Document Reference: OFS-GEN-015-R2

Functional Specification

SCADA and Telecommunications

		Revision History				
Revision	**Date**	**Description**	**Originator**	**Reviewers**	**Checkers**	**Approvers**
R0	25/05/2022	First Issue, for industry feedback	DNV Coen Berenschot	Vitali Garon, James Staunton, Martin Kavanagh	Neil Cowap, Leon Notkevich	Richard Blanchfield, Aidan Corcoran
R1	07/10/2022	Issued for use after industry feedback	DNV Coen Berenschot	Vitali Garon, James Staunton, Martin Kavanagh	Neil Cowap, Leon Notkevich	Louise O'Flanagan
R2	14/12/2022	Issued for use after industry feedback	DNV (Coen Berenschot), Vitali Garon	James Staunton	Neil Cowap,	Louise O'Flanagan

1 ABBREVIATION LIST

List of Abbreviation is given in table below.

AC	Alternating Current
ACS	Access Control System
AIS	Automatic Identification System
AMS	Access Management System
ASM	Ancillary System Monitoring
BCU	Bay Control Unit
CB	Citizens' Band (radio)
CCTV	Closed-circuit TeleVision
CM	Condition Monitoring
COSHH	Control Of Substances Hazardous to Health
DSM	Dynamic System Monitoring
DST	Daylight Saving Time
ECC	Emergency Control Centre
EM	ElectroMagnetic
EMC	ElectroMagnetic Compatibility
EHV	Extra High Voltage (OCC voltage of 220kV or 400kV)
EPC(&I)	Engineering, Procurement, Construction (& Installation)
ER	EirGrid’s Requirements
E2E	End-to-End (testing)
FAT	Factory Acceptance Test
FO	Fibre Optic
GMDSS	Global Maritime Distress and Safety System
GPS	Global Positioning System
GUI	Graphical User Interface
HD	High Definition
HLO	Helicopter Landing Officer

HMI	Human Machine Interface
HV	High Voltage (above 52kV but less than OCC voltage of 220kV or 400kV)
IED	Intelligent Electronic Device
I/O	Input / Output (signals or data)
ITP	Inspection and Test Plan
LAN	Local Area Network
LoS	Line of Sight
MODU	Mobile Offshore Drilling Unit
NCC	National Control Centre
NTP	Network Time Protocol
OCC	Onshore Compensation Compound
O&M	Operations and Maintenance
OPC DA	Data Access protocol of the OPC Foundation (Open Platform Communication – Data Access)
OS	Operating System
OSP	Offshore Substation Platform
OSS	Offshore Substation
OTDR	Optical Time Domain Reflectometer
OWR	Oscillographic Waveform Recording
PC	Personal Computer
PLC	Programmable Logic Controller
PoE	Power over Ethernet
PTU	Personal Tracking Unit
PTZ	Pan, Tilt, Zoom (for CCTV cameras)
RACON	Radar beacon
SAT	Site Acceptance Test
SCADA	Supervisory, Control and Data Acquisition
SCS	Substation Control System

SER	Sequential Events Recorder
SLA	Service Level Agreement
SLC	Station Level Controller
SOE	Sequence Of Events
SOLAS	Safety Of Life at Sea
TEMPSC	Totally Enclosed Motor Propelled Survival Craft
UHF	Ultra-High Frequency
UPS	Uninterruptible Power Supply
VDU	Visual Display Unit
VHF	Very High Frequency
VLAN	Virtual Local Area Network
VOIP	Voice Over IP (Internet Protocol)
WTG	Wind Turbine Generator

2 SCOPE

This Functional Specification is applicable for use in offshore wind transmission assets delivered by the Customer as Contestable Works, to be owned and operated by EirGrid.

This functional specification document describes the requirements for the supply of a Transmission Supervisory Control and Data Acquisition (SCADA) system and the data communication / telecommunication environment for the entire transmission link between the Customer's offshore assets and the existing onshore transmission grid, including the Onshore Compensation Compound (OCC) and Offshore Substation Platform (OSP). It is provided in connection with other functional specifications which cover the various aspects of the auxiliary systems on the OSP and the systems in the OCC.

This document includes the specification of the telecommunication related auxiliary systems and describes the internal interfaces with other (auxiliary) subsystems and the external interfaces with parties involved.

3 GOVERNING STANDARDS

Unless another regulation, standard or guideline is specifically mentioned in this specification document, all materials used and provided under this specification document, and all design calculations and tests, shall be in accordance with the regulations, standards or guidelines listed below.

The Transmission SCADA equipment shall be supplied in compliance with the Irish Network and Information Systems Regulations (SI 360) to protect the transmission system operation

from malicious / non-malicious cyber security threats. See OFS-GEN-17- Cyber Security Systems for additional information,

Customers who do not normally manufacture to the regulations, standards or guidelines listed may offer plant or equipment in accordance with other recognised regulations, standards or guidelines provided that they draw attention to any differences between them. Furthermore, this is subject to review by EirGrid that the performance, quality, and finish of the equipment complying with such regulations, standards or guidelines shall be comparable or higher to that complying with those regulations, standards or guidelines listed in this Section.

IEC 60870-5-104 Ed.2 and IEC 61850 ed.2 protocols, communication standards are preferred and shall be used. IEC 60870-5-101, OPC UA, DNP3 or Modbus TCP/IP and other communication protocols can be proposed, but they require consultation with EirGrid prior to its adoption. For the implementation of all communication protocols the Customer shall align with EirGrid to discuss the required protocol implementation settings.

The following lists detail relevant regulations, standards, and guidelines of relevance to the specification of the Transmission SCADA and telecommunication systems. Customer shall ensure compliance to the listed standards. Unless otherwise stated, the Customer shall use the latest versions of the documents listed.

Table 1 - Listing of Governing Standards & References

Organisation / Code	Title / Description
European Commission	EU strategic framework on health and safety at work 2021-2027
International Maritime Organization (IMO)	International Convention for the Safety of Life at Sea (SOLAS), 1974
MODU Code	Code for the construction and equipment of Mobile Offshore Drilling Units
IMO Res. A.1021(26)	Code on alerts and indicators, 2009
IMO Res. 192(79) (RACON)	Adoption of the revised performance standards for radar equipment
IMO Res. MSC. 98(73)	FSS-Code (Fire Safety Systems Code
IMO Resolution A.917(22)	Guidelines for the onboard operational use of shipborne automatic identification systems (AIS)
EirGrid OFS-CAB-100	220kV Submarine Cables
EirGrid OFS-GEN-017	Functional Specification Cyber Security Systems
EirGrid OFS-SSS-400	Onshore Compensation Compound General Requirements
EirGrid XDS-SDM-00-001	Safe by Design Methodology
EN ISO 14001	Environmental management systems - Requirements with guidance for use
EN ISO 45001	Occupational health and safety management systems - Requirements with guidance for use
EN 50167	Sectional specification for horizontal floor wiring cables with a common overall screen for use in

Organisation / Code	Title / Description
	digital communication
EN 50173	Information technology – Generic cabling systems
IEC 11801	Information technology – Generic cabling for customer premises
ISO / IEC 27001	Information technology - Security techniques - Information security management systems - Requirements
IEC 60793	Optical fibres
IEC 60794	Optical fibre cables
IEC 60864	Standardization of interconnections between broadcasting transmitters or transmitter systems and supervisory equipment.
IEC 60870	Telecontrol equipment and systems
IEC 60870-5-101 Ed.2	Telecontrol equipment and systems - Part 5-101: Transmission protocols - Companion standard for basic telecontrol tasks
IEC 60870-5-104 Ed.2	Telecontrol equipment and systems - Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles
IEC 60870-6	Inter-Control Centre Protocol (or TASE.2)
IEC 60945	Maritime Navigation and Radiocommunication Equipment and Systems – General Requirements – Methods of Testing and Required Test Results
IEC 61400-25	Communications for monitoring and control of wind power plants
IEC 61784-1	Communication Profile 15/1 (Modbus TCP/IP)
IEC 61850 ed.2	Communication networks and systems in substations
IEC 61892	Mobile and fixed offshore units – Electrical installations
IEC 62320-2	Maritime navigation and radiocommunication equipment and systems - Automatic identification system (AIS)
IEC 62351	Power systems management and associated information exchange - Data and communications security
IEC 62443	Industrial communication networks - Network and system security
DNVGL-ST-0145	Offshore Substation
IEC 60073	Basic and safety principles for man-machine interface, marking and identification
IEC 60529	Degrees of protection provided by enclosures (IP Code)

Organisation / Code	Title / Description
IEC 61311	Programmable controllers
IEC 61850-3	Communication Networks and Systems for Power Utility Automation – Part 3: General requirements
IEC 62439-3	Industrial communication networks. High availability automation networks, Part 3: Parallel Redundancy Protocol (PRP) and High availability Seamless Redundancy (HSR)
IEEE 1815	Distributed Network Protocol (DNP3)

The list of standards in the above table is non-exhaustive. Customer shall also comply with other national and international standards that are relevant to the scope of the specification.

4 GENERAL REQUIREMENTS

4.1 OVERVIEW

Figure 1 below shows a typically anticipated schematic of the connection of an offshore wind farm to the onshore electricity grid. Wind turbines are connected through “inter-array” cables (in orange) to the offshore collection point at the offshore substation, from which electricity is transported to shore via the export cable to an onshore compensation compound, which again is connected to the existing onshore transmission grid.

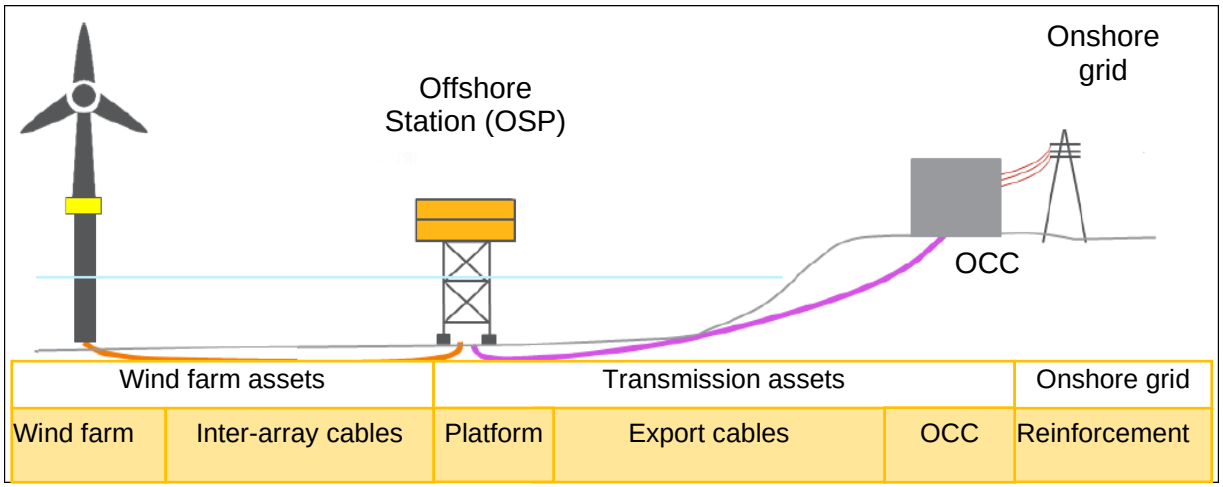

Figure 1 - Schematic of the offshore electrical grid

The design and its installation shall comply with this Specification unless any deviation which has been specifically requested by the Customer is accepted in writing by EirGrid. Where deviations from the functional specifications are proposed in the design, the Customer shall submit a formal Derogation Request providing a detailed explanation of why the non-compliance is expected and any additional information to support the request for EirGrid to consider and review on a case-by-case basis.

Further information is outlined in EirGrid’s Derogation Process OFS-GEN-024. Early engagement pre-construction with EirGrid is required for any proposed deviations.

Supervisory control and data acquisition for offshore wind power projects will impose greater demands on equipment and interfaces than the traditional onshore SCADA systems. The design of all equipment and systems must take this into account as well as the high costs of outages. Robustness, redundancy and resilience are important.

Need for offshore intervention and operation shall also be minimised as much as possible to reduce operational costs and increase availability.

Open communication protocols must be applied to maximise integration of various systems. These communication protocols shall be of TLS/SSL encryption, SIP trunking encryption (for VoIP), WEP/WPA1,2,3 (for Wireless) secured communication types.

The Transmission SCADA system shall be split into components that are located either offshore or onshore. The starting point for both the Transmission SCADA design and the telecom design is the delivery of an integral system that includes all necessary onshore and offshore system components.

4.2 QUALITY OF MATERIALS

All equipment that is part of the installation to be implemented shall be of state-of-the-art design and have a proven track record at the start of the installation in wind power plants or power transmission operating companies (to be proven by the Customer).

All materials shall be suitable for operation in EirGrid remote control centre, onshore compensation compound (OCC) and offshore substation environment. Transmission SCADA servers and BCUs/IEDs shall conform to the appropriate standards as laid out in IEC 60870. Low Voltage AC UPSs shall conform to standards laid out in IEC 62040. Fibre optic cables and their connectors shall conform to IEC 60793 and IEC 60794.

All devices, cables or connectors that are not kept in a controlled environment shall be of a standard that protects them from humid and salty environments. The standard for marine devices is IEC 60945.

Mobile and fixed VHF equipment, personal safety devices and any automatic identification devices shall conform to the appropriate parts of standards IEC 60945 and IEC 61993.

Materials within the scope of supply that may be dangerous to health, as defined in the EU strategic framework on health and safety at work 2021-2027 regulation, shall be disclosed, in writing, to EirGrid a soon as practicable

Materials shall be suitable for the purpose and environment and shall withstand the variations of temperature and atmospheric conditions occurring in service without damage, deterioration or the creation of abnormal stresses, and without significantly affecting the strength and the suitability of the various parts.

Where dissimilar metals are in contact with each other than through oil, approved means shall be provided to prevent electro-chemical action and corrosion.

The materials selected shall have the ability to maintain satisfactory quality through transportation. Where necessary, the Customer shall design and install sea fastening for the equipment during transportation.

The Customer shall provide sufficient monitoring during storage and/or transportation to ensure

the quality of materials upon final installation and handover to EirGrid.

Quality of materials shall be ensured during and after transportation. Suitable measures shall be applied to check the quality of the material upon final installation (for example, installation checklists shall be completed).

The Customer must not install any equipment or components if it is suspected that they have been damaged during storage or transit and that their quality is compromised as a result.

4.3 TRANSMISSION SCADA AND TELECOMMUNICATION BASIC SYSTEM ARCHITECTURE

Figure 2 shows a high-level monitoring and control architecture. A more detailed Transmission SCADA architecture with indicative data flows is included in appendix A.

EirGrid's Transmission SCADA system for onshore and offshore assets shall be designed as a common integrated system and shall perform all the functions for equipment within EirGrid's ownership boundary required for monitoring and control of the offshore and onshore substations, compensation compounds, other auxiliary systems on the platform and onshore.

The Transmission SCADA system shall have a redundant interface with the EHV and HV protection devices and IED of EirGrid in order to provide information on protection operations, settings, alarms, statuses to relevant control centres

The system will be divided by functions, so tasks will be performed at the lowest possible level of the hierarchy.

The wind farm owner will have its own SCADA system and control centre, which is depicted in Figure 2 with orange boxes / symbols.

From control structure point of view, EirGrid's Transmission SCADA system shall be designed as multi-level control system including:

- Control room level (including remote central control room of EirGrid to control and monitor several wind farm assets and NCC)
- Onshore / offshore station control level (incl. Platform Technical Services, Telecom)
- Bay level control (LCC, Protection devices, IEDs, etc.)
- Primary equipment control (actual devices like circuit breakers, disconnectors, earth switches, etc.)

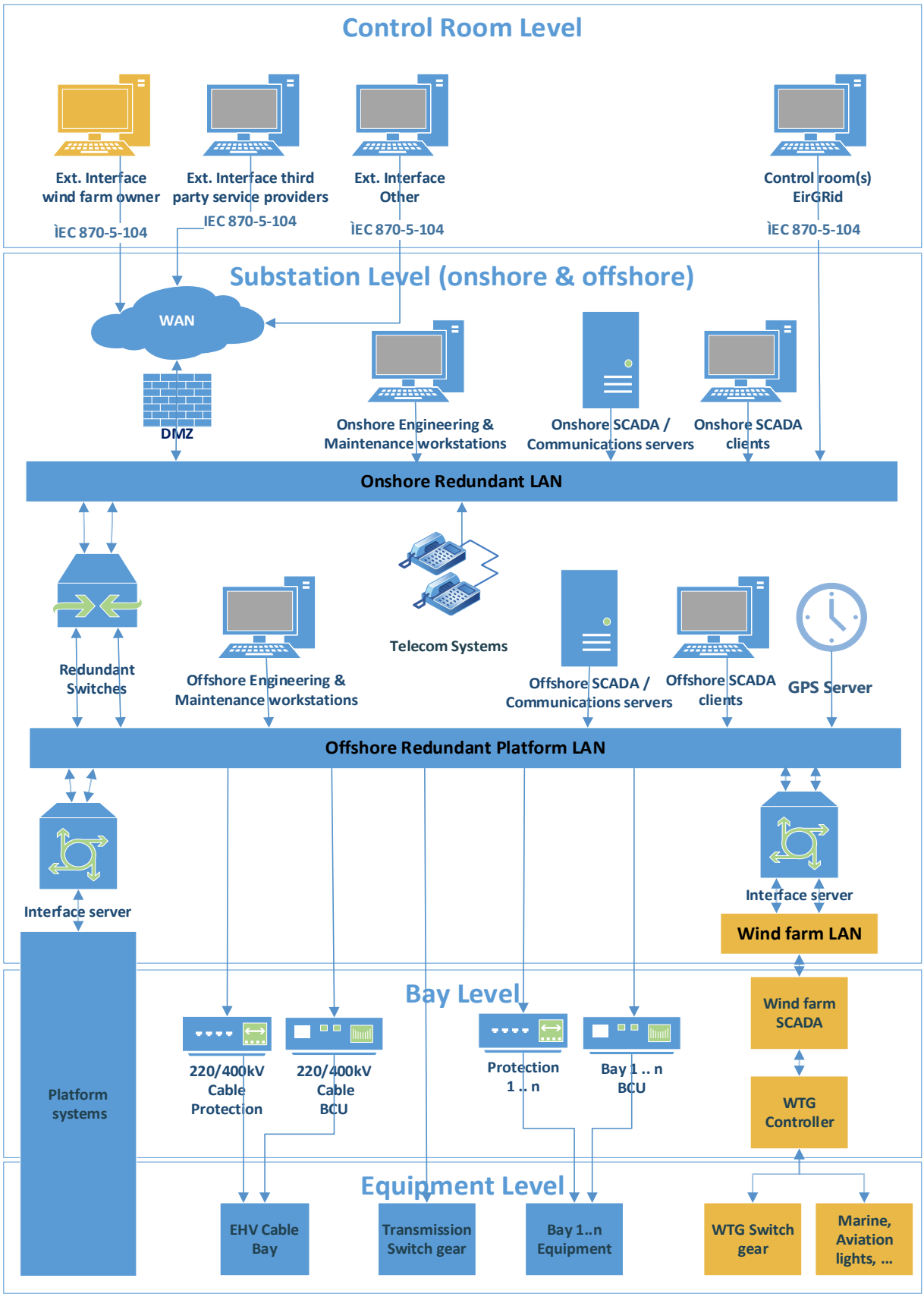

Figure 2 - High Level Control and Monitoring structure

Monitoring and controls of the equipment in the offshore platform or onshore must be possible from the following locations:

- switching equipment (position indications).
- the local control cabinet (where BCUs/IEDs are equipped with local user displays, showing single line diagrams of the bay).
- from the station HMI (workstations).
- remotely from the Control Rooms (OSP, OCC and EirGrid remote-control centre(s), NCC). Full control and monitoring facilities of EirGrid assets shall be available at OSP, OCC and EirGrid Remote Control Centre and are expected to be similar in the three locations. Signal lists to NCC shall be agreed with EirGrid during detailed design.

It is the customer's responsibility to design, engineer, install and ultimately transfer this integral system to EirGrid so that it can be operated and maintained according to EirGrid's requirements.

4.4 ONSHORE/OFFSHORE EQUIPMENT SPLIT

The monitoring and control functions available onshore (OCC and EirGrid remote control centre(s)) shall match those available offshore. To achieve this, the Transmission SCADA system shall have a highly resilient gigabit network connection between the offshore platform and the onshore control rooms / buildings. The main and back-up communication will be through fibre optic cables but depending on the situation the back-up communication may be through microwave, satellite, etc. (To be proposed and consented by Customer). However, no safety critical functions shall rely on this network. For this reason, the offshore level shall contain application and communications servers at least to allow predefined independent control measures in case of disruptions of communication with the onshore compensation compound. The onshore level shall contain data storage and communications servers as well as (at least) access to the application servers. Workstations shall be located both onshore and offshore.

4.5 DATA COMMUNICATION STRUCTURE

Since the Offshore station is the hub of the electrical infrastructure offshore, it shall be natural to become the hub of the communications infrastructure as well. It shall be the collection point for all electrical cables and shall contain the equipment which requires the highest bandwidth data connections. The Data communications system can be split into three separate segments:

1. Communication to EirGrid’s Control Centre (which controls all EirGrid’s transmission assets related to offshore wind farms),
2. Communication to/from/around the offshore platform(s) and Onshore Compensation Compound(s),
3. Communication to Customer’s assets (including inter-array switchgear, wind turbines)

Communications around the platform and onshore station shall be carried on a communications backbone. This shall connect to the external data connections through redundant gateways. This is especially important for systems that are related to safety (the movement of people offshore and monitoring approaching vessels and aircraft). Backup safety communications and communications to moving vessels should be using radio. Any backup should have a different

transport medium, and a different power source. In addition, the wind farm owner's communication system must be completely separate functionally and independent from the EirGrid communication system. Some physical communication media or infrastructure can be shared in consultation and with EirGrid, like the communication mast or the optical fibres in the export cable to shore.

The customer in their design proposal shall consider all the possible communication routes and submit it to EirGrid for review.

The proposed design by the customer shall differentiate the channels, servers, storage, synchronisation and controls for the SCADA type of communication needs from the telephony, LAN, and other non-control non-SCADA related telecoms, such as distributed wireless sensors, mobile and worker hand-held devices etc.

4.6 SUBSTATION CONTROL SYSTEM

This specification covers the design, engineering process, delivery and technical support of the Substation Control System (SCS) for contestably built substations as part of the scope of the wind farm project.

For the Substation control system (SCS) the requirement is for latest most suitable solutions to be provided. SCS proposed vendor shall be reviewed by EirGrid. SCS shall be:

a. Of state-of-art technology (i.e. be at the most recent stage of technological development; having or using the latest techniques or equipment),

b. has experience of the use within transmission industry and has good track records in EHV transmission networks in at least three EU, EEA or UK utilities.

c. has been used in at least three offshore wind power projects in the EU, EEA or the UK.

d. A vendor presence in Ireland for support of such system

The Customer shall be required to purchase and install all the necessary hardware associated with the SCS.

The Customer is responsible for the system design, procurement, installation, pre-commissioning and commissioning of the SCS. The Customer shall engineer the complete SCS database and configurations for the substation SCS.

At system handover the Customer shall issue a complete set of as-built documentation, test records, operation and maintenance manuals and any other data or documentation required for EirGrid to undertake the SCS operation, support, modification, and maintenance services (including spare parts as described in section 13.4). Further information is outlined in EirGrid's Operations and Maintenance Specification OFS-GEN-009 document.

A Substation Control System provides access to the higher monitoring and control level (Control Room Level) and to the monitoring and control level in the substation in addition to local control and monitoring from the Human Machine Interface (HMI) in the substation. The SCS also forms the control interface to the underlying monitoring and control layers at bay and equipment level. A typical control system architecture (onshore and offshore) consists of the following levels:

- Substation Level – The common level within the station at which the HMI, Station Level

Controller (SLC) and central SCS panels reside. The SLC provides Substation Control System for Contestable Built Substations, data concentrator and communication gateway functions, including connections to the Control Room Level (OCC control room, OSP / OSS control room, Remote Control Centre(s) of EirGrid or National Control Centre). All general substation signals are interfaced to the SLC also.

The HMI provides the Operator with the means to control and monitor the substation equipment, in addition to displaying event and alarm information acquired from all SCS devices in the substation.

- Bay Level – The level where the BCUs and protection devices are located for a particular bay. Data acquisition is performed at the bay level using dedicated Bay Control Unit (BCU) devices, which communicate to the rest of the system using communication protocols over fibre optic and ethernet cable interfaces. Signalling from the protection system is also integrated into the SCS using various open communication protocols to transfer alarm and event data to the higher levels (Equipment Level – The level where the actual devices are located like circuit breakers, disconnectors, earth switches, etc. At this level, the I/O data is received and sent from the primary equipment to the higher monitoring and control levels.

4.7 REMOTE / LOCAL CONTROL

The onshore and offshore parts of the Transmission SCADA system shall be equipped with a soft local/remote operated switch integrated in the HMI that should prevent operation from the higher control levels, like EirGrid's Remote Control Centre(s). Operations from the prevailing and underlying levels shall not be affected by the position of this switch. Protection and Emergency Trips breakers opening) shall work at all times.

It shall be possible to turn off remote control for the entire substation and/or for individual bays.

For each bay Local / Remote spring-loaded key operated switches shall be provided with two positions as follows:

a) Remote position: remote control possible, local control inhibited.

b) Local position: local control possible, remote control disabled.

Local/remote switches shall be provided with enough contacts to allow separate (double pole) switching of circuits for both remote and local operation, together with auxiliary contacts for indication of switch position to the Transmission SCADA system. They shall have provisions to prevent unauthorised use in the form of a locking mechanism or by means of a separate padlock. All locks must be provided with the same key.

5 SYSTEM REQUIREMENTS

The full functionality of the Transmission SCADA system (including all necessary communication infrastructure) is to be secured during the whole design life cycle.

The Transmission SCADA system must perform its functions whenever they are required, and it shall not perform incorrect functions.

Module replacement in the Transmission SCADA system shall be done without changes in the data model.

The construction and operation of the Transmission SCADA system shall be so designed, that testing of the Transmission SCADA system shall be possible during operation.

The overall system requirements mentioned in this section also apply to the underlying local control systems or auxiliary systems.

5.1 SYSTEM RELIABILITY

The Transmission SCADA system shall have a high level of operational reliability.

The system as a whole and each subsystem by itself shall be 'fail-safe' which means that in the event of faults or failure of a (sub)system, the relevant functions can adopt a safe state or be taken out of operation safely where appropriate.

Any data overflows shall not lead to the system no longer being able to perform its functions.

All Transmission SCADA communications, fibres, equipment, gateways, ports, switches, servers, etc shall be fully redundant at all levels to maximise reliability (No single points of failure).

All network equipment shall be equipped to have a redundant power supply. Both supplies shall have a separate UPS backup. Failure of the one supply shall not cause any loss of operation.

All hardware SCADA, communication equipment shall be designed for a redundant, UPS / battery backed power supply.

5.2 SYSTEM AVAILABILITY

A fault in a part (subsystem) of the Transmission SCADA system shall not cause the failure or disturbance of other subsystems.

The system shall be fully redundant: in servers, network and communication.

The following minimum system availabilities shall be provided:

- 99.9% within the warranty period.
- 99.5% during the complete system life cycle.

The Customer shall provide an availability calculation of the Transmission SCADA system to demonstrate that the availability requirement is met.

5.3 SYSTEM FAILURE BEHAVIOUR

After failure and subsequent restoration of the power supply, the system should restart automatically.

Internal system operator inputs such as automatic alarm acknowledgment and manual operation must be kept fail-safe.

Spontaneous commands are never permitted, especially in the following cases:

- When a function was inactive and becomes active and is put into operation.
- In case of failure and restoration of the communication link.
- When the power supply is restored.

- During testing

If a failure arises, it shall be possible to take just the relevant part of the system out of operation without affecting the remaining parts of the system.

5.4 SYSTEM RESPONSE TIME

The execution of control functions must not be hindered by high data traffic from the process.

Partitioning technique for SCADA and non-SCADA systems shall be implemented to increase reliability and robustness. Customer shall submit the partitioning proposal to EirGrid for review.

The Transmission SCADA system shall provide a rapid and consistent response to substation system events and user inputs. Responsiveness to events and inputs shall be within the designed/agreed requirements under both the steady state and high activity state.

5.5 SELF-MONITORING

The system shall be equipped with self-monitoring programs that carry out regular, automatic online checks on the functioning of the system and the software. It shall be possible to carry out tests both offline and online. Any fault which occurs in single devices or in the system shall be logged and also reported as an alarm to the Transmission SCADA system.

5.6 CYBER SECURITY

Security of the communications and Transmission SCADA systems are of primary importance and need to be a key principle of the design. Cyber security shall be in accordance with international standards referred to and include, at a minimum, the following considerations:

- Authentication of users.
- Role based authorization of authenticated users. (Segregation of duties)
- Separation of systems within the project.
- Separation of Transmission SCADA system from the internet (Network segregation)
- Secure transfer of information.
- Compliance with appropriate standards.
- Physical access to equipment.
- User and organizational aspects.
- Intrusion detection.
- System hardening.
- Physical network segmentation from non-SCADA and SCADA communications.
- Cryptography / encryption of data
- DOS protection
- Malware on all devices where possible
- Secure protocols / session authentication

- Centralised log servers and log distribution
- Edge firewalls for all individual LANs

Cyber security shall follow all legal requirement and international standards including but not limited to as referred to in Section 3.

Extent of cyber security provisions required, and its benefits and implications shall be further explored during the basic design phase in consultation with EirGrid.

The cyber security design shall comply with EirGrid's functional specification on cyber security systems (OFS-GEN-017).

The above security aspects with the reference to EirGrid's functional specification and to the relevant international standards should be regarded as the minimum requirements to include in the system and network design to make it sufficiently secure. It is up to the customer to propose a design that is appropriate.

5.7 SIGNAL RECORD ON HMI

In the event of a major incident where there is a "burst" of signals and/or measured values in the bay units, all information and commands on the system must be available and displayed in the operator HMI's (workstations) offshore and onshore.

5.8 REDUNDANCY REQUIREMENTS

As the Transmission SCADA and communication systems shall be used for condition monitoring, safety, control and operation, they shall be fully redundant.

All the Transmission SCADA, SCS equipment in the offshore platform, onshore compensation compound and any other related equipment shall have a redundant design of power supply and communication networks. There should be no single points of failure in the Transmission SCADA and telecom architectures. A single point of failure is defined as a device, connection or piece of software, which if it fails limits the functionality of the Transmission SCADA system.

Failure of any of the devices (IED or switch) shall not prevent communications between the healthy devices. Failure/disconnection of a single fibre connecting any two Ethernet switches shall not impact control and communications.

Any failures in any equipment shall initiate an alarm.

The primary communication transport medium shall be fibre optic cable. However, there will be no communication route between devices within the scope of the project that rely on a single fibre optic cable. The design must be based on a fully redundant primary communication architecture at all communication levels, including the lowest equipment level (including protection relays / IEDs).

Primary communications shall be over redundant fibre optic links. Communication redundancies shall be reviewed by EirGrid.

Communication from OSP to OCC shall be in the form of a high capacity, low latency link. An example of a redundant primary communication architecture between OSP and OCC is shown in Figure 3.

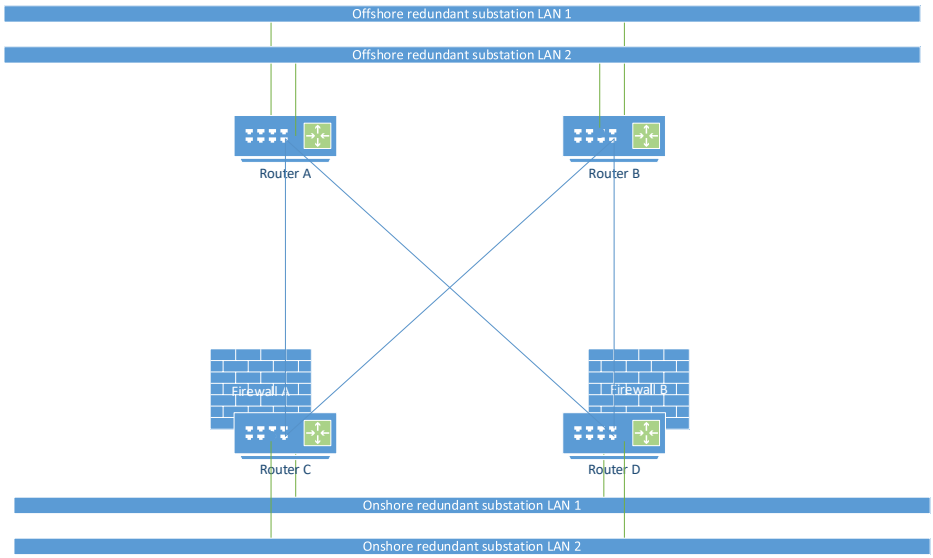

Figure 3: Redundant connection between OSP and OCC

In addition, a back-up communication medium is required preferably via fibre optic cable.

In case a second export cable is available to the OCC, this cable could be used to make the backup for the primary communication path based on fibre optics.

When a wind farm is so large that several offshore platforms exist, backup communication can also be realized via the export cables of another platform. For this purpose, a fibre optic interconnection must be created between the platforms, whereby a similar redundant architecture is required as indicated in Figure 3.

In the event a backup for the primary communication based on a fibre optic connection cannot be created, the Customer shall propose a second back-up communication medium depending on project specific conditions for EirGrid. This back-up communication medium shall be proposed by Customer for EirGrid's review and can be supplied through the following means, with priority from top to bottom:

- Microwave LoS
- VHF/UHF radio
- Satellite

To maintain the redundancy required, all major components within the network should be connected to the LAN by at least two separate cables using separate routes. A major component is a device which handles data traffic from more than one source. An individual CCTV camera, or sensor is not considered a major component, however Transmission SCADA servers, gateways, switches, and condition monitoring servers are.

All network equipment shall be equipped to have a redundant power supply. Both supplies shall have a separate UPS backup. Failure of the one supply shall not cause any loss of operation.

Time synchronisation system shall be redundant. The customer shall provide the level of redundancy for EirGrid review.

6 INTERFACES AND SUPPORTING SYSTEMS

This chapter describes the functional requirements for interfaces of the Transmission SCADA and Telecom systems with other systems. In addition, the functional requirements for several telecom and (marine) safety-related subsystems are described.

6.1 INTERFACE TO PRIMARY EQUIPMENT

Primary equipment concerns all equipment used in the primary circuits / process of the electricity supply (transformers, switchgear, shunt reactors, reactive compensation equipment, harmonic filters, statcom, EHV/HV cables, etc.) including the systems and components that support the primary process. Examples of such supporting systems are all types of protection systems.. HV / LV auxiliary transformers and LV main switchboard(s) are also considered as primary equipment for SCADA.

All primary equipment that is part of the project scope must be connected to the Transmission SCADA via the required communication protocols, so that all equipment can be monitored and controlled.

SCADA shall include and display all alarms, control commands, status and monitoring indications and measurement signals for the primary systems. Alarms, events shall be time stamped so that they remain uniquely identifiable in the whole system.

Signal lists for each primary system (input, outputs) shall be reviewed by EirGrid.

In each bay the following analogue signals shall be collected and processed by the respective analogue modules in the BCU:

- V/mA signals: originating from the A/D transducers.
- V/A measured values: direct from the measuring current and voltage transformers.

The electrical characteristics of the signal will not be affected by the inputs.

The individual analogue input channels shall be electrically isolated from each other.

Digital signals shall be collected and processed by the respective digital I/O modules in the BCU. As digital signals are considered: alarms status of switching devices and protection signals. Digital signals can be both 1 bit and 2 bit and can be handled as events or alarms.

Alarms and status signals from the primary substation equipment can be hardwired into the BCU, and as for the IED signals they shall be transmitted to the BCU via protocol (IEC 61850).

A separate command output shall be provided for each control function. The outputs shall be potential free and suitably rated to operate the primary switchgear.

Commands for operating the primary equipment are given by means of command outputs. Command can be initiated by protection IEDs (trip), BCU and from offshore and onshore Transmission SCADA system (including onshore EirGrid central remote-control centre(s)).

Commands initiated at the offshore and onshore Transmission SCADA shall be checked at the BCU, thus ensuring that not more than one device is selected.

Commands given at bay level have top priority followed by commands from the offshore and onshore Transmission SCADA system.

6.2 INTERFACE TO AUXILIARY SYSTEMS

The Transmission SCADA system shall have I/O modules or communication links (communication protocols) to interface with all auxiliary systems. Table 2 provides a non-exhaustive overview of possible auxiliary systems for guidance. Customer shall submit systems to be monitored for EirGrid review. All auxiliary systems will be accessible from Transmission SCADA and its alarms, statuses / positions shall be monitored from Transmission SCADA HMI. Relevant controls of the auxiliary systems shall also be included into SCADA. Signal lists for each auxiliary system (input, outputs) shall be reviewed by EirGrid.

Table 2 - non-exhaustive list of possible auxiliary systems

Auxiliary Systems	Offshore	Onshore
Cable Condition monitoring / DTS	X	X
Foundation condition monitoring	X	
Corrosion protection systems	X	
Power Quality meters and operational metering	X	X
CCTV system (PTZ and fixed cameras)	X	X
Fire detection / Fire fighting	X	X
Access Control	X	X
SCADA system components	X	X
Data network monitoring	X	X
Intruder Alarm Systems (IAS)	X	X
LV distribution systems	X	X
UPS / backup power supplies	X	X
Meteo systems (including ocean data)	X	
GPS systems / Time synchronization (can be shared between EirGrid and Customer)	X	X
Heating, Ventilation, Air-Conditioning systems (HVAC)	X	X
Marine and aeronautical radio communication / coordination systems	X	
Material handling systems (Cranes, elevators, etc.)	X	
Potable water systems	X	
Wastewater systems	X	
Diesel generators, storage	X	X
Power quality monitoring	X	X
Earthing and lightning strikes	X	X
Marine and aviation navigation / safety lights (Nav. Lights, Foghorns, , etc.)	X	

Auxiliary Systems	Offshore	Onshore
Automatic identification system (AIS)	X	
Battery systems	X	X
Metering Systems	X	X
Public Address and General Alarm (PAGA) system	X	
Telecommunication systems (Telephones, Wi-Fi, VHF/UHF radio, microwave, etc.	X	
ASM / DSM panel monitoring	X	X
Perimeter Intrusion Detection System (PIDS)		X
Security lights	X	X
Audio Intercom devices	X	X

For each interface in scope, the Customer provides EirGrid with a signal list for review and approval. A generic template for this must be agreed in advance with EirGrid.

6.3 TIME SYNCHRONISATION

A radio-time receiver based on GPS time synchronization shall be used for time synchronisation. Time server must synchronise all devices of the substation Transmission SCADA system.

In case of GPS failure, all devices shall be synchronised by their internal time clock.

If the GPS server fails, the backup should be an NTP server. In case of failure of both GPS and NTP servers the internal clock shall be used. Failure in GPS and NTP time sync shall issue an alarm.

It shall be preferred that the Transmission SCADA system operates in “standard time” (no DST switch). That means that the events shall be time stamped and stored with “standard time”. However, the information displayed in the HMI shall be in “actual calendar time” (incl. DST).

When starting up the system or parts thereof, synchronisation needs to take place automatically.

6.4 TELECOMMUNICATIONS MEDIA

Fibre optics shall conform to standards IEC 60793 and IEC 60794.

Substation-to-shore communications shall be provided by single mode fibres embedded in the export power cable.

6.5 TELECOMMUNICATION COMPONENTS

The substation telecommunications network will be made up of a TCP/IP based network over Ethernet. Traffic will be segregated using VLANs on the basis of destination and security requirements.

All Ethernet switches inside the substation shall be manageable and capable of separating traffic into virtual LANs (VLANs). The switches shall facilitate Power over Ethernet (PoE).

Redundant gateways shall be manageable and separate internal substation traffic to other segments.

IEC 61850 requires that the substation backbone be made up of redundant connections forming a single Ethernet network, with traffic being directed through the use of VLANs.

6.6 LAN AND WAN SYSTEMS

IP services Local Area Network (LAN) system shall be provided to facilitate OSP internal communications and systems interfacings, as well as communications with the OCC and the communication with the remote control centres.

All Transmission SCADA and telecommunication subsystems will be connected to the substation LANs through the dedicated VLANs.

Each LAN should be designed with redundant principle with dedicated A and B switches located in the designated A and B cabinets for switches and servers. Redundant links to access-layer switches have equal capacity and are physically separated, see Figure 4.**Error! Reference source not found.**

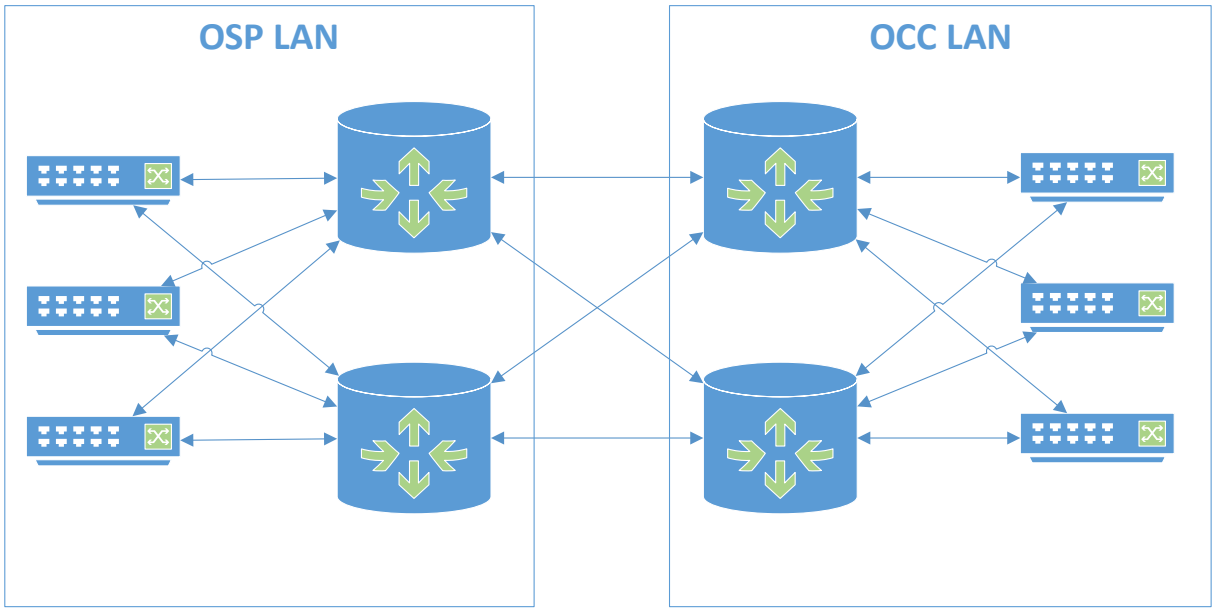

Figure 4: Redundant LAN structure

LAN system(s) shall be integrated with EirGrid's IP systems through installed core switches on the OSP and in the OCC. Number and configuration of the core switches depends on the requirements and shall be defined accordingly.

The system back bone shall meet the requirements IEC 11801.

6.7 WIRELESS LAN (WI-FI)

Wireless LAN infrastructure shall be installed on the OSP and OCC and its access points shall allow connections between workers on the platform.

The Wireless LAN system shall consist of wireless network controller, switches, and access points to be installed indoor and outdoor at OSS platform and all areas of OCC.

The required bandwidth and coverage area shall be proposed by the customer and reviewed by EirGrid. Wi-Fi service shall be considered for all indoor and outdoor areas. It shall be designed in compliance with EirGrid's requirements. WIFI service should be an extension to the wired LAN.

Different Wi-Fi security configurations shall be applied for:

- Customer's users, EirGrid users or guest users,
- access to the OSP, OCC network or to Internet,
- access to the OSP, OCC network by using Customer owned, EirGrid owned or private computing devices.

The outdoor Wi-Fi services shall be designed to provide full coverage over the whole offshore installation with particular emphasis on the production/process areas.

6.8 VOICE COMMUNICATION SYSTEMS (VOIP)

Voice communications are safety critical. For this reason, VoIP communication shall be provided in OCC, OSP and EirGrid remote control centre(s).

VoIP shall be primarily based for fibre optic communication. In case, FO communication is not available a redundant communication medium shall be used.

VoIP equipment shall be powered from UPS backed source of supply.

Locations of emergency VoIP phone sets shall be proposed by Customers for review by EirGrid .

6.9 RADIO SYSTEMS

The usage of a radio system is one of the mandatory communication ways on offshore platforms according to the maritime laws. The radio system shall meet the latest SOLAS convention requirements and should be designed to provide reliable and highly available service(s) with no single points of failure.

Mobile radio systems shall be provided for the following reasons:

- Mandatory SOLAS radio systems to provide communications from TEMPSC/lifeboats (if applicable), life rafts and fast rescue craft to the control and emergency response rooms.
- Marine band radio for communications to support vessels and ships.
- Aviation band radio system for communications from helicopter landing offices to helicopter pilots (If applicable).
- Onboard radio system to provide communications between base stations and mobile handheld radios, with coverage over 90% of the facility.
- Crane radio to allow communication between crane operator, supply vessel and deck crew.

Mandatory radio equipment shall conform to the latest GMDSS amendments of 1974 SOLAS convention concerning radio communications and to the latest amendments to the 1989 code for the construction and equipment of MODUs.

In accordance with GMDSS regulations, the radio equipment shall be designed and provided

according to the applicable requirements to the sea area where the offshore facility is located.

The customer shall ensure that the radio systems comply with the Irish regulations.

6.9.1 MARINE RADIO SYSTEM

The OSP shall be equipped with a multi-channel VHF FM marine band radio in compliance with marine communication standards IEC 60945, IMO SOLAS and GMDSS requirements for communications with nearby shipping, the landing deck and other facilities.

The marine radio shall be equipped with digital selective calling (DSC) Class A function for emergency voice communications on the marine distress frequency.

The marine radio should be capable of interfacing (directly/indirectly) with platform LAN system or platform Transmission SCADA system for integrated communication connectivity and recording. This allows for voice recording of radio traffic.

For emergency situations, an additional VHF marine band radio unit shall be provided in the emergency shelter, if the location is different from the location specified in above.

The primary communication media for approaching ships or aircraft shall be via VHF FM radio. The backup route for this is the site's IP telephone system, which must be rerouted to a local Coast Guard station.

6.9.2 MARINE RADAR TRANSPONDER BEACON

A marine radar transponder beacon (RACON) system provides information on the location of nearby vessels and hazards in relation to the offshore facility in all-weather or restricted visibility conditions.

The RACON system is mandatory and shall be installed on the OSP platform as an offshore facility to meet national or international maritime regulation requirements.

The RACON system shall be installed on a location with unobstructed view of the horizon.

The RACON system shall be powered by UPS system. The battery back-up shall be made available due to criticality of the system. The duration of the battery autonomy time is determined by local and regulatory (i.e., SOLAS) requirements, typically 96 hours.

The above requirement for EirGrid’s separate RACON system may be reviewed and possibly modified / waived if Customer proposes an adequate alternative system for marine coordination and traffic monitoring.

6.9.3 AVIATION / AERONAUTICAL RADIO SYSTEM

Radio communication between the OSP and support helicopters shall comply with relevant regulations.

The aviation radio system shall use VHF AM mobile radio system, per the requirements of the national / civil aviation authority (NAA / CAA), to facilitate communication between helicopter pilots and the helicopter landing officer (HLO), if applicable.

The aviation radio system should facilitate routine and emergency communications and operate in specified frequency band and channel spacing in ITU Radio Regulations.

The VHF AM system shall be powered by UPS system. The battery back-up or other sources of emergency power supply back-up shall be made available due to operation and safety needs of the system. The duration of the battery autonomy time is determined by SOLAS requirements at minimum.

6.9.4 ONBOARD RADIO SYSTEM

A fixed marine band VHF FM (or UHF) radio system shall be provided to ensure safety and operational communications throughout the OSP if the use of normal and fixed telephones or fixed intercom is not possible or unavailable. The radio system must support both the operational and emergency communication needs of the facility. Therefore, during and in the event of an emergency, the system must be fully operational and have comprehensive coverage across the entire site, including emergency locations and muster stations.

Since the OSP is a small facility with low volume of radio users, a non-trunked radio system providing a single or multi channels radio system should be used to support operations.

The radio system should employ the latest technology with a capability to integrate with analogue radios, the IP Telephony system, PAGA system and the platform control / Transmission SCADA system.

The radio system should be implemented as base stations in permanent locations (HLO room or local control room) or as handheld devices for mobile use. Radios should operate in both peer-to-peer (radio-to-radio) or in group fashion (radio-repeater-radio).

An alternative mobile / transportable OSP radio system can be proposed by Customers for EirGrid review and approval.

6.10 4G LTE SYSTEM

If required, a 4G LTE system shall be installed on the OSP to allow 4G data exchange between workers, equipment on the OSP and data access to vessels and helicopters near the platform.

4G LTE station shall be connected to the OSS telecommunication system LAN.

Two options for 4G LTE system shall be considered with the order of preference:

1. Option 1: Private cellular system
2. Option 2: Public service

In the former option, the system shall connect with onshore 4G LTE system via subsea FO connection. 4G station coverage and bandwidth shall be defined with EirGrid. As a preliminary figure, OSS 4G system shall cover an area around 10 kms with a minimum speed of 20 Mbps up to 100 Mbps close to the source.

In the latter option, OSS should be connected to the cloud of a 3rd party provider via LoS. This can be an option during the OSS installation period when platform systems are not yet in service. During the basic design phase of the project, coverage of the OSS area by a 3rd party 4G system shall be checked if this option is decided to be considered.

Besides the communication with onshore location(s), 4G LTE system of the OSS and / or supporting vessel(s) can also be used for communication during the installation phase of the OSS platform.

The requirement for 4G LTE system shall be determined during the design stage.

6.11 MICROWAVE COMMUNICATION – LINE OF SIGHT

As described in the section about redundancy, a microwave system shall be considered as the first choice to provide back-up connections between the OSP and OCC in case of losing of primary redundant communications to onshore through subsea fibre optic cables.

Two options shall be investigated in the basic design phase of the project with the order of preference:

- Direct communication with the OCC location via Microwave antennas
- Communication via the network cloud of a 3rd party service provider

The exact location of antennas and towers and its use by different parties for different applications shall be determined during detailed design in consultation with EirGrid.

6.12 VSAT (SATELLITE COMMUNICATION) SYSTEM

Communications with the OCC may be done via VSAT system as a backup communication path (subsea FO is the main way) but is considered the least preferred alternative for communications to shore.

A Multiband C/Ka- and Ku/Ka-band stabilised maritime VSAT system should be installed to broadband communications and high-speed communication services with the OSP and OCC VSAT stations via the airtime provider VSAT network.

The VSAT system with dish and transceiver equipment at both OSP and OCC locations must be connected to the substation LANs via IP connections as shown in Figure 5

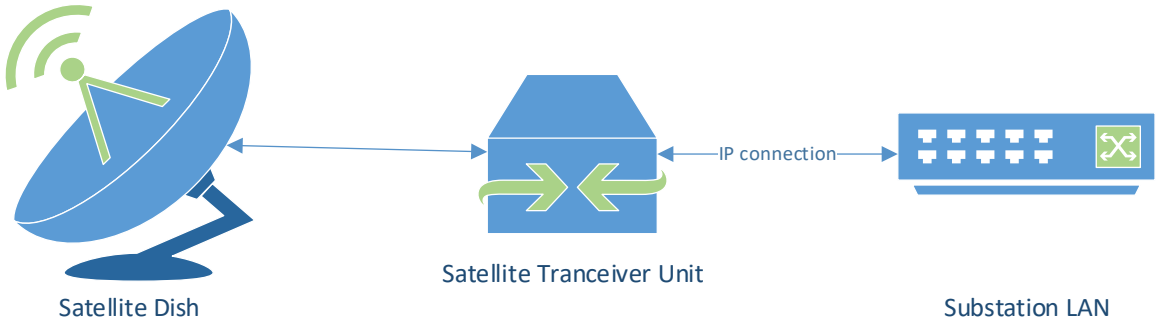

Figure 5 - VSAT substation setup

Required bandwidth and airtime provider shall be specified during the basic design phase of each OSS platform.

6.13 CLOSED CIRCUIT TELEVISION (CCTV) SYSTEM

An integrated IP based closed HD CCTV system shall be provided at the OSP and OCC for the following functions:

- Security surveillance: Continuous perimeter surveillance, Surveillance on all gates and entrances to the buildings, compound, perimeter intrusion verification and Access verification. In addition, at the OSP to monitor vessels approaching the platform.
- Plant surveillance: monitoring of equipment so that abnormal plant behaviour can be identified allowing early intervention.
- Personnel surveillance: (if required) The monitoring of staff working at OCC or OSP so that their safety and well-being is monitored.

Location of cameras and their types shall be reviewed by EirGrid.

A CCTV system generally consists of various types of equipment, such as cameras, video storage system, video displays, a video management system, and a media server.

The CCTV system shall be connected to the LAN via an IP connection. The operational and plant monitoring CCTV system and security surveillance CCTV system shall be designed to use 2 separate VLANs on the LAN.

CCTV stations with dedicated screens shall be placed in all control rooms.

Moreover, the camera interface shall be integrated into the Transmission SCADA and thus available on all the operator workstations including the Remote-Control Centres. Beside the Transmission SCADA integration, a web interface and direct client connection are also available.

A prioritised system of access to control each camera is required, with local customisation of user group priority levels.

The CCTV surveillance system shall form part of the security system specifically the intruder detection system (IDS, if applicable), by providing visual monitoring of perimeter fencing and entrances through wide area (thermal) cameras installed at specific locations. The usage of thermal cameras is optional. These must be used when the light intensities are expected to be too low to provide high-quality camera images. The system should include automated video content analysis or video analytics capability.

The surveillance system shall provide a fully interactive alarm management and archiving facility.

The recommendations of BS-EN 50132-7 (Alarm systems – CCTV surveillance systems for use in security Applications – Part 7 Application Guidelines) shall be adhered to in the installation and commissioning of the CCTV system.

To fulfil EN requirements the security systems the Customer shall ensure the following is submitted on the completion of the installation:

- Full technical supporting data of all the equipment and cameras
- Schematic diagram showing the inter relations between items of equipment and the configuration of proposed hardware

The cameras in general shall be capable of remote control to cover defined areas of the plant, have sufficient zoom capability to provide detailed views, and operate in the visible light spectrum and infrared spectrum (for thermal imaging of the equipment).

The camera coverage should cover equipment without blind spots and, where appropriate, should be of shielded EMC type. For OSP/OCC outdoor surveillance, the CCTV design requires the deployment of a combination of different types of surveillance systems e.g. fixed and Pan, Tilt and Zoom (PTZ) High Definition (HD) cameras.

PTZ HD CCTV cameras are installed to enable the full surveillance of the site remotely. Fixed HD cameras shall be used to provide continuous surveillance on selected access points to be reviewed by EirGrid e.g. gates, doors to buildings etc.

The surveillance system shall be capable of producing live and recorded images with time and date stamp. Minimum acceptable images required are Recognition Level images (image fills 50% of the monitor screen).

PTZ: The PTZ camera and lens must be compatible with Video Management System (VMS). The camera must be suitably equipped for mounting on 4m de-mountable CCTV poles and building corners for servicing and maintenance.

External Fixed Camera: The Fixed camera must be compatible with the security management system. All fixed cameras shall be vandal resistant devices suitably equipped for mounting on 4m CCTV poles or building.

Dome type cameras, where used, shall be constructed using clear non-scratch replaceable polycarbonate dome inserts to conceal and protect the camera and components.

Cable entry shall be from the back with no conduit knockouts on the sides, to maintain the integrity of the housing. The housing shall be brushed aluminium.

Furthermore, the following CCTV specifications also apply:

- All CCTV images on site shall be recorded onto a Network Video Recorder (NVR) with sufficient TB memory to facilitate 31 days recording at 11 FPS (minimum storage capacity on site.
- Recorded CCTV images shall be accessible locally and remotely.
- Sequencing and switching of CCTV cameras shall be user programmable remotely and automatically switched for repeater monitors.
- Intercommunication shall be provided between CCTV cameras and PIDS, Intruder Alarm System and Access Control system and shall enable PTZ cameras and fixed cameras to automatically present images of areas in alarm through the security management system to relevant CCTV monitor(s).
- CCTV images shall be recorded at a rate of 11 Frames Per Second (FPS). However, in the event of an alarm activation, CCTV images shall be programmed to record at a rate of 25 FPS.
- Resetting of the recording rate shall be executed through CCTV controls (including remotely).
- The primary control and monitoring position shall be from a remote EirGrid control centre.

CCTV cameras in general shall have the following performance requirements:

- CCTV camera lenses shall use Auto-Iris and Vari-Focal lenses for precise adjustment.
- All motorised lens functions shall be fitted with limit switches.
- Full alpha-numeric camera / scene identification shall be provided to all pictures.
- All equipment and materials used shall be standard components.

The basic operation of the system shall enable all cameras to be live at all times, and record at all times via the system software. Additionally, at the OSP, CCTV cameras may monitor the following items or other relevant items determined by the Customer:

- Helideck (if applicable)
- Marine loading and crane operations.
- Muster point and lifeboat station
- An interface with WTG CCTV system is not required.

National and European privacy and data protection laws (e.g., Directive 2002/58/EC, Regulation (EU) 2016/679 (GDPR) regarding monitoring of workplaces by CCTV system shall be followed in design and installation of CCTV system equipment.

6.14 NETWORK VIDEO RECORDER (NVR)

NVR's shall be compatible with security management system. Customer shall ensure sufficient memory is provided to facilitate 31 days recording at 11 FPS (minimum).

Customer shall provide a Flat Panel LCD CCTV monitor for each monitoring location. CCTV monitor to have the following performance-enhancing features.

- VGA and DVI (digital visual interface) inputs
- PIP (picture-in-picture)
- Looping BNC output
- HD resolution
- Compatibility with multi-viewers

Flat panel LCD monitor shall provide a front panel that allows the user to adjust image quality, brightness, size, position, and geometry for optimal viewing. The flat panel MCD monitor shall meet or exceed the following design and performance specifications.

Minimum Electrical Specifications:

- Input Voltage - 1230 VAC, 50/60 Hz
- Video Input Interfaces - 2, BNC, looping; 1, S-Video, looping; 1, RGB; 1, DVI; 1, component
- Audio Input Interfaces - 2, audio L/R, RCA jack
- Horizontal Frequency - 31 kHz to 69 kHz
- Vertical Frequency - 56 Hz to 85 Hz
- Sync Format - PAL

Minimum Environmental Specifications:

- Operating Temperature 0° to 40°C
- Operating Humidity - 20% to 80%, non-condensing

6.15 PUBLIC ADDRESS / GENERAL ALARM SYSTEM (PAGA)

An IP-based (or hybrid) PA/GA system shall be considered for general announcements on the OSP. The announcements shall be done from the OSP local control room or control rooms at OCC or EirGrid remote control centre(s). The announcements should also be possible from any phone on the OSP.

The General Alarm system shall be used to broadcast audible Alarm tones to all parts of the installation. The Public Address system shall be used to broadcast Emergency Verbal Announcements which shall be intelligible in all parts of the installation where personnel may be present during normal operation and ambient noise levels permit. These areas shall include muster stations and survival life raft areas.

The Public Address system shall allow broadcasting of routine messages over the whole OSP (exterior and interior areas). Emergency and routine messages may be pre-recorded. The

facility to record the messages shall be provided with the ability to set and change priority hierarchy.

System shall be interfaced to fire detection and alarm system, telephone system and radio system. Coverage and sound level of all audible alarms and broadcast messages shall be in accordance with IMO document MSC/Circ.808, IMO Resolution A.1021, and project requirements.

6.16 MARINE SAFETY EQUIPMENT

6.16.1 AUTOMATIC IDENTIFICATION SYSTEM (AIS)

The OSP shall have Class A, type 3 AIS transponder as an automated autonomous system for the exchange of navigational information between suitably equipped vessels and shore stations using distinct messages and operating on two designated marine VHF channels. The system must be tested for interference with all other devices, and it shall comply with IEC 62320-2.

The AIS AtoN (Aid to Navigation) is an IALA/IMO/ITU/IEC 62320-2 compliant beacon that is designed to be installed on navigational hazards, offshore wind farms, oil and gas platforms/pipelines etc as well as fixed or floating aids to navigation such as buoys and markers, further enhancing their operation by alerting any AIS equipped vessels that are within range, while also providing additional data such as position, current status, real time warnings and reducing the risk of collision even in poor visibility.

It shall be confirmed with other vessels and OCC that they can receive AIS information correctly during the system commissioning.

Besides the international regulations, rules and standards, AIS shall comply with national regulations as well.

6.16.2 GPS PERSONAL TRACKING UNIT (PTU)

Personal tracking units or the Personnel Locator Beacon shall be available to any personnel who needs to be present within the vicinity of the offshore wind farm. The system shall comply with the Irish regulatory requirements.

7 FUNCTIONAL REQUIREMENTS

7.1 DATA ACQUISITION

The combined offshore and onshore Transmission SCADA system such as being present on the platform in the OSP as well as in the OCC and Remote-Control Centre shall acquire data from all (sub)systems including data from the Transmission SCADA system components as well as from data communication / telecommunication systems and networks.

The offshore/onshore Transmission SCADA shall acquire data by polling (master/slave relationship between the Transmission SCADA and the data source) and by spontaneous reporting (peer-to-peer). Data shall be transmitted by the source as a full report or by exception.

Data acquisition shall support the collection of Sequence-of-Events (SOE) data, i.e., time-stamped reports of status change events.

Any data value in the real-time database of the Transmission SCADA system shall be available for collection and storage into an historian database. Data stored into this database shall be

considered as archive or “off-line” data. The retention period, to be determined during detailed design, shall be the minimum length of time the data shall be kept on-line (real-time database). Data older than the retention period shall be transferred to historian database. The Customer shall provide a list with the retention period for each of the data items / groups defined during the design phase of the project for review by EirGrid. SCADA historian shall be available onshore and offshore where OSP historian can be a lighter version (see appendix A). Capacity shall be calculated based on the amount of selected datapoints and future needs by EirGrid.

7.2 DATA PROCESSING

Each bay unit shall be capable of processing data from the connected installations and from its own unit. The following types of data processing are to be supported:

- Status signals.
- Operating, control, monitoring signals.
- System signals.
- Alarms.
- Measured values:
    - Analogue measured values.
    - Digital measured values.

All alarms, indications and measurement must have a date and time stamping with accuracy of +/- 1ms.

As OSP and OCC are not going to be manned, the Customer shall ensure during the test phase (End-to-End test, FAT and SAT) that all type of signals shall be correct and available in Transmission SCADA at the Remote-Control Centre. This should include all LV distribution, outgoing feeders, MCB trips, all subsystems like AC UPS, DC Chargers, battery management systems, telecom systems, communication equipment, CCTV, fire control panel, etc.

7.3 CONTROL

The daily operation of the offshore substation shall be carried out from the onshore Transmission SCADA system consoles / workstations (normally from EirGrid Remote Control Centre(s)). The suitable selection of local/remote control shall be implemented. A software switch to manually override control hierarchies shall be implemented. Operations from the prevailing and underlying levels shall not be affected by the position of this switch.

It shall be possible to use the control system to initiate or block the controls for the primary and the secondary equipment. Control also includes the posting of warnings, the acknowledgement of alarms and accessing data and displays.

It shall be possible for all control operations in a bay to be carried out with the help of a menu-driven, graphic human-machine interface.

It shall be possible to cancel a selection made at any time easily. The selection shall be reset automatically if the subsequent command is not the right execution command or if this command is not received within a period of time to be defined after the selection is made.

7.4 USER INTERFACE

The user interface to the Transmission SCADA system shall be through full-graphic consoles (workstations) in both offshore and onshore local control rooms and in the EirGrid Remote-Control Centre. It shall be possible to view all the signals configured that come from the Transmission SCADA system. The signals shall be populated on various operator/user displays:

- Schematic or geographical single line diagram displays.
- Tabular displays.
- Summary displays.
- Trending and graphic displays.

Different types of displays (and maybe other types of displays as listed above as well) are required for the operator to operate the offshore substation platform.

As part of the HMI important signals, such as statuses, alarms, controls, etc) of systems and equipment, at least the following must be visible on the screens:

- All primary electrical EHV and HV plant should be visible and controllable
- Main LV switchboard including outgoing feeders should be visible and controllable
- Incomers to LV lower-level distribution should be visible and controllable
- Back-up DG should be visible and controllable, including remote testing facilities
- Statuses and alarms of all auxiliary systems

A sufficient number of screens should be provided in order to not overwhelm the operator. All displays, graphics, control and monitoring points must be reviewed by EirGrid.

7.5 MONITORING

Signals and measured values shall be monitored for the occurrence of changes in status, and limit values being exceeded or not met (alarms). It shall be possible to monitor all information, including status and numerical information as well as the data generated by the computer systems, the components of the Transmission SCADA system itself, and data communication / telecommunication systems and networks. The system shall generate a signal in each case given below:

- Limits being exceeded (numerical values).
- Change in status.
- Delay time being exceeded.
- Communication link failure.
- Occurrence of combinations of the above-mentioned states.

The failure or disturbance of a sub-system shall be displayed on the sub-system itself and at higher control levels. The overflowing of buffers or files shall be reported.

7.6 REMOTE ACCESS

In order to carry out limited remote monitoring it shall be possible to access the Transmission SCADA system information remotely via a secure web HMI interface. If HMI interface is not possible, a suitable alternative shall be proposed by Customer.

This remote access is for authorised users only to access Transmission SCADA from any remote location with an internet access. It is different from EirGrid Remote Control Centre.

The remote access shall include at least the status information, measured values, alarm lists, historical data as well as all read-only displays. These displays will show the actual status of the equipment and Transmission SCADA system. It shall also be possible to access data, which relates directly to plant monitoring, maintenance such as counter positions, statuses, etc. Exact details of what can be accessed remotely shall be developed and agreed during detailed design.

It shall be possible to access these facilities via a safe connection where it will not be possible to operate objects using this function. In cases where remote access to Web HMI devices is required, the VPN technology shall be used.

7.7 AUTHORISATION

User authorization shall be created by assignment of area of responsibility to a user and definition of the level of permission as either read-only, read/write, engineer, super-user (controlling program tuning and execution parameters), or maintenance permission level.

8 SYSTEM DESIGN

8.1 DESIGN LIFE

SCADA and telecommunications equipment shall have an expected lifetime of at least 25 years.

It is recognised that some Transmission SCADA related hardware and software may have a shorter expected design life. Hence, Customer shall list such equipment with a design life less than 25 years and propose a replacement strategy.

Customer shall ensure that all components can be replaced, modified or configured without loss of overall system functionality and without loss of power transmission capability.

8.2 GENERAL

The design produced by the Customer shall comply with EirGrid functional requirements and to the referenced international standards.

The Design shall be submitted for EirGrid review.

Any omissions, issues and/or non-compliances identified by EirGrid during the design review and construction phase shall be logged in the Design Review and Construction Monitoring comments logs.

All comments raised during the design phase shall be addressed and rectified by the Customer in revised designs submission in advance of construction commencing.

The Transmission SCADA and telecommunications systems design documents, drawings and calculations shall be submitted to EirGrid for reviewing.

The design requirements and environmental protection for equipment will be similar to those required for marine communication systems as many of the same hazards will be faced and the systems will cover the same safety role.

The I/O list, HMI design, data reporting, the type of equipment like displays and printers, their locations and the numbers shall be proposed by the customer for review by EirGrid.

9 HARDWARE

9.1 REQUIREMENTS

All hardware that is located in an onshore compensation compound and offshore substation shall be suitable for operation according to IEC 61850, IEC 60945 or any applicable standard from Table 1.

9.2 PLC AND IED

PLCs and IEDs shall be suitable for operation within a substation environment, be microprocessor based and provide a combination of functions including protection, monitoring, control, and automation. They shall be capable of automatic disturbance recording with settable pre-fault duration and user-defined triggering. They shall also allow Oscillographic Waveform Recording (OWR). They shall be connected to the Transmission SCADA servers using a redundant topology, using redundant network interface cards. They shall have no moving parts. They shall have a failure mode which will allow them to have their software updated remotely.

They shall have a self-check function and capability to be remotely reset/restarted.

They shall have two (2 x 100%) FO communication ports to support redundant Transmission SCADA communication.

The IEDs and PLCs shall be able to communicate via IEC 61850

9.3 SERVERS

All servers shall make use of redundant, hot-swappable power supplies, redundant hot-swappable disks and redundant communication cards. Where further redundancy is required, each server should have a redundant partner which is kept up to date, and to which it can fail without loss of operation.

The customer is allowed to use Virtual Machine (VM) based architectures in the system design, but only without prejudice to the stated hardware redundancy requirements

All servers shall have the capability to be remotely reset/restarted.

9.4 DATA STORAGE

Main data storage should be onshore. There shall be the ability to buffer data at the offshore location in a fault tolerant queue, but data should be transferred to the onshore data store as soon as there is a viable link. Recent data should be accessible from a console offshore in the occasion of a lost link to shore. Data storage shall be on a secure onshore location. The data should be backed up on redundant, hot swappable disks. The data shall be backed up every 24 hours. The data store and the backup data store shall be configured in such a way that data is stored on redundant storage media (e.g., duplicate disks) at all times. Backup media shall be rotated to ensure that if data does become corrupted, there is still a valid backup of good

data.

Data collection and processing servers should also be located offshore, so that in the event of failures in the connection to onshore, no data is lost and can be stored for a period of at least 96 hours.

Data storage, user interface and reporting servers shall be located onshore.

9.5 CONSOLES (WORKSTATIONS)

All the functionality of the Transmission SCADA system should be available onshore and at Remote Control Centre(s). Operation and Engineering workstations shall be provided at onshore and offshore control rooms for operation, configuration and diagnostics of the control system applications and other control system equipment.

In cases where the link is operating at a reduced bandwidth, priority should be given to displaying safety critical status information and the issuing of commands to the substation.

HMI should be accessible via the operator user interface and/or web user interface.

10 PHYSICAL INTERFACES

10.1 POWER REQUIREMENTS

All equipment shall be supplied from UPS power supplies with battery back-up. Any switch-overs shall not result in any downtime within the system.

10.2 COMMUNICATION REQUIREMENTS

Communication systems between all servers should be redundant and fault tolerant. Communications systems between BCUs / IEDs and servers should be fault tolerant and using industry standard protocols. All communications outside controlled enclosures should be shielded appropriately to work in wet (24h average relative humidity > 95%), or EMC environments.

Offshore servers and BCUs / IEDs equipment shall not have direct access to and shall not be directly accessible from the internet. Remote access to the offshore servers shall be through the onshore servers.

10.3 EQUIPMENT LOCATIONS

All servers and core communications equipment shall be located in the offshore and onshore local control rooms.

Workstations shall be placed in the offshore at OSP and onshore at OCC local control rooms and in the EirGrid Remote-Control Centre.

10.4 EQUIPMENT SIZES

All offshore Transmission SCADA and telecommunication equipment shall be of a size that it can be easily transported offshore fully assembled.

11 SOFTWARE

11.1 GUI (GRAPHICAL USER INTERFACE)

All user interfaces shall conform to IEC 60445.

User interface technology is likely to change over the lifetime of the project so the user interface that is presented to remote users should be independent of the rest of the system. Interfaces between the user interface and the rest of the system should be via industry standard protocols.

11.2 ALARM MANAGEMENT

A list of all active and historical alarms shall be available to the user. The user shall have the option to configure the alarm user interface as needed, for example defining alarm levels and priorities, alarm responses, alarm categories, etc. High priority alarms shall be highlighted on the user interface. Selected users shall have the rights to acknowledge each alarm. An alarm shall remain visible after being acknowledged until it is resolved.

11.3 REPORTING

All data stored within the system shall be available for reporting. This will include status and analogue signals, derived signals, user input signals, alarm signals and configuration items. Reports shall be able to run over a period which covers the lifetime of the project. All data from different sources shall be time-stamped using a time source that is common throughout the system.

11.4 DATA STORAGE AND BACKUP

All alarms, events, commands and relevant analogue signals must be stored by occurrence.

All data items must be temporarily buffered locally for a period of at least 96 hours before being stored in the historical database. All data must be kept in the historical database for a period of 60 months.

It shall be possible for EirGrid to extract data from the historical database via software communications.

11.5 DATA LOGGING

All the relevant systems and applications shall provide automated change logging and change attribution, The log entries for events shall include a timestamp, an event description, and the role causing the event. Events caused by engineers are linked to individual users.

11.6 SOFTWARE CHANGE CONTROL

No software shall be set to accept automatic updates. All changes to the software shall be through a change control process provided by the Customer which includes regression testing of the system. This includes operating systems.

Customer shall propose a software for detection and protection against viruses and malware for review by EirGrid. The software shall be installed and running throughout the development, test, commissioning, and acceptance of the system to ensure that its performance impact is known and tested. The software shall operate in a manner not having noticeable interference

with Transmission SCADA operations.

Procedures for the secure updating of configuration and signature files are to be provided, to ensure that the tools remain current with updates and releases and under tight control of the EirGrid's staff. Customer to further refer to the OFS-GEN-017 Cyber Security Systems specification document.

The Customer shall ensure that the servers and PCs shall be subject to periodically security patching of the OS. Security updates shall not be automatic and must be authorised by EirGrid.

11.7 LICENSING

All software shall have a valid license which ensures that its use is legal.

12 PHYSICAL PROPERTIES

12.1 DIMENSIONS AND WEIGHT

All servers shall be sized to fit in the space made available for them in the local control rooms on the platform and onshore compensation compound. Equipment weight shall be kept to a minimum.

12.2 RUGGEDIZATION

All equipment shall have coatings, enclosures, connections, ventilation, cooling, and heating appropriate to its location. In particular, equipment shall be protected from excessive humidity and salt spray environments. All equipment and connections shall be able to withstand shocks, vibrations and interference that would be expected to occur during the lifetime of the project.

The degree of ruggedization shall depend on the environment available to house the equipment; however, a combination of the equipment and its housing should be able to withstand the conditions it shall encounter both offshore and in a substation.

13 OPERATIONS AND MAINTENANCE

13.1 REQUIREMENTS

The requirement of any operations and maintenance regime is to ensure as close to 100% availability as possible. Inspections and monitoring should be designed to predict failure as well as alert of failure.

13.2 MODULARITY AND REPLACEMENT

All interfaces between components of the Transmission SCADA system and between components of the telecommunication system shall be via industry standard protocols. This will allow the replacement of components with similar components if a component of the original specification is not available.

Wherever possible the same transport media should be used throughout the whole telecommunications network. For example, if multi-mode fibre optic cables are used for parts of the substation LAN, then this should be used for all parts. This will allow the replacement of components with similar components if a component of the original specification is not available.

Each component of the Transmission SCADA and telecommunications systems will continue to operate when disconnected from the rest of the system. A disconnection may not lead to

failure of the component, so that when reconnected the system shall work immediately. Any data collected when the rest of the system is disconnected shall be buffered so that it can be retrieved once a connection is restored.

13.3 INSPECTION AND MAINTENANCE

The system should be self-monitoring. Alarms shall be raised when any component fails or loses power supplies. Alarms shall be raised when any component is subjected to conditions outside its tolerance. Information on the operating environment and operating conditions shall be stored along with the rest of the data so that condition monitoring of the system can be undertaken.

The Transmission SCADA and telecommunications design should consider operation and maintainability including routine visual inspections by operations staff. The Customer shall propose an inspection plan, a business continuity plan and an emergency preparedness plan. As part of it, all safety critical voice communication devices should be regularly tested for correct operation. All portable device charging points should be monitored.

The Customer shall consider expected maintenance and component failures for a period of 5 years.

The Customer shall recommend how to store all parts and consumables in accordance with local climatic conditions to prevent degradation (e.g., corrosion).

Standardised and interchangeable components shall be used for the scope of supply wherever the applications permit.

Components which are subject to replacement shall be interchangeable. The Customer shall demonstrate this capability regarding the possibility to carry out these works offshore, tools necessary, personnel and training/knowledge required.

All parts which are liable to deterioration by atmospheric pollution, humidity or ingress of foreign matter shall be totally sealed in appropriate packaging, suitable for long term storage. All parts which are subject to deterioration due to condensation shall be additionally protected by packs of silica gel or other approved desiccants. Packages shall be crated in robust waterproof and protective wooden packing cases. Large items shall be crated separately and shall be securely clamped against movements. Each packing case shall be clearly labelled, with the label providing the following information:

a. Part name
b. Description of serial number of contents
c. Lifting and storage / stacking instructions
d. If multiple cases pertain to an individual joint or termination, then the relationship must be clearly labelled e.g., box 2 of 3.

The complete documentation required for installation (installation instructions, part lists, hazard and safety data sheets, technical drawings) shall also be attached to the packaging.

If the case contains fragile parts, it should be clearly indicated on the label and on the crate.

13.4 SPARES

The Customer, in consultation with their OEM's, shall list all recommended spare parts.

All recommended spare parts shall be provided with associated drawings and instructions.

Refer to OFS-GEN-009 for more details. .

13.5 TOOLS

Tools (software or hardware) shall be located or readily available at the appropriate location to allow access and replacement of all Transmission SCADA and telecommunications equipment. Transmission SCADA and telecommunication equipment enclosures should be designed to reduce the number of tools required for servicing, while maintaining security and environmental protection.

The Customer shall supply any special tools and/or test equipment required to perform the installation, commissioning and lifetime operation and maintenance of the Transmission SCADA and telecommunication systems. Such tools shall remain with EirGrid after handover. The Customer shall provide a suitable storage facility for this equipment (where the tools are required).

The Customer shall provide a list of any specialist equipment necessary for the operation and maintenance of the entire Transmission SCADA system and related equipment. An adequate number, including spares, of each tool or piece of equipment shall be supplied by the Customer.

The Customer must ensure that all necessary data and working methods, such as passwords, folder structures, maintenance tools, back-up files, are properly transferred to EirGrid at the time of handover.

14 ENVIRONMENT

14.1 GENERAL

It is expected that most of the Transmission SCADA and telecommunications equipment (gateways, switches, servers, etc) shall be housed in an environmentally controlled local control room. This room shall provide protection from the corrosive environment found offshore and near shore as well as EM interference. This room shall be normally locked to provide data security.

The environmental conditions for most of the Transmission SCADA equipment on an offshore substation shall be the same as for an onshore substation. For Transmission SCADA equipment that is not housed in a controlled environment, particular attention must be made to protecting the equipment from humidity and salty environments.

Connection points are particularly susceptible to corrosion in humid environments. Connections should be made inside a controlled environment. No metal joints where different metals meet should be exposed to high humidity or salt. Cable entry points to environmentally controlled enclosures should be made to ensure that the environmental seals are not broken.

Standards for protecting computer equipment at sea are contained in IEC 60945.

14.2 LOCAL CONTROL ROOMS

Customer shall provide local control rooms onshore and offshore that are lockable spaces

which are temperature and humidity controlled to a standard suitable for the equipment located in it. The room shall also be shielded for RF interference suitable for the equipment that is located there. Since these rooms are also a place of work, suitable climate control must be installed to conform to the relevant health and safety at work requirements.

The Customer shall supply and install the Operator's desks and chairs.

The Customer shall provide and install all equipment/cabling required for VDU configuration, mouse and keyboard, so as to implement the HMI in the substation control rooms.

Typically 2 x 24" monitors shall be provided per workstation. However, this may be enhanced if there are task specific requirements.

The Customer shall provide and install all equipment/cabling required for the hardcopy printer in the substation control rooms.

The rooms shall have two independent power circuits for powering redundant equipment. These will be labelled to indicate which power sockets are on the same power supply.

The rooms will be large enough to house the communications equipment in one or more racks with clear access to both front and rear of the rack.

Layout of the rooms, locations and number of operator workstations, workstation equipment, other equipment shall be reviewed by EirGrid.

14.3 SECURITY

Any equipment located outside the locked control room will have a lockable cover.

14.4 COATINGS

Devices and cables which shall not be in a controlled environment will have a coating which protects their operation from environmental conditions according to standards IEC 61850-3 for equipment and IEC 11801 for cables. Particular attention must be paid to protection from humidity, salt and electromagnetic conditions found within substations.

14.5 VIBRATION AND ACCELERATIONS

Vibration and acceleration sensors shall be delivered with Transmission SCADA system in the OSP control room. These will be calibrated to send an alarm if the vibration or acceleration conditions exceed that of any equipment located in the room.

Shock recorders and acceleration detectors shall be included within the Customer's scope of supply and attached to all relevant components for transportation.

Maximum acceleration values shall be as per manufacturer's recommendation and shall not be exceeded.

14.6 STORAGE AND TRANSPORTATION

All equipment shall be transported according to OEM's recommendations, in suitable watertight packing that will protect it from environment, impacts and vibration beyond its designed tolerance. All equipment shall be transported fully configured and fully assembled where possible in order to reduce installation time.

Where required, suitable transport fixtures shall be provided by the Customer.

Where required, the Customer shall supply monitoring equipment to measure and verify that equipment limits have not been exceeded during transportation.

Quality of materials shall be ensured during transportation, handling and storage.

14.7 INTERCHANGEABILITY

Standardised and interchangeable components shall be used for the scope of supply wherever the applications permit. Wherever possible, equipment shall be of a standard type, so that the equipment in a non-critical part of the Transmission SCADA system can be cannibalised to repair the equipment in a critical part of the Transmission SCADA system. This means that the same mode of fibre should be used for all fibre optic communications, as well as the same grade of network switch, and cables for any copper network. Mobile devices should have a common power connector for recharging, and recharging stations should be available at all platforms within the site.

Components which are subject to replacement shall be interchangeable. The Customer shall demonstrate the use of standard interfaces and connectors through the definition of appropriate work procedure(s) in the O&M manual.

15 TESTING

15.1 GENERAL REQUIREMENTS

The Customer shall submit to EirGrid method statements, inspection and test plans (ITPs), procedures for the FAT, installation, SAT, functional, end-to-end tests and commissioning of the system for review before any testing or installation work commences at the factory or on site / fabrication yard.

The documents described above shall be provided in sufficient time to allow a full review by EirGrid.

All devices shall be supplied by their manufacturer pretested; however, each device shall be verified for correct operation before being shipped to site (offshore or onshore). All equipment must be tested for interference from other equipment.

All individual components shall be tested separately to ensure functionality, robustness, and fault tolerance. Particular attention shall be paid to testing for fault tolerance in any external interfaces.

Testing shall take account of normal operation as well as fault conditions.

Software shall be white box tested so that complete code coverage is achieved.

Any failure mode software shall also be tested to ensure complete code coverage.

All system installation and testing work shall be carried out in accordance with the manufacturer’s procedures, reviewed by EirGrid. The Customer shall advise EirGrid well in advance of commencement of any works so that a representative may be made available to witness the works and provide a document submittal schedule.

EirGrid will witness the tests (FAT, SAT, end-to-end) and the commissioning.

15.2 FACTORY ACCEPTANCE TEST (FAT)

The complete Transmission SCADA and telecommunication system, including functionalities, interfaces, inputs / outputs, shall be tested at the factory during the FAT. Failure modes should be tested. Testing should be carried out on the actual components that shall be used within the system. Tests should be carried out against a specific, identifiable build of software. The software build shall include any configuration files.

No changes to the software build or any configuration items shall be made during or after the test without performing a regression test which demonstrates that the system is still fit for purpose.

All FAT test results should be recorded and submitted to EirGrid for review.

15.3 END-TO-END TESTS

All data inputs and outputs to the Transmission SCADA system shall be tested for accuracy and calibration.

All physical and wireless (backup) connections shall be tested for correct operation.

All signals for the remote-control interface shall be tested.

All fibre optic terminations should be tested, those that are not initially in operation. The Customer shall provide OTDR reports for every installed fibre, even if these are not in use.

Data speed tests and switchover between data links should be tested.

All safety critical voice communication devices should be tested for correct operation (including all charging equipment).

All E2E test results should be recorded and submitted to EirGrid for review.

15.4 SITE ACCEPTANCE TEST (SAT) AND HARBOUR ACCEPTANCE TESTS (HAT)

The Customer shall perform site acceptance tests on a fully assembled platform, including all communications systems. The system shall be in full operation with all connection to the process and every connection and data exchange in operation. This means that SAT shall be performed on the system in the state it is intended to operate in the years to come. The SAT can be done at Harbour as HAT. If the SAT is carried out prior to the platform being sent offshore, then an in-situ set of tests must also be performed. This may be done to limit the time personnel spend offshore testing a normally unmanned platform. The placement of any VHF radio or radar equipment, including antennae, should be tested for interference from the substation equipment.

The SAT shall include but is not limited to:

- Verification of equipment delivered.
- Verification of installation work.
- Verification of software delivered.
- Verification of data and functionality.
- Verification of data communication and interfaces.

- Verification of physical interfaces.
- Verification of documentation.
- Verification of capacity and response time.
- Verification of signal for remote control.
- Verification of operation of the Transmission SCADA.
- All functional and loop tests

All SAT test results should be recorded, and all documentations shall be submitted to EirGrid for review.

SAT / system acceptance shall not be accepted until 100% of I/O (inputs / outputs), system functionally and components are verified and checked in operation including integration of the onshore remote centre, OCC and OSP Transmission SCADA components and loops

15.5 COMMISSIONING

The Customer shall provide a certificate, test records to EirGrid detailing all testing, and checks carried out in the pre-commissioning phase and a statement of full compliance of the system with approved drawings and Specifications.

Commissioning of the full integrated system shall be arranged and managed by the Customer and demonstrated to EirGrid as witness.

EirGrid may request further inspections, tests as deemed necessary, during review of the ITP and test procedures. Any such inspections or tests do not absolve the Customer from full responsibility for ensuring the satisfactory completion of the works.

The Customer shall engage with EirGrid for details of the specific test equipment requirements.

As part of the commissioning, the Customer shall carry out any necessary remedial work within the frameworks and timelines as included in the test plan reviewed by EirGrid. The repaired work shall be submitted to EirGrid for review.

15.6 REJECTION OF MATERIALS

If any item's functionality or testing fails to comply with the requirements of this specification in any respect whatsoever at any stage of manufacture, test, assembly or on completion at Site, Customer shall be responsible for rectification works so that compliance to the standards, project specifications is achieved.

16 DOCUMENTATION

16.1 DOCUMENTATION PLAN

At the start of the project, the Customer shall provide a project documentation plan/list (Master Document Register and Supplier Document Registers), for review by EirGrid. The documentation plan describes at least:

- The documents, drawings that shall be delivered in each phase of the project.
- The delivery and review process including deadlines.

- A RACI table with responsibilities.

The documentation lists must be complete and therefore includes all documentation to be supplied by Customer as well its contractor's suppliers.

16.2 TEST CERTIFICATION

A test certificate should be issued for the entire system upon leaving the factory and upon installation.

A test certificate should be completed for each component within the system which demonstrates that the component is as per design specification.

If any components are changed within the system, then that component should be supplied with a module test certificate, as well as a system regression test certificate.

16.3 DOCUMENTATION

Documentation shall be provided for each item of equipment and shall include at least the following:

- Functional and architectural design documentation for all OSP/OCC equipment and networks, including signal list.
- Technical descriptions (including circuit diagrams, schematics, block diagrams, general arrangements, functional descriptions, I/O list, equipment datasheets, cable routes, etc.).
- As built documentation.
- Network setup specifications (including firewall settings, VLAN setups, etc.).
- Inspection and Test plans, test books and test procedure for all test phases (FAT, E2E and SAT).
- Installation instructions including any usernames and passwords.
- Commissioning instructions, test protocols.
- Parameterization and diagnoses description.
- Maintenance instruction manuals (both preventive and corrective maintenance).
- Operating and system instructions.
- Software system functional descriptions and design.
- Software licenses and update procedures.
- Hardware specifications for all hardware.
- Software engineer's user manual.
- Design, installation, and commissioning strategies
- SCADA display plans
- Alarm and Events Lists

- Cyber Security Risks' Assessments
- Cyber Security Safeguard Testing Plan
- Hardening details
- Back up restore and recovery processes, Testing certificates for all cables (including OTDR reports for fibre optic cables).
- Recommended maintenance tools list.

FAT, pre-commissioning and commissioning records.

17 TRAINING

The Customer shall submit a training plan which shall describe in detail how the Customer proposes to train EirGrid staff for operation of future EirGrid assets.

Training requirements will be detailed further in OFS-GEN-009 - Operation and Maintenance General Specification.

18 APPENDIX A – INDICATIVE TRANSMISSION SCADA ARCHITECTURE AND DATA FLOW OVERVIEW

Note that the below system architecture is high level and is to be used as a guidance. It does not cover all the systems. Different interfaces may be proposed. Project specific, comprehensive Transmission SCADA system architecture to be developed and proposed by Customer. The extent of control and monitoring capabilities and communication connection details of EirGrid Remote Control Centre(s) to be defined during details design phase. The below architecture does not show these details. The network architecture must fulfil all requirements of the specification and relevant international standards, for example in the field of redundancy, availability and cyber security. It is therefore up to the customer to come up with a design that meets all requirements. Which network components should be redundant and to what extent or how the network segmentation should look exactly, where firewalls should be placed, etc. are issues that must be solved by the customer within the design and within the framework of this functional specification.