

Strategic Scope OT Security Environment Enhancements



Part of the Energy Queensland Group

Revision History

Revision date	Version number	Description of change/revision
31/01/2019	1	AER Document Initial release

Document Approvals

Name	Position title	Date
Ana Smith De Preze	GM Intelligent Grid Solutions	31/01/2019
Peter Price	EGM SASP	31/01/2019

Document Tracking Details

Network and Non-Network Document Hierarchy Reference Number	Regulatory Proposal Chapter Reference	Document	File Name
NET AUG - 026	7.133	Strategic Scope – OT Security Environment Enhancement - Energex & Ergon Energy	EGX ERG 7.133 Strategic Scope - Security Environment Enhance JAN19 PUBLIC

Contents

- 1. Project Summary 1
- 2. Existing Arrangements / Background..... 1
- 3. Rationale / Benefits 2
- 4. Drivers 3
- 5. Scope 3
- 6. Exclusions 3
- 7. Assumptions..... 4
- 8. Supporting Information 4
- 9. Options Considered..... 4
 - 9.1 Option One 4
 - 9.2 Option Two (Preferred Option)..... 4
- 10. Risk Assessment 5
- 11. Delivery Timeframe 6
- 12. Project Cost Summary 6
- Appendix 1. Definitions, Abbreviations and Acronyms 7

1. Project Summary

PROJECT SUMMARY INFORMATION			
Work Request Description	OT Security Environment Enhancements (Energex and Ergon Energy)		
Work Request Number	1365272	Work Request Required by Date	
Initiating Work Group	Intelligent Grid Solutions	Strategic Scope Contact	
Business Owner	AS&P		
Direct Value:	\$7.05M		

NOTE: – This document does not constitute approval of any funds or financial delegation. It is used to provide a high-level description and justification of an allocation of funds in future years. The direct value presented above is in \$18/19 direct dollars.

2. Existing Arrangements / Background

This initiative is based upon Energy Queensland's Cyber Security Strategy which focuses on improving the cyber-security capability maturity model (C2M2) rating as part of the broader increase in cybersecurity awareness and capability. Energy Queensland is following the lead of AEMO and ENA in adopting the framework and using it to track performance and capability.

This initiative is also based upon the strategies defined in the Future Grid Roadmap and the Intelligent Grid Technology Plan. From these strategies, a technology solution and its associated costing and benefits have been described below.

Currently, both Energex and Ergon have significant security infrastructure to protect and manage the operational networks. This security specific infrastructure has constantly evolved as the security threat has evolved. Ergon Energy had a major upgrade in 2007-08 as part of the Link project (centralised Control Rooms and SCADA). Energex had a major upgrade in 2010-11 as part of Matrix and the DMS project. Ergon Energy recently had a further major upgrade in 2015-16 to bring it up to the current standards.

These solutions around perimeter security, access and identity management, and threat detection and prevention are currently suitable to meet the currently understood threats.

The security landscape, however, is not static, and new and emerging threats are regular occurrences. As well as the regularly reported data breaches (Facebook, Ashley Madison etc.), there is an increase in attacks on critical infrastructure globally. A recent example was the admission by the US Department of Homeland Security that Russia had penetrated 6 US-based power utilities. The Russian successful direct cyber-attack on Ukraine's power network in 2015 has demonstrated the consequences of a security breach.

When these breaches occur, the security industry analyses the exploit and develops a "kill chain" which is then used to determine the best defence against the attack. Generally, the existing security

specific infrastructure in Energex and Ergon Energy's power networks can be reconfigured to provide the relevant defences. However, the broad variety of attacks such as the VPNFilter exploit which targeted actual network devices (such as Routers) means that how the power networks are protected will need to be regularly reviewed and updated to the latest capability. This is likely to require changes in technology infrastructure. Historical examples include moving from ID and password for access to 2-factor authentication (e.g. physical or virtual token) and requiring completely separate identities across Corp and Operational networks. Security companies are now investing heavily in artificial intelligence to do the "heavy lifting" in threat intelligence and data analysis.

The power networks are also becoming more connected to the outside environment. There is an expectation of more customer choice in how the power network is used. This means that Energy Queensland will need exponentially more operational data about the networks particularly closer to the customer. This increases the surface area of potential attacks that will need to be mitigated.

In 2015-16 Ergon Energy completed a security project which implemented significant new capability in areas such as security segregation, intrusion detection and prevention, identity and authorisation and perimeter management. The security components of this project cost approx. \$3.5M. It is expected that approximately every 3-5 years that new capability in these areas will be required, as both Ergon and Energex have had to enhance their security capability to counter the most recent threat. Using this information from the most recent project as a financial benchmark, it is expected that in the 2020-25 period that both networks will need to spend an additional \$3.5M to enhance capability and deter emerging threats.

3. Rationale / Benefits

There are a number of concurrent events that justify this initiative to continue to invest in new security capability.

- a) The threat landscape is constantly changing. Critical Infrastructure internationally has been targeted and there have been localised attempts on elements of the Australian electricity market.
- b) The Federal Government has recently legislated that distribution networks are now considered critical infrastructure and will be engaging directly with them on security prevention. The Federal Government has also implemented restrictions in technology purchases and how technology is implemented and supported if it impacts the power network. These restrictions are now in place for Transgrid and Ausgrid in NSW.
- c) Both CERT Australia (Federal Government Security) and ENA are working closely together to educate utilities on the security risk, and assessment tools to assist in improving an organisation's security posture
- d) Cyber threats are now being assessed as a risk that is similar to natural disasters in terms of impact to distribution networks.

The above demonstrates that as an industry, the cybersecurity threat is seen as credible. By continuing to enhance the security capability of the networks, this will reduce the risk of power loss and equipment damage as well as reputational damage caused by such an event.

The customer benefits for this initiative will be a more secure distribution network leading to less chance of adverse network issues, including customer outages.

4. Drivers

There are a number of drivers that influence this initiative:

1. Electricity Network Transformation Roadmap which has been used as the basis for Energy Queensland's Intelligent Grid roadmap. A key element is Power System Security. It is expected utilities have a close focus on physical and cyber security.
2. Threat Landscape – there are now credible attempts occurring on critical infrastructure around the world (including Australia). The increase in the points of connection for the OT network associated with Intelligent Grid initiatives vastly increases this landscape.
3. Federal Government Oversight – the Critical Infrastructure legislation is the start of more direct government involvement on how utilities manage security.

These drivers indicate that Energy Queensland will need to be proactive in its approach to managing the evolving threats posed by cyber events.

5. Scope

The scope of this initiative is based on a number of assumptions around the threat landscape and the maturity of security technology.

- It is expected that the current infrastructure will be suitable to deter and manage attacks until 2021-22 across the network. This is because there isn't expected to be significant changes to the way the power network operates until that point.
- In 2021-22, there will be significant increases in consumer assets (PV and Battery) that will be targeted for attack, with implications for utilities requiring investment in new capabilities.
- The growth in a consumer-led network from 2022 onwards will see regular attempts to impact the operation of the power network either as a strategic element (nation-state involvement) or financial gain element (organised crime). This will require regular investment in new security capability in 2022/23 and annually after that.

The technical solutions to be implemented will depend on the threat landscape at the time. As an example, the current Energex and Ergon Energy Intrusion detection technology did not exist when Ergon Energy implemented security solutions as part of the Link project in 2007-08.

Areas that are likely to be required for enhancement include the following:

- Perimeter enhancements to support 3rd party data services and cloud-based connections to meet DER and hosting capacity requirements.
- Cyber Security analytics based upon OT protocols (compared to IT-based solutions).
- 2-factor authentication for all staff accessing OT devices and systems.
- IED audit and authentication services.
- Encryption and certificate services at the OT device layer.

6. Exclusions

This initiative is for implementation of new OT security capability only. It is not to maintain the existing systems and technology that relates to security in the power network.

This initiative relates to security infrastructure (technology hardware and software) and does not account for any changes required in staffing to operate the new capability.

7. Assumptions

Assumptions include:

- Existing security capability is maintained and operated to meet the needs of the current threat environment.
- Any additional staffing required to operate the new capability will be provided as required.

8. Supporting Information

This initiative forms part of Energy Queensland's Future Grid Roadmap, which is the response to meeting the requirements of the ENA/CSIRO Electricity Network Transformation Roadmap.

Specific information on strategies can be found in the Intelligent Grid Technology Plan.

9. Options Considered

9.1 Option One

Do nothing impact

The current Energex and Ergon Energy OT cybersecurity infrastructure has been designed to meet the current threat landscape. This infrastructure will continue to operate effectively if maintained and supported and the threats don't change.

Based upon the history of cyber events, the method of attack evolves regularly and significant investment occurs by malicious actors to achieve their goal.

The impact on this will be that the likelihood of a cyber event in the power networks will continue to increase with a risk rating that will make it intolerable to the business. A worst-case scenario is that a successful attack occurs which causes widespread and sustained power outages causing significant economic loss and significant reputational damage to Energy Queensland.

The "Do Nothing" has a direct and negative impact on customers.

- Increased risk of outages and prolonged outages due to the deliberate targeting of the power network by threat actors,
- Increased risk of data theft which may have a direct or indirect impact on customers,
- Increased risk of damage to customer equipment through the deliberate mal-operation of network equipment causing voltages outside statutory requirements.

9.2 Option Two (Preferred Option)

Implement the initiative to regularly invest in new OT cyber security capability

This option is considered to be the best solution to maintain a reasonable degree of protection from a cyber event in the power networks. It is unlikely that cyber risk will ever drop to a low level, however by implementing this initiative; the goal is to maintain the risk rating at its current level.

This means that the expenditure of \$7M across the 5 years for new capability is the cost of maintaining a reasonable risk exposure to operate the power network going forward.

10. Risk Assessment

The network (business) risk the organisation would be exposed to if the project was not undertaken.

Risk Scenario	Risk Type	Consequence (C)	Likelihood (L)	Risk Score	Risk Year
Cybersecurity threats and vulnerabilities are not detected and managed resulting in inability to remotely control the majority of the Energex/Ergon network.	Business Impact	6	4	24	2020
Cybersecurity threats and vulnerabilities are not detected and managed resulting in inability to maintain supply and widespread customer outages >70,000.	Customer Impact	6	3	18	2020
Cybersecurity threats and vulnerabilities are not detected and managed resulting in inability to maintain supply or quality of service and EQL are subject to adverse national media attention.	Customer Impact	4	3	12	2020

Table 1 – Risk Assessment

Network Risk Evaluation Matrices:

- [Consequence and Likelihood Table](#)
- [Tolerability Scale](#)

The preferred option (OT Security Environment Enhancements) is the right option to reduce this risk, as it provides the additional capability to manage new threats as they occur. There is a growing awareness that the number and complexity of cyber threats against the energy industry are increasing, and this option will allow the power networks to stay current with new capability at all times.

Risk Assessment Outcome

The network (business) risk the organisation would be exposed to if the project was not undertaken is not deemed to be as low as reasonably practicable (ALARP). Addressing the risks as detailed above through implementation of the preferred option will reduce Energy Queensland's risk exposure.

11. Delivery Timeframe

The delivery timeframe will depend on two factors:

1. When new threats become known
2. Availability of new technology that enhances our ability to detect, and repel any attacks.

The initiative is currently modelled around an expectation of projects in 2021/22, 2023/24 and 2024/25 that will deploy the new technology across both networks.

It is also expected that these projects will be biased towards software, and potentially solutions as a service models, rather than hardware-based infrastructure however that will depend on the issues being solved.

12. Project Cost Summary

The numbers below are based on 2018/19 dollars

ENERGEX	FY 2020/21	FY 2021/22	FY 2022/23	FY 2023/24	FY 2024/25
Equipment		\$500,000		\$1,000,000	\$500,000
Labour		\$200,000		\$125,000	\$125,000
Material		\$450,000		\$350,000	\$275,000
Grand Total:		\$1,150,000		\$1,475,000	\$900,000

Table 2 – Energex Cost Summary

ERGON ENERGY	FY 2020/21	FY 2021/22	FY 2022/23	FY 2023/24	FY 2024/25
Equipment		\$500,000		\$1,000,000	\$500,000
Labour		\$200,000		\$125,000	\$125,000
Material		\$450,000		\$350,000	\$275,000
Grand Total:		\$1,150,000		\$1,475,000	\$900,000

Table 3 – Ergon Energy Cost Summary

NOTE: The numbers presented above in the cost summary are \$18/19 direct dollars.

Appendix 1. Definitions, Abbreviations and Acronyms

BESS	Battery Energy Storage System
CSIRO	Commonwealth Scientific and Industrial Research Organisation
DER	Distributed Energy Resource
DSO	Distribution System Operator
ENA	Energy Networks Association
ENTR	Electricity Network Transformation Roadmap
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
HV	High Voltage (35kV – 230kV AC)
IS	Isolated System
LV	Low Voltage (50V – 1 000V AC)
MEGU	Micro Embedded Generating Units
MV	Medium Voltage (1kV – 35kV AC)
NER	National Electricity Rules
PQ	Power Quality (of the network)
PV	(Solar) Photovoltaic System
QoS	Quality of Supply (to a customer)
SCADA	Supervisory Control and Data Acquisition
ZS	Zone Substation