SULTANATE OF OMAN

هيئة تنظيم الكهرباء - عمان
AUTHORITY FOR ELECTRICITY REGULATION, OMAN

AUTHORITY FOR ELECTRICITY REGULATION

SCADA AND DCS CYBER SECURITY STANDARD

FIRST EDITION

AUGUST 2015

Contents

1. Introduction

This standard describes the baseline mandatory requirements for industrial control systems including SCADA and DCS. The licensees are required to comply with it and retain and provide evidence of compliance, both for internal and external audit.

In addition to the baseline which set the minimum requirements, each authorised entity may implement additional controls to mitigate specific risks identified as part of the authorised entity's risk assessment process.

2. Definitions

Table 1 below provides a list of the abbreviations used throughout this standard.

Table 1: Glossary

Abbreviation	Description
CSMS	Cyber Security Management System
DCS	Distributed Control System
DMZ	Demilitarized Zone
HMI	Human Machine Interface
SCADA	Supervisory Control and Data Acquisition
SPoA	Single Point of Accountability
SLA	Service Level Agreement

3. Baseline Mandatory Requirements

3.1 Establish effective governance of the SCADA/DCS environment

3.1.1 Single Point of Accountability

An ultimate Single Point of Accountability (SPoA) shall be identified for SCADA/DCS security, who shall be a member of the senior management team.

3.1.2 Cyber Security Management System

A SCADA/DCS cyber security management system (CSMS) shall be in place, and shall:

- Address SCADA and DCS cyber security explicitly (even if the CSMS is embedded into a larger enterprise-wide information security management system);
- Include in its scope all procedures and specifications of evidence to be retained in order to demonstrate compliance with this baseline standard and with any additional risk-based controls that have been selected;

- Be approved by the SPoA;
- Be formally communicated to all employees, contractors and relevant external parties;
- Be subject to regular review (at least annually or when significant changes occur).

3.1.3 Cyber security policy

A SCADA/DCS cyber security policy shall be in place, and shall:

- Address SCADA and DCS cyber security explicitly (even if the policy is embedded into a larger enterprise-wide information security policy);
- Provide high level commitment and direction with regards to SCADA and DCS cyber security;
- Be approved by the SPoA;
- Be formally communicated to all employees, contractors and relevant external parties;
- Be subject to regular review (at least annually or when significant changes occur).

3.1.4 Cyber security roles and responsibilities

SCADA/DCS cyber security roles and responsibilities shall be defined at all levels. Linkages between these and other related roles and responsibilities (e.g., IT security) shall be defined.

3.1.5 Asset management

SCADA/DCS asset management shall be in place such that up-to-date network and system drawings shall be maintained for each SCADA/DCS system, and an inventory of all SCADA/DCS system assets shall be maintained. At least the following shall be identified and maintained for each system/asset in the inventory:

- Name and description;
- Identification details (e.g., version number, serial number);
- Criticality (potentially based on site criticality);
- Owner (i.e., Person responsible for the system/asset);

3.1.6 Information security classification

A security classification scheme shall exist to mark sensitive SCADA/DCS system information as Confidential. Confidential information shall be protected from unauthorised access.

3.1.7 Exception handling

An exception procedure shall be in place to ensure that:

- Any part of the baseline standard that cannot be complied with for a given SCADA/DCS system/asset shall be documented and approved by the system/asset owner, the SPoA, and the Authority;
- Any aspect of the additional risk-based controls that have been selected but cannot be complied with for a given SCADA/DCS system/asset shall be documented and approved by the system/asset owner, the SPoA and the Authority.

3.1.8 Internal compliance audits

Internal auditing procedures shall be in place to check for compliance with the baseline standard and any additional risk-based controls that have been selected. Such internal audits shall take place on a regular basis, ensuring coverage of all SCADA/DCS systems/assets over a three year cycle.

3.1.9 Annual SCADA/DCS cyber security report

An annual report shall be provided to the Authority (as confidential) on the anniversary of the initial approval of the SCADA/DCS cyber security policy, which shall provide the Authority with assurance of the level to which the authorised entity is compliant with the mandatory standard. Suggested contents for the annual report are provided in Appendix A.

The Authority shall review the annual report and may decide to undertake its own audit to validate the authorised entity's annual report, or to audit areas not covered in the report should it consider the report to give some cause for concern.

3.2 Understand the business risk due to SCADA/DCS cyber security

In order to ensure that it is managed appropriately, SCADA/DCS cyber security risk management shall be linked to SCADA/DCS asset management and SCADA/DCS change management.

A SCADA/DCS cyber security risk assessment shall be carried out for each system/asset by appropriate personnel, which should include the system owner, the SPoA or appointed delegate, system users, and personnel with SCADA/DCS cyber security expertise.

The risk assessment shall be updated on an annual basis or whenever there is a significant:

- Change in threat levels;
- Change in system configuration;
- System upgrade;
- Change in system criticality.

The risk assessment shall, at a minimum, cover the following threat scenarios:

- Physical tampering;
- Local denial of service (DoS);
- DoS for remote connections;
- Loss of integrity of control/safety data;
- Unauthorised control/operation (via local access);
- Unauthorised control/operation (via remote access);
- Malware infection;
- Unauthorised access to critical/confidential data (e.g. network diagrams, IP addresses, passwords etc.);
- Loss of view of operations.

The risk assessment shall consider the likelihood and impact of each threat scenario, and determine a risk level for each scenario. There shall be at least three risk levels (e.g., High, Medium, Low).

The risk assessment results shall be documented and the risk treatment for each risk agreed, prioritised and actioned.

3.3 Establish and maintain secure SCADA/DCS systems and architecture

3.3.1 Baseline architectural requirements

For each SCADA/DCS system, the architecture shall comply with the following baseline requirements:

- Electronic and physical security perimeters shall be identified, along with all access points into the system;
- SCADA/DCS networks shall be segregated from corporate and all other networks, including the Internet. At least a three tier architecture shall be deployed, implementing a DMZ between SCADA/DCS networks and corporate and other networks;
- Where it is not feasible to implement a DMZ as the access point into a SCADA/DCS network, as a minimum a firewall shall be implemented at the access point;
- The boundary of control for the SCADA/DCS system shall not extend beyond the electronic security perimeter of the system i.e., it shall not be possible to issue controls to the SCADA/DCS system from outwith the electronic security perimeter;
- Wireless communications technologies shall only be used for sections of SCADA/DCS networks where there is no feasible alternative to provide critical functionality. In such

cases, the use of wireless communications shall be authorised by the system owner, and security controls shall be in place to ensure confidentiality, integrity, availability and non-repudiation.

3.3.2 Firewall configuration

All firewalls implemented shall be stateful inspection hardware firewalls. The firewall rules shall be configured to deny all traffic with the exception of traffic which is required explicitly for the system.

Firewalls shall be subject to a ruleset review at least annually, to ensure that only the necessary traffic is permitted. The firewall ruleset review shall not be carried out by the person responsible for maintaining the firewall ruleset.

3.3.3 Malware protection

All servers and workstations, and all other equipment capable of running malware protection, shall have malware protection installed and operational, which shall be kept up to date.

3.3.4 Patch management

From time to time software and hardware patches and updates may be made available by vendors for applications, operating systems and firmware. These patches may be to address security and/or application or functionality issues.

Operators shall maintain a patch management procedure, which shall include review of the applicability of the patch, the risk of not applying it and the risk of applying it, prior to making the decision to apply it or not. The procedure shall also consider the prioritisation of patch deployment.

Patches shall be verified to be authentic prior to installation on live systems.

Patches shall be tested prior to application on live systems.

Patches shall usually be applied with involvement and/or approval from the system vendor/supplier. However, in some circumstances operators may choose to apply patches without the vendor/supplier's approval subject to an appropriate risk assessment and testing/validation process.

It is recognised that under certain circumstances it may not be possible to apply patches to systems (e.g. legacy operating system or application or vendor advice that a patch is not safe or advised). In these cases alternative compensating controls shall be identified and deployed and an exception shall be requested (as per section 3.1.7) detailing the reason for not applying the patch and the compensating controls that have been identified and deployed.

3.3.5 Intrusion detection and intrusion prevention

Intrusion detection or intrusion detection and prevention systems shall be implemented for SCADA/DCS systems, as a minimum at the DMZ between the SCADA/DCS network and corporate and other networks.

3.3.6 Network monitoring

SCADA/DCS network traffic shall be monitored and logs retained for at least 6 months. Logs shall be used to investigate suspected cyber security incidents.

3.3.7 Dial-up modems

Dial-up modems shall not be used for direct remote access to SCADA/DCS systems.

3.3.8 Vulnerability assessment

Vulnerability assessment and/or testing shall be undertaken for SCADA/DCS systems on a regular basis, subject to risk assessment. Assessment/testing may include desktop reviews and lab testing or testing backup systems.

3.3.9 Physical security

Physical security controls shall be applied commensurate with risk assessment results. The baseline standard for physical security is that the following should be within a physical security perimeter i.e., a locked building or room with physical access controls:

- SCADA/DCS servers and workstations;
- SCADA/DCS networking equipment;
- SCADA/DCS field equipment and HMIs (displays) e.g., in substations.

3.3.10 User access management and user accounts

User access to SCADA/DCS systems and networks shall be managed, and shall ensure that the principles of least privilege and individual user management are followed wherever technically feasible. New users shall be formally authorised to use the system, and users who no longer require access shall have their access revoked promptly. User access shall be limited to areas of functionality which are necessary for the user to fulfil their role, so if a user's role changes, their level of access shall be changed promptly. User access management shall be linked to human resources management in order to ensure that only authorised personnel have user access to the system, and that authorisation is granted based on personnel screening processes commensurate with the criticality of the system to which access is to be authorised. SCADA/DCS systems and networks shall not have default or guest user accounts.

User accounts shall be subject to a review at least annually, to ensure that only valid accounts are configured. The user account review shall not be carried out by the person responsible for managing user accounts.

Account passwords shall be a minimum of 8 characters and contain at least one number, and be changed at least annually.

3.3.11 Removable media

The use of removable media shall be restricted to cases where there is no feasible alternative to provide critical functionality. In such cases the use shall be authorised by the system owner, only specified media shall be used and the media shall be scanned for malware prior to each use in the SCADA/DCS system. Unless otherwise authorised, all removable media ports shall be blocked and drivers disabled or removed from the system.

3.3.12 Engineering laptops

The use of engineering laptops for temporary connection to SCADA/DCS systems for engineering purposes shall be carefully managed. Dedicated engineering laptops shall be used which are never directly connected to the Internet or used for web or email access. Where data from external sources (e.g., configuration files) require to be copied onto an engineering laptop in order to be used with a SCADA/DCS system, the files shall be transferred onto the engineering laptop only via authorised and controlled removable media.

3.3.13 Change management

SCADA/DCS systems shall be subject to rigorous change management. This includes the control of changes to the configuration of SCADA/DCS network assets as well as upgrades.

All changes shall be authorised by the system owner and cyber security risk assessment shall be part of the change management process.

3.3.14 System hardening

Only software which is necessary for the correct functioning of the SCADA/DCS system shall be installed. Unnecessary software and services shall be removed, or disabled as a minimum. The SCADA/DCS system shall only have those services running and ports open on its network interfaces which are necessary for the correct functioning of the system.

3.3.15 Equipment disposal or redeployment

Disposal or redeployment of equipment from SCADA/DCS systems shall be managed to ensure that SCADA/DCS information security is protected. In this context information security includes the security of software code modules and data communications protocols.

3.4 Implement incident response, business continuity and disaster recovery plans for SCADA/DCS systems

All SCADA/DCS systems shall have a comprehensive and documented backup regime in place. This shall include regular backups and testing of the restoration process.

For each SCADA/DCS system plans shall be in place for incident response, business continuity and disaster recovery. These plans shall cover SCADA/DCS cyber security incidents explicitly, and at least the key threat scenarios identified during the risk assessment process.

A single plan may cover more than one system and can cover either a single system, groups of systems or whole site(s).

The incident response, business continuity and disaster recovery plans shall be reviewed, updated (if required), rehearsed and tested on at least an annual basis.

All SCADA/DCS cyber security incidents shall be documented and reported to the Authority.

3.5 Establish a SCADA/DCS cyber security training and awareness programme

A SCADA/DCS cyber security awareness programme shall be established which informs employees, contractors and relevant third party personnel of SCADA/DCS cyber security risks, trends and developments on a regular basis. Records shall be kept of all awareness activities and the personnel participating.

The SCADA/DCS cyber security awareness programme shall take input from publicly available sources, SCADA/DCS system and equipment suppliers and relevant national and international authorities. Such inputs shall be linked to SCADA/DCS risk management such that risk assessment may be triggered.

A reporting mechanism shall be in place to allow employees, contractors and third party personnel to report suspected SCADA/DCS cyber security risks or incidents.

A SCADA/DCS cyber security training plan shall be established to ensure that personnel responsible for SCADA/DCS cyber security have appropriate training to allow them to fulfil their roles. Operational and support staff shall have baseline training to ensure at least a basic understanding of SCADA/DCS cyber security requirements and their obligation to report suspected SCADA/DCS cyber security risks or incidents.

Records shall be kept of all training activities and the personnel attending, and plans shall be in place to ensure that training is kept up to date e.g., training for new personnel and refresher training for existing personnel.

3.6 Manage third party SCADA/DCS cyber security risks

Any connections from SCADA/DCS systems to third party systems shall be documented and authorised by the SCADA/DCS system owner.

Where there is a requirement for remote support of SCADA/DCS systems, secure connectivity solutions shall be implemented to ensure that:

- Communications outside of the electronic security perimeter are encrypted;
- Users are authenticated by user accounts with passwords which conform at least with the baseline password standard;
- User privileges are restricted to only those required to fulfil remote support roles.

Connectivity for remote access shall only be available when required and authorised by the system owner i.e., remote access connectivity shall not be in place permanently.

Third parties providing remote support services shall provide assurances to the authorised entity concerning their own security management arrangements, including but not limited to details of:

- IT/information security policy;
- Physical security at sites from which remote support is provided;
- Password management procedures for remote support passwords;
- Segregation of systems used to provide remote support;
- Security controls for systems used to provide remote support;
- Security controls for personnel providing remote support.

The requirement to comply with this baseline standard and any additional risk-based controls that have been selected shall be incorporated into contracts and service level agreements (SLAs) for remote support.

Support and maintenance arrangements shall be in place with SCADA/DCS system vendors, whether including remote support or not. These arrangements shall ensure that:

- The vendor discloses known and relevant cyber security vulnerabilities in any element of the system provided by them;
- The vendor provides tested and validated patches, workarounds or other fixes to known and relevant cyber security vulnerabilities in any element of the system provided by them. These patches, workarounds or other fixes shall be provided in a timely manner as defined in the SLA for the services provided;
- The vendor provides support and advice on applying security patches, workarounds or other fixes.

3.7 Ensure security controls are included in SCADA/DCS system changes and projects

Changes to SCADA/DCS systems shall only be made through formal change management which is linked to SCADA/DCS cyber security risk assessment and SCADA/DCS asset management.

All SCADA/DCS system change projects (such as significant modifications or upgrades), and SCADA/DCS implementation or replacement projects, shall:

- Include security requirements, for inclusion in specifications and tenders, as required to ensure compliance with the baseline standard and any additional risk-based controls that have been selected;
- A Security Assurance and Testing plan which describes how assurance will be provided that the required security controls are in place prior to the system being put into service;
- Have a single point of accountability for SCADA/DCS cyber security during the project lifecycle;
- Have a formal handover of SCADA/DCS cyber security responsibilities from the project into production, including acceptance into production of vendor support and maintenance arrangements as specified on support and maintenance contracts and SLAs.

Appendix A: *Annual report contents*

The annual report from each authorised entity could provide at least the following information:

- Report on the SCADA/DCS cyber security policy:
  - approval status,
  - date of last review,
  - date of last update,
  - policy changes since last report;
- Report on the SCADA/DCS CSMS:
  - approval status,
  - date of last review,
  - date of last update,
  - CSMS changes since last report;
- SCADA/DCS asset management statistics and details:
  - number of entries in asset inventory,
  - number of additions to asset inventory since last report,
  - number of changes to asset inventory since last report;
- SCADA/DCS cyber security baseline standard exceptions:
  - number and details of documented exceptions,
  - number of new documented exceptions since last report,
  - number of changes to documented exceptions since last report;
- SCADA/DCS cyber security internal audit statistics and details:
  - number of audits since last report,
  - scope of audits since last report,
  - audit observations (not requiring action) since last report,
  - audit findings (requiring action) since last report,
  - status of all open audit findings requiring action;
- SCADA/DCS cyber security risk management statistics and details:
  - number of annual risk assessments undertaken since last report,

  - number of risk assessments redone for other reasons since last report:
    - due to change in threat level,
    - due to change in system configuration,
    - due to system upgrade,
    - due to change in system criticality;
  - number of new risk assessments undertaken (for new systems/assets) since last report,
  - risk statistics (e.g., numbers of high risks, medium risks and low risks),
  - number of new risk treatment actions from annual or redone risk assessments since last report,
  - number of risk treatment actions from new risk assessments since last report,
  - status of all outstanding risk treatment actions (number of risk treatment actions outstanding for high risks, medium risks and low risks).
- SCADA/DCS architecture details:
  - number of firewalls in place,
  - number of wireless networks in place,
  - number and details of firewall ruleset reviews completed since last report,
  - number of patches made available by vender since last report,
  - number and details of patches applied since last report,
  - number and details of times network logs have been analysed since last report,
  - number and details of dial-up modems in use,
  - number and details of vulnerability assessments undertaken since last report,
  - number and details of physical security audits on SCADA/DCS locations since last report,
  - number and details of new, changed or revoked accounts since last report,
  - number and details of user accounts reviews carried out since last report,
  - number and details of authorisations to use removable media,
  - number and details of engineering laptops in use,
  - number and details of all changes progressed through change management since last report.

- SCADA/DCS incident response, business continuity and disaster recovery
  - Number of tests of restore process for backups,
  - Number of incident response plan reviews since last report,
  - Number and details of incident response plan updates since last report,
  - Number and details of incident response tests/rehearsals since last report,
  - Number and details of incidents triggering incident response since last report,
  - Number of business continuity plan reviews since last report,
  - Number and details of business continuity plan updates since last report,
  - Number and details of business continuity tests/rehearsals since last report,
  - Number and details of incidents triggering business continuity since last report,
  - Number of disaster recovery plan reviews since last report,
  - Number and details of disaster recovery plan updates since last report,
  - Number and details of disaster recovery tests/rehearsals since last report,
  - Number and details of incidents triggering disaster recovery since last report,
- SCADA/DCS cyber security incident statistics and details:
  - number of suspected incidents reported since last report,
  - number of suspected incidents investigated since last report,
  - incident investigation findings and conclusions since last report,
  - status of all open incident investigation findings requiring action.
- SCADA/DCS cyber security training and awareness:
  - Number and details of awareness activities since last report,
  - Number and details of risk assessments triggered through awareness inputs since last report,
  - Number and details of reported suspected SCADA/DCS cyber security risks or incidents since last report,
  - Number and details of all SCADA/DCS cyber security training activities since last report.
- Third party SCADA/DCS cyber security risks:
  - Number and details of all connections from SCADA/DCS systems to third party systems,

  - Details of assurances sought from third parties providing remote support services since last report,
  - Number of support and maintenance arrangements reviewed since last report, and details of findings.
- SCADA/DCS system changes and projects:
  - Number and detail of SCADA/DCS change projects currently in progress;
  - Number and detail of SCADA/DCS implementation or replacement projects currently in progress.