Transport Asset Standards Authority

T HR EL 11003 ST

Standard

Electrical SCADA System

Version 1.0

Issue date: 25 June 2019

© State of NSW through Transport for NSW 2019

Important message

This document is one of a set of standards developed solely and specifically for use on Transport Assets (as defined in the Asset Standards Authority Charter). It is not suitable for any other purpose.

The copyright and any other intellectual property in this document will at all times remain the property of the State of New South Wales (Transport for NSW).

You must not use or adapt this document or rely upon it in any way unless you are providing products or services to a NSW Government agency and that agency has expressly authorised you in writing to do so. If this document forms part of a contract with, or is a condition of approval by a NSW Government agency, use of the document is subject to the terms of the contract or approval. To be clear, the content of this document is not licensed under any Creative Commons Licence.

This document may contain third party material. The inclusion of third party material is for illustrative purposes only and does not represent an endorsement by NSW Government of any third party product or service.

If you use this document or rely upon it without authorisation under these terms, the State of New South Wales (including Transport for NSW) and its personnel does not accept any liability to you or any other person for any loss, damage, costs and expenses that you or anyone else may suffer or incur from your use and reliance on the content contained in this document. Users should exercise their own skill and care in the use of the document.

This document may not be current and is uncontrolled when printed or downloaded. Standards may be accessed from the Transport for NSW website at www.transport.nsw.gov.au

For queries regarding this document, please email the ASA at
standards@transport.nsw.gov.au or visit www.transport.nsw.gov.au

© State of NSW through Transport for NSW 2019

Standard governance

Owner: Lead Electrical Engineer, Asset Standards Authority

Authoriser: Chief Engineer, Asset Standards Authority

Approver: Executive Director, Asset Standards Authority on behalf of the ASA Configuration Control Board

Document history

Version	Summary of changes
1.0	First issue

© State of NSW through Transport for NSW 2019

Preface

The Asset Standards Authority (ASA) is a key strategic branch of Transport for NSW (TfNSW). As the network design and standards authority for NSW Transport Assets, as specified in the *ASA Charter*, the ASA identifies, selects, develops, publishes, maintains and controls a suite of requirements documents on behalf of TfNSW, the asset owner.

The ASA deploys TfNSW requirements for asset and safety assurance by creating and managing TfNSW's governance models, documents and processes. To achieve this, the ASA focuses on four primary tasks:

- publishing and managing TfNSW's process and requirements documents including TfNSW plans, standards, manuals and guides
- deploying TfNSW's Authorised Engineering Organisation (AEO) framework
- continuously improving TfNSW’s Asset Management Framework
- collaborating with the Transport cluster and industry through open engagement

The AEO framework authorises engineering organisations to supply and provide asset related products and services to TfNSW. It works to assure the safety, quality and fitness for purpose of those products and services over the asset's whole-of-life. AEOs are expected to demonstrate how they have applied the requirements of ASA documents, including TfNSW plans, standards and guides, when delivering assets and related services for TfNSW.

Compliance with ASA requirements by itself is not sufficient to ensure satisfactory outcomes for NSW Transport Assets. The ASA expects that professional judgement be used by competent personnel when using ASA requirements to produce those outcomes.

About this document

This document covers the general system requirements for electrical supervisory control and data acquisition (SCADA) systems used on the TfNSW Metropolitan Heavy Rail Network.

This is a first issue.

© State of NSW through Transport for NSW 2019

Table of contents

1. Introduction ... 7
2. Purpose ... 7
2.1. Scope ... 7
2.2. Application ... 7
3. Reference documents ... 7
4. Terms and definitions ... 8
5. System architecture ... 9
5.1. Master station ... 10
5.2. Telecommunications ... 10
5.3. RTUs ... 10
6. Equipment monitored and controlled ... 11
7. Data ... 11
7.1. Analogue input data ... 11
7.2. Digital input data ... 12
7.3. Data history storage and archiving ... 12
8. Functionality ... 13
8.1. Monitoring and control functionality ... 13
8.2. Reporting ... 13
8.3. Calculated points ... 13
8.4. Manual points ... 14
8.5. Alarm functionality ... 14
8.6. Event and alarm lists ... 16
8.7. RTU functionality ... 17
9. Interfaces ... 17
9.1. Operator interface ... 17
9.2. System internal interfaces ... 20
9.3. System external interfaces ... 21
10. Availability ... 21
10.1. Incident response ... 22
11. Integrity ... 22
11.1. Safety integrity level ... 23
11.2. Audits ... 24
12. Security ... 24
12.1. Remote access ... 25
13. Configuration management ... 25
14. Maintainability ... 27
15. Performance ... 27
16. Training and competency ... 28

© State of NSW through Transport for NSW 2019

17. Future expansion and enhancement 29

Appendix A Strategic benefits 30

Appendix B Audit topics 31

B.1. Reliability and availability 31

B.2. Change control 31

B.3. Security 32

B.4. Assets 34

© State of NSW through Transport for NSW 2019

1. Introduction

Electrical supervisory control and data acquisition (SCADA) systems monitor and provide the ability to control TfNSW electrical traction power and distribution networks. The components of a SCADA system are a master station, communication network and field equipment. This document provides the system wide standards for electrical SCADA systems.

2. Purpose

The purpose of this standard is to define the high-level electrical SCADA system requirements. These requirements are defined as the following:

- the information required for network planning and incident investigation
- the specific data needed in fulfilling real-time electrical network operational responsibilities
- the operational requirements for the SCADA system to ensure availability of real-time control and monitoring

2.1. Scope

This document covers overall, general system requirements for electrical SCADA systems used by TfNSW on the TfNSW Metropolitan Heavy Rail Network. It includes requirements for all the components that comprise the SCADA system, that is, a master station, a communication network and field equipment. Some of these components may be owned or operated by third parties.

2.2. Application

This document applies to all components of the electrical SCADA system on the TfNSW Metropolitan Heavy Rail Network.

This standard is intended to be used by AEOs that undertake work on the SCADA system related to the master station, communication network and remote terminal unit (RTU).

3. Reference documents

International standards

IEC 60870 (series) Telecontrol equipment and systems

IEC 61131-3 Programmable controllers - Part 3: Programming languages

IEC 61850 (series) Communication networks and systems for power utility automation

IEEE 1815-2012 IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)

© State of NSW through Transport for NSW 2019

Australian standards

AS 61508.0 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 0: Functional safety and AS 61508

AS IEC 62682 Management of alarm systems for the process industries

Transport for NSW standards

EP 00 00 00 13 SP Electrical Power Equipment - Design Ranges of Ambient Conditions

T HR EL 11002 SP Electrical SCADA System Remote Terminal Unit

T HR EL 11004 ST Electrical SCADA Interface Requirements

T HR TE 21003 ST Telecommunications for Traction Substations and Section Huts

T MU HF 00001 ST Human Factors Integration – General Requirements

T MU SY 10010 ST Cybersecurity for IACS - Overview

T MU SY 10012 ST Cybersecurity for IACS - Baseline Technical Cybersecurity System Requirements and Countermeasures

T MU SY 10013 PR Cybersecurity for IACS – Cyber Risk Management Procedure

T MU TE 41001 ST Packet Switched Networks – Wired Networks

T MU TE 61007 ST Time Synchronisation of Industrial Automation and Control Systems

4. Terms and definitions

The following terms and definitions apply in this document:

AEO Authorised Engineering Organisation

AI analogue input

DI digital input

DNP3.0 distributed network protocol

DO digital output

ESO electrical system operator

GPS global positioning system

HV high voltage

IED intelligent electronic device

IP internet protocol

PLC programmable logic controller

point unique identifier assigned to a device, measurement or calculation in the master station

© State of NSW through Transport for NSW 2019

RTU remote terminal unit

SCADA supervisory control and data acquisition

shelve or tag to temporarily suppress an alarm, initiated by the operator

suppress to prevent the annunciation of the alarm to the operator when the alarm is active

5. System architecture

To monitor the electrical network, the SCADA system has three major components, which are the master station (consisting of the operator interface, the engineering interface and the SCADA application), the telecommunications network and remote terminal units (RTUs). These components are detailed in Section 5.1 to Section 5.3.

Figure 1 is a guide to typical SCADA architecture.

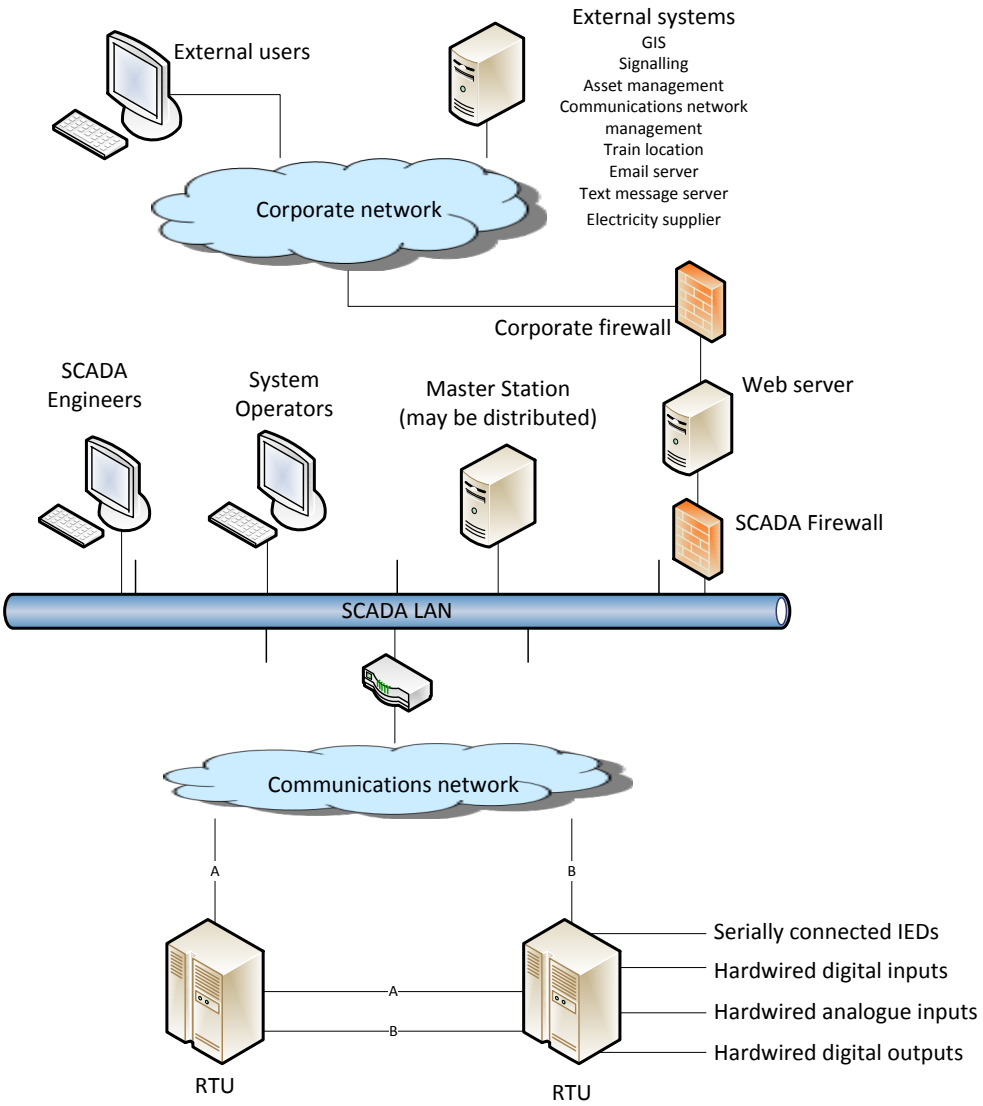

Figure 1 - Typical SCADA architecture

© State of NSW through Transport for NSW 2019

5.1. Master station

The master station consists of hardware and software components. These components may be geographically distributed to meet other requirements, such as availability or business requirements.

The master station hardware shall comprise commercial off the shelf (COTS) information and communication technology (ICT) parts and technology. It may be hosted in an ICT data centre, which meets Australian government requirements for critical infrastructure, where dedicated contracts already exist for the environment, maintenance, reliability and change management. The hardware shall support and meet the integrity, availability, security, maintenance and performance requirements detailed in this standard. All hardware used to run the master station software shall be located in New South Wales.

The application software shall be able to run on virtual machines on the hardware described in this section. It may be part of a railway software application that performs other functions.

5.2. Telecommunications

A telecommunications network shall be used to connect the SCADA master station with the RTUs located in substations and other locations.

The telecommunications network shall comprise an ethernet wide area network using TCP/IP, which may use links and hardware provided by external suppliers. The communications network shall have duplicate fibre-optic connections at each high voltage (HV) substation. Locations where SCADA is required shall use fibre optic cables for SCADA communications. No copper communication cables shall cross a substation boundary, as defined by the earth grid. A risk assessment shall determine the communication requirements for other locations.

The protocols used on the SCADA system shall not be proprietary. The master station and RTUs shall be able to use at least two common SCADA protocols. Secure DNP3 (refer to IEEE 1815-2012 *IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)*) or an IEC protocol (for example IEC 61850 or IEC 60870-5) shall be used.

5.3. RTUs

At each SCADA monitored location within the electrical network, a type approved RTU shall be used to communicate with the master station.

The data shall be transferred to the master station when requested by the master station or, if configured, the data can be transferred using unsolicited responses. The RTU shall predominantly be used to pass monitoring and control information between the field equipment and the master station. The RTU shall also have local programmable logic to implement local

© State of NSW through Transport for NSW 2019

automation functions independent of the master station. As an example, this function shall be used to provide the logic for the operation of a test circuit breaker.

6. Equipment monitored and controlled

The electrical SCADA system provides the strategic benefits listed in Appendix A. These benefits are achieved by monitoring and controlling equipment on the electrical network. The SCADA system shall monitor and control equipment at the following locations:

- traction substations
- HV distribution substations (33 kV and above)
- underground station substations (11 kV and above)
- 1500 V (or other traction voltage) sectioning huts
- safety or operationally critical traction (for example, 1500 V or 750 V dc) field switches
- normally open mid-points of HV feeders (11 kV and above)

The SCADA system may be used to monitor or control equipment at other locations as determined by a risk assessment, such as the following:

- high voltage and low voltage supplies at critical locations (for example, signal boxes and control centres)
- underground pumping stations
- tunnel lighting
- spark gaps

7. Data

Data shall be obtained, recorded and stored for various uses such as real-time operations, incident investigation and network planning. Data includes analogue and digital point state changes, operator actions, analogue point limit crossings, SCADA system changes, communication events and other events as determined by the operator and maintainer.

7.1. Analogue input data

The accuracy of analogue inputs from source to master station shall be equal to or better than ±1% (except for dc currents which shall be equal to or better than ±5%) over the full scale and for the temperature range specified in EP 00 00 00 13 SP *Electrical Power Equipment - Design Ranges of Ambient Conditions*. The RTU equipment (resistors, analogue to digital converter and software accuracy) shall have accuracy better than 0.25%.

The resolution shall be at least 11 bits plus sign.

© State of NSW through Transport for NSW 2019

Each analogue shall be continuously monitored by the RTU. The value shall be sent to the master station at least once every 5 s or sooner if a change greater than 1% (5% for dc currents) of the full scale range is detected.

All measured values shall be accompanied with a quality label to indicate whether the value is valid or suspected of being invalid (manually changed, out of scan, and so on).

The range of measurement shall be appropriate for the value being measured, covering the expected extremes.

The master station shall be able to export the history of an analogue point in a commonly used format.

7.2. Digital input data

Double point indications shall have separate SCADA indications of the fully open state, and the fully closed state (refer to IEC 60870.1.3).

7.3. Data history storage and archiving

Changes to data shall be recorded with all necessary information (for example, location, point name, equipment type, operator, value, full time stamp, quality tag).

The master station shall take less than 5 s to access and display a graph of 1 week of 1 analogue point from 12 months ago.

The master station shall take less than 10 s to perform a filtered search of events or alarms from the last 12 months.

At least the previous 1 year shall be accessible on the master station hardware; at least the previous 5 years shall be accessible through the history system (on master station hardware) and all data more than 1 year old shall be available by the use of an archive system. The archive system shall be located on TfNSW's premises or the operator's premises.

The master station and the history system shall provide the ability to search, filter and extract data.

The master station and the history system shall provide the capability to perform data analysis, such as performing functions on points (such as averages, Boolean searches, and so on).

The history system shall have the ability to modify history, but it shall be noted on the point itself. Access to modify history shall be restricted to authorised users.

The master station shall have the ability to load a snapshot of a particular time in the past to view the state of the electrical network.

A record of state changes shall be maintained on the RTU until it has been read by the master station.

© State of NSW through Transport for NSW 2019

8. Functionality

RTUs shall send real-time information from field equipment to the master station, which shall process the information based on configuration settings. The master station shall then distribute, store and act on this information and update user displays. An operator with permission to control equipment shall be able to control equipment in real time. The RTU and master station shall also provide the capability to perform user programmable logic routines to execute actions based on certain conditions.

The master station shall have different modes for different purposes, such as online, offline development and simulator.

Any SCADA process, programme, RTU, workstation or server shall not restart inadvertently. A restart shall only occur when planned or a warning is provided to the operator.

8.1. Monitoring and control functionality

The SCADA system shall be able to monitor and control the electrical network and ancillary systems in real time and provide this functionality for multiple operators concurrently. The system shall have the capability to support and meet performance requirements with at least five operators. It shall provide and process information for the management of and the planning of maintenance for the electrical network.

8.2. Reporting

The master station shall be capable of producing reports. This includes the following:

- circuit breaker opening reports
- error checking reporting (for example, identifying analogues that have not changed in a certain period or are reading zero when a quantity should be measured)
- SCADA master station and RTU performance reports

To ensure that the SCADA system and the electrical network are functioning correctly, these reports shall be checked regularly for trends that require investigation (for example, transformer temperatures, number of trips and other condition monitoring parameters).

8.3. Calculated points

The master station shall have the capability to perform calculations using both digital and analogue points in real-time (for example, average value), which can be alarmed and configured in the same way as a monitored point.

© State of NSW through Transport for NSW 2019

8.4. Manual points

Configuration of manual or hand-dressed points shall be possible on the master station. These are points that are not telemetered, but are still able to change state after an operator action.

8.5. Alarm functionality

An alarm is an audible or visible means of indicating to the operator an abnormal condition requiring a response. The purpose of the alarm system is to provide the operator with a clear indication of abnormal conditions on the electrical network and the SCADA system. The alarm system shall be designed with human factors considerations. Refer to T MU HF 00001 ST *Human Factors Integration – General Requirements* and AS IEC 62682 *Management of alarm systems for the process industries* for information.

The indications in the alarm system shall be designed and configured appropriately to provide the following functionality:

- alarm priorities
- visible annunciation functionality, such as colours, symbols and animation (such as blinking)
- audible alarm annunciation
- alarm summary display
- alarm shelving or tagging
- alarm suppression
- alarm configuration such as dead-band and on-delay and off-delay (de-bounce)
- alarm log
- alarm system audit functionality

An alarm shall be able to transition to the following states:

- acknowledged or unacknowledged
- active or inactive (abnormal or normal)
- suppressed or unsuppressed
- shelved or un-shelved (tagged or untagged)
- out of service or in service (maintenance or non-maintenance)

Shelved alarms are temporarily suppressed by the operator and can preferably be automatically un-shelved after a certain time. The alarm shelving function shall have the capability of being access controlled.

© State of NSW through Transport for NSW 2019

Alarms shall be able to be suppressed or shelved based on logic, which shall only be modified by an authorised person.

Out of service and maintenance is where the alarm is removed from service for maintenance. It is under control of the maintenance operator.

All of the state changes and operator actions mentioned in this section shall be logged as events with appropriate detail.

8.5.1. Indication or alarm definition

The indication shall be defined by the following:

- when it should it alarm
- the consequences of not responding (immediate and long term)
- the people who need to know about the alarm
- the response time
- how people are to be notified (such as operator alarm, phone call, SMS, email, irregularity report)
- the action required, including the following:
    - information only (event, but no alarm)
    - delayed action required (event, alarm, no immediate action required)
    - immediate action (event, alarm, immediate action required)

An indication should not alarm if any of the following apply:

- the operator does not need to do anything
- the event is not an indication of a problem
- there are no consequences if the operator does not respond
- the same problem is indicated elsewhere (more than one alarm for one root cause)

New alarms and indications (not previously configured on the SCADA system) shall be provided with the following:

- interface description
- operating procedures
- maintenance procedures (if any)
- testing procedures
- operator interface design requirements

© State of NSW through Transport for NSW 2019

8.5.2. Alarm prioritisation

Alarms shall be able to be prioritised, based on the following:

- severity of the consequence
- time required to respond
- safety and operational criticality

Any prioritisation should be completed as part of a risk assessment during the design stage.

8.5.3. Setting analogue alarm limits

Refer to T HR EL 11004 ST *Electrical SCADA Interface Requirements* for setting some analogue alarm limit values. Other alarm limit setting requirements shall be determined by the operator and maintainer after an engineering evaluation and risk assessment.

8.5.4. Alarm system performance monitoring

The alarm system and the status of alarms shall be reviewed as determined appropriate by the operator. This review shall identify the following (the time periods shall be determined by the operator):

- alarms suppressed or shelved for an extended period
- indications that have been in the alarm state for an extended period
- alarms that have not been commissioned after equipment has been placed in service
- indications that have alarmed without reason or without operator action

These shall be collated into a report where responsibility for actions to mitigate the issues is allocated. The report shall be provided to the responsible person for action.

8.6. Event and alarm lists

An alarm or event record shall have the following record attributes, which shall appear in the event or alarm list:

a. point name

b. point description

c. state

d. priority

e. type

f. time and date of occurrence of the state change (including milliseconds)

g. value at the time when the alarm record is recorded

© State of NSW through Transport for NSW 2019

h. location

i. alarm message

All lists shall be able to be filtered based on each field. Alarms and events that are for information only (low priority) shall be able to be filtered out. A point shall be able to be chosen by selecting it from a list and by typing its name.

8.7. RTU functionality

The RTU shall record all state changes and maintain a record of these until the information has been transferred to the master station, or maintain the record for at least four hours. If the RTU cannot send analogue changes to the master station, it shall store the analogue at least every five seconds.

The RTU shall receive time information from the master station or from a local time source such as a global positioning system (GPS) clock and shall time stamp all information. Time synchronisation shall be in accordance with T MU TE 61007 ST *Time Synchronisation of Industrial Automation and Control Systems*.

The inputs and outputs of the RTU shall meet the requirements of T HR EL 11002 SP *Electrical SCADA System Remote Terminal Unit*.

The RTU shall have the following:

- a test circuit breaker implemented in logic to test control and monitoring
- capability of the RTU from the control centre
- logic to monitor the doors for intruders and provide an alarm to the control centre, if there is no dedicated intruder alarm

For the programming of logic, the RTU shall support at least three standard programming languages in accordance with IEC 61131-3 *Programmable controllers - Part 3: Programming languages*, one of which shall be structured text.

9. Interfaces

The interfaces shall be standard and non-proprietary wherever possible.

9.1. Operator interface

For operators, the SCADA master station shall provide facilities by means of an operator interface to remotely monitor and control equipment on the electrical supply network and other associated equipment. The operator interface shall present information in the form of schematic diagrams representing the actual field equipment layout. Information shall also be presented geographically. Symbols and alarm text on the diagrams shall change colour, symbol or text in

© State of NSW through Transport for NSW 2019

real time to reflect the current state of the field equipment that the indication represents. The electrical system operators (ESOs) shall be able to remotely control field equipment such as circuit breakers and switches using the symbols on the screen. Analogue changes and limit breaches, such as those for busbar voltages and feeder currents, shall be able to be displayed, alarmed, recorded and stored for incident analysis and planning.

The operator interface screen size shall be sufficient to view multiple displays (for example, substation, event list, alarm list) so that the operators can clearly read symbols and labels.

Each type of display interface shall be appropriate for its purpose, such as the following:

- schematic diagrams
- alarm management
- tabular displays for events, alarms and reports
- SCADA system administration and status displays showing communication, connected users and RTU status
- reports such as circuit breaker openings
- configuration

Schematic diagrams shall display the electrical network by means of different types of pictures such as the following:

- overview and interconnection displays showing the entire electrical network at a high level (for example, high voltage)
- substation displays (single line diagrams)
- traction supply (for example, overhead wiring) displays

The interface shall be designed with human factors considerations; refer to T MU HF 00001 ST. The interface shall be easy to navigate with common navigation symbols and concise steps (less than four mouse clicks to get to the target screen). Performing controls and other operator functions shall be easy using common industry terms and symbols. The positioning of windows and dialogue boxes shall not impede the safe operation and clear understanding of the state of the network.

Displays shall have the ability to use coloured, animated symbols by means of a standardised, customisable and user configurable library. The date, time, location and labels to identify equipment shall be visible on each display. The SCADA application shall not restrict the number and location of simultaneously open displays.

The master station shall provide the ability to modify or add new display diagrams so that they reflect changes to the electrical network using common computer drawing tools. The updates shall be deployed to the online system in a controlled manner, alerting the system operators of the change while avoiding undue disturbance to them.

© State of NSW through Transport for NSW 2019

User interfaces shall be provided for electrical network operating staff, engineering staff for administration and configuration, and managerial staff to view the network status.

9.1.1. Operator alarm interface

The operator alarm interface shall provide the ability for the operator to do the following:

a. silence audible alarm indications (that is, without acknowledging the alarm)

b. acknowledge alarms

c. place alarms out of service through access controlled methods

d. modify alarm attributes through access controlled methods only

e. initiate an alarm shelving function

f. display alarm messages

g. assign alarms to operator stations or operating area

The operator interface shall provide the capability for the following, or equivalent:

a. alarm summary displays

b. alarm indications on schematic displays

c. alarm indications on point detail display

d. shelved alarm summary displays

e. out-of-service summary displays

The operator interface shall display at least the following point states:

a. normal

b. unacknowledged alarm (abnormal)

c. acknowledged alarm (normal and abnormal)

d. return-to-normal unacknowledged alarm

e. shelved alarm

f. suppressed-by-design alarm

g. out-of-service alarm

© State of NSW through Transport for NSW 2019

9.2. System internal interfaces

9.2.1. Communication network

Refer to T HR TE 21003 ST *Telecommunications for Traction Substations and Section Huts* for communications requirements into TfNSW heavy rail locations. It may also be used as a guide for all Transport electrical networks.

Alternate, diverse paths for redundancy shall be provided for communications to the master station.

For information about interfacing to RTUs at field locations, refer to T HR EL 11004 ST, which can be used as a guide for other transport modes.

9.2.2. RTU inputs and outputs

The RTUs receive analogue and digital inputs from the field equipment. The RTU shall interface with digital inputs, which can be either wired circuits from status and alarm contacts (hardwired) or communicated by means of a serial connection from the field equipment. Digital inputs shall present either a ‘high’ (the battery voltage or a '1') or a 'low’ signal (zero volts or a '0') into the RTU input. The RTU shall also interface with analogue inputs, which are used to transmit the present value of a voltage, current, temperature or other analogue value from field equipment by means of a transducer and signal cabling.

The RTU shall output controls to field equipment, such as trip or close and raise and lower commands to switches, HV and traction circuit breakers, tap changers and some miscellaneous items such as the substation bell or buzzer. Outputs shall operate by closure of a contact in an output relay associated with each channel. An external circuit is wired to this contact to apply voltage to energise a trip or close relay in a switch or circuit breaker. Outputs shall normally be energised for a pulse period of two seconds, although constant level (latched) outputs shall also be available.

9.2.3. Intelligent electronic devices

The RTU shall be able to communicate to protection relays, programmable logic controllers (PLCs) and other intelligent electronic devices (IEDs) across a serial communication link. This allows certain analogue and digital inputs and digital outputs from these devices to be transmitted directly to the RTU without the need for individual circuits hardwired to digital inputs.

The serial communication link shall use protocols that are not proprietary. The RTU shall be able to use at least two common SCADA protocols. Secure DNP3 (refer to IEEE 1815) or an IEC protocol (for example IEC 61850 or IEC 60870-5) shall be used. The Modbus protocol may be used for compatibility with existing devices.

© State of NSW through Transport for NSW 2019

9.3. System external interfaces

The architecture shall provide standard interfaces for integration with corporate applications, databases and other systems. These interfaces shall treat the external systems as less secure and the interface itself shall meet the security requirements in Section 12. These may include a geographical information system, signals, asset management, corporate information technology, train location system, network management system, email, text and other SCADA systems.

10. Availability

The system shall have an availability of no less than 99.95% (four hours unavailable over a one year period), excluding planned outages. Refer to IEC 60870-4 *Telecontrol equipment and systems Part 4: Performance requirements* for availability calculations and classes.

The communications availability shall be 99.99% with dual redundancy for the SCADA telecommunications network. Refer to T MU TE 41001 ST *Packet Switched Networks – Wired Networks* for more information.

All availability figures shall be measured over a rolling six month period.

Each critical part of the master station shall have redundancy, for example the communications' interface or the part that processes information from the field. No single point of failure shall affect the main functionality of the SCADA system. At least two locations shall be provided for operator interfaces, both of which shall be capable of operating on the entire SCADA network. This functionality shall be tested at appropriate intervals as determined by the operator's risk study. The master station core software shall be capable of being run from at least two locations. This functionality shall be tested at least annually.

Loss of any one component (hardware or software) shall only affect one of the following:

- the monitoring and control of one substation
- one workstation
- one RTU

The loss of any one device (such as substation, RTU, workstation, overview display, or printer) shall have no impact on the master station delivering the following:

- main functional requirements
- performance requirements at full capacity
- secure operation and handling of data

© State of NSW through Transport for NSW 2019

10.1. Incident response

10.1.1. Response to failures

The operator shall develop appropriate risk based response procedures, including but not limited to the following:

a. promptly repair any failure, taking into account the SCADA system and electrical network reliability requirements

b. keep the operator's electrical operating centre informed of progress to repair any failure that is causing a critical outage

c. consult with the operator's electrical operating centre regarding the priority of work to correct failures causing or likely to cause a critical outage, with the objective of minimising the impact of outages

When an RTU fails, visibility and control of the electrical network is lost in part. The discretion to call out appropriate assistance remains with the ESO.

In normal working hours, the engineer responsible for the SCADA system shall always be advised in the first instance and advise appropriate action and callouts.

10.1.2. Outage coordination

The operator shall develop appropriate risk based procedures for planned outages, including but not limited to the following:

a. any planned outage of SCADA equipment affecting a substantial part of the operational data shall be advised with at least five business days' notice to the operator's electrical operating centre

b. if a planned outage is proposed such that five business days' notice cannot be given, the outage shall be deferred if practicable

11. Integrity

The SCADA system shall monitor and control the field equipment as shown to the operators on the display diagrams.

After any failure, the RTUs and master station shall return to normal in an appropriate and predictable manner without unauthorised controls or alarms. For example, the master station shall not attempt to reclose circuit breakers that were open before a restart and have remained open.

The master station shall be self-monitoring and shall do the following:

- monitor the SCADA telecommunications network

© State of NSW through Transport for NSW 2019

- monitor the RTUs and other SCADA field equipment
- monitor the electrical network
- maintain an accurate record of the state of the entire network
- maintain an accurate record of the SCADA system itself

The architecture of the master station database shall enable it to receive, process and display all field changes while meeting performance requirements specified in Section 15.

The RTUs shall be self-monitoring and report faulty cards, modules and internal errors.

For digital outputs (controls), select before operate (two pass operation) shall be used where it is available in the protocol.

A quality flag shall be used to indicate the reliability of the actual state of a point. The quality flag shall indicate if the point has been manipulated or modified or if a scanning or calculation error occurred.

11.1. Safety integrity level

According to AS 61508.0 *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 0: Functional safety and AS 61508*, the electrical SCADA system is neither considered a safety critical system nor a safety related system due to the presence of external mechanical, procedural or independent electronic mitigations. The main hazard scenarios associated with traction power distribution are electrocution of, or electrical shocks to, workers or the public, and workers or the public becoming injured from faulty electrical equipment or equipment under fault conditions. In these situations, the SCADA system is deemed not to be safety related because it does not significantly reduce the risk of the hazards mentioned nor does it prevent initiation of a hazard, detect the onset of a hazard or take the necessary action to terminate a hazardous event.

Nevertheless, the SCADA system is often used to alert network operators and control certain equipment in hazardous situations. For example, it can be used to quickly remove power where there is a risk of electrocution. Its advantage, in providing centralised supervision and control of a complex system, is important and unreliability or unavailability of the SCADA system may increase the overall risk of failed hazard management.

If the SCADA system controls switches that connect equipment to rail or to earth or perform safety related operations, then the requirement for the system to meet a safety integrity level shall be reassessed.

© State of NSW through Transport for NSW 2019

11.2. Audits

Auditing is required to ensure the effective use of rail assets. Requirements for auditing apply to the maintainer and operator of the electrical SCADA system. Section 11.2.1 and Section 11.2.2 briefly outline of the type and frequency of different audits.

See Appendix B for audit topics.

11.2.1. Annual asset integrity audit

The annual asset integrity audit provides information for the annual asset integrity report.

Annual integrity audits shall be conducted every 12 months and shall be completed in time to provide input into the combined electrical asset report.

The audit includes SCADA system performance, incident analysis, data, standards, capacity, state of hardware and software and covers the master station, RTUs, SCADA telecommunications, and security with physical inspections of the master station and selected field locations.

11.2.2. Major audit

The major audit provides information for the upgrading or replacement of the electrical SCADA system. The audit shall be performed in conjunction with an external consultant.

Major audits shall be conducted every five years.

The audit includes all parts of the SCADA system, including control centre location, master station, RTUs, SCADA telecommunications, staff and security with a physical inspection of the master station and selected field locations. The audit report shall recommend actions to ensure the SCADA system continues to operate reliably.

12. Security

The SCADA system is considered critical infrastructure and shall be secured accordingly. The security category of the SCADA system shall be the following:

- confidentiality – LOW
- integrity – HIGH
- availability – HIGH

Confidentiality, the ability to prevent disclosure of information and access to the SCADA system and its information to unauthorised users or systems, is considered to have a low to medium impact if it was breached. Master station to RTU and master station to external system communications should be encrypted.

© State of NSW through Transport for NSW 2019

The master station shall provide the ability to limit access to authorised users. It shall ensure that only users authorised to view the electrical network are able to and that only users authorised to perform controls on the electrical network are able to.

Security features of the operator interface (access control, area, roles) shall be able to be changed without restarting the workstation or operator interface. The roles shall include: administrator, configurator, tester, operator, trainee operator and visitor.

The protection of the SCADA system applies to the storage of data even if that data is not held within the SCADA system.

The SCADA system shall limit external access based on the strictest criteria possible whilst still allowing normal operation.

Products capable of secure DNP3 with secure authentication shall be installed and this functionality shall be used where both master and slave have the capability.

The SCADA system shall comply with T MU SY 10010 ST *Cybersecurity for IACS – Overview*, T MU SY 10012 ST *Cybersecurity for IACS - Baseline Technical Cybersecurity System Requirements and Countermeasures* and T MU SY 10013 PR *Cybersecurity for IACS – Cyber Risk Management Procedure*.

Any security measures implemented shall not reduce the availability of the SCADA system.

12.1. Remote access

The master station shall allow remote access by SCADA staff, operators, other staff and maintainers. This access shall be restricted to ensure that those who access the SCADA system can be identified by username and either internet protocol (IP) or media access control (MAC) address.

13. Configuration management

The SCADA system shall enable users to perform configuration management by using version control, user access control and recording changes.

All historical SCADA records shall use secure, computer-generated, time-stamped audit trails to independently record the date and time of user actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information.

Procedures for updating configuration or displays and firmware or application shall be created and used.

Master station software application or hardware changes and RTU configuration changes shall be recorded with date, time, name of person performing the change and a comment about the change.

© State of NSW through Transport for NSW 2019

The operator shall develop a change procedure, which shall include, as a minimum, the following requirements:

- record the request for change
- determine if the change requires configuration control (analyse the change for impact)
- approve the change
- implement the approved change
- verify the correct implementation of the change
- close the change request

The master station shall allow SCADA database changes such that:

- It shall be possible to make changes to the real-time database without interruption to the normal day-to-day SCADA operations.
- The master station shall allow multiple users to make database changes simultaneously, for example, updates from two workstations, using the configuration tool and direct updates (such as SQL updates). In such a case, the users shall receive a warning message in order to prevent users updating the same table resulting in lock conflict or database corruption.
- The software shall provide an error handling feature in all utility scripts and functions. For example, in the event of a planned failover to the disaster recovery location, the shutdown shall be executed in a predictable manner. The status of the system shall be known throughout the failover and no records shall be locked or deleted. If any transaction update was in place, no unauthorised controls shall be performed and no status changes shall be ignored.

The master station shall allow display updates such that individual operators shall be allowed to download an updated schematic to their workstation at their convenience, for example, during off peak time.

A message from the system administrator or other operator developed procedure shall prompt each operator at workstations to update their schematics with the following or similar options:

- schedule before or after a planned project and maintenance work
- on request from the operators or the maintenance staff
- schedule the message for future date and time
- update or delete the message
- save these messages for future reference

© State of NSW through Transport for NSW 2019

14. Maintainability

The SCADA system shall be designed to be in continuous service such that maintenance activities do not require the SCADA system to be shut down.

The SCADA system shall have a mean time to repair (MTTR) of not more than four hours at any location where the SCADA system or its components are installed. This time is from the dispatch of a technician to restoration of SCADA functionality and includes travel time. The mean repair time (MRT) shall be less than one hour.

The RTU and master station software and hardware shall be supportable over the expected life time, which is a minimum of ten years.

The whole-of-life costs, including the cost and impact of maintenance, shall be documented during the procurement process.

SCADA system operation and maintenance documentation shall be included. Distribution of, access to, and use of this documentation shall be adequately controlled and subject to change control procedures.

Equipment complying with this standard shall be maintainable by trained personnel at service facilities and in the field. The supplier shall, upon request, provide a list of test equipment and quantities of replacement parts deemed necessary for the maintainability class. The extent of the spare parts shall take into consideration the time required to repair or replace a faulty component and return it to a serviceable condition. Refer to IEC 60870-4 for more information.

15. Performance

The performance of the SCADA system can impact the rail network and, as a result, shall meet the performance requirements in this section. These requirements apply to the master station and the RTUs.

State changes shall be recorded with ±1 ms accuracy. Refer to T MU TE 61007 ST for further requirements.

Maximum time to perform a control (master station to RTU relay output) shall be 2 s.

Maximum time to display a state change from an RTU shall be 2 s.

Maximum time to display a state change from another workstation shall be 1 s (for example, manual point).

Maximum time to display a diagram after clicking on the link to the diagram shall be 1 s.

The master station shall achieve the following capacity:

a. an elapsed time of no greater than 0.5 s for 95% of the time, with no instances to exceed 1 s, measured between a digital data point status change at the master station interface

© State of NSW through Transport for NSW 2019

point to the communications network and the corresponding update of all affected workstation displays

b. an elapsed time of no greater than 1 s between an analogue data point change at the SCADA interface point to the communications network and the corresponding update of all affected workstation displays

c. an elapsed time of no greater than 0.5 s for 95% of the time, with no instances to exceed 1 s, between the initiation of a command at any workstation and the corresponding output signal to the RTU, measured at the SCADA interface point at the communications network

d. incorporation of RTU time tagged digital data points into the real-time database within 1 s of receipt

e. no false data storage, no loss of digital or analogue data point data and no deterioration in performance under electrical network disturbances that result in data processing no greater than both of the following:

   i. a total of 300 digital data point status changes spread evenly over 2 s, initiating from at least 50% of all RTUs (with an even 5% spread of digital data points across the RTUs)

   ii. a total of 75% of all analogue data points, spread evenly across all RTUs, varying by no less than 5% of input range every 2 s

A gradual deterioration in the performance of the SCADA system is acceptable in the case of excessive data processing. The gradual deterioration shall allow the operator to still perform actions. A total processing failure is not acceptable.

The aforementioned performance requirements assume that no third party applications (such as virus checking software) impact the performance of the host machine and that the SCADA system operates at a normal operational load based on the future SCADA system capacity.

Alarm acknowledgement shall be updated on all workstations in less than 2 s.

16. Training and competency

Operators and maintainers shall be able to use the system (RTUs and master station) effectively through appropriate training, documentation and competency assessment. This shall be possible through the master station's development and simulator modes.

Online help and manuals shall be available for RTU configuration, master station operation and master station configuration.

Instructions for electrical network operators which cover the most likely network events shall be provided.

© State of NSW through Transport for NSW 2019

17. Future expansion and enhancement

The SCADA system shall allow for expansion including the I/O count. This shall be specified in the procurement contract as an expected percentage increase per year for RTUs, points (digital, analogue and controls) and locations.

© State of NSW through Transport for NSW 2019

Appendix A Strategic benefits

The electrical SCADA system provides the operator and maintainer with the ability to monitor and control the HV electrical network and other associated equipment. This harnesses technology to improve customer and network outcomes by providing the following:

- a reliable record of changes and actions on the electrical network for planning and incident investigation
- lower staff numbers as substations need not be staffed
- a reduction in staff travel and associated risks
- business continuity by allowing remote switching to circumvent failures and maintenance
- automatic reclose of certain feeders to reduce interruptions
- improvement to community safety by disabling auto reclose during high fire danger
- the ability to do condition monitoring with SCADA data by viewing long-term data

© State of NSW through Transport for NSW 2019

Appendix B Audit topics

B.1. Reliability and availability

Important reliability and availability considerations for the electrical SCADA system include the following questions:

- What is the down time of the system and its parts?
- Is there a formal disaster recovery and business continuity procedure? Is it tested?
- Are SCADA incidents (master station, telecommunications, RTUs) reviewed and analysed?
- Are incident reports corrected and updated to accurately represent the problem and resolution?
- What are the actions required and completed after incident analysis?
- Is the analogue and digital data recorded continuously? Is it checked each day?
- Are telecommunications, RTU and master station service level agreements (SLAs) reviewed regularly?
- Are there sufficient spares in accordance with incidents or criticality?
- Are critical components of the SCADA system supported by an uninterruptable power supply (UPS) and are these batteries tested on a regular basis to ensure that they are reliable?
- How is staff competency managed?

B.2. Change control

Important change control considerations for the electrical SCADA system include the following questions:

- What formal change control procedures exist for the SCADA environment?
- Are there any policies covering the introduction of new devices to the SCADA environment?
- Are database updates (for changes to field equipment) being documented?
- Is there a record of who did what change when?
- Are there signed test results?
- Are ESOs formally notified of changes?
- How are RTU configurations kept? What is the version control?
- Are new RTUs designed, installed and commissioned to TfNSW standards?

© State of NSW through Transport for NSW 2019

- Are new types of digital and analogue points documented for ESOs?
- Are non-electrical points approved?
- Has the change been approved (approved advice, cable and I/O schedule)?
- Where is the status (progress and conformance) of a change available?
- Where is the approval of variations?
- Where is the completed testing checklist?
- Where is the status of nonconformances (the defects list)?

B.3. Security

Important security considerations for the electrical SCADA system include the following general questions:

- How can users gain access to the SCADA application?
- What are the username and password requirements of the SCADA application? Are users allowed multiple login attempts? Are legal captions used? Is there a session timeout?
- How is the administrator password controlled?
- Are user reviews and associated access rights performed on a regular basis?
- What are all interfaces for remote access?
- Are staff screened when hired to work in the SCADA environment (including suppliers)?

Important security considerations for the electrical SCADA system include the following questions about policies and procedures:

- Is there a defined security strategy for the SCADA environment?
- Who is responsible for security management within SCADA environment? Is this documented?
- Are there periodic security reviews of the SCADA network performed?
- What are the procedures for the disposal of SCADA network media and devices?
- What security logs are maintained for critical equipment and how often are the logs reviewed?
- Who is responsible for the reviewing of security logs?
- Has access to event logs been restricted?
- Are users provided with further information on security issues on a periodic basis?

© State of NSW through Transport for NSW 2019

Important security considerations for the electrical SCADA system include the following questions about physical access:

- How is physical access to SCADA terminals controlled?
- Are SCADA control rooms segregated from other rooms?
- What building security exists at remote sites to prevent unauthorised access?

Important security considerations for the electrical SCADA system include the following questions about network security:

- Have routers and other devices been configured to filter unauthorised telecommunications?
- How is suspicious or unusual activity detected on the SCADA wide area network (WAN)?
- How is the management of firewall, router and workstation patches controlled?
- What backup and recovery measures are in place for system devices?
- Has simple network management protocol (SNMP) been implemented on core infrastructure?
- Has any wireless equipment been deployed within the SCADA environment?
- Are all default passwords removed from SCADA devices after implementation?
- Is there a development system to test changes prior to deployment on the production system?
- Is internal and external penetration testing performed?

Important security considerations for the electrical SCADA system include the following questions about workstation security:

- What operating systems (version) are installed on SCADA terminals?
- Have operating system level passwords been activated on all SCADA terminals?
- Do passwords have an indefinite expiry date?
- What file and directory permission controls, including USB memory devices, have been implemented on SCADA terminals to restrict unauthorised access by general users?
- What tools and services at the operating system level have been restricted for general users?
- Who is responsible for patch management of SCADA terminals? Is there a procedure?
- Has an audit feature been enabled for all SCADA terminals?
- Is virus protection implemented? Is this software manually or automatically updated?

© State of NSW through Transport for NSW 2019

B.4. Assets

Important asset considerations for the electrical SCADA system include the following questions:

- Is asset data up to date for SCADA equipment?
- What is the capacity for new projects?
- What are the recommendations from other audit reports? Are these being implemented?
- Is there a list of assets (equipment, hardware and software) including age, obsolescence, possible replacement parts, warranty information and service level agreement information?

© State of NSW through Transport for NSW 2019