HEDNO

Technical Specification for Online Condition Monitoring System on Power Transformers

Contents

1 Project Overview:

The project involves the development and implementation of a software platform for online condition monitoring of power transformers as well as the supply of the corresponding subsystems for measuring and monitoring the transformers actual condition. The project involves the corresponding hardware that will be needed for the above software in order to be delivered as a turn key solution.

The objective of the platform is to act as equipment management system, to collect data from subsystems, **regardless of subsystem manufacturer**, and provide real-time monitoring, trend analysis, equipment health condition estimation, and calculation of relative models using AI tools to provide recommendations also avoid false alarms.

2 Scope of Work:

An integrated condition monitoring system will be procured, installed and commissioned by the Contractor.

Develop a software platform that integrates data from various subsystems for comprehensive monitoring.

Ensure compatibility and seamless integration with subsystems made by other manufacturers, utilizing standard communication protocols and interfaces. Implement communication protocols based on industry standards to ensure seamless data exchange.

Provide data analysis, trend visualization, and equipment health estimation capabilities.

Utilize suitable AI tools to analyze the collected data and identify genuine fault alarms while minimizing false alarms.

Provide a user-friendly interface for data visualization, trend analysis, and reporting.

3 Technical Requirements:

The online condition monitoring system should collect and process data from the following subsystems:

- Dissolved Gas Analysis (DGA) of transformer oil to monitor gas levels and identify potential faults.
- Thermal Models to calculate and display temperature distribution within the transformer.
- Bushings Monitoring to monitor insulation condition and detect abnormalities.
- Cooling Monitoring to monitor cooling system performance and detect anomalies.
- On-Load Tap Changer (OLTC) Monitoring to monitor the condition and operation of OLTC.
- Partial Discharge (PD) to monitor and detect the PD at the transformer.
- The system should be based on a Modular and retrofittable architecture using selectable standard add-on cards will provide coverage of the most important parts of the transformer.

- All necessary connections pipes, flanges, manholes, oil pockets, electrical wiring, junction and control boxes shall be incorporated on the transformer as is on site.
- The manufacturer shall be able to guarantee the availability of spare parts for a period of at least 10 years.
- The system and its components shall be in compliance with CE directives, standards and legislation. The CE certificate shall be in accordance with standards and test methods (EN, IEC, etc.) for equipment in industrial environments.
- Each system should include a detailed technical description of the offered integrated condition monitoring system, including software capabilities and communication requirements.
- Technical datasheets, operation and maintenance manuals, schematics/wiring diagrams, and exploded view drawings of all devices shall be provided in English or Greek language.
- The wiring drawings, layout drawings and detailed data sheets of the integrated condition monitoring system and of all its components will be submitted to DEDDHE.
- The manufacturer shall provide a full maintenance program and maintenance method statement for the offered systems.
- The manufacturer shall provide a guarantee of at least two (2) years of operation for all devices and systems, starting from the date of installation acceptance.
- The manufacturer shall provide analytical information on the expected lifetime/MTTF of consumables and spare parts.
- Historical data should be stored and easily accessible for trend analysis and comparison.

3.1 Software platform

The software platform shall provide the following functionalities:

- Data collection from subsystems.
- Data visualization and presentation.
- Trends analysis.
- Modular approach in order to expand depending on maintenance strategies
- Ability to support and cooperate with 3rd party transformer online monitoring systems.
- The vendor should provide support on the integration of future 3rd party transformer online monitoring systems on the platform
- Ability to import offline data and measurements.
- Provides asset full equipment geographical view.
- Automatic creation of customizable reports, supporting well established file formats
- Should provide health index for each transformer (eg Low, medium and high risk state) combining PD, Bushing Monitoring (BM) and DGA with risk assessment (good, normal, long-term risk, medium-term risk, short-term risk).
- Equipment health condition estimation.
- Calculation of relative models.
- Comparative analysis among transformers located at different substations.
- Comprehensive overviews and reports on operational risks.
- Concrete recommendations on corrective measures.
- Evaluation of fault probability, criticality, and consequences.

- Real-time evaluation of transformer condition, providing comprehensive overviews, operational risk reports, and concrete recommendations for corrective measures, while minimizing false alarms through AI analysis.
- Simultaneous assessment of fault probability, criticality, and potential consequences for the transformer, along with options for rectifying the fault, utilizing AI tools for accurate decision-making.
- The platform should support industry-standard communication protocols for seamless integration with subsystems, such as IEC 61850, Modbus, or DNP3.
- It should facilitate data collection, storage, and retrieval from subsystems in a structured manner.
- The system should be expandable to accommodate future needs.
- The system shall be capable, with configuration, of communicating with existing data history and SCADA systems.
- Perform self-diagnostics on the main systems and the sensors as well.
- For handling purposes, it shall be possible to import stored settings from USB or PC and export data to CSV file to MS EXCEL directly on USB or PC

3.1.1 Software platform models, calculations and outcomes

System shall consider or calculate at least the followings:

- Calculated Hottest Spot with IEC 60076-7 or ANSI/IEEE C57.91
- Bubbling temperature
- Calculation of the aging rate
- Calculation of remaining life
- Capability of transformer to handle overload in the short or long term with live calculation and simulation of overload forecasts in accordance with IEC 60076-7 or ANSI/IEEE C57.91

Optional Requirements

- Calculation of paper moisture content
- Breakdown of the paper
- Monitoring of temperatures (e.g., oil temperature and calculated winding temperature)
- Relative Saturation at standard temperature
- System voltage, load current, frequency, load factor, active power, reactive power, apparent power
- Oi dielectric breakdown voltage
- Losses calculation model
- Normalized energy intensity

3.2 Integration of already existing conventional sensors on the Transformer

- Status monitoring of the protective devices (e.g., RS2001, Buchholz relay, PRD)
- Main tank’s oil temperature.
- Windings temperatures.
- Main tank’s oil level.
- OLTC’s oil level.

Where there is no analog output, the vendor should install a suitable sensor.

3.3 Dissolved Gas Analysis (DGA) Subsystem Requirements

3.3.1 Subsystem Overview:

The DGA subsystem is designed to perform online analysis of dissolved gases in transformer oil for the purpose of transformer condition monitoring.

The subsystem collects samples of transformer oil and analyzes the concentration levels of 8 gases (hydrogen, methane, ethane, ethylene, acetylene, carbon monoxide, carbon dioxide, and oxygen) in addition to moisture (H_2O) content.

3.3.2 Sampling and Analysis:

The subsystem should be capable of extracting oil samples from the transformer at specified intervals.

The collected oil samples should undergo analysis using reliable techniques to determine the concentrations of the 8 gases and moisture content.

The analysis should be conducted in compliance with relevant industry guidelines.

In the case of indoor power transformers, when a carrier gas bottle (pressure vessel) is needed, the gas bottle should be installed in a separate room from the transformer.

3.3.3 Sampling Method and Frequency:

The subsystem should utilize a representative sampling method to ensure the collected oil samples accurately reflect the condition of the transformer.

The sampling frequency should be configurable to meet the monitoring requirements, with the ability to adjust sampling intervals as needed.

In normal operating conditions the sampling frequency must be one measurement in 24 hours.

3.3.4 Communication and Integration:

The subsystem should support standard communication protocols to facilitate seamless integration with the overall monitoring system.

Data collected from the DGA subsystem should be readily accessible and compatible with the software platform for further analysis and monitoring.

The subsystem should have the ability to be integrated in 3rd party software platforms via standard communication protocols.

3.3.5 Alarming and Notification:

The subsystem should be equipped with a reliable alarming system to promptly notify operators of abnormal gas concentrations and moisture content.

Alarms should be configurable based on predefined thresholds and adjustable to suit specific transformer models and operating conditions.

Notifications should be delivered through various channels (e.g., visual, audible, and remote notifications) for efficient monitoring.

3.3.6 Data Visualization and Reporting:

The DGA subsystem should provide a user-friendly interface for real-time data visualization, allowing operators to monitor gas concentrations and moisture content trends.

The subsystem should generate comprehensive reports summarizing the analysis results, trends, and any identified abnormalities.

3.3.7 Calibration and Maintenance:

The subsystem should provide accurate measurement data. For this purpose, it should have the ability for regular calibration, if needed. In normal operating conditions the sampling frequency must be one measurement in 24 hours. Given this, each vendor must provide all the necessary procedures for accurate measurements, like calibration schedule and the related cost.

Maintenance requirements, such as sensor cleaning or replacement, should be clearly defined, and the subsystem should provide alerts or reminders for scheduled maintenance tasks. In normal operating conditions the sampling frequency must be one measurement in 24 hours. Given this, each vendor must provide all the necessary maintenance procedures and maintenance schedules and the related costs.

3.3.8 Security and Data Privacy:

The subsystem should incorporate robust security measures to protect data integrity and prevent unauthorized access.

Compliance with relevant data privacy regulations and industry standards should be ensured, particularly when handling sensitive transformer data.

3.3.9 DGA-9 models, calculations and outcomes

Besides the software platform capabilities, the DGA subsystem shall have embedded capabilities itself to provide at least the following outcomes:

- Trending (rate of change and absolute)
- Duval's Triangle 1, 4, and 5
- Duval's Pentagon 1 and 2
- Dornenburg's Ratios v. Rodgers' Ratios
- Relative moisture of oil %

Optional Requirements

- AI-based Transformer Oil Analysis and Notification in local operation

3.4 Bushing Monitoring Subsystem Requirements

3.4.1 System Overview

The Bushing Monitoring (BM) subsystem is designed to monitor and assess the condition of power transformer high voltage (170 kV) bushings. The subsystem

should collect data related to bushing parameters and provides real-time monitoring, analysis, and reporting.

3.4.2 Sensor Placement

Place sensors at appropriate locations on each high voltage (170 kV) bushing to ensure accurate parameter monitoring. Follow bushings manufacturers' guidelines and industry best practices for sensor placement and installation.

The vendor should provide all required accessories for sensor mounting, ensuring proper installation and secure attachment of the BM sensors to the transformer. This may include mounting brackets, clamps, or fixtures designed specifically for the BM sensors provided by the vendor.

3.4.3 Data Acquisition

Utilize suitable sensors and data acquisition systems to capture real-time data from the bushing monitoring sensors. Ensure reliable and accurate data acquisition to enable effective analysis.

The BM subsystem should compensate for weather and power network fluctuation.

3.4.4 Communication and Integration:

The subsystem should support standard communication protocols to facilitate seamless integration with the overall monitoring system.

Data collected from the BM subsystem should be readily accessible and compatible with the software platform for further analysis and monitoring.

The subsystem should have the ability to be integrated in 3rd party software platforms via standard communication protocols.

3.4.5 Alarming and Notification

The subsystem should incorporate an alarm system to promptly alert operators in case of abnormal bushing conditions. Configure alarms based on predefined thresholds and adjust them to suit specific transformer models and operating conditions. Enable various notification methods (visual, audible, and remote notifications) for efficient monitoring.

3.4.6 Data Visualization and Reporting

Provide a user-friendly interface for real-time data visualization, allowing operators to monitor bushing parameters and trends. Store historical data for trend analysis and comparison. Generate comprehensive reports summarizing the monitoring results, trends, and any identified abnormalities.

3.4.7 Diagnostic Analysis

Implement diagnostic algorithms to analyze the collected data and identify potential issues or degradation trends. Utilize AI techniques and pattern recognition to enhance fault detection and diagnosis accuracy.

3.4.8 Bushing Monitoring Subsystem models, calculations and outcomes

The Bushing Monitoring subsystem shall provide at least the following measurements and calculations:

- Tan delta
- Capacitance C1

Optional Requirements

- Leakage Current

3.5 Cooling Monitoring Subsystem Requirements

3.5.1 System Overview

The Cooling Monitoring subsystem is designed to monitor and assess the cooling system of power transformers. The subsystem collects data related to cooling parameters, monitors the cooling performance, and provides real-time monitoring, analysis, and reporting.

3.5.2 Parameter Monitoring

The subsystem should monitor various parameters associated with the cooling system, including:

- Oil Temperature: Monitor the temperature of transformer oil to assess cooling effectiveness. Where there is no analog output, the vendor should install a suitable sensor.
- Ambient Temperature: Monitor the ambient temperature surrounding the transformer to evaluate cooling conditions.
- Cooling Systems: Monitor the operation and performance of cooling systems (cooling fans, fan sections, etc.).
- Cooling Medium level: Monitor the level of the cooling medium (oil) to identify any abnormalities with correlation to ambient temperature. Where there is no analog output, the vendor should install a suitable sensor.

3.5.3 Sensor Placement

Place sensors at critical locations within the cooling system to ensure accurate parameter monitoring. Follow manufacturer guidelines and industry best practices for sensor placement and installation.

3.5.4 Communication and Integration:

The subsystem should support standard communication protocols to facilitate seamless integration with the overall monitoring system.

Data collected from the cooling monitoring subsystem should be readily accessible and compatible with the software platform for further analysis and monitoring.

The subsystem should have the ability to be integrated in 3rd party software platforms via standard communication protocols.

3.5.5 Data Acquisition

Utilize suitable sensors and data acquisition systems to capture real-time data from the cooling monitoring sensors. Ensure reliable and accurate data acquisition to enable effective analysis.

3.5.6 Alarming and Notification

The subsystem should incorporate an alarm system to promptly alert operators in case of abnormal cooling conditions. Configure alarms based on predefined thresholds and adjust them to suit specific transformer models and operating conditions. Enable various notification methods (visual, audible, and remote notifications) for efficient monitoring.

3.5.7 Data Visualization and Reporting

Provide a user-friendly interface for real-time data visualization, allowing operators to monitor cooling parameters and trends. Store historical data for trend analysis and comparison. Generate comprehensive reports summarizing the monitoring results, trends, and any identified abnormalities.

3.5.8 Cooling Monitoring Subsystem models, calculations and outcomes

The cooling monitoring subsystem should monitor at least the following parameters:

- Operating status (on, off and fault) per cooling stage
- Number of starts per cooling stage
- Operating time per cooling stage

Optional Requirements

- Cooling efficiency monitoring

3.6 OLTC Monitoring Subsystem Requirements

3.6.1 System Overview

The OLTC Monitoring subsystem is designed to monitor and assess the performance and condition of the On-Load Tap Changer of power transformers. The subsystem collects data related to tap changer operation, position, and other parameters, providing real-time monitoring, analysis, and reporting.

3.6.2 Sensor Placement

Place sensors at critical locations within the OLTC to ensure accurate parameter monitoring. Follow manufacturer guidelines and industry best practices for sensor placement and installation.

3.6.3 Communication and Integration:

The subsystem should support standard communication protocols to facilitate seamless integration with the overall monitoring system.

Data collected from the OLTC monitoring subsystem should be readily accessible and compatible with the software platform for further analysis and monitoring.

The subsystem should have the ability to be integrated in 3rd party software platforms via standard communication protocols.

3.6.4 Data Acquisition

Utilize suitable sensors and data acquisition systems to capture real-time data from the OLTC monitoring sensors. Ensure reliable and accurate data acquisition to enable effective analysis.

3.6.5 Alarming and Notification

The subsystem should incorporate an alarm system to promptly alert operators in case of abnormal tap changer conditions. Configure alarms based on predefined thresholds and adjust them to suit specific transformer models and operating conditions. Enable various notification methods (visual, audible, and remote notifications) for efficient monitoring.

3.6.6 Data Visualization and Reporting

Provide a user-friendly interface for real-time data visualization, allowing operators to monitor tap changer parameters and trends. Store historical data for trend analysis and comparison. Generate comprehensive reports summarizing the monitoring results, trends, and any identified abnormalities.

3.6.7 Diagnostic Analysis

Implement diagnostic algorithms to analyze the collected data and identify potential tap changer issues, performance deviations, or mechanical problems. Utilize AI techniques and pattern recognition to enhance fault detection and diagnosis accuracy.

3.6.8 OLTC Monitoring Subsystem models, calculations and outcomes

The subsystem should monitor various parameters associated with the OLTC, including:

- Temperature differential between the transformer tank oil temperature and the OLTC temperature
- Tap Position and total tap switching counter
- Oil level. Where there is no analog output, the vendor should install a suitable sensor.
- The system shall be applicable for on-load tap-changers of all manufacturers and types.

Optional Requirements

- The system must detect and report mechanical irregularities and time differences in the switching process or anomalies in the on-load tap-changer (optional).
- Breakdown voltage.

3.7 Partial Discharge (PD) Monitoring Subsystem Requirements

3.7.1 System Overview

The PD Monitoring subsystem is designed to monitor and assess the occurrence and severity of partial discharges in power transformers. The subsystem collects data related to PD activities, analyzes the data, and provides monitoring, analysis, and reporting capabilities.

3.7.2 PD Detection

Utilize suitable sensors and detection techniques to capture and detect partial discharge events within the main tank of the transformer. Ensure the ability to distinguish between PD signals and other electrical noise sources.

Spatial detection of the source of the PD is not required.

Optional Requirements

Utilize suitable sensors and detection techniques to capture and detect partial discharge events within the HV Bushings of the transformer. Ensure the ability to distinguish between PD signals and other electrical noise sources.

3.7.3 Sensor Placement

The vendor should provide all required accessories for sensor mounting, ensuring proper installation and secure attachment of the PD sensors to the transformer. This may include mounting brackets, clamps, or fixtures designed specifically for the PD sensors provided by the vendor.

3.7.4 Communication and Integration:

The subsystem should support standard communication protocols to facilitate seamless integration with the overall monitoring system.

Data collected from the PD monitoring subsystem should be readily accessible and compatible with the software platform for further analysis and monitoring.

The subsystem should have the ability to be integrated in 3rd party software platforms via standard communication protocols.

3.7.5 Data Acquisition

Utilize appropriate data acquisition systems to capture PD data from the monitoring sensors. Ensure reliable and accurate data acquisition to enable effective analysis.

3.7.6 Alarming and Notification

The subsystem should incorporate an alarm system to promptly alert operators in case of abnormal PD activities. Configure alarms based on predefined thresholds and adjust them to suit specific transformer models and operating conditions. Enable various notification methods (visual, audible, and remote notifications) for efficient monitoring.

3.7.7 Data Visualization and Analysis

Provide a user-friendly interface for real-time data visualization, allowing operators to monitor PD activities, trends and predict potential failures.

3.7.8 Diagnostic Analysis

Implement advanced signal processing and pattern recognition algorithms to analyze PD data and identify potential issues or degradation trends. Utilize AI techniques, such as machine learning, to enhance PD detection accuracy and classification.

3.7.9 Partial Discharge (PD) Monitoring Subsystem models, calculations and outcomes

The subsystem should monitor various parameters associated with the PD, including:

- Total count
- Amplitude
- Repeat Rate
- Partial Discharge Index (PDI)

3.8 Through-Fault Current monitoring (Optional requirement)

The Through-Fault Current Monitoring subsystem is designed to monitor and assess the occurrence and severity of external events such as through faults. The subsystem collects data related to through fault activities, analyzes the data, and provides monitoring, analysis, and reporting capabilities.

3.9 Metallic Enclosure Type and Electrical Panel

3.9.1 Requirements

The vendor should place all electronic devices (like central processing units, electronic PCBs, etc.) and auxiliary electronic equipment (like network devices, adapters, etc.) into an appropriate metallic enclosure.

For outdoor installation, the metallic enclosure should be constructed of stainless steel to provide durability and resistance to harsh environmental conditions. Ensure that the enclosure meets at least the IP65 rating, suitable for outdoor installations.

For indoor installation, the enclosure should be made of standard metal coated with RAL 7032 for protection against corrosion.

3.9.2 Human Machine Interface

The systems should have a local display (Human machine interface - HMI) to monitor the process values and alarms on the field. Allow alarms management and system configuration locally.

3.9.3 Communication options and security

Provide RS485, USB, RJ45 Ethernet connections as standard.

Have hardware communication options available for RS485, Gigabit Ethernet, Fiber Optic.

Support either of the following communications protocols either natively or via additional hardware options: IEC 60870-5-101/104, DNP3.0 and any other industrial protocol necessary for the communication of the installed solution with third party systems such as SCADA Systems.

3.9.4 Weatherproof Design

The outdoor enclosure should have a weatherproof design to protect the internal components from rain, dust, and other environmental factors. Ensure that the enclosure meets at least the IP65 rating, suitable for outdoor installations.

3.9.5 Air Conditioning System

The enclosure (indoor and outdoor) should be equipped with an air conditioning system to maintain optimal operating temperature within it. The air conditioning system should have sufficient cooling capacity to ensure reliable operation of the control panel components in high-temperature environments, as well as heaters system to avoid condensation.

3.9.6 Locking Mechanism

The enclosure should be securely locked using a key-operated locking mechanism to prevent unauthorized access and ensure the safety and security of the equipment.

3.9.7 Cable Installation

Provide proper cable management within the electrical control panel enclosure. Include cable trays, ducts, or other suitable cable management systems to organize and secure the cables. Ensure that cable routing is neat, allowing easy access for maintenance and minimizing the risk of cable damage or interference.

3.9.8 Internal Component Mounting

The electrical control panel should have a modular and flexible design to accommodate various control and monitoring components. Use standardized mounting rails or panels to allow easy installation and replacement of components within the enclosure.

3.9.9 Safety Features

Incorporate safety features such as circuit breakers, fuses, and surge protection devices within the electrical control panel to protect the connected equipment from electrical faults or surges. Include appropriate grounding and earthing provisions to ensure electrical safety.

3.9.10 Labeling and Marking

Clearly label the electrical control panel components, circuits, and terminals for easy identification and troubleshooting. Include marking for power supply connections, communication interfaces, and any other relevant indicators or switches.

3.9.11 Access and Serviceability

Design the electrical control panel enclosure to allow easy access for maintenance and servicing of the internal components. Include removable panels or doors that provide convenient access to the components and allow for swift troubleshooting or repair.

3.9.12 Documentation and Certifications

Provide comprehensive documentation including technical specifications, installation guidelines, and wiring diagrams for the electrical control panel. Ensure

that the control panel complies with relevant safety standards, electrical codes, and regulations.

3.10 Requirements of Signal Cable Installation

3.10.1 Signal Cable Installation

Signal cables should be properly shielded to minimize electromagnetic interference (EMI) and ensure reliable signal transmission. The shielding should be designed to provide adequate protection against external electromagnetic fields and reduce the risk of signal degradation. Signal cables must be installed in separate cable traces from power cables.

3.10.2 Metal Gland Protection Systems

For outdoor installations metal gland protection systems should be used for the rooting tubes, entry and exit points of signal cables in the control panel enclosure. The metal glands should be made of high-quality materials, such as stainless steel or brass, to provide robust protection against mechanical stress, moisture, and environmental contaminants.

3.10.3 Adequate Cable Support and Routing

The control panel should provide adequate cable support mechanisms, such as cable trays, clamps, or brackets, to maintain the integrity of the signal cables. Proper cable routing on the field should be implemented to minimize cable stress, prevent entanglement, and avoid sharp bends that may lead to signal degradation or cable damage.

3.10.4 Grounding

The signal cables should be properly grounded at designated grounding points within the control panel. The grounding points should be securely connected to the panel's grounding system to provide a low-impedance path for electrical currents and to minimize the risk of induced noise or ground loops.

3.10.5 Labeling and Identification

Each signal cable should be appropriately labeled or identified to facilitate easy identification during installation, troubleshooting, and maintenance. Clear and durable cable labels or markers should be used, indicating cable names, identification numbers, or relevant information for quick and accurate cable identification.

3.11 Requirements of ancillary works in scope

3.11.1 Scope of work

The installation scope includes laying and terminating fiber optic communication cables from the electrical cabinet of each power transformer to the control rooms of the substations in the scope of the project. The termination of fiber optics will be done on fiber optic patch panels provided by the contractor that will be installed in existing racks of each substation. Fiber optics should be protected in plastic shielding from the power transformer to the patch panel suitable for harsh

environmental conditions. Contractor should be responsible for the laying and works related to the deployment of fiber optics to each substation.

A fiber optics network switch will be provided by the contractor with adequate number of SFP/SFP+ ports and modules for connecting with each power transformer and at least two Gigabit Ethernet for the interconnection with existing Cisco Routers in the substations. Fiber optic network switch should mount in a standard 1U. PoE-in functionality is desired to power from existing RTU or alternatively through mains. In case of lack of space in the existing racks, the contractor will provide small size racks for the interconnection with Cisco IR 1101 via Fast Ethernet/Gigabit cabling.

The contractor will conduct site surveys in the substation included in the project to collect information regarding the installation of laying, cabling, fiber optics OM3/OM4 required, optical patch panels need to be installed, network switches for the connection of the fiber optics, UTP cabling between the provided fiber optic network switch and Cisco IR 1101.

The contractor will provide unit prices for each of the aforementioned components for the communication of the modules installed in power transformers with the Cisco IR 1101 including all the intermediate components (fiber optics, cabling, optical patch panel, netwotk switches) along with unit price for the effort required for the installation of the aforementioned material per power transformer.

The effort involves all the actions need to be taken to install the modules of the solution in the power transformers, the cabling between the controllers and the control room, the deployment and termination of one vendor fiber optics in same vendor optical patch panels and the connections with network switch. The laying of fiber optics will be conducted using environmental conditions protection materials which are compatible with the solution and the standards for extreme weather conditions.

Specifically, the network switches will have adequate number of ports, according to the number of fiber optics installed for the substation and extra ports for future expansion and scalability. Furthermore, the network switch shall have at least 2 ethernet ports available for the connection with Cisco IR 1101. The network switch will use TCP/IP protocols for the communication of the power transformer modules with the Server components installed in the HEDNO DATA CENTER.

Alternatively, it is accepted a solution of fiber to ethernet converter for each component and the collection of ethernet cables on a network switch.

The contractor is responsible for the communication of components installed in each power transformer with the Cisco IR 1101 and provides support and warranty for the installed active and passive network equipment.

It is explicitly mentioned that that available ports in each Cisco IR 1101 are 1-3 according to the size and significance of substations. The contractor should consider that it will be provided one fast ethernet port from Cisco IR 1101 along with the appropriate IP addressing per substation for the connectivity and the IP assignment. The IP subnets size per substation is a class C private network (/24,

netmask 255.255.255.0). IP addressing in each substation is provided by HEDNO and the contractor is responsible for installation, deployment and parametrization of the equipment in compliance with HEDNO instructions.

Ensure that the installation is performed in accordance with industry best practices and relevant standards for fiber optic cable installations.

The contractor should conduct site surveys in substations and determine the specific needs per substation to deliver the solution as specified. The site survey shall determine the installation of racks in the substation if current racks cannot accommodate installation of network elements and materials of the solution provided by contractor.

Select fiber optic cables suitable for the intended application, taking into consideration factors such as bandwidth requirements, distance, and environmental conditions. The cables should have the necessary capacity to handle the data transmission needs of the monitoring system.

The monitoring system shall make use of the currently installed routers on the substations. The automation control panels shall be delivered without routers so that during the installation the central controllers(e.g.PLCs) will be connected through newly installed switches to the existing Cisco IR1101 routers.

All the central controllers(e.g.PLCs) of the automation control panels of each substation have to be connected to a network switch (part of the offer of the contractor) which will be placed in the control room. The switch has to be connected with an ethernet cable through its ethernet interface to available ethernet switched ports of the existing Cisco routers.

No routers or firewalls are necessary in the scope of the project.

The WAN/LAN networking in the substations and the cybersecurity issues are addressed by HEDNO and the solution of the contractor should be compliant with HEDNO security and network framework policy of the organization.

3.11.2 Cable Routing and Protection

Plan the cable routing path from the electrical cabinet to the control room, considering the shortest and most efficient route while avoiding interference with other systems or potential hazards. Use appropriate cable trays, conduits, or other cable management systems to secure and protect the fiber optic cables against physical damage, moisture, and excessive bending.

3.11.3 Cable Installation

Install the fiber optic cables following recommended installation procedures and guidelines. Ensure that proper cable tension is maintained during installation to prevent cable damage or signal degradation. Adhere to bend radius specifications to avoid exceeding the cable's bending limitations.

Fiber optics specifications should address the specific requirements per substation in terms of distance, bandwidth needs, termination technology, etc. Fiber optics technology for distances of typical substation dimensions should be used in the project and the contractor must explicitly present the technology, material and the

passive and active equipment necessary for the fiber optics cabling (fiber optics patch panels, fiber switches, environmental conditions protection material).

3.11.4 Termination and Splicing

Properly terminate and splice the fiber optic cables at both ends (electrical cabinet and control room) using industry-standard techniques. Use high-quality connectors and splicing equipment to ensure reliable and low-loss connections. Perform testing and verification of the terminated cables to ensure proper signal transmission and minimal insertion loss.

Evidence and documentation of proper termination and transmission through the fiber optiscs should be provided. The contractor is responsible to conduct measurements and tests with fiber testing equipment to verify the performance of optical fiber cabling. At least insertion loss, optical return loss, and fiber length should be included in the performance tests conducted with a valid accreditation equipment.

3.11.5 Cable Labeling and Documentation

Label the fiber optic cables at both ends with clear and unique identifiers to facilitate identification and troubleshooting. Prepare documentation that includes a cable schedule, labeling scheme, fiber identification, and any relevant test results.

3.11.6 Cable Testing and Commissioning

Perform cable testing using appropriate equipment, such as an optical time-domain reflectometer (OTDR), to verify the cable integrity and identify any potential issues. Conduct end-to-end testing to ensure proper signal transmission and compliance with performance requirements. Commission the installed fiber optic communication cable and validate its functionality within the overall monitoring system.

3.11.7 Documentation and As-Built Drawings

Maintain accurate documentation throughout the installation process, including as-built drawings, schematics, and any changes made during the installation. Update the documentation to reflect the actual installation layout and cable routing.

4 Testing and Quality Assurance:

4.1 Online Condition Monitoring System

The Contractor shall propose User Acceptance Tests and System Acceptance Test cases and agree with HEDNO the appropriate controls to verify the functionality of the provided components and solution. The solution should be fully aligned with the technical specifications and the functionalities described in the paragraphs above.

4.2 Software

The Contractor shall propose User Acceptance Tests and System Acceptance Test cases and agree with HEDNO the appropriate controls to verify the functionality of the provided components and solution. The solution should be fully aligned with the technical specifications and the functionalities described in the paragraphs above.

5 Connectivity and System Architecture Specifications

The central controllers(e.g. PLCs) shall be able to communicate using HEDNO's Data Center. Real-time data transmission and retrieval shall be supported for efficient monitoring and analysis. The solution should provide appropriate interfaces (API) for the integration of the solution with third party systems

The central controllers (e.g. PLCs) shall be able to operate as web servers. This will enable the remote configuration of the controllers by accessing them with a web browser or an application.

5.1 System Architecture

In regard to the SERVER side, the contractor will provide a turnkey solution taking into account the virtualization environment of HEDNO DATA CENTER. The solution should provide all the distinct elements with fully supported operating systems, databases, application servers, hardware as physical appliance, etc. The contractor shall provide the licenses for all the components of the SERVER side (OS, virtualization, etc) and will include a detailed plan of scheduled checks and controls for the support, upgrade, maintenance and troubleshooting of all layers for the provided turnkey solution (application level, firmware, virtualization, DBs, application servers, OS, etc) including their security hardening

The application and the accompanying software solutions will be installed in HEDNO DATA CENTER virtualized environment. HEDNO will not provide any licenses or software or hardware required for the solution. The contractor is responsible for the installation of the solution components in HEDNO DATA CENTER and the maintenance, upgrade and support of the software elements of the solution (operating system, databases, application, web application, etc).

The solution should provide a web interface for the end users to login and access the data collected via browser. There may be other ways to access the application, such as client software installed in endpoints, however the preferable way is through HTTPS protocol.

The system shall be designed as a centralized software platform with distributed data acquisition modules. The asset fleet management platform should enable the operator to access and monitor simultaneously the whole fleet of the power transformers. Each new monitoring system on each power transformer shall be integrated on the monitoring platform. A replicate QA and DEV environment should be provided along with the main platform.

For the central software platform (central server) of the system it is required to monitor the SLA Indicator, which should be at least 99%. The contractor should either propose its own implementation (solution) for monitoring the SLA or assist HEDNO in integrating its own existing implementation (solution) for monitoring the SLA.

The contractor will be responsible for the maintenance and support of the solution as a whole and provide updates and resolve vulnerabilities provide bug fixes and support for the solution.

The monitoring software shall be installed on virtual machines in the datacenter of the enterprise.

The data acquisition modules shall be deployed at each substation to collect data from the respective power transformers. Each substation is equipped with Cisco IR1101 routers for the communication with SCADA VRF MPLS network. The security of the network is relied on the security solutions incorporated by HEDNO and is out of the scope of the project.

The communication architecture in the substation level is dependent on the connection of the network switch that collects information/data from all installed modules on the power transformers with one port on the Fast Ethernet module of Cisco IR 1101 that enables reliable and secure communication via TCP/IP network (MPLS) with HEDNO DATA CENTER.

The system architecture shall ensure secure and reliable data transmission between the data acquisition modules and the centralized software platform.

Redundancy measures, such as backup servers or failover mechanisms, shall be implemented to ensure continuous operation and data availability.

The backup solution is not part of the project. The solution should be compatible with HEDNO's backup solution (CommVault backup solution). The proposal of backup scenarios and backup tasks in the side of the solution described (eg providing the info or installation of agents needed for the backup solution) is included in scope.

The new system shall have scalable architecture to accommodate the addition of new transformers or substations in the future.

5.2 Security and Data Privacy

The system shall implement robust security measures to protect the integrity and confidentiality of data in the server side of the solution and the access of users to the web interface (HTTPS).

User access control mechanisms shall be implemented to ensure authorized access to the system and data. Integration with HEDNO's IAM solution (Oracle IAM) for access management and users management is included in scope.

Data encryption protocols shall be employed to secure data during transmission and storage.

The system shall comply with relevant data privacy regulations, such as GDPR (General Data Protection Regulation) or local data protection laws.

HEDNO's Baseline Cyber Security compliance statement (see Annex I) should be answered – documented and included to the technical offer.

5.3 Integration and Interoperability

The system shall provide APIs (Application Programming Interfaces) (e.g. RESTfull API's) to facilitate seamless integration with other enterprise systems or third-party applications. The API's functions shall be enabled already during the installation process and the monitoring software shall be able to communicate directly with other applications without using intermediary components.

The contractor will include optional cost (effort, licenses) for integration of the provided solution with third party systems, using standardized technologies and protocols via APIs. The cost of integration from the third-party system will be covered by HEDNO if the option of integration with third party system is activated.

Integration with existing asset management systems or maintenance management systems should be supported to streamline workflows and data exchange.

Interoperability with different manufacturers' devices and equipment shall be ensured to enable flexibility in choosing hardware components.

5.4 Remote Monitoring and Support

The system shall support remote monitoring and control capabilities to enable remote access and troubleshooting. Remote monitoring refers to the remote access of users with credentials and secure protocols (https) to the web server of the solution that provides dashboards with data visualized, alarms and alerts. Users will have the option to access directly the controllers of the substations to acquire data and alerts/Alarms using secure protocols (https).

6 Commissioning Support Services

The vendor shall provide expert commissioning support services to ensure the successful installation, configuration, and integration of the online condition monitoring system.

Assistance shall be provided in setting up communication protocols, configuring data acquisition modules, and verifying data transmission and retrieval.

The vendor shall conduct thorough testing and validation of the system to ensure its functionality and performance.

On-site support during the commissioning process shall be provided, including troubleshooting and resolving any technical issues that may arise.

7 Documentation and Training:

Provide detailed user manuals and technical documentation for the software platform.

Provide analytical architectural diagrams for the solution.

Provide administrator manuals and administrator training.

All subsystems should be accompanied by comprehensive documentation, including user manuals and technical specifications.

The vendor/supplier shall provide comprehensive training to our personnel on the operation, maintenance, and troubleshooting of the online condition monitoring system.

Training sessions shall cover topics such as system navigation, data interpretation, alarm management, and reporting functionalities.

Hands-on training sessions shall be conducted, allowing our personnel to gain practical experience in using the system effectively.

Training materials, including user manuals, training guides, and reference documents, shall be provided to educate operators on the proper use, maintenance, and interpretation of data generated by the subsystem and support ongoing training and knowledge retention.

The vendor/supplier shall offer both on-site and remote training options to accommodate the availability and location of our personnel.

The vendor/supplier should provide a detailed training schedule for at least 6 individuals and the related cost. Training sessions will take place in Greece both at the HEDNO's substations (where the monitoring system will be installed) and in conference rooms (face-to-face meetings).

8 Delivery and Implementation:

Develop a clear implementation plan with milestones and timelines. The installation sequency must be in series order. The installation and commissioning of the monitoring systems in every substation must be completed to proceed to the next one.

Coordinate with relevant stakeholders for a smooth implementation process.

The minimum requirements in terms of Health and Safety are:

- Assignment of safety officer at the local Labor Inspectorate Authority
- Submission of the Occupational Risk Assessment Study

Safety officer: A vendor's designated engineer should carry out duties according to L.3850/2010 on the field.

Occupational Risk Assessment Study (O.R.A.S.): A risk analysis for the working activities of the contractor on HEDNO site.

9 Support and Maintenance:

Provide ongoing technical support for the software platform, hardware and subsystems, including updates and bug fixes for 5 plus 5 years option.

Provide support and interpretation of alarms and indexes in case of emergency - critical situations. Define response times for addressing any issues or inquiries.

The vendor should provide support on the integration of future 3rd party transformer online monitoring systems on the platform.

The vendor should provide support for the necessary time for training the AI models with the measuring data.

The vendor should be able to provide remote meetings (videoconferences) within 5 days and for situations where the interpretation of results and the provision of advice are required.

10 Prerequisites for participation in the competition

The online condition monitoring project is considered as a turnkey solution and it is crucial to conduct a detailed analysis of the facilities by performing a site visit. This analysis will provide valuable insights and information necessary for the vendor to submit a relevant and accurate offer.

Here are some key points to include in the specification regarding the analysis and site visit.

10.1 Facility Analysis

The vendor should perform a comprehensive analysis of the facilities where the online condition monitoring system will be installed. The analysis should include an assessment of the power transformers and their operational characteristics and configurations. Evaluate the existing monitoring infrastructure, if any, and identify any limitations or gaps that need to be addressed.

10.2 Site Visit

Participants in the tender process can visit all transformers' premises to become aware of the special conditions and specific requirements of each facility.

10.3 Data Collection and Documentation

The vendor should collect relevant data during the site visit, including transformer specifications, electrical drawings, and other technical documentation. Data should be provided by HEDNO or by vendor request from the equipment manufacturers. Document the physical constraints, space availability, and any specific considerations that may impact the installation of the online condition monitoring system. Capture site-specific requirements, safety regulations, and environmental factors that need to be considered during the project implementation.

10.4 Risk Assessment

Perform a risk assessment to identify potential risks and challenges associated with the installation and operation of the online condition monitoring system. Assess factors such as system integration complexities, compatibility with existing equipment, and potential impact on facility operations during installation and commissioning.

10.5 Confidentiality and Security

Ensure that all collected data and information during the analysis and site visit are treated with utmost confidentiality and comply with relevant data protection regulations.

==========

Annex I

HEDNO Baseline Security Requirements

Please fill the compliance statement for each Security Requirement, as follows:

Yes (Y): the Deliverable fulfils the requirement without any restriction. Additional information about how requirements are met should be provided.

No (N): The Deliverable does not fulfil the requirement.

Partial (P): The Deliverable fulfils only part of the requirement. Additional information about how partial requirements are met should be provided.

ID	Statement	Compliant (Y/N/Partial)	Please describe requirement implementation method
1. Architecture and design			
1.1 Solution Design			
1.1.1	The solution design shall follow a 3-tier architecture (front-end, application/middle tier, back-end).		
1.1.2	Different environments shall be utilised, at least for development, UAT and production.		
1.1.3	The supplier shall provide a Security Architecture Study for the Solution in order to record all technical and operational requirements and to design according to them a suitable security architecture both at the network and systems level and at the web application level.		
1.2 Security Hardening			
1.2.1	The individual components of the solution (such as web server, operating system, database) shall be security hardened according to security good practices, including, but not limited to the following: - Default passwords shall be changed on all components without exception; - Unused communication interface shall be disabled;		

ID	Statement	Compliant (Y/N/Partial)	Please describe requirement implementation method
	- Default configurations shall be modified to enhance the security; - Any web services/API and applications that are not required shall be deactivated; - User sessions shall be protected against the unauthorised high-jacking by other users; - Only standardised or certified security algorithms, protocols and functions shall be used.		
1.3 Patch Management			
1.3.1	All system components shall be installed with the latest stable version, with all security patches applied.		
1.3.2	Software updates and security patches shall be installed on a regular basis.		
1.3.3	Critical security patches shall be installed within 10 days of their release and after appropriate communication with HEDNO's relevant stakeholders.		
1.3.4	The supplier shall verify the integrity and authenticity of all software updates prior to deploying any software to any HEDNO-related environment.		
1.4 Endpoint Detection and Response (EDR)			
1.4.1	All systems shall have an approved by HEDNO EDR solution installed and active.		
1.4.2	EDR shall be configured to be updated automatically using a centralised system with the ability to push updates.		
1.5 OT security			
1.5.1	The communication of the solution with other systems (e.g. SCADA), shall follow known guidelines and standards such as IEC 60870-5-101/104, DNP3.0. The supplier shall define which communication protocols will be used.		

ID	Statement	Compliant (Y/N/Partial)	Please describe requirement implementation method
1.5.2	The central controllers (e.g. PLCs) shall be able to communicate using at least one of the following protocols IEC 60870-5-101/104, DNP3.0 serial. The supplier shall define which communication protocols will be used.		
1.5.3	All messages from the OT environment shall be authenticated.		
1.5.4	Only Secure Time Protocols shall be used (such as NTPSec, PTP, IRIG-B) for time synchronization.		
1.5.5	Industry security standards (e.g. IEC 62443 (SL 1 to SL 4)) shall be followed where applicable.		
1.5.6	The data collection process from the OT infrastructure by the solution shall not adversely affect the normal operation of the systems, including outbound communications.		
2. User Access and Authentication			
2.1 Access, Identification, Authentication			
2.1.1	All user access shall be granted and approved on the principles of least privilege and need to know, as per HEDNO's Access Control Policy.		
2.1.2	The solution shall provide support for single-sign-on or federated identities, where technically feasible, in order to identify, authenticate, and authorise HEDNO users.		
2.1.3	If single-sign-on cannot be supported, the solution shall support custom password policy where pattern for strong password can be defined in operation.		
2.1.4	If single-sign-on cannot be supported, the solution shall provide functionality to enforce users to periodically change their password (at a maximum of 90 days).		
2.1.5	If single-sign-on cannot be supported, when an administrator creates a new user account or reset a user password, the user shall be enforced to change the password at first login.		
2.1.6	All sessions shall be encrypted and logged.		

ID	Statement	Compliant (Y/N/Partial)	Please describe requirement implementation method
2.1.7	The solution shall support Role Based Access (RBAC) Model for user accounts and access rights.		
2.1.8	Passwords shall not be displayed in clear text while being entered, transmitted and stored.		
2.1.9	Log-on information shall be validated only upon completion of all input data - if an error condition arises, the system shall not indicate which part of the data is correct or incorrect.		
2.2 Minimum Authentication Requirements (MFA / 2FA)			
2.2.1	The solution shall support Multi-Factor Authentication for user access.		
2.3 Authentication security			
2.3.1	The solution shall not store passwords hard coded (e.g. in its source code).		
2.3.2	Passwords shall be stored in a securely hashed form, using only algorithms specifically designed for password storage.		
2.3.3	Authenticated sessions shall have a maximum duration of 12 hours, and shall expire after the session has been inactive for a maximum of 15 minutes, as per HEDNO's Identity and Authentication Standard.		
2.4 Privileged Access Management			
2.4.1	Administrative access to the solution shall be controlled through HEDNO's PAM solution (IBM Secret Server).		
3. Network			
3.1 Network Segregation			
3.1.1	The solution shall be deployed in an internal network zone.		
3.2 Network Security			
3.2.1	The solution shall be adequately protected from unauthorised access and malicious attacks,		

ID	Statement	Compliant (Y/N/Partial)	Please describe requirement implementation method
	utilising HEDNO's security solutions (e.g. firewalls).		
4 Data Management			
4.1 Data Validation			
4.1.1	All processes that receive data input (both manual and automated) shall control and validate input data, e.g. in terms of format, length and syntax.		
4.2 Data Protection			
4.2.1	All data shall be encrypted at rest and in transit, using secure and up-to-date algorithms, as per HEDNO's Encryption Standard.		
5 Logging and Monitoring			
5.1 Logging and Monitoring			
5.1.1	The solution shall have the capability to log the following events (in application, database, operating system and network): a) successful logins and logouts b) failed login attempts c) privilege escalation attempts (e.g. switch user on privileged accounts) d) rejected connections e) violations of access restrictions f) manipulation attempts (e.g. shutdown of the system, modification of system time) g) creation or modification of user accounts h) access to the security logs i) attempts to modify the security policy *In case of partial compliance, state the non-compliant point(s) from the above.*		
5.1.2	The solution shall have the capability to log the following details for each event: a) time b) date c) type of event d) IP address of the origin e) user ID		

ID	Statement	Compliant (Y/N/Partial)	Please describe requirement implementation method
	In case of partial compliance, state the non-compliant point(s) from the above.		
5.1.3	The solution shall be able to send the relevant logs (e.g. security logs) to HEDNO's SIEM (ArcSight).		
5.1.4	Read-only access to the logs shall be restricted to specific privileged accounts or authorised user profiles.		
5.1.5	Logs shall be retained for a period of at least 12 months.		
6. API Design			
6.1 Secure API Design			
6.1.1	The solution shall provide functionality that supports industry standards for secure integrations, i.e., API endpoints (e.g. Open Authentication version 2 (OAuth2) for REST API's and similar for web services/SOA or other supported API.).		
6.1.2	Requests containing unexpected or missing content types shall be rejected with appropriate headers.		
6.1.3	API URLs shall not expose sensitive information, such as the API key, session tokens etc.		
6.1.4	API requests shall be performed over HTTPS.		
6.1.5	REST services shall explicitly check the incoming Content-Type to be the expected one, such as application/xml or application/JSON		
6.1.6	Enabled RESTful HTTP methods shall be a valid choice for the user or action, such as preventing normal users using DELETE or PUT on protected API or resources.		
6.1.7	REST services shall have anti-automation controls to protect against excessive calls, especially if the API is unauthenticated		
6.1.8	The use of the HTTP PATCH method on binary data in APIs shall not be used.		

ID	Statement	Compliant (Y/N/Partial)	Please describe requirement implementation method
6.1.9	The HTTP DELETE method shall only be exposed where it is absolutely required, and may need to be made available differently for the same API depending on whether the requesting party is internal or external.		
6.1.10	All API endpoints shall be protected by the designated HEDNO WAF solution (where applicable).		
7 Backup Management			
7.1 Backup & Restore			
7.1.1	A backup plan shall be provided covering the following types of data: a) operating system b) application c) database d) log data *In case of partial compliance, state the non-compliant point(s) from the above.*		
7.1.2	Backup and disaster recovery capabilities shall be aligned with HEDNO's business requirements and tested periodically.		
8 Web Application			
8.1 Secure Web Application Design			
8.1.1	Unnecessary information from HTTP response headers shall be removed related to the OS, web-server version, application frameworks, etc.		
8.1.2	Application Directory listing shall be disabled.		
8.1.3	Client-side validation shall be used as a second line of defence, in addition to server-side validation.		
8.1.4	HTTP methods which are supported by the application shall be defined and limit the usage of GET/POST requests (e.g. disallow GET when POST is required).		

ID	Statement	Compliant (Y/N/Partial)	Please describe requirement implementation method
8.1.5	Data in transit shall be encrypted (e.g. TLS v1.2 and above) and shall not fall back to insecure or unencrypted protocols.		
8.1.6	All third-party components used by the application, such as libraries and frameworks, shall be identified (e.g. version) and checked for known vulnerabilities.		
8.1.7	The application shall appropriately validate input and shall have protections/security controls in place to prevent against the latest OWASP top 10, and be tested for protection against these vulnerabilities/exploits (https://owasp.org/www-project-mobile-top-10/).		
8.1.8	SQL queries shall be protected through the use of prepared statements or query parameterisation, and thus not susceptible to SQL injection.		
8.1.9	The web application shall have a strong and consistent framework for session ID management. Creation and deletion shall be protected throughout their life cycle, taking, among others, the following measures: a) The session ID shall not be included in the URL. b) The session ID shall be built with high complexity (using numbers, characters, special characters, length, randomness or encryption) so that it can not be easily guessed. c) Session IDs based on source IP or personal information shall not be used. d) Numerically incremental session IDs shall not be used. e) Active sessions shall be controlled to avoid multiple instances of the application with the same session ID. f) Session IDs shall expire 1. after a predefined inactivity time. 2. when the user logs out. 3. when the browser's window is closed. g) Session IDs shall not be re-used. h) Users shall not be allowed to choose or change the session ID.		

ID	Statement	Compliant (Y/N/Partial)	Please describe requirement implementation method
	In case of partial compliance, state the non-compliant point(s) from the above.		
8.1.10	The web application shall not disclose any kind of information that can lead to information leakage, and shall ensure that: a) there are no visible and user-downloadable files containing information about the application (e.g. admin manuals) b) code presented to the user does not contain sensitive information about the application (e.g. references to databases, passwords, user IDs, application structure, programmer comments) c) information sent through hidden variables is controlled d) information sent by the application is limited to a minimum (e.g. no unnecessary information on welcome or help messages) e) identification of the web server type and version shall be removed (e.g. from the HTTP responses) *In case of partial compliance, state the non-compliant point(s) from the above.*		
8.1.11	Default pages from the web server and from the web application (e.g. error messages) shall be disabled and no unnecessary details shall be shown. A generic error page shall be used instead.		
8.1.12	All unnecessary HTTP methods (e.g. PUT, DELETE, TRACE, OPTIONS) and WEBDAV methods (e.g. MOVE, PROPFND) shall be disabled on web application servers.		
8.1.13	Untrusted ActiveX controls and applets shall not be used. Any such objects in the application shall be signed.		
8.1.14	The web application shall have provisions against Cross-Site Request Forgery (CSRF or XSRF) attacks.		
8.1.15	The web application shall implement HTTP Strict Transport Security (HSTS) in critical sections or when transmitting critical data. In other		

ID	Statement	Compliant (Y/N/Partial)	Please describe requirement implementation method
	scenarios the use of SSL plus user authentication is sufficient.		
8.2 Web Application Cookies			
8.2.1	The 'HttpOnly' attribute shall always be set to 'true'.		
8.2.2	If the connection between client and server is protected by HTTPS then all cookies shall have the 'secure' flag set.		
8.2.3	The 'domain' attribute shall be set restrictively. This means that it shall only be set for the server that really needs the cookie. If the application, for example, can be reached under 'application.mysite.com', the corresponding cookie should be set to '; domain=application.mysite.com', NOT to '; domain=.mysite.com'.		
8.2.4	The 'path' attribute shall be set restrictive. If the application is accessible under '/myapplication', the 'path' attribute shall be set correspondingly: '; path=/myapplication/'. A wrong setting would be: '; path=/myapplication', as the browser would also send the cookie to '/myapplication-exploited/'.		
8.3 SSL/TLS Configuration			
8.3.1	Only strong cipher suites shall be used. Weak and deprecated ciphers shall be avoided.		
8.3.2	Strong encryption algorithms such as AES (Advanced Encryption Standard) with key lengths of 128 bits or more shall be used.		
8.3.3	For hashing: a) Use SHA-2 algorithms (SHA-256 recommended) b) Use SHA-1 only for SHA-2 incompatible clients (some web browsers) c) Disable all other hashing algorithms (e.g. MD5) *In case of partial compliance, state the non-compliant point(s) from the above.*		

ID	Statement	Compliant (Y/N/Partial)	Please describe requirement implementation method
8.3.4	When implementing the SSL/TLS channel, the following considerations shall be taken: a) Disable compression. b) Enable secure renegotiation. c) Disable client initiated renegotiation. d) Enable session resumption. e) Select most secure compatible cipher based on server preference. *In case of partial compliance, state the non-compliant point(s) from the above.*		
8.4 Web Applications Security Compliance			
8.4.1	Before go-live, all critical and high security vulnerabilities (e.g. identified through penetration tests / vulnerability assessments) shall be remediated.		

Assessment of Cyber Security Specifications

n.	Criteria	weight
1	Architecture and design	16/75
2	User Access and Authentication	14/75
3	Network	2/75
4	Data Management	2/75
5	Logging and Monitoring	5/75
6	API Design	10/75
7	Backup Management	2/75
8	Web Application	24/75
Total		100%

Technical Offers which rank bellow 65 % on the Cyber Security Specifications will be rejected