Revised Proposal

Attachment 5.13.L.6

Industry Best Practice for Operational Technology Cyber Security

January 2019

Content

1 OPERATIONAL TECHNOLOGY CYBER SECURITY

1.1 Purpose

This document outlines the recent history regarding the cyber security uplift to Ausgrid’s operational technology domain, including a summary of obligations and background to the introduction of the Critical Infrastructure Licence Conditions, the Critical Infrastructure Act 2018 and associated implications to Ausgrid’s Operational Technology environment. This document also outlines Ausgrid’s interpretation of ‘best industry practice for electricity network control systems’ as referenced in Ausgrid’s Licence Conditions.

1.2 Background

The industrial control systems within the electrical network industry, known as Operational Technology (OT), are defined as the application of information technology systems for the purpose of directly operating or managing devices on the electricity network, including the integration of remote devices (field and substation) with supervisory control and data acquisition (SCADA) systems using communications links to provide a platform that is used to monitor and operate the underlying asset.

Historically, industrial control systems utilised specialised, bespoke hardware and dedicated communication channels. However, in the last 25 years, SCADA systems have moved away from bespoke hardware to utilising similar or identical Information Technology (IT) platforms. These platforms provide improved functionality, flexibility and redundancy for lower cost, however require different skills and capability to manage. Importantly these systems share some security vulnerabilities that can affect corporate IT systems that bespoke industrial systems were not exposed to. Management of these security vulnerabilities in the OT environment is a fast-evolving area and has become a significant focus of utilities and governments around the world.

1.3 Challenges of OT / IT Convergence

The trend of industrial control systems and OT platforms making increased use of IT technology is commonly referred to as OT / IT Convergence (or OT / IT Integration).

Although OT and IT technologies are converging there remain a number of important differences between the two domains. Traditional IT security objectives (heavily influenced by the banking and financial sectors) typically follow the priorities of confidentiality, integrity and availability. In the case of control systems, and particularly electricity networks, the consequences of a security breach are very different and therefore the priorities are different.

The combined importance of availability and integrity within an OT system mean that nothing must be done on the active control systems network that would interfere or disrupt the time-critical operations of the system. In the control systems environment, the security objectives of the IT world are replaced by human health and safety, availability of the system, and timeliness and integrity of the data.

Table 1 illustrates the key differences in the priority of system objectives and the key consequences from the loss of system function from a cyber security intrusion.

Table 1 - IT / OT Cyber Security Differences

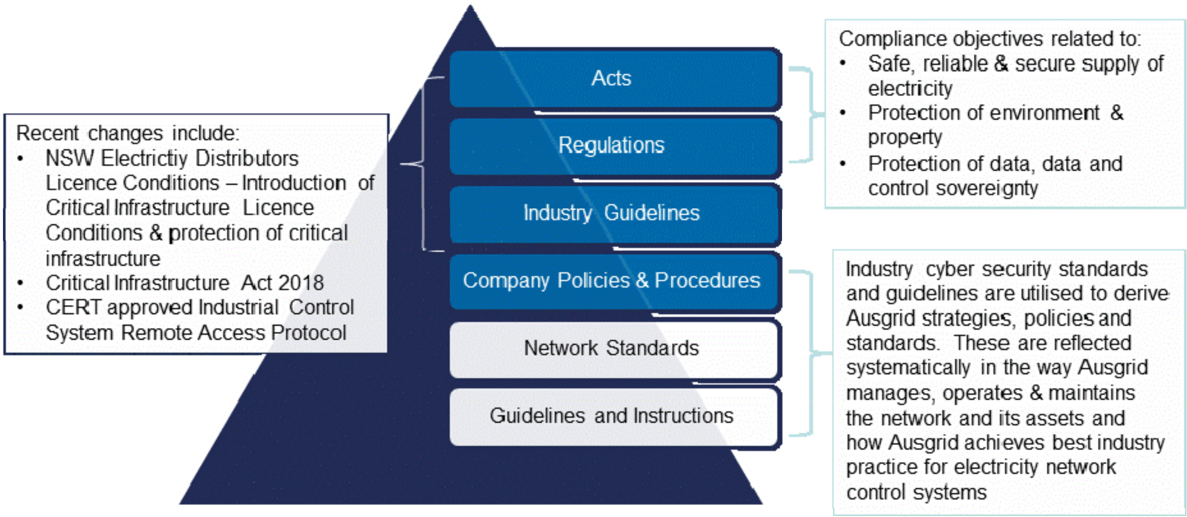
IT / OT Cyber Differences	Operational Technology	Information Technology
Objectives: Information & Operational Technology systems and processes have differing objectives given their differing purposes	Objectives by priority 1. System Integrity 2. System Availability 3. Information Confidentiality	Objectives by priority 1. Information Confidentiality 2. System Integrity 3. System Availability
Consequences: The criticality and type of realised consequences differ between information and operational systems for a failure or potential cyber intrusion.	• Power Outages • Damage to Assets • Reputational Damage • Injury • Death • Regulatory Fines • Work Cover Investigations • Court Actions and/or Coroner's Court	• Loss of Privacy • Loss of Productivity • Financial Loss • Reputational Damage • Loss of Data • Regulatory Fines • Court Actions

Due to these differences, while the OT and IT domains often use similar or identical technology, differences in focus between the two domains drives the need for specific industry-aligned approaches appropriate to cyber security for the OT domain.

1.4 Ausgrid's Regulatory Environment

Ausgrid operates in a highly regulated environment. Ausgrid's cyber security governance, at a high level, is shown in Figure 1.

Figure 1 - Ausgrid Compliance Requirements



Recent changes include:
- NSW Electrictiy Distributors Licence Conditions – Introduction of Critical Infrastructure Licence Conditions & protection of critical infrastructure
- Critical Infrastructure Act 2018
- CERT approved Industrial Control System Remote Access Protocol

Compliance objectives related to:
- Safe, reliable & secure supply of electricity
- Protection of environment & property
- Protection of data, data and control sovereignty

Industry cyber security standards and guidelines are utilised to derive Ausgrid strategies, policies and standards. These are reflected systematically in the way Ausgrid manages, operates & maintains the network and its assets and how Ausgrid achieves best industry practice for electricity network control systems

1.5 Ausgrid's Critical Infrustructrue Licence Conditions

Ausgrid has key obligations in its Distributor's Licence to operate a distribution system under the Electricity Supply Act 1995 (NSW). The NSW Minister for Industry, Resources and Energy grants the distribution licence under section 14 of the Electricity Supply Act 1995 (NSW). The Minister also imposes on Ausgrid a schedule of Licence Conditions for the Operator (Ausgrid) of a Transacted Distribution System.

On 1 December 2016 Ausgrid transitioned to a 50.4% long term lease with private ownership. As part of the lease transaction, the NSW Minister updated the schedule of Licence Conditions for the Operator (Ausgrid).

A key change at this point in time was the introduction of additional 'Critical Infrastructure Licence Conditions' (Conditions 9, 10 and 11). These requirements describe the significance of infrastructure being managed by Ausgrid, as described in the excerpt below:

> CRITICAL INFRASTRUCTURE LICENCE CONDITIONS
>
> *… the assets which the Licence Holder operates may constitute "critical infrastructure" being those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the security, social or economic wellbeing of the State of New South Wales … These licence conditions will be reviewed by the Minister from time to time (and where necessary) in consultation with responsible Ministers of the Commonwealth ...*

The Critical Infrastructure Licence Conditions included in the schedule of Licence Conditions were developed by NSW Government and Commonwealth agencies. This review included Foreign Investment Review of the Licence Condition provisions. The licence conditions require a:

- Substantial presence must be held in Australia and prevent operation or control of the control systems or the supporting ICT from outside of Australia (Condition 9); and
- Data Security must be maintained that prevents access to operational technology, ICT or bulk load and customer information from outside of Australia or from unauthorised persons (Condition 10).

Condition 9 contains clear requirements for Ausgrid to use industry best practice. As industry best practices are evolving, Ausgrid interprets best industry practice in a manner consistent with industry participants, such as the Australian Energy Market Operator (AEMO). This includes adoption of a hierarchy of industry standards, guidelines and advice as outlined in Table 2 – Hierarchy of reference material representing industry best practice, and the best practice reference list attached in Appendix 1.

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

As the Licence Conditions require Ausgrid to use best industry practice, an annual plan is developed to maintain compliance in line with the evolving frontier of industry best practice. Ausgrid consults with industry participants and bodies continuously and incorporates feedback into each annual planning cycle.

Ausgrid's Critical Infrastructure Licence Conditions were revised and re-issued in December 2017 following the first IPART audit against the conditions in 2017, and subsequent detailed engagement with IPART, the NSW Minister for Industry, Resources and Energy, and relevant Commonwealth agencies.

The key revisions to the Critical Infrastructure Licence Conditions were:

- Introduction of the Remote Access Protocol; and
- Adjustment of Data Security requirements and definitions.

[redacted]

[redacted]

[redacted]

1.6 Critical Infrastructre Act 2018

The Security of Critical Infrastructure Act 2018 commenced in July 2018, to provide a framework for managing risks to national security relating to critical infrastructure through:

- improving the transparency of the ownership and operational control of critical infrastructure in Australia in order to better understand those risks; and
- facilitating cooperation and collaboration between all levels of government, and regulators, owners and operators of critical infrastructure, in order to identify and manage those risks.

A critical Infrastructure asset is defined to include critical electricity assets, which are defined broadly to include a network, system, or interconnector, for the transmission or distribution of electricity. Ausgrid's distribution system is a critical electricity asset and its entire network is captured by the definition within the Act.

The act includes powers of direction and information provision.

The Critical Infrastructure Centre has been formed to administer the Act and carry out the following high-level activities:

[1] https://www.cert.gov.au/sites/g/files/net3281/f/remote_access_protocol.pdf

- Conduct national security risk assessments to support the Foreign Investment Review Board;
- Develop and implement targeted mitigations in concert with industry, states and territories; and
- Develop improved best practice guides for industry.

Ausgrid has closely engaged with the Critical Infrastructure Centre during the development of the Act, the 2017 revision to the Ministerial Distributor's Licence Conditions and the Advanced Distribution Management System (ADMS) project. All of these engagements have informed and refined Ausgrid's understanding of what constitutes industry best practice for electricity network control systems.

1.7 Industry Best Practice

In 2016 Ausgrid developed an OT / Control System Security Strategy which was further refined with the introduction of the Critical Infrastructure Licence Conditions and its subsequent revision. This strategy has informed the Operational Technology Security Strategy and the cyber security program.

This strategy references current good and best practice in SCADA systems and, where applicable, IT Cyber Security practices from the following key reference material outlined in the best practice reference list attached in Appendix 1. This approach is in alignment with Ausgrid's obligations under Critical Infrastructure Licence Condition 9.2.

A hierarchy of reference material has been developed with the most authoritative being IEC-62443 – Security for industrial automation and control systems as depicted in Table 2 – Hierarchy of reference material representing industry best practice. In cases where the primary reference offers no (or insufficient) guidance, secondary and more detailed reference materials are utilised.

Table 2 – Hierarchy of reference material representing industry best practice

Hierarchy of Preferred Best Practice Standards	Applicable Standard
Primary Reference Standards • International standard for control systems • Backup coordination, storage and orchestration tools	IEC-62443 – Security for Industrial Automation and Control Systems
Secondary Reference Standards • Authoritative (US Government) guide for control systems	NIST SP800-82 – Guide to Industrial Control Systems (ICS) Security
Detailed References • Authoritative Government guide for specific issues and where relevant vendor recommendations	Generic Cyber Security Government Guides and Standards • NIST Special Publications • ASD Strategies & Guidance Vendor Recommendations • Recommended configurations • Reference architectures • Support notices

Note, this is a current view of industry OT cyber best practice. As the cyber threat landscape continues to change, industry and general cyber security best practice is expected to change and evolve. Ausgrid will continue to monitor and update this reference list during its annual planning cycle.

1.8 Appendix 1 – Best Practice Reference List

International		
ISA	International Society for Automation	• TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems, • TR99.00.02-2004 Integrating Electronic Security Into The Manufacturing And Control Systems Environment
IEC	International Electrotechnical Commission	• 62443-1-1 Security for Industrial Automation and Control Systems – Models and Concepts, formerly ISA-TR99.00.01 • IEC 62351 (TC57, WG15) – Security standards for the power system information infrastructure
ISO	International Organization for Standardization	• Common Criteria for Information Technology Security Evaluation
Australia		
ASD	Australian Signals Directorate Formerly Defence Signals Directorate (DSD)	• Strategies to Mitigate Targeted Cyber Intrusions • ASD Top 35 Mitigation Strategies • ASD Top 4 extending to the Essential 8 • CERT – Industrial Control System Remote Access Protocol
AEMO	Australian Energy Market Operator	• Australian Energy Sector Cyber Security Framework (AESCSF).
TISN	Trusted Information Sharing Network	• Generic SCADA Risk Management Framework For Australian Critical Infrastructure • Risk Management for Industrial Control Systems (ICS) And Supervisory Control Systems (SCADA) Information For Senior Executives • SCADA Security Good Practice Guide - Hardening of SCADA ICT Systems
AGD	Attorney Generals Department	• Critical Infrastructure and Protective Security Policy
	Edith Cowan University Research Online	• Safeguarding Australia from Cyber-terrorism: A Proposed Cyber-terrorism SCADA Risk Framework for Industry Adoption
United States of America		
NERC	North American Electric Reliability Corporation	• NERC-1200 - North American Electric Reliability Corporation Cyber Security Standards • NERC 1300 – Cyber Security o CIP-002 –Critical Cyber Assets o CIP-003 –Security Management Controls o CIP-004 –Personnel and Training o CIP-005 –Electronic Security o CIP-006 –Physical Security o CIP-007 –Systems Security Management o CIP-008 –Incident Reporting & Response Management o CIP-009 –Recovery Plans
NIST	National Institute of Standards and Technology	• SP 800-82, Guide to Industrial Control Systems (ICS) Security • SP 800-77, Guide to IPsec VPNs • SP 800-30, Risk Management Guide for Information Technology Systems • SP 800-40, Creating a Patch and Vulnerability Management Program
SANS	SANS Institute - Escal Institute Of Advanced Technologies, Inc	• Security for Critical Infrastructure SCADA Systems
DOE	U.S Department of Energy	• 21 Steps to Improve Cyber Security of SCADA Networks • Lessons Learned from Cyber Security Assessments of SCADA and Energy Management Systems • The Department of Energy (DOE) developed the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
DHS	U.S. Department of Homeland Security	• Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies • Good Practice Guide: Cyber Security Assessments of Industrial Control Systems
DISA	Defense Information Systems Agency	• The Security Technical Implementation Guides (STIGs)
CIS	Center for Internet Security	• Cyber Security Procurement Language for Control Systems
EEI	Edison Electric Institute	• Patch management strategies for the Electric Sector
United Kingdom		
CPNI	Centre for the Protection of National Infrastructure	• Good Practice Guide on Patch Management • Configuring and Managing Remote Access for Industrial Control Systems • Cyber security assessments of industrial control systems • Process control and SCADA security - General Guidance • Firewall deployment for SCADA and process control networks • Process Control and SCADA Security Guides 1- 7