



Trusted Information
Sharing Network
for Critical Infrastructure Protection

.....

Generic SCADA Risk Management Framework

for the

IT Security Expert Advisory Group (ITSEAG)

DECEMBER 2006

Disclaimer: To the extent permitted by law, this document is provided without any liability or warranty. Accordingly it is to be used only for the purposes specified and the reliability of any assessment or evaluation arising from it are matters for the independent judgement of users. This document is intended as a general guide only and users should seek professional advice as to their specific risks and needs.

Change History

Version	Changes
1.0a	Initial version for internal review
1.0b	Incorporated internal review feedback
1.1	Final changes for ITSEAG presentation
1.2	Incorporated monitoring cycle into section 3.7.
2.0	Added preface and addressed final review comments.

Table Of Contents

PREFACE	4
1 INTRODUCTION	5
1.1 BACKGROUND	5
1.2 SCOPE	5
1.3 KEY TERMS AND DEFINITIONS	5
1.4 REFERENCES	6
1.5 ACKNOWLEDGEMENTS	7
2 TAILORING THE RISK MANAGEMENT FRAMEWORK	8
3 RISK MANAGEMENT METHODOLOGY	9
3.1 OVERVIEW	9
3.2 FRAMEWORK	9
3.3 ESTABLISHMENT OF THE CONTEXT	10
3.4 CONDUCT OF THE TRA	11
3.5 TREATING RISK	13
3.6 COMMUNICATION AND CONSULTATION ENVIRONMENT	14
3.7 FRAMEWORK MONITORING AND REVIEW	14
4 GENERIC SCADA ASSETS	17
4.1 GENERIC SCADA PROCESS MODEL	17
4.2 GENERIC SCADA ENABLERS	17
5 WORKED EXAMPLE OF THE TRA FRAMEWORK	18
6 THREAT AND RISK ASSESSMENT (TRA)	19
7 RISK TREATMENT PLAN (RTP)	26
8 PRESENTATION OF RESULTS TO SENIOR MANAGEMENT	43
8.1 OVERVIEW	43
8.2 SAMPLE RADAR CHART	43
9 ONGOING MONITORING AND REVIEW	45
9.1 OVERVIEW	45
9.2 SSMS REVIEWS	45
9.3 COMMUNICATING RISK EXPOSURES	45
9.4 RISK ASSESSMENT UPDATES	46

Preface

SCADA systems have traditionally been viewed as being isolated and therefore 'safe' and impenetrable from remote attack. Risk assessment and management methodologies, correspondingly, have largely been directed at legacy SCADA systems in which underlying protocols were designed without modern security requirements in mind.

In more recent times, SCADA systems have become interconnected with corporate business networks, and directly or indirectly with the Internet. This, together with the rapid advance of technology, the shifting threat landscape and the changing business environment, is increasing the exposure of SCADA systems to network vulnerabilities and Internet security threats.

Such changes and attitudes have meant that a new approach to risk management is required – one that takes into account IT security as well as physical security needs, the interconnection of SCADA systems with corporate business networks and the Internet and which fosters a culture of security at all levels of SCADA system management, operations and procedures.

The SCADA Community of Interest, a working group of the Information Technology Security Expert Advisory Group*, has identified risk management as a key issue in maintaining continuity of business and in protecting Australia's critical infrastructure.

The SCADA Risk Management Framework (RMF) is a generic high-level document that provides a cross-sector approach to identifying and assessing risks for owners and operators of SCADA systems. The Risk Management Framework can be tailored to suit a particular sector or organisation and also contains advice on how information security risks can be simplified and presented to senior management.

**The ITSEAG is part of the Trusted Information Sharing Network for critical infrastructure protection (TISN) which enables the owners and operators of critical infrastructure to share information on important issues. The TISN is made up of a number of sector-specific Infrastructure Assurance Advisory Groups and Expert Advisory Groups which are overseen by the Critical Infrastructure Advisory Council. One of the expert advisory groups is the ITSEAG which provides advice to the TISN on IT security issues relating to critical infrastructure protection. The ITSEAG consists of academic specialists, vendors and industry association and government representatives who are leaders in the information technology/e-security field. More information on the TISN can be found at <http://www.tisn.gov.au>*

For more information on the ITSEAG's work on SCADA security, please contact the Secretariat in the Department of Communications, Information Technology and the Arts on (02) 6271 1595 or SCADA@dcita.gov.au

1 Introduction

1.1 Background

- 1.1.1 The Australian Government Critical Infrastructure Advisory Council (CIAC) oversees a number of expert and advisory bodies and advises the Attorney General’s Department on matters associated with the national approach to Critical Infrastructure Protection (CIP).
- 1.1.2 These bodies, referred to as Infrastructure Assurance Advisory Groups (IAAGs), cover key industry sectors across Australia. The IT Security Expert Advisory Group (ITSEAG) has also been formed to advise all IAAGs on IT Security matters affecting all industry sectors.
- 1.1.3 This report has been commissioned via the ITSEAG’s SCADA working group that contributes to the operation of the CIAC by assisting with the assessment and implementation of security for SCADA systems across industry sectors.

1.2 Scope

- 1.2.1 The scope of this report is to detail an industry-wide framework whereby owners and operators of key SCADA systems can assess security risk exposures faced by these systems and implement security controls to manage these risk exposures within acceptable limits.
- 1.2.2 SCADA systems considered within the scope of the report comprise large-scale distributed control systems designed to deliver essential and stabilising services within the Australian economy.

1.3 Key Terms and Definitions

Term	Description
ACSI 33	The Australian Government Information and Communications Technology Security Manual published by DSD containing minimum information security standards for Commonwealth Government organisations and often used as a reference by other Australian organisations. ACSI 33 is available from DSD at: http://www.dsd.gov.au/library/infosec/acsi33.html
All hazards approach	A risk assessment approach intended to identify generic risks common to most, if not all, SCADA systems
AV	AntiVirus
BCP	Business Continuity Plan
COTS	Commercial Off The Shelf – a term used to describe software that can be purchased and integrated with little or no customisation

Term	Description
DR	Disaster Recovery – a component of business continuity management
DRP	Disaster Recovery Plan
ITSEAG	Information Technology Security Expert Advisory Group
NII	National Information Infrastructure
OS	Operating System
PSM	Protective Security Manual – published by the Australian Attorney General's Department, with information security requirements being carried through to ACSI 33
QoS	Quality of Service
Raw risk exposure	The level of risk associated with an asset before the application of any risk mitigation measures
RTP	Risk Treatment Plan
SCADA	Supervisory Control and Data Acquisition
SSMS	SCADA Security Management System
TRA	Threat and Risk Assessment
Treated risk exposure	The level of risk associated with an asset after the application of risk mitigation measures
VoIP	Voice over Internet Protocol

1.4 References

- International Critical Information Infrastructure Protection (CIIP) Handbook 2006
- ACSI 33 – Australian Government Information and Communications Technology Security Manual, Defence Signals Directorate, March 2006
- IEC 60870.1 Telecontrol Equipment and Systems – General Considerations
- IEC 60870.5 – 101 to 104 Telecontrol Equipment and Systems – Transmission Protocols
- AS/NZS 4360:2004 Risk Management, Standards Australia
- AS/NZS 7799.2:2003 Information Security Management, Standards Australia
- ISO/IEC 27001:2005 Information Security Management – Specification With Guidance for Use, International Standards Organisation (ISO), First edition, 15 Oct 2005
- Protective Security Manual 2005, Attorney General's Department, October 2005

- System Protection Profile – Industrial Control Systems, National Institute of Standards and Technology (NIST), Version 1.0.

1.5 Acknowledgements

SecureLink would like to acknowledge the assistance provided by the following sector and government-based personnel during the development of the Generic SCADA Risk Management Framework:

- **DCITA** : Allan Le Busque, Catherine Overy and Peter Beaver
- **ITSEAG** : Kim Duffy, David Campbell and Steven Stroud
- **Water** : Michael Wassell, Peter Murphy, Ian Appleby, Ron Southworth and Michael Byrn
- **Energy** : David Walcott, Cameron McKay, Darryl Argus, Bob Allison, Bill Harris, Patrick McConnell, Craig Brookes, Lyndon Branscomb, Paul James and Martin Stacey
- **Broadcasting** : Mike Squirrell, Martin Duane and Neville Bradley
- **Transport** : Ian McColl
- **Other** : Karl Williams and Bill Tarlinton.

2 Tailoring the Risk Management Framework

When tailoring this SCADA risk management framework to suit a particular sector or organisation, the following points should be noted:

- The framework has been developed to cover the basic functions of a distributed SCADA system. Organisation and sector-specific risks will need to be evaluated, and if necessary, incorporated into SCADA risk management frameworks at the sector or organisational level.
- The definition of threat likelihood, consequence of risk realisation and the matrix in which risk is calculated at a National Information Infrastructure level is given in Section 3.4. These values may not align with organisational risk calculation parameters and therefore may require updating before being used for sector or organisational risk management.
- When establishing the context of any sector or organisational risk management activities, Figure 3-2 should be assessed and possibly refined as appropriate to the applicable sector or organisation – this will also lead to a re-evaluation and update of SCADA process enablers as shown in Figures 3-2, 4-1 and Table 4-1.

The second column of the TRA as tabulated in Section 6 is headed ‘Owner’ – at a sector or organisational level, this column must identify the business or operational owner, as appropriate, with corporate responsibility for the associated process enabler.

In accordance with previously noted definitions in Section 3.4, the ‘Raw Risk’ columns in the Section 6 TRA will need to be updated should these values be altered.

Treatment options in Section 7 (RTP) are in some cases opportunistic. A significant goal of this RMP is to highlight the ‘desirable’ requirements of a secure SCADA system, and it is recommended that each of the RTP security controls be used when determining the most appropriate information security configuration for a secure SCADA system.

Finally, the determination of information security risk exposures, and the level to which they are reported to senior management, often results in the confusion of security issues with technical and operational details. Section 7 of this framework suggests a mechanism by which such information can be summarised and presented.

3 Risk Management Methodology

3.1 Overview

- 3.1.1 The methodology adopted for the generic SCADA risk management process is detailed in the following subsections.
- 3.1.2 The methodology is compliant with recognised standards including *AS/NZS 4360:2004 Risk Management* and *ISO/IEC 27001:2005 Information Security Management – Specification With Guidance for Use* (supersedes *AS/NZS 7799.2:2003 Information Security Management*).
- 3.1.3 Of note is that the risk management methodology encompasses an all hazards approach to risk management in the SCADA sector to identify and analyse the risk exposures presented through a wide variety of potential security vulnerabilities.

3.2 Framework

- 3.2.1 The SCADA risk management framework is based on the traditional standards-based risk management framework as described in AS/NZS 4360 and shown in Figure 3-1:

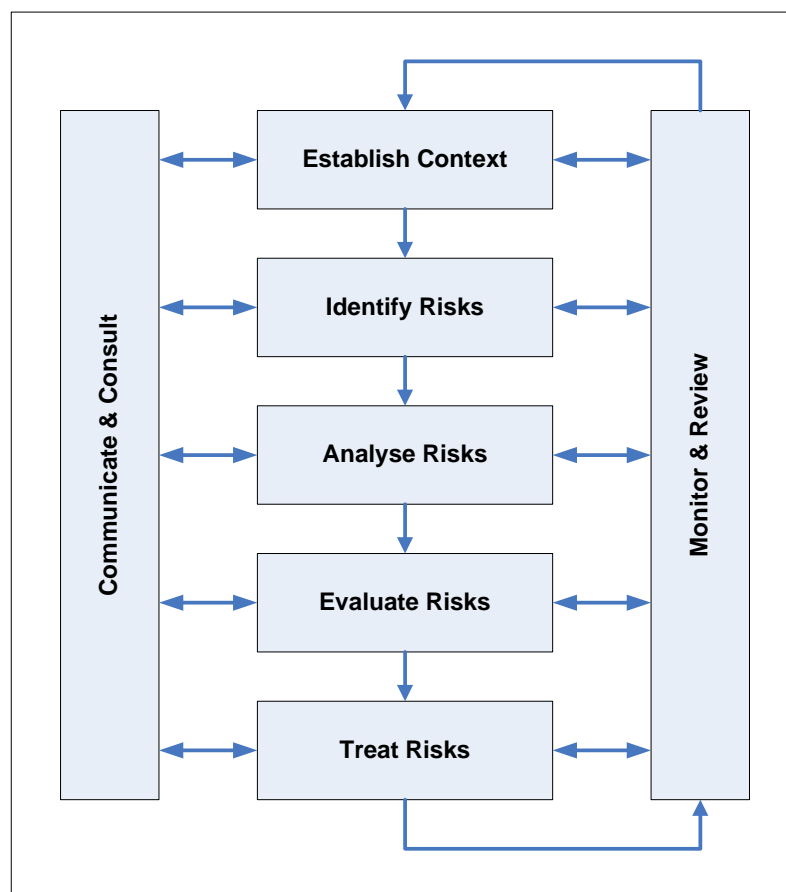


Figure 3-1 : Risk Management Framework (AS/NZS 4360:2004)

- 3.2.2 Establishment of the context for the SCADA Risk Management Framework involves defining the framework scope and identifying the assets that are potentially at risk.
- 3.2.3 Identification, analysis and evaluation of risks together comprise the Threat & Risk Assessment (TRA) component of the framework.
- 3.2.4 The risk treatment component comprises the development of a Risk Treatment Plan to address the identified levels of risk exposure to the assets within scope of the framework.
- 3.2.5 Communication and consultation comprises the identification and involvement of stakeholders associated with the secure implementation and operation of the SCADA system under consideration.
- 3.2.6 The monitor and review component of the process comprises the controls put in place specifically to ensure that the SCADA Risk Management Framework operates effectively over time.
- 3.2.7 Each of these components is described in more detail in the subsections to follow.

3.3 Establishment of the Context

- 3.3.1 The scope of the generic SCADA Risk Management Framework encompasses the core components of a distributed SCADA network that would be expected to be found in the majority of Critical Infrastructure utility service provider organisations.
- 3.3.2 This comprises the process components as shown in Figure 3-2.

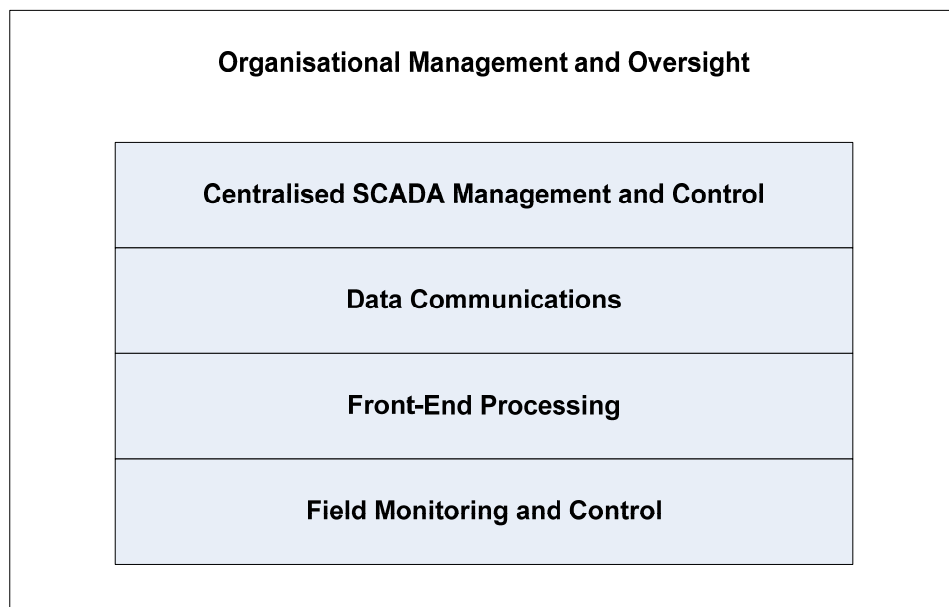


Figure 3-2 : Generic SCADA Processes

- 3.3.3 The assets that are likely to be threatened can therefore be derived by considering the ‘enablers’ that allow the identified processes in Figure 3-2 to occur.
- 3.3.4 These enablers can be derived by identifying the people, the places, and the products required to ensure the processes can be carried out.
- 3.3.5 Each enabler is owned. The owner is the responsible authority within operational sections of the organisation for ensuring that mitigating controls are appropriately implemented. The typical authority who is responsible for the enablers is contained in the “Owner” column, however each organisation using this guide ultimately determines who the responsible authority is. Table 3-1 below describes typical owners.

Owner	Description
CEO	Chief Executive Officer – Head of organisation
CIO	Chief Information Officer – IT infrastructure and architecture
HR	Human Resource Executive – personnel and contracting
SA	Security Advisor – covering physical and environmental enablers
ITSA	Information Technology Security Advisor – covering information security and logical access controls
CFO	Chief Financial Officer – covering asset purchasing/disposal and financial delegation

Table 3-1 : Owners of Enablers

- 3.3.6 Section 4 of this framework identifies generic enablers through the analysis of the generic SCADA processes.

3.4 Conduct of the TRA

- 3.4.1 Having identified the assets required to enable generic SCADA processing to occur, the next activity is to identify the vulnerabilities to which each asset is exposed.
- 3.4.2 Vulnerabilities to assets can be identified through consideration of the potential threats, whether they be malicious, accidental, natural or environmental, to:
 - Confidentiality of systems and information;
 - Integrity of systems and information stores; and/or
 - Availability of systems and the information that they contain.

3.4.3 Having identified vulnerabilities to assets, they should be analysed to determine the associated **raw** risk exposure in terms of:

- **Likelihood** of occurrence; and
- **Consequence** of realisation.

3.4.4 Each of these parameters is to be determined in accordance with appropriate scales suited to the organisation’s internal risk management framework. The scales used in this generic framework are shown in Tables 3-2 and 3-3, and correspond to those used by the Australian Government NII agencies:

Likelihood	Description
Almost Certain	The event is EXPECTED to occur in most circumstances
Likely	The event will PROBABLY occur in most circumstances and is expected at some time
Possible	The event MIGHT occur at some time but is not expected
Unlikely	The event COULD occur at some time
Rare	The event MAY occur in exceptional circumstances

Table 3-2 : Likelihood of Occurrence Descriptors

Consequence	Description
Insignificant	Would have insignificant impact on operations and could easily be handled through normal operational processes within the organisation.
Minor	Would be likely to require line management involvement to resolve, but would be expected to be handled within normal operational budgets and existing procedures.
Moderate	Would be likely to be escalated through line management to senior management, but would be unlikely to have a noticeable effect on the organisation’s operations.
Major	Would require escalation to senior management and could have an impact on the organisation’s business activities, operating budgets and industry reputation.
Catastrophic	Would endanger the organisation’s ability to carry out its business and could also be expected to have a social or economic impact within the Australian population base.

Table 3-3 : Consequence of Realisation Descriptors

3.4.5 Raw risk exposure can then be determined using the matrix provided at Table 3-4 and the selected likelihood and consequence values.

Likelihood	Consequence				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	H	H	H
Unlikely	L	L	M	M	H
Rare	L	L	M	M	H

Table 3-4 : Risk Calculation Matrix

3.4.6 Risk exposure levels indicated in Table 3-4 are as follows:

- **L** : Low Risk – unlikely to have an impact that could not be satisfactorily dealt with via normal operational procedures
- **M** : Medium Risk – likely to result in short term, localised, disruption to services and require escalation through line management. Could generate localised adverse media comment and moderate penalties or costs unable to be borne via normal operational budgets
- **H** : High Risk – would be expected to have a significant impact on corporate budgets and organisational reputation. Could lead to extended service disruption and seriously inconvenience or have health impacts on a wide section of the customer base
- **E** : Extreme Risk – would be expected to seriously damage the organisation’s ability to continue to operate with the confidence of its customer base or corporate owners. Could result in serious social or economic damage and may affect the organisation’s ability to continue operations.

3.5 Treating Risk

3.5.1 Once risk has been determined all risks must be treated. Treatments include:

- Accept**: - do nothing to reduce the evaluated threat
- Avoid**: - cease doing the business activity that brings about the possibility of the threat occurring
- Transfer**: - pass the responsibility for implementing mitigating controls to another entity. Responsibility for threat and risk management remains the responsibility of the organisation
- Reduce**: - implement controls to reduce risk to an acceptable level.

- 3.5.2 The risk table provided in Section 6 contains a column for recording risk treatment. It also contains a cross-reference to the Risk Treatment Plan (RTP) which is shown in Section 7. This plan details the controls that may be used to reduce risk to an acceptable level. Organisations may interpret these controls for their own use – and provide additional controls if required. The cross-reference in the RTP points to where the identified threat has been addressed.
- 3.5.3 The RTP provides for a reassessment of risk once controls have been selected and implemented. The RTP can also act as a management plan to provide a “status” of implementation.
- 3.5.4 The example provided at the end of this section illustrates the process flow used in this risk framework.

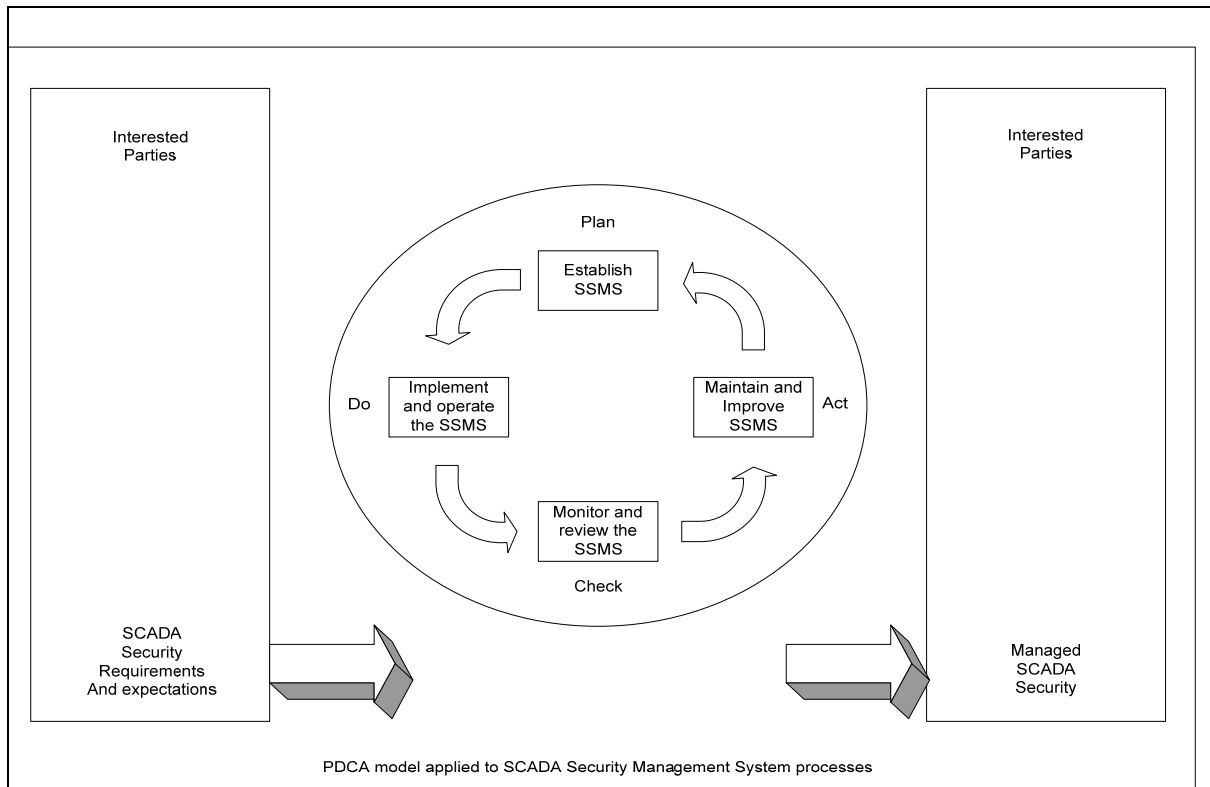
3.6 Communication and Consultation Environment

- 3.6.1 This environment comprises the identification and involvement of all stakeholders involved in the operation of the SCADA network and the management of corporate risk across the company.
- 3.6.2 In addition to the day-to-day operation of the SCADA system(s), it is important to ensure that risk information is communicated through the organisation’s management and is highlighted (generally in summarised form) to the executive forum charged with overall organisational risk management.
- 3.6.3 The manner in which this environment is implemented will be highly dependent on the operation of each affected organisation, and is therefore considered to be outside the scope of this report, however suggested management reporting techniques are included in this report.

3.7 Framework Monitoring and Review

- 3.7.1 The monitoring and review component needs to be implemented to ensure that:
- a) Risk exposures are monitored, re-evaluated and revised as appropriate over time;
 - b) Risk exposures are updated in a timely fashion in response to significant events such as changes to the organisation’s operations and influencing external events; and
 - c) The risk management framework itself is operating effectively.

3.7.2 As with the communications and consultation environment, the mechanism(s) used to implement this component of the risk management framework need to be implemented within current organisational management and monitoring processes. The following diagram and table provides a guide to successful implementation and ongoing effectiveness.



Plan (establish the SSMS)	Establish SCADA Security Management System policy, objectives, processes and procedures relevant to managing risk and improving security to deliver results in accordance with an organisation’s overall policies and objectives
Do (implement and operate the SSMS)	Implement and operate the SCADA Security Management System policy , controls, processes and procedures
Check (monitor and review the SSMS)	Assess and, where applicable, measure process performance against SCADA Security Management System policy, objectives and practical experience and report the results to management for review
Act (maintain and improve the SSMS)	Take corrective and preventative actions, based on the results of the internal SMS audit and management review or other relevant information to achieve continual improvement of the SCADA Security Management System.

Table 3-5 : SSMS Management and Monitoring Guide

4 Generic SCADA Assets

4.1 Generic SCADA Process Model

4.1.1 The following diagram illustrates the generic nature whereby the SCADA-related processes have been decomposed in order to implement a generic risk management framework.

4.1.2 This facilitates the identification of affected organisational SCADA assets through the identification of the enablers associated with these processes.

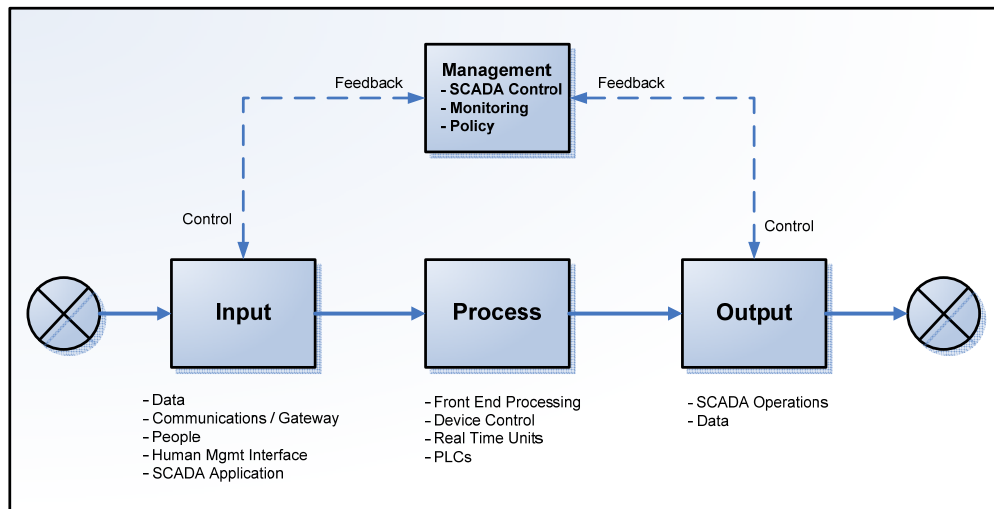


Figure 4-1 : Generic Process Model

4.2 Generic SCADA Enablers

4.2.1 As partially identified in the previous subsection, the following table identifies the enablers likely to be found in a generic SCADA system:

Type	Enabler Description
People	Users and operators of the SCADA system
Products	Buildings and Sites
	Communications and Networks
	SCADA Application Software
	SCADA Hardware and Operating System (OS)
	SCADA Field Devices
	Power Supply
Processes	Management Control and Feedback
	Information Management

Table 4-1 : Generic SCADA Process Enablers

5 Worked Example of the TRA Framework

Step 1 – we identify what process we are protecting – in this instance it is the SCADA system.

Step 2 – we identify the enablers that make this process occur – in this example we will select “Application Software”

Step 3 – we assess risk against the threat of the “Loss of Confidentiality”. The result is in the table below.

Enablers	Owner	Common potential points of failure and known vulnerabilities	Threat Type	Raw Risk			Treatment Option & reference
				Consequence	Likelihood	Risk Rating	
Application - Software	CIO	<ul style="list-style-type: none"> Lack of security hardening 	Loss of Confidentiality	Moderate	Likely	H	Reduce F1

Step 4 – as the risk rating is “High” from this threat we treat the risk by selecting the “Reduce” option – how we reduce this risk is detailed in the “Risk Treatment Plan” at “F1”. An extract from the RTP is provided below.

Enabler	Threat Type & Treatment reference	Control Objectives	Selection of controls to achieve objectives	Controlled Risk		
			Controls	Consequence	Likelihood	Risk Rating
Application – Software	Confidentiality F1	To ensure software can withstand unauthorised access attempts.	Secure SCADA software configuration	Moderate	Rare	M

Step 5 – once the control can be proven to be in place the risk level for that threat can then be re-evaluated. In this example risk has been reduced from “HIGH” to “MEDIUM” because we have reduced the likelihood from “Likely” to “Rare”.

6 Threat and Risk Assessment (TRA)

Enablers	Owner	Common potential points of failure and known vulnerabilities	Threat Type	Raw Risk			Treatment Option & reference
				Consequence	Likelihood	Risk Rating	
People	HR	<ul style="list-style-type: none"> Social Engineering – obtaining information on system layout and on those who manage it. Known to have occurred Information security breaches - past employees or service providers freely disclose information to unauthorised persons 	Loss of Confidentiality	Moderate	Likely	H	Reduce A1
		<ul style="list-style-type: none"> High Staff turnover – unable to fill positions Lack of skills / knowledge – this leads to accidental issues and deprives senior staff of their properly allocated role Industrial relations breakdown – leading to staff not being available for long periods of time or to perform critical functions. Legal activity may result. Health related event – absenteeism 	Loss of Availability	Moderate	Almost Certain	H	Reduce A2
		<ul style="list-style-type: none"> Disgruntled Staff including contractors – who subsequently lose their integrity in relation to job performance 3rd Party dependencies – where the integrity of the 3rd party is essentially unknown Issue-motivated interference – leading to biased or one dimensional thinking which affects job performance 	Loss of Integrity	Moderate	Likely	H	Reduce A3
Management Control &	CEO	<ul style="list-style-type: none"> Broadcast of sensitive information to unauthorised sources 	Loss of Confidentiality	Minor	Possible	M	Reduce B1

Enablers	Owner	Common potential points of failure and known vulnerabilities	Threat Type	Raw Risk			Treatment Option & reference
				Consequence	Likelihood	Risk Rating	
Feedback		<ul style="list-style-type: none"> Lack of succession planning Lack of executive support Ineffective and/or one-way communication Conflicting priorities 	Loss of Availability	Moderate	Possible	H	Reduce B2
		<ul style="list-style-type: none"> Lack of timely decision making Inappropriate management structure Poor decision making Failure in duty of care Policy lacking or non-conformance 	Loss of Integrity	Minor	Almost Certain	H	Reduce B3
Building / Site	SA	<ul style="list-style-type: none"> Degraded security environment through site isolation 	Loss of Confidentiality	Minor	Possible	M	Reduce C1
		<ul style="list-style-type: none"> Natural disaster DR process failure Accidental damage Sabotage OH&S non-compliance Poor design 	Loss of Availability	Moderate	Unlikely	M	Reduce C2
		<ul style="list-style-type: none"> Vandalism Poor maintenance Environmental disaster 	Loss of Integrity	Minor	Possible	M	Reduce C3

Enablers	Owner	Common potential points of failure and known vulnerabilities	Threat Type	Raw Risk			Treatment Option & reference
				Consequence	Likelihood	Risk Rating	
Information Management	ITSA	<ul style="list-style-type: none"> Inappropriate access control Inappropriate equipment disposal Lack of security controls in contracts 	Loss of Confidentiality	Moderate	Almost Certain	H	Reduce D1
		<ul style="list-style-type: none"> Untested procedures (Back-up etc.) Lack of capacity planning 	Loss of Availability	Moderate	Almost Certain	H	Reduce D2
		<ul style="list-style-type: none"> Poor version control Poor data quality Too much information Lack of documentation Incorrect documentation 	Loss of Integrity	Moderate	Almost Certain	H	Reduce D3
Communications & Networks	ITSA	<ul style="list-style-type: none"> Unauthorised disclosure via 3rd party carrier services Open communication protocols are used Mis-configuration leading to unauthorised disclosure Security holes in protocols and equipment Data path is over shared networks resulting in uncontrolled access to data Network scanning used to discover IP vulnerabilities 	Loss of Confidentiality	Minor	Likely	M	Reduce E1

Enablers	Owner	Common potential points of failure and known vulnerabilities	Threat Type	Raw Risk			Treatment Option & reference
				Consequence	Likelihood	Risk Rating	
		<ul style="list-style-type: none"> QoS issues No redundancy / false redundancy Interference from other transmissions Vendor pricing or service level changes 	Loss of Availability	Moderate	Almost Certain	H	Reduce E2
		<ul style="list-style-type: none"> Lack of diversity Data path interference Failure of voice communications (inc VoIP) 	Loss of Integrity	Moderate	Almost Certain	H	Reduce E3
SCADA Application - Software	CIO	<ul style="list-style-type: none"> Lack of security hardening 	Loss of Confidentiality	Moderate	Likely	H	Reduce F1
		<ul style="list-style-type: none"> Lack of visibility and access to sourcecode Lack of scalability in software solutions SCADA Application failure Licence costs – locked in to vendors Vested interests in particular products 	Loss of Availability	Major	Likely	H	Reduce F2

Enablers	Owner	Common potential points of failure and known vulnerabilities	Threat Type	Raw Risk			Treatment Option & reference
				Consequence	Likelihood	Risk Rating	
		<ul style="list-style-type: none"> Loss of provider Offshoring Takeovers and mergers Change / patch management and lack of flexibility to adapt to changing requirements Technology changes – leading to software being outdated System complexity Unaware of implications in implementing security controls 	Loss of Integrity	Major	Likely	H	Reduce F3
SCADA Hardware including operating system	CIO	<ul style="list-style-type: none"> Obsolete equipment or Operating System – unable to be patched Lack of hardening Inappropriate access controls 	Loss of Confidentiality	Moderate	Almost Certain	H	Reduce G1
		<ul style="list-style-type: none"> Vested interests in particular products Equipment failure Environmental failure such as air conditioning, UPS Damage as a result of lack of electrical isolation Malicious software Lack of capacity Lack of redundancy No spares management 	Loss of Availability	Moderate	Almost Certain	H	Reduce G2

Enablers	Owner	Common potential points of failure and known vulnerabilities	Threat Type	Raw Risk			Treatment Option & reference
				Consequence	Likelihood	Risk Rating	
		<ul style="list-style-type: none"> Improper patch management / change management Incompatibility with the application 	Loss of Integrity	Moderate	Likely	H	Reduce G3
SCADA field devices	CIO	<ul style="list-style-type: none"> As for SCADA HW, SW App Open access – security issues including access back to central systems Bypassing traditional security framework Default security configuration Lack of security hardening – also inability to security harden 	Loss of Confidentiality	Moderate	Likely	H	Reduce G1
		<ul style="list-style-type: none"> As for SCADA HW, SW App Failure to operate - dependence on communications links (Denial of Service) More vulnerable to physical damage Lacking in remote management capability 	Loss of Availability	Moderate	Almost Certain	H	Reduce G2
		<ul style="list-style-type: none"> As for SCADA HW, SW App dependency and use of COTS devices Introduction of open technology field devices (inc unstable operating Systems, less robust hardware) 	Loss of Integrity	Minor	Likely	M	Reduce G3
Power	SA	<ul style="list-style-type: none"> Breach of confidentiality when power fails 	Loss of Confidentiality	Minor	Possible	M	Reduce H1

Enablers	Owner	Common potential points of failure and known vulnerabilities	Threat Type	Raw Risk			Treatment Option & reference
				Consequence	Likelihood	Risk Rating	
		<ul style="list-style-type: none"> • Failure of supply • Lack of backup power • Lack of reliability • Non-diversity of supply • Lightning, Fire etc. • Lack of capacity planning for peak periods 	Loss of Availability	Major	Likely	H	Reduce H2
		<ul style="list-style-type: none"> • Quality • Lack of prioritization of services 	Loss of Integrity	Moderate	Likely	H	Reduce H3

7 Risk Treatment Plan (RTP)

Enabler	Threat Type & Treatment reference	Control Objectives	Selection of controls to achieve objectives	Controlled Risk		
			Controls	Consequence	Likelihood	Risk Rating
People	Confidentiality A1	To ensure that people maintain the confidentiality of sensitive SCADA information	Confidentiality Agreements in employment contracts <i>Include survivability clauses and obtain legal advice on drafting</i>			
			Confidentiality Provisions in 3 rd Party and outsourcing contracts <i>Mandate security briefing for new providers who are working in critical areas to highlight obligations</i>			
			SCADA security training at induction including security incident reporting <i>Incident reporting should define alert levels and timely reporting of critical incidents</i>			
	Availability A2	To ensure that appropriate resources are available to manage and operate SCADA systems	Fully documented operating procedures <i>Operating procedures should be in place to supplement training and reduce the risk of accidents. Training environments should be established to support learning objectives</i>			

Enabler	Threat Type & Treatment reference	Control Objectives	Selection of controls to achieve objectives	Controlled Risk		
			Controls	Consequence	Likelihood	Risk Rating
			Implement a combination of resource types – including contractors, 3 rd parties <i>Have a different type of resource to backup primary resourcing</i>			
			Implement cross-skilling for critical areas			
	Integrity A3	To ensure that SCADA resources are appropriately trained, motivated and are trustworthy	Personnel vetting <i>The Protective Security Manual (PSM) Part D provides guidance on vetting</i>			
			Concise job descriptions			
			On-going training and assessment in operating SCADA systems			
			Defined Entry and Exit procedures <i>Different levels of briefing/interviews depending on the job performed. Exit interviews are particularly important for staff & management in operational areas</i>			

Enabler	Threat Type & Treatment reference	Control Objectives	Selection of controls to achieve objectives	Controlled Risk		
			Controls	Consequence	Likelihood	Risk Rating
Management Control & Feedback	Confidentiality B1	To control SCADA Management information	Establish a data classification schema <i>The PSM Part C provides guidance on classification and how to classify documents</i>			
			Formal procedures for publication of SCADA management information <i>Information is often incorrectly published to web sites when it should be for internal use only – often as a result of confusing internal “unclassified” documents with information intended for the general public.</i>			
	Availability B2	To ensure that required management controls are defined	Approved and documented Roles and Responsibilities for Management			
			Approved management framework and Charter <i>Quality Management procedures provide guidance on how a management framework should function</i>			
		To provide dedicated and effective Management support for SCADA systems	Documented SCADA management policies and procedures <i>These document should be brief and not change significantly over time</i>			

Enabler	Threat Type & Treatment reference	Control Objectives	Selection of controls to achieve objectives	Controlled Risk		
			Controls	Consequence	Likelihood	Risk Rating
	Integrity B3	To provide correct and controlled access to SCADA information	Controlled repository for SCADA related information <i>An information/knowledge management system may assist with achieving a controlled and secure storage</i>			
		To provide competent and effective management support	Documented Management Outcomes <i>These should be endorsed with executive support</i>			
		To assess management effectiveness	Establish Key Performance Indicators for Management <i>These should be reportable, repeatable and achievable</i>			
Building / Site	Confidentiality C1	To prevent compromise of assets and interruption to business activities	Equipment siting standards for remote devices <i>Suitable racks/cabinets may be identified for remote servers/switches. Do not allow unprotected, live network access points</i>			
	Availability C2	To prevent loss of assets and interruption to SCADA operations	Defined security perimeters <i>Restrict access to sites – do not allow broad access simply for convenience</i>			
	Redundant power supply <i>Consider Uninterruptible Power Supply (UPS) or alternate power supply for key sites.</i>					

Enabler	Threat Type & Treatment reference	Control Objectives	Selection of controls to achieve objectives	Controlled Risk		
			Controls	Consequence	Likelihood	Risk Rating
			<p>Implementation of cabling standards</p> <p><i>All cabling should be bundled, labelled and use proper layout trays.</i></p>			
	Integrity C3	To minimise impact of Site loss and damage	<p>Disaster Recovery and Business Continuity Plans</p> <p><i>These site specific strategies should be aligned with the whole of organisation DR strategy</i></p>			
Information Management	Confidentiality D1	To control access to SCADA information	<p>Documented SCADA access control policy</p> <p><i>A high level access policy should be part of Information management controls communicated to management and users</i></p>			
			<p>Formal user registration procedures in place</p> <p><i>Registration should exist for all user types: staff, contractors, and contracted service providers</i></p>			
			<p>Regular audit review of access rights</p> <p><i>Ensure that all remote and "temporary" accounts are also reviewed</i></p>			
			<p>Encrypt sensitive information stored on Networks</p> <p><i>Encryption of certain classifications should be part of an organisational information classification schema. The PSM</i></p>			

Enabler	Threat Type & Treatment reference	Control Objectives	Selection of controls to achieve objectives	Controlled Risk		
			Controls	Consequence	Likelihood	Risk Rating
			<p><i>Part C provides details on how information may be classified. The Australian Government Information and Communications Technology Security Manual (ACSI 33) also provides details on encryption standards – see www.dsd.gov.au</i></p>			
	Availability D2	To maintain the availability of information processing	<p>Documented and tested backup procedures</p> <p><i>Often only certain types of systems are backed up. Organisations should ensure that ALL critical information is backed up and that effectiveness is tested on a regular basis</i></p> <p>Capacity monitoring and forecasting</p> <p><i>Network monitoring and service delivery reports from vendors may effectively provide these controls</i></p>			
	Integrity D3	To ensure the correct operation of information processing facilities	<p>Documented SCADA operating procedures</p> <p><i>To have full effect; operating procedures should be consistent, available, clear and changes must be efficiently applied according to proper versioning control.</i></p> <p>Incident management and response procedures</p> <p><i>Should be documented and tested regularly - Available tools include Network and Host Intrusion Detection Systems, System Integrity Verification, Log Analysis and Intrusion Repulsion – see ACSI 33 “Managing Security Incidents” for</i></p>			

Enabler	Threat Type & Treatment reference	Control Objectives	Selection of controls to achieve objectives	Controlled Risk		
			Controls	Consequence	Likelihood	Risk Rating
			<i>guidance</i>			
			Appropriate segregation of duties for information processing tasks			
Communications & Networks	Confidentiality E1	To protect the transmission of SCADA information broadcast over Public Networks	Encrypt transmission of SCADA information <i>Ensure that appropriate encryption protocols are applied – ACSI 33 Chapter 9 provides detailed advice on suitable cryptography techniques</i>			
			Perform vulnerability assessments on a periodic basis on all access points into the SCADA network <i>Regular scenarios should be defined and tested to identify network vulnerabilities</i>			
	Availability E2	To maintain SCADA network connectivity	For key services, route communications lines via multiple exchanges / mediums			
			Deploy intelligent networking devices to handle peak loads <i>Routing devices and modern switching equipment can be tailored to meet specific load patterns and provide alerts for unusual activity</i>			
	Integrity E3	To verify SCADA network configurations	Deploy network monitoring services to identify and localise network trouble spots			

Enabler	Threat Type & Treatment reference	Control Objectives	Selection of controls to achieve objectives	Controlled Risk		
			Controls	Consequence	Likelihood	Risk Rating
SCADA Application – Software	Confidentiality F1	To ensure that such software utilises recognised best practice security mechanisms and is able to withstand unauthorised access attempts.	Secure SCADA software configuration <i>Where possible, computerised systems should be hardened to minimise the opportunity for unauthorised access. Hardening should also ensure that any vendor application software support is maintained throughout the life of the product whilst the underlying system is hardened.</i> <i>Access control mechanisms should also exist to ensure that centralised system access controls are protected in accordance with corporate password and account usage policies.</i>			
			Minimisation of user access rights <i>Users should only be granted the minimum access required in order to perform their duties. Such access, and the functionality assigned to SCADA system roles, should also be regularly reviewed and updated.</i>			

Enabler	Threat Type & Treatment reference	Control Objectives	Selection of controls to achieve objectives	Controlled Risk		
			Controls	Consequence	Likelihood	Risk Rating
			<p>Logging of access attempts and user actions</p> <p><i>All access attempts, whether they be successful or not, should be logged to a protected audit trail.</i></p> <p><i>In addition, significant activities (such as the changing of state of SCADA devices and updates to access lists) should also be logged.</i></p> <p><i>The audit trail should be periodically reviewed for suspicious activity.</i></p> <p><i>It is desirable that suspicious activity be alerted to operational personnel in near real-time.</i></p>			
	Availability F2	To ensure that the software is scalable and reliable in operation.	<p>Capacity planning</p> <p><i>SCADA systems should be designed to provide scalability for future growth and information storage requirements. Collection and retention of audit trails should also be addressed.</i></p> <p>Capacity monitoring</p> <p><i>SCADA functionality should include a function to allow for potential bottlenecks such as CPU, memory, disk and communications usage to be monitored and analysed.</i></p>			

Enabler	Threat Type & Treatment reference	Control Objectives	Selection of controls to achieve objectives	Controlled Risk		
			Controls	Consequence	Likelihood	Risk Rating
			<p>Acceptance testing</p> <p><i>Acceptance testing procedures and criteria should be developed for all changes to SCADA software. These procedures should encompass software updates, bug fixes and security patches.</i></p> <p><i>In cases where emergency security patching is required, Business Continuity Plans should allow for the implementation of such patches and the recovery from failed operational implementations.</i></p>			
			<p>Use of open architectures and protocols</p> <p><i>Where possible, open architectures and protocols should be adopted to prevent vendor-specific architectures and protocols from potentially 'hiding' security issues and constraining system scalability and interoperability.</i></p>			

Enabler	Threat Type & Treatment reference	Control Objectives	Selection of controls to achieve objectives	Controlled Risk		
			Controls	Consequence	Likelihood	Risk Rating
	Integrity F3	To maintain the correct operation of the software over time.	<p>Vendor support arrangements</p> <p><i>Contractual arrangements should be in place with the software vendor to ensure that:</i></p> <ul style="list-style-type: none"> • <i>Software patches are made available in a timely manner</i> • <i>Support arrangements such as subcontracting and off-shoring do not occur without the agreement of all contracted parties</i> • <i>The customer is to be notified of any takeover or merger activities that may affect the level or manner in which the vendor support arrangements are provided</i> <p>Critical software escrow arrangements</p> <p><i>Where a SCADA system comprises a vendor-specific software package, an escrow agreement should be entered into with the vendor to ensure product availability should the vendor organisation fail to be able to support the product into the future.</i></p>			
SCDA Hardware including operating System	Confidentiality G1	To ensure that the SCADA computing platform is resilient against unauthorised access attempts.	<p>Security hardening of the computing platform</p> <p><i>Computer platforms should be hardened to remove unnecessary services, accounts and software packages.</i></p> <p><i>Vendor support agreements should allow for basic hardening of supported computer platforms.</i></p>			

Enabler	Threat Type & Treatment reference	Control Objectives	Selection of controls to achieve objectives	Controlled Risk		
			Controls	Consequence	Likelihood	Risk Rating
			<p>Operating System access controls</p> <p><i>OS access controls should be implemented to ensure that sensitive information is protected from unnecessary and unauthorised disclosure</i></p> <p><i>Unnecessary user accounts should also be removed and default account passwords changed.</i></p>			
			<p>Vendor support arrangements</p> <p><i>Vendor support arrangements should ensure that system hardening measures do not void support arrangements and that measures such as timely security patching of systems are supported.</i></p>			
	Availability G2	To ensure that the SCADA computing platform is reliable in the event of component failure, environmental disturbance, or attempted malicious disruption.	<p>System redundancy</p> <p><i>Critical system components should be designed to withstand single points of failure.</i></p> <p><i>Business Continuity Plans (and/or if necessary, Disaster Recovery Plans) should be updated and tested to ensure that systems are able to withstand loss of single physical, personnel and procedural dependencies.</i></p>			

Enabler	Threat Type & Treatment reference	Control Objectives	Selection of controls to achieve objectives	Controlled Risk		
			Controls	Consequence	Likelihood	Risk Rating
			<p>Spares holdings</p> <p><i>Adequate spares should be held (or covered by vendor support arrangements) for timely recovery from component failures.</i></p>			
			<p>Protection against malware</p> <p><i>Antivirus measures should be implemented on SCADA networks as they would with other corporate IT environments.</i></p> <p><i>Malware protection should be applied and updated in a timely manner on SCADA server, FEP, field device and workstation platforms.</i></p> <p><i>NOTE: it is becoming increasingly common to find field devices operating via well-known operating systems (such as Windows XP). Any virus attack on the system can therefore also have major repercussions on field devices and they should therefore be brought into the corporate AV regime.</i></p>			
			<p>Capacity planning and monitoring</p> <p><i>Measures should be in place to monitor and manage SCADA system capacity and address potential bottlenecks in advance of them impacting on system operations.</i></p>			

Enabler	Threat Type & Treatment reference	Control Objectives	Selection of controls to achieve objectives	Controlled Risk		
			Controls	Consequence	Likelihood	Risk Rating
			<p>Business Continuity Plans</p> <p><i>BCPs and associated DRPs should be in place and tested to ensure that the SCADA system can cope with the loss of components (and potentially sites) and that the system can be restored to normal operations as faults are rectified.</i></p>			
	Integrity G3	To ensure that the configuration of the SCADA computing platform is in a known and approved state.	<p>Formal configuration management and control procedures</p> <p><i>There should be measures in place to ensure that the SCADA system is in a known and approved state, and that changes are appropriately analysed, tested and authorised.</i></p>			
			<p>Vendor support arrangements</p> <p><i>Contractual support arrangements should be in place with the SCADA software vendor to ensure that timely installation of security patches to supported hardware and OS is possible.</i></p>			
SCADA field devices	Confidentiality G1	To prevent unauthorised monitoring and control of these devices.	<p>Encrypted data communications</p> <p><i>Where communications with field devices occurs over a communications line susceptible to external interception and / or compromise, information should be encrypted to minimise the opportunity for external parties to compromise the communications channel.</i></p>			

Enabler	Threat Type & Treatment reference	Control Objectives	Selection of controls to achieve objectives	Controlled Risk		
			Controls	Consequence	Likelihood	Risk Rating
			<p>Private communications channels</p> <p><i>Where possible, sensitive communications with field devices should be performed over dedicated leased-line services rather than using a public communications infrastructure.</i></p>			
	Availability G2	To ensure that these devices can be monitored and controlled as required.	<p>Device maintenance</p> <p><i>A maintenance regime should be in place to ensure that all peripheral devices are regularly tested</i></p>			
			<p>Alternate communications channels</p> <p><i>Critical field establishments and devices should be connected to the SCADA system via redundant communications channels.</i></p> <p><i>The central control station should also be configured such that it has control over the communications channel(s) available to the field device.</i></p>			
Integrity G3	To ensure that these devices are in a stable and known state.	<p>Periodic device polling</p> <p><i>Field devices should be periodically polled to ensure that their status is verified to the central control system and, if necessary, that discrepancies are investigated and verified.</i></p>				

Enabler	Threat Type & Treatment reference	Control Objectives	Selection of controls to achieve objectives	Controlled Risk		
			Controls	Consequence	Likelihood	Risk Rating
Power	Confidentiality H1	To ensure that power failures do not lead to a security compromise of the SCADA system.	<p>Backup power source</p> <p><i>Critical system components should be fed through both mains and backup power supplies.</i></p>			
	Availability H2	To prevent disruption to SCADA operations during power failure conditions.	<p>Backup power source</p> <p><i>Critical system components should be fed through both mains and backup power supplies.</i></p>			
			<p>Redundant control centres</p> <p><i>There should be redundancy built into centralised control sites to mitigate against damage to, or loss of availability of, critical establishments.</i></p>			
<p>Contingency planning</p> <p><i>Contingency plans should ensure that centralised services can be transitioned to alternative arrangements during such interruptions and be able to be transitioned back into service once central sites are restored to normal operations.</i></p>						

Enabler	Threat Type & Treatment reference	Control Objectives	Selection of controls to achieve objectives	Controlled Risk		
			Controls	Consequence	Likelihood	Risk Rating
			<p>Disaster recovery testing</p> <p><i>Contingency plans should be tested periodically. Where a physical failover test is not able to be performed, formal scenario testing should be undertaken, with results and lessons learned documented, analysed and actioned as appropriate.</i></p>			
	Integrity H3	To ensure that SCADA systems operate as expected during power supply disruptions.	<p>Backup power source</p> <p><i>A medium-to-long term power supply alternative (such as a long term diesel power unit) should be available to power critical SCADA system components during power interruptions.</i></p> <p><i>Should core SCADA components be installed in dedicated control environments, power supply should also be capable of powering support environments such as air conditioning and fire detection.</i></p>			
			<p>Power conditioning</p> <p><i>System-critical devices should be connected to a conditioned and uninterruptible power supply.</i></p>			

8 Presentation of Results to Senior Management

8.1 Overview

- 8.1.1 Whilst the detailed analysis and documentation contained within an organisation's full SCADA risk management plan is likely to form a significant report, it is suggested that measures be undertaken to summarise the plan for presentation to senior management.
- 8.1.2 Whilst detailed documentation is available to senior management personnel, a summarised report is more often an effective format to communicate the results to such an audience.
- 8.1.3 A number of organisations already use a 'traffic light' approach to present such data to senior management, where each risk is assigned a green, amber or red status depending on the current health of risk management measures.
- 8.1.4 The following subsection presents the use of a 'radar chart' to display risk management status to an organisation's senior management. It can be a highly effective mechanism in cases where identified SCADA process enablers are not overly complex and it has a number of advantages as follows:
- The entire risk management story is presented via a single graphic diagram
 - It is easy to explain and intuitive to understand
 - It can be used to show risk management progress over time by including historical data to demonstrate the organisation's risk profile over time.
- 8.1.5 The radar chart is a standard Microsoft charting option. Applications such as PowerPoint or Visio can be used to create the background colour scheme onto which the chart can be overlaid for presentation purposes.

8.2 Sample Radar Chart

- 8.2.1 Figure 8-1 provides a sample radar chart based on the enablers identified in this report and arbitrary treated risk exposure data.
- 8.2.2 It shows on the one diagram:
- The health of risk management against each of the identified enablers; and
 - The current (May 06) risk management profile in comparison to the profile 12 months previous (May 05).

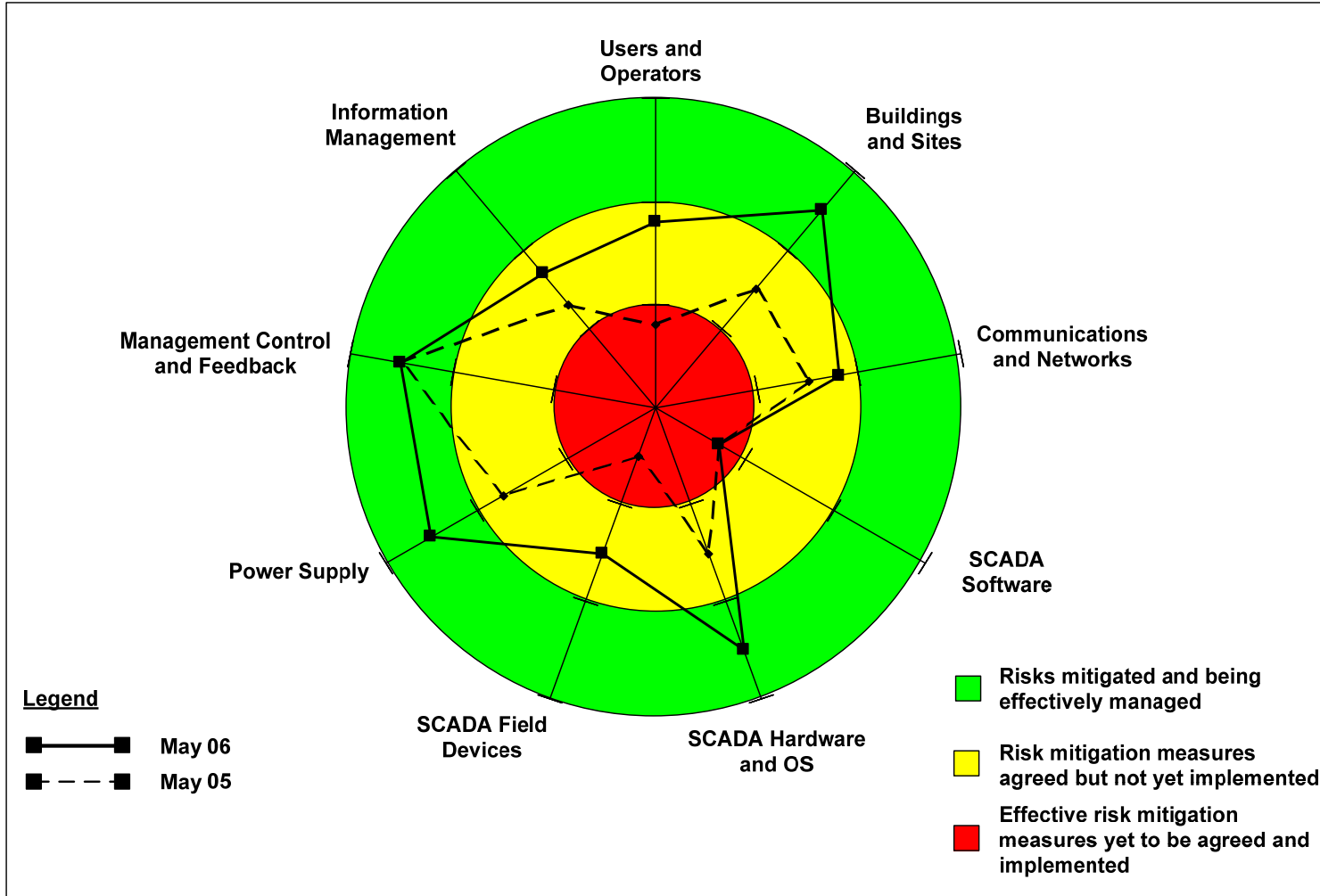


Figure 8-1 : Sample Radar Chart Presentation of Risk Management

9 Ongoing Monitoring and Review

9.1 Overview

9.1.1 The effectiveness of a risk management approach is dependent not only on the methodology applied to the development of risk assessment data, but also on its continued update as influencing factors change over time.

9.1.2 Examples of such factors can include:

- Changes to business processes and / or technologies within the organisation
- Alteration to the external threat environment (e.g. the organisation may decide to undertake a project that brings it into conflict with an issue-motivated group).

9.1.3 In addition, the risk management framework itself needs to be monitored, measured and refined (refer figure 3-5) to ensure that it continues to provide relevant information to the organisation.

9.1.4 The subsections to follow indicate measures that are likely to contribute to the ongoing effectiveness of the SCADA Risk Management Framework.

9.2 SSMS Reviews

9.2.1 The overall SCADA Security Management System should be reviewed over time to ensure that it functions effectively. Measures that can be undertaken to assist in this activity include, but are not necessarily limited to, the following:

- Internal process reviews
- External (independent) process reviews and audits
- Implementation of Key Performance Indicators (KPIs) designed to monitor SSMS processes.

9.2.2 Where possible, it is recommended that KPIs be chosen, and limited in number, to an easily measurable set to minimise the impact of process monitoring on normal day-to-day activities.

9.3 Communicating Risk Exposures

9.3.1 Having measured corporate risk exposures associated with the operation of the SCADA system(s), Section 8 of this document provides a suggested management reporting tool.

- 9.3.2 Where the organisation implements risk management at an organisation-wide level (e.g. a risk and audit committee reporting directly to the board of executives), SCADA risk exposures should also be formally reported to this risk management group to allow SCADA risk exposures to be assessed and managed at the corporate level.

9.4 Risk Assessment Updates

- 9.4.1 As noted, both the internal and external threat environment is likely to change over time.
- 9.4.2 To maintain the currency of RMF deliverable(s), a program should be put into place to:
- Trigger a refresh at defined intervals (e.g. annually)
 - Allow the risk environment to be re-evaluated in response to defining changes (e.g. the introduction of new technologies or the emergence of a significant external threat source).