

AN OVERVIEW OF WSSA SCADA GUIDELINES

Luke Hellowell – Manager Operational Technology and Energy @ Seqwater
May 2018

WSA 302-2018 SCADA GUIDELINE V2.0



AGENDA

Background

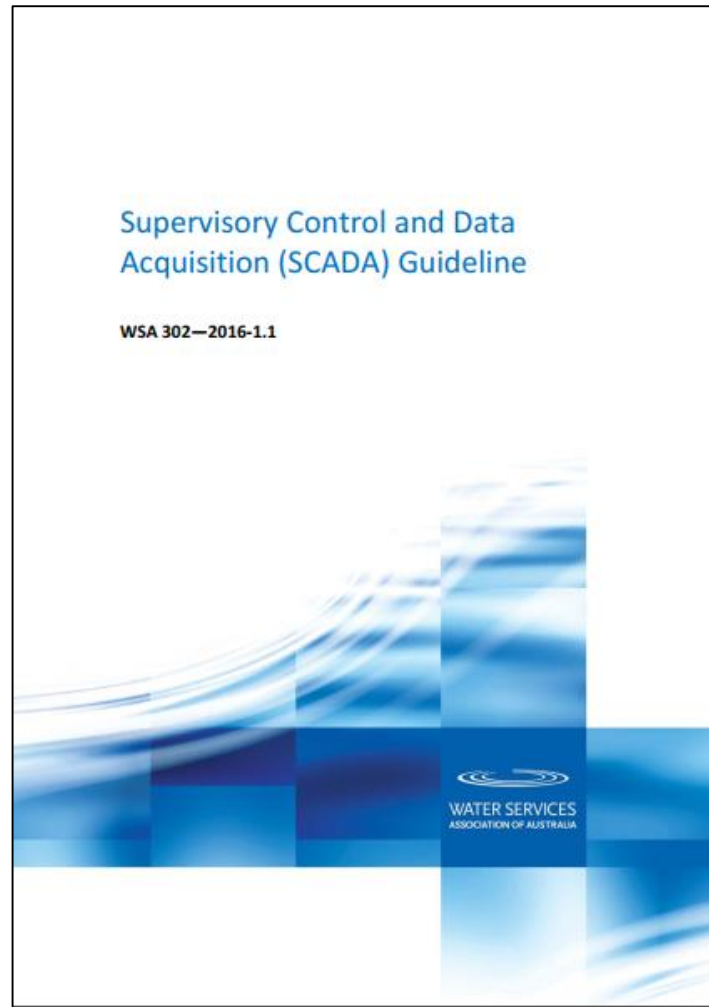
Contents

Maturity Model

Cybersecurity

Availability

Community



BACKGROUND – PROJECT NEED

Individual utilities have developed a range of standards associated with their SCADA systems from the very basic to the highly sophisticated dependent upon organisational strategy, size or capability.

These standards are generally prepared in isolation and do not provide clear benefits across different utilities nor to the wider market place in providing SCADA solutions.

There is also no clear guidance to current industry practice in application of SCADA systems to water utilities.

BACKGROUND – STAGE 1 – 2015/16

It was considered that it would be highly beneficial to all water utilities if there were a common set of standards or guidelines that were available for all aspects of the SCADA lifecycle.

The Mechanical, Electrical and SCADA (MES) CoP recommended a project to produce a WSAA endorsed SCADA Guidelines which would provide direction in the development and implementation of SCADA systems for the Australian Water Industry.

BACKGROUND – STAGE 2 – 2017/18

Expand the scope to cover field equipment and Data Analytics/Business intelligence in respect to SCADA data.

Update the Guideline to address a range of suggestions in relation to the Guideline and in particular to provide a detailed tool to assist with benchmarking the SCADA Maturity model.

Update any errors, omissions or improvements (including statutory and regulatory) identified prior to the release.

BACKGROUND - PARTICIPANTS

STAGE 1

- Mark Abela (TasWater)
- Jim Baker (Water Corporation)
- Matthew Grills (Barwon Water)
- Luke Hellowell (Seqwater)
- Scott Humphreys (Water NSW)
- Matthew Nicholson (East Gippsland Water)
- Ben O'Halloran (Coliban Water)
- Dan Smith (Coliban Water)
- Michael Wassell (Sydney Water)

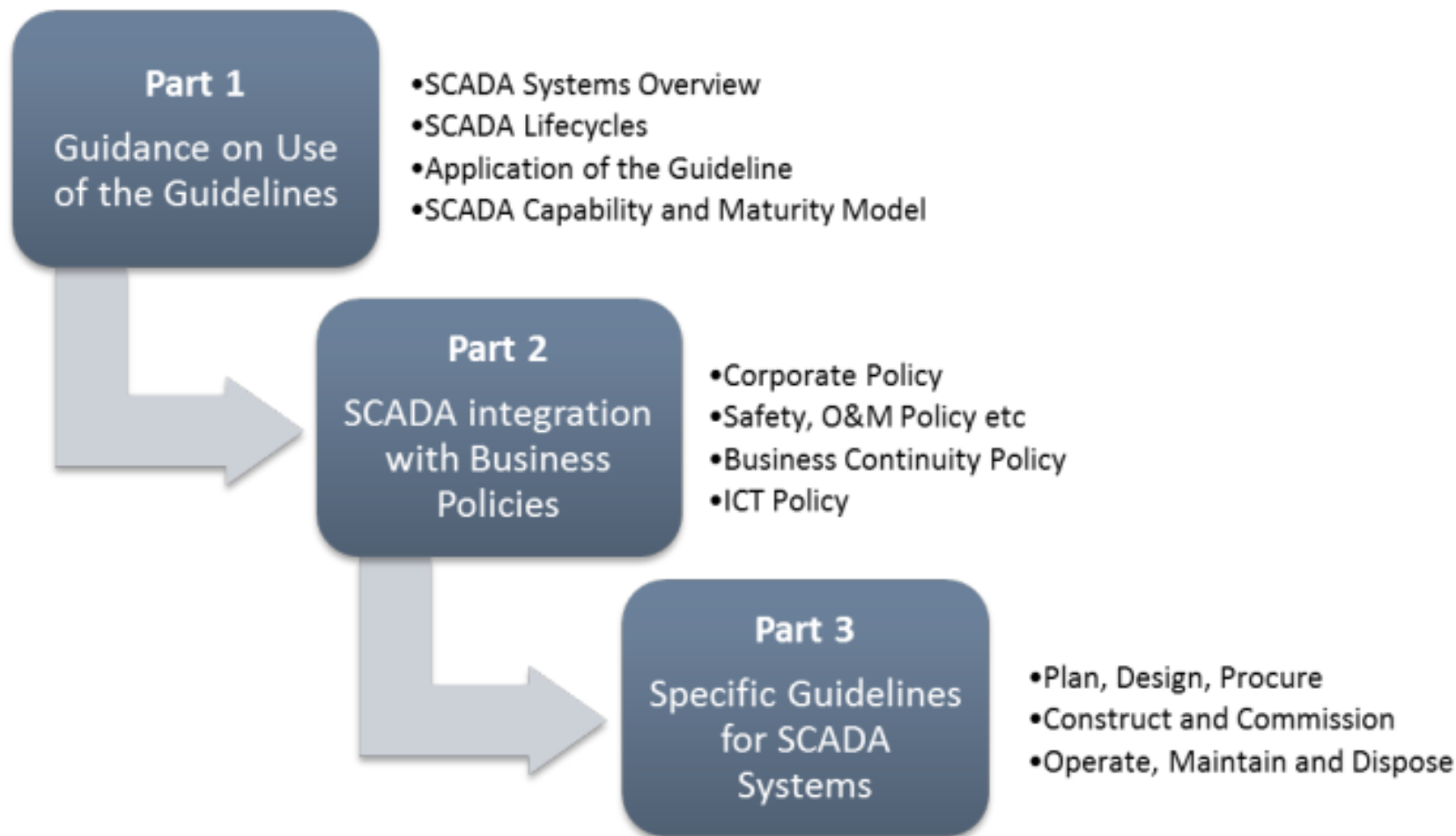


STAGE 2

- Michael Wassell (Sydney Water)
- Jim Baker (Water Corporation_)
- Ross Foster (SA Water)
- Daniel Smith (Coliban Water)
- Luke Hellowell (Seqwater)
- Russell Riding (Melbourne Water)
- Deva Chinnarajan (Lower Murray Water)



CONTENT - STRUCTURE

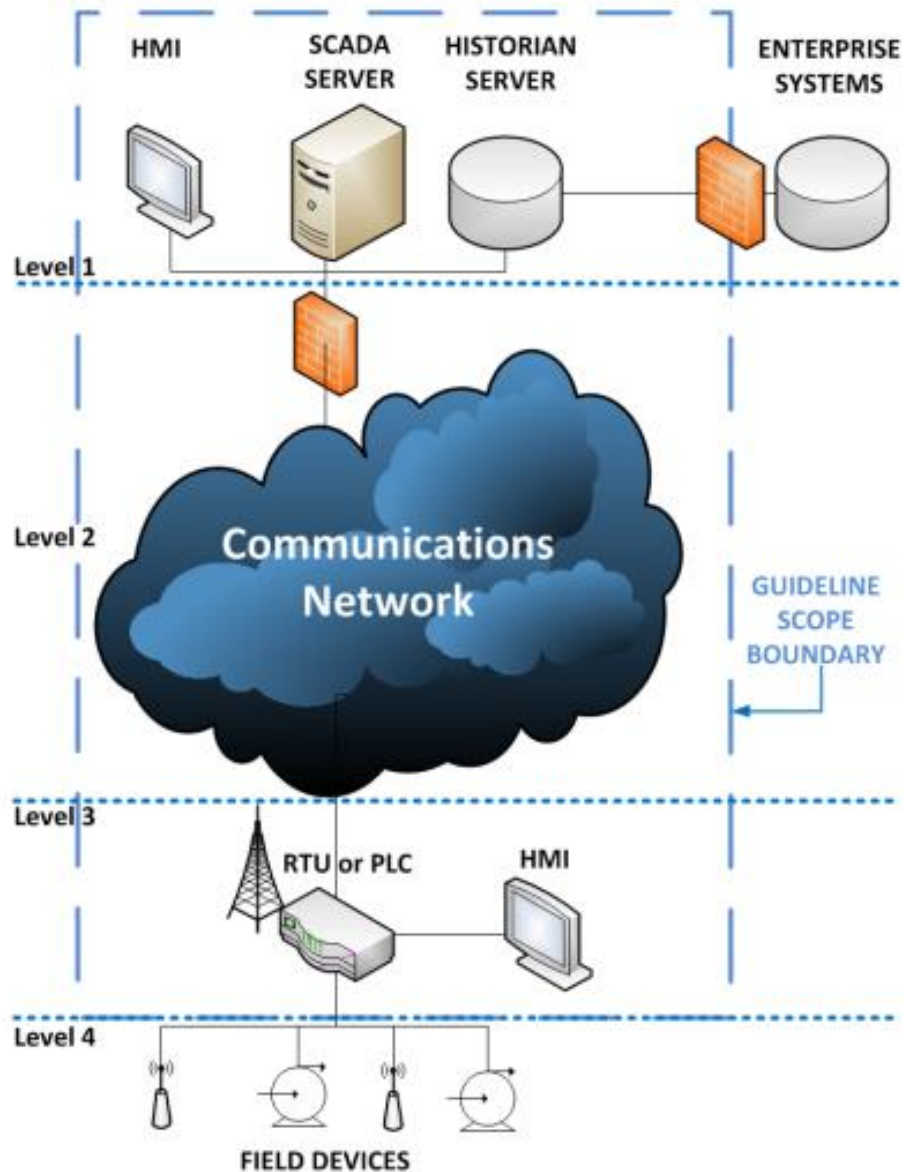


CONTENT - STRUCTURE

STRUCTURE OF GUIDELINE SECTIONS

Level	Heading	Purpose
X.X.1	Rationale/Overview	This outlines the context of what this section of the Guideline is covering, key definitions for major topics and key concepts. This section is purely informative, which may guide the application process.
X.X.2	Minimum Acceptable Requirements	These are normative requirements that are the minimum level acceptable that a Water Agency seeking to implement the Guideline will implement. These typically are correlated to the Level 2 of the Capability Maturity Model.
X.X.3	Good Practice	These are normative requirements that are recognised as providing good level of performance that meets the technical needs of a Water Agency. These typically are correlated to the Level 3 or Level 4 of the Capability Maturity Model.
X.X.4	Best Practice	These may be at times aspirational practices and requirements which however are still practical and achievable and are recognised as providing a Water Agency the best results to achieve high levels of performance. These typically are correlated to the Level 4 or Level 5 of the Capability Maturity Model.
X.X.5	References	This contains informative relevant industry reference documentation that outlines material that may be used to help a Water Agency apply the Guideline.
X.X.6	Examples	This contains informative examples of how other Water Agencies have implemented processes, requirements and practices to meet requirements of this Guideline for this section.

CONTENT - SCOPE



CONTENT – MATURITY MODEL

Domain/ Level	Vision & Strategy	Organisation & Structure	Technology	Operations & Maintenance	Standards	Customer	Benefits
5	<ul style="list-style-type: none"> SCADA supports organisations customer objectives New business model opportunities arise Continued Whole of Business based investment in SCADA 	<ul style="list-style-type: none"> Culture drives ongoing process improvement across value chain Collaboration with partners, suppliers is entrenched across Whole Of Business Readily adapt to changes in the environment e.g. regulatory SCADA innovation is encouraged and rewarded 	<ul style="list-style-type: none"> Seamless integration extends enterprise systems to workforce, customers and partners Autonomous decision support systems integrated across core business processes Predictive Analytics integrated into SCADA operations and drives business efficiencies SCADA architecture and technology meets WSAA Best Practice guidelines 	<ul style="list-style-type: none"> Systems Operations Centre meets or exceeds best practice A complete view of assets is available in the field in real time – and available to service partners SCADA Operations and Maintenance meets WSAA Best Practice guidelines BCP regularly exercised Comprehensive KPIs in place and met Comprehensive SCMP in place 	<ul style="list-style-type: none"> SCADA Standards aligned with WSAA Best Practice guidelines Corporation wide change management standards enforced across all critical Business Information Systems SCADA software libraries and templates enforce standards SCADA Security meets DSD Best Practice guidelines 	<ul style="list-style-type: none"> Customers raise service requests from their mobile device (BYOO) Organisation is regarded as supplier of choice with a reputation for quality, safety, reliability and cost-effectiveness Customer satisfaction rating meets defined Best Practice 	<ul style="list-style-type: none"> Benefits KPIs meet defined best practice Benefits are acknowledged at Board level and utilised in development of Corporate Strategy
4	<ul style="list-style-type: none"> Whole of business SCADA governance implemented and refined Whole of business SCADA Policy implemented SCADA vision aligned with and contributes to Corp Strategy SCADA is recognised as core competency 	<ul style="list-style-type: none"> SCADA has increased workforce skills and competencies Staff utilise SCADA in value add activities, more complex problem solving Increased maturity allows leadership to drive further productivity Promotion & reward of cross functional planning, design & operations 	<ul style="list-style-type: none"> Extended enterprise & customer integration implemented SCADA architecture is integrated – reduces cost & time to implement End to end system integration implemented Framework Agreements in place for all core technologies Technology stack aligns with Corporate Strategy Decision Support systems implemented Data Analytics in place to utilise SCADA data 	<ul style="list-style-type: none"> Dedicated Systems Operations Centre (SOC) in place SCADA data used to drive operational and maintenance strategies Monitoring of key KPIs done in real time SCADA Operations and Maintenance meets or better WSAA Good Practice guidelines Comprehensive Disaster Recovery Plans and BCP's in place and audited 	<ul style="list-style-type: none"> Comprehensive SCADA Standards in place covering all Agency SCADA Systems Corporate wide Data Standards utilised for SCADA and all critical information Systems Alarm Management Standards in place and audited SCADA Configuration Change Management standards mandated and audited SCADA Security meets DSD Good Practice guidelines 	<ul style="list-style-type: none"> Customer has direct access to critical SCADA data and field work status Customers can request a greater range of information via multiple medium Services expand to provide regular updates on planned outages Customer satisfaction rating meets defined Good Practice 	<ul style="list-style-type: none"> Benefits KPIs meet defined good practice Benefits are acknowledged at CFO level and utilised in development of Business strategy
3	<ul style="list-style-type: none"> SCADA vision and strategy approved across whole of business SCADA Policy developed Funding supports the Whole Of Business investment Management KPIs incorporate SCADA strategy Whole Of Business governance developed 	<ul style="list-style-type: none"> SCADA strategy drives organisational change and priorities Workforce training and recruitment requirements embedded SCADA KPIs linked to compensation and SCADA milestones Organisation is aligned around end-to-end processes Dedicated SCADA SMEs embedded in business 	<ul style="list-style-type: none"> Decisions made on future evolution of SCADA architecture Extended enterprise SCADA integration is designed Rationalisation of all core technologies underway Core technology stack is vendor independent (facilitates change of different levels of SCADA architecture independent of others) 	<ul style="list-style-type: none"> SCADA Operations and Maintenance integrated with key business processes SCADA system performance and KPI's analysed on a regular basis Workforce deployed based on skills, location etc. Basic Disaster Recovery and Business Continuity Plans in place 24x7 support in place for all aspects of SCADA system operations 	<ul style="list-style-type: none"> Detailed SCADA Standards in place for individual SCADA systems Detailed I&C Standards developed Detailed interface standards in place Detailed Data Standards in place for all aspects of SCADA systems Coding Standards defined for SCADA software SCADA Configuration Change Management standards in place SCADA Security Policy in place 	<ul style="list-style-type: none"> Whole Of Business customer interaction strategy developed in line with SCADA vision Service requests initiated directly from customer systems SCADA provides near real time status updates to the end customer Customer Survey incorporated into KPI's 	<ul style="list-style-type: none"> Benefits Register aligned with Corporate and KPIs defined Benefits are acknowledged at CM level and utilised in development of Divisional strategy
2	<ul style="list-style-type: none"> Funding approved for SCADA investment Operational investment aligned to Business Unit strategy Clear ownership and accountability defined for SCADA operations and maintenance 	<ul style="list-style-type: none"> Workforce awareness of SCADA efforts Competency needs recognised Organisational training needs have been identified and planning being undertaken 	<ul style="list-style-type: none"> Tactical SCADA solutions are rolled out with limited integration Data quality improvement in place 	<ul style="list-style-type: none"> Business unit level rollouts continue Work orders issued and data captured electronically Accountability for alarm handling and response defined SCADA workforce skills captured electronically Basic support and maintenance services in place 	<ul style="list-style-type: none"> Basic SCADA standards developed for hardware and software Basic I&C Standards developed Basic interface standards in place Basic Data Standards in place for SCADA systems Basic SCADA Security standards in place 	<ul style="list-style-type: none"> Customer service processes are streamlined based on Business Unit implementations of SCADA Research undertaken on customer advice services options e.g. Web, SMS, social media Formalised customer feedback process implemented 	<ul style="list-style-type: none"> Benefits Register implemented at local business level Benefits tracking reviewed on a regular basis
1	<ul style="list-style-type: none"> Business Unit based trials begin Experimentation is supported SCADA goal is operational improvement 	<ul style="list-style-type: none"> Formal & Informal discussions within Business Unit in relation to SCADA Recognition of need to build SCADA capability Leadership initiates SCADA awareness 	<ul style="list-style-type: none"> Organisation recognises SCADA needs Technical evaluation of infrastructure proposed SCADA technology pilots underway 	<ul style="list-style-type: none"> Business case development Asset & workforce systems & equipment being evaluated No clear accountability for alarm handling and response Maintenance processes ad-hoc or reactive 	<ul style="list-style-type: none"> No SCADA Standards in place Solutions are engineered on a project by project basis 	<ul style="list-style-type: none"> Research conducted into how SCADA can improve customer experience Baseline levels of customer satisfaction are recorded Customer Requests are via e-mail and/or ad hoc 	<ul style="list-style-type: none"> No formal benefit capture process in place Expected benefits being developed

CONTENT - OVERVIEW

WSA 302—2016-1.1

56

TABLE 7.1
EXAMPLE CHECKLIST OF BUSINESS INTERDEPENDENCY

Driver	Context	Interdependency	Chk
Asset Management	A Water Agency's operational license agreement will generally require efficient operation of its supply area which shall be measurable by internal and external KPIs.	SCADA systems shall be designed to meet the asset management lifecycle requirements.	
	The availability and reliability of SCADA assets for the purposes of reporting and decision making is crucial to meeting those obligations.	SCADA systems shall be included in the asset management plans for the Water Agency.	
		The performance of SCADA systems shall allow for the asset management strategies to be delivered.	
Enterprise Data Warehouse	NOTES: Enterprise Data Warehouses are centralised repositories of data from one or more sources.	The SCADA system shall be designed to provide interface with the Enterprise Data Warehouse requirements of the Water Agency.	
	NOTES: They store current and historical data and are used for creating reports including but not limited to engineering analysis and business applications for such as annual operational reporting.		
Energy Management	NOTES: Energy management systems can be used to centrally monitor and/or control plant and equipment across the SCADA system monitored locations.	SCADA systems shall be designed to monitor, measure, and/or control the Water Agencies electrical loads in the system.	
	NOTES: Energy management systems can also provide metering and monitoring functions that allow the Water Agency to gather data and insight that allows them to make more informed decisions about energy activities across their sites.	Implementation of remote control functions for energy management shall be assessed as part of their risk strategies for each plant that may be controlled.	

COPYRIGHT

70

has what specific SCADA system requirements are needed for the initial and procurement process. As project planning is an iterative process, this is stated over the lifecycle of the SCADA system and specific projects.

RATEGY

Overview

gy defines the vision and the roadmap for the implementation and DA within a Water Agency. The purpose of a SCADA Strategy is to obtain approval for the required investment and outcomes expected of the SCADA defined period. The purpose of obtaining executive level buy-in is to ensure the strategy is adhered to across organisational boundaries.

gy will typically be informed by a number of other key organisational inter-dependent systems. These are discussed further in Part 2 of this

gy should be a key input to the planning and implementation of all work within a Water Agency.

gy will typically be based on key stakeholder requirements.

er to ensure that a SCADA Strategy is successfully implemented is to enshrine in policy and underpinned by appropriate standards. The shall be used by the Water Agency to guide or supplement long term plans.

acceptable requirements

gy shall have a defined SCADA Strategy in place.

gy shall be endorsed/approved at executive level (or a level that will have credibility) within the Water Agency.

gy shall define clear objectives and timeframes for the implementation of a Water Agency.

gy shall ensure accountability for the development and ongoing review/update of the strategy within a Water Agency.

gy shall be reviewed at least once every two years.

gy shall address key issues associated with Vendor selection and no reliance on a single Vendor, pre-qualification etc.).

gy shall define the required level of monitoring and/or automation for SCADA within a Water Agency.

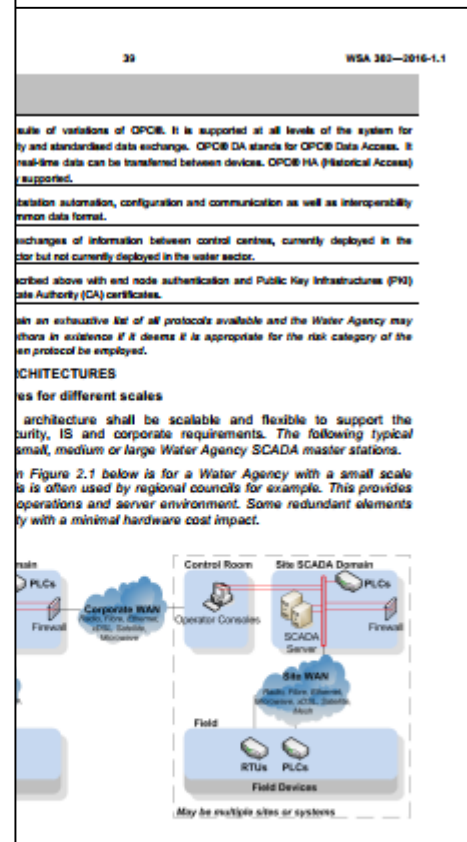
gy shall define the required governance for SCADA within a Water Agency.

gy shall define accountability for all aspects of the SCADA Lifecycle from procurement to disposal.

gy shall be reviewed and updated annually.

gy shall ensure that key strategic objectives are met and that the SCADA project is successful.

COPYRIGHT



CONTENT – APPENDICIES



Process Alarms are a control measure employed to manage and reduce the likely consequence of ignoring an alarm, all other risk mitigation strategies are (such as configured process interlocks, pressure relief devices, redundant ex of the consequence occurring if the alarm is triggered is typically incorporated required response" assessment. Refer to Appendix C: Alarm Priority Determin examples on how this assessment can be undertaken. Optionally likelihood a more quantitative approach.

6.4.3 Priority Distribution

An ideal future state of the alarm system will target a distribution of configured will assist in achieving an appropriate ratio of Critical, Conditional High, High during operation that is ergonomically acceptable to the operator.

Table 2 Priority Distribution

Alarm Severity	Configured Alarms
Critical	5% of total
High / Conditional High	15% of total
Low	80% of total

6.5 Other event notification types

In addition to the above alarms which are enunciated on the alarm list and event types are also in use. Process and System events which do not meet above may be displayed in the Control System as one of the following:

Table 3 Other Event Types

Notification Type	Usage
Event (Journal)	An event which requires historical cap Log but no operator action. It is not an operator.
Maintenance Alarm	This alarm does not require action from initiates a maintenance action

Event/Journal level abnormal events are those that require no operator notification alarms are typically assigned for user actions, normal device operations, equipment records.

Maintenance Alarm events are that require the Electrical/Mechanical to fix a device. This works would typically be fixed within a 4 week period.

The use of process deviation alarms shall be restricted to those important to alarms are unable to provide adequate warnings, for example because the depending on the operator setpoint. Where used, the deviation setpoints shall generation of chattering alarms, particularly during normal operator response Suppressing such alarms during operator changes to the controller setpoint

To minimise the incidence of nuisance, irrelevant and chattering alarms, the following:

6.5.1 Deadbands and Filters

Alarm deadbands, input filters and debounce timers shall be set carefully to

Title Record No: 1201589
Issue Date: 14 November 2014

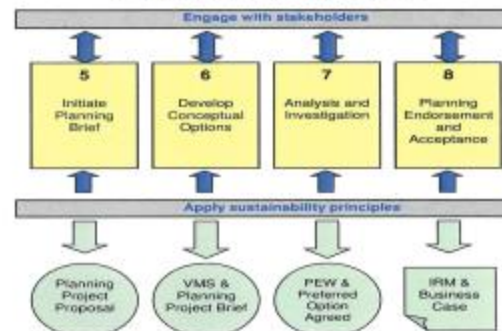
Document No: AN5MAN04
Unless Stated/this document is Uncontrolled
Scada Alarm Philosophy

Sydney Water Integrated Instrumentation & Telemetry System (IICATS) Alarm Management Philosophy



Asset Acquisition Guideline

Figure 4: Infrastructure Planning Branch Process



A diagram that shows the Infrastructure Planning activities is available from [About the process - Planning Phase](#) on the Asset Acquisition Process WaterNet site.

5.1.3 Plan Land Servicing

Development Services Branch facilitate the planning and provision of water services for land and building development and secures existing and future water infrastructure through the land planning process. The process contributes on average over \$200 million in reticulation assets and headwork's charges and connects approximately 20,000 new customers annually.

Reticulation is funded and provided by the developer. Headworks and distribution assets, are funded by the Corporation and their asset acquisition is managed as part of the CIP. Further information is available on the Development Services Branch WaterNet site, in particular in the Developers Manual aquaDOC #601933.

Where a developer requires specific headworks (usually distribution assets) earlier than the date planned in the CIP, those headworks may be funded by the developer. If the headworks being funded by the developer meet the requirements of PCY330 Prefunding of Headworks and as detailed in S362 Infrastructure Prefunding, the developer will be reimbursed in accordance with an agreed Developer's Constructed Works Scoping Agreement (DCSWA) and Developer's Constructed Works Agreement (DCWA).

Specific procedures apply to projects funded by developers, irrespective of whether they are constructed by a contractor or by the Corporation acting as a contractor, and more detail is available in the Developers Manual or Advanced Works Manual. The provision of headworks assets outside the 5 year CIP, or unplanned for, to serve what was previously referred to as 'pioneer' development, are planned for and funded by the developer, then transferred to the Corporation where it agrees to be the service provider.

CYBERSECURITY – ARCHITECTURE GUIDELINES

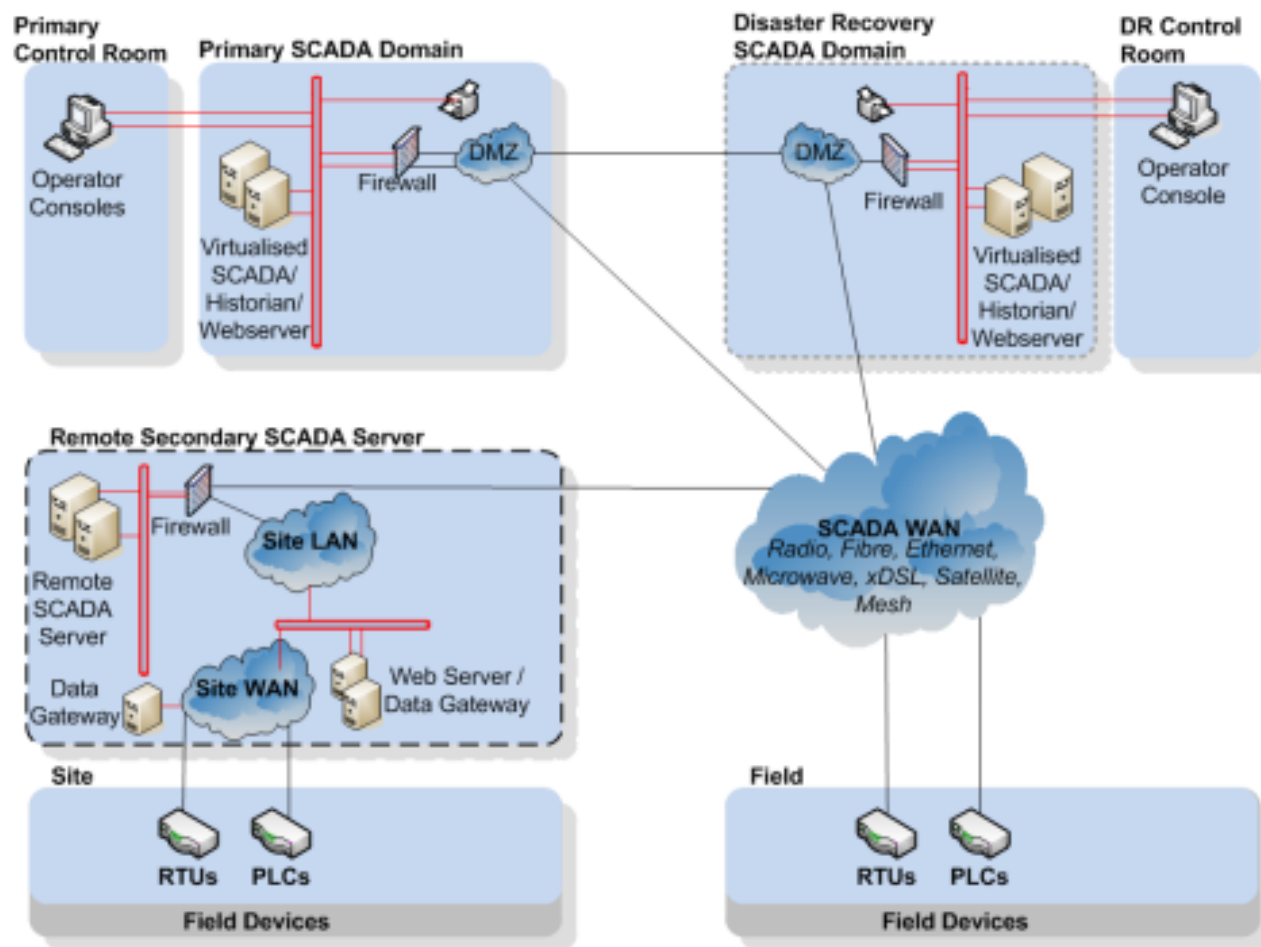


FIGURE 2.2 EXAMPLE MEDIUM SCALE WATER AGENCY CENTRALISED SCADA ARCHITECTURE

CYBERSECURITY – AREAS OF FOCUS

PART 2 - SCADA INTEGRATION WITH BUSINESS POLICIES

Section 12.1 ICT Infrastructure

PART 3 - SPECIFIC GUIDELINES FOR SCADA SYSTEMS

Section 16.7 Design – Non-functional Requirements

Section 20.12 Operate And Maintain

CROSS-REFERENCE OF TECHNICAL AREAS OVER LIFECYCLE

Area	High Level Requirements	Plan, Design, Procure	Construct Commission	Operate, Maintain, Dispose
Architecture	Part 2, 11	Part 3, 14.6 Part 3, 14.7 Part 3, 15.2		Part 3, 20.14
Alarms		Part 3, 15.8		Part 3, 20.4
SCADA Communications		Part 3, 15.3 Part 3, 15.4 Part 3, 15.5 Part 3, 15.6		Part 3, 20.13
Performance and Specifications	Part 2, 7 Part 2, 11	Part 3, 15.4	Part 3, 19.8 Part 3, 19.9	Part 3, 20.2 Part 3, 20.3 Part 3, 20.9 Part 3, 20.11
HMI		Part 3, 15.10		Part 3, 16.3
Control		Part 3, 15.9		Part 3, 20.13
Security	Part 2, 12	Part 3, 16.7		Part 3, 20.12
Trending and Reporting		Part 3, 15.13		

CYBERSECURITY – HIGH LEVEL REQUIREMENTS

12 ICT INFRASTRUCTURE

12.1 Rationale/overview

A Water Agency should generally have in place a specific ICT Security policy. Given the strong interdependency of SCADA systems on ICT infrastructure for transmission, storage and use, any ICT infrastructure security policy will have a large impact on SCADA systems and vice versa.

12.2.2 Minimum acceptable requirements

The Water Agency shall conduct a risk assessment on the potential impact of compromised security on the SCADA system, and use this assessment to inform strategy outcomes.

The Water Agency shall have a defined ICT infrastructure security policy in place that considers the requirements of a SCADA system to use or be accessed through ICT infrastructure.

The Water Agency shall have a defined process in place for managing any changes to legislation, relevant standards or recommendations that may impact their existing security processes or policies.

For an IT infrastructure security policy, the impact and interaction between the IT infrastructure backbone and the SCADA system shall consider:

(a) Access to SCADA server control and configuration through corporate IT system.

(b)

CYBERSECURITY – PLAN DESIGN PROCURE

16.7 SCADA SECURITY

16.7.1 Rationale/overview

As a Water Agency is responsible for managing critical infrastructure, customer records, and complex sites the security of a Water Agency SCADA system is vital. The benefits of taking adequate controls for security have to be measured against the cost of implementation and the risk of a security breach. This section provides Water Agency specific advice for SCADA security.

There is substantial literature and guidelines for SCADA system security, in particularly for critical infrastructure produced by TISN. The full list of appropriate standards is provided in the references.

16.7.2 Minimum acceptable requirements

The Water Agency shall have accountable resources in place with clearly defined responsibilities to manage SCADA security

Subject to a risk assessment, the Water Agency shall adopt a documented and standardised defence in depth approach. This shall include:

- (a) Secure access control;
- (b) Role and security levels management;
- (c) Standardised physical security and access control based on roles and responsibilities, in line with the Water Agency's site access requirements;
- (h)

CYBERSECURITY – OPERATE MAINTAIN DISPOSE

20.12 SECURITY

20.12.1 Rationale/overview

As part of the ongoing security management of the system, this section outlines general security requirements that shall be considered by a Water Agency.

It is important to ensure that the SCADA system is maintained kept up to date with the current versions of applications and operating systems to ensure that known vulnerabilities and performance issues are upgraded in a timely manner. Using the latest software upgrades may also expose the Water Agency to software stability risk. The Water Agency shall balance the needs of security against the risk of availability performance impacts. It is imperative to liaise with the vendors regarding their procedures for testing their own software developments and the testing of the interaction of their software with updates to underlying, possibly third party, operating systems.

20.12.2 Minimum acceptable requirements

20.12.2.1 General monitoring

20.12.2.2 Manage access

20.12.2.3 Asset register

20.12.2.4 Specific security upgrades

20.12.2.5 OS patching and application patching

20.12.2.6 Hardware and software upgrades

20.12.2.7 Management of keys

13

WSA 302 — 2018

A2SECTION 3 AND 4 - DESIGN EXAMPLES

A2.1INTRODUCTION

This Appendix outlines detailed examples of topics covered by Section 3 and 4 covering the different stages of Design of a SCADA system. This includes SCADA security, architecture, alarm management, control and automation.

A2.2SCADA SECURITY

A2.2.1 System Security

(a) Compartmentalise the Network - The network shall be subdivided into compartments to compartmentalise and segregate the network. This shall be achieved by implementing:

- (i) A firewall protected network connection between the SCADA network and External networks.
- (ii) A firewall with Deep Packet Inspection (DPI) capability together with intrusion detection and prevention.
- (iii) A Demilitarized Zone (DMZ) shall be established between the SCADA network and the business network. Any future connection to external provider IP network or establishment of a Data Warehouse shall take place in the DMZ.
- (iv) A firewall which shall be configured to limit communication traffic to that which is essential.
- (v) Modems provided for connection to alarm paging services shall be dial out only. Modems provided for PSTN connection to remote sites shall be connected to an RTU and not commercial- off-the-shelf computer or network equipment. PSTN Modems should have hardware Keylocks on them.
- (vi) Process control networks shall be autonomous and shall not rely upon the SCADA network for their operation; remote sites shall continue to operate and store data even while there is no radio connectivity to the SCADA system.
- (vii) Communication between the SCADA network and Process Control networks shall be hard wired wherever possible.
- (viii) Where serial communication between the SCADA network and a Process Control network is unavoidable, the RTU and PLC shall be configured to minimise the danger of reprogramming the PLC or corruption of its control data via the serial port.
- (ix) There shall be no connection between the Process Control networks and External Networks. The process control networks can include standalone Ethernet I/O networks.
- (x) Where possible, radio communications shall be encrypted. With a minimum standard of AES-128. This is dependent on available technology and hardware installed at remote sites.

(b) Hardening the Network - The network shall be hardening against threats by implementing the following:

- (i) At the time of first connection of any computer equipment to SCADA a review shall be carried out to determine which services can be safely disabled without impact on normal SCADA operation. This shall form part of the SCADA standard operating environment.

14

WSA 302 — 2018

- (ii) These services shall be disabled and shall require justification and SCADA System Administrator authority to be re-enabled.
- (iii) All network daemons that are not required for legitimate SCADA and Process Control communication functions shall be removed.
- (iv) No SCADA workstation, file server, Historian server, or general purpose computer which is connected to the SCADA network shall have e-mail client software installed.
- (v) SCADA servers that require the installation of e-mail client software for alarm messaging shall have the receipt of e-mails disabled and shall require justification and SCADA System Administrator authority to be re-enabled.
- (vi) CD/DVD and external USB drive usage shall be restricted to authorised users only.
- (vii) The installation of word processing and spreadsheet software on SCADA connected computers shall be limited to those computers where it is strictly necessary for operational reasons and subject to the case-by-case approval of the SCADA System Administrator.
- (viii) No SCADA connected computer shall have internet browsing software activated.

A2.2.2Existing PLCs - Various Form Factors

FIGURE A2.2.5
Example architectures for controllers.



Connection to the Process Group controller that requires a large amount of data shall be by means of an Ethernet connection (Modbus* TCP/IP, Profinet* or EthernetIP*) with the ultimate selection of protocol being determined by the ability to support natively the proposed connections on both devices. That is, using the branded Network Interface Cards / on-board ports at both the controller, without the use of gateways or 3rd party cards.

Connection to the Process Group controller that requires a small amount of data and interlocks shall be by means of hardwiring from a remote I/O node on the new installation. Where there is not a solution that meets the criteria above the designer and supplier shall

WSAA Shop: Guidelines and manuals

[Sydney Water Codes](#)[Melbourne Retail Water Agencies Codes](#)[Hunter Water Codes](#)[WSAA Codes](#)[Superseded Codes](#)[Compendia](#)[Guidelines and manuals](#)

[Home](#) > [WSAA Shop](#) > Guidelines and manuals

Guidelines and manuals


There are a total of 7 products in this category.

Name	Type	Label	Date	Price
Failure Modes in Pressurised Pipeline Systems	PDF		August 2012	Free
WSA 302 SCADA Guideline	PDF	PC061	January 2016	\$250.00
H2S Hydrogen Sulphide Control Manual Volume 1 & 2	PDF	PP007	December 1989	\$275.00
Australian Sewage Quality Management Guidelines	PDF	PC040	June 2012	\$495.00

COMMUNITY



WATER SERVICES
ASSOCIATION OF AUSTRALIA

[Events](#) | [Community](#) | [Groups](#) | [WSAA Shop](#) | [Luke Hellowell](#)  | [Log out](#)

[Home](#)

[About us](#)

[WSAA Shop](#)

[News](#)

[Publications](#)



[Home](#) > [Community](#) > [Project](#) > SCADA Guidelines Stage 2 (UE-Sub16) Project

SCADA GUIDELINES STAGE 2 (UE-SUB16)

The initial release of the SCADA Guidelines was limited in scope due to available finance; hence it did not address field equipment nor Data Analytics/Business Intelligence due to time and resource constraints. At the completion of the guidelines, feedback from participating organisations was that the guidelines should include these areas as well as a range of other feedback (eighteen to date) for a future release of the Guidelines.

The project proposes to undertake an update to the SCADA Guidelines (Version 1.0), recently released, to expand the scope to cover field equipment and Data Analytics/Business Intelligence in respect to SCADA data. The project would also update the Guideline to address a range of suggestions in relation to the Guideline and in particular to provide a detailed tool to assist with benchmarking the SCADA Maturity model.

In addition to increasing the scope of the Guideline the project would also update any errors, omissions or improvements (including statutory and regulatory) identified prior to the release.

GHD was engaged to deliver this project.

The project delivery team for this project are: Michael Wassell (Sydney Water), Jim Baker (Water Corporation), Ross Foster (SA Water), Daniel Smith Coliban Water), Luke Hellowell (Seqwater), Russell Riding (Melbourne Water) and Deva Chinnarajan (Lower Murray Water).

[All](#)

[Announcements](#)

[Events](#)

[Discussions](#)

[Documents](#)

[Polls](#)

GROUP OWNER



Kristy Drzewucki
Asset Program Advisor
[kristy.drzewucki@wsaa...](mailto:kristy.drzewucki@wsaa.com.au)

PROJECT CHAIR




Michael Wassell
[michael.wassell@sydne...](mailto:michael.wassell@sydneywater.nsw.gov.au)

MEMBERS





Last Day to Register - UE Sub 16 SCADA Guidelines Stage 2 Project Delivery Workshop

COMMUNITY



WATER SERVICES
ASSOCIATION OF AUSTRALIA

Events | **Community** | Groups | WSA Shop | Luke Hellowell  | Log out

Home About us WSA Shop News Publications Search 


Home > Community

MY COMMUNITY ACTIVITY

Who else from my organisation is involved with WSAA?

30 Oct 2017

Each WSAA member has an organisations page that shows which staff are part of WSAA groups. Once you are logged into the WSAA community site simply visit your account, click on '[my community profile](#)', and click on your organisation.



Electricity procurement and wholesale spot market exposure

Discussion posted in [Climate Change, Energy and Environment Network](#) a month ago by [Kris Robinson](#)

MY GROUPS

Community of practice ▲

Network ▲

Project ▼

Energy-efficiency, management, mitigation, generation - Information sharing

PP3-028 Project Handover - Complete

PP3-030 Mechanical, Electrical Benchmarking - Complete