Automation Technical and Functional Requirements

C256-EQ-J-SP-00002

Title:		
Automation Technical and Functional Requirements -		
Document no: **C256-EQ-J-SP-00002**	Contract no.:	Project: MFW

Classification: **Internal**	Distribution:
Expiry date:	Status **Final**

Distribution date: 12.12.2022	Rev. no.: **01**	Copy no.:

Author(s)/Source(s):	
Subjects: Design premises necessary for the front-end engineering and design (FEED) and execution phase of the MFW offshore wind projects.	
Remarks:	
Valid from: **12/12/2022**	Updated:
Responsible publisher:	Authority to approve deviations:

Technical. responsible (Organization unit / Name):	Date/Signature: eApproved: 17.11.2022
Responsible (Organization unit / Name):	Date/Signature: eApproved: 12.12.2022
Recommended (Organization unit / Name):	Date/Signature: eApproved: 22.11.2022
Approved by (Organization unit / Name):	Date/Signature: eApproved: 22.11.2022

Table of contents

1. Introduction 6
1.1. Purpose 6
1.2. Introduction 6
1.3. Wind farm description 6
1.4. Design Criteria 6
1.5. HSE 6
1.6. Regulations, Standards, Codes and Specifications 6
1.7. Conflict/Deviations 7
2. Control and Design Philosophy 7
2.1. General 7
2.2. Design Philosophy 7
2.2.1. Functional design 9
2.2.2. Data to Company IMS 9
2.2.3. Interface to top level Scada system 9
3. Industrial Automation and Control System (IACS) 11
3.1. General 11
3.2. Control system objective 11
3.2.1. System description 11
3.3. High Voltage Control and Protection system 12
3.4. Power Control, Topologies and Grid Compliance 13
3.4.1. Wind Farm Power control 15
3.4.2. Grid Code Compliance 15
3.4.3. ESI Power Controller 16
3.4.4. Breakers/Disconnector Status information 17
3.4.5. Input from Cable monitoring systems 17
3.5. Communication between EPC and WFPC 17
3.6. Test facility 18
4. Cyber Security 18
5. System Requirements 18
5.1. Hardware and Software 18
5.1.1. General 18
5.1.2. System Software 19
5.1.3. PC's/Servers and client applications and software tools 20
5.1.4. Back-up 20
5.1.5. System Hardware 20
5.1.6. Time synchronization 21
5.1.7. Time stamping 21
5.1.8. Manufacture requirements 21
5.1.9. Availability and redundancy requirements 22
5.1.10. SCADA servers and operator stations 22

5.1.11. Data archiving 22
5.1.12. Monitoring 23
5.1.13. Application configuration 23
5.2. Human Machine Interface (HMI) 23
5.2.1. General requirements 23
5.2.2. HMI Displays 24
5.2.3. Integration of OSS SUS 25
5.2.4. Integration of HMI from WTG SCADA 26
5.2.5. Alarm and events 26
5.2.6. Alarm management system 28
5.2.7. Blocking and suppression of alarms 28
5.2.8. Trending 29
5.3. Printing facilities 29
5.4. Safety system 29
5.4.1. Shutdown system 29
5.4.2. Fire detection/Protection System 30
5.4.3. Gas detection 30
5.5. Heating, Ventilation and Air Conditioning (HVAC) 30
6. Network, communication, and Interface requirements 31
6.1.1. General requirements 31
6.1.2. Network hierarchy/topology 31
6.1.3. Network redundancy 32
6.1.4. Network Segregation 32
6.1.5. Interface to IMS system 32
6.1.6. Communication/Interface to TSO 33
6.1.7. Communication/interfaced protocols 33
7. Metering, Condition Monitoring, and Instrumentation 34
7.1. Metering System 34
7.2. Power Quality Metering 34
7.2.1. PQM Server 35
7.3. Condition Monitoring System (CMS) 36
7.4. Monitoring of export- and inter-array cables 37
7.5. Phasor Measurement 38
8. Field design 38
8.1. General 38
8.2. Cabinets 38
8.2.1. Terminations 39
8.3. Field instruments 39
8.3.1. Degrees of protection 40
8.3.2. Material selection 40
8.3.3. Material selection table 40
8.3.4. Field architecture and segregation 41
8.3.5. Fire detection equipment 41

8.3.6. Winterization 42
8.3.7. Temperature instruments 42
8.3.8. Level instruments 42
8.3.9. GIS (Gas Insulated Switchgear) breaker and SF6 monitoring 42
8.3.10. Spare requirements 42
8.3.11. Tag plates 42
8.4. Power supply and power distribution 43
8.5. Earthing 43
9. Performance 43
9.1. Logic Solver performance 43
9.2. Response times 43
9.3. IACS/SCADA lifetime 44
9.3.1. IACS/SCADA component lifetime 45
9.4. Equipment operational requirements 45
10. Testing 45
10.1. FAT (Factory Acceptance Test) 45
10.2. Testing of system 46
11. Life Cycle Information (LCI) 46
12. Additional information 46
12.1. Abbreviations 46
12.2. Definitions 48
12.3. Changes from previous version 49
12.3.1. Changes from revision 01 49

1. Introduction

1.1. Purpose

The purpose of this document is to describe the technical and functional requirements for the Automation system for the MFW . The content of this document describes the requirements for the

1.2. Introduction

This document provides the overall design criteria for the Industrial Automation and Control System (IACS) and shall form the basis for the functional design specifications for IACS sub-systems, including Supervisory Control and Data Acquisition (SCADA) systems, with the required interfaces to all other related systems and external interfaces. Fiscal metering and TSO communication needs to be clarified and agreed with TSO

1.3. Wind farm description

Reference is made to Design basis MFW – PM735-PMS-050-001

1.4. Design Criteria

The design and operation of the entire Wind Power Plant (WPP) shall be demonstrated to be in accordance with all applicable laws, rules and regulations as required by the regulatory authorities, including but not limited to, Contract Appendix E document.

It is the Contractor's responsibility to ensure that the design, material, and equipment provided meets all relevant requirements.

Contractor shall indicate in their proposal if any part of this specification deviates from Contractor's usual design so that a significant increase in the cost is expected without providing a corresponding increase in quality; or if Contractor's usual design will provide better quality than the design required by this specification.

1.5. HSE

Contractor shall ensure that the design incorporates HSE best practices and gained experiences so that construction, testing, installation, maintenance, and normal production activities can be carried out in an efficient manner, and without risk to people, environment, or the asset.

1.6. Regulations, Standards, Codes and Specifications

All engineering, design and construction covered by this specification shall be in line with relevant Polish Laws and Regulations and practices applicable for the offshore wind sector.

For roject specific design requirements towards Polish Transmission System Operator (TSO) is defined in the Grid Connection Agreements between TSO and , Technical Conditions for the Connection to the Telecommunication Network of PSE S.A., Grid Code and any other relevant TSO requirements for Telecommuncation systems.

Contractor shall be responsible to ensure and document that its products are designed in accordance with applicable laws, regulations, standards given in App E of the Contract.

1.7. Conflict/Deviations

If there are inconsistencies between the various requirements given within the regulations, requirements, and standards, reference is made to the contractual Order of Precedence.

2. **Control and Design Philosophy**

2.1. General

The wind power plant shall be built for unmanned operation. This shall include the Onshore Substation (ONS), Offshore Substation (OSS) and Wind Turbine Generators (WTGs). It shall be possible to control and monitor the Wind Power Plant (WPP) from remote sites, including e.g. utility systems.

The WPP shall have an integrated automation system for supervision, control and monitoring of the Wind Farm including ONS, OSS, WTGs and cable monitoring. The automation system shall control utilities, or interface third party utility control systems supplied by package suppliers such as HVAC, UPS, etc. The overall automation system for is denoted Industrial Automation and Control System (IACS), see section 3 for further details.

The control system and electrical HV Control & Protection system/ equipment, MV, LV equipment/systems and utility equipment/systems for ONS / OSS and the WTGs shall be remotely operated and controlled from the Multi wind farm Central Control Room (CCR), located at the O&M base.

The IACS system in the wind farm shall be designed with three levels of control.

1. Remote Control from CCR at O&M base
2. Station control from ONS and OSS.
    - The Control Room on the ONS shall serve as a backup for the CCR and the ONS Station control must therefore be designed with necessary facilities to accommodate this.
3. Local control including:
    - WTG in local Control
    - Local control of substations equipment (CB (Circuit Breakers), Disconnector, earth switch etc)

The control philosophy with different control levels shall be described and detailed during the detail engineering phase.

2.2. Design Philosophy

The SCADA control and monitoring system for the wind farm including ONS, OSS and WTGs shall be designed for unmanned operation and remote maintenance. A Power System Philosophy will be developed by Contractor's power consulting team, and shall be the base for the power control and protection system.

Unmanned operation includes:

1. Remote control and monitoring of all systems from CCR at O&M Base

2. All SCADA PCs and servers (both physical and VM (Virtual Machine)) are available via a remote access solution for remote operation
3. All equipment located in normally unmanned locations can be remotely reset from HMI
4. No SCADA HMI PC on wind turbines. Service technicians will require a mobile solution including dedicated port (RJ45-socket) on the SCADA network switch for local monitoring and control.

It shall be possible to perform remote troubleshooting, diagnostics, SW updating/modification/changes of all programmable monitoring and control devices/units, sub systems, database system/servers, Client workstation remotely via dedicated servers and Engineering workstations both locally and from the O&M Base CCR via Company secure access solution. This also includes third-party control systems for utilities

It shall be possible to modify and change set-points, alarms and reset alarm, alarm inhibits/suppressions on any devices remotely from CCR either from Operator Station (OS) or from Engineering Workstations (EWS) Human Machine Interfaces (HMIs). Different roles/accesses to operate the WF, to do HV switching, operation of ESI / WTG or both, change parameters/setpoints shall be defined.

The IACS, SCADA, Control and protection system, Instrumentation and local control systems shall be designed to provide safe, reliable, and efficient operation of the wind farm. This shall include the following:

- Fail safe design
- Redundant design of the component/system listed here:
  - Network
  - Individual equipment assemblies. Including electrical power supplies.
  - Connection to Local Control Units (LCUs)/Intelligent Electrical Devices (IED's).

Network infrastructure must be setup for this purpose i.e., network to be available and WAN connection to be established.

The SCADA systems, control & protection system/equipment including necessary network shall be fully redundant and a fail-safe philosophy shall be evaluated and defined for all related equipment, network, and critical signals.

The is designed with one OSS each, which has two separate "production trains". The two trains shall be functionally segregated to the extent that one may be taken out of service for maintenance whilst the other is fully operational. This concept shall be reflected in the IACS design.

In case of equipment failure or communication failure, the system and equipment shall move to a predefined safest state with regards to the severity of the failure. The IACS shall have robust and fault tolerant protocols for the dual redundant communication network. The IACS shall have intuitive alarms and diagnostics tools for the communication network.

SCADA firewalls shall be included with required function and software for remote monitoring and management/control by Company.

The SCADA data system servers shall be capable of collecting real time, historical Open database Connectivity (ODBC) and analysed data from all systems. The data shall be available on trend displays and for forwarding of all data to Company Information Management System (IMS) via the office LAN for transmission to land organizations.

SCADA clients shall be available at the ONS (backup for CCR), OSS, and CCR.

Required engineering and service workstation shall also be installed at same locations and shall be accessible via Company secure access service.

Fiber optic connections embedded into the two export cables shall be provided for redundant communication between ONS and offshore substations.

External WAN data lines for communication to Company sites shall be based on redundant fiber optical network and preferably MPLS-TP.

2.2.1. Functional design

All systems on shall have a uniform, consistent and standardized design. This applies to all aspects of system design, including both hardware (cabinet design, cabling etc), software (user interfaces etc), condition monitoring capabilities and so on.

2.2.2. Data to Company IMS

All relevant real-time data shall be made available to the Company IMS/Wind Farm Management System. This shall include both raw and analysed data from all SCADA systems. Raw data shall be available without any filtering or compression, via agreed interface protocols. Definition of “all relevant real-time data” shall be detailed during the detail engineering phase and agreed with Company.

Both raw and analysed data shall include historical records, plus data from SCADA and Control and Protection systems, monitoring systems, database system, Conditioning Monitoring systems (CMS) Metering Systems, etc. Data shall flow from the source systems directly to the company IMS buffer servers on the company network without leaving and re-entering the Company network. Data transfers should, unless agreed with Company, occur continuously and with minimal delay.

2.2.3. Interface to top level Scada system

The automation systems, including ESI SCADA, WTG SCADA and SUS SCADA (if not integrated part of ESI SCADA) shall have OPC UA interface to a future Top Level/Common SCADA in the CCR for operation of the windfarm. The WTG SCADA for could be combined, the ESI SCADA for could be combined and the SUS SCADA (if not integrated part of ESI SCADA) could be combined for . Top Level/Common SCADA will probably not be made until B is built. This to be clarified with Company during FEED.

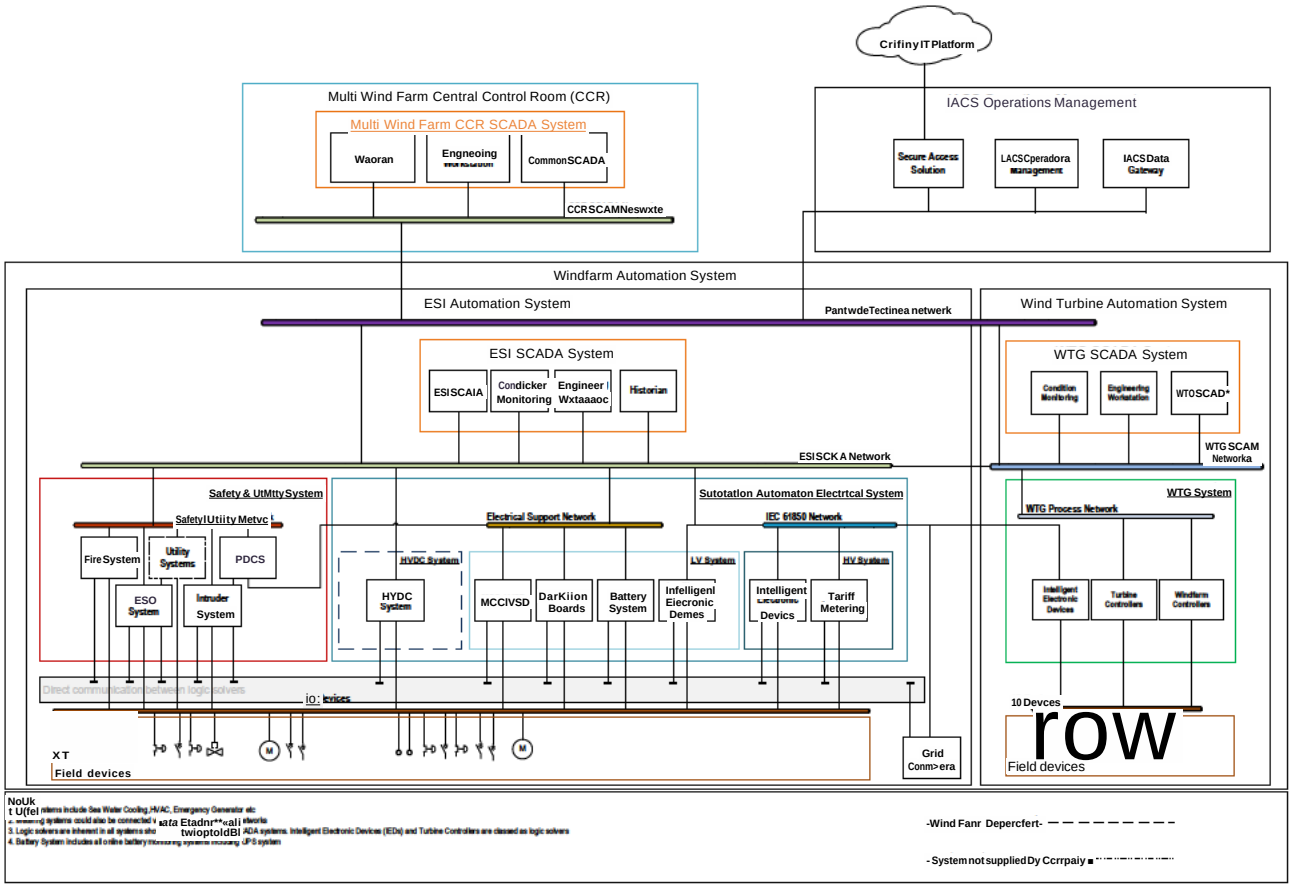

Figure 1 - IACS General Architecture

The interface shall support OPC UA companion specification OPC 10040 - UA for IEC 61850 for monitoring and operation of the IED's exposing the information models to the above systems. In addition, the interface shall support other relevant OPC UA companion standards for non-IED equipment in the ESI systems exposing the information models to the above systems. The information model shall be inclusive of alarms and events.

The OPC UA interface should as a minimum support the following features:

A. OPC UA clients shall support the "Standard UA Client 2017 Profile" (http://opcfoundation.org/UA-Profile/Client/Standard2017).

B. OPC UA clients shall support the "Documentation - Client" profile (http://opcfoundation.org/UA-Profile/Client/Documentation).

C. OPC UA clients shall support the "Base Client Behaviour Facet" profile (http://opcfoundation.org/UA-Profile/Client/Behaviour)

D. OPC UA clients shall support the "Reverse Connect Client Facet" profile (http://opcfoundation.org/UA-Profile/Client/ReverseConnect)

E. OPC UA servers shall support the "Standard UA Server 2017" profile" (http://opcfoundation.org/UA-Profile/Server/StandardUA2017).

F. OPC UA servers shall support the "Data Access Server Facet" profile (http://opcfoundation.org/UA-Profile/Server/DataAccess)

G. OPC UA servers shall support the "Documentation - Server" profile (http://opcfoundation.org/UA-Profile/Server/Documentation).

H. OPC UA servers shall support the "Base Server Behaviour Facet" profile (http://opcfoundation.org/UA-Profile/Server/Behaviour).

I. OPC UA servers shall support the "Reverse Connect Server Facet" profile (http://opcfoundation.org/UA-Profile/Server/ReverseConnect) K

J. OPC UA client shall support the “Alarm & Condition Server Facet” profile http://opcfoundation.org/UA-Profile/Client/ACBaseCondition
K. OPC UA server shall support the “Alarm & Condition Server Facet” profile http://opcfoundation.org/UA-Profile/Server/ACBaseCondition2021

The OPC UA interface should support the following feature:
OPC UA clients should support the “Pub/Sub facet”
OPC UA servers should support the “Pub/Sub facet”

3. Industrial Automation and Control System (IACS)

3.1. General

An overall Automation and Control System shall be installed for monitoring and control of the wind farm.
For the IACS shall comprise one or more of the following components: Industrial control systems, including but not limited to distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), Intelligent Electronic Devices (IEDs), Supervisory Control and Data Acquisition (SCADA) systems, network components, networked electronic sensing and control, and monitoring and diagnostic systems. All systems designated for operational use shall be compliant for real-time monitoring and control. The ESI SCADA shall therefore be designed with complete functionality for real-time monitoring, and for control of all electrical and utility equipment on the ONS/OSS. The control system shall be compliant with the IEC 61850 standard for substation automation and support other standard communication protocols as listed in chapter 6.1.6.

Figure 1 - IACS General Architecture gives a general overview of the IACS and does also indicate main interfaces towards systems and parties external to IACS. Please note that the outline of the IACS is only functional, hence not necessarily reflecting location or the Automation network topology correctly.

3.2. Control system objective

The objective of the IACS is to control and monitor the power generation, the electrical power distribution network, and auxiliary systems.

The IACS shall control and monitor the 400/220 kV switchboards, HV, MV and LV and all auxiliary equipment on the ONS, and controlling the 220/66 kV switchboards, HV, MV and LV and all auxiliary equipment on OSS including 66kV inter array cable incomers from the WTGs, with required signals and set point to/from the WTG SCADA Plant Control/Wind Farm Power Control (WFPC) system.

The ESI SCADA shall also control and monitor the WTG 66 kV switchgear in the WTGs via the IEC 61850 network.

3.2.1. System description

The IACS shall in basis consist of the following systems:

- ESI SCADA performing Supervisory control and monitoring of the high voltage distribution, medium voltages and low voltage distribution system and transmission system from the high voltage connections in the WTGs.
- High Voltage Control & Protection system including control equipment for:

  - Onshore 400/220 kV high voltage substation switchgear and other high voltage components, transformers, reactors etc.
  - Offshore 220 kV/66 kV high voltage substation switchgears and other high voltage components, transformers, reactors etc.
  - 66 kV inter array cable distribution system, including 66 kV WTG switchgear and the 66/0,690kV WTG transformer.
- ONS auxiliary system/equipment including but not limited to Low Voltage switchgears/distribution system, power supplies, battery systems, UPS, fire detection, HVAC systems as needed to obtain remote capabilities to the SCADA system
- OSS Safety and Utility automation system (SUS SCADA), including, but not limited to:
  - Shutdown System
  - Fire (and Gas) detection
  - Protection systems
  - Auxiliary and Utility systems
  - Low Voltage switchgears/distribution system and UPS's
  - HVAC control system
  - Intruder system
- WTG SCADA performing Supervisory control, monitoring of the WTGs, and controlling Active Power (MW) and Reactive Power (MVAr) from the WTGs.
- Interface between ESI SCADA and WTG SCADA/WFPC for power control of the WTGs in the Wind Farm.
- ESI SCADA HMI systems including operator and engineering workstation remote monitoring and control of the wind farm electrical system infrastructure, including remote monitoring and control of OSS SUS.
- WTG SCADA HMI systems including operator and engineering workstation for remote monitoring and control of the WTGs including remotely controlled medium voltage breaker at 690V side of WTG transformer, if poss. This to be further detailed in FEED.
- Interface to Information Management System (IMS) for data acquisition from the above systems.
- Interface to TSO for inter-tripping, monitoring and metering.
- Interface to Settlement metering Agency/operation.
- Interface to Condition Monitoring System (CMS), including WTG Main Bearing CMS system.
- Interface to cable monitoring systems, such as Distributed Temperature Sensing (DTS) and similar.
- Interface to telecommunication systems (WTG WAN, Wifi, Telephony system, TMS, CCTV, Met-Ocean, GPS Clock system, Access Control, Intruder system, PVTS, radio and /radar systems).
- Interface to top level SCADA
- TCP/IP based interface to WTG Contractors Navigation and aviation aid system (Sabik)
- Interface to WTG Contractors Fleet leader systems (SiDAC in Baltyk) on two WTGs.

3.3. High Voltage Control and Protection system

A dedicated and redundant PRP control and protection network utilizing the IEC 61850 protocol for the control & protection shall be established. IEDs for control and monitoring function shall be implemented. Control & Protection systems and related equipment's shall support PRP network, IEC61850 MMS and GOOSE communication.

400/220/66kV switchboard and LV transformer incomers shall be connected to the IEC61850 network for control and protection. The local control units (LCU) and protection relays/IEDs shall be integrated to the SCADA system via agreed interface/communication protocol. IEC 61850 GOOSE shall be used for intertrip and permissive signals, hardwired interlocks/intertrips shall be limited to what is strictly necessary.

Local Control Units (LCU) shall provide fully integrated monitoring functions of all 400/220/66 kV switchgear within the wind farm, e.g., circuit breaker, disconnector, earth switch, 3-pos-switch, etc. The LCU shall allow the operator to control switchgear locally at the relay or remotely from the SCADA.

Protection relays provide fully integrated protection functions of all 400/220/66 kV circuits within the wind farm. The protection relays also provide monitoring and control functionality for all the WTG 66 kV switchgear. These shall be controlled from the ESI SCADA system.

Required inter tripping signals shall be included for tripping of the circuit breakers for stop of the production and protection of equipment and export cable including soft stop and/or Hard stop of the WTG's/400kV grid circuit breakers in compliance with TSO Operational Tripping Schemes (OTS).

Arming, disarming and reset functions shall be included from the ESI SCADA HMI, according to TSO.

All required HW, SW and functions shall be included for local and remote maintenance access, diagnostic, trouble shooting and SW updating via the Company secure access solution. The foregoing is applicable for all programmable and configurable equipment. Contractor to ensure all Sub Suppliers meet this requirement.

3.4. Power Control, Topologies and Grid Compliance

The three main parts of the "power supply chain" in are;

- The WTGs – the offshore wind turbines and the cables between the WTGs and the OSS.
- The transmission system - consisting of the OSS, ONS, HV cables between the two, and the interconnection to the grid
- The grid – TSO receiving the power from . This is owned by an external party; Company does therefore not have any control over the grid. The IACS shall comply with the TSO Manuals, such that grid-related control and status signals can be sent and received. Fiscal metering must also be incorporated.

For these three parties to work efficiently together, it is necessary to exchange some crucial information and act in a timely manner based on the information. The main objectives are to

1) Align power production with the demand,
2) Handle de-loading and inter-tripping efficiently and reliably, and finally,
3) Ensure the technical integrity of the wind farm is not compromised.

The power control requirements will be described in the Power System Philosophy and shall be basis for the Power Control philosophy and design.

Power Control
From the grid there is a requirement to not provide more active power (MW) at any given time than the grid can handle. Normally the grid can handle full production, but during maintenance of power lines onshore and high amount of wind a need to limit the active power produced may be informed by the TSO.
To ensure grid compliance the reactive power control shall use voltage and reactive power reference at POI. The reactive power support requirement is specified in the grid code and the system shall be designed accordingly. TSO may, in special operation scenarios, specify how reactive power shall be controlled, by providing a reference value for voltage, reactive power or power factor at POI. The Power Control system shall be suited for different power control modes to enable input from TSO and manual input of set points. The concept for reactive power control shall be in line with the Projects Grid Connection Conditions and shall be agreed with the TSO.

De-load and inter-tripping; Under certain operational scenarios the grid owner may need to rapidly reduce the power production from the wind farm. In this situation the wind farm must be able to efficiently and reliably de-load as required by the grid owner. Should the required de-loading not be executed sufficiently fast, a trip shall be initiated according to a pre-defined inter-tripping scheme agreed with TSO.

1) **Technical integrity;** During operation of the wind farm there will be a limited number of pre-defined operational scenarios, sometimes referred to as Configurations and Topologies. Configuration means a clearly defined combination of open and closed HV breakers, and thereby a defined set of transformers, reactors, and WTGs in operation. Different Configurations may require different needs of support from the WFPC units. Topology is a term used by the WTG Contractor for identifying scenarios where a sub-set of WTGs may be controlled by another WFPC

than then normal one. If for instance a transformer on the OSS is inoperable and a bus-tie breaker is closed to reroute power towards the grid on-shore, the power generated by a set of WTGs may now be routed in such a way that it is measured by another WFPC module than before. Such change of Topology required a Topology change sequency to be performed before resuming operation to inform the WFPC about the change in WTGs under its measurement and control.

For some pre-defined scenarios there can be limitations to permitted power production to prevent overloading components (e.g., cables & transformers). Rerouting power by opening and closing of HV breakers in the system often means changing from one Topology or Configuration to another. A Topology Change procedure must be developed for the project since it involves informing the WFPC system about which WTGs are under which WFPC units' control. The procedure shall define the necessary steps to be performed by operators in ESI Scada HMI, and for a given topology the system may be permitted only to change to a few other topologies, e.g., if the operator attempts to change to a topology for which there is insufficient capacity in transformers or export cables, they will be warned that this is an invalid topology.

These three functions are implemented in a common interface where the ESI Power Controller (EPC) and the Wind Farm Power Controllers (WFPC) are the main units at the side. The number and location of the EPCs and WFPCs necessary to implement reliable, maintainable, and safe solutions shall be assessed as part of the overall system design.

Figure 2 gives a high-level overview of the functional split between the different controllers, as well as the signals exchanged between them.

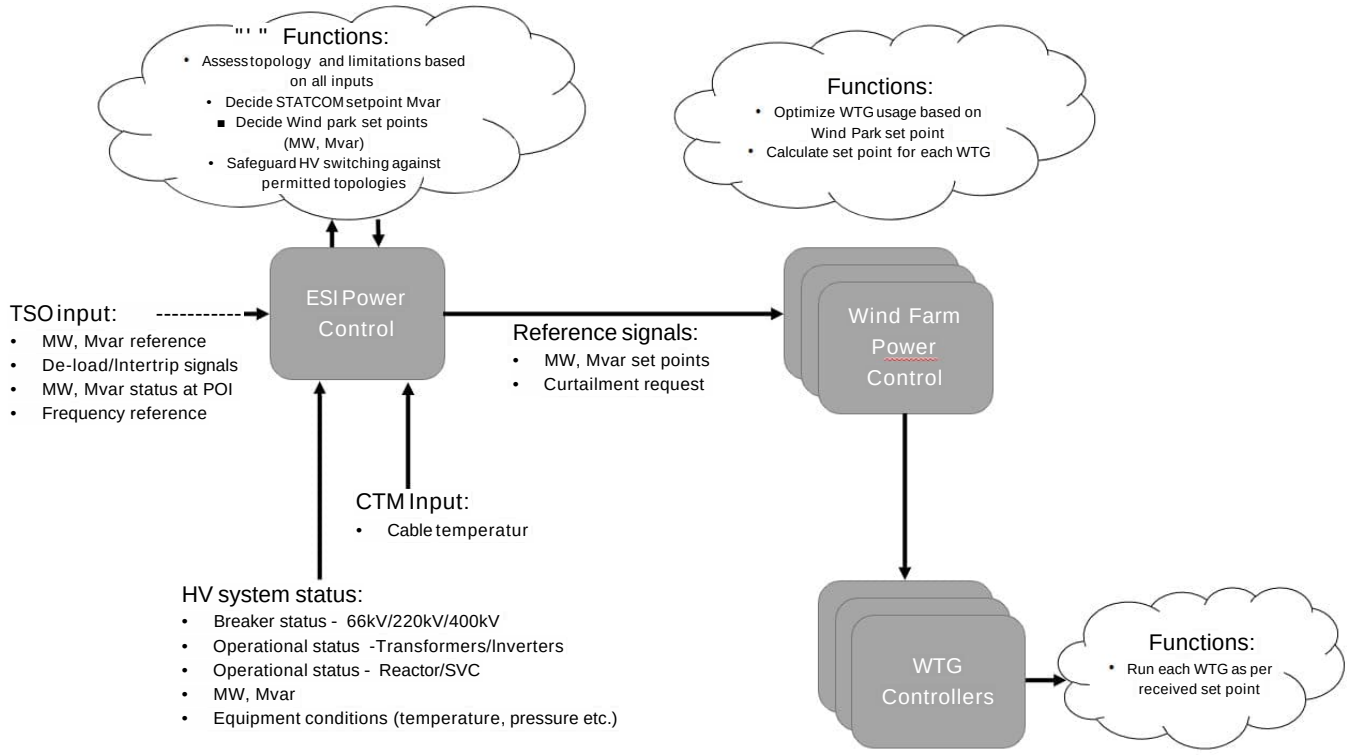

Figure 2 Power Control, Interlocks and Grid Compliance. ESI Power control to be delivered by ESI contractor. WFPC and WTG controllers are WTG delivery.

The purpose of EPC is to receive external information from the TSO, in addition to information from within the Wind Farm. The information is typically MW, MVAr references, de-load/intertrip requests and so on from the TSO, as well as HV breaker status, transformer/reactor status, power production and export cable temperature from within the Wind Farm. Based on this information the EPC shall determine the optimized power production. The other main task for the EPC is to maintain an overview of the current topology based on the current status of all relevant equipment.

The purpose of the WFPC is to adjust the Wind Farm power production according to the demand dictated by TSO, and within the limits dictated by the ESI Power Controller. Based on the set points received from the ESI Power Controller, the WFPC shall give set points to each WTG in operation to meet the overall requirement for MW and MVAr while still adhering to the limitations.

Further details of the different controllers and interfaces are described in the following sections.

A separate Power Control system philosophy describing the required topologies, tripping schemes and interfaces between the ESI SCADA, the WFPC and TSO for Grid Compliance shall be developed. Also, Power Control functional drawing and equipment scope drawing showing the entire windfarm shall be made, by collecting input from TSO, WTG and OSS.

3.4.1. Wind Farm Power control

The Wind Farm Power Controller (WFPC) shall be installed by the WTG supplier for control of the reactive and active power from the WTG's. For SGRE WFPC is normally referred to as High Performance Park Pilot (HPPP).

The WFPC shall be able to receive various active power limiting "runback signals" from the Wind Farm Electrical System Infrastructure, e.g., bus tie circuit breaker position indication, external run back signals from grid operator, fault indications on transformer breakers etc. and take action by reducing total wind farm power output according to the new condition in the wind farm. The runback signal with the lowest power limiting shall have priority over runback signals with less reduction in allowable power production.

The intertrip/ run back signals from TSO control centre shall have duplicated communication routes between the POI and ONS. TSO intertrip shall have priority above all other intertrip signals, as long as the isolation of a fault is according to relevant electrical system studies, to ensure the safest intertrip scheme for every fault cause and location. This will be specified in the Power System Philosophy.

To perform required power control the interface signals per WFPC /Balancing mechanism units (BMU) must be included, such as: MW and MVAr references, MW measurements, MW and MVAr Set point, MW production, MW at Grid entry point, De-load request, Breaker configuration/constellation, and voltage measurements to be included and presented on the ESI SCADA HMI.

Required Trip and De-load signals shall be included as defined by TSO requirements.

It is the responsibility of the Contractor to coordinate the WFPC settings with the ESI system so that the overall integrity of the power system is not degraded. The WFPC shall have functionality supporting the different possible operating modes of the WTGs

A Function design document, equipment scope and cause and effect scheme shall be developed showing all exchanging signals with ESI SCADA.

3.4.2. Grid Code Compliance

The wind farm shall be designed to operate and be energized under different operation scenarios without overloading the plant.

Required functions, logic, interlocks, control of the different breaker positions/constellation, topologies and operation limits shall be included to maintain the active power and reactive power needed within defined limits to ensure the primary plant is not overloaded and the compliance to the grid code is met.

To fulfil this requirement a dedicated ESI Power Controller (EPC), for single point of contact with the WTG WFPC, shall be included for handling automatic verification of different topologies for the "Grid Code" Compliance towards TSO. Required

topologies/logic, trip, and de-load signals (Soft stop), breakers status and control signals (MW, MVAr setpoints) shall be implemented between the EPC and the WFPC. Alternatives to a PLC-based implementation may be accepted by Company provided it can be documented that reliability, maintainability and uptime is comparable to the PLC.

The purpose of the EPC is to automate the response regarding power flow in each export cable dependent on a set of operational modes, scenarios (contingencies) and topologies/breaker constellations for the ONS and OSS.

- The functionality to be implemented in the EPC for grid code compliance will be described in the Power System Philosophy, and shall be followed. The main functionality shall be:
  - Power limitation dependent of operating scenario and a defined set of power limitation inputs (onshore/offshore)
  - Reactive power setpoint as a function of active power output and operational scenario.

Modes of operation and limitation scenarios shall be included. The below table indicate some examples, based on previous experience. It is the responsibility of the Contractor to develop the required modes for operation and limitations scenarios applicable to according to the project specific Power System Philosophy.

Configuration	Scenario
A	Normal operation
B	Loss of one 66kV WTG string/feeder
C	Loss of one 66 kV SWB
D	Loss of one OSS 220/66 kV transformer
E	Loss of one 220 kV export cable
F	Loss of one ONS 400/220 kV transformer
G	Loss of any reactive compensation or filter unit

Table 1

The wind farm may be energized to operate under any of the above configurations by the operating personnel.

Depending on the configuration, the active power and reactive power needs to be maintained within defined limits to ensure the primary plant and component limits are not exceeded and the agreed compliance for the specific scenario to the grid code is met. To meet this functionality the required topologies and logic shall be implemented in dedicated controllers – the EPC and WFPC.

3.4.3. ESI Power Controller

The ESI Power Controller shall include all relevant functionality to comply with the Power System Philosophy. It will include, but not limited to, the following:

- Receive WTG 66kV switchgear configuration information from the IEDs monitoring the WTG 66kV switchgears.
- Receive offshore 66 kV switchgear configuration information from the IEDs monitoring the switchgear.
- Receive onshore 220 kV switchgear status information, receive necessary measurements from WTG and ESI SCADA.
- Use reactive power controller at POI to give feedback to STATCOM to ensure the voltage and reactive power delivered is within the given limits in the Grid Code.
- Use active power controller at POI to give feedback to the WTG production to ensure the frequency and active power delivered is within the given limits in the Grid Code.
- Use the WTG and offshore 66 kV circuit breaker configuration and onshore 220 kV switchgear status information and measurements to provide the MW and MVAr set points to WFPC to ensure optimized compensation of the 220kV export cables.
- Utilise the CTS/DRS/DTS information to reduce the loading on the export cable when required.
- Detect and prevent invalid topologies and fault operation.
- Raise an alarm and/or initiate interlocks if the operator prepares to run the wind farm into a configuration which is not permitted.

- Raise alarm and suggest a safe reconfiguration of the network in case an EAT (including 66kV earth reference point) at OSS is lost
- Either automatically and/or manually from the O&M Base CCR execute de-loading of the wind farm, based on instruction from TSO.
- Either automatically and/or manually curtail the MW output of the wind farm if required.
- Raise an alarm, de-load and/or trip if the overall control interface fails.
- One push button energization sequence for the wind farm (ONS-OSS-WTG), including relevant time delay for the sequence to energizing the WTG transformers.

The wind farm MW and MVAr at the 66 kV or 220kV side offshore is handled via WFPCs which shall be interfaced to the EPC by means of a WFPC PLC to achieve the above aims of the overall control interface. The number and electrical placement of the WFPC controllers shall be evaluated during ESON FEED based on Grid code requirements, regulations related to need Balancing Mechanism Units (as in the United Kingdom or Polish equivalent) and subsidy CfD rules.

De-load/tripping signals/Request from TSO.

The need and method for de-load and tripping signals or requests shall be agreed with the TSO through workshops. The functionality must be in accordance with all grid code requirements for different operating modes and with the Power System Philosophy. TSO requirements to signal interfaces must be clarified through FEED.

Redundancy and Failure
A fault function will need to be included to detect any problems caused by the program logic execution or interface/communication fault.

- Failure of EPC shall raise an alarm to the ESI SCADA.
- Failure of WFPC shall raise an alarm to the ESI SCADA.
- Communication error between the EPC and WFPC shall raise an alarm to the ESI SCADA

Redundancy of the interface between ESI Power Control and WFPC shall be included.

3.4.4. Breakers/Disconnector Status information

The EPC and ESI SCADA shall receive breaker status information from the POI connection point, ONS, OSS and WTG 66kV switch gear. The short circuit levels are high in the WTG system. LV breakers on 690 V will most likely not be allowed manual operation of. Status and possible operation of all 690 V breaker is mandatory in WPS/ESI scada

3.4.5. Input from Cable monitoring systems

The DTS for both IAC and EC shall be integrated to the EPC for cable monitoring and power control to ensure cable integrity in all operational scenarios/configurations/topologies.

3.5. Communication between EPC and WFPC

For all information and interface signals described above, it shall be ensured that information is exchanged as direct as possible if the units communicating are connected to the same network. Firewall crossings shall be done at the lowest possible level. Communication and available network architecture shall be thoroughly assessed when hardware for implementation of EPC and WFPC functionality is considered. Horizontal communication shall be limited to the extent necessary.

3.6. Test facility

The IACS test facility shall accommodate testing of all changes to applications, configurations, and settings prior to implementation on the live system. Testing shall be performed without relying on any part of the operating IACS. Software simulators shall be utilized to emulate IACS components to the extent possible, hardware components shall be delivered for units where this is not possible. The test facility shall have necessary network connections to permit download of security patches and other software updates for test and connected to the company secure access solution for remote activities.

The test facility functionality shall include but not be limited to;

- One ESI SCADA Server
- One ESI SCADA Client
- Relevant auxiliary interface PLC(s)
- One IED of each type delivered
- One of each network component delivered
- WTG simulator

4. Cyber Security

IACS networks shall be designed according to reference standards and requirements document as described in Appendix E, which gives the framework for the design and specific requirements to the proposed solution. This design and requirements are based on IEC62443. This includes, but are not limited to, zoning and conduits, firewall requirements, OS patching, malware, and antivirus protection. All systems delivered (including subsystems) shall be assessed, designed, implemented, and documented according to the requirements and guidance in these frameworks and requirements, including (dependent on project phase):

- Network, Security Zones and Conduit drawings shall be made by Contractor. The template for the drawing shall be provided by Employer.
- The Zones and Conduit drawing shall contain Security Level-Targets substantively following the processes as set out by IEC62443-3-3:2019. The SL-Ts will be based on the Reference Architecture Model in IEC62443-3-3:2019 and the SL-Ts shown therein and documented as a part of the topology drawing agreed between Company and Contractors/Suppliers
- Cyber Security tests shall be a part of the Contractors and Suppliers' FAT procedure and report
- The Contractor shall conduct a detailed Cyber Security Risk and Vulnerability Assessment. A Detailed Risk and Vulnerability Assessment report shall be provided to Company. The assessment should follow the processes defined in IEC 62443-3-2
- Create backups and test the backup and recovery procedures.
- Antivirus and patch management procedures shall be described. All systems, servers and clients shall be tested to ensure that required antivirus and security OS patches are installed.
- The Contractor shall make procedures and strategies for hardware, OS and software upgrades for all systems.

5. System Requirements

5.1. Hardware and Software

5.1.1. General

Each computer and Server on the technical and process network shall be kept up to date with security patches and virus protection software during project execution and at handover to Company. The system shall also be designed to enable patching and malware protection during normal operation.

All hardware and software shall when commissioning is complete have at least 10 years left before End of Life, i.e., before Support is no longer officially available from the Manufacturer. This shall be from the date when Contractor has completed his commissioning scope, as well as all assistance to Company during offshore commissioning.

The systems on the technical network shall have local access to a recovery backup. Recovery backup shall be performed after all software changes. The automated backup solution shall be able to hold minimum 10 previous backups.

The arrangement and configuration of servers and communication equipment shall be based on a redundancy philosophy. If any of the substation SCADA server / communication equipment fails, then a standby server shall take over, or communication shall be routed through another channel. Performance of the backup channel shall be equal to that of the primary communication channel.

5.1.2. System Software

The SCADA Logic Solvers/logic controllers shall be based on a true real-time operating system to achieve the necessary degree of security, reliability, and reduced maintenance, i.e., operating systems like Microsoft Windows are not allowed for Logic Solvers.

Process values shall be in engineering units throughout the system (engineering tools and run-time system).

When powered up after being powered down, the total IACS shall automatically restart, including all internal system communication mechanisms, without manual intervention. Power-up shall not cause spurious activation of outputs. Restart shall take less than 10 minutes.

Configuration changes to the logic solvers/IEDs shall be persistent, such that the configuration is not affected by power loss and restart.

All system software changes shall be recorded in defined system for logging changes visible (auditable and unalterable log) to Company.

There shall be facilities for read-out of current versions of all system software and firmware, including logic solvers, control and protection devices, I/O cards, servers, and operator stations.

The IACS software tools shall be available through Company Secure access solution.

The software tools shall be available from a central management server and/or from the engineering-/maintenance workplace.

Software should allow for a central management server to apply all updates, modifications, patches, etc from a single location. This should be accessible via Company Secure access solution.

If several engineering stations are used, then the SCADA shall have means of preventing online configuration conflicts.
SCADA applications and system performance shall not be influenced by utilization of engineering tools.

The system shall be self-documenting including both suppliers' standard application blocks and project specified application blocks. The documentation shall be "as programmed" in the executing SCADA logic solvers, servers, and Control and protection unit/devices.

It shall be possible to document the application program directly from the system including utility systems, Control and Protection devices and IED's and make it available as a graphical report. In special cases, program listings can be accepted based on Company preapproval. An automatic cross reference between graphical report interconnections shall be included.

There shall be a tool for automatic read-back of the current online parameters and comparison with the engineering master. It shall be possible to perform an update of the master configuration files for all or for selected parameters. This tool shall

provide a report showing the parameter differences. In the case of deviations these shall be reported as maintenance alarms/advisories, not to the main operator alarm list.

5.1.3. PC's/Servers and client applications and software tools

There shall be admin/management tools for remote monitoring and management for the system. The system shall send diagnostic information in case of failure. The information shall be available in the admin/management tools to address problems rapidly and take corrective actions.

Servers / clients shall all be supplied with both Administrator and Operator logins

The system shall have role-based security to prevent unauthorized access to functionality.
Any thick client Application shall support 64-bit client Operating System, e.g., Windows 10.

The system server application shall support Windows Server 2019 or newer.
Unless system servers have need for special interfaces that prevents virtualization, servers shall be provided with VMWare Workstation Pro 14 (or newer) Virtualization software.

5.1.4. Back-up

Required back-up solution shall be provided to be able to perform automatic and regular back-up of the SCADA and subsystems software including Network, HMI, and engineering workstation.

For any backup media used by the backup / recovery solution, it shall be possible to store the backup media in a separate location (either on a physical backup media, or by file transfer to a Company server).

A backup and recovery solution shall be included, covering all equipment with software, configuration settings and other data needed to recover the system to resume normal operation.

5.1.5. System Hardware

The IACS shall be distributed and designed to be self-contained (autonomous)

SCADA servers and Logic devices/Logic Solvers hardware shall be unified, i.e., a limited number of hardware types shall be used to ease maintenance and spare part handling. It shall be possible to replace redundant components in SCADA during normal operation of the system, without any loss of functionality or production.

Any SCADA unit shall be able to survive loss of power for an indefinite period without irrecoverable loss of application programs, configuration or parameters which have been set by the user/operator.

Approximate recovery time for each SCADA unit shall be documented and verified.

Electrically powered devices shall comply with relevant test limits and performance criteria in EN 61326 or IEC 61000-6-2 and IEC 61000-6-4 with respect to electromagnetic emission and immunity in an industrial environment.

Company assigned IP addresses shall be used for all systems. Note that IP addresses shall not be openly displayed on the HMI or in system documentation.

5.1.6. Time synchronization

To ensure network time synchronization and provide coordinated time stamping for alarms and events, between all IACS system units, electrical, instrumentation and telecommunications systems, a common and reliable NTP, or better, time server (real-time clock) shall be used.
The time server shall receive Network Time Protocol (NTP) coordinated universal time (Universal Time Coordinated (UTC)) or better from the telecommunication system real-time clock (RTC) and distribute the time to other system equipment including networked field devices.
If possible, the RTC shall be a common clock used for telecom, IACS, electro and Control & Protection equipment, to avoid multiple sets of GPS antennas on the facility.

Contractor shall ensure all relevant components receive the UTC time and maintain correct time. This is applicable to all components connected to a network.

The time server shall be equipped with 10/100Mbit/s outputs, in an RJ45 format, for direct connection to the SCADA backbone, technical network and other consumers. Instrumentation, telecommunication systems shall request NTP (Network Time Protocol) (or better) information from the time server for time synchronization.

The SCADA shall be capable of providing a time synchronization signal to IEDs via IEC 61850 protocol to ensure all events are time stamped.

The HMI shall have the possibility of enabling daylight saving summertime (Wintertime + 1 hour) including alarm list.

5.1.7. Time stamping

All events, process and system alarms shall be time stamped in order to identify the correct sequence of events. Time stamping should be performed by the SCADA units, and the accuracy of the time stamping shall be according to the defined cycle time. Timestamps shall use UTC.

Independent of configuration and number SCADA control devices/units, the protection alarms in SCADA, control and protection equipment and all sub-systems shall be time stamped with the accuracy of 10 ms, or better, relative to when they physically appear.

All IO values in the system shall include Quality and Timestamp (VQT). VQT shall be propagated throughout the system, from the IO device (e.g., IED or PLC) through to the HMI and IMS.

Timestamps shall be in UTC.

The quality code shall be an industry standard. Company’s preference is the OPC UA quality codes.

5.1.8. Manufacture requirements

All SCADA hardware modules shall have been tested in accordance with recognised industrial standards regarding susceptibility to environmental conditions such as:
1. Variations in signal and supply voltages
2. Electrostatic and electromagnetic noise
3. Temperature and humidity
4. Vibration and mechanical stress

Test certificates specifying the tests conducted and the results obtained shall be available.
For components which are critical or particularly susceptible to the conditions encountered on the specific site of installation, more comprehensive tests may be required.

5.1.9. Availability and redundancy requirements

IACS failure shall in general not cause a production loss. This includes all components in the SCADA system.

In addition, Mean Time Between Failure (MTBF) and Mean Time to Repair (MTTR) figures shall be documented and calculations of overall IACS availability shall be performed. The overall system availability requirement is set to 99,5%, the IACS shall be designed such as it will not contribute to a lower total availability than 99,5%.
No single IACS failure shall have the effect to disrupt the process.

Design of safety instrumented functions shall be based on the Safety Requirement Specification developed on basis of the Hazard and Risk analysis.

Redundancy shall be evaluated based on the following:
1. Production availability requirements
2. Consequence classification
3. Operational criticality
4. Modification requirements, like online configuration

5.1.10. SCADA servers and operator stations

The following requirements apply:

- Servers shall be of the same hardware product family, i.e., software and hardware compatible
- Operator station clients shall be of the same hardware family, i.e., software and hardware compatible
- Servers and operator station clients shall be of fit for industrial use preferably rack or rail mounted type
- Servers disk storage shall be fault tolerant and with automatic online recovery when replacing a disk
- Servers shall be rack mounted with one common maintenance terminal (VDU, keyboard, mouse) per cabinet
- Clients shall be connected to different network switches to obtain robustness with respect to switch failure
- Servers shall be redundant and connected to both redundant networks and shall handle automatic switchover between the networks. If a client/server architecture is used for SCADA OS, no HMI screen shall lose its functionality because of failure of a single server.
- Servers and operator stations shall be suited for continuous 24/7 operation
- All servers and operator stations shall be provided with hot swappable disks

Computers for CCR Operator Stations located outside CCR shall be rack or rail mounted. Connections to VDUs/keyboards/mice in the CCR shall be by individually wired connections, e.g., Keyboard, Video, Mouse (KVM) extenders or networked KVM solution. Operator stations and servers shall fulfil requirements to limitation of noise in the rooms where they are located.

Rack type of server and PC shall be used. No tower type of servers and client workstation/PC is allowed. Mini desk type client workstation may be used upon company acceptance.

5.1.11. Data archiving

The SCADA system servers shall be capable of storing analogue data with an update rate of 0.25 second (4Hz) and shall support alarm and events timestamped with a resolution of 1ms. The SCADA system shall be able to display real time data, raw data, and historical data. It shall be possible to configure automatic transfer of data from the database servers to Company IMS via e.g., OPC XML, OPC-UA, OPC UA/DA, OPC HDA/ODBC/SQL. OPC UA is preferred.

Short time data shall be possible to store for at least 30 days.

Database storage with RAID 0+1 striping is preferred.

The different database servers such as OPC, ODBC etc shall have required direct interface to Company IMS.

5.1.12. Monitoring

All units on the IACS network, including network components and IEDs shall be monitored and detected fault or malfunction shall be alarmed. IACS unit, fault type and card (if relevant) shall as a minimum be referenced in the alarm text.

5.1.13. Application configuration

Programming for logic solvers shall comply with IEC 61131-3 Function Block Diagram, Sequential Function Chart and
Structured Text. Structured Text shall be used for function block coding only.

It shall be possible to configure SCADA and Logic Solver applications semi automatically, as well as manually, utilising different configuration levels and libraries of function blocks and templates (ref. section 9.5) to maintain the consistent use and quality throughout the configuration. The use of a central management server shall be considered for maintenance of SCADA software and libraries.

SCADA and Logic Solver functionality shall support application configuration on the following levels:
1. Function blocks
2. Templates

Application configuration shall be based upon the application blocks as well as elementary function blocks like AND, OR, logical inversion, RS latches, pulses, timers, etc.

The application blocks shall be coded with version control, and the application block version shall be visible in the application.

Function blocks cycle times shall be documented. Order of execution of the function blocks shall be editable and visible.

It shall be possible to collect the function blocks and their interconnections in a typical control structure and instantiate it as a “template.” When an object is deleted or altered in a template, a warning shall be given. All function blocks shall be shown at the instance of the template.

5.2. Human Machine Interface (HMI)

5.2.1. General requirements

TR4036 “SCADA Operator Station HMI” should be the basis for development of an HMI philosophy.
The Project will have two SCADA systems, one dedicated to the WTGs, referred to as WTG SCADA, and one dedicated to the ESI (power distribution systems and utilities) referred to as the ESI SCADA. There shall be some exchange of information between the two, but they will not be fully integrated. The ESI SCADA and WTG SCADA system shall include all necessary HMI, operator, engineering, and service workstations for remote monitoring and control. The SCADA operator station represents the main HMI between the operator and the electrical distribution and utility facilities.

The HMI solution shall include equipment and functionality for Large Screen solution. Dedicated mimics shall be developed for the Large Screen Display solution to ensure correct information as well as level of detail and readability is ensured.

An HMI philosophy detailing the HMI functionality shall be developed during detail design. The philosophy shall cover HMI solutions, alarm, and trend solutions as well as the Large Screen Display solution, and any other functionality foreseen to be covered from the Operator Stations.

The HMI (Human Machine Interface) for all systems in the control room shall be built to a common standard/philosophy, as agreed with Company. This HMI standard shall include:

- Consistent use of colours, layout, and sounds
- Consistent screen navigation and functions, for example:
  - One-click alarm acknowledgement
  - One-click navigation from alarm summary to associated HMI display
- Clear indication of the relevant wind farm and plant area/system

Required HMI/Operator Workstations shall be available at the CCR in O&M Base situated in Leba, on the OSS and ONS.

Engineering workstations shall be installed at ONS/OSS and remotely accessed from CCR and Company secure access solution.

From the engineering workstation, it shall be possible to perform maintenance, troubleshooting, without any interference with the monitoring and control of the process.

Use of symbols and colours for operator interface shall be consistent throughout. Tagging of alarms and events for the local operator interfaces, shall be consistent and harmonized with the WTG Supplier Wind Power workstation.

In line with the agreed HMI philosophy, the IACS and SCADA HMI shall have required functionality and interface for viewing and selection of all SCADA HMI mimics, alarm and events, IMS information, CCTV (Closed circuit television) information/mimics, Intruder information/mimics.

5.2.2. HMI Displays

The layout of the HMI displays shall be function-oriented and based on Single Line Diagrams, Key Line diagram, SCADA Topology Drawings, Fire Detection Layouts, Area Layout drawings, P&ID, etc. The display shall enable the operator to monitor and control ESI electrical and utility section functions. Where interfaces and interaction with TSO is needed, the symbols and naming shall be the same as TSO to avoid misunderstandings.

WTG displays shall enable monitoring and control of relevant WTG functions.

The electrical and utility detail display shall contain all electrical process-related variables and control functions for each section.

The HMI display for the electrical system shall be split into different HV and LV electrical main and sub levels, including but not limited to Generator, UPS system, and utility process sub level displays. In addition, there shall be separate displays for all utility systems, including but not limited to;

- Fire Detection
- Fire Fighting
- Gas Detection
- HVAC
- Intruder Detection

- Condition Monitoring

The use of colours shall be fully based on applicable standard for similar offshore wind projects and agreed with Company. TR4036 should be used as guideline. There shall be a clear distinction between dynamic symbols and static symbols on the displays.

The operator shall be able to select the corresponding trend displays from the process detail display. All signals shall have trend facility with adjustable time and range span.

The HMI system shall be object based.
From the object faceplate, it shall be possible to:

- Operate the equipment. All commands that will change the state of the equipment (e.g., Open, Close) shall require confirmation. No more than one level of confirmation is required.
- View any current interlocks on the equipment, and the origin of these interlocks
- View any current alarms on the equipment
- View the current quality and timestamps, including timestamp of last good value
- Acknowledge alarms
- Manage alarms (see section 5.2.4)
- View/modify operator notes

The HMI system shall include the following functionality:

- Operator notes/comments. It shall be possible to associate operator notes with any HMI object (e.g. circuit breaker, disconnector, earth switch). A symbol next to the object shall indicate that there is an active operator note. Operator notes shall be timestamped and shall record the name of the operator as well as the actual text entered. The contents of the operator notes shall be logged on the SCADA server and retrievable via the report system.

The HMI displays shall be based on recognized standards, such as the following:

- ISA 101, Human-Machine Interfaces
- EEMUA 201, edition 3

The use of static text shall be minimized. Branding (the inclusion of the supplier's name or logo within the HMI) is not permitted.

Bad-value representation: HMI displays shall normally display the current value of the IO tag. In the event of bad or uncertain quality, this shall be clearly indicated on the HMI. The last good value shall be shown on the HMI. It shall be possible to see the timestamp of the last good value, for example in the object faceplate.

5.2.3. Integration of OSS SUS

Control and monitoring of OSS systems at the CCR shall be through the ESI SCADA, not a separate OSS HMI. OSS SUS shall be integrated in the ESI SCADA to allow supervisory control, monitoring and alarm handling of OSS SUS and the related sub-systems noted in Section 3.2.1.

HMI summary screens from the OSS SUS shall be reproduced in the ESI SCADA including supervisory control functionality. Alarm and event handling shall be per Section 5.2.5. Remote troubleshooting of OSS SUS or subsystems shall be possible using engineering workstations at the CCR; Contractor and OSS Contractor shall coordinate on automation and telecoms system design to allow this remote accessibility.

ESI SCADA integration with OSS systems and end devices shall include:

- Hardwired interfaces to OSS lighting controls as noted in OSS Specification.

- Hardwired interfaces to LV switchgear and Standby Diesel Generator (SDG) for trip commands: main and generator breaker trips, diesel generator unit trip.
- Hardwired interfaces to LV switchgear, UPS, and SDG for key status points: main and generator breaker status, UPS common alarm contact, other key status points at ~4-5 per device.
- Hardwired interfaces for any OSS safety-related functions executed by ESI-SCADA. Above-noted LV main breaker and SDG trips are examples of this.
- Hardwired or soft interfaces to Motor MCB's that are controllable directly by ESI SCADA. Interface method is to be agreed with OSS Contractor.
- Soft interfaces to LV switchgear, MCC's, UPS and SDG for the remainder of SCADA functionality for electrical systems. This could be a combination of direct interfaces with the end devices or through the OSS SUS.
- Soft interfaces to protective relays for integration into P&C networks (e.g., IEC 61850).
- Hardwired interfaces to sub-panel breaker status as noted in OSS specification.
- ESI SCADA interfacing with non-electrical OSS systems, e.g., HVAC and F&G, shall be through soft link with OSS SUS except as noted above.

Hardwired interface method including typical loop configurations are to be agreed with OSS Contractor. Interposing relays, where required, shall be provided by OSS Contractor.

5.2.4. Integration of HMI from WTG SCADA

To ease the workload for the operators in CCR, several HMI components from WTG SCADA shall be displayed in ESI SCADA as a minimum the following functionality and information shall be induced:

1. A Wind Farm overview picture showing total power production parameters, individual WTG power production and status
2. HMI picture(s) for display and setting of all relevant setpoints for Wind Farm Power Control from ESI Power controller
3. All WTG SCADA alarms shall be shown in a common alarm list with ESI, including alarm management
4. Functionality for starting and stopping of individual WTGs and strings.

Details for necessary data exchange, protocols etc shall be agreed with WTG Contractor through interface management.

5.2.5. Alarm and events

There shall be a common (centralized) alarm facility in the CCR localized in the O&M Base at Leba, where alarms from all systems e.g., CCTV, ESI SCADA, OSS SUS, WTG, Fire Detection etc, can be collected, displayed, and acknowledged.

The main objectives of an alarm system are:
- To warn the operator about a situation that is undesirable or unsafe
- To serve as an event log

The alarm lists, status lists and event log shall be updated dynamically. The alarms shall be listed in chronological order and be time-stamped in the unit that first registered the alarm. The latest alarm/status/event shall be presented at the top of the list. All lists shall be available from all operators stations and on the Large Screen solution.

It shall be possible to navigate from the alarm list to the process page that shows the alarm. This shall be done with only one operator command.

Alarms shall be prioritized to guide the operator in his decision to select which alarm/abnormal situation to handle.

Alarms shall be prioritized according to the severity of consequences that could be avoided by corrective actions and the time available for successful corrective operator action.

Alarm management capabilities (e.g., the ability to filter, block, suppress, handle nuisance alarms, sort or re-prioritize) shall be provided.

A common alarm prioritisation scheme shall be used, approved by Company prior to implementation. At least 4 priorities shall be supported. It shall be possible to direct certain alarm priorities to different users.

The alarms shall be presented with text, colours, symbols, and sound, clearly differentiated from other information.

Alarm description shall be understandable and self-explanatory for the operation.

The operator shall be alerted by means of audible and visual indication. The alarm shall present information defining the problem e.g., descriptive alarm text in alarm lists and change in graphic displays on operator stations.

Each tag/alarm should have an associated free-text comment field available for use by the operator.

The operator shall be allowed to sort and filter lists.

Alarm and event shall be in separate lists on SCADA HMI.

The system shall include the following alarm/event categories:

- Action alarms (Trip)
- Pre-alarms (warnings)
- Fault alarms (instrument, equipment, or system)
- Events

Alarm implies an audible alarm requiring acknowledgement by the operator. Before acknowledgement, the object shall be flashing. When acknowledged, the object is shown with steady light. An acknowledged alarm shall reflect the abnormal process condition until the process variable has returned to normal state.

A common sounder system shall be implemented to avoid multiple sounders simultaneously sounding and causing confusion.

Event requires neither audible alarm nor acknowledgement by the operator. When applicable, events shall result in a visual change of state on the associated dynamic symbol.

Alarms and events shall be reported on separate summaries and recorded on disk. Options shall exist to recall alarms/events on search criteria like time, tag, process section, event type, etc. Suppressed alarms are not logged.

Alarm list

The following information shall be available for each alarm / status:

1. Priority*
2. Acknowledged/unacknowledged status*
3. Alarm/State status (i.e., Active / passive)
4. Tag name
5. Tag service description
6. Alarm type (i.e., HH) *
7. Current value, violated limit, Eng. Unit.
8. Timestamp (Date and time alarm/status was generated)
9. Area (Physical area or part of plant, process, or unit, if system alarm indicate system part)**

10. Operator alarm comment**
* Alarms only
** Available on demand (e.g., tool tip, right click, mouse click etc.)

Statistical performance analysis of the alarm system shall be possible, using standard recommendations such as:
- Alarm rates (e.g., alarms per 10 minutes)
- Alarm priority distributions
- Number of active / standing alarms

Event list
The event log shall be available for the operator on the operator station and shall also be transferred to an external database for long term storage.
Actual events that should be logged:
- All alarms
- All operator intervention / commands
- All automatic discrete actions
- Blocking, suppressing, override, hiding, shelving, contexts
- System alarms and messages
- Operator logon/logoff, if implemented

The alarms presented to the operator must be marked in the event log, to be able to perform alarm analysis.
To make it possible to search through the events, the events must be stored in a database indexed by tag number. The events shall be stored for at least 30 days and be available via the SCADA operator station.
Unnecessary events shall be avoided.

5.2.6. Alarm management system

An alarm management system tool shall be provided to enable tracing of any alarm to the applicable detail. The alarm management tool shall give the possibility to analyse the alarm re-occurrence, top-5 alarms, cause for the alarms and potential actions to be taken.

5.2.7. Blocking and suppression of alarms

The system shall have functionality to suppress signals both manually and by control logic.

1. It shall be possible to suppress individual alarms and pre-defined groups of tags.
2. The system shall provide facilities for reporting any blocking or suppression.

The system shall also enable the operator to trace where the blocking/suppression is active.

There must be a clear visual distinction of alarms suppressed or blocked by the operator on the SCADA HMI VDU displays (electrical overview displays as well as on any related detail display). Additionally, the system must be able to produce lists of all suppressed/blocked alarms on request.

Clear and easily visible instructions shall be posted in local language in the Local HMI.

Colours shall be used to draw attention to the various alarms. The colours used for alarms shall:
1. Be clearly different from other colours
2. Not be used for other purposes.

5.2.8. Trending

SCADA shall provide a facility for real time and historical trending for all binary and analogue variables, independent of the IMS. Real time trending shall be with the same time resolution as the cycle time of the application in the Logic solver.

Historical trending shall have user selectable sampling time, normally 1 second. Sampling time for selected values shall be possible from 100 ms. SCADA shall store relevant values for a minimum of 35 days for trending purposes.

5.3. Printing facilities

Print server functionality on the SCADA servers shall be included for printing of alarm and event list/reports, HMI mimic from all the Operator workstation via DMZ print server via Company secure access solution to a printer on the office network and to a SCADA local printer.

Failure of one operator station shall not prevent printer access.
Silent type of colour printers shall be used.

A printer shall be available at the CCR.

It shall be possible to generate printouts, e.g., screen dumps, list, reports from the SCADA engineering station.

Required printers shall be installed on the O&M Base CCR and ONS.

5.4. Safety system

A Safety system shall be installed for detection of abnormal conditions and to perform necessary action. Reference is made to safety strategies in Appendix E.

For the Safety system consists of minimum:
- Control & Protection System
- Fire Detection system
- Gas Detection system
- Fire Fighting System

Control & Protection system shall shut down necessary equipment during an fault situation, automatically or manually and remotely from the CCR.

The Fire Detection and Fire Fighting systems shall be integrated in the ESI SCADA system via agreed interface protocol.

5.4.1. Shutdown system

The purpose of the shutdown system is to prevent escalation of abnormal conditions into a major hazardous event and to limit the extent and duration of any such events that do occur.

The shutdown logic shall be implemented by use of Logic Solvers.

The probability of single defects / failures causing inadvertent trip actions shall be as low as reasonably possible, e.g., provide fault tolerance by means of automatic diagnostic features and redundancy according to cost-benefit assessment.

Safety system shall have facilities to allow for testing and maintenance without interrupting production or operation.

Safety system shall be in compliance with DNVGL-ST-0145.

Manual initiating of the different shutdown levels shall be possible from CCR via reliable connection to the ESD/Fire/safety logic solver.

5.4.2. Fire detection/Protection System

A Fire detection system for continuously monitoring of the fire status and execute safety related functions upon fire detection shall be installed. The fire detection system shall comply to applicable Polish standards as defined in appendix E requirements.

Aspiration smoke detection shall be used for areas not accessible in normal operation.

The control logic/Cause & effect for the ONS shall preferably be included by use of separate Logic Solvers but may also be included locally in the fire detection panel. Solution to be agreed upon.

The safety related parts of HVAC, such as closing of fire dampers and trip of fans and heaters, shall be part of the Fire Fighting system.

The Fire Detection system shall have the capability to handle addressable detectors either directly or interfaced through dedicated Fire detector panels via agreed interface protocol.

Silent testing shall be possible, i.e., for the functions being tested it shall be possible to disable audible alarm annunciation and also inhibit release of Fire Fighting agent.

All safety critical loops for the Fire Detection System shall be line monitored, enabling detection of abnormalities (e.g., earth fault detection, short circuit detection, open circuit detection in the entire circuits, etc.).

When powered up after being powered down, the total Fire system shall automatically restart itself, including all internal system communication mechanisms, without manual intervention. This also includes F detector interface centrals. Power-up shall not cause spurious activation of outputs.

All fire Detection Systems/Panels shall be powered from two independent UPS electrical sources.

The UPS shall offer 100 percent redundancy, such that loss of one power source shall not cause any malfunction within the system.

5.4.3. Gas detection

Gas detection may be provided in battery rooms for Hydrogen, and in switchgear rooms for SF6 leakage. Gas alarms shall be enunciated locally both inside and at the entrance to the electrical rooms. Gas alarms shall also be sent to the ESI SCADA system via robust industry standard protocol, to be decided during detailed design.

5.5. Heating, Ventilation and Air Conditioning (HVAC)

A control system for monitoring and control of HVAC system on ONS and OSS shall be implemented. The HVAC Control System shall be fully integrated in ESI SCADA for operation and monitoring. For chilled water system, supplier's local control system shall be used. System status and operation signals shall be transferred to ESI SCADA system for information.

Fire dampers shall be initiated from the Fire Detection system with damper position limit switches also connected to the Fire Detection system. The HVAC system including fire dampers, fans, instrumentation shall be shown on a separate HVAC HMI picture. Fire dampers shall be redundant to allow for periodic testing. Failure of a fire damper in closed position during testing shall not be critical for power production/affect platform operations. Design of fire dampers and control systems shall allow for remote testing, monitoring and recording of opening and closing times. If maximum limits for opening/closing times are exceeded, alarm shall be given.

The HVAC logical programmable logic devices/Logic Solvers should preferably be connected to the ESI SCADA system via OPC UA, IEC-104 protocol or by Profibus protocol. Use of Profibus shall be agreed upon.

All data from the HVAC control and monitoring system shall be available in the SCADA system servers/HMI.

All real time values, analogue data from the HVAC system shall be available to the IMS via agreed interface.

It shall be possible for remote connection to the HVAC Control system for diagnostic, troubleshooting and SW updating via Company Secure Access solution.

6. Network, communication, and Interface requirements

6.1.1. General requirements

Communication line between ONS and Company administrative network, O&M Base CCR and TSO operator, and between OSS and ONS, shall be redundant and through Multi-Protocol Label Switch with Transport Profile (MPLS-TP) infrastructure and it shall support routable communication protocols such as IEC104 and OPC UA. Interface requirements and capacity shall be as described in the Telecom Technical and functional requirements document C256-EQ-T-SP-00001.

A fiber optic network based on the fiber cores in electrical cables shall be established for control/monitoring and telecommunication purposes both for all WTGs and the OSS. The WTGs shall be connected to the OSS via fibers in the inter array subsea electrical cables.

Communication to shore shall be via redundant single mode fiber optics, G.652, as part of the subsea export cable. All communication to shore shall be equipment redundant i.e., if one link goes down, the communication shall automatically switch over to the other link. Communication between ONS and OSS as well as internal communications on substations shall be done by standard protocols e.g., TCP/IP, IEC104 and IEC 61850 through the MPLS-TP infrastructure.

All networks shall be monitored, and an alarm shall be raised in the ESI SCADA if any part of the network does not perform as expected to permit the first line maintenance to action the problem. In addition, the networks will be monitored by Company's specialist service during the operational phase, therefore some central network components shall be Company Provided Items to ensure monitoring systems already established can be used. Furthermore, to ensure the IACS networks are fully transparent to the monitoring system, also some network components further "down" in the system require Company approval. Close cooperation with Company's network specialist is required.

Some signalling may require full redundancy/different routing between ONS and OSS, according to Grid Connection Agreement, Grid Code and Technical Conditions for The Connection to The Telecommunication Network of PSE S.A. Agreement with TSO (App E), and the required communication systems shall be installed to fulfil this requirement.

6.1.2. Network hierarchy/topology

A typical Architecture model of Integrated Automation and Control system is shown in figure 1. Based on this an overall SCADA network hierarchy/topology drawing including all SCADA process network, technical network, and Company Wide Area Network (WAN) network structure shall be developed and detailed during detail engineering phase, including input from OSS, WTG, IT, TSO or others where relevant.

6.1.3. Network redundancy

Each SCADA network (ESI and WTG) shall be fully redundant, and a fail-safe philosophy shall be evaluated for critical signals. In case of communication failure, the system shall move to predefined state with regards to the severity of the failure, where the predefined state shall be defined in the fail-safe philosophy. The SCADA systems shall have robust and fault tolerant protocols for the dual redundant communication network and shall have intuitive alarms and diagnostics tools for the communication network.

The network shall include RSTP (Rapid Spanning Tree Protocol) functionality, with high priorities on the backbone switches to ensure an uninterruptible changeover if one part of the network fails

6.1.4. Network Segregation

There shall be a separate process critical data network for the control and monitoring system (process technical network) of all SCADA monitoring and control system. All equipment that needs to communicate together or to remote systems shall be connected via dedicated firewalls to technical network.

The following requirements shall apply:

1. The network infrastructure shall be divided into levels with clearly defined interfaces between these levels.
2. Firewalls shall be used to control network traffic between zones of different security levels. Traffic that is allowed to pass between zones shall be limited to what is necessary.
3. The Technical Network shall be implemented on dedicated switches, separate from (not shared with the administrative Network) the Company Corporate Network.
4. Integration endpoints shall be properly secured.
5. Communication between systems at a plant shall be implemented in a robust and secure way.
6. Data from the SCADA shall be made available at the office network and information security updates shall be made available for IACS. Secure remote access to resources shall apply.

6.1.5. Interface to IMS system

All SCADA systems and subsystems shall provide necessary gateways and interfaces to Company Information Management System (IMS). This interface shall be separate from other interfaces, e.g interface to a possible CCR/Top level SCADA.

The purpose of the IMS is to collect and store plant time stamped process values and discrete/alarm/event data for historic storage, and distribution to other user applications across the Company Network. The IMS collects data both from SCADA and non-SCADA data sources and shall be the common data repository for the facility.

All real-time data, raw data (un-filtered, un-compressed), historical and analysed data shall be made available to Company IMS via agreed protocol interface

The SCADA gateway shall make all SCADA real time data, historical data, analysed data and selected parameters available for IMS server. Alarm and event data shall be included in this interface function. The SCADA gateways shall be able to supply data to IMS for all tagged objects in SCADA with no more than 5 seconds latency.

The SCADA facility data transferred to IMS shall have a timestamp and quality code as part of the message.

The SCADA gateway shall support self-configuration of the IMS:

- Automatic configuration of tags shall be implemented when possible. This will involve the detection of a new tag being created in a related system, transfer of configuration data, and automatic initiation of data communication.

New data shall only need to be defined once, with one single engineering tool.
The interface between SCADA gateway and IMS shall be one of the following protocols:

- OPC UA
- ODBC

OPC UA is the preferred solution.

Plant data export shall not have a negative influence on SCADA primary functions, i.e., safeguarding, control and monitoring.
The SCADA gateway shall have the buffer capacity to store all SCADA real time data and selected parameters for 7 days.
Status information of the interface shall be available in SCADA.

The I/O list shall clearly define what is an alarm and what is an event.

6.1.6. Communication/Interface to TSO

Communication to TSO (monitoring of electrical Infrastructure at TSO control centre) and settlement metering/trading agency shall also be established, communication protocols to be used to be agreed and approved by TSO.

Communication between TSO and ONS should go through a dedicated and redundant link including firewall and malware protection. Secure IT solution and access control shall be established.

Signals to be transferred to / from TSO shall be agreed as part of Detail design

IEC60870-5-101 and/or IEC60870-5-104 is the preferred standard for data exchange between TSO and ONS on the application layer of the communication link. Alternatively, the DNP3 protocol could be used.
Signals sent from TSO to substation control system shall also be available in the SCADA system.

Telephone interconnection will be based on VoIp. All telephone communications initiated/received by TSO to be recorded. Retention time of recordings according to local regulations.

Handling of inter-trip signals and installation of Dynamic System Monitoring and Ancillary Service Monitoring Equipment must be provided in accordance with TSO requirements.

6.1.7. Communication/interfaced protocols

For data exchange of signals for monitoring and control between/to the ESI/WTG SCADA systems, the following communication interfaces may be used:

- IEC 60870-5-101 and/or 104
- Profibus DP
- ProfiNet
- OPC UA
- Modbus TCP/IP
- IEC 61580 serial Communication
- IEC 61580-9-2 (Process Bus)
- SNMP protocol
- DNP3
- IEC 62439-3 PRP protocol

For data exchange of signals for monitoring and control to TSO, workshops need to be done with TSO. Also see "Technical Conditions for the Connection to the Telecommunication Network of PSE S.A", I.e.:

- IEC 60870-5-104 based on TCP/IP
- ICCP/TASE.2 based on TCP/IP
- ARNE/ARST automatic voltage and reactive power control system - communication
- The communication between ONS and TSO should be established through a multiplexing system based on Optical Transport Network (layer 1), MPLS-TP with resiliency-robustness, traversal time, network latency, synchronization (time/phase) as needed by selected Tele-protection and SCADA protocols.

7. Metering, Condition Monitoring, and Instrumentation

7.1. Metering System

The primary revenue metering for the WPP will be at Slupsk Substation, delivered and installed by TSO, The back-up revenue metering for the WPP will be at Sfupsk Substation, delivered by contractor but installed by TSO. In order to mitigate the risk of change of ownership of Slupsk substation and export cable to PSE/ there will be established 0,2 class (revenue grade) VT's & CT's in 220 kV GIS bus bar at OSS. This is to safeguard always to have a correct fiscal metering independent of ownership boundaries.

At the Sfupsk, check metering shall be provided at the 400kV circuits at POI, for operational and verification purposes. Check metering shall use revenue grade current and voltage measurements, but these measurements may be shared with other functions, e.g., PQ metering. Check metering values shall be transmitted to TSO via a Remote Intelligence Gateway (RIG).

7.2. Power Quality Metering

Permanently PQ measurement system, including PQ server to continuously monitor and report on the electrical system power quality parameters with the ability to provide remote reporting and feed this information to the SCADA system and PQ Server shall be installed at POI, at ONS 400 kV side of transformers, at 220kV ONS and 66kV OSS.

The PQ measurement system shall include necessary PQ meters, sensors, PQ server, network, and interfaces for connection of the PQ meters to PQ servers and to SCADA network, and with required interface to Company IMS server.

The PQ meters shall be type Class A meters as defined in IEC 61000-4-30, and the system shall be able to obtain an evaluate up to the 100th harmonics data. Alternative standards for PQM metering shall be approved by Company.

Typical data shall be available, but not limit to:

	Signal Description	Analogue Units
1	Current IA	Amps
2	Current IB	Amps
3	Current IC	Amps
4	Voltage VAB	KV
5	Voltage VBC	KV
6	Voltage VCA	KV
7	Frequency	Hz
8	Active Power	MW
9	Reactive Power	MVAr
10	Power Factor	%
11	Voltage Unbalance:	&

	• Voltage flickers • Voltage fluctuating • Harmonics	

Tabel 2.

PQ data shall be transferred via IEC-61850, IEC-60970-5-101/104, DNP3 or OPC-UA. Type of protocol to be agreed upon.

For locations other than 400kV, the ESI SCADA shall gather non-metering grade P and Q measurements from throughout the system, for HMI viewing of system power flow, and ability to approximate system losses. This includes P and Q to auxiliary systems, O&M base, and both ends of the export cables.
These P and Q values may be through P&C relays using protection class instruments, i.e., standalone hardware is not required.

7.2.1. PQM Server

All PQM data to be stored for long time storage in the PQM server such as.

- Current, phase voltage, frequency, active/reactive power, import/export for all PQMs in system
- In addition: Voltage unbalance
    - Harmonics
        - PQMs shall be installed for all voltages levels (66kV, 220kV onshore and 400kV ONS/TSO). Sampling interval, time-average and how high frequencies shall be according to grid code and Polish requirements and shall be grid compliant
        - The data shall be shown in a clear and correct way where the planning levels from Engineering Recommendation G5/4 is shown in the figure as threshold values
        - Flag in system, timestamp and save applicable data for long term storage when crossing thresholds
    - Voltage flickers and voltage fluctuating
        - If not derived from any of the other items here, it must be set up with thresholds, so the PQM record the data and store it during an event.
    - DSM derived values
        - The same values as TSO can see through the DSM onshore and offshore shall be included on the PQM server.
        - As per TSO requirements, the same data shall be gathered and presented so it is easy to see if we are within or outside the bounds
        - Flag in system, timestamp and save applicable data for long term storage when crossing thresholds
    - ASMU derived values
        - Same as for DSM, as per TSO requirements
        - To monitor the mandatory ancillary services

Required SW for monitoring and analysing of all required data shall be included/installed on the PQM server.

All available and collected data, measurements, real time data, raw data, historical and analysed data and stored in the PQM server shall be available and transferred to Company IMS server via agreed interface protocol

Web interface for remote access to the PQM server and PQM meters for retrieving of required data and data analysing shall be included and shall be based on Company's secure access solution.

The PQM solution shall store all PQM data for a pre-defined time, at least 3 months, before transfer to Company's long-term storage solution. No data shall be lost, redundant data shall be removed.

PQM measurements shall be transmitted to TSO via a RIG. Data shall also include:
- gross MW and MVAR quantities at the generator terminals,
- generator terminal voltage and current magnitudes and angles;
- generator terminal frequency and frequency rate of change;

- generator field voltage and current, where available;
- breaker status, if available.

Above noted data relating to WTG measurements shall be transmitted from WTG SCADA to ESI SCADA. ESI SCADA shall transmit data to TSO. There is not a separate data link from the WTG SCADA to TSO, ESI SCADA shall act as a pass-through / data concentrator.

7.3. Condition Monitoring System (CMS)

Condition monitoring shall be included for equipment on ONS, OSS, cables and WTG with the following goals:

- Solutions to reduce maintenance need or requirement for facility visits (e.g., online monitoring rather than physical readings)
- Solutions to monitor asset condition by data collection and analysis to review asset health and future maintenance need

Condition monitoring solutions may perform “dual roles” by also being used in other applications. For example, a Distributed Temperature Sensing (DTS) system on export cable can be used for condition monitoring, but also used in conjunction with Dynamic cable Rating System (DRS) engine to perform dynamic power set point analysis and control. Also, Depth of Burial (DoB) Monitoring shall be included.

Required equipment, interfaces, protocols, signals, and instrumentation shall be included for transfer of required signals into SCADA and to Company IMS for Conditioning Based maintenance and monitoring and analysing of electrical, mechanical and instrument equipment to reduce lifetime cost and reduce time for offshore maintenance.

Equipment that shall have online condition monitoring system, including but not limited to are:

1. Transformers
2. WTG main bearing
3. Shunt reactors
4. Export Cables (Cable monitoring system)
5. Gas monitoring of switchgear/boards
6. Battery systems
7. Pumps
8. Motors
9. Generators
10. HVAC system components (E.g., fans, filters, heat exchangers etc.) Scope and extent of condition monitoring for HVAC shall be agreed with Company
11. Network infrastructure (E.g., switches, fire walls, protocol converters, fiber cables etc.)
12. IACS components (E.g., servers, workstations, IEDs, PLCs, Fire central, PQM meters, Field instruments etc.)
13. Fire detection panel (sensor data)
14. Tanks, to be agreed with Company

All real-time, raw data, historical data and analysed data shall be automatically transferred to Company IMS system via OPC UA protocol. The signalling route for different data may vary, but the following strategy shall apply:

1. Condition monitoring data critical for the operation shall be transferred to SCADA for alarms, then further on to IMS
2. Condition monitoring data that needs analysis or postprocessing by a system outside SCADA shall first be transferred to that system, then:
    a. If data is critical for the operation shall be transferred to SCADA for alarms, then further on to IMS
    b. If data is not critical for operation, it may also be transferred directly to IMS from the analysing system
3. If data does not require post processing/analyses by a separate system, or is deemed critical for operation, it may be transferred directly to IMS, possibly via an OPC UA gateway.

7.4. Monitoring of export- and inter-array cables

To reduce risk for overheating of the submarine cable system, a system for monitoring of cable temperature, shall be installed. In addition will a system for Dynamic cable Thermal Rating (DTR) be delivered, this system will dynamically calculate the maximum rating of the cables based on cable temperature. Both systems will be supplied by others as part of export cable delivery.

The Distributed Temperature Sensing (DTS) system shall be utilized to monitor the status of the two windfarm submarine export cables, in particular the temperature of the cables. It shall achieve this by utilizing two fiber optical cores within each of the submarine export cables. The same system may also be used for monitoring of the inter-array cables, in which case all requirements described for the export cables shall also apply for the inter-array cable.

The system shall monitor the cables with required measured values, signals, status, and alarm to/from the ESI SCADA system via agreed interface protocol. Separate OPC UA interface to Company IMS shall be included. Contractor shall ensure tags are not duplicated between SCADA and the DTS towards the IMS, this is to avoid the same signal being transferred with two different tags, and to avoid redundant information in the IMS.

Required measured values, faults and alarms shall be presented on the ESI SCADA HML

Critical alarm shall be hardwired to SCADA.

The following interface shall be included:

a) Between DTS and SCADA HMI, Protocol (Ref section 6.1.6, but shall be agreed upon)
b) Between DTS and ESI SCADA PLC (IF implemented), Protocol (Ref section 6.1.6, but shall be agreed upon)
c) Between DTS and IMS, Protocol OPC UA
d) Between DTS and Company Technical Network for service

The below list of parameters transferred between the DTS, and other systems is based on previous experience. Final list of data to be transferred between the DTS and other systems for to be agreed during design phase based on signal lists from Contractor. All data available in the DTS shall be made available on signal lists for transfer to other systems.

From DTS to SCADA

Parameter	Unit
Max Measured Temperature Cable 1	°C
Max Calculated Temperature Cable 1	°C
Max Actual Current Cable 1	A
Max Measured Temperature Cable 2	°C
Max Calculated Temperature Cable 2	°C
Max Actual Current Cable 2	A
Alarm on Export Cable 1 - Zone n	0/1
Alarm on Export Cable 2 - Zone n	0/1
System Status	o/i
System Fault	o/i

Tabel 3.1.

From SCADA to DTS Parameter	Unit
Current Export Cable 1	A
Voltage Export Cable 1	kV

Active Power Export Cable 1	MW
Reactive Power Export Cable 1	MVAr
Current Export Cable 2	A
Voltage Export Cable 2	kV
Active Power Export Cable 2	MW
Reactive Power Export Cable 2	MVAr

Tabel 3.2.

From DTS to Power Control PLC

Parameter	Unit
Max Measured Temperature Export Cable 1	°C
Max Calculated Temperature Export Cable 1	°C
Max Actual Current Export Cable 1	A
Max Load Export Cable 1	MW
Max Measured Temperature Export Cable 2	°C
Max Calculated Temperature Export Cable 2	°C
Max Actual Current Export Cable 2	A
Max Load Export Cable 2	MW
System Status	0/1
System Fault	0/1
Alarm on Export Cable 1 - Zone n	0/1
Alarm on Export Cable 2 - Zone n	0/1

Tabel 3.3.

Required software/application for remote connection for remote support, maintenance, trouble shooting, diagnostics, software updates and fil transfer shall be included.

7.5. Phasor Measurement

If TSO requires phasor measurement unit, this shall be included for the 400kV circuit.

8. Field design

8.1. General

Location and segregation shall be assessed for all IACS components for which a redundant design is chosen for reliability or availability reasons. This applies to cable routing, segregation of power feeds, physical location of components in panels, and so on. The main principle is to ensure a redundant system or function is not rendered inoperable because of a single failure.

All equipment shall be fully functional in the environmental conditions in which it is installed, ref is made to C218-ST-Z-SP-00001.

8.2. Cabinets

The requirements in this section shall apply to all IACS cabinets, including but not limited to server cabinets, Network panels. Field Termination Cabinets (FTCs) and RIO cabinets.

The IACS cabinets including panels for protection relays shall be segregated from the telecom panels.

Cabinet layout, sizes and material shall be standardized.

All cabinets design shall consider passive thermal cooling techniques to maintain operating conditions, and all cabinets, except server cabinets should be designed to avoid need for cabinet cooling fans. Special considerations, such as perforation of cabinet/doors and enforced cooling, shall be taken for server cabinets.

All cabinets shall be equipped with door locks, and it shall be possible to connect lifting lugs easily.

For cabinets installed in rooms with computer raised access floor, cable entry shall be in the bottom of the cabinets.

Equipment inside cabinets shall be easily accessible with door(s) open, and cabinet doors shall self-lock in the fully opened position.

Cabinets shall have sufficient space to permit cables to be installed without going below the minimum bend radius given by the cable manufacturer. Special attention shall be paid to arrangements for fiber optical and network cables to ensure installation in line with manufacturers recommendation is achievable for all cables. These requirements are applicable also to future cables not installed at the time of handover to Company.

8.2.1. Terminations

It shall be possible to isolate field signals from the SCADA units without disconnecting the cable cores from the terminals. This applies to all field signal terminations, including those in RIO units and field junction boxes.
Field termination blocks shall be spring-loaded.
It shall be possible to disconnect the termination part of the logic solvers without affecting the possibilities for application program testing. Reconnection facilities shall be pluggable.
C&P circuits (e.g., CT and PT terminations) shall incorporate the necessary test switches to perform the tests required in Grid Connection Agreement and Grid Codes. The required test switches shall be placed such that they allow relay and overall protection circuit testing, including operation of lockout relays, while preventing breaker failure schemes from operating and causing unnecessary breaker operations and/or the tripping of the Facility.

8.3. Field instruments

The field topology design shall be based on proven standard products in the offshore environment.

Advanced diagnostics with use of smart/intelligent field instruments/devices with field bus/HART protocol should be used to reduce maintenance and unscheduled stops in production. Field transmitters and final control elements should have configuration and self-diagnostic capabilities to enhance safety and support maintenance planning.

Industrial network for signal transfer based on fieldbus protocols may be used. This shall be in accordance with IEC 61158. The preferred choices are Profibus PA and Foundation Fieldbus.

Field transmitters and final control elements using Foundation Fieldbus or Profibus PA shall have documented interoperability, e.g., tick marked.

Analogue instruments shall be used instead of mechanical switches.

8.3.1. Degrees of protection

IEC 60529/ NEMA 250: Minimum degree of protection provided by local control panels, enclosures, instrument housing (i.e., transmitter housing) and junction boxes shall be as follows:

Location	IEC 60529	NEMA250
Outdoor areas, naturally ventilated areas and wash down areas	IP 56	4X
Dry indoor areas	IP 20	12
Other areas	IP 44 (IP 54 for indoor areas with water mist)	13/3S

Table 4 Enclosure protection.

8.3.2. Material selection

All equipment and materials shall as a minimum be flame retardant (fire retardant) and with preferably no halogen content (e.g., no fluoride, chloride, bromide, or iodide).

Equipment enclosures located outdoors in naturally ventilated areas and wash down areas shall be made of proven sea water resistant material. Alternatively, the enclosures shall be a protected by an approved coating system according to Appendix E material requirements.

Operating temperatures for 316 Stainless Steel shall be limited to 60 Deg C to limit the risk of chloride stress cracking in a saliferous environment.

Precautions against galvanic corrosion shall be made when considering the use of dissimilar materials and applying insulating layers where required.

Sensor materials shall be suitable for the application, with respect to process parameters, measurement uncertainty and repeatability.

8.3.3. Material selection table

The material requirements in Table 5 shall be applied wherever possible.

Atmosphere/ field environment	Instrument housing	Fire&Gas detectors	Protective shades	Local Control Panels	Enclosures
Indoor and dry atmosphere or external non-saliferous atmosphere	SSType AISI 316 SS or Fire retardant plastic (Note 1)				
External and saliferous atmosphere					

Note 1: Fire retardant plastic shall have a documented experience with regard to fire resistance and material degradation resistance in the applied environment.

Table 5 - Material requirements for local control panels, enclosures, instrument housings, instrument shades and junction boxes

Manual call points shall be manufactured from either glass fiber reinforced plastic or type 316 Stainless Steel.

8.3.4. Field architecture and segregation

The field architecture shall reflect project split-location fabrication and ease final assembly by minimizing hook-up items.

Field instrument and valve signals shall be hardwired directly to Remote Input/Output (RIO) units located locally in different areas. Junction boxes should be avoided but can be used if a field device has several signals that connect to the same automation system.

Fire detectors shall either be looped to a Fire central or directly wired from field.

8.3.5. Fire detection equipment

Fire detection may use flame, smoke or temperature measuring instrument as appropriate. Location, sensor range, cone of vision, plus sensor direction and angle shall be considered when selecting and placing fire detection instruments.

The fire detection system shall be designed and installed in such a way that it can be functionally tested without interrupting the normal plant operation.

The installation shall be such that testing and routine maintenance of fire detection equipment can be carried out without the use of ladders or scaffolding.

Flame detectors shall be installed to facilitate cleaning of the optics. Sensors exposed to weather shall be protected by drip or splash guards. All detectors shall be provided with spare cable length in the form of a “pig tail,” such that the equipment can be moved in any direction without disconnecting or stressing the cable. The pig tail shall be approximately 3m in length. Cables shall be installed such that water cannot run down towards the cable entry.

Manual call points shall be mounted 1.5 meters above ground level at locations that are prominent and easy to reach.

8.3.6. Winterization

Winterization shall be accomplished by first considering indoor installation, then outdoor installation with suitable instruments and heated enclosure and heat tracing of instruments and process tubing.

8.3.7. Temperature instruments

When thermowell is used, the temperature transmitter should be mounted directly on top of the thermowell and in such a manner that the element can be installed and removed from the thermowell for maintenance, without disconnecting the cable.

8.3.8. Level instruments

Level gauges and transmitters shall be physically accessible, removable, and capable of isolation from the tank, without having to drain down inventory. This is to facilitate calibration and maintenance.

8.3.9. GIS (Gas Insulated Switchgear) breaker and SF6 monitoring

GIS shall be provided with intelligent circuit breaker monitoring solution based on the Supplier's standard instruments cabled to the applicable controller. Functionality shall include monitoring and alarming of SF6 pressure, temperature, and leakage rate. The ESI SCADA shall monitor the SF6 status and provide alarms. No manual registration shall be necessary. The signal sent to SCADA shall be an analogue value, and not based on level switching, to be able to monitor and register small SF6 leakages over time or other operating point deviations.

8.3.10. Spare requirements

The following spare capacity that shall be provided at the time of plant start-up.

- Spare space in panels/cabinets (for equipment and internal wiring): 15%
- Spare in installed multicore cables and terminations (shall be terminated at both ends) excluding Cat cables: 25%
- Spare space in main cable ladders/trays and Multi cable transits for (MCTs) for telecom and instrument cabling: 10%
- Spare space in equipment rooms for future panels/cabinets, 10% based on final number of panels/cabinets installed

8.3.11. Tag plates

All tagged instruments shall be delivered with a 316 Stainless Steel tag plate of minimum size 50mm x 20mm, with etched or embossed characters of minimum 5 mm high. This tag plate shall contain the tag number only. The plate shall either be affixed to the instrument with Stainless Steel screws or Stainless-Steel wire.

Field instrument nameplates shall as a minimum contain the following information:

- Service description.
- Instrument model number.
- Instrument serial number.
- Explosion protection category and ingress protection rating (if applicable).

8.4. Power supply and power distribution

Electrical power shall be provided at 220 VDC and 230 VAC, 50 Hz.

All IACS cabinets, instrumentation, OWSs (Operator Workstations), EWSs (Engineering Workstations), plus SCADA backbone and Instrument Technical Network equipment shall remain operable following a main power failure. This shall be accomplished by installation of an Uninterruptable Power Supply (UPS).

All IACS panels shall be powered from two independent sources, one being via the UPS. All IACS equipment is to be served from one common UPS.

The IACS panels shall be equipped with redundant AC/DC power supplies in an N+1 arrangement, for provision of DC power to electronics equipment such as logic controllers, I/O cards, network components etc. Electrical isolators shall be installed such that replacement of an individual power supply unit shall be possible without interrupting normal operations.

A common alarm shall be provided for each system cabinet, to alert the operator of a power supply unit failure.

All IACS components shall be designed for continuous dual electrical power feed inputs. Where this proves impractical a changeover unit with dual power inputs shall be provided.

Galvanic isolation shall be used within the AC/DC power supplies to ensure that cable borne electrical interference does not adversely impact operation of either logic controllers, I/O cards, or field instruments.

The UPS shall interface to the ESI SCADA system via a serial data interface, for performance monitoring and power failure, as defined for Class 2 equipment. Trip signals shall be hardwired.

8.5. Earthing

Required protection earth (PE), instrument earth (IE) and equipotential bonding shall be included.
The IE shall be the common earth reference for instrumentation and telecommunication 0 V references and earthing of cable screen.

For OSS, see C256-EQ-Z-SP-00009 chapter 6.10 for details.

9. Performance

9.1. Logic Solver performance

The maximum cycle time for the logic solver shall be 100ms. Individual applications may require shorter cycle times. Where required, selected logic solvers shall be able to handle applications with cycle times down to 10 ms.

9.2. Response times

HMI response time is how fast the system responds to user interaction, that is how fast the response is after the user gives information to the system or demands information from the system. The speed of computer response to user entries should be appropriate to the transaction involved. In general, the response should be faster for those transactions perceived by a user to be simple.

Required response time shall be defined such as:

- HMI interaction response time

- Logic solver response time

The following are requirements for some key interactions and shall be satisfied for pages containing typically up to 1000 dynamic data points (See Note 1 below Table 2):

	Sec.
Call-up time for new picture included dynamic parts	1.0 (Note 3)
Dynamic elements update (measured from change in input signal value on I/O card terminals until dynamic element shows same state/value)	2.0 (Note 4)
Operator control activation (mouse click, keyboard entry, cursor controller movement)	0.25 (Note 3)
Request for a dialogue window	0.25 (Note 3)
Operator command (measured from operator command until output card/channel has reached new state)	2.0 (Note 4)
Operator alarm acknowledge (measured from operator action until acknowledgement is observed on the operator VDU)	2.0 (Note 4)
Alarm announcement (measured from alarm limit is reached until alarm text is displayed)	2.0 (Note 4)
When no response from the application occurs (system “freeze”), an “abort” dialogue window shall appear	10.0

Table 6.1 - HMI interaction response times

Notes:
2. Exception is made for drawing the trend line in mini-trends, where requirement is maximum 2.0 seconds for all trends up to 10 mini-trends on a page. (Showing the rest of the symbol shall satisfy the demand of 1.0 second).
3. Based on recommendations given in NUREG-0700, 2002.
4. This requirement is related to 1 second cycle time in logic solver.

9.3. IACS/SCADA lifetime

IACS/SCADA lifetime shall be understood as the time from site acceptance test to necessary major change out of hardware and software to maintain the original functionality due to unavailability of spare parts, lack of system competence/support/ capacity or high fault frequency.

Components and systems for the Wind Farm Plant shall have an expected lifetime as defined in table included in chapter 9.3.1.

It may be necessary to replace the originally installed IACS/SCADA with a newer SCADA generation during the lifetime of the facility.

Forethought and careful planning will minimize the impact and cost of IACS/SCADA upgrade that are due to technology change or components no longer available.

9.3.1. IACS/SCADA component lifetime

SCADA component types	Lifetime requirements (Years)
SCADA servers	10
SCADA operation station	10
Programable Logic Controllers	20
I/O cards	20
Logic solver power supply	20
SCADA network components	20
SCADA applications and tools	Life cycle support through version upgrades.

Contractor shall provide lifecycle plan for delivered equipment.

9.4. Equipment operational requirements

Equipment shall as a minimum be certified for operation under the following conditions.

Equipment rooms:
1. Ambient temperature: +5 - +35° C (+41 - +95° F)
2. Temperature gradient: 10 ° C/hour (18° F/hour)
3. Relative humidity: 10 - 90 %, non-condensing

Central Control Rooms:
1. Ambient temperature: +10 - +35° C (+50 - +95° F)
2. Temperature gradient: 10° C /hour (18° F/hour)
3. Relative humidity: 20 - 80 %, non-condensing

RIO cabinets including RIO units and field equipment in general:
1. Ambient temperature: -20° C - +40° C (-4° F - +104° F)

Equipment shall be certified for non-operation under the following conditions:
1. Ambient temperature: -25° C - +50° C (-13° F - +122° F)
2. Temperature gradient: 20° C/hour (36° F/hour)
3. Relative humidity: 5 - 95 %, non-condensing

10. Testing

10.1. FAT (Factory Acceptance Test)

The entire IACS, including internal and external interfaces shall undergo a full FAT. All IACS component parts shall be connected for the FAT, as planned for the final installation. The FAT shall include all I/O cabinets (including RIOs) logic solvers, servers, screens, and network components within the Contractor’s scope of supply.

For both ESI SCADA, WTG SCADA and telecoms, Contractor shall perform for each system a fully integrated FAT at the supplier's premise, including cybersecurity testing. These fully integrated FATs shall include O&M Base, onshore and offshore equipment. At the Telecom FAT, Contractor shall include some of the ESI SCADA panels to confirm correct integration.

The FAT shall include HMI equipment for testing of all interfaces at the Contractor's site. All communication interface signals and protocols shall be fully tested during the FAT.

All communications interface equipment shall be fully tested against telecom and relevant HMI operator station(s) for remote and local operation and monitoring.

All systems, servers and clients shall be tested to ensure that required antivirus and security OS patches are installed. In addition, testing shall ensure that OS and other software is correctly password protected and that all Universal Serial Bus ports are disabled. Verification of enabling for remote access shall also be performed.

Additional FAT testing to be performed shall include the following:

- Required Cyber Security Hacking/Penetration.
- Remote connection/Remote Desktop function for all equipment.
- Remote end to end connection
- Firewall rules.
- Hardening of equipment
- Software and configuration back-up
- Network capacity
- Dataflow volume testing to IMS

10.2. Testing of system

Test equipment for simulating all types of connected equipment and signals shall be supplied with the system.
Test programs simulating values on equipment and signals shall also be supplied. These programs shall be equipped with an appropriate operator interface.

11. Life Cycle Information (LCI)

LCI documentation shall be delivered as described in LCI requirement in Appendix E documents.

12. Additional information

12.1. Abbreviations

Abbreviation	**Explanation**
ASMU	Ancillary Service Monitoring System
AVPF	Anti-virus protection functions
BCA	Bilateral Connection Agreement
BMU	Balancing Mechanism Unit
BW	Black and White
C&P	Control and Protection
CAP	Critical Action Panel
CB	Circuit Breaker
CCTV	Closed Circuit Television
CCR	Central Control Room
CMS	Condition Monitoring System
CoP	Code of Practice

CPMS	Condition and Performance Monitoring System
CPU	Central Processing Unit
CT	Current Transformer
DMS	Dynamic Monitoring System
DMZ	Demilitarized Zone
DRS	Dynamic Rating System
DSM	Dynamic System Monitoring
DTS	Distributed temperature sensing
DTR	Dynamic cable Thermal Rating
EPC	ESI Power Controller
ESD	Emergency Shutdown System
ESI	Electrical System Infrastructure
ESON	Electrical system design and onshore substation contractor
EWS	Engineering Work Station
FAT	Factory Acceptance Test
FEED	Front End Engineering and Design
FDS	Functional Design Specification
FTC	Field Termination Cabinets
F&G	Fire and Gas
GEP	Grid Entry Point
GIS	Gas Insulated Switchgear
GMS	Grid Measurement System
GPS	Global positioning system
HART	Highway Addressable Remote Transducer protocol
HMI	Human Machine Interface
HPPP	High performance park pilot
HVAC	High Voltage Alternating Current
HV	High Voltage
IACS	Industrial Automation and Control System. Note: Industrial control systems, including distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, supervisory control, and data acquisition (SCADA), networked electronic sensing and control, and monitoring and diagnostic systems
IEC	International Electro Technical Commission
IED	Intelligent Electronic Device
IMS	Information Management System
I/O	Input/Output
KVM	Keyboard Video Mouse switch/extender
LAN	Local Area Network
LCI	Life Cycle Information
LCU	Local Control Unit
LOGIC SOLVER	Programmable Control Unit (PLC and similar devices)
LV	Low Voltage
LVAC	Low Voltage Alternating Current
MCT	Multi Cable Transit
MPLS	Multiprotocol Label Switching
NG	National Grid
NTP	Network Time Protocol
TSO	Polish Transmission System Operator
ODBC	Open Database Connectivity

OMS	Operating Metering Summator
ONS	Onshore Sub Station
OPC	OLE for Process Control
OS	Operating System
OSS	Offshore Sub Station
OTS	Operational Tripping Scheme
OWS	Operator Workstation
O&M	Operation and Maintenance
PCC	Plant Control Center
PDCS	Power Distribution Control System
PFO	Prepare for Operation
PLC	Programmable Logic Controller
PQ	Power Quality
PQM	Power Quality Monitoring
RIO	Remote Input/Output
RSTP	Rapid Spanning Tree Protocol
RTTR	Real Time Thermal Rating
SCADA	Supervisory Control and Data Acquisition
SD	Shutdown
SNMP	Simple Network Management Protocol
SOV	Service Operation Vessel
SoW	Scope of Work
SVC	Static VAr Compensator
SW	Soft Ware
TCM	Turbine Condition Monitoring
TCP/IP	Transmission Control Protocol/Internet Protocol
TP	Transition Piece
TSO	Polish Transmission System Operator
UPS	Uninterruptable Power Supply
UTC	Coordinated Universal Time
VDU	Video Display Unit
VT	Voltage Transformer
WAN	Wide Area Network
WFMS	Wind Farm Management System
WFPC	Wind Farm Power Controller
WTC	Wind Turbine Controller
WTG	Wind Turbine Generator

12.2. Definitions

Company Secure Access solution	standard system for access and services to technical systems. The solution provides two factor login, user access management, and services like WSUS, antivirus, backup etc.
Control Class 1	All control and monitoring are fully integrated in the SCADA, utilizing standard software and unit hardware
CCR	Central Control Room (CCR) shall have the capability to control multiple farms from a single location, each with a predefined set of control, monitoring and communication services. CCR is located at the O&M base.

Backup CCR	The Control Room on the ONS shall serve as a backup for the CCR and the ONS Station control must therefore be designed with necessary facilities to accommodate this.
ESI	Electrical System Infrastructure for offshore-onshore power transmission, including performing control and supervision of all functions and installations at Onshore Substation and Offshore Substation. Hereunder all infrastructure elements such as switchgears, transformers, back-up generators, reactive power components and auxiliaries.
GMS	(Grid measurement system) performing the control of the WTGs power at the Grid Connection Point in the wind farm power network to achieve grid code compliance.
IACS	Industrial control systems, including distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, supervisory control, and data acquisition (SCADA), networked electronic sensing and control, and monitoring and diagnostic systems.
OSS SUS	Offshore substation Plant Automation System. Automation, SCADA, safety, and condition monitoring system with interfaces to other systems.
SCADA	Integrated Automation Control System is the overall integrated system for Electrical Power control system including ESI SCADA and WTG SCADA, Shutdown system, fire and gas detection system which included the basic control system, power distribution control limited to Control Class 1 systems. SCADA comprises the main HMI for the facility.
Logic Solver	That portion of the IACS that performs one or more logic function(s). Examples are electronic systems, programmable electronic systems, pneumatic systems, hydraulic systems. Sensors and final elements are NOT part of the Logic Solver
Operator Workplace	All the equipment that the operator has for his disposal to do the monitoring and control of his facility area. Consists of one or more operator stations.
HVAC	Heating, Ventilation and Air-Conditioning

12.3. Changes from previous version

12.3.1. Changes from revision 01

Chap	Topics	PCP Clari.	Part of Old Text	Part of New Text
			This is revision 01	