OPTIONS EVALUATION REPORT (OER)

BKH SVC Server Upgrade

OER- 000000002062 revision 0.0

Ellipse project no(s):
TRIM file: [TRIM No]

Project reason: Capability - Obsolescence/Manufacturer support withdrawn
Project category: Prescribed - Replacement

Approvals

Author	Mohsin Yusuf	Digital Infrastructure Analyst
Endorsed	Adam Hoare	Digital Infrastructure Asset Manager
	Debashis Dutta	Asset Analytics and Insights Manager
Approved	Lance Wee	Head of Asset Management
Date submitted for approval	15 October 2021	

Change history

Revision	Date	Amendment
0	15/10/2021	First Issue

Executive summary

Proprietary SVC server PCs provide core automation functions within an SVC system including the communications link to TransGrid's on-site Data Concentrators. The Broken Hill (BKH) substation SVC, and its associated servers, are required into the foreseeable future.

The asset investigated under this need is TransGrid's existing SVC server at BKH which has been identified as running unsupported Windows XP (developer version) and presents a cybersecurity risk to the TransGrid operational network. In accordance with the Australian Cyber Security Centre Essential 8 strategies to mitigate cyber security incidents, the existing asset will fail to prevent the delivery of malware and limit the extent or detect and respond to the cyber security incidents.

A significant element of concern is the reliability consequence associated with malicious exploitation of known security vulnerabilities within the server. In addition, being a proprietary SVC server, experience with similar systems within the TransGrid network has shown numerous complexities in defect rectification work, lengthy lead times for replacement parts and an inherently long project cycle in the event of a complete upgrade. Based on this there is a significant risk of a protracted outage should severe failure occur.

In order to reduce TransGrid's cyber risk exposure and maintain our cyber security maturity, this server is proposed to be updated to a proprietary variant with a supported operating system in the 2023/24 –2027/28 regulatory control period.

The assessment of options considered to address this need appears in Table 1. Under the Base Case TransGrid continues to run the SVC server to failure, however this approach will not address the cyber risk and obsolescence of the unsupported assets.

Table 1 - Evaluated options ($ million)

Option	Description	Direct capital cost	Network and corporate overheads	Total capital cost[1]	Weighted NPV	Rank
Option A – 2062A	SVC Server Replacement	0.82	0.07	0.89	0.09	1

The preferred option is Option A as it is meets the requirements of the need, and is the only technically and commercially feasible option that enables TransGrid to meet its obligations in maintaining secure and reliable critical infrastructure.

It is the recommendation that Option A – SVC Server Replacement, be scoped in detail.

[1] Total capital cost is the sum of the direct capital cost and network and corporate overheads. Total capital cost is used in this OER for all analysis.

1. Need/opportunity

Proprietary SVC server PCs provide core automation functions within an SVC system including the communications link to TransGrid's on-site Data Concentrators. The Broken Hill (BKH) substation SVC, and hence its associated servers, are required into the foreseeable future.

The asset investigated under this need is TransGrid's existing SVC server at BKH which has been identified as running unsupported Windows XP (developer version) and presents a cybersecurity risk to the TransGrid operational network. In accordance with the Australian Cyber Security Centre (ACSC) Essential 8 strategies to mitigate cyber security incidents, the existing asset will fail to:

- prevent the delivery of malware
- sufficiently limit the extent of cyber security incidents
- adequately detect and respond to the cyber security incidents

A significant element of concern is the reliability consequence associated with malicious exploitation of known security vulnerabilities within the server. In the event of a sophisticated targeted attack, it is conceivable that further penetrations into the network including SCADA and substation security zone may be achieved, and therefore the risk will limit TransGrid's ability to return the system to service efficiently.

Being a proprietary SVC server, experience with similar systems within the TransGrid network has shown numerous complexities in defect rectification work, lengthy lead times for replacement parts and an inherently long project cycle in the event of a complete upgrade. Based on this there is a significant risk of a protracted outage should severe failure occur.

In order to reduce TransGrid's cyber risk exposure and maintain our cyber security maturity, the SVC server is proposed to be updated to a proprietary variant with a supported operating system in the 2023/24 –2027/28 regulatory control period.

2. Related needs/opportunities

Nil.

3. Options

3.1 Base case

The Base Case for this Need is to continue running the SVC server to failure. This approach does not address the risk cost associated with maintaining obsolete assets or the reliability and financial risk resulting from a cybersecurity incident targeting known network security vulnerabilities. The cost will likely increase due to:

- The probability of failure increasing as assets move further along their failure curves. Failures are the result of unrepairable internal electronic subcomponents requiring the replacement of complete assets.
- TransGrid's limited ability to effectively recover from asset failure due to obsolescence and the lack of manufacturer support.

Key drivers for this risk cost are:

- The asset is running unsupported operating system and therefore is unable to be updated or patched to effectively address or control cybersecurity risk.
- The reliability consequence to TransGrid, resulting from long-term failure of the network asset due to a cybersecurity related compromise.
- The asset identified has reached their end of life and has very limited manufacturer support. The underlying technology is no longer produced in the market and thus replacements are reliant on depleting stocks held by

TransGrid. This increases the likelihood that TransGrid won't be able to mitigate or repair failures effectively should a hazardous even occur.

Increasing maintenance on the equipment cannot reduce the likelihood of a cybersecurity event occurring in order to reduce the risk cost.

3.2 Options evaluated

Option A — SVC Server Replacement [NOSA 2062, OFS 2062A]

This option involves replacing the existing SVC server running unsupported Windows operating systems, to a proprietary variant with a supported operating system. This will include installation and commissioning of new control computers including hardware and licences.

This option provides malware detection capabilities, enables patch management and security updates of the server which would deliver cyber risk mitigation. This option further delivers reduced corrective maintenance benefits to consumers and the network by addressing the probability of failure of identified asset. This option will not deliver any additional operational benefits such as improved capabilities.

This option is planned for deployment in the 2023/24-2027/28 regulatory control period. The targeted asset will be in service for approximately 10 years.

3.3 Options considered and not progressed

Table 2 - Option not progressed

Option	Reason for not progressing
Decommissioning of SVC Server	This can only be achieved through retirement of the associated primary assets, which is not technically or economically feasible.
Non-network solutions	It is not technically feasible for non-network solutions to provide the functionality of secondary systems assets for protection, control, communications and metering

4. Evaluation

4.1 Commercial evaluation methodology

The economic assessment undertaken for this project includes three scenarios that reflect a central set assumptions based on current information that is most likely to eventuate (central scenario), a set of assumptions that give rise to a lower bound for net benefits (lower bound scenario), and a set of assumptions that give rise to an upper bound on benefits (higher bound scenario).

Assumptions for each scenario are set out in the table below.

Table 3 - Scenario assumptions

Parameter	Central scenario	Lower bound scenario	Higher bound scenario
Discount rate	4.8%	7.37%	2.23%
Capital cost	100%	125%	75%
Operating expenditure benefits	100%	75%	125%
Risk costs benefits	100%	75%	125%

Parameter	Central scenario	Lower bound scenario	Higher bound scenario
Other benefits	100%	75%	125%
Scenario weighting	**50%**	**25%**	**25%**

Parameters used in this commercial evaluation are shown in Table 4

Table 4 - Commercial evaluation parameters

Parameter	Parameter Description	Value used for this evaluation
Discount year	Year that dollar values are discounted to	2020/21
Base year	The year that dollar value outputs are expressed in real terms	2020/21 dollars
Period of analysis	Number of years included in economic analysis with remaining capital value included as terminal value at the end of the analysis period.	10 years
Safety disproportionality	Multiplier of the environmental and safety related risk cost included in NPV analysis to demonstrate implementation of obligation to reduce to ALARP.	Refer to section 4.3 for details.

The capex figures in this OER do not include any real cost escalation.

4.2 Commercial evaluation results

The commercial evaluation of the technically feasible options is set out in Table 5. Details appear in Appendix A.

Table 5 - Commercial evaluation ($ million)

Option	Capital Cost PV	Central scenario NPV	Lower bound scenario NPV	Higher bound scenario NPV	Weighted NPV	Ranking
Option A	0.74	0.06	-0.35	0.60	0.09	1

4.3 ALARP evaluation

TransGrid manages and mitigates bushfire and safety risk to ensure they are below risk tolerance levels or 'As Low As Reasonably Practicable' ('ALARP'), in accordance with the regulation obligations and TransGrid's business risk appetite. The need for replacement of the identified asset is not driven by these risks and there is no quantifiable safety risk reduction by addressing the condition of this asset.

4.4 Preferred option

The preferred option to meet the identified need by 2027/28 is Option A. Option A is the only technically and commercially feasible solution enabling TransGrid to continue meeting its obligations in maintaining secure and reliable critical infrastructure. Option A, was found to have positive net economic benefits.

Capital and Operating Expenditure

There is no change in predicted ongoing planned routine operational expenditure between the option and the Base Case.

Resultant corrective maintenance under the base case strategy is anticipated to result in higher expenditure over the upcoming regulatory period. Delivery of proposed works under Option A will reduce the risk of increasing direct defect response costs.

Based on the failure rate of these assets it has been modelled that once limited spares deplete, maintaining the unsupported Windows XP based server means we will incur significant operational expenses to respond to any potential defect.

These operating expenditure benefits have been captured in the economic evaluation.

Regulatory Investment Test

The program and estimate allows for the appropriate Regulatory approvals as required.

5. Optimal Timing

The test for optimal timing of the preferred option has been undertaken. The approach taken is to identify the optimal commissioning year for the preferred option where net benefits (including avoided costs) of the preferred option exceeds the annualised costs of the option. The commencement year is determined based on the required project disbursement to the meet the commissioning year based on the OFS.

The results of optimal timing analysis is:

- Optimal commissioning year: 2025/26
- Commissioning year annual benefit: $0.23 million
- Annualised cost: $0.11 million
- Based on the optimal timing, the project is expected to commence in the 2023/24-2027/28 Regulatory Period.

6. Recommendation

It is the recommendation that Option A – SVC Server Replacement, be scoped in detail.

The total project cost associated with this option is $0.89 million including an amount of $0.10 million to progress the project from DG1 to DG2.

Appendix A – Option Summaries

Project Description	FY24-28 BKH SVC Server Upgrade		
Option Description	Option A - SVC Server Replacement		
Project Summary			
Option Rank	*1*	Investment Assessment Period	*10*
Asset Life	*10*	NPV Year	2020/21
Economic Evaluation			
NPV @ Central Benefit Scenario (PV, $m)	0.06	Annualised CAPEX @ Central Benefit Scenario ($m)	Annualised Capex - Standard (Business Case) 0.11
NPV @ Lower Bound Scenario (PV, $m)	-0.35	Network Safety Risk Reduction ($m)	Network Safety Risk Reduction 0.00
NPV @ Higher Bound Scenario (PV, $m)	0.60	ALARP	ALARP Compliant? NA
NPV Weighted (PV, $m)	0.09	Optimal Timing	Optimal timing (Business Case) 2025/26
Cost (Central Scenario)			
Total Capex ($m)	0.89	Cost Capex (PV,$m)	0.74
Terminal Value ($m)	0.00	Terminal Value (PV,$m)	0.00
Risk (Central Scenario)	**Pre**	**Post**	**Benefit**
Reliability (PV,$m)	Reliability Risk (Pre) 0.00	Reliability Risk (Post) 0.00	Pre – Post 0.00
Financial (PV,$m)	Financial Risk (Pre) 0.00	Financial Risk (Post) 0.00	Pre – Post 0.00
Operational/Compliance (PV,$m)	Operational Risk (Pre) 0.00	Operational Risk (Post) 0.00	Pre – Post 0.00
Safety (PV,$m)	Safety Risk (Pre) 0.00	Safety Risk (Post) 0.00	Pre – Post 0.00
Environmental (PV,$m)	Environmental Risk (Pre) 0.00	Environmental Risk (Post) 0.00	Pre – Post 0.00
Reputational ($m)	Reputational Risk (Pre) 0.00	Reputational Risk (Post) 0.00	Pre – Post 0.00
Total Risk (PV,$m)	Total Risk (Pre) 0.00	Total Risk (Post) 0.00	Pre – Post 0.00
OPEX Benefit (PV,$m)			OPEX Benefit 0.00
Other benefit (PV,$m)			Incremental Net Benefit 0.80
Total Benefit (PV,$m)			Business Case Total Benefit 0.80