Attachment G.25

SAPN_Telecommunications Network Operations Centre Business Case

03 July, 2015

SA Power Networks

Contents

1. Executive Summary

The purpose of this business case is to seek approval for $5.8 (June 2015, $ million) to invest in management systems for the Telecommunications Network Operations Centre (**TNOC**) to maintain the reliability and security of SA Power Networks' distribution system. This capex investment is essential as the operating expenditure step change proposal has not been accepted by the AER.

This investment would provide SA Power Networks with a single ubiquitous operational telecommunications management platform that in turn offers a significantly more secure and reliable end-to-end communications network for the delivery of services that are critical in the management of our distribution system.

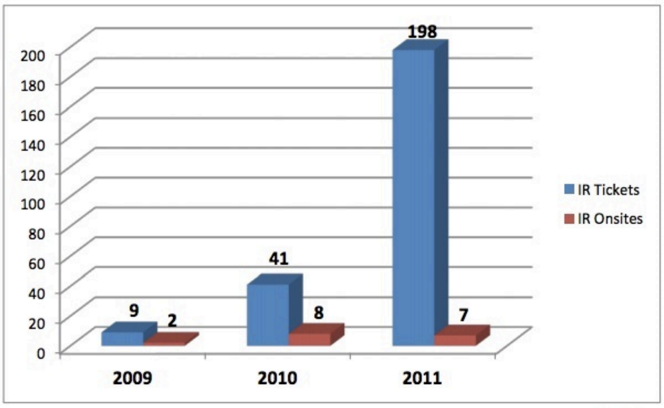
The Network Management Systems (**NMS**) is a collection of software and hardware applications that support back-office activities that are used for monitoring, control and operation of the telecommunications network to maintain customer services. The NMS is a platform to provide integration between systems and business processes. As a collection of integrated applications, the NMS supports the planning, design, build and running of both the communications network as a whole and the individual services that make use of that network. The NMS encompasses many highly technical network management processes but ultimately its purpose is to ensure the telecommunications network is efficient and services are meeting their service level regulatory obligations.

SA Power Networks currently relies on its legacy NMS to control the telecommunications network. These NMS are inefficient in managing the day-to-day operations of the telecommunications network as the existing systems operate independently of each other, requiring significant levels of manual intervention. SA Power Networks' reliance on its telecommunications network has grown significantly over the last five years and as a result reliance on our NMS alone is no longer sustainable without employing additional resources.

Furthermore, security threats such as cyber attacks are on the rise. The increasing use of network automation and mobile devices exposes the distribution network to these increasing security threats.

Globally the rise of cyber security incidents specifically targeted against Industrial Control Systems (**ICS**) has seen a sharp rise (Figure 1). While most data available is from US based agencies, Australian utilities have observed the same trends.

To date SA Power Networks has limited visibility of specific (targeted) activity against our ICS network.



ICS-CERT Incident Response Trends Data (2009-2011)

Fig. 1

Given the increasing network security risks and the increasing reliance on the telecommunications network to manage and control SA Power Networks' operations and assets, it is imperative that we have a secure streamlined and integrated NMS platform.

2. Rule requirement

Clause 6.5.7(a) of the NER provides that SA Power Networks must submit a building block proposal including a forecast of capital expenditure it requires to meet the capital expenditure objectives for the 2015-20 RCP. This includes capital expenditure required to maintain the quality, reliability and security of SA Power Networks' SCS.

The AER **must** accept the capital expenditure forecast that SA Power Networks includes in its building block proposal if the AER is satisfied the forecast capital expenditure for the 2015-20 RCP reasonably reflects the capital expenditure criteria. In making this assessment, the AER must have regard to the capital expenditure factors.

3. Background

3.1 Historical Performance

SA Power Networks owns and operates a state-wide communications network for the provision of critical operational services supporting the electrical distribution network. In addition, SA Power Networks leases communications bearers and/or services from ElectraNet and commercial carrier networks where efficient to do so.

In simplistic terms SA Power Networks' telecommunications network comprises of the following:

- in excess of 20 servers;
- circa 1,500km of fibre optic cable;
- over 20 microwave radio links;
- over 200 point to point and point to multipoint radio links;
- 35 PABX nodes including critical console communications equipment that supports the management of our electricity distribution network;
- 210 Synchronous Digital Hierarchy[1] (**SDH**) nodes; and
- 316 Plesiochronous Digital Hierarchy[2] (**PDH**) nodes.

In addition to the components listed above, our telecommunications network includes legacy pilot cable infrastructure that supports outdated substation inter-trip protection schemes.[3] The pilot cable network is being gradually phased out, however there remains in excess of 300 kilometres of pilot cable in use today.

SA Power Networks also uses the Telstra Next–G network to access more than 600 remote field devices via a dedicated Access Point Name (**APN**) within the Telstra IP-WAN network. These services are expected to grow significantly over the 2015-20 Regulatory Control Period (**RCP**). These end points and the Telstra interface are managed by the TNOC.

The TNOC also operates 30 disparate NMS to manage and control all aspects of the State-wide communications network in addition to managing and supporting the NMS systems themselves. These NMS are listed in Appendix E.

[1] SDH is a standard technology for synchronous data transmission via fibre optic's.

[2] PDH is a technology used in telecommunications networks to transport large quantities of data over digital transport equipment such as fibre optic and microwave radio systems.

[3] An 'inter-trip protection scheme' is the interconnection of protection systems between multiple substations, eg if a circuit breaker in substation fails to operate, a signal to trip the upstream circuit breaker will be sent via the pilot cable network.

3.2 Challenges

The existing NMS is no longer capable of managing SA Power Networks' increasing risks and demand for telecommunications. The challenges experienced are numerous and include:

- The inability to manage the rapidly increasing cyber security exposure of industrial control systems (**ICS**). More sophisticated supporting systems are required to address the threat of cyber attacks requiring investment in next generation firewall technology, intrusion detection and prevention (**IDS/IPS**), Authentication Authorisation and Accounting (**AAA**), operator and staff training and awareness programs, SME review, testing and continuous improvement programs.

- The demands for more telecommunications services for electrical distribution infrastructure, requires more efficient use of more telecommunications systems to off set the need for a growth in resources to cater for an increasing work load.

- The increasing demand for field telemetry to manage the electrical distribution network, including the expansion of SCADA enabled reclosers, increased demand for SCADA to substations beyond the metropolitan area, demand for SCADA to other switching devices such as Ring Main Units (**RMU**), remote engineering access to RTU's and telemetry for power quality monitoring systems.

- Evolution of telecommunications technology and protocols in particular IP based systems requiring specialised commissioning and network management tools, plus changing skill sets requires dedicated training programs for operators, system administrators and field staff.

- The need to maintain legacy communications systems. There is a long term requirement to maintain legacy systems due to the limitation of connected equipment such as protection relays that are typically deployed for periods beyond 20 years. Because these devices have limited communications interface options, they require communications equipment capable of legacy protocols/interfaces to be maintained well beyond their intended working life. This creates increased operating costs due to maintaining older communications devices and NMS.

- Business demands for greater remote access and control of electrical distribution infrastructure. The traditional substation based footprint of communications networks are evolving into a far wider network coverage, as a result the complexity and number of communication nodes are increasing to meet the these demands.

- SA Power Networks current NMS have no reporting output capability, all performance reporting requires significant manual tasks to extract information and manipulate, this makes it difficult to interpret failure mode trends and provide worthwhile KPI statistics.

4. Business Case Objectives

4.1 Objectives

The business case objective is to optimally address the existing inefficient NMS explained in Section 3 while maintaining existing resource levels, in a manner consistent with SA Power Networks' long-term strategic objectives, operational directives, telecommunication Asset Management Plans and the Operational Telecommunications Strategy 2013-2025.

Specifically the objective of this project is to provide a highly secure, reliable, high availability communications system to meet long term business requirements.

4.2 Relationship to Business Strategies and Programs

The TNOC upgrade project contributes to achievement of SA Power Networks' strategic objectives as described below in Tables 1 and 2.

Table 1 - Contribution to corporate strategic objectives

Corporate Strategic Objective	Contribution
Delivering on the needs of our shareholders by achieving our target returns, maintaining the business' risk profile, and protecting the long term value of the business	This program is expected to maintain SA Power Networks' risk profile.
Providing customers with safe, reliable, value for money electricity distribution services, and information that meets their needs	This program is expected to deliver a cost effective means to manage SA Power Networks' telecommunications network and reduce the likelihood of cyber attack impacting our distribution network.
Maintaining our business standing in the community as an exemplary corporate citizen of South Australia.	This project is expected to support SA Power Networks' standing in the community by efficiently managing the distribution network with minimal telecommunications related supply interruptions.
Ensuring that our workforce is safe, skilled and committed, and that our resourcing arrangements can meet our work program needs	This program will project will ensure secure telecommunications for field staff.
Maintenance and development of key capabilities that will help sustain our success into the future	This project will set up SA Power Networks' telecommunications operations for the long term future.

Table 2 - Contribution to corporate core areas of focus

Corporate Core Areas of Focus	Contribution
Energised and responsive customer service	Positive
Excellence in asset management and delivery of service	Positive
Growth through leveraging our capabilities	Not applicable
Investing in our people, assets and systems	Positive

4.3 Relationship to National Electricity Rules Expenditure Objectives

Table 3 - Contribution to the National Electricity Rules expenditure objectives

National Expenditure Objectives	Contribution
Meet or manage expected demand over the period	Not applicable.
Comply with regulatory obligations	In submitting its regulatory proposal, SA Power Networks must satisfy the AER of the extent to which the capital expenditure forecast includes expenditure to address the concerns of electricity consumers as identified in the course of engagement with electricity consumers. This program seeks to directly address this requirement.
Maintain the quality, reliability and security of supply of services provided by SA Power Networks	This project is required to maintain the quality, reliability and security of the telecommunications network.
Maintain the reliability and security of the distribution system ie. the electricity networks.	This project is required to maintain the quality, reliability and security of SA Power Networks' distribution network.

4.4 Meeting the National Electricity Rules Expenditure Criteria

The costs estimated to achieve this program represent efficient and prudent expenditure as detailed below.

Table 4 - Activities to Meet the National Electricity Rules expenditure criteria

National Expenditure Criteria	Activity
Efficient cost of achieving the objective(s)	All estimated costs have been calculated based on actual historical costs or vendor pricing where applicable. Where possible competitive prices have been obtained.
Cost of a prudent operator	The planned scope of works to upgrade TNOC NMS is prudent as it will enable the efficient management of SA Power Networks' telecommunications network without the need to increase operational TNOC resources in the 2015-20 RCP.

5. Project Scope

The scope this project is to invest in a suite of connected and integrated systems in order to realise the benefits of having a single ubiquitous operational telecommunications management platform that provides a long term solution for efficiently managing a secure and reliable distribution network. Furthermore, the implementation of this project will obviate the requirement to employ additional TNOC staff resources in the 2015-20 RCP.

The existing NMS is a collection of software applications and hardware that support network and back-office activities in order to provision and maintain business services. These applications and hardware platforms have little or no integration and mostly operate on dissimilar operating systems. Refer to Appendix A for a diagrammatic representation of the existing NMS.

A collection of integrated applications within an integrated NMS will support the planning, design, commissioning and management of both the communications network as a whole and the individual services that make use of that network. Refer to Appendix B.

Such NMS encompass many highly technical network management processes but ultimately its purpose is to ensure the network is managed and operated in a secure, safe, effective and efficient manner allowing for services to be delivered in line with customer and business expectations.

6. Business Case Options

The key options considered to address the poor performing TNOC NMS are summarised in Table 5 below.

Table 5 – Summary of options (June 2015, $ million)

Options	Description	Estimated Cost
Option 1: (Not recommended) Base case – Do nothing	Maintain the current TNOC NMS network and systems without addressing increasing levels of risk.	BAU
Option 2: (Recommended) Upgrade TNOC and NMS	Upgrade the current SA Power Networks TNOC facilities and NMS.	Capex: $5.8M
Option 3: (Not Recommended) Use of Outsourced Network Management Functions (Not recommended)	Seek external service providers to perform some or all of the TNOC and NMS functions.	

6.1 Option 1 – Do nothing

The 'do nothing' option is not an acceptable option because SA Power Networks would be required to maintain inefficient legacy NMS to manage the telecommunications network. This means SA Power Networks would not be able to adequately manage significant new threats to the network, which have been acknowledged in the fields of cyber security, network scalability and resourcing to manage the expanding coverage of the network.

6.1.1 Delivery Costs

Not Applicable as this option is the do nothing case.

6.1.2 Expected Benefits

No benefits are expected for this option.

6.1.3 Expected Disbenefits

An additional seven full time employees would be required over the 2015-20 RCP.

With the increase in network expansion and the greater reliance on telecommunications the existing NMS are inefficient at managing the day-to-day operation of the telecommunications network because the NMS are both disparate and independent of each other. This means significant manual tasks are required to analyse the root cause for network outages or to interpret system data and in many cases this has caused delayed restoration times for our customers.

The increase in field devices and expansion of the network coverage over the 2010-15 RCP has highlighted operational limitations within current NMS and the forecast telecommunications business requirements for the 2015-20 RCP will be further impacted by these limitations.

SA Power Networks engaged DGA consulting to undertake an analysis of future operations of the TNOC. This analysis has found a steady increase in resourcing will be required to operate the legacy NMS due to the increased network reliance on telecommunications. The forecast additional operational resourcing requirements for the 2015-20 RCP are shown in Table 6. This represents ongoing OPEX increases.

Table 6 – Option 1: resourcing requirements for the 2015-20 RCP

Period	Year 1 (2015)	Year 2 (2016)	Year 3 (2017)	Year 4 (2018)	Year 5 (2019)	Year 6 (2020)	Total
Additional TNOC resources	2	1	1	1	1	1	**7**

If we do nothing then there will be WH&S implications.

6.1.4 Timescale

Not applicable as option 1 is to do nothing.

6.1.5 Major Business Risks

The key risks as identified through our risk analysis relate to the security, reliability, operation and maintenance of the existing network and supporting NMS infrastructure and the WH&S implications for resources who work excessive hours to manage the existing inefficient systems. These (NMS) systems represent the core telemetry functions used by the Advanced Distribution Management System (**ADMS**) and SCADA networks. Interruption, degradation or unauthorised access to these communications networks will have severe consequences for the safety and supply continuity of the distribution network. Also refer to Appendix D.

Major business risks of not proceeding with this program are as follows:

Table 7 - Major business risks of not proceeding with the program

Risk ID	Risk Description (Risk Line Item)	Consequence Description	Inherent Likelihood	Inherent Consequences	Risk Rating
1.1	Unauthorised network access	• Electrocution of field staff working on the network • Major supply disruption	Low	Catastrophic	High
1.2	Insufficient resourcing	• Staff working longer hours resulting in WH&S concerns • Supply disruption due to human error	Likely	Moderate	Medium

6.2 Option 2 – Upgrade the TNOC and NMS

The preferred strategy is to upgrade the TNOC and NMS to encompass next generation technologies to manage the increasing demands on the telecommunications network, and mitigate the increasing threat of cyber attacks.

6.2.1 Delivery Costs

To achieve the specified objectives, a budget of $5.8 (June 2015, $ million) has been estimated over the 2015-20 RCP to upgrade the TNOC and NMS. The total is comprised as follows:

Table 8 - Delivery costs

Communications	2015/16	2016/17	2017/18	2018/19	2019/20	Total
Telecommunications Network Operations Centre	0.4	1.5	2.1	1.2	0.6	**5.8**

6.2.2 Delivery cost assumptions

The estimated cost of delivery of this program has been estimated based on DGA investigation into NMS solutions and advice from current SA Power Networks vendors.

6.2.3 Expected benefits

The preferred strategy is to evolve and upgrade the TNOC and NMS to encompass next generation technologies to manage the increasing demands on the telecommunications network, the increasing threat of cyber attacks and enables the optimisation of human resources.

The expected benefits are as follows:

WHS&E

Increased automation, analytics and intelligent integrated systems will reduce the potential for accidents caused by human error, including errors caused by repetitive manual tasks. It simplifies complex system topologies, and reduces the need for top tier experts to be on call 24/7 to address system issues.

High confidence in data, records and systems will result in faster response to system outages, faster restoration of services, better understanding of system events and root cause analysis, and provides a clear and precise understanding of cyber security related occurrences.

This combination of clear visibility, understanding and response will aid in the reduction of risks to staff and field crews operating the distribution network.

Technical

Automated intelligent data analysis using next generation security systems will enable rapid assessment of security threats and enable system operators to maintain the highest levels of network integrity. Detailed reporting and network monitoring will also provide the ability to investigate and trace unauthorised network activity in a timely manner and ensure security breaches are actioned in the shortest possible time.

Latest generation, integrated systems with full vendor support offer significant improvements for day to day operation of the TNOC and enable higher work flow without the need for a corresponding increase in human resources.

A single ubiquitous system for monitoring, control and provisioning on all aspects of the communications network will improve service performance and reliability and reduce manual tasks currently undertaken by TNOC staff.

Reliability

Deployment of fit for purpose, high availability systems designed for failure redundancy will ensure the highest level of communications network reliability necessary to maintain the distribution network reliability.

Next Generation equipment supports multiple fail over redundancies including redundancy in power supplies, 48V DC supply, enabling long duration survival during power outages, link aggregation technologies, load balancing and site redundancy topologies.

Expert design and peer review of logical and physical network architecture will ensure the survivability of the communications network, while maintaining serviceability and security.

Alignment

The upgrade of the TNOC and NMS will achieve alignment with SA Power Networks’ long-term strategic objectives, Operational Directives, Telecommunication Asset Management Plans, and the Operational Telecommunications Strategy 2013-2025.

6.2.4 Implementation

The program is planned to be undertaken over the entire 2015-20 RCP.

SA Power Networks engaged DGA consulting to develop a high level requirements brief. It is intended this brief would be developed into full tender document for release to the open market, for the provision of a suitable suite of NMS platforms.

Demonstration architecture and industry research will be used as tools sets to clearly define system expectations and areas of uncertainty or needing further development.

Standard business process will be undertaken during the procurement process and appropriate risk assessments and business justifications will be adhered to during implementation.

6.2.5 Major business risks

Residual business risks after mitigation by this option are as follows.

Table 9 - Major business risks associated with Option 2

Risk ID	Risk Description (Risk Line Item)	Consequence Description	Inherent Likelihood	Inherent Consequences	Risk Rating
1.1	Unauthorised network access	• Electrocution of field staff working on the network • Major supply disruption	Low	Catastrophic	High
1.2	Insufficient resourcing	• Staff working longer hours resulting in WH&S concerns • Supply disruption due to human error	Unlikely	Moderate	Low

6.3 Option 3 – Outsourcing telecommunications management

This option has only been considered in a simplistic form because SA Power Networks believes that the current risk profile associated with this outsourcing option is not satisfactory.

A review found the majority of DNSPs in Australia maintain their own communications networks due to their unique network design and diverse manufacturers equipment.

Likewise, SA Power Networks has significant variations of telecommunications equipment, vendors, topology, service delivery and functional requirements within its network. Additionally the age of this equipment ranges from current generation to legacy systems that have been installed over a 30 year period.

SA Power Networks is aware there are no suitable service providers in South Australia that could provide a full set of services across our broad range of telecommunications network elements.

Furthermore, based on preliminary information, the OPEX expenditure to outsource such services, along with the internal management and monitoring of the performance of any such service provider would be prohibitively expensive.

7. Investment appraisal

7.1 Options identification and analysis

The key options considered to address the poor performing TNOC NMS are summarised in Table 10 below.

Table 10 – Summary of options (June 2015, $ million)

Options	Description and assessment	Estimated Cost
Option 1: (Not recommended) Base case – Do nothing	Maintain the current TNOC NMS network and systems without addressing increasing levels of risk. This is unacceptable to our business because: • it does not align with our corporate risk profile; • it does not address the increasing cyber security threats; • it increases WH&S implications due to increasing use of overtime per person; and • provides inefficient and incomplete network management.	BAU
Option 2: (Recommended) Upgrade TNOC & NMS	Upgrading the current SA Power Networks TNOC and NMS will: • obviate the requirement to employee seven full time telecommunications employees; • leverages new technology developments and better automation of NMS systems; • improve network security and recovery, reliability and integrity; • enable better outage diagnosis and response to security events; • improve network safety by providing greater clarity of service function and delivery.	Capex: $5.8M
Option 3: (Not Recommended) Use of Outsourced Network Management Functions (Not recommended)	Seek external service providers to perform some or all of the TNOC and NMS functions. Preliminary investigations have determined there are no suitable service providers for this type of service within South Australia and it's unlikely that such services will be developed to a competent level within the 2015-20 RCP.	

7.2 Options evaluation

Each option has been assessed against the following evaluation criteria:

1. Health, Safety & Environment;
2. Technical functionality (i.e. benefits);
3. Maintain reliability (Operational Restoration);
4. Alignment to SA Power Networks long-term objectives and strategies; and
5. Economic risks (Financial impact/Risks).

Tables 4 and 5 below outline the scoring framework applied to assess these options:

Table 11 - Scoring framework for option evaluation

Mostly Negative Impacts	Some Negative Impacts	Neutral Impact	Some Positive Impacts	Mostly Positive Impacts
1-2	3-4	5	6-8	9-10

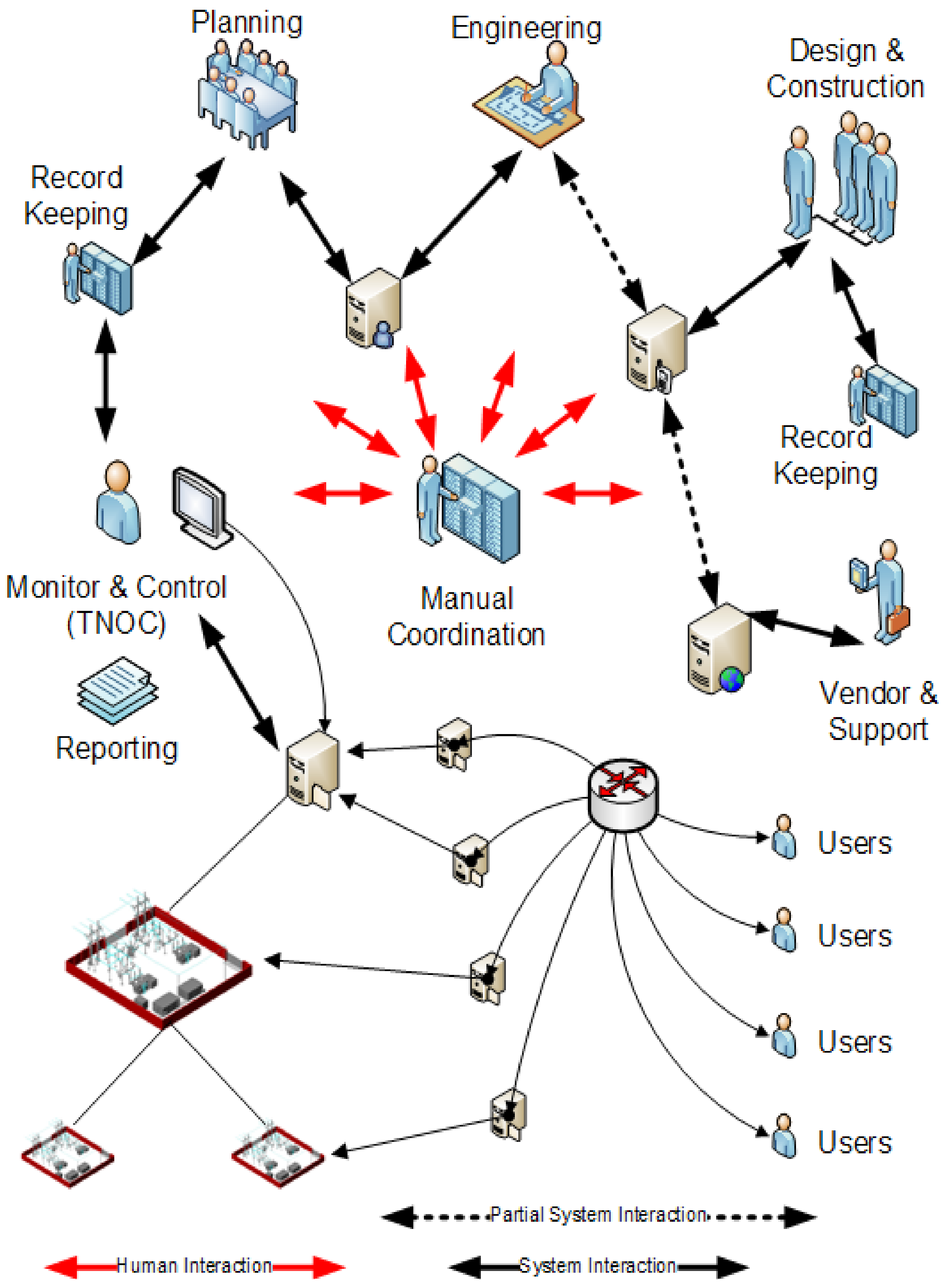
Table 12 - Evaluation results

	WHS&E	Technical (benefits)	Maintain Reliability	Alignment	Economic Risks	Total
Do Nothing	4	3	5	3	4	**19**
TNOC NMS Upgrade	6	9	7	9	6	**37**
3rd Party TNOC Operation	6	1	5	2	2	**16**

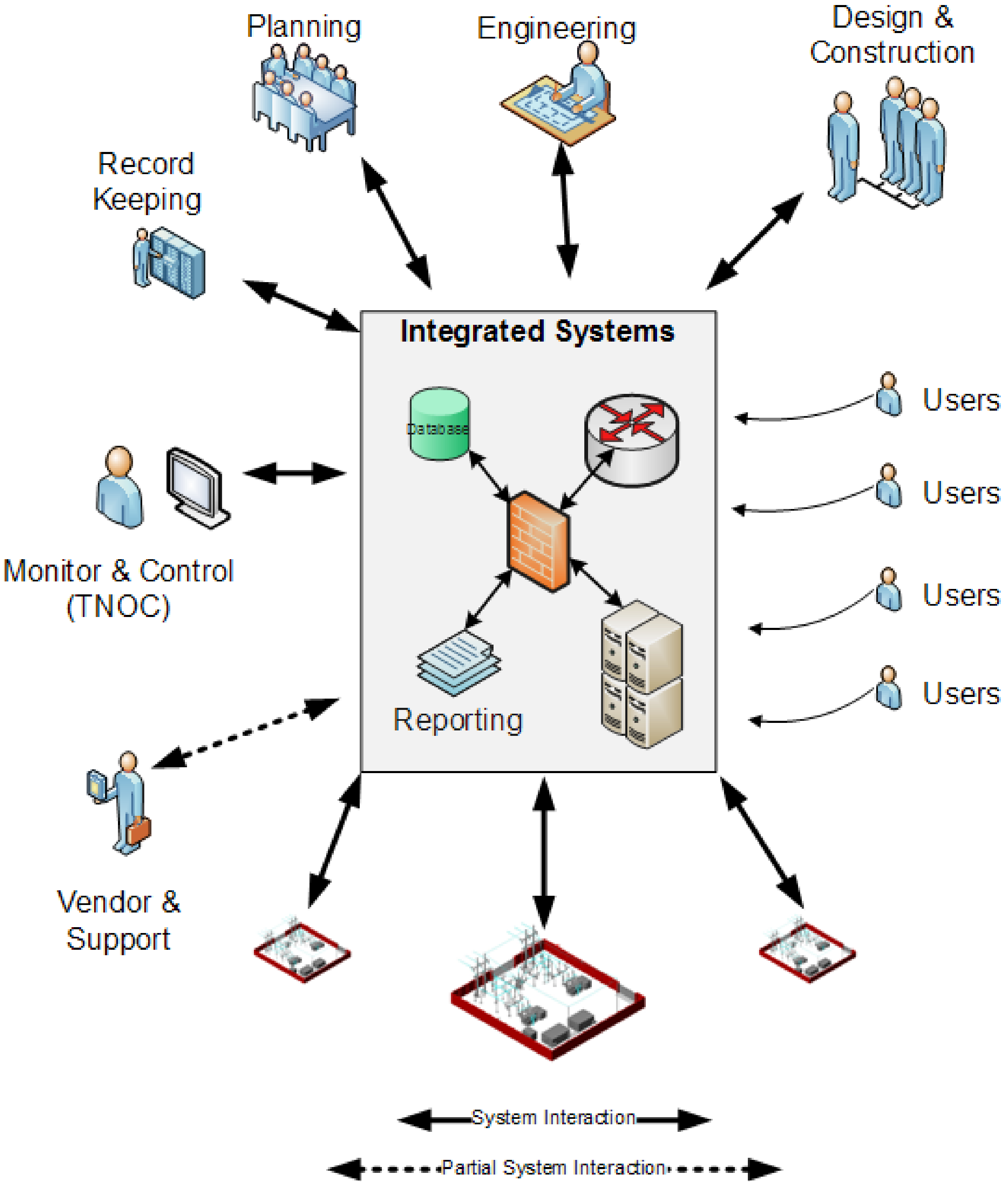
8. Recommendation

It is recommended that funding be endorsed for Option 2, with an allocation of $5.8 (June 2015, $ million) in capital expenditure over the 2015-20 RCP to upgrade the TNOC and NMS.

Appendix A - Option 1: Existing TNOC NMS Systems

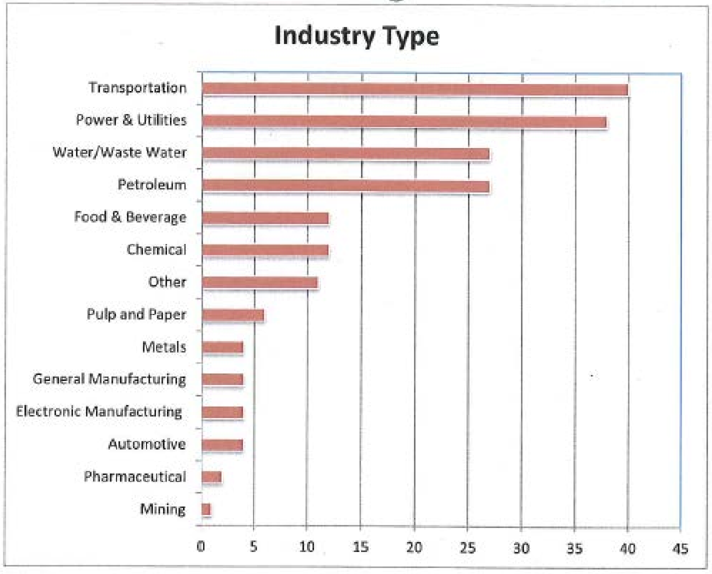


Appendix B - Option 2: Upgraded TNOC NMS Systems



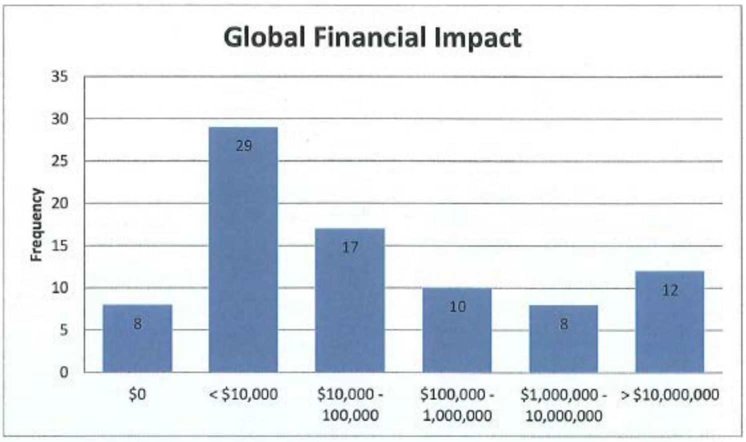
Appendix C - Cyber Security Attack Profiles

Who is Getting Attacked?



Source: RISI (2012)

Financial Impacts of Incidents



Source: RISI (2012)

Appendix D – Risk Assessment

Risk ranking Report

PART 'B' – FORMAL RISK ASSESSMENT

Description of Job/Product	Assessment Team:	Date	Consultation With:
TNOC NMS and Systems Integration	M Hough G Axon D Lim	15/6/15	

Revisions/Updates Completed By	Details	Date

RISK ASSESSMENT WORKSHEET

Table 10: Risk Assessment

Source of Risk (SOR) e.g., Equipment failure, fire, oil leak	**Element at Risk (EAR)** E.g. Operator. General public. Reliability. etc	**Interaction Consequence *(IC)** E.g. Operator exposed to ……………… Gen public exposed to ……………… Reliability impacted	**Probability (Likelihood)** *See table 1. List level number & key comments.*	**Consequence** *See table 2 List level number & key comments.*	**Level of Risk** *See table 3 List level of risk & key comments.*	**Acceptability #** *Yes or No*	**Existing Controls** **Cross-Reference Documents** **General Comments**	**Risk Treatment Options/Actions** *(Use where risk level is unacceptable)*	**Residual Risk - Probability (Likelihood)** *See table 1. List level number & key comments*	**Residual Risk - Consequence** *See table 2 List level number & key comments.*	**Residual Risk - Level of Risk** *See table 3 List level of risk & key comments.*	**Residual Risk - Acceptability #** *Yes or No*	**Residual Risk - Comments**
Cyber Security - Targeted	Safety	Operators exposed to electrical hazards from unauthorised network access	Unlikely (2)	Catastrophic (5)	High	No	Close switch gear on lines being worked on. Remotely change protection settings to cause catastrophic failure						.
Cyber Security - Targeted	Reliability	Electrical network outages from unauthorised network access	Unlikely (2)	Catastrophic (5)	High	No	Cascade outages of CBD, damage switch boards and T/F, Damage aging feeder cables						
Cyber Security - Targeted	Financial	SPS impacts and/or recovery costs from unauthorised network access	Unlikely (2)	Major (4)	Medium	No	Sophisticated, sustained system interruption resulting in multiple SPS impacts.						
Cyber Security - General	Safety	Operators exposed to electrical hazards from unauthorised network access	Unlikely (2)	Major (4)	Medium	No							
Cyber Security - General	Reliability	Electrical network outages	Possible (3)	Minimal (1)	Low	Yes							

		from unauthorised network access											
Cyber Security - General	Financial	SPS impacts and/or recovery costs from unauthorised network access	Possible (3)	Moderate (3)	Medium	No							
Network and Systems Reliability	Reputation	Business reputation impacted by service interruption due to systems failure	Likely (2)	Minor (2)	Medium	No							
Network and Systems Reliability	Reliability	Service interruption due to systems failure	Likely (2)	Minimal (1)	Low	Yes							
Network and Systems Reliability	Financial	SPS impacted service due to systems failure	Likely (2)	Moderate (3)	High	No							
Business Communications	Financial	Finance impacts of loss of corp. comms and IT backhaul services	Possible (3)	Minor (2)	Low	Yes							
Business Communications	Reputation / Customer Service	Customer service impacts from the SAPN contact centre	Possible (3)	Minor (2)	Low	Yes							
Business Communications	Legislative and Regulatory	Regulatory reporting for contact centre (grade of service)	Possible (3)	Minor (2)	Low	Yes							
Business Communications	Organisational	Business impacts from loss of corp. comms and IT backhaul services	Possible (3)	Moderate (3)	Medium	No							

Table 11: Qualitative Measures of Probability (Likelihood)

Rating	Description	Description	Probability	Typical Frequency
5	Almost certain	Is expected to occur	96-100%	At least one event per year
4	Likely	Will probably occur	81-95%	One event per year on average
3	Possible	May occur	21-80%	One event per 2-10 years
2	Unlikely	Not likely to occur	6-20%	One event per 11-50 years
1	Rare	Most unlikely to occur	0-5%	One event per 51-100 years

Table 12: Qualitative Measures of Consequence or Impact

Level	**1 Minimal**	**2 Minor**	**3 Moderate**	**4 Major**	**5 Catastrophic**
Financial	Less than $100 000	$100 000 or more, but less than $1 m	$1 m or more, but less than $10 m	$10 m or more, but less than $100 m	$100 m or more
Safety	• Incident but no injury.	• Medical treatment only.	• Lost time injury.	• Death or permanent disability.	• Multiple fatalities.
Environment	• Brief spill incident. • No environmental damage.	• Minor spill incident. • Pollution on site. • No environmental damage.	• Escape of pollutant causing environmental damage.	• Significant pollution on and off site <$0.5 m.	• Long term environmental damage.
Reputation / Customer Service	Localised customer complaints.	Widespread customer complaints or complaints to Ombudsman or Regulator.	Intervention by the Ombudsman or Regulator.	Repeated intervention by the Ombudsman or Regulator.	Loss of Distribution Licence
	Adverse regional media coverage	Adverse state media coverage	Adverse media campaigns by customers, media, industry groups	Severe negative impact on both regulated and unregulated businesses	Loss of Distribution Licence
Legislative and Regulatory	Minor breaches by employees resulting in customer complaints or publicity	Act or Code infringements resulting in minor fines.	Severe Company or Officer fines for Act or Code breaches.	Prison sentences for Directors or Officers	Loss of distribution licence.
	ACCC require apology and/or corrective advertising.	ACCC require special offer be made to all customers / suppliers.	ACCC minimum level penalties.	ACCC moderate level penalties.	ACCC maximum level penalties.
	Directors/Officer given minimum fines.	Directors/Officer given moderate fines.	Directors/Officer given severe fines.	Directors / Officers given prison sentences.	Loss of distribution licence.
Organisational	Absorbed without additional management activity.	Absorbed with minimal management activity.	Significant event which requires specific management.	Critical event that can be endured with targeted input.	Disaster which can cause collapse of business.
Reliability	2000 customers without supply for a min. of 12 hours (i.e. A medium size urban feeder)	10,000 customers without supply for a min. of 24 hours (i.e. a major storm related outage or major substation outage)	Up to 40,000 customers without supply for a min. of 48 hours (i.e. major multiple zone substation coincident	Over 40,000 customers without supply for longer than 48 hours (i.e. major geographical areas off supply)	Adelaide CBD without supply for longer than 24 hours.

			outages)		

Table 13: Qualitative Risk Analysis Matrix (Level of Risk)

	Consequences				
Probability	Minimal 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
5 Almost Certain	Medium	High	High	Extreme	Extreme
4 Likely	Low	Medium	High	High	Extreme
3 Possible	Low	Low	Medium	High	High
2 Unlikely	Negligible	Low	Low	Medium	High
1 Rare	Negligible	Negligible	Low	Low	Medium

Table 14: Risk Management - Response Level Required

Risk Level	Responsible Person	Action
Extreme	General Manager	Manage via a detailed control plan.
High	General Manager	Allocate responsibility to appropriate manager.
Medium	Manager	Manage by specific monitoring and response procedures.
Low	Manager	Manage by routine procedures.
Negligible	Manager	Monitor.

Appendix E – Network Management Systems

The Telecommunications Network Operations Centre (**TNOC**) currently operates 30 disparate Network Management Systems (**NMS**) to manage and control all aspects of the state wide communications network in addition to managing and supporting the NMS systems themselves.

The NMS under management of the TNOC include:

No.	Network Management System
1	Synchronous Digital Hierarchy (**SDH**) over fibre and microwave links;
2	SDH NMS (1350 NMS);
3	Plesiochronous Digital Hierarchy (PDH) over fibre and microwave links;
4	PDH NMS (CNMS - CastleRock);
5	Console system management for NOC communications (mobile radio and telephony – Zetron);
6	Packet based and PDH/SDH Microwave Radio equipment;
7	Packet based and TDM point to point/multi-point radio equipment;
8	SNMP NMS (CNMS-CastelRock and CNMS-NG);
9	Asset management, tracking systems and data base (Connect Master);
10	IP address assignment and management;
11	Layer 2 IP switch equipment and environments;
12	Layer 3 IP routing equipment and environments;
13	3G and 4G based remote systems via commercial carriers;
14	Security management of the network and users;
15	Next generation firewall infrastructure;
16	IPSec tunnelling and security related functions and protocols;
17	RADIUS, Active Directory, Authentication, Authorization and Accounting (AAA) systems;
18	Ethernet encapsulated in TDM;
19	Analogue PABX based telephony;
20	VoIP/ SIP PABX based telephony;
21	Various serial based communications equipment;
22	ESX virtual server environments in HA and synchronous replication mode;

No.	Network Management System
23	SNMP master stations and remote polling functions;
24	HP-UX Unix systems in standby arrangement;
25	GPS based precision clock and synchronisation sources;
26	Database and system management oversight;
27	PABX, call centre management systems, voice mail and voice recording functions;
28	Analogue VHF based Mobile Radio;
29	Environmental management solutions; and
30	DC (batteries & Rectifiers) system management.