Section 6 Employer Requirements

Attachment E – SCADA and Controls

# Definitions

Unless explicitly stated in this document, or the Contract, definitions are as per the Standards.

# Standards

All equipment shall be installed, and all work shall be carried out in accordance with statutory requirements. Where explicit regulations are not applicable, all equipment and works supplied shall conform to the latest editions of relevant international standards (as at the time of Tender). The following order of precedence shall apply[[1]](#footnote-0):

* Australia/New Zealand standards (AS/NZS)
* International Electrotechnical Commission (IEC) standards, and International Standards Organisation (ISO) standards
* Institute of Electrical and Electronics Engineers (IEEE) standards

Key standards include, but are not limited to:

* AS 3000 The Wiring Rules
* AS 60870 Suite of Standards that defines Telecontrol equipment and systems
* AS/NZS 3947 Low Voltage Switchgear & Control gear
* AS/NZS 61439 Low Voltage Switchgear & Control gear Assemblies
* AS/NZS Lightning Protection
* IEC 61724 Photovoltaic system performance monitoring
* IEC 62351 Cyber Security Series for the Smart Grid
* IEC 62443 Series for security for industrial automation and control systems
* IEC 62446 Photovoltaic (PV) systems - Requirements for testing, documentation and maintenance
* IEEE 1815 IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)

In case the equipment or materials offered from a country where the relevant standards to which the equipment or materials offer better performance or safeguards for Solomon Power than the relevant AS/NZS, IEC, ISO, or IEEE specifications, these are acceptable. The Contractor must substantiate any such claims by submitting an independent assessment by an appropriately qualified person that identifies differences in the standards and demonstrates the benefit for Solomon Power.

All listed standards must be complied with unless an exception is granted by Solomon Power.

Standard(s) referred to shall mean the current Edition / Revision together with Amendments issued.

All installations, materials and cabling shall be in accordance with AS 3000.

# Scope of work

The Contractor has a single responsibility for delivery of all SCADA of plant required for the operation of the entire project facility, including but not limited to solar PV plants, Battery Energy Storage System (BESS) and substation. This includes the design, documentation, certification, supply, delivery, installation, testing and commissioning of balance of plant works, meeting the functional requirements of this specification.

The scope shall also include training and capacity building of local staff to operate and maintain the system as well as provide warranties for equipment and workmanship and performance guarantees and defects liability for the complete system as a whole.

The works shall include but not be limited to the following:

* Compatible connection to the Solomon Power SCADA network for SCADA, protection and communications use.
* Site SCADA system, including local HMI and historian.
* SCADA system ancillary systems and all required communications links.
* A cyber security assessment.
* Integration to the site maintenance building, including at the operator workstation, at Ambu Solar Hybrid and Henderson Solar PV.

This scope of work does not apply to solar school projects, where instead, proprietary control and communications, including web-based monitoring, associated with the selected equipment shall be used. For solar school projects, each building shall be provided with a terminal to monitor system performance and identify faults.

# Architecture

The site SCADA system shall accommodate all site plant and equipment such as solar PV plants, BESS, substation, weather stations and remaining balance of plant.

A robust site wide SCADA network shall be implemented, with redundancy and no single point of failure. The SCADA system and associated network shall be built with open protocols and standards to seamlessly integrate all the major elements on a single user-friendly platform. Where possible, Ethernet will be used for both SCADA and Engineering Access to all devices.

The SCADA system shall interface to and respond to network dispatch and control commands over the existing optical fibre systems. A cellular connection shall also be provided for remote access purposes.

This shall be in accordance with all relevant grid rules, network dispatch requirements, connection agreements and all applicable regulations, permits and standards.

The Contractor shall allow for complete and compatible connection to the Employer’s SCADA for protection and communications use.

# Technical requirements

## General

The basic function of the SCADA system is for continuous acquisition of data from the plant and its systems (including the substation, BESS, inverters, meters, weather station, sensors and other local processes) for monitoring and reporting purposes as well as the manual and automatic communication of instructions to control the operation of the Plant.

The systems shall comprise of:

* Specific control and monitoring hardware (including server, data loggers, RTUs, gateway, cabling, connectors, etc.) with industry recognised communication protocols and specific UPS capability.
* A local area network to allow the reliable and secure communication of data between the local components of the monitoring system.
* A local database hosted on an onsite server to receive, consolidate and store information in real time supported with the UPS.
* Applications to process the received data, run calculations, manage alarms and present information to users.

The main features shall comprise:

* Ability to collect, store, send and receive operational data information in real time.
* Industrial-grade with proven reliability in continuous applications and with multiple communication ports.
* The system shall use reliable and established communication protocols used in the electricity generation industry (e.g. Modbus, DNP3/IP, IEC61850, IEC60870, etc.).
* SCADA network redundancy and recovery features which ensure that the failure of individual components or the loss of power does not affect the functioning of the system. Including the protection switches, SCADA network switches and redundant ring topology for the PV plant.
* The SCADA database can be referenced and accessed from a standard third-party application.
* A full set of alerts and alarms for all the plant components will be programmed into the system, along with a set of standard procedures for response and solution of incidents.
* The control system also stores and files historic data, which can later be consulted and analysed by the system operators and can be exported to commonly used file formats, e.g. xlsx, csv or txt.
* The system administrator will have full control over access to the system with differentiated authorisations controlled by usernames and passwords.
* The control system will have a ticketing application that will issue text and e-mail messages to operators and defined users to communicate errors, incidents or anomalies that require their intervention.
* The system will have a set of pre-configured reports and sufficient flexibility to permit simple configurations of new reports based on existing data models. Reports will be exportable in at least one of the major formats, including Word, PDF, XLS, CSV, etc.
* The system must be capable of being an (S)NTP or IRIG-B client to ensure correct time synchronisation with the grid, security system and the Plant’s operators.

The SCADA system shall be capable of being accessed remotely to examine and retrieve both real-time and historical data. The SCADA system shall log and store all facility data locally for a period of at least 60 days.

A HMI must be available at each site. All supervisions of that site facility must be able to be undertaken by this HMI.

The SCADA system will record and report all necessary operational details. The software will be capable of undertaking availability and performance ratio calculations of the facility and providing daily, monthly and yearly operation reports.

Communication cabling between the site and Employer’s SCADA will be via fibre optic cable. Communication between the inverters, BESS and control room will also be by fibre optic cable.

All SCADA modules and HMIs shall be supplied by an uninterruptible power supply (UPS) to provide at least four (4) hours of power in the event of a grid failure. Should the SCADA system fail, the individual inverters, PPC, meteorological stations, and electrical systems shall continue operation unless such operation compromises the safety of the equipment (or as specified in the relevant Attachments).

## Functionality

The SCADA system will have the following functionalities:

* Remote internet access via a high-speed broadband connection (such as 3G, 4G or optical fibre) to permit remote monitoring.
* Following a loss of grid or auxiliary supply or the communications system to a PCU/BESS, store data locally in non-volatile memory at that PCU/BESS and resync this data automatically with the main SCADA server when communication is re-established.
* Data at each PCU/BESS will be stored locally for a period of 60 days or more on one or more SCADA servers. Following the expiration of this time period, the oldest data shall be overwritten. The SCADA system must provide an alarm to the remote operator following the loss of communication with a device.
* The SCADA system allows remote access with varying levels of user access.
* The SCADA system remotely monitors the PCU/BESS MV circuit breakers.
* The facility will continue to run unaffected in the event of minor or critical failure of the HMI.
* Virus detection and removal software are provided for all PC-based systems.
* Sufficient security will be provided to protect the system from unauthorised access.
* A control release prompt (two step operation) will be implemented to prevent accidental operations from the screen and or keyboard.
* A maximum response time of 1.5 seconds (from given command to feedback) to be maintained.
* Data from the SCADA system will be time-stamped, displayed in tabular and graphical form and exportable to common file formats such as TXT, CSV or XLS.
* SCADA system to be capable of recording intervals of 1 second.
* A minimum of 60 days of data will be available on the local SCADA servers before archival to the historian system. The data in online storage will be automatically transferred to archival storage on a periodic basis.

## Miscellaneous

The SCADA system shall also allow for the following general requirements.

### Data transfer to Third Party Server

The monitoring system will provide the option of interfacing to a third-party server on site for forwarding specific data from the provider’s server to an off-site server on a real time basis using Modbus TCP protocol.

### Data storage

All data will be stored on a data server onsite as well as a secured offsite server, to be agreed with Solomon Power, with a minimum storage capacity of 25 years and continuous backups to guarantee availability of all data throughout the entire lifetime of the Project.

### Secure remote access

Remote access to the SCADA system will be implemented through a secure VPN connection and Firewall. An appropriate data traffic protocol (i.e. QoS) prioritises the available bandwidth to ensure critical data is communicated with the highest priority. An automatic failover system is to be implemented to switch over between the primary and secondary internet connections when required.

### Self-diagnostics

The SCADA system equipment and all control devices shall be provided with a self-diagnostic feature that all the system components are monitored and alarmed appropriately. Diagnostic alarms shall include the following as a minimum:

* Power supply health check
* Diagnostics of each module
* Communication health monitoring

### Spare capacity

A minimum of 20% spare capacity shall be provided for each element of the SCADA system, including both hardware and software.

### Expandability

The SCADA system shall be designed and configured to perform future modifications with minimum interruption to the system. The data model shall have the capacity to integrate future equipment and capacity.

### Interoperability

The IEC61850 features of the SCADA system and control devices shall be designed and configured such that these devices can be swapped with other manufacturer devices as per the interoperability requirements specified in the IEC61850 standards.

### Control hierarchy

The plant control is performed from the following four levels:

* **Field Equipment:** This level allows control of equipment from its local marshalling/control box fitted on/with the equipment. The control operations performed at this level are only allowed if other means are not operational.
* **Control Panels:** These are located at the relevant control panels, and control operations can be performed from control switches installed in the control panel.
* **SCADA System:** All control operations are executed from the SCADA HMI computer and sent to equipment via SCADA Servers.
* **Remote Location:** This is from the Contractor’s control centre or from Solomon Power’s dispatch and control centre, from where monitoring and control of the plant is performed.

### Control and interlocks scheme

The SCADA system shall provide control of the following equipment at minimum:

* Circuit breakers and disconnectors.
* MV switchgears at the Solar PV and BESS.
* Plant generation (active power, reactive power and voltage) control.
* Inverter/BESS control (on/off).

The circuit breaker, isolator and earth switch interlocking shall be managed in the hardwired control circuits or relevant IEDs, interlocks shall not be performed by the SCADA system.

All soft signals which are used for BESS/inverter interlocking or controls shall have watchdog monitoring configured for secure operation.

## Cybersecurity

All site control, security, protection and communications systems shall be designed and implemented in accordance with IEC 62443 and IEC 62351.

As per IEC 62443, a detailed cyber risk study (Cyber-HAZOP) shall be completed, documenting each zone and conduit of the systems. A detailed risk Assessment must be completed with control measures that shall be incorporated into the final design and testing documentation of the systems.

### Security requirements

The most important security requirements that shall be considered during the design/commissioning of all equipment connected to the site network are:

* Authentication and authorisation of the users.
* Assurance of the integrity of the transmitted data.
* Protection against viruses, Trojans, and other malware.
* Collection and saving of log files.
* Operation of the system in a protected environment (physical security).
* Every user is given only those rights that are necessary to fulfil the corresponding work.
* Requirement to change password after a defined period of time.
* Assurance that in case of a system failure, a restoration is possible without or only with marginal data loss.
* Only activate required services and ports.

## UPS and auxiliary systems

All SCADA equipment must have an uninterruptible power supply (UPS) source to provide power in the event of a grid failure. The system must have autonomous power for at least four hours in case of loss of the main electricity supply to the system and be able to recover data from the local equipment (data loggers, PLC, meters) as soon as communication has been restored. The UPS capability shall be extended to 24 hours for the pyranometer collecting the horizontal irradiance and at least one of the pyranometers collecting the global plane of irradiance.

The Contractor must demonstrate capability in order to be deemed compliant with minimum UPS storage requirement.

# Quality management

## Factory acceptance testing

In addition to the overarching quality management requirements, the below are typical testing requirements to be provided by the Contractor as part of the scope of supply.

### Scope

The following equipment shall be tested at the manufacturer's works prior to delivery to the site:

* SCADA panels.
* Communication panels.
* SCADA servers, HMIs, and associated control interfaces.
* Managed Ethernet switches.
* Router/Firewalls.
* GPS clock and time synchronisation.
* All ancillary items associated with the SCADA system.

The supplier shall develop an Inspection Test Plan (ITP) and inspection checklists for all SCADA equipment prior to commencing factory testing and submit to Solomon Power’s representative for review at least fourteen (14) days prior to the planned test date.

FAT testing will be passed and accepted based on the merits of the test case itself. It is expected that the SCADA supplier shall check all data-mapping, text referencing and coding according to their own QA/QC procedures to assure accuracy and integrity. All defects found post-FAT will require the SCADA supplier to resolve these defects at their own costs, including site travel if necessary. It is the SCADA supplier’s best interest to ensure the system has been implemented and tested rigorously and meticulously before being deployed to the site.

Upon completion of the FAT, the supplier shall submit the relevant test reports within one week from completion. The report shall certify in writing that the equipment and control system is tested in accordance with the relevant Australian/New Zealand (AS/NZS) Standards and the SCADA system is ready to be delivered or commissioned. The supplier shall obtain Solomon Power’s / Project Owner’s representative acknowledgement that the FAT has been satisfactorily completed and reported. Upon completion of commissioning and energisation, the supplier shall submit a certificate.

### Test requirements

The panel inspection and test program shall include:

• Insulation resistance tests on power supply systems and associated wiring.

• Functional testing of SCADA system and communication interfaces by utilising appropriate test simulators.

• Point to point checking of all wiring and cabling to verify continuity and connection to correct terminals and correct identification/labelling.

• Configuration and programming of all SCADA equipment within the SCADA and Communication panel(s) to verify all communication interfaces.

Test panels and alternative simulation techniques shall be used wherever possible to check the functional operation of the system. The simulation shall include, but not be limited to, all input signal simulation (analogue, discrete and digital), device operation simulation, SCADA system and other operator interfaces as required to demonstrate a replica of the site SCADA system. Solomon Power will not free-issue any hardware required for testing.

## Site Acceptance Testing (SAT)

Below are typical site testing requirements to be provided by the Contractor.

• A SAT plan and procedure. The SAT procedure shall describe all acceptance tests required to meet the functional requirements of the plan and a methodology to qualify the test as passed or failed.

• The SAT testing shall be carried out at the site with the rest of the equipment installed and wired and all software loaded. Internal and external communication links are to be functionally checked before the SAT can be started.

• The SAT testing shall verify and assure the integrity of the system without utilising simulators.

• A SAT check sheet shall be prepared and submitted.

### End-to-end testing

The end-to-end testing of the SCADA system is a complete functional test between the plant owner, Network operator and network dispatch and control system as applicable. The test shall be managed and executed by the SCADA supplier in co-ordination with other stakeholders. The latest version of all SCADA documentation, including documents, drawings, and software, shall be available for testing and shall demonstrate tag ID’s, link speed, and dialog between SCADA system components, plant owner, network operator and network dispatch and control system.

# Documentation

Documentation is to be submitted for the design, quality assurance and final construction of the balance of plant works.

Where noted, documents are to be provided in the local language as well as English and on a per-installation basis.

Typical deliverables are listed below. These are specific to the balance of the plant.

|  | **Deliverable** | **Typical revisions (IFU=issued for use; IFC=issued for construction)** | **Local language version** | **Per-installation** |
| --- | --- | --- | --- | --- |
|  | **Design** |  |  |  |
| 1 | Design drawing package to include, at a minimum: |  |  |  |
| a | Basis of design report | 30% / 80% / IFC |  | Yes |
| b | SCADA and Communications Architecture | 30% / 80% / IFC |  | Yes |
| c | SCADA and Communications Functional Specification | 30% / 80% / IFC |  | Yes |
| d | Detailed design and drawings for SCADA system | 80% / IFC |  | Yes |
| e | Detailed design and drawings for communications | 80% / IFC |  | Yes |
| f | Detailed design and drawings for UPS | 80% / IFC |  | Yes |
| g | HMI Screen Graphics | 80% / IFC | Yes | Yes |
| s | SCADA Signal List | 80% / IFC |  | Yes |
|  | **Prior to factory testing** |  |  |  |
| 2 | ITP and ITC containing, as a minimum, the following information for each significant activity identified in the relevant process: | Draft / IFU |  |  |
| a | Description of activity |  |  |  |
| b | Specification requirements/reference |  |  |  |
| c | Person responsible for activity (title) |  |  |  |
| d | Hold Points and Witness Points |  |  |  |
| e | Activity checklists |  |  |  |
| f | Inspection and test type |  |  |  |
| g | Tolerances or other acceptance criteria |  |  |  |
| h | Identification of relevant procedure and quality records |  |  |  |
| i | Test/inspection frequency |  |  |  |
| j |  Work item or work lot identification |  |  |  |
| k | The Employer may request the Contractor to include additional Hold Points or Witness Points, and the Contractor must make provision for the Contractor and the Employer to sign off at such points. |  |  |  |
| 3 | **Prior to site works** |  |  |  |
| 1 | ITP and ITC containing, as a minimum, the following information for each significant activity identified in the relevant process: | Draft / IFU |  |  |
| a | Description of activity |  |  |  |
| b | Specification requirements/reference |  |  |  |
| c | Person responsible for activity (title) |  |  |  |
| d | Hold Points and Witness Points |  |  |  |
| e | Activity checklists |  |  |  |
| f | Inspection and test type |  |  |  |
| g | Tolerances or other acceptance criteria |  |  |  |
| h | Identification of relevant procedure and quality records |  |  |  |
| i | Test/inspection frequency |  |  |  |
| j |  Work item or work lot identification |  |  |  |
| k | The Employer may request the Contractor to include additional Hold Points or Witness Points, and the Contractor must make provision for the Contractor and the Employer to sign off at such points. |  |  |  |
| 4 | **During site works** |  |  |  |
| 1 | Completed ITCs and quality documentation | Final |  | Yes |

1. If similar standards exist in different suites of standards, the lower priority standard need not be applied. Alternatively, the Contractor may seek Solomon Power’s approval of application of the lower priority standard without application of the higher priority standard. Such approval shall not unreasonably be withheld. [↑](#footnote-ref-0)