management	• Integration architecture; • Protocol specifications; • Data mapping documentation; • Latency requirements; • Redundancy design	• Simulate 100 outage events' • Verify SCADA integration; • Test event correlation; • Measure detection time; • Test restoration tracking • Verify real-time - status of the circuit breaker at the connection point; - measurement of active and reactive power flows, current and voltage at the connection point

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
HES-FR-035	Power quality event detection and reporting	• PQ parameters monitored; • Detection algorithms; • Reporting templates; • Threshold configurations; • Standards compliance	• Generate PQ disturbances; • Verify detection accuracy; • Test report generation; • Validate measurements; • Check EN 50160 compliance

7.7 Meter brand compatibility

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
HES-FR-036	Full integration support for ADD (All ADDAX models)	• Integration documentation; • Protocol implementation proof; • Feature support matrix; • Test lab results; • Reference deployments	• Test 10 ADDAX meters; • Verify all functions; • Test firmware updates; • Check security features; • 7-day stability test
HES-FR-037	Full integration support for NIK ELECTRONIKA (2100 and 2300 series)	• Model-specific documentation; • Communication protocols used; • Feature compatibility list; • Integration certificates; • Performance benchmarks	• Test 10 meters per series; • Verify data collection; • Test remote controls; • Check event handling; • Validate VEE integration
HES-FR-038	Full integration support for LANDIS+GYR (ZMD, ZMG and ZMY series)	• L+G certification documents; • Protocol compliance proof; • Security implementation; • Feature coverage matrix; • Integration examples	• Test 5 meters per series; • Full functionality check; • Security validation; • Performance testing; • Load profile verification
HES-FR-039	Full integration support for ZIV (5CTB series)	• ZIV integration guide; • Protocol specifications; • Supported features list;	• Test 10 5CTB meters; • Verify all registers; • Test configurations;

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Test results documentation; • Known limitations	• Check firmware update; • Validate events
HES-FR-040	Full integration support for APATOR (smart ESOX and OTUS1/3 models)	• APATOR compatibility docs; • Feature support details; • Communication methods; • Security compliance; • Reference sites	• Test both model types; • Verify communications; • Test advanced features; • Check interoperability; • Stress testing
HES-FR-041	Full integration support for ISKRAEMECO (MT and ME series)	• ISKRA protocol docs; • Integration architecture; • Feature mapping; • Performance data; • Deployment examples	• Test MT and ME series; • Full feature validation; • Communication testing; • Security verification; • Long-term stability
HES-FR-042	Full integration support for LUNA (LSM series)	• LUNA integration specs; • Protocol implementation; • Feature compatibility; • Test lab results; • Support documentation	• Test 10 LSM meters; • Verify all functions; • Test configurations; • Check data quality; • Integration testing
HES-FR-043	Full integration support for ABB (Alpha 2 model)	• ABB Alpha 2 documentation; • Protocol compliance; • Feature coverage; • Security implementation; • Performance metrics	• Test 5 Alpha 2 meters; • Full functionality test; • Security validation; • Performance check; • Event handling test
HES-FR-044	Full integration support for ELSTER (A1800 model)	• ELSTER integration guide; • A1800 specific features; • Communication protocols; • Test certifications; • Deployment evidence	• Test 5 A1800 meters; • Verify all registers; • Test load profiles; • Check PQ features; • Firmware update test
HES-FR-045	Full integration support for ELGAMA (GAMA 3000 model)	• ELGAMA protocol docs; • Integration specifications;	• Test 5 GAMA 3000; • Full feature check; • Communication test; • Security validation;

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Feature support matrix; • Security compliance; • Reference deployments	• Performance verification
HES-FR-046	Full integration support for METCOM (MCS301)	• METCOM integration docs; • MCS301 specifications; • Protocol implementation; • Feature coverage; • Test results	• Test 5 MCS301 meters; • Verify functionality; • Test communications; • Check data accuracy; • Stability testing

7.8 Data analytics and reporting

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
HES-FR-047	Real-time dashboard with key performance indicators	• Dashboard design mockups; • KPI definitions and calculations; • Refresh rate specifications; • User role customization; • Performance optimization	• Load dashboard with 100 K meters; • Verify real-time updates; • Test KPI accuracy; • Check responsiveness; • Multi-user testing
HES-FR-048	Configurable reports for operational and management needs with predefined templates (standard operational reports) as well as user-defined ad-hoc queries.	• Report template library; • Configuration interface; • Scheduling capabilities; • Distribution mechanisms; • Sample report outputs	• Create 20 custom reports; • Test scheduling options; • Verify data accuracy; • Test distribution methods; • Performance validation • role-based access control
HES-FR-049	Data export capabilities (CSV, XML, JSON, PDF, XLSX)	• Export format specifications; • Data mapping documentation; • Performance specifications;	• Export 100K records; • Test all formats; • Verify data integrity; • Measure export time;

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Compression options; • API documentation	• Test large datasets
HES-FR-050	API for external analytics platforms	• API documentation (Open API); • Authentication methods; • Rate limiting design; • Data models exposed; • Integration examples	• Test API endpoints; • Verify data access; • Load test APIs; • Check security; • Integration testing

7.9 Advanced functionalities

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
HES-FR-051	Support for Virtual Power Plants (VPP) management	• VPP architecture design; • Aggregation capabilities; • Control mechanisms; • Integration approach; • Scalability analysis	Not required for initial acceptance
HES-FR-052	Energy Communities management with peer-to-peer trading support	• Community model design; • P2P trading logic; • Settlement mechanisms; • Security considerations	Not required for initial acceptance
HES-FR-053	Integration with Asset Management platforms	• Integration architecture; • Data synchronization design; • API specifications; • Workflow integration; • Reference implementations	• Test asset data sync; • Verify bi-directional flow; • Test work order integration; • Check data consistency; • Performance validation
~~HES-FR-054~~	~~Support for electric vehicle charging infrastructure monitoring~~	~~• EV charger integration design;~~ ~~• Protocol support (OCPP);~~ ~~• Load management approach;~~ ~~• Billing integration;~~	~~Not required for initial acceptance~~

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		~~• Scalability considerations~~	
~~HES-FR-055~~	~~Integration with weather data for predictive analytics~~	~~• Weather API integration;~~ ~~• Data correlation methods;~~ ~~• Predictive algorithms;~~ ~~• Accuracy improvements;~~ ~~• Use case examples~~	~~Not required for initial acceptance~~

8. HES TECHNICAL SPECIFICATIONS

8.1 Architecture requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
HES-T-001	Multi-tier architecture (presentation, business logic, data layers)	• Detailed architecture diagrams showing tier separation; • Component deployment model; • Inter-tier communication protocols; • Scalability approach per tier; • Security boundaries documentation	Architecture review and documentation validation only
HES-T-002	Microservices or service-oriented architecture for modularity	• Service decomposition documentation; • Service catalog with responsibilities; • Inter-service communication design; • Service discovery mechanism; • Container orchestration approach	• Deploy modular components; • Test service independence; • Verify service scaling; • Test service failure isolation; • Validate API contracts
HES-T-003	Container support (Docker/Kubernetes) for deployment	• Container architecture design; • Docker file/manifest examples; • Orchestration configuration; • Resource requirements;	• Deploy in container environment; • Test container scaling; • Verify resource limits; • Test rolling updates; • Validate persistence

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• CI/CD pipeline integration	
HES-T-004	RESTful API architecture with OpenAPI documentation	• Complete OpenAPI 3.0 specifications; • API design principles document; • Versioning strategy; • Authentication / authorization design; • Sample API responses	• Validate against OpenAPI spec; • Test all endpoints; • Verify HATEOAS compliance; • Check response formats; • Load test APIs

8.2 Technology stack requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
HES-T-005	Database: Enterprise-grade RDBMS (Oracle, PostgreSQL, SQL Server)	• Database selection justification; • Schema design documentation; • Performance benchmarks; • HA/DR configuration; • Licensing model and period covergare included in the offer	• Install and configure database; • Performance benchmark tests; • Failover testing; • Backup/restore validation; • Load testing at scale
HES-T-006	Support for time-series databases for meter data	• Time-series DB architecture; • Data retention policies; • Compression strategies; • Query optimization approach; • Integration with RDBMS	• Store 1 year of 15-min data; • Query performance testing; • Compression ratio validation; • Aggregation performance; • Data aging tests
HES-T-007	Message queuing system for asynchronous processing	• Message queue selection rationale; • Queue architecture design; • Message schemas documentation; • Reliability guarantees; • Performance specifications	• Queue throughput testing; • Message persistence verification; • Failover scenario testing; • Dead letter queue handling; • Performance under load

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
HES-T-008	In-memory caching for performance optimization	• Caching strategy documentation; • Cache architecture design; • TTL and eviction policies; • Cache warming procedures; • Performance impact analysis	• Cache hit ratio measurement; • Performance improvement validation; • Cache invalidation testing; • Memory usage monitoring; • Failover behavior

8.3 Integration requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
HES-T-009	Web services (SOAP/REST) for system integration	• Web service specifications; • WSDL/OpenAPI documentation; • Security implementation; • Error handling design; • Integration patterns used	• Test all service endpoints; • Validate SOAP/REST compliance; • Error scenario testing; • Security validation; • Performance benchmarking
HES-T-010	Message-based integration (JMS, AMQP, MQTT)	• Messaging architecture design; • Protocol selection rationale; • Message format specifications; • QoS configurations; • Topic/queue structure	• Message flow testing; • Protocol compliance verification; • Reliability testing; • Performance measurement; • Failover scenarios
HES-T-011	File-based integration with configurable formats	• File format specifications; • Transfer mechanism design; • Scheduling capabilities; • Error handling procedures; • File size limitations	• Test all file formats; • Large file handling (>1GB); • Transfer reliability testing; • Format validation; • Error recovery testing
HES-T-012	Real-time streaming capabilities (Kafka, RabbitMQ)	• Streaming architecture design; • Topic/exchange configuration; • Partitioning strategy; • Consumer group design; • Performance projections	• Stream throughput testing; • Latency measurement; • Partition rebalancing; • Consumer lag monitoring;

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
			• Fault tolerance testing

8.4 Performance specifications

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
HES-T-013	Concurrent user support: minimum 100 users	• User session architecture; • Resource allocation per user; • Session management design; • Performance projections; • Reference deployment data	• Load test with 100+ users; • Measure response times; • Monitor resource usage; • Test session management; • Verify no degradation
HES-T-014	Transaction throughput: 10,000 TPS for meter readings	• Performance architecture design; • Throughput calculations; • Bottleneck analysis; • Scaling approach; • Benchmark test results	• Sustained load test 24 hours; • Measure actual TPS; • Monitor system resources; • Verify data integrity; • Test burst scenarios
HES-T-015	Data latency: < 5 seconds from meter to database	• Data flow architecture; • Latency breakdown analysis; • Optimization strategies; • Network considerations; • Processing pipeline design	• End-to-end latency testing; • Measure at each stage; • Test various data volumes; • Different network conditions; • Peak load validation
HES-T-016	Command execution: < 30 seconds end-to-end	• Command flow documentation; • Timeout configurations; • Retry mechanisms; • Priority handling design; • Performance optimization	• Execute 1000 commands; • Measure execution times; • Test under load conditions; • Verify success rates; • Priority queue testing

8.5 Security specifications

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
HES-T-017	Minimum TLS 1.3 (or latest version upon implementation stage) for all external communications	• TLS implementation documentation; • Certificate management process; • Cipher suite configuration; • Protocol downgrade prevention; • Performance impact analysis	• SSL/TLS scanner validation; • Cipher suite verification; • Certificate chain testing; • Protocol version enforcement; • MITM attack simulation
HES-T-018	Minimum AES-256 encryption for data at rest	• Encryption architecture design; • Key management procedures; • Encryption scope definition; • Performance impact data; • Compliance documentation	• Verify encryption status; • Test key rotation; • Attempt data recovery; • Performance measurement; • Compliance validation
HES-T-019	OAuth 2.0/SAML for authentication	• Authentication flow diagrams; • Token management design; • IdP integration approach; • Session management; • Security considerations	• Test OAuth flows; • SAML assertion validation; • Token expiry handling; • Multi-factor authentication; • Session security testing
HES-T-020	API rate limiting and DDoS protection	• Rate limiting architecture; • DDoS mitigation strategy; • Threshold configurations; • Alert mechanisms; • Recovery procedures	• Rate limit testing; • DDoS simulation; • Threshold validation; • Alert verification; • Recovery time measurement

9. USE CASES AND BUSINESS PROCESSES

9.1 Meter data collection use cases

UC-001: Scheduled meter reading

Aspect	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Moldova customization
Use case design	• Workflow diagrams; • Scheduling algorithm; • Data flow documentation; • Error handling procedures	-	-
Interval configuration	• Configuration interface; • Supported intervals list	• Configure all intervals; • Verify execution accuracy	• Local utility intervals; • DSO requirements
Success rate (98%)	• Historical performance data; • Reference site metrics	• 30-day continuous test; • Success rate calculation; • Failure analysis	• Network conditions; • Local meter types
Data validation	• Validation rules design; • Data quality checks	• Validation accuracy test; • Error detection rate	• Moldova data formats; • Local standards

UC-002: On-demand meter reading

Aspect	Evidence required at Offer evaluation stage	Acceptance (handover) test method
UI/API design	• UI mockups; • API specifications; • User workflows	• UI usability testing; • API functional testing
Priority handling	• Priority algorithm; • Queue management design	• Priority verification; • Queue behavior under load
Response time (<30s)	• Network optimization design; • Performance projections	• Response time measurement; • Various load conditions
Retry mechanism	• Retry logic documentation; • Configuration options	• Retry behavior testing; • Success after retry

UC-003: Meter event processing

Aspect	**Evidence required at Offer evaluation stage**	Acceptance (handover) test method
Event detection capability for power outages, tamper attempts, voltage anomalies, meter cover removal	• Event types catalog with descriptions; • Detection algorithm documentation; • Event priority classification;	• Generate each event type on 50 meters; • Verify 100% detection rate; • Measure detection latency; • Test simultaneous events; • Validate event accuracy

Aspect	**Evidence required at Offer evaluation stage**	Acceptance (handover) test method
	• Hardware/firmware requirements; • Reference implementation examples	
Real-time event transmission from meter to HES with guaranteed delivery	• Communication protocol for events; • Delivery guarantee mechanisms; • Retry logic documentation; • Buffer management design; • Network optimization approach	• Disconnect/reconnect network during transmission; • Verify event delivery under poor signal; • Test event buffer overflow; • Measure transmission time; • Validate no event loss
Event processing and categorization with configurable rules engine	• Event processing architecture; • Categorization rule examples; • Rule engine capabilities; • Performance specifications; • Customization procedures	• Configure 20 categorization rules; • Process 10,000 events/hour; • Test rule conflicts resolution; • Verify processing accuracy; • Measure categorization time
Automated action triggering based on event types and severity	• Action framework documentation; • Trigger condition examples; • Workflow engine design; • Integration mechanisms; • Escalation procedures	• Configure actions for each event type; • Test action execution timing; • Verify workflow completion; • Test escalation scenarios; • Validate action logging

Aspect	**Evidence required at Offer evaluation stage**	Acceptance (handover) test method
Event logging with complete audit trail and notification distribution	• Logging architecture design; • Audit trail specifications; • Notification channels supported; • Distribution rules engine; • Retention policies	• Generate 1,000 events across types; • Verify complete audit trail; • Test notification delivery; • Check log integrity; • Validate search capabilities
Event correlation for outage management and root cause analysis	• Correlation algorithm design; • Topology awareness approach; • Pattern recognition methods; • Integration with GIS/ADMS; • Visualization capabilities	• Simulate area-wide outage; • Verify correlation accuracy; • Test root cause identification; • Measure analysis time; • Validate visualization

9.2 Remote control use cases

UC-004: Remote disconnect/reconnect

Aspect	**Evidence required at Offer evaluation stage**	**Acceptance (handover) test method**	**Critical considerations**
Security design	• Authentication flow; • Authorization matrix; • Audit trail design; • Encryption methods	-	Moldova regulations compliance
Command flow	• Command sequence diagram; • State management; • Rollback procedures	• End-to-end execution; • State verification; • Failure scenarios	Safety procedures required
Multi-factor authentication	• MFA implementation; • Integration options	• MFA functionality test; • Bypass prevention	Mandatory for critical operations

Aspect	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Critical considerations
Confirmation process	• Confirmation protocol; • Timeout handling	• Confirmation timing; • Reliability testing	Legal requirements

UC-005: Load limitation

Aspect	Evidence required at Offer evaluation stage	Acceptance (handover) test method
Load control design	• Control algorithm; • Threshold management; • Override capabilities	• Threshold enforcement; • Accuracy verification
DR integration	• DR program support; • Event handling; • Customer opt-out	• DR scenario testing; • Multi-meter coordination
Monitoring	• Real-time monitoring design; • Alert mechanisms	• Monitoring accuracy; • Alert delivery

9.3 Configuration management use cases

UC-006: Firmware update

Aspect	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Risk mitigation
Update process	• FOTA architecture; • Version management; • Rollback design	• Update execution; • Success rate; • Rollback testing	Mandatory rollback capability
Batch management	• Batch sizing logic; • Network optimization; • Progress tracking	• 1000 meters/hour; • Network impact; • Failure isolation	Phased rollout required
Validation	• Pre/post validation; • Integrity checks; • Compatibility matrix	• Validation accuracy; • Meter functionality; • No service disruption	Critical for stability

UC-007: Time synchronization

Aspect	Evidence required at Offer evaluation stage	Acceptance (handover) test method
Periodic time drift monitoring with configurable check intervals	• Time monitoring architecture; • Drift detection algorithms; • Configurable parameters; • Threshold specifications; • Alert mechanisms	• Monitor 1,000 meters for 30 days; • Configure various check intervals; • Measure drift detection accuracy; • Test threshold alerts;

Aspect	**Evidence required at Offer evaluation stage**	Acceptance (handover) test method
		• Verify monitoring overhead
Automated synchronization command generation and distribution	• Command generation logic; • Distribution mechanisms; • Priority handling design; • Batch processing capability; • Network optimization	• Synchronize 10,000 meters; • Test batch synchronization; • Measure command distribution time; • Verify priority handling; • Test under network load
Device clock update with minimal service disruption	• Clock update procedures; • Service continuity design; • Data integrity measures; • Rollback mechanisms; • Impact mitigation strategies	• Update clocks on active meters; • Verify no data loss; • Test during data collection; • Measure service disruption; • Validate data continuity
Synchronization logging and compliance reporting	• Logging framework design; • Compliance report templates; • Audit trail specifications; • Success/failure tracking; • Historical analysis tools	• Review 30-day sync logs; • Generate compliance reports; • Verify log completeness; • Test failure tracking; • Validate analytics
Time accuracy maintenance < 1 second across all devices	• Accuracy assurance methods; • NTP server architecture; • Network latency compensation; • GPS integration (if any);	• Measure accuracy on 1,000 meters; • Test over 30 days continuous; • Verify <1 second deviation;

Aspect	Evidence required at Offer evaluation stage	Acceptance (handover) test method
	• Accuracy monitoring design	• Test DST transitions; • Validate under load
Daylight Saving Time (DST) transition handling	• DST handling procedures; • Data continuity approach; • Billing impact mitigation; • Communication protocols; • Testing procedures	• Execute spring transition; • Execute fall transition; • Verify no data gaps/overlaps; • Test billing continuity; • Validate event handling

9.4 Security management use cases

UC-008: Key rotation

Aspect	Evidence required at Offer evaluation stage	Acceptance (handover) test method
Key management	• Key lifecycle design; • HSM integration (optional); • Key distribution protocol	• Key generation test; • Distribution success; • No service interruption
Rotation schedule	• Policy documentation; • Automation design; • Exception handling	• Schedule execution; • Completion tracking; • Failure recovery
Audit trail	• Audit log design; • Retention policy; • Compliance mapping	• Audit completeness; • Log integrity; • Compliance verification

9.5 Analytics and reporting use cases

UC-009: Energy balance calculation

Aspect	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Moldova specifics
Calculation method	• Algorithm documentation; • Accuracy projections; • Loss categorization	• Calculation accuracy; • Performance testing; • Result validation	Local loss factors
Aggregation logic	• Data model design; • Hierarchy handling; • Time synchronization	• Aggregation testing; • Large-scale performance; • Data completeness	Network topology
Report generation	• Report templates; • Scheduling options; • Distribution methods	• Report accuracy; • Generation time; • Format validation	Regulatory formats

UC-010: Power quality analysis

Aspect	Evidence required at Offer evaluation stage	Acceptance (handover) test method
PQ event collection from capable meters (voltage, frequency, harmonics)	• PQ parameters monitored list; • Collection mechanisms; • Data formats specification; • Meter capability detection; • Storage architecture	• Collect from 100 PQ meters; • Verify all parameters captured; • Test collection reliability; • Validate data accuracy; • Check completeness
Pattern analysis and trend identification algorithms	• Analysis algorithm documentation; • Pattern recognition methods; • Statistical models used; • Machine learning integration; • Visualization approaches	• Analyze 30 days of PQ data; • Identify known patterns; • Test trend predictions; • Verify algorithm accuracy; • Validate visualizations
EN 50160 compliance violation detection and classification	• EN 50160 implementation guide; • Violation detection rules; • Classification methodology; • Compliance thresholds; • Exception handling	• Inject standard violations; • Verify detection accuracy; • Test classification logic; • Validate against EN 50160; • Check edge cases
Automated PQ report generation with customizable templates	• Report template library; • Customization capabilities; • Scheduling mechanisms; • Distribution options; • Format specifications	• Generate all report types; • Test customization options; • Verify data accuracy; • Check scheduling reliability; • Validate formats
Real-time alerting for PQ threshold violations	• Alert framework design; • Threshold configuration; • Notification channels; • Escalation procedures; • Alert suppression logic	• Configure 20 alert rules; • Test threshold detection; • Verify notification delivery; • Test escalation paths; • Validate suppression

Aspect	Evidence required at Offer evaluation stage	Acceptance (handover) test method
Integration with grid management systems for PQ improvement	• Integration architecture; • Data exchange formats; • Real-time capabilities; • Action recommendations; • Feedback mechanisms	• Test SCADA integration; • Verify data exchange; • Test improvement actions; • Measure response times; • Validate feedback loop

10. MDMS FUNCTIONAL REQUIREMENTS

10.1 Data collection and storage

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Moldova customization
MDMS-FR-001	Automatic downloading with scheduling	• Scheduler architecture • Configuration interface • Database design	• Configure schedules • Verify execution • Performance under load	Local time zones
MDMS-FR-002	Multiple collection frequencies	• Supported frequencies list • Configuration documentation	Configuration verification only	DSO requirements
MDMS-FR-003	Multiple HES integration	• Integration architecture • Protocol support • Past implementations	• Test with 2+ HES systems • Data consistency • Performance impact	Local HES systems
MDMS-FR-004	18 months live + 6 years archive	• Storage architecture • Archival strategy • Sizing calculations	• Storage verification • Archive/retrieve test • Performance impact	Regulatory requirements
MDMS-FR-005	Interval and scalar data	• Data model documentation • Type definitions	Data type verification	Local data formats
MDMS-FR-006	Automatic timestamping	• Timestamp methodology • Time zone handling	• Timestamp accuracy • DST handling • End-of-interval verification	Moldova time zone

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Moldova customization
MDMS-FR-007	Standardized units	• Unit conversion design • Standards compliance	• Unit verification • Conversion accuracy	Local standards
MDMS-FR-008	Duplicate handling	• Deduplication algorithm • Performance impact	• Duplicate scenarios • Data integrity • Performance testing	Network conditions

10.2 Data validation, estimation and editing (VEE)

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Critical aspects
MDMS-FR-009	Configurable validation rules	• Rule engine design • Rule templates • Configuration UI	• Rule configuration • Validation accuracy • Performance impact	Moldova-specific rules
MDMS-FR-010	Anomaly flagging	• Detection algorithms • Reason code catalog	• Detection accuracy • False positive rate • Alert generation	Local consumption patterns
MDMS-FR-011	Manual editing with audit	• Edit workflow • Audit trail design • Security controls	• Edit functionality • Audit completeness • Authorization testing	Regulatory compliance
MDMS-FR-012	Estimation algorithms	• Algorithm documentation • Accuracy projections • Historical methods	• Estimation accuracy • Various scenarios • Performance testing	Local patterns
MDMS-FR-013	Status code maintenance	• Status model • Transition rules	• Status tracking • Reporting accuracy	Status definitions
MDMS-FR-014	Automatic updates	• Update logic • Trigger mechanisms	• Update scenarios • Data integrity • Notification testing	Update policies
MDMS-FR-015	Data integrity checks	• Checksum methods • Validation points	• Integrity verification • Error detection rate	Critical for billing
MDMS-FR-016	Check meter support	• Check meter model • Variance calculation	• Installation process • Variance reporting	Quality assurance

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Critical aspects
			• Alert thresholds	

10.3 Data processing and transformation

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MDMS-FR-017	Meter provisioning	• Provisioning workflow • Automation design • Integration points	• Add/update/delete tests • Bulk operations • Error scenarios
MDMS-FR-018	DST correlation	• DST handling logic • Historical approach	• Spring/fall transitions • Data continuity • Reporting accuracy
MDMS-FR-019	Unbilled energy calc	• Calculation methodology • Accounting integration	• Monthly calculations • Accuracy verification • Reconciliation
MDMS-FR-020	Anomaly detection	• Detection algorithms • ML models (if used) • Threshold management	• Detection accuracy • False positive rate • Response time
MDMS-FR-021	Fraud detection	• Detection patterns • Alert mechanisms • Case studies	• Known fraud scenarios • Detection rate • Investigation tools
MDMS-FR-022	Aggregation/trends	• Aggregation engine • Statistical methods	• Various aggregations • Performance at scale • Accuracy verification
MDMS-FR-023	Energy communities	• Community model • Settlement algorithms • P2P trading logic	• Community scenarios • Settlement accuracy • Scale testing
MDMS-FR-024	TOU processing	• TOU engine design • Rate structures • Calendar handling	• Rate application • Transition handling • Billing accuracy

10.4 Meter and asset management

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MDMS-FR-025	Complete device lifecycle management from registration to decommissioning	• Lifecycle workflow documentation • State transition diagrams • Business rules for each stage • Integration with procurement/disposal • Audit trail mechanisms	• Register 500 new meters • Move 100 through all lifecycle stages • Decommission 50 meters

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
			• Verify data retention • Test workflow automation
MDMS-FR-026	Maintain meter location and consumer relationship information	• Data model for location/consumer • Relationship management design • Historical tracking approach • Data validation rules • Integration with CMS/GIS	• Create 1,000 meter-consumer links • Test location updates • Verify relationship history • Test bulk updates • Validate data integrity
MDMS-FR-027	Track meter status and communication equipment from installation date	• Status tracking architecture • Communication equipment model • Real-time update mechanisms • Status change triggers • Reporting capabilities	• Track 500 meters for 30 days • Simulate status changes • Verify equipment tracking • Test alert generation • Validate reporting accuracy
MDMS-FR-028	Complete in-service history including location references with dates	• Historical data model design • Location change tracking • Date/time stamp approach • Data retention policies • Query optimization	• Review 2-year history simulation • Test location change tracking • Verify date accuracy • Query performance testing • Export history validation
MDMS-FR-029	Support for meter damage and deterioration reporting	• Damage categorization schema • Reporting interface design • Workflow integration • Photo attachment capability • Mobile app support	• Report 50 damage cases • Test severity classification • Verify workflow triggers • Test photo attachments • Validate report generation

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MDMS-FR-030	Device inventory management (in-use and in-stock)	• Inventory management design • Warehouse integration approach • Stock level monitoring • Procurement triggers • Reconciliation procedures	• Manage 10,000 device inventory • Test stock movements • Verify location tracking • Test low stock alerts • Validate reconciliation
MDMS-FR-031	Relationship tracking between communication modules and meters	• Module-meter relationship model • Association/disassociation logic • Version compatibility matrix • Historical tracking design • Bulk update capabilities	• Associate 1,000 modules • Test module swapping • Verify history retention • Test bulk operations • Validate compatibility checks
MDMS-FR-032	Historical tracking of device-transformer relationships	• Transformer relationship model • Network topology integration • Historical change tracking • Load calculation impact • Reporting capabilities	• Track 100 transformer areas • Test relationship changes • Verify historical accuracy • Test load calculations • Validate topology updates

10.5 Integration and Interoperability - Revised

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MDMS-FR-033	Common Information Model (CIM) support per IEC 61968-9	• CIM compliance documentation • Data model mapping • Message format examples • Validation tools used • Certification evidence	• Validate CIM message formats • Test data model compliance • Verify message exchange • Check standards adherence • Interoperability testing

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MDMS-FR-034	Real-time data synchronization with Billing systems	• Integration architecture design • Synchronization mechanisms • Data mapping documentation • Error handling procedures • Performance specifications	• Sync 10,000 meter readings • Test real-time updates • Verify data consistency • Measure sync latency • Test error recovery
MDMS-FR-035	Integration with Customer Management System (CMS)	• CMS integration architecture • API specifications • Data synchronization approach • Master data management • Conflict resolution design	• Sync 5,000 customer records • Test bi-directional updates • Verify data integrity • Test conflict scenarios • Validate business rules
MDMS-FR-036	Integration with ADMS technological platforms	• ADMS interface specifications • Real-time data exchange design • Event correlation approach • Network model synchronization • Performance requirements	• Exchange operational data • Test event correlation • Verify topology sync • Measure latency • Test failover scenarios
MDMS-FR-037	Market system integration for daily meter read publication	• Market interface specifications • Data format compliance • Publication scheduling design • Validation procedures • Retry mechanisms	• Publish 100,000 daily reads • Verify format compliance • Test schedule adherence • Validate data accuracy • Test error handling
MDMS-FR-038	Asset management platform interoperability	• Asset system integration design • Data synchronization approach • Work order integration • Asset lifecycle coordination • Master data alignment	• Sync 1,000 asset records • Test work order flow • Verify lifecycle updates • Test data consistency • Validate workflows
MDMS-FR-039	GIS integration for location and network topology	• GIS interface specifications	• Validate 5,000 meter locations

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Coordinate system support • Network model mapping • Visualization capabilities • Update mechanisms	• Test coordinate accuracy • Verify network topology • Test map visualization • Check update propagation
MDMS-FR-040	Integration with OMS for outage correlation	• OMS integration architecture • Event correlation logic • Real-time data exchange • Outage prediction models • Restoration tracking	• Simulate 50 outage events • Test correlation accuracy • Verify customer impact • Measure detection time • Test restoration updates

10.6 Reporting and analytics

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MDMS-FR-041	Energy consumption reports by various aggregation levels with export in user-friendly formats (PDF, XLSX, CSV), in addition to existing technical formats	• Report template samples • Aggregation level options (hourly, daily, monthly, yearly) • Grouping capabilities (by area, customer type, voltage level) • Performance specifications • Export format options	• Generate reports for 100,000 meters • Test all aggregation levels • Verify calculation accuracy • Measure generation time • Test export formats
MDMS-FR-042	Peak demand analysis and reporting	• Peak detection algorithms • Demand calculation methods • Time period configurations • Coincidence factor analysis • Visualization examples	• Analyze 30 days of demand data • Verify peak identification accuracy • Test multiple time windows • Validate against manual calculations

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
			• Test report scheduling
MDMS-FR-043	Billing summary generation with configurable formats	• Billing report templates • Format customization options • Multi-language support • Calculation rule documentation • Integration with billing systems	• Generate billing for 50,000 accounts • Test format configurations • Verify calculation accuracy • Test language options • Validate system integration
MDMS-FR-044	Regulatory compliance reporting capabilities	• Regulatory report inventory • Moldova-specific templates • Automated submission capabilities • Validation rules • Archive procedures	• Generate all regulatory reports • Verify compliance with formats • Test submission mechanisms • Validate data accuracy • Check archive retrieval
MDMS-FR-045	Reconciliation reports for non-communicating meters	• Non-communication detection logic • Reconciliation procedures • Exception handling design • Manual reading integration • Trend analysis capabilities	• Identify 1,000 non-communicating meters • Test reconciliation process • Verify manual data integration • Generate exception reports • Validate accuracy
MDMS-FR-046	Technical and non-technical loss calculation reports	• Loss calculation methodology • Network model integration • Baseline establishment procedures • Anomaly detection algorithms • Visualization capabilities	• Calculate losses for 10 feeders • Compare technical vs non-technical • Verify calculation accuracy • Test anomaly detection • Validate against field data
MDMS-FR-047	Power quality event reporting and analysis	• PQ event categorization	• Process 10,000 PQ events

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• EN 50160 compliance mapping • Statistical analysis methods • Trend identification • Report template examples	• Generate compliance reports • Verify statistical accuracy • Test trend analysis • Validate visualizations
MDMS-FR-048	Configurable ad-hoc reporting capabilities	• Report builder interface design • Available data fields catalog • Query optimization approach • User permission model • Performance limitations	• Create 20 custom reports • Test complex queries • Verify data access controls • Measure query performance • Test report sharing

10.7 Event management and alarm handling

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MDMS-FR-049	Identification and processing of power outage events	• Outage detection algorithms • Last gasp processing design • Topology awareness approach • Customer impact calculation • Integration with OMS	• Simulate 100 outage scenarios • Verify detection accuracy • Test customer impact calculation • Measure detection latency • Validate OMS integration
MDMS-FR-050	Tamper detection and alert generation	• Tamper event types catalog • Detection rule configurations • Alert priority matrix • Notification channel options • False positive handling	• Generate 500 tamper events • Test detection reliability • Verify alert generation • Measure notification speed • Test false positive filtering
MDMS-FR-051	Abnormal consumption pattern detection	• Pattern detection algorithms • Baseline calculation methods	• Analyze 10,000 meter patterns • Test anomaly detection accuracy

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Threshold configuration options • Machine learning capabilities • Investigation workflow	• Verify threshold effectiveness • Measure detection latency • Validate investigation tools
MDMS-FR-052	Configurable event escalation and notification rules	• Escalation rule engine design • Notification channel integration • Time-based escalation logic • Role-based routing • Override mechanisms	• Configure 50 escalation rules • Test time-based triggers • Verify role-based routing • Test notification delivery • Validate override functions
MDMS-FR-053	Support for voltage sags, spikes, and power quality events	• PQ event type definitions • Threshold configurations • Duration tracking capabilities • Severity classification • Impact assessment methods	• Process 1,000 PQ events • Verify event classification • Test threshold detection • Measure processing time • Validate impact calculations
MDMS-FR-054	Event correlation across multiple meters	• Correlation engine architecture • Spatial correlation algorithms • Temporal correlation methods • Root cause analysis approach • Visualization capabilities	• Test 50 multi-meter scenarios • Verify correlation accuracy • Test root cause identification • Measure correlation time • Validate visualization tools
MDMS-FR-055	Complete event logging with user tracking	• Event logging architecture • User action tracking design • Audit trail specifications • Log retention policies • Search and filter capabilities	• Generate 100,000 event logs • Verify user action tracking • Test audit trail completeness • Validate search functionality • Check log integrity

10.8 Customer interface and services

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MDMS-FR-056	Customer web portal for consumption viewing	• Portal architecture documentation • UI/UX design mockups • Responsive design approach • Browser compatibility matrix • Performance specifications	• Test with 1,000 concurrent users • Verify data display accuracy • Test on multiple browsers • Measure page load times • Validate responsive design
MDMS-FR-057	Mobile application support for customer access	• Mobile app architecture • Platform support (iOS/Android) • Feature parity with web portal • Offline capabilities • Security implementation	Documentation review only (Optional feature)
MDMS-FR-058	Real-time consumption curve visualization	• Visualization technology stack • Data refresh mechanisms • Chart types and options • Performance optimization • Data granularity options	• Display curves for 100 meters • Verify real-time updates • Test zoom/pan functionality • Measure rendering performance • Validate data accuracy
MDMS-FR-059	Historical consumption comparison features	• Comparison logic documentation • Time period selection options • Visualization methods • Statistical calculations • Export capabilities	• Compare multiple time periods • Test various comparison modes • Verify calculation accuracy • Test data export functions • Validate user experience
MDMS-FR-060	Energy calculation transparency for customers	• Calculation display methodology • Tariff breakdown presentation • Multi-language support • Help/explanation features • Regulatory compliance	• Display calculations for 500 accounts • Verify tariff application • Test language switching • Validate accuracy • Check regulatory compliance
MDMS-FR-061	Configurable alerts for consumption thresholds	• Alert configuration interface • Threshold types supported	• Configure 100 customer alerts • Test threshold triggers

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Notification channels • Alert history tracking • Customization options	• Verify notification delivery • Test alert management• Validate alert history
MDMS-FR-062	Self-service features for basic account management	• Self-service functionality list • Security considerations • Integration with CRM/billing • Workflow automation • User experience design	Documentation review only (Optional feature)

10.9 Security and access control

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MDMS-FR-063	Management of security keys and certificates	• Key management architecture • Certificate lifecycle procedures • Storage security measures • Rotation policies • Recovery procedures	• Create and manage 100 certificates • Test key rotation process • Verify secure storage • Test recovery procedures • Validate expiry handling
MDMS-FR-064	Role-based access control with granular permissions	• RBAC model documentation • Permission matrix • Role hierarchy design • Delegation capabilities • Integration with AD/LDAP	• Configure 20 different roles • Test permission inheritance • Verify access restrictions • Test delegation functions • Validate AD integration
MDMS-FR-065	Complete audit trail for all system activities	• Audit logging architecture • Events captured list • Storage and retention design • Search capabilities • Tamper protection measures	• Generate 10,000 audit entries • Verify completeness • Test search functionality • Validate tamper protection • Check retention policies
MDMS-FR-066	Multi-factor authentication support	• MFA implementation options • Supported factors (SMS, TOTP, etc.) • Enrollment procedures • Bypass mechanisms	• Test all MFA methods • Verify enrollment process • Test bypass procedures • Validate security strength

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Integration capabilities	• Check user experience
MDMS-FR-067	Data encryption at rest and in transit	• Encryption architecture • Algorithm specifications • Key management integration • Performance impact analysis • Compliance documentation	• Verify encryption implementation • Test data recovery • Measure performance impact • Validate key management • Check compliance
MDMS-FR-068	Session management and timeout controls	• Session architecture design • Timeout configuration options • Concurrent session handling • Session persistence approach • Security considerations	• Test session creation/termination • Verify timeout enforcement • Test concurrent sessions • Validate persistence • Check security controls
MDMS-FR-069	GDPR compliance for personal data handling	• Data privacy documentation • Personal data inventory • Consent management design • Data retention policies • Right-to-erasure procedures	• Test data export functions • Verify erasure procedures • Check consent tracking • Validate retention policies • Test anonymization

10.10 Scalability and performance

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MDMS-FR-070	Support for minimum 100 K meters	• Scalability architecture • Resource calculations • Database sizing model • Reference deployments • Growth projections	• Load test with 100 K meter data • Verify system stability • Monitor resource usage • Test all functionalities • Measure performance metrics
MDMS-FR-071	Process minimum10 million meter readings per day	• Processing architecture • Throughput calculations • Parallel processing design • Queue management	• Process minimum 10M readings/24 hours • Monitor processing rates • Verify data integrity • Test error handling

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Performance benchmarks	• Measure resource usage
MDMS-FR-072	Sub-second query response for individual meter data	• Query optimization strategy • Indexing approach • Caching mechanisms • Database tuning • Performance test results	• Query 10,000 random meters • Measure response times • Test under load conditions • Verify cache effectiveness • Validate consistency
MDMS-FR-073	Batch processing capabilities for large datasets	• Batch architecture design • Job scheduling capabilities • Parallel processing options • Error handling mechanisms • Performance specifications	• Process minimum 100K meter batches • Test job scheduling • Verify parallel execution • Test error recovery • Measure throughput
MDMS-FR-074	Horizontal scaling support for future growth	• Scaling architecture documentation • Node addition procedures • Load distribution design • Data partitioning strategy • Zero-downtime approach	• Add processing nodes • Verify load distribution • Test performance improvement • Validate data consistency • Check service continuity
MDMS-FR-075	Database partitioning for performance optimization	• Partitioning strategy documentation • Partition key selection • Maintenance procedures • Query optimization approach • Archive strategy	• Implement partitioning scheme • Test query performance • Verify maintenance operations • Test archive/retrieval • Validate improvements

11. METERING POINT PROFILE

11.1 Core metering point data

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MPP-001	Unique Metering Point ID with format per national standards	• National ID format specification • Validation algorithm documentation • Character set support • Check digit calculation • Error handling procedures	• Validate 10,000 ID formats • Test check digit accuracy • Verify uniqueness enforcement • Test error messages • Check duplicate prevention
MPP-002	Integration with National Registry for ID validation	• Integration architecture design • API specifications • Authentication mechanisms • Data synchronization approach • Offline validation fallback	• Test registry connectivity • Validate 1,000 IDs • Test offline scenarios • Verify sync procedures • Check error handling
MPP-003	Complete address information from CMS metadata	• Address data model • CMS integration design • Field mapping documentation • Validation rules • Multi-language support	• Import 5,000 addresses • Verify field completeness • Test special characters • Validate against CMS • Check language handling
MPP-004	Connection voltage level classification (HV/MV/LV)	• Voltage classification schema • Validation rules per level • Default assignment logic • Change tracking design • Reporting capabilities	• Classify 1,000 connections • Test validation rules • Verify categorization logic • Test bulk updates • Validate reporting
MPP-005	Contracted power information from CMS	• Power data model • CMS synchronization design • Unit conversion handling • Historical tracking • Validation thresholds	• Sync 5,000 power values • Test unit conversions • Verify historical tracking • Validate against limits • Check update propagation
MPP-006	EIC Code support where applicable	• EIC code format specification • Validation algorithm • Optional field handling • Integration requirements	• Test EIC code validation • Verify optional handling

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Display formatting	• Test format compliance • Check integration points • Validate displays

11.2 Customer classification

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MPP-007	Customer category: according to regulatory documents	• Category definitions document • Classification rules • Migration from legacy codes • Reporting structures • Change procedures	• Classify 10,000 customers • Test migration logic • Verify category rules • Test reporting accuracy • Validate changes
MPP-008	RES classification: Prosumer, Eligible Producer, Energy Community	• RES classification criteria • Regulatory compliance mapping • Status change workflows • Integration with market systems • Certification tracking	• Classify 500 RES customers • Test status transitions • Verify compliance rules • Test market integration • Validate certifications
MPP-009	Installed power capacity for producers	• Capacity data model • Validation ranges • Unit specifications • Change authorization workflow • Audit trail design	• Record 200 producer capacities • Test validation limits • Verify unit handling • Test change workflows • Check audit trails
MPP-010	Energy distribution percentage for communities	• Distribution model design • Percentage calculation rules • Validation constraints (sum=100%) • Change management process • Settlement integration	• Configure 50 communities • Test percentage validation • Verify calculations • Test updates • Check settlement impact
MPP-011	Evidence type: Commercial or Technical	• Evidence type definitions	• Assign 1,000 evidence types

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Assignment rules • Impact on processes • Reporting categorization • Change restrictions	• Test assignment rules • Verify process impacts • Test reporting • Validate restrictions

11.3 Meter information

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MPP-012	Meter model information from AMS	• Meter model catalog • AMS integration interface • Model validation rules • Capability mapping • Update synchronization	• Import 500 meter models • Verify model accuracy • Test capability mapping • Check synchronization • Validate updates
MPP-013	Meter serial number tracking	• Serial number format specs • Uniqueness enforcement • Manufacturer mapping • Duplicate handling • Search capabilities	• Track 10,000 serial numbers • Test uniqueness • Verify manufacturer links • Test duplicate detection • Validate searches
MPP-014	Metrology term validity dates	• Validity period rules • Alert generation logic • Regulatory compliance • Extension procedures • Reporting capabilities	• Set validity for 5,000 meters • Test expiry alerts • Verify compliance checks • Test extensions • Generate reports
MPP-015	Meter firmware version from HES	• Version tracking design • HES synchronization • Version comparison logic • Update history • Compatibility matrix	• Track 1,000 firmware versions • Test HES sync • Verify comparisons • Check history • Test compatibility
MPP-016	Meter configuration parameters	• Parameter catalog • Configuration templates • Validation rules • Change tracking • Bulk update capabilities	• Configure 500 meters • Test parameter validation • Apply templates • Track changes • Test bulk updates

11.4 Transformer information

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MPP-017	Current transformer (CT) model and serial number	• CT catalog structure • Serial number format • Manufacturer database • Association rules • Replacement tracking	• Record 200 CT installations • Test serial validation • Verify associations • Test replacements • Check tracking
MPP-018	CT metrology term tracking	• Metrology period rules • Certification tracking • Alert mechanisms • Compliance reporting • Extension procedures	• Track 200 CT terms • Test alert generation • Verify compliance • Test extensions • Generate reports
MPP-019	Voltage transformer (VT) model and serial number	• VT catalog structure • Serial format specs • Quality tracking • Installation records • Maintenance history	• Record 100 VT installations • Validate serials • Test associations • Track maintenance • Verify history
MPP-020	VT metrology term tracking	• VT metrology rules • Synchronization with CT • Combined reporting • Alert coordination • Regulatory compliance	• Track 100 VT terms • Test synchronization • Verify reporting • Test alerts • Check compliance
MPP-021	Transformer ratio configurations	• Ratio calculation rules • Standard ratio library • Custom ratio support • Validation constraints • Impact on calculations	• Configure 200 ratios • Test calculations • Verify standards • Test custom ratios • Validate impacts

11.5 Communication information

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MPP-022	Communication technology type (PLC/IP/Cellular)	• Technology catalog • Selection criteria • Performance characteristics • Migration paths • Reporting categorization	• Classify 1,000 devices • Test type assignment • Verify characteristics • Test migrations • Check reporting
MPP-023	Communication device model and serial number	• Device catalog design • Serial number formats • Manufacturer mapping • Compatibility matrix • Lifecycle tracking	• Record 1,000 devices • Validate serials • Test compatibility • Track lifecycle • Verify mappings
MPP-024	IP addresses for WAN interfaces	• IP address management • IPv4/IPv6 support • DHCP integration • Static assignment	• Assign 500 IP addresses • Test both protocols

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Conflict detection	• Verify DHCP integration • Test conflict detection • Validate assignments
MPP-025	Communication device firmware version	• Version tracking schema • Update coordination • Compatibility checking • Rollback tracking • Alert mechanisms	• Track 500 firmware versions • Test update tracking • Verify compatibility • Test rollback records • Check alerts
MPP-026	Communication parameters and settings	• Parameter catalog • Technology-specific settings • Validation rules • Performance optimization • Bulk configuration	• Configure 500 devices • Test parameter validation • Verify optimizations • Test bulk updates • Check performance

12. MDMS TECHNICAL SPECIFICATIONS

12.1 Architecture requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MDMS-T-001	Service-oriented architecture with clear service boundaries	• Service catalog documentation • Service interaction diagrams • API contracts between services • Service governance model • Reference architecture examples	Architecture documentation review only
MDMS-T-002	Microservices support for modular deployment	• Microservices architecture design • Service decomposition strategy • Container orchestration approach • Service mesh implementation • DevOps pipeline documentation	Design documentation review only (Optional)

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MDMS-T-003	Multi-tier architecture (presentation, business, data layers)	• Layer separation documentation • Component deployment diagrams • Inter-layer communication protocols • Security boundaries definition • Scalability per layer	• Deploy all architectural layers • Verify layer independence • Test inter-layer communication • Validate security boundaries • Check component isolation
MDMS-T-004	Stateless service design for scalability	• Stateless design documentation • Session management approach • State externalization strategy • Load balancing compatibility • Horizontal scaling design	• Test service statelessness • Verify session handling • Test load distribution • Validate scaling behavior • Check failover impact
MDMS-T-005	Event-driven architecture for real-time processing	• Event architecture design • Event catalog and schemas • Publishing/subscription model • Event store implementation • Processing guarantees	• Generate 10,000 events/hour • Verify event processing • Test pub/sub mechanisms • Measure processing latency • Validate event ordering

12.2 Database requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MDMS-T-006	Enterprise RDBMS (Oracle, PostgreSQL, SQL Server) inclusive delivery of licenses(if applicable)	• Database selection justification • Licensing model details • Performance benchmarks • HA/DR capabilities • Migration tools availability	• Install selected RDBMS • Verify enterprise features and licenses activation • Test performance benchmarks • Validate HA configuration • Check migration tools
MDMS-T-007	Time-series database integration for meter data	• Time-series DB selection	• Store 1 year meter data

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Data retention strategies • Compression algorithms • Query optimization techniques • Integration architecture	• Test compression ratios • Verify query performance • Validate data retention • Test integration points
MDMS-T-008	NoSQL support for unstructured data	• NoSQL database choice • Use case documentation • Data model design • Consistency model • Integration approach	Documentation review only (Optional)
MDMS-T-009	Database clustering for high availability	• Clustering architecture • Node configuration specs • Replication strategy • Failover mechanisms • Split-brain prevention	• Deploy database cluster • Test node failures • Verify data replication • Measure failover time • Test split-brain scenarios
MDMS-T-010	Automated backup and recovery procedures	• Backup strategy documentation • Recovery procedures • Backup scheduling design • Retention policies • Test restoration plans	• Execute backup procedures • Test full restoration • Verify backup integrity • Measure recovery time • Validate retention policies

12.3 Integration specifications

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MDMS-T-011	RESTful APIs with OpenAPI 3.0 documentation	• Complete OpenAPI specifications • API design guidelines • Versioning strategy • Security implementation • Code generation tools	• Validate OpenAPI compliance • Test all API endpoints • Verify documentation accuracy • Test version handling • Check code generation

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MDMS-T-012	SOAP web services for legacy integration	• WSDL specifications • Legacy system mapping • Security implementation • Error handling design • Performance considerations	• Deploy SOAP services • Test with legacy systems • Verify WSDL compliance • Test error scenarios • Measure performance
MDMS-T-013	Message queuing (JMS, AMQP, Kafka)	• Message queue architecture • Topic/queue design • Message schemas • Delivery guarantees • Performance specifications	• Configure message queues • Test message delivery • Verify guarantees • Measure throughput • Test failure scenarios
MDMS-T-014	Batch file processing (CSV, XML, JSON)	• File format specifications • Processing workflows • Error handling procedures • Performance optimization • Scheduling capabilities	• Process various file formats • Test large files (>1GB) • Verify error handling • Measure processing speed • Test scheduling features
MDMS-T-015	GraphQL support for flexible queries	• GraphQL schema design • Query optimization approach • Security considerations • Performance implications • Client library support	Documentation review only (Optional)

12.4 Performance specifications

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MDMS-T-016	Process minimum 500K meter readings per hour	• Performance architecture design • Resource calculations • Bottleneck analysis • Optimization strategies • Reference benchmarks	• Execute sustained load test • Process minimum 500K readings / hour • Monitor resource usage • Verify data integrity • Test for 24 hours
MDMS-T-017	VEE processing within 5 minutes of receipt	• VEE engine architecture	• Submit 100K readings

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Rule processing optimization • Parallel processing design • Queue management • Performance metrics	• Measure VEE completion time • Test various rule sets • Monitor queue depth • Verify accuracy
MDMS-T-018	Report generation < 30 seconds for standard reports	• Report engine architecture • Pre-aggregation strategy • Caching mechanisms • Standard report inventory • Performance optimization	• Generate all standard reports • Measure generation time • Test with full data volume • Verify report accuracy • Test concurrent requests
MDMS-T-019	API response time < 500ms for 95% of requests	• API performance design • Caching strategy • Database optimization • Connection pooling • Load distribution	• Execute API load test • Measure response times • Calculate percentiles • Test various endpoints • Monitor under load
MDMS-T-020	Support 200 concurrent user sessions	• Session management design • Resource allocation model • Load balancing strategy • Performance projections • Scaling approach	• Simulate 200+ users • Monitor session handling • Test user interactions • Measure response degradation • Verify resource usage

12.5 Security specifications

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MDMS-T-021	OAuth 2.0 / OpenID Connect for authentication	• OAuth implementation design • Token management strategy • Identity provider integration • Scope definitions • Security considerations	• Test OAuth flows • Verify token handling • Test IdP integration • Validate scope enforcement • Check security controls
MDMS-T-022	TLS 1.3 for all communications	• TLS implementation plan • Certificate management • Cipher suite selection	• Verify TLS 1.3 only • Test certificate validation

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Performance impact analysis • Compatibility matrix	• Check cipher suites • Test protocol downgrade • Scan for vulnerabilities
MDMS-T-023	AES-256 encryption for sensitive data	• Encryption architecture • Key management design • Data classification • Performance considerations • Compliance mapping	• Verify encryption implementation • Test key rotation • Check data classification • Measure performance impact • Validate compliance
MDMS-T-024	API rate limiting and throttling	• Rate limiting design • Throttling algorithms • Per-client/global limits • Bypass mechanisms • Monitoring approach	• Test rate limit enforcement • Verify throttling behavior • Test limit configurations • Check bypass mechanisms • Monitor effectiveness
MDMS-T-025	WAF integration for web security	• WAF solution selection • Rule set configuration • False positive handling • Performance impact • Monitoring integration	• Deploy WAF solution • Test security rules • Verify false positive rate • Measure performance impact • Test attack scenarios

13. MDMS USE CASES AND BUSINESS PROCESSES

13.1 Data management use cases

UC-011: Meter data collection and storage

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
UC-011-01	HES data push interface with multiple protocol support	• Interface specifications • Protocol documentation • Data format schemas • Error handling procedures • Performance benchmarks	• Push 100,000 readings • Test all protocols • Verify data integrity • Test error scenarios • Measure throughput

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
UC-011-02	Data format and completeness validation upon receipt	• Validation rule catalog • Format specifications • Completeness criteria • Rejection handling • Performance impact	• Submit various data formats • Test validation accuracy • Verify rejection handling • Test edge cases • Check performance
UC-011-03	Automated VEE processing integration	• VEE workflow design • Processing triggers • Queue management • Priority handling • Monitoring capabilities	• Process 10,000 readings • Verify VEE execution • Test queue behavior • Monitor processing time • Check data flow
UC-011-05	Exception notification system	• Notification framework • Exception categories • Routing rules • Delivery channels • Escalation procedures	• Generate exceptions • Test notifications • Verify routing • Check delivery • Test escalation
UC-011-06	End-to-end processing < 5 minutes	• Performance architecture • Optimization strategies • Bottleneck analysis • Scaling approach • Monitoring design	• Process 100K readings • Measure end-to-end time • Test under load • Verify 5-minute target • Monitor resources

UC-012: Data validation and estimation

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
UC-012-01	Configurable validation rules engine	• Rule engine architecture • Rule types catalog • Configuration interface • Performance specifications • Rule versioning	• Configure 50 rules • Test rule execution • Verify priorities • Test performance • Check versioning
UC-012-02	Anomaly detection and flagging system	• Detection algorithms • Flag categories • Threshold management • Pattern recognition • False positive handling	• Test anomaly detection • Verify flag accuracy • Test thresholds • Check patterns

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
			• Measure false positives
UC-012-03	Missing interval estimation algorithms	• Estimation methods • Algorithm selection logic • Accuracy specifications • Historical data usage • Seasonal adjustments	• Remove data segments • Test estimation accuracy • Compare algorithms • Verify seasonality • Check accuracy
UC-012-04	Data status tracking and marking	• Status model design • Transition rules • Audit trail approach • Query capabilities • Reporting integration	• Process mixed data • Verify status marking • Test transitions • Check audit trail • Query by status
UC-012-05	Validation report generation	• Report templates • Content specifications • Distribution options • Scheduling capabilities • Archive procedures	• Generate daily reports • Verify content accuracy • Test distribution • Check scheduling • Test archive
UC-012-06	>95% automatic validation rate achievement	• Validation strategy • Rule optimization • Performance tuning • Success metrics • Improvement process	• Process 1M readings • Measure validation rate • Verify >95% automatic • Test rule effectiveness • Monitor trends

UC-013: Billing determinant preparation

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
UC-013-01	Billing system integration interface	• Interface specifications • Request/response formats • Authentication methods • Error handling • Performance requirements	• Test interface calls • Verify data formats • Test authentication • Check error handling • Measure response time
UC-013-02	Consumption data aggregation engine	• Aggregation algorithms • Time period handling • Missing data treatment • Performance optimization • Accuracy specifications	• Aggregate 50K meters • Test time periods • Handle missing data • Verify accuracy • Check performance
UC-013-03	TOU rate application and calculations	• Rate structure support • Calculation engine	• Apply complex rates • Test calculations

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Holiday handling • Rate change management • Validation procedures	• Verify holidays • Test rate changes • Validate results
UC-013-04	Billing determinant generation and formatting	• Determinant specifications • Format requirements • Validation rules • Error handling • Performance targets	• Generate determinants • Test formats • Verify validation • Check completeness • Measure timing
UC-013-05	Billing window completion guarantee	• Processing schedule • Priority mechanisms • Resource allocation • Monitoring tools • Contingency procedures	• Process full cycle • Meet time windows • Test priorities • Monitor completion • Test contingencies

13.2 Customer service use cases

UC-014: Customer portal access

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
UC-014-01	Web portal authentication system	• Authentication architecture • Login flow design • Password policies • Session management • Security measures	• Test login process • Verify authentication • Test password rules • Check session handling • Test security
UC-014-02	Multi-factor authentication support	• MFA implementation • Factor options (SMS, app • Enrollment process • Fallback mechanisms • Security analysis	• Test MFA methods • Verify enrollment • Test fallbacks • Check security • User experience
UC-014-03	Consumption dashboard display	• Dashboard design • Widget specifications • Data refresh rates • Customization options • Performance targets	• Load dashboards • Verify data accuracy • Test refresh rates • Check customization • Measure performance
UC-014-04	Historical data viewing capabilities	• Data retention periods • Query interface design • Comparison features • Export options • Performance optimization	• Query historical data • Test time ranges • Verify comparisons • Test exports • Check performance
UC-014-05	Report download functionality	• Report types available • Format options • Generation process • Security controls • Performance limits	• Download all reports • Test formats • Verify content • Check security • Measure speed

UC-015: Consumption alert management

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
UC-015-01	Real-time consumption monitoring engine	• Monitoring architecture • Data processing pipeline • Latency specifications • Scalability design • Resource requirements	• Monitor 10K meters • Verify real-time processing • Test latency • Check scalability • Monitor resources
UC-015-02	Configurable threshold management	• Threshold types • Configuration interface • Validation rules • Change management • Multi-threshold support	• Configure thresholds • Test validations • Verify changes • Test combinations • Check accuracy
UC-015-03	Alert generation and queuing system	• Alert engine design • Queue management • Priority handling • Deduplication logic • Performance specs	• Generate 1000 alerts • Test queue behavior • Verify priorities • Check deduplication • Measure throughput
UC-015-04	Multi-channel notification delivery	• Channel options (email/SMS • Delivery mechanisms • Template management • Retry logic • Delivery tracking	• Send notifications • Test all channels • Verify delivery • Test retries • Track success
UC-015-05	Customer acknowledgment tracking	• Acknowledgment methods • Status tracking • Reminder logic • Reporting capabilities • Integration options	• Test acknowledgments • Track status • Verify reminders • Generate reports • Test integration

13.3 Analytics use cases

UC-016: Energy balance calculation

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
UC-016-01	Supply point data aggregation	• Aggregation methodology • Hierarchy handling • Time synchronization • Missing data treatment • Accuracy requirements	• Aggregate 100 supply points • Test hierarchies • Verify time sync • Handle missing data • Check accuracy
UC-016-02	Customer consumption summation	• Summation algorithms • Customer grouping • Meter multipliers	• Sum 50K customers • Test groupings • Apply multipliers

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Exception handling • Performance optimization	• Handle exceptions • Verify performance
UC-016-03	Technical loss calculation engine	• Loss calculation methods • Network model integration • Loss factors • Seasonal variations • Accuracy specifications	• Calculate for 10 feeders • Test models • Apply factors • Test seasons • Verify accuracy
UC-016-04	Non-technical loss identification	• Detection algorithms • Pattern analysis • Threshold settings • Investigation tools • Reporting features	• Analyze loss patterns • Test detection • Verify thresholds • Use tools • Generate reports
UC-016-05	Balance report generation with 0.5% tolerance	• Report specifications • Calculation validation • Tolerance handling • Distribution lists • Archive procedures	• Generate reports • Verify calculations • Test tolerance • Check distribution • Validate accuracy

UC-017: Load profile analysis

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
UC-017-01	Analysis parameter selection interface	• Parameter options • UI design mockups • Validation rules • Default settings • Help documentation	• Test parameter selection • Verify UI functionality • Test validations • Check defaults • Review help
UC-017-02	Interval data retrieval system	• Query optimization • Data access methods • Performance targets • Memory management • Error handling	• Retrieve 1 year data • Test query speed • Monitor memory • Test errors • Verify completeness
UC-017-03	Statistical analysis engine	• Analysis algorithms • Statistical methods • Accuracy specifications • Performance requirements • Visualization options	• Run analyses • Verify statistics • Check accuracy • Test performance • Review visuals
UC-017-04	Load curve generation	• Curve types supported • Rendering engine • Customization options • Export capabilities • Performance specs	• Generate curves • Test types • Verify rendering • Test customization • Check exports
UC-017-05	Results export in multiple formats	• Format options (PDF, Excel)	• Export all formats • Verify structure

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Data structure specs • Export performance • File size limits • Security controls	• Test performance • Check limits • Validate security

13.4 Integration use cases

UC-018: Market data publication

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
UC-018-01	Market data preparation engine	• Data selection logic • Aggregation rules • Quality checks • Performance design • Error handling	• Prepare daily data • Test aggregations • Verify quality • Check performance • Test errors
UC-018-02	Market format compliance	• Format specifications • Validation rules • Version handling • Change management • Compliance matrix	• Generate market files • Validate formats • Test versions • Verify compliance • Check standards
UC-018-03	Data completeness validation	• Completeness criteria • Validation algorithms • Exception handling • Reporting mechanisms • Recovery procedures	• Validate datasets • Test completeness • Handle exceptions • Generate reports • Test recovery
UC-018-04	Market platform publication interface	• Interface specifications • Security protocols • Transfer mechanisms • Retry logic • Monitoring tools	• Publish test data • Verify security • Test transfers • Check retries • Monitor success
UC-018-05	Delivery confirmation and deadline compliance	• Confirmation mechanisms • Deadline management • Alert systems • Contingency procedures • Audit trail	• Test confirmations • Meet deadlines • Verify alerts • Test contingencies • Check audit trail

UC-019: Asset management synchronization

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
UC-019-01	Asset update reception interface	• Interface design • Message formats • Authentication methods	• Receive updates • Test formats • Verify authentication

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Queue management • Error handling	• Test queuing • Handle errors
UC-019-02	Asset data validation engine	• Validation rules • Data quality checks • Reference data usage • Exception handling • Reporting features	• Validate asset data • Test quality checks • Verify references • Handle exceptions • Generate reports
UC-019-03	Meter relationship updates	• Relationship model • Update procedures • Consistency checks • History tracking • Rollback capability	• Update relationships • Test consistency • Verify history • Test rollback • Check integrity
UC-019-04	Configuration synchronization	• Sync mechanisms • Conflict resolution • Version control • Audit logging • Performance targets	• Sync configurations • Test conflicts • Verify versions • Check logs • Measure performance
UC-019-05	Real-time and batch mode support	• Mode selection logic • Performance differences • Queue management • Priority handling • Monitoring capabilities	• Test both modes • Compare performance • Verify queuing • Test priorities • Monitor execution

13.5 Special scenarios

UC-020: Energy community settlement

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
UC-020-01	Member consumption/production collection	• Collection mechanisms • Data aggregation logic • Time synchronization • Missing data handling • Performance for 100+ members	• Collect from 100 members • Test aggregation • Verify time sync • Handle missing data • Check performance
UC-020-02	Distribution percentage application	• Percentage calculation engine • Validation rules (sum=100%) • Change management • Historical tracking • Rounding handling	• Apply percentages • Verify sum validation • Test changes • Check history • Test rounding
UC-020-03	Internal settlement calculations	• Settlement algorithms • Netting procedures • Currency handling	• Calculate settlements • Test netting

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Precision requirements • Audit trail	• Verify precision • Check currency • Review audit trail
UC-020-04	Community report generation	• Report templates • Member statements • Aggregate reports • Distribution options • Multi-language support	• Generate all reports • Test statements • Verify aggregates • Test distribution • Check languages
UC-020-05	Financial settlement processing	• Settlement workflows • Payment integration • Reconciliation procedures • Exception handling • Compliance features	• Process settlements • Test payments • Verify reconciliation • Handle exceptions • Check compliance

UC-021: Virtual power plant operations

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
UC-021-01	Distributed generation monitoring	• Monitoring architecture • Data collection methods • Real-time requirements • Scalability design • Visualization tools	• Monitor 50 generators • Test collection • Verify real-time • Check scalability • Test visualization
UC-021-02	Available capacity aggregation	• Aggregation algorithms • Forecast integration • Constraint handling • Update frequency • Accuracy requirements	• Aggregate capacity • Test forecasts • Apply constraints • Verify updates • Check accuracy
UC-021-03	Optimization scenario calculations	• Optimization engines • Scenario parameters • Calculation speed • Result validation • Comparison tools	• Run optimizations • Test scenarios • Measure speed • Validate results • Compare options
UC-021-04	Dispatch command execution	• Command interface • Security protocols • Acknowledgment handling • Failover procedures • Audit logging	• Execute commands • Verify security • Test acknowledgments • Check failover • Review logs
UC-021-05	Performance tracking with <1 minute latency	• Tracking mechanisms • KPI definitions • Real-time processing • Dashboard updates • Alert generation	• Track performance • Measure latency • Verify KPIs • Test dashboards • Check alerts

TERMS OF REFERENCE - PART III

NON-FUNCTIONAL REQUIREMENTS FOR HES AND MDMS

14. SCALABILITY REQUIREMENTS

14.1 HES scalability requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Critical notes
NFR-HES-S01	100K meters scaling to 1.5M	• Architecture documentation • Scaling methodology • Reference deployments >500k	• Progressive load testing • Resource monitoring • Performance benchmarks	Phased validation
NFR-HES-S02	10,000 concurrent connections	• Connection pooling design • Thread management • Load balancer specs	• Connection storm testing • Stability under load • Resource utilization	Critical for operations
NFR-HES-S03	5,000 commands/second	• Performance benchmarks • Queue architecture • Processing design	• Sustained load testing • Peak load handling • Latency distribution	Peak hour requirement
NFR-HES-S04	Horizontal scaling	• Scaling architecture • Node addition process • Load distribution	• Add node testing • Performance linearity • No service disruption	Future growth
NFR-HES-S05	Multi-protocol streams	• Protocol handlers • Resource isolation • Performance data	• Mixed protocol testing • Resource contention • Throughput verification	Moldova mix
NFR-HES-S06	Dynamic resource allocation	• Auto-scaling design • Burst handling • Resource policies	• Burst scenario testing • Response time • Recovery behavior	Network variations

14.2 MDMS scalability requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
NFR-MDMS-S01	100K meters, 15-min intervals	• Data architecture • Storage calculations • Processing pipeline	• 30-day volume test • Performance monitoring • Storage growth tracking
NFR-MDMS-S02	Scale to 1.5M without architecture change	• Scalability design • Architecture flexibility • Growth accommodation	Architecture review only
NFR-MDMS-S03	100M readings/day	• Throughput design • Database optimization • Benchmark data	• Sustained load testing • Performance metrics • Resource monitoring
NFR-MDMS-S04	5 HES integrations	• Integration framework • Isolation mechanisms • Performance impact	• Multi-HES testing • Data consistency • Conflict resolution
NFR-MDMS-S05	Diverse data sources	• Adapter architecture • Data normalization • Format support	• Source variety testing • Processing accuracy • Performance impact
NFR-MDMS-S06	Elastic scaling (optional)	• Cloud architecture • Auto-scaling design	Documentation review

15. PERFORMANCE AND LATENCY REQUIREMENTS

15.1 HES performance requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Test specifics
NFR-HES-P01	On-demand read <30s (95%)	• Network optimization • Communication design	• 1000 random reads • Percentile analysis • Various conditions	Production only
NFR-HES-P02	Command latency <5s	• Command pipeline • Priority handling	• End-to-end timing • Load conditions • Protocol variations	Critical metric
NFR-HES-P03	Event processing <100ms	• Event architecture • Processing pipeline	• Event injection testing • Latency measurement • Load impact	Safety critical
NFR-HES-P04	Firmware 1000/hour	• Update mechanism • Batch processing • Network optimization	• Batch update testing • Success rate • Network impact	Maintenance window

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Test specifics
NFR-HES-P05	Configurable retry	• Retry logic design • Configuration options	• Retry scenarios • Success rates • Resource impact	Network conditions
NFR-HES-P06	Priority queue <1s	• Queue architecture • Priority algorithm	• Priority testing • Queue behavior • Fairness verification	Emergency commands

15.2 MDMS performance requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
NFR-MDMS-P01	VEE <5 minutes	• VEE engine design • Parallel processing	• Various data volumes • Rule complexity impact • Resource usage
NFR-MDMS-P02	Query <1s (90%)	• Database optimization • Indexing strategy	• Query variety testing • Load conditions • Data volume impact
NFR-MDMS-P03	Billing <30min/100k	• Billing engine design • Batch processing	• Full billing cycle • Various scenarios • Accuracy verification
NFR-MDMS-P04	Dashboard <5s refresh	• Dashboard architecture • Caching strategy	• User simulation • Concurrent users • Data freshness
NFR-MDMS-P05	Reports <30s	• Report engine • Pre-aggregation	• All report types • Data volumes • Concurrent requests
NFR-MDMS-P06	API <500ms (95%)	• API optimization • Caching design	• API load testing • Various endpoints • Payload sizes

16. AVAILABILITY AND RELIABILITY REQUIREMENTS

16.1 System availability requirements (for both HES and MDMS)

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Criticality
NFR-AR-01	99.9% availability	• HA architecture • Component redundancy • Reference Service-level requirements	• 90-day monitoring • Downtime tracking • Incident analysis	Annual target
NFR-AR-02	99.99% critical functions	• Critical path analysis • Redundancy design	• Critical function monitoring • Failover testing	Billing, commands

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Criticality
			• Recovery timing	
NFR-AR-03	Active-active/passive clustering	• Cluster architecture • Data synchronization • Split-brain prevention	• Cluster testing • Failover scenarios • Data consistency	1+1 configuration
NFR-AR-04	Failover <60 seconds	• Failover design • Detection mechanisms • Automation	• Timed failover tests • Various failure types • Service continuity	Critical requirement
NFR-AR-05	Geographic redundancy 50km	• Site locations • Network architecture • Replication design	Site verification only	Disaster protection
NFR-AR-06	Load balancing	• LB architecture • Distribution algorithms • Health checks	• Load distribution testing • Failure scenarios • Performance impact	Even utilization

16.2 Disaster recovery requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
NFR-DR-01	Recovery Time Objective (RTO) < 1 hour for complete system	• DR architecture documentation • RTO calculation methodology • Historical DR performance data • Automated recovery procedures	• Execute full DR scenario • Measure actual recovery time • Verify all system components operational • Document recovery steps and timing
NFR-DR-02	Recovery Point Objective (RPO) < 15 minutes for transactional data	• Data replication architecture • RPO achievement methodology • Replication technology specifications • Data loss prevention measures	• Simulate unexpected failure • Measure data loss window • Verify transaction completeness • Validate data integrity post-recovery
NFR-DR-03	Automated backup every 4 hours with verification	• Backup automation design • Verification process documentation • Backup storage architecture	• Monitor 48-hour backup cycle • Verify backup completion logs • Test restoration from random backups

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Retention policy specifications	• Validate backup integrity checks
NFR-DR-04	Quarterly DR drills with documented results	• DR drill procedures template • Drill scheduling framework • Documentation standards • Success criteria definitions	• Review DR drill calendar • Examine drill execution procedures • Verify documentation templates • Assess drill result tracking system
NFR-DR-05	Hot standby site with real-time data replication	• Standby site architecture • Replication technology details • Network connectivity design • Synchronization monitoring approach	• Verify standby site readiness • Test real-time replication lag • Perform controlled failover • Measure data synchronization delay

17. INTEROPERABILITY AND INTEGRATION REQUIREMENTS

17.1 Standards compliance

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
NFR-INT-01	CIM IEC 61968-9	• CIM compliance docs • Data model mapping • Certification	• Data exchange testing • Standard validation • Interoperability verification
NFR-INT-02	IEC 62351 security	• Security implementation • Standard compliance • Certificates	• Security protocol testing • Vulnerability assessment • Compliance verification
NFR-INT-03	DLMS/COSEM	• Protocol implementation • Compliance matrix • Test results	• Protocol analyzer testing • Meter compatibility • Feature support
NFR-INT-04	OpenAPI 3.0	• API documentation • Specification files • Validation results	• Specification compliance • Documentation accuracy • Tool compatibility
NFR-INT-05	IEC 61850 (Optional)	• Implementation docs • Integration examples	Documentation only

17.2 API and integration capabilities

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
NFR-API-01	RESTful APIs supporting JSON and XML data formats	• API architecture documentation • REST design principles compliance • JSON/XML schema definitions • API versioning strategy	• Execute CRUD operations via REST • Validate JSON request/response • Validate XML request/response • Verify HTTP status codes compliance
NFR-API-02	GraphQL support for flexible data queries	• GraphQL implementation approach • Schema definition documentation • Query optimization strategy • Performance benchmarks	• Test complex nested queries • Verify query response flexibility • Validate schema introspection • Measure query execution performance
NFR-API-03	SOAP web services for legacy system integration	• WSDL definitions • SOAP protocol compliance • Legacy system compatibility matrix • Security implementation (WS-Security)	• Test SOAP endpoint availability • Validate WSDL contracts • Execute legacy system transactions • Verify SOAP fault handling
NFR-API-04	Message broker integration (Kafka, RabbitMQ, AMQP)	• Message broker architecture • Topic/queue design documentation • Message format specifications • Guaranteed delivery mechanisms	• Publish test messages to brokers • Verify message consumption • Test message persistence • Validate failover scenarios
NFR-API-05	Webhook support for event-driven notifications	• Webhook architecture design • Event catalog documentation • Retry mechanism specifications • Security implementation approach	• Register webhook endpoints • Trigger notification events • Verify delivery confirmation • Test retry logic and timeouts
NFR-API-06	Batch file interfaces (CSV, XML, JSON) with scheduling	• File interface specifications • Scheduling framework documentation • File validation rules • Error handling procedures	• Process sample batch files • Verify scheduling functionality • Test file format validation • Validate error reporting mechanisms

18. CYBERSECURITY REQUIREMENTS

18.1 Data protection requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Security level
NFR-SEC-01	AES-256 at rest	• Encryption architecture • Key management • Implementation details	• Encryption verification • Performance impact • Key rotation testing	Mandatory baseline
NFR-SEC-02	TLS 1.3 in transit	• Protocol configuration • Certificate management • Cipher suites	• Protocol verification • Vulnerability scanning • Performance testing	Current standard
NFR-SEC-03	FIPS 140-2	• Module certification • Compliance documents • Vendor attestation	Certificate verification	Compliance requirement
NFR-SEC-04	HSM support (optional)	• HSM integration design • Key management architecture	• HSM integration testing • Performance impact • Failover behavior	Enhanced security
NFR-SEC-05	Data masking	• Masking rules • Environment separation • Data flow controls	• Masking effectiveness • Data leak testing • Performance impact	Privacy protection
NFR-SEC-06	Command signing	• Signing architecture • Certificate management • Verification process	• Signature verification • Tamper detection • Performance impact	Critical commands

18.2 Access control and authentication

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
NFR-AC-01	Role-based access control (RBAC) with minimum 20 configurable roles	• RBAC design documentation	• Create 20 distinct roles

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Role hierarchy structure • Permission matrix template • Role configuration procedures	• Assign varied permissions per role • Test role inheritance • Verify permission enforcement
NFR-AC-02	Multi-factor authentication (MFA) for all privileged accounts	• MFA implementation approach • Supported authentication factors • Privileged account definitions • MFA bypass procedures	• Enable MFA for admin accounts • Test multiple authentication methods • Verify MFA enforcement • Validate emergency access procedures
NFR-AC-03	Integration with enterprise IAM (Active Directory, LDAP, SAML)	• IAM integration architecture • Protocol support documentation • Attribute mapping specifications • SSO implementation approach	• Configure AD/LDAP connection • Test user authentication flow • Verify SAML assertions • Validate group synchronization
NFR-AC-04	OAuth 2.0 / OpenID Connect for API authentication	• OAuth implementation design • Token management strategy • Scope definitions • OIDC compliance documentation	• Generate OAuth tokens • Test token validation • Verify scope enforcement • Validate OIDC claims
NFR-AC-05	Session timeout after 15 minutes of inactivity	• Session management design • Timeout configuration approach • Session persistence strategy • Warning notification mechanism	• Monitor inactive sessions • Verify 15-minute timeout trigger • Test session termination • Validate re-authentication flow
NFR-AC-06	Account lockout after 5 failed login attempts	• Lockout mechanism design • Counter reset procedures • Unlock workflow documentation • Notification system approach	• Attempt 5 failed logins • Verify account lockout • Test unlock procedures • Validate alert notifications

18.3 Threat management

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
NFR-TM-01	Integration with SIEM solutions (Splunk, QRadar, ArcSight – tbc specific tool used by Beneficiary)	• SIEM integration architecture • Log format specifications • Event correlation rules • Data retention approach	• Configure SIEM connector • Send test security events • Verify event reception in SIEM • Validate correlation rules
NFR-TM-02	Real-time intrusion detection for OT protocols (DNP3, IEC 61850)	• IDS architecture for OT • Protocol parsing capabilities • Anomaly detection algorithms • Alert threshold configurations	• Generate OT protocol traffic • Simulate protocol anomalies • Verify real-time detection • Measure detection latency
NFR-TM-03	DDoS protection for public-facing interfaces	• DDoS mitigation architecture • Traffic filtering rules • Rate limiting configurations • Failover mechanisms	• Execute controlled DDoS simulation • Verify traffic filtering • Test rate limiting effectiveness • Validate service availability
NFR-TM-04	Vulnerability scanning quarterly with remediation within 30 days	• Scanning tool specifications • Scan coverage documentation • Remediation workflow process • Tracking system approach	• Review scanning schedule • Examine scan configuration • Verify remediation tracking • Validate 30-day Service-level requirements delivery mechanism
NFR-TM-05	Annual penetration testing by certified professionals	• Penetration testing scope • Certification requirements • Testing methodology framework • Remediation process workflow	• Verify tester certifications • Review testing methodology • Examine scope documentation • Validate reporting framework
NFR-TM-06	Security incident response plan with 4-hour response time	• Incident response plan template • Escalation matrix	• Simulate security incident • Measure response initiation time

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Response team structure • Communication protocols	• Verify escalation procedures • Test communication channels

19. DATA GOVERNANCE AND QUALITY

19.1 Data integrity

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
NFR-DQ-01	Automated validation	• Validation framework • Rule engine design • Error handling	• Validation accuracy • Performance impact • Error detection rate
NFR-DQ-02	Checksum verification	• Checksum algorithms • Implementation points • Performance data	• Integrity testing • Error detection • Performance overhead
NFR-DQ-03	Daily reconciliation	• Reconciliation process • Discrepancy handling • Automation design	• Reconciliation accuracy • Processing time • Issue resolution
NFR-DQ-04	Anomaly detection	• Detection algorithms • Threshold management • Alert mechanisms	• Detection accuracy • False positive rate • Response time
NFR-DQ-05	Data lineage	• Lineage architecture • Tracking mechanisms • Visualization tools	• Lineage completeness • Query performance • Accuracy verification

19.2 Audit trail requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
NFR-AUD-01	Comprehensive logging of all user and system actions	• Audit logging architecture • Event catalog documentation • Log format specifications • Coverage matrix for actions	• Execute various user actions • Verify complete action logging • Review system event capture • Validate log completeness
NFR-AUD-02	Immutable audit logs with tamper detection	• Log immutability design	• Attempt log modification

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Cryptographic signing approach • Tamper detection algorithms • Chain of custody procedures	• Verify modification detection • Test cryptographic validation • Validate integrity mechanisms
NFR-AUD-03	Log retention for minimum 5 years online, 10 years archived	• Retention policy documentation • Storage architecture design • Archival process workflow • Retrieval procedures	• Verify online storage capacity • Test archive migration process • Validate retrieval from archives • Check retention policy enforcement
NFR-AUD-04	Audit log search and reporting capabilities	• Search engine specifications • Query language documentation • Report template catalog • Performance benchmarks	• Execute complex log searches • Test search performance • Generate standard reports • Verify export capabilities
NFR-AUD-05	Real-time alerting for suspicious activities	• Alert rule engine design • Suspicious pattern definitions • Notification channel setup • Escalation procedures	• Trigger suspicious patterns • Measure alert latency • Verify notification delivery • Test escalation workflows

20. COMPLIANCE AND REGULATORY

20.1 Data protection compliance

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Legal priority
NFR-GDPR-01	Data minimization	• Data collection design • Privacy by design docs • Data flow diagrams	• Data audit • Collection verification • Compliance check	High - Legal requirement
NFR-GDPR-02	Right to access	• Export functionality • Process documentation • Timeline compliance	• Export testing • Format verification • Timeline measurement	30-day requirement
NFR-GDPR-03	Right to erasure	• Deletion procedures • Data retention policies • Cascade deletion	• Deletion testing • Completeness verification • Audit trail	Upon request
NFR-GDPR-04	Breach notification	• Incident procedures • Notification templates • Contact mechanisms	• Breach drill • Timeline verification • Communication test	72-hour requirement
NFR-GDPR-05	Privacy by design	• Privacy architecture • Impact assessments • Design documentation	• Privacy audit • Control effectiveness • Documentation review	Fundamental principle
NFR-GDPR-06	DPA templates	• Template documents • Legal review • Compliance mapping	Legal review only	Contract requirement

20.2 Energy sector compliance

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
NFR-ES-01	Compliance with Moldova's critical infrastructure protection laws	• Legal compliance matrix • Critical infrastructure controls • Protection measures documentation • Compliance gap analysis	• Review compliance documentation • Verify protection controls • Audit security measures • Validate legal requirements coverage
NFR-ES-02	EU NIS Directive compliance for network security	• NIS compliance checklist • Network security architecture • Incident response procedures • Risk assessment methodology	• Verify NIS control implementation • Test incident reporting capability • Review security measures • Validate compliance artifacts

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
NFR-ES-03	Data localization within Moldova or EU	• Data residency architecture • Geographic location certificates • Data flow documentation • Backup location specifications	• Verify primary data location • Confirm backup site locations • Test geo-restriction controls • Validate data sovereignty
NFR-ES-04	Support for regulatory reporting requirements	• Regulatory report templates • Reporting automation design • Data collection mechanisms • Submission interface specifications	• Generate sample reports • Test report accuracy • Verify submission channels • Validate report scheduling
NFR-ES-05	Compliance with national metering standards	• Metering standards mapping • Accuracy specifications • Calibration procedures • Certification documentation	• Verify metering accuracy • Test data collection standards • Review calibration records • Validate standard compliance

21. OPERATIONAL REQUIREMENTS

21.1 Maintenance and upgrade requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
NFR-MNT-01	Zero-downtime deployment	• Deployment architecture • Blue-green design • Rollback procedures	• Deployment testing • Service continuity • Performance impact
NFR-MNT-02	Rolling updates	• Update strategy • Component isolation • Orchestration tools	• Update execution • No service disruption • Version consistency
NFR-MNT-03	5-minute rollback	• Rollback procedures • Automation scripts • State management	• Rollback timing • Data consistency • Service restoration
NFR-MNT-04	Version control	• VC system choice • Branching strategy • CI/CD integration	• Repository structure • Change tracking • Deployment pipeline
NFR-MNT-05	24-hour patching	• Patch procedures • Emergency process • Testing requirements	• Patch deployment • Verification process • No regression

21.2 Monitoring and diagnostics

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
NFR-MON-01	Real-time monitoring dashboards for system health	• Dashboard architecture design • Health metrics catalog • Visualization specifications • Refresh rate capabilities	• Access monitoring dashboards • Verify real-time data updates • Test health status indicators • Validate metric accuracy
NFR-MON-02	Automated alerting for performance degradation	• Alert rule configuration • Threshold setting methodology • Notification channel design • Escalation matrix	• Simulate performance degradation • Verify alert triggering • Test notification delivery • Validate escalation paths
NFR-MON-03	Predictive analytics for capacity planning	• Analytics algorithm documentation • Prediction model specifications • Historical data requirements • Forecasting accuracy metrics	• Review prediction models • Test capacity forecasts • Validate trend analysis • Verify planning recommendations
NFR-MON-04	Root cause analysis tools for incident investigation	• RCA tool capabilities • Investigation workflow design • Log correlation features • Forensic analysis procedures	• Simulate system incidents • Execute root cause analysis • Test correlation capabilities • Verify investigation workflow
NFR-MON-05	Performance metrics collection and trending	• Metrics collection architecture • KPI definitions catalog • Data retention policies	• Verify metric collection • Test data aggregation • Review trending reports

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Trending visualization tools	• Validate historical analysis

22. USABILITY AND TRAINING REQUIREMENTS

22.1 User interface requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method	Priority
NFR-UI-01	Role-based dashboards	• Dashboard designs • Role definitions • Customization options	• Usability testing • Role verification • Performance testing	User efficiency
NFR-UI-02	RO/EN mandatory, RU optional	• Localization architecture • Translation process• Language switching	• Language coverage • Translation quality • Switching functionality	Moldova requirement
NFR-UI-03	WCAG 2.1 AA	• Accessibility design • Compliance checklist • Testing tools	• Accessibility audit • Screen reader testing • Keyboard navigation	Legal compliance
NFR-UI-04	Responsive design	• Responsive framework • Device support matrix • Design mockups	• Multi-device testing • Functionality verification • Performance testing	Modern requirement
NFR-UI-05	Context help	• Help system design • Content strategy • Tooltip framework	• Help effectiveness • Coverage verification • User feedback	User support

22.2 Training requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
NFR-TRN-01	Role-specific training modules for all user types	• Training curriculum outline • Module-to-role mapping • Learning objectives per module	• Review training modules • Verify role coverage • Test module effectiveness

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Assessment methodology	• Validate assessment criteria
NFR-TRN-02	Hands-on training environment/sandbox	• Sandbox architecture design • Environment specifications • Data anonymization approach • Reset/refresh procedures	• Access training environment • Execute practice scenarios • Test environment isolation • Verify data refresh capability
NFR-TRN-03	Comprehensive documentation in local language - Romanian	• Documentation inventory • Translation methodology • Quality assurance process • Update procedures	• Review Romanian documentation • Verify translation accuracy • Test documentation completeness • Validate technical terminology
NFR-TRN-04	Train-the-trainer program with certification (if apply/available – bidder must specify this in the offer)	• Trainer curriculum design • Certification requirements • Assessment criteria • Program availability confirmation	• Review trainer program content • Verify certification process • Test knowledge transfer method • Validate trainer competencies
NFR-TRN-05	Online learning management system (LMS) access (if apply/available – bidder must specify this in the offer)	• LMS platform specifications • Content delivery methods • Progress tracking features • Availability confirmation	• Access LMS platform • Test content delivery • Verify progress tracking • Validate user experience

23. ENVIRONMENTAL AND EFFICIENCY REQUIREMENTS

23.1 Resource efficiency

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
NFR-EFF-01	CPU <70% normal load	• Resource planning • Optimization strategies	• Resource monitoring • 30-day average • Peak analysis

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
NFR-EFF-02	Memory <80%	• Memory management • Garbage collection	• Memory profiling • Leak detection • Long-term stability
NFR-EFF-03	Query <100ms avg	• Query optimization • Index strategy • Database design	• Query profiling • Performance testing • Optimization verification
NFR-EFF-04	Bandwidth optimization	• Compression strategy • Protocol efficiency • Batch mechanisms	• Bandwidth monitoring • Compression ratios • Network impact
NFR-EFF-05	PUE <1.5 (Optional)	• Data center specs • Efficiency measures	Documentation only

TERMS OF REFERENCE - PART IV

SERVICES REQUIREMENTS FOR HES AND MDMS

24. CUSTOMIZATION AND CONFIGURATION SERVICES

24.1 HES customization services

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
SVC-HES-C01	Communication protocol customization for Moldova-specific meter models	• Protocol adaptation methodology • Meter model compatibility matrix • Configuration approach documentation • Previous customization examples	• Test protocol communication • Verify meter model connectivity • Validate data exchange • Review adapter documentation
SVC-HES-C02	Custom command sequences for local utility requirements	• Command sequence design approach • Automation framework specifications • Template creation methodology	• Execute custom commands • Test automation scripts • Verify command responses

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Utility requirement analysis	• Validate template functionality
SVC-HES-C03	Meter firmware management customization	• Firmware repository architecture • Update procedure design • Version control approach • Rollback mechanisms	• Test firmware upload process • Verify update procedures • Validate version tracking • Review repository structure
SVC-HES-C04	Alert and event configuration based on local regulations	• Alert rule framework • Regulatory mapping documentation • Notification template designs • Event categorization approach	• Trigger configured alerts • Test notification delivery • Verify regulatory compliance • Validate event processing
SVC-HES-C05	Performance tuning for Moldova's communication infrastructure	• Performance analysis methodology • Infrastructure assessment approach • Optimization techniques • Benchmarking procedures	• Measure baseline performance • Apply tuning parameters • Test optimized performance • Review performance reports
SVC-HES-C06	Custom dashboards for operations center	• Dashboard design approach • Widget development framework • Layout customization capabilities • User requirement analysis	• Review dashboard layouts • Test widget functionality • Verify data visualization • Validate user workflows

24.2 MDMS customization services

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
SVC-MDMS-C01	VEE rules customization for Moldova market requirements	• VEE rule design methodology • Market requirement analysis • Validation logic documentation • Rule testing procedures	• Execute VEE validations • Test rule effectiveness • Verify market compliance • Review validation results

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
SVC-MDMS-C02	Billing determinant calculations for local tariff structures	• Calculation engine architecture • Tariff structure analysis • Configuration methodology • Testing approach	• Process billing calculations • Verify tariff application • Test calculation accuracy • Validate configuration flexibility
SVC-MDMS-C03	Report templates for regulatory compliance	• Report design framework • Regulatory requirement mapping • Template creation process • Scheduling capabilities	• Generate compliance reports • Verify report accuracy • Test scheduling functionality • Validate regulatory coverage
SVC-MDMS-C04	Energy community settlement algorithms	• Settlement algorithm design • Distribution rule framework • Community model support • Calculation methodology	• Execute settlement calculations • Test distribution rules • Verify algorithm accuracy • Review settlement outputs
SVC-MDMS-C05	Custom analytics for grid loss calculation	• Analytics model architecture • Loss calculation methodology • Reporting framework design • Accuracy validation approach	• Run loss calculations • Verify analytics accuracy • Test report generation • Validate model outputs
SVC-MDMS-C06	Time-of-use processing for Moldova's rate schedules	• TOU engine design • Rate schedule mapping • Configuration framework • Processing logic documentation	• Process TOU calculations • Test rate applications • Verify schedule handling • Validate configuration changes

25. INTEGRATION SERVICES

25.1 Enterprise system integration requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
INT-01	GIS (Smallworld Electric Office) - Meter location synchronization, Asset data exchange, Network topology updates, Real-time status sharing	• Smallworld integration experience • API compatibility documentation • Data mapping specifications • Real-time sync architecture	• Test meter location sync • Verify asset data exchange • Validate topology updates • Test real-time status flow
INT-02	ERP (SAP) - Asset lifecycle management, Work order integration, Inventory synchronization, Financial data exchange	• SAP integration methodology • Asset lifecycle mappings • Work order interface design • Financial posting specifications	• Execute asset lifecycle flows • Test work order creation • Verify inventory updates • Validate financial transactions
INT-03	ADMS (Onesite Grid Platform) - Outage event correlation, Load data sharing, Network status updates, Incident management integration	• Onesite platform experience • Event correlation logic • Load data interface specs • Incident workflow design	• Test outage correlation • Verify load data transfer • Validate status updates • Test incident integration
INT-04	CMS (TBD - 2026 implementation) - Customer data synchronization, Service point management, Account status updates, Contact information exchange	• Generic CMS integration framework • Data model flexibility • Synchronization approach • Adapter architecture	• Review integration framework • Test data model mapping • Verify sync mechanisms • Validate adapter design
INT-05	Billing (Multiple supplier platforms) - Consumption data delivery, Billing determinants, Rate application, Exception handling	• Multi-platform integration approach • Data delivery mechanisms • Billing determinant specs • Exception handling procedures	• Test data delivery to platforms • Verify billing determinants • Validate rate applications • Test exception processing

25.2 HES-specific integration services

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
INT-HES-01	GIS integration for meter location validation via REST API, batch files	• REST API design documentation • Batch file specifications • Location validation logic • Mapping rule definitions	• Test REST API connectivity • Execute batch file processing • Verify location validation • Review mapping accuracy
INT-HES-02	ADMS integration for outage correlation via real-time messaging	• Messaging architecture design • Event correlation algorithms • Message format specifications • Performance benchmarks	• Send test outage events • Verify real-time delivery • Test correlation accuracy • Measure message latency
INT-HES-03	Asset management synchronization with SAP via web services, batch	• Web service specifications • Batch processing design • Synchronization procedures • Error handling approach	• Test web service calls • Execute batch synchronization • Verify data consistency • Validate error recovery
INT-HES-04	Network topology updates from GIS via scheduled batch, API	• Update procedure design • Validation rule framework • Scheduling mechanisms • API specifications	• Execute topology updates • Test validation rules • Verify update scheduling • Validate data integrity
INT-HES-05	Meter event forwarding to ADMS via event streaming	• Event streaming architecture • Event type configurations • Routing rule definitions • Performance specifications	• Generate meter events • Test event streaming • Verify routing logic • Measure throughput rates

25.3 MDMS-specific integration services

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
INT-MDMS-01	Billing system integration for all suppliers via REST API, file transfer	• Multi-supplier API design • File transfer specifications	• Test API connections • Execute file transfers

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Data format documentation • Error handling procedures	• Verify data formats • Validate error handling
INT-MDMS-02	CMS integration for customer data via real-time sync, batch	• Real-time sync architecture • Batch processing design • Data mapping specifications • Synchronization procedures	• Test real-time sync • Execute batch updates • Verify data mappings • Validate sync accuracy
INT-MDMS-03	SAP integration for financial posting via web services	• Financial posting logic • Web service specifications • Posting rule definitions • Reconciliation procedures	• Execute financial postings • Test web service calls • Verify posting accuracy • Validate reconciliation
INT-MDMS-04	GIS integration for service point validation via REST API	• Service point validation logic • REST API specifications • Error handling procedures • Validation rule framework	• Test service point validation • Execute API calls • Verify error handling • Review validation results
INT-MDMS-05	Market operator data exchange via standardized file formats	• File format specifications • Exchange schedule design • Validation procedures • Error recovery mechanisms	• Generate exchange files • Test format compliance • Verify exchange scheduling • Validate error handling

26. TESTING SERVICES

26.1 System testing requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
TST-01	Functional Testing - All system functions per requirements with 100% requirement coverage	• Test case design methodology • Requirements traceability matrix • Test coverage approach • Functional test procedures	• Execute functional test cases • Verify requirement coverage • Review test results • Validate functionality completeness
TST-02	Integration Testing - All system interfaces and data flows with successful data exchange validation	• Integration test strategy • Interface test specifications • Data flow validation approach • End-to-end test scenarios	• Test all system interfaces • Validate data exchange • Verify data integrity • Confirm interface functionality
TST-03	Performance Testing - Load, stress, and scalability testing to meet all NFR performance metrics	• Performance test methodology • Load testing scenarios • Scalability test approach • Performance benchmarks	• Execute load tests • Run stress test scenarios • Verify scalability limits • Validate NFR compliance
TST-04	Security Testing - Vulnerability assessment, penetration testing with no critical vulnerabilities	• Security test methodology • Vulnerability scan approach • Penetration test scope • Remediation procedures	• Run vulnerability scans • Execute penetration tests • Review security findings • Verify remediation completion
TST-05	Disaster Recovery Testing - Failover, backup, and recovery procedures to achieve RTO/RPO targets	• DR test scenarios • Failover procedures • Recovery test methodology • RTO/RPO measurement approach	• Execute failover tests • Test backup procedures • Verify recovery processes • Measure RTO/RPO achievement
TST-06	Regression Testing - System stability after changes with no functionality degradation	• Regression test strategy • Test suite maintenance approach • Automation framework	• Run regression test suite • Verify system stability • Test functionality preservation

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Change impact analysis	• Validate change impacts

26.2 HES-specific testing services

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
TST-HES-01	Meter communication testing - Individual meter reading, Group reading commands, Communication retry mechanisms, Multiple protocol testing	• Communication test procedures • Protocol test specifications • Retry logic documentation • Success criteria definitions	• Test individual meter reads • Execute group commands • Verify retry mechanisms • Validate protocol support
TST-HES-02	Command execution testing - On-demand reads, Remote disconnect/reconnect, Firmware updates, Configuration changes	• Command test scenarios • Execution validation approach • Firmware update procedures • Configuration test methods	• Execute on-demand reads • Test disconnect/reconnect • Verify firmware updates • Validate configuration changes
TST-HES-03	Load balancing testing - Communication load distribution, Failover scenarios, Peak load handling	• Load distribution strategy • Failover test procedures • Peak load test scenarios • Performance metrics	• Test load distribution • Execute failover scenarios • Verify peak load handling • Measure performance impact
TST-HES-04	Event processing testing - Real-time event capture, Event prioritization, Alert generation	• Event test scenarios • Prioritization logic testing • Alert generation procedures • Real-time validation approach	• Generate test events • Verify event capture • Test prioritization logic • Validate alert generation
TST-HES-05	Manual data import testing - CSV/XML import, Data validation, Error handling	• Import test procedures • Data format specifications • Validation rule testing • Error scenario coverage	• Test CSV imports • Test XML imports • Verify data validation • Validate error handling

26.3 MDMS-specific testing services

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
TST-MDMS-01	VEE testing - Validation rule execution, Estimation algorithms, Exception handling	• VEE test methodology • Rule test scenarios • Algorithm validation approach • Exception test cases	• Execute validation rules • Test estimation algorithms • Verify exception handling • Validate VEE accuracy
TST-MDMS-02	Billing integration testing - Data export formats, Billing cycle processing, Exception reporting	• Billing test procedures • Export format validation • Cycle processing tests • Exception report testing	• Test data exports • Execute billing cycles • Verify exception reports • Validate format compliance
TST-MDMS-03	Data aggregation testing - Consumption calculations, Loss calculations, Settlement processing	• Aggregation test scenarios • Calculation validation methods • Settlement test procedures • Accuracy verification approach	• Test consumption calculations • Verify loss calculations • Execute settlement processing • Validate aggregation accuracy
TST-MDMS-04	Report generation testing - Standard reports, Custom reports, Scheduled distribution	• Report test catalog • Custom report procedures • Schedule test scenarios • Distribution validation	• Generate standard reports • Test custom reports • Verify scheduling • Validate distribution
TST-MDMS-05	Data archival testing - Archive procedures, Data retrieval, Performance impact	• Archival test methodology • Retrieval test procedures • Performance test approach • Data integrity validation	• Execute archival procedures • Test data retrieval • Measure performance impact • Verify data integrity

26.4 User acceptance testing (UAT) requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
UAT-01	Report Generation - User-defined reports with arithmetic operations, Mathematical functions, Data filtering and sorting, Export capabilities	• UAT test scenarios • Report generation guide • Function documentation • Business user criteria	• Create custom reports • Test mathematical functions • Verify filtering/sorting • Validate export functions
UAT-02	Automated Reporting - Schedule configuration, Format selection, Email distribution, Recipient management	• Automation test cases • Configuration procedures • Distribution test approach • Operations team criteria	• Configure report schedules • Test format options • Verify email distribution • Validate recipient management
UAT-03	Data Validation - Plausibility checks, Threshold monitoring, Exception identification, Alert generation	• Validation test scenarios • Threshold configuration guide • Exception handling tests • Data analyst criteria	• Execute plausibility checks • Test threshold monitoring • Verify exception detection • Validate alert generation
UAT-04	Alert Management - Missing data alerts, Threshold violations, Consumption anomalies, System alerts	• Alert test procedures • Configuration documentation • Anomaly detection tests • Operations criteria	• Test missing data alerts • Verify threshold alerts • Validate anomaly detection • Test system alerts
UAT-05	Event Management - Meter event capture, Event categorization, Alarm generation, Event reporting	• Event test scenarios • Categorization procedures • Alarm configuration guide • Technical team criteria	• Verify event capture • Test categorization • Validate alarm generation • Test event reports
UAT-06	System Monitoring - Connection loss detection, Communication status, Performance monitoring, Health checks	• Monitoring test cases • Status check procedures • Performance criteria • IT team requirements	• Test connection monitoring • Verify status displays • Validate performance metrics • Test health checks

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
UAT-07	Backup and Recovery - Configuration backup, Database archival, Recovery procedures, Data integrity	• Backup test procedures • Recovery test scenarios • Integrity check methods • IT team criteria	• Execute configuration backup • Test database archival • Verify recovery procedures • Validate data integrity
UAT-08	Time Synchronization - System time accuracy, Meter time sync, Daylight saving handling, Time zone management	• Time sync test cases • Accuracy requirements • DST handling procedures • Operations criteria	• Verify system time accuracy • Test meter synchronization • Validate DST transitions • Test time zone handling

27. TRAINING SERVICES

27.1 Training program structure

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
TRN-01	System Administration - IT administrators, 5 days, Classroom + hands-on	• System admin curriculum • Lab environment specifications • Training materials samples • Instructor qualifications	• Review training materials • Attend sample session • Test lab environment • Verify knowledge transfer
TRN-02	HES Operations - HES operators, 4 days, Classroom + hands-on	• HES operations curriculum • Hands-on exercise catalog • Operator skill requirements • Training effectiveness metrics	• Review course content • Test hands-on exercises • Verify operator readiness • Validate skill acquisition
TRN-03	MDMS Operations - MDMS operators, 4 days, Classroom + hands-on	• MDMS operations curriculum • Practice scenarios • Operator competency framework	• Examine course materials • Execute practice scenarios

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Assessment methodology	• Test operator competency • Verify operational readiness
TRN-04	Data Analytics - Business analysts, 3 days, Classroom + workshop	• Analytics curriculum outline • Workshop exercise descriptions • Analytics tool documentation • Business case examples	• Review analytics content • Test workshop exercises • Verify tool proficiency • Validate analysis skills
TRN-05	Integration Management - Integration team, 3 days, Technical workshop	• Integration curriculum • Technical lab specifications • Interface documentation • Troubleshooting scenarios	• Review technical content • Test lab exercises • Verify integration skills • Validate troubleshooting ability
TRN-06	Report Development - Report developers, 2 days, Hands-on workshop	• Report development guide • Template library • Workshop exercises • Development best practices	• Test report creation • Review template usage • Verify development skills • Validate report quality
TRN-07	Executive Overview - Management team, 1 day, Presentation + demo	• Executive presentation outline • Demo scenario scripts • Business value materials • ROI documentation	• Review presentation content • Attend demo session • Verify business alignment • Validate executive readiness

27.2 HES-specific training requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
TRN-HES-01	Communication Management - Protocol configuration, Channel management, Retry mechanisms, Performance tuning	• Communication training manual • Lab exercise descriptions • Protocol documentation • Performance guidelines	• Execute protocol configuration • Test channel management • Verify retry mechanisms • Validate tuning procedures

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
TRN-HES-02	Meter Operations - Reading procedures, Command execution, Firmware management, Troubleshooting	• Operation guide content • Command scenarios • Firmware procedures • Troubleshooting flowcharts	• Test reading procedures • Execute meter commands • Verify firmware operations • Validate troubleshooting skills
TRN-HES-03	Event Handling - Event configuration, Alert management, Escalation procedures, Reporting	• Event catalog documentation • Alert configuration guide • Escalation procedures • Report templates	• Configure test events • Test alert management • Verify escalation flow • Validate reporting capability
TRN-HES-04	System Maintenance - Backup procedures, Performance monitoring, Log management, Updates	• Maintenance manual outline • Checklist templates • Monitoring procedures • Update guidelines	• Execute backup procedures • Test performance monitoring • Verify log management • Validate update processes

27.3 MDMS-specific training requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
TRN-MDMS-01	Data Management - VEE configuration, Data quality monitoring, Exception handling, Manual corrections	• Data management guide outline • VEE configuration examples • Quality metrics documentation • Correction procedures	• Configure VEE rules • Test quality monitoring • Handle test exceptions • Execute manual corrections
TRN-MDMS-02	Billing Operations - Billing cycles, Rate application, Exception processing, Reconciliation	• Billing procedures manual • Rate configuration guide • Exception scenarios • Reconciliation templates	• Execute billing cycles • Test rate applications • Process exceptions • Perform reconciliation

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
TRN-MDMS-03	Analytics and Reporting - Report creation, Dashboard configuration, Analytics tools, Data export	• Analytics guide content • Report templates • Dashboard examples • Export procedures	• Create sample reports • Configure dashboards • Use analytics tools • Test data exports
TRN-MDMS-04	Integration Management - Interface monitoring, Error handling, Data synchronization, Troubleshooting	• Integration manual outline • Interface specifications • Error handling procedures • Sync validation methods	• Monitor test interfaces • Handle integration errors • Test data synchronization • Verify troubleshooting skills

28. DOCUMENTATION SERVICES

28.1 Technical documentation requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
DOC-01	System Architecture - Component diagrams, Data flows, Integration points, Security architecture (PDF, Visio, HTML)	• Architecture document template • Diagramming standards • Security documentation approach • Sample architecture documents	• Review architecture completeness • Verify diagram accuracy • Validate integration documentation • Check security coverage
DOC-02	Installation Guide - Prerequisites, Step-by-step procedures, Configuration, Verification (PDF, HTML)	• Installation guide outline • Procedure documentation standards • Configuration templates • Verification checklist samples	• Test installation procedures • Verify prerequisite accuracy • Validate configuration steps • Execute verification process
DOC-03	API Documentation - Endpoint descriptions, Parameters, Examples, Error codes (OpenAPI, HTML)	• API documentation framework	• Review endpoint coverage • Test API examples

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• OpenAPI specification approach • Example generation methodology • Error code catalog template	• Verify parameter descriptions • Validate error code documentation
DOC-04	Database Schema - Table structures, Relationships, Indexes, Procedures (PDF, SQL scripts)	• Database documentation approach • Schema generation tools • Relationship mapping standards • Script documentation format	• Verify table documentation • Review relationship diagrams • Check index documentation • Validate procedure descriptions
DOC-05	Security Guide - Security controls, Best practices, Incident response, Audit procedures (PDF, encrypted)	• Security guide template • Control documentation standards • Incident response templates • Encryption methodology	• Review security control coverage • Verify best practices • Test incident procedures • Validate encryption implementation

28.2 Operational documentation requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
DOC-06	User Manuals - Function descriptions, Step-by-step procedures, Screenshots, FAQs (RO, EN)	• User manual templates • Translation methodology • Screenshot standards • FAQ compilation approach	• Review manual completeness • Verify translation quality • Check screenshot clarity • Validate FAQ relevance
DOC-07	Operations Guide - Daily procedures, Monitoring tasks, Troubleshooting, Escalation (RO, EN)	• Operations guide structure • Procedure documentation format • Troubleshooting framework • Bilingual documentation approach	• Test daily procedures • Verify monitoring coverage • Validate troubleshooting steps • Check escalation accuracy

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
DOC-08	Administration Guide - System configuration, User management, Backup procedures, Performance tuning (RO, EN)	• Admin guide outline • Configuration documentation • User management procedures • Performance guidelines	• Review configuration coverage • Test user management steps • Verify backup procedures • Validate tuning guidelines
DOC-09	Quick Reference Cards - Common tasks, Shortcuts, Emergency procedures, Contact information (RO, EN)	• Reference card templates • Task prioritization approach • Emergency procedure format • Layout design samples	• Review task selection • Verify shortcut accuracy • Test emergency procedures • Validate contact information
DOC-10	Training Materials - Presentations, Lab exercises, Case studies, Assessments (RO, EN)	• Training material framework • Exercise development approach • Case study methodology • Assessment templates	• Review presentation content • Test lab exercises • Evaluate case studies • Verify assessment effectiveness

28.3 Maintenance documentation

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
DOC-11	Configuration Baseline - Updated after each change by Vendor/Contractor	• Baseline documentation approach • Version control methodology • Change tracking procedures • Update workflow	• Review baseline accuracy • Verify version control • Test update procedures • Validate change tracking
DOC-12	Change Log - Real-time updates by Vendor/Contractor	• Change log format • Real-time update mechanism • Change categorization • Notification procedures	• Test change logging • Verify real-time updates • Review categorization • Validate notifications

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
DOC-13	Known Issues List - Weekly updates by Vendor/Support team	• Issue tracking methodology • Weekly update procedures • Categorization framework • Resolution tracking	• Review issue documentation • Verify update frequency • Test categorization • Check resolution tracking
DOC-14	Performance Reports - Monthly updates by Operations team	• Report template design • Performance metrics catalog • Analysis methodology • Distribution procedures	• Review report templates • Verify metric coverage • Test report generation • Validate distribution
DOC-15	Incident Reports - Per occurrence updates by Support team	• Incident report template • Severity classification • Root cause documentation • Resolution procedures	• Review report format • Test incident documentation • Verify classification system • Validate resolution tracking

29. CONTRACT MANAGEMENT SERVICES

29.1 Contract management requirements

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
PM-01	Contract Planning - Project plan, WBS, Resource plan, Risk register (Once, updated monthly)	• Project planning methodology • WBS template and approach • Resource allocation framework • Risk management procedures	• Review project plan completeness • Verify WBS structure • Validate resource allocations • Test risk tracking mechanisms
PM-02	Progress Reporting - Status reports, Milestone tracking, Issue log, Change requests (Weekly)	• Reporting template samples • Milestone tracking tools • Issue management procedures • Change control process	• Review weekly report format • Test milestone tracking system • Verify issue log functionality • Validate change request workflow

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
PM-03	Quality Management - Quality plan, Test reports, Review records, Compliance matrix (Per milestone)	• Quality management framework • Test reporting templates • Review procedure documentation • Compliance tracking methodology	• Examine quality plan structure • Review test report samples • Verify review processes • Test compliance tracking
PM-04	Stakeholder Management - Communication plan, Meeting minutes, Decision log, Feedback tracking (Ongoing)	• Communication plan template • Meeting management procedures • Decision tracking methodology • Feedback collection approach	• Review communication plan • Test meeting documentation • Verify decision logging • Validate feedback mechanisms
PM-05	Knowledge Transfer - Transition plan, Skills matrix, Handover documents, Lessons learned (End of contract)	• Knowledge transfer methodology • Skills assessment framework • Handover documentation templates • Lessons learned procedures	• Review transition plan • Verify skills matrix coverage • Test handover completeness • Validate lessons learned process

30. SUPPORT AND MAINTENANCE SERVICES

30.1 Post-implementation support

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
SUP-01	Critical (P1) - 30 minutes response, 4 hours resolution, 24x7 coverage	• P1 incident procedures • 24x7 support team structure • Escalation matrix • Historical P1 performance data	• Simulate P1 incident • Measure response time • Verify resolution timeframe • Test 24x7 availability
SUP-02	High (P2) - 2 hours response, 8 hours resolution, 24x7 coverage	• P2 incident procedures • Support team capabilities	• Simulate P2 incident • Measure response time

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Resolution methodology • Service-level requirements compliance history	• Verify resolution process • Validate 24x7 support
SUP-03	Medium (P3) - 4 hours response, 2 business days resolution, Business hours coverage	• P3 support procedures • Business hours definition • Ticket management system • Resolution tracking approach	• Create P3 test ticket • Verify response time • Test resolution workflow • Validate business hours support
SUP-04	Low (P4) - 8 hours response, 5 business days resolution, Business hours coverage	• P4 handling procedures • Priority classification criteria • Queue management approach • Service desk capabilities	• Submit P4 request • Measure response time • Track resolution progress • Verify support coverage

30.2 Maintenance services

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
MNT-01	Preventive Maintenance - System health checks, optimization (Monthly)	• Preventive maintenance checklist • Health check procedures • Optimization methodology • Maintenance schedule template	• Review maintenance checklist • Execute health checks • Verify optimization procedures • Validate monthly scheduling
MNT-02	Corrective Maintenance - Bug fixes, patches (As required)	• Bug tracking procedures • Patch management process • Testing methodology • Release procedures	• Test bug reporting process • Verify patch deployment • Review testing procedures • Validate fix effectiveness
MNT-03	Adaptive Maintenance - Updates for new requirements (Quarterly)	• Change management process • Requirement analysis approach	• Review change procedures • Test requirement handling

Req ID	Requirement description	Evidence required at Offer evaluation stage	Acceptance (handover) test method
		• Update planning methodology • Quarterly review procedures	• Verify update process • Validate quarterly cycles
MNT-04	Performance Tuning - Optimization, capacity planning (Quarterly)	• Performance analysis tools • Tuning methodology • Capacity planning approach • Optimization procedures	• Test performance analysis • Review tuning procedures • Verify capacity planning • Validate quarterly execution
MNT-05	Security Updates - Patches, vulnerability fixes (As released)	• Security update procedures • Vulnerability assessment process • Patch testing methodology • Emergency response plan	• Test security patch process • Verify vulnerability handling • Review testing procedures • Validate rapid deployment

Note:

- Beneficiary endorsement is needed for maintenance services
- Bidders shall submit along with their proposal, the Declaration(free-form statement) on one's own responsibility confirming that the proposed HES+MDM software release version, including all national customizations, will remain supported and not reach End of Support (EOS) or End of Life (EOL) for a minimum period of five (5) years (60 months) following the commissioning of the solution on the Beneficiary's production environment. The declaration shall also confirm the availability of warranty, support, and maintenance services from the Vendor throughout this period) under the same general terms.

31. SUPPORT LEVEL DEFINITIONS AND USE CASES FOR HES/MDMS

31.1 CRITICAL (P1) - SYSTEM DOWN OR MAJOR FUNCTIONALITY LOSS

Definition:

Critical issues that cause complete system failure, major data loss risk, or impact more than 30% of meters/users, requiring immediate intervention to prevent significant business disruption.

Response: 30 minutes | Resolution: 4 hours | Coverage: 24x7

Specific P1 Scenarios for HES

Scenario	Description	Business Impact	Example
Complete HES Failure	Entire HES platform is down	No meter communication possible	System crash, database corruption
Mass Communication Loss	>30% of meters unreachable	Unable to collect consumption data	Head-end system failure
Data Collection Stopped	No new meter readings processed	Billing cycle at risk	Collection engine failure
Command Execution Failure	Cannot send any commands to meters	No remote operations possible	Command processor down
Critical Security Breach	Active cyber attack or data breach	Data integrity/confidentiality at risk	Ransomware, unauthorized access
Database Failure	Primary database inaccessible	Complete data unavailability	Database server crash

Specific P1 Scenarios for MDMS

Scenario	Description	Business Impact	Example
MDMS Core Failure	Complete MDMS platform down	No data processing possible	Application server crash
VEE Engine Failure	Validation/Estimation stopped	Invalid data for billing	VEE service failure
Billing Export Failure	Cannot generate billing files	Billing cycle blocked	Integration breakdown
Data Corruption	Widespread data integrity issues	Incorrect billing risk	Database corruption
Integration Platform Down	All external interfaces failed	No data exchange with other systems	ESB/Integration layer crash
Settlement System Failure	Energy settlement calculations stopped	Financial reconciliation blocked	Settlement engine down

P1 Escalation Path:

1. **0-15 min**: First-line support acknowledgment
2. **15-30 min**: Senior engineer engaged, vendor contacted
3. **30-60 min**: Crisis team assembled, war room activated
4. **1-4 hours**: Root cause identified, fix implemented, testing completed

31.2 HIGH (P2) - SIGNIFICANT FUNCTIONALITY DEGRADATION

Definition:

Issues causing substantial system degradation affecting 10-30% of meters/users or critical business processes, but with workarounds available.

Response: 2 hours | Resolution: 8 hours | Coverage: 24x7

Specific P2 Scenarios for HES

Scenario	Description	Business Impact	Example
Regional Communication Loss	One region/concentrator down	10-30% meters affected	Regional network failure
Slow Performance	System response >10x normal	Operations significantly delayed	Resource exhaustion
Scheduled Reading Failure	Automatic readings not executing	Manual intervention required	Scheduler malfunction
Firmware Update Issues	Cannot deploy firmware updates	Meter updates blocked	Update service failure
Partial Command Failure	Some command types failing	Limited operational capability	Specific protocol issues
Event Processing Delays	Events queued >1 hour	Delayed outage detection	Event processor overload

Specific P2 Scenarios for MDMS

Scenario	Description	Business Impact	Example
Report Generation Failure	Cannot produce critical reports	Management visibility lost	Reporting engine down
Single Integration Failure	One external system disconnected	Manual data transfer needed	SAP interface down
VEE Rule Failures	Specific validation rules failing	Data quality issues	Rule engine errors
Performance Degradation	Processing time >3x normal	Delayed data availability	Database performance issues
Portal Unavailable	Customer/User portal down	No self-service access	Web server failure
Partial Data Loss	One day's data missing	Gap in consumption history	Import failure

P2 escalation path:

1. **0-1 hour**: Support team diagnosis
2. **1-2 hours**: Specialist engaged, workaround implemented
3. **2-4 hours**: Root cause analysis, fix development
4. **4-8 hours**: Fix tested and deployed

31.3 MEDIUM (P3) - MODERATE FUNCTIONALITY ISSUES

Definition:

Issues affecting less than 10% of meters/users or non-critical functionality with minimal business impact and acceptable workarounds.

Response: 4 hours | Resolution: 2 business days | Coverage: Business hours

Specific P3 Scenarios for HES

Scenario	Description	Business Impact	Example
Individual Meter Issues	Specific meters not responding	<10% meters affected	Device-specific problems
Non-critical Feature Failure	Optional features unavailable	Minor inconvenience	Advanced analytics down
UI/Dashboard Issues	Display problems, not data loss	User experience degraded	Visualization errors
Report Formatting Issues	Reports generated incorrectly	Manual correction needed	Template problems
Minor Integration Delays	Slight delays in data sync	Non-critical data lag	Queue processing slow
Configuration Issues	Cannot modify settings	Changes delayed	Config service issues

Specific P3 Scenarios for MDMS

Scenario	Description	Business Impact	Example
Non-critical Report Issues	Optional reports unavailable	Alternative reports available	Custom report failure
Data Quality Warnings	Minor validation issues	Manual review required	Edge case validations
User Access Problems	Individual users cannot login	Specific user impact	Authentication issues
Export Format Issues	File format problems	Manual conversion needed	Export template error
Historical Data Queries	Slow archive data access	Delayed analysis	Archive performance
Dashboard Widget Failure	Specific widgets not loading	Partial dashboard functionality	Widget configuration

P3 resolution process:

1. **Day 1 AM**: Issue logged and prioritized
2. **Day 1 PM**: Initial investigation, workaround documented
3. **Day 2 AM**: Fix developed and tested

4. **Day 2 PM**: Fix deployed to production

31.4 LOW (P4) - MINOR ISSUES OR ENHANCEMENTS

Definition:

Minor issues with negligible business impact, cosmetic problems, or enhancement requests that don't affect system operations.

Response: 8 hours | Resolution: 5 business days | Coverage: Business hours

Specific P4 Scenarios for HES

Scenario	Description	Business Impact	Example
Cosmetic UI Issues	Display alignment, colors	No functional impact	CSS styling issues
Documentation Requests	Missing/unclear documentation	User questions	User guide updates
Feature Requests	New functionality desired	Enhancement opportunity	Additional report types
Log Verbosity	Too many/few log entries	Log management overhead	Logging level adjustment
Performance Tuning	Non-critical optimization	Slight improvement possible	Query optimization
Training Requests	Additional training needed	Knowledge gaps	Refresher training

Specific P4 Scenarios for MDMS

Scenario	Description	Business Impact	Example
Report Enhancements	Additional report fields	Nice-to-have features	Column additions
UI Preferences	User interface preferences	Personal customization	Theme changes
Data Export Options	New export formats requested	Alternative available	Additional file formats
Notification Preferences	Email notification adjustments	Communication preferences	Alert frequency
Help Text Updates	Tooltip improvements	Clarity enhancement	Context help updates
Archive Requests	Old data retrieval	Historical analysis	Data >2 years old

P4 handling process

1. **Within 8 hours**: Acknowledgment and initial assessment
2. **Day 1-2**: Prioritization and planning

3. **Day 3-4**: Development/configuration (if approved)
4. **Day 5**: Testing and deployment (if applicable)

31.5 SUPPORT LEVEL DETERMINATION GUIDELINES

Quick decision matrix:

Impact	Urgency	Affected Scope	Support Level
System Down	Immediate	>30% meters/users	**P1 - Critical**
Major Feature Loss	Hours	10-30% meters/users	**P2 - High**
Feature Degraded	Days	<10% meters/users	**P3 - Medium**
No Operation Impact	Weeks	Individual users	**P4 - Low**

Factors for classification:

1. **Business impact assessment**
   - **Revenue impact**: Direct effect on billing/collection
   - **Customer impact**: Number of affected customers
   - **Regulatory impact**: Compliance violations risk
   - **Operational impact**: Effect on daily operations
2. **Technical severity**
   - **Data integrity**: Risk of data loss/corruption
   - **System availability**: Percentage of system affected
   - **Security risk**: Vulnerability exposure level
   - **Recovery complexity**: Effort required to restore
3. **Examples of classification scenarios**
   1. **"Cannot read 50 meters in one building"**
      - Impact: <1% of total meters
      - Workaround: Manual reading possible
      - **Classification: P3 - Medium**
   2. **"Billing export failed for monthly cycle"**
      - Impact: Entire billing process blocked
      - No workaround for deadline
      - **Classification: P1 - Critical**
   3. **"Dashboard loading slowly"**
      - Impact: User inconvenience
      - Data still accessible via reports

- **Classification: P4 - Low**

4. **"Cannot remotely disconnect meters"**
    - Impact: Critical operation unavailable
    - Safety and revenue implications
    - **Classification: P2 - High**

31.6 SUPPORT PROCESS WORKFLOWS

P1 Critical response workflow:

Detection → Alert (automated/manual) → Support acknowledgment (15 min)
→ Initial assessment (30 min) → Vendor escalation → War room setup
→ Root cause analysis → Fix development → Testing → Deployment
→ Monitoring (24 hrs) → RCA report → Process improvement

P2 High priority workflow

Issue reported → Ticket created → Assignment (30 min)
→ Investigation (2 hrs) → Workaround provided → Fix planning
→ Development → Testing → Scheduled deployment → Verification

P3 Medium priority workflow

Issue logged → Daily review → Assignment → Investigation
→ Solution design → Customer communication → Implementation
→ Testing → Deployment → Closure

P4 Low priority workflow

Request submitted → Weekly review → Prioritization
→ Approval decision → Planning → Implementation (if approved)
→ Documentation update → Closure

31.7 SUPPORT METRICS AND KPIs

Key performance indicators:

Metric	P1 Target	P2 Target	P3 Target	P4 Target
First Response	95% < 30 min	90% < 2 hrs	85% < 4 hrs	80% < 8 hrs
Resolution Rate	90% < 4 hrs	85% < 8 hrs	80% < 2 days	75% < 5 days
Customer Satisfaction	>95%	>90%	>85%	>80%
Escalation Rate	<10%	<15%	<20%	<25%

Metric	P1 Target	P2 Target	P3 Target	P4 Target
Root Cause Provided	100%	100%	90%	As needed

Monthly reporting requirements:

- Incident volume by priority
- Resolution time performance
- Top 5 incident categories
- Trend analysis

32. Annex no. 2.1. – BPMNs LOT 1 HES/MDM RED NORD