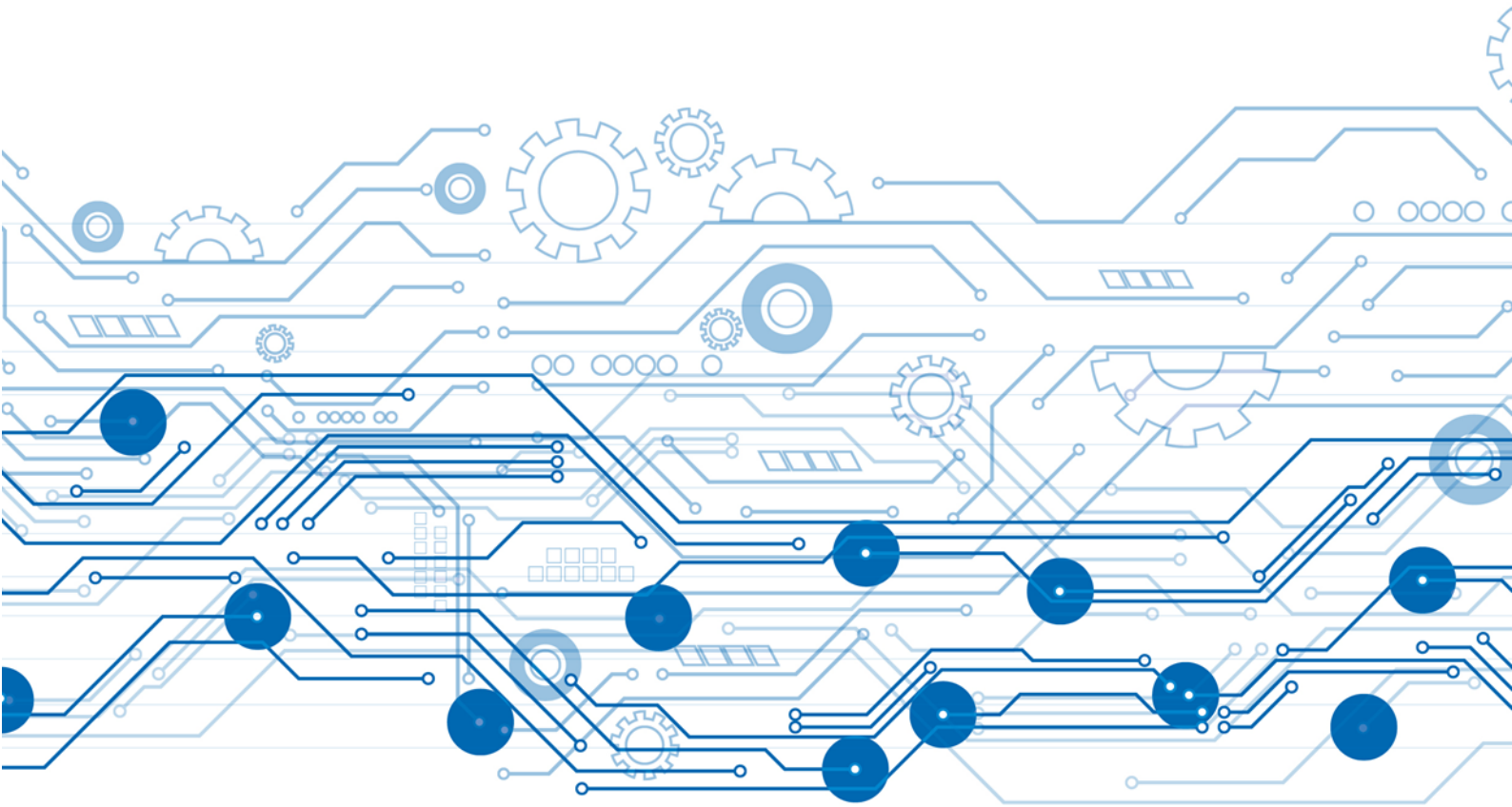
RISSB

RAIL INDUSTRY SAFETY AND STANDARDS BOARD



Rail Cyber Security for Rolling Stock & Train Control Systems

Code of Practice

This Rail Industry Safety and Standards Board (RISSB) product has been developed using input from rail experts from across the Rail Industry. RISSB wishes to acknowledge the positive contribution of all subject matter experts and DG representatives who participated in the development of this product.

The RISSB Development Group for this Code of Practice consisted of representatives from the following organisations:

TfNSW	Advantgard	AQ Advisory
BHP	Rio Tinto	Rail Systems Australia
Aurizon	Koupatech	Sydney Trains
Downer Group	Rail Assurance Consulting	V/Line
Roy Hill	Bombardier	Queensland Rail
Monash University		

Development of this Code of Practice was undertaken in accordance with RISSB's accredited processes. It was approved by the Development Group, endorsed by the Standing Committee, and approved for publication by the RISSB Board.

I commend this Code of Practice to the Australasian rail industry as part of the suite of RISSB products assisting the rail industry to manage rail safety, improve efficiency and achieve safety outcomes through interoperability and harmonisation.

Deborah Spring
Executive Chair | Chief Executive Officer
Rail Industry Safety and Standards Board

Notice to users

The reliance upon or manner of use of this RISSB product is the sole responsibility of the user who is to assess whether it meets their organisation's operational environment and risk profile.

RISSB
RAIL INDUSTRY SAFETY AND STANDARDS BOARD

Keeping codes of practice up-to-date

To maintain their currency, CoP developed by RISSB are periodically reviewed, and new editions published when required. Between editions, amendments can be issued.

It is important that readers assure themselves of that they are using a current RISSB Code of Practice. Information about RISSB Codes of Practice amendments, can be found by visiting www.rissb.com.au.

RISSB welcomes suggestions for improvements and asks readers to notify us immediately of any apparent inaccuracies or ambiguities, please contact us via email at info@rissb.com.au or write to Rail Industry Safety and Standards Board, PO Box 518, Spring Hill, QLD 4004, Australia.

RISSB product can be found at: http://www.rissb.com.au/products/.

Document Control

Identification

Document Title	Version	Date
Rail Cyber Security for Rolling Stock & Train Control Systems – Code of Practice	PC Draft	24 Jan 2020

Document History

Publication Version	Effective date	Page(s) Affected	Reason for and extent of changes
PC Draft	24 Jan 2020		Public Consultation

Approval

Name	Date
Rail Industry Safety and Standards Board	

Copyright

Contents

1 Introduction

1.1 Purpose

The intent of this Code of Practice is to provide principles and practices to address the cyber threat and vulnerabilities associated with rolling stock and train control systems and supporting infrastructures, and provide industry (rail transport operators (RTOs), rail infrastructure managers (RIMs), vendors and third parties) with requirements to assist in the continued progress in the maturity of cyber security risk management.

This Code of Practice (CoP) forms part of the Rail Cyber Security Framework which consists of AS 7770 Rail Cyber Security (Reference A) as well as supporting guidelines (Ref B).

This CoP is designed to support the rail industry in reducing its vulnerability to both deliberate and non-deliberate cyber-attacks. It sets out the principles and general approach to cyber security with specific guidance for rolling stock and train control systems.

1.2 Scope

This document covers rolling stock and train control systems including:

a) rolling stock control systems;
b) rolling stock information systems;
c) rolling stock borne signalling systems.
d) data and voice communication systems;
e) onboard signalling systems;
f) remote conditioning monitoring systems.
g) signalling systems;
h) level crossing monitoring systems; and
i) traffic management systems.

The principles outlined within this CoP can also be generally applied to other rolling stock and train control systems.

The principles outlined within this CoP can also be generally applied to other systems within the infrastructure domain encompassing rail operations and communication systems.

1.3 Terms and definitions

AS 7770 provides definitions of terms which for consistency will be used in this CoP. Descriptions of systems under consideration (SuC) in this CoP are detailed in section 2.

1.4 References

1.4.1 Normative references

The following documents are referred to in the text and have been referred to in such a way that some of their content forms requirements for this CoP:

a) AS 7770 Rail Cyber Security
b) RISSB - Rail Cyber Security - Guideline
c) NIST Special Publication 800-53 (Revision 4) Security and Privacy Controls for Federal Information Systems and Organizations, National Institute of Standards and Technology, Department of Commerce (US), April 2013

All checklists and indexes provided in this document are decision support tools only and do not substitute for good engineering practice.

1.4.2 Informative references

The following are informative references are relevant in supporting the development of this CoP:

a) Rail and Metro Cybersecurity: Where is the industry now? 2019, Cybersecurity Observatory
b) Rail Cyber Security Guidance to Industry, Feb 2016, Department for Transport (UK)
c) Cyber Security Informed Safety Cases for the Rail Industry: Code of Practice, 15 May 2016, Fraser-Nash-Consultancy for UK Department for Transport (UK)
d) Cyber Security Procurement Language for Control Systems, Department for Homeland Security (US), September 2009
e) ISA-62443-1-1 - Models and Concepts, September 2016, ISA. (in ISA-62443 - Security for Industrial Automation and Control Systems, vol. D6E2, no. September 2016, pp. 3–115)
f) CYbersecurity in the RAILway sector (CYRAIL) D2.1 Safety and Security requirements of Rail transport system in multi-stakeholder environments. EU Project 730843 (Cyrail), June 2017.
g) IEC 62443-2-4, Security for industrial automation and control systems, 2015, IEC
h) NIST Cybersecurity Framework for Improving Critical Infrastructure Security Version 1.1,16 April 2018, National Institute of Standards and Technology.

1.5 Audience

This CoP applies primarily to rail transport operators (RTO) and rail infrastructure managers (RIM) as well as the associated suppliers, subcontractors and maintenance contractors. This CoP is designed to provide a consistent approach for the Australian rail industry to help inform, educate and protect their organisations and customers in relation to cyber security risks and their rail safety experience.

This CoP has been written for:

a) implementation by digital systems engineers or security architects who have a detailed knowledge of rail control systems, critical systems design and cyber security; and
b) the information of management and all staff who have responsibility for cyber security.

1.6 Review

This CoP is designed to reflect existing relevant good practices. In this evolving space it is important to be cognisant that the threat landscape (and ability to maintain an appropriate security posture within it) will continue to evolve and it is not possible to capture all good practice at once.

2 Rail cyber security for rolling stock and train control systems

2.1 Section overview

The intent of this section is to set the context for this CoP by identifying the rolling stock and train control systems that are to be considered as well as discussing the threat environment, vulnerabilities and how they might be exploited, and the potential impacts of cyber incidents, both deliberate and accidental.

The first step in setting the context for this CoP is to identify the systems that are being discussed. Rolling stock and train control systems operated in Australia vary significantly across the Australian rail network with many RTOs operating multiple types and generations of rolling stock concurrently. Because of this variety, this CoP should be considered as technology neutral, that is, it is applicable across networks and systems but not linked to specific proprietary technologies. It will be a responsibility of the individual system owners and operators to identify the nuances for specific systems and identify the most effective way in which to apply this CoP.

This Code of Practice applies to new systems being introduced as well as current[1] systems and legacy[2] systems.

SuC in this CoP are identified in the following paragraphs.

2.1.1 Rolling stock control systems

Rolling stock control systems encompass all train borne sub-system components necessary to control the safe operation and movement of the vehicle. In addition, these systems perform the basic set of vehicle control functions required to protect both train crew and passengers whilst journeying through the rail corridor.

Typically rolling stock control systems include:

a) driver/train interface control and driver information systems;
b) conventional driver and train protection systems;
c) traction and brake control systems;
d) battery and auxiliary power systems;
e) door systems;
f) heating, ventilation and air conditioning systems;
g) lighting systems; and

[1] Current Systems are systems that are in operation mid-lifecycle.
[2] Legacy stems are technologically obsolete systems still in operation.

h) "black box" event and data recorder systems.

In the past, rolling stock control systems relied heavily on simple electrical and mechanical componentry to realise this basic level of train operation. However, this technology often referred to as conventional train control is increasing being replaced on modern rollingstock by software running on general-purpose micro-controllers generally distributed throughout the vehicle and interconnected together via train wide communication networks.

Internationally recognised open-standard interfaces are implemented on these train-wide communication networks to ensure information exchange from multiple systems can be intelligently integrated thereby enabling rollingstock control systems to offer increased functional complexity, safety and reliability.

Rolling stock control systems typically provide vehicle operational status information to other rolling stock systems both on and offboard.

2.1.2 Rolling stock information systems

Rolling stock information systems refer to the train borne sub-system components that keep passengers informed, safe and entertained throughout the duration of their trip. These systems can be stand-alone but are typically interfaced with the rolling stock control systems to exchange information about the vehicles operational status in order to enhance functionality.

Modern rolling stock information systems are typically interconnected with off-board central processing systems to provide real-time information exchange between passengers and train operational control to ensure passenger safety and efficient passenger flow across the transit network.

Rolling stock information systems encompass multiple technologies and include:

a) access control systems;
b) public address, emergency intercom and on-board train audio systems;
c) route and timetable information displays;
d) passenger infotainment systems;
e) CCTV surveillance systems;
f) electronic seat reservation;
g) train occupancy and passenger counting systems; and
h) passenger Wi-Fi.

Rolling stock information systems are defined as those systems offering benefits to the train operators and enhancing passenger comfort; these sub-systems differ to rolling stock control systems in that these systems do not provide a vital role in the rollingstock's ability to physically move throughout the rail network.

2.1.3 Data and voice communications systems

Data and voice communication systems refer to equipment installed on-board rolling stock that enables the train crew to establish voice communications between each other, with train crews on other trains, yardmasters or with the train control and operations centre.

This equipment is usually stand-alone but can exchange train operational status information and/or train positional information with other rollingstock on-board systems.

In many railway systems, voice communication is essential for the purposes of safe train operation and control of vehicle movement.

Data and voice communication systems can operate over both private and public communications networks and employ various wireless communication technologies, examples include:

a) train radio;
b) commercial mobile phone and/or cellular communications systems;
c) satellite communications; and
d) Wi-Fi networks.

2.1.4 Onboard signalling systems

Onboard signalling systems comprise all train-borne equipment having a direct interface to the enable the rollingstock to interact with the operators signalling infrastructure.

Onboard signalling equipment helps to ensure the safe movement of the vehicle around the railway network and aids in keeping trains always clear of each other. Equipment may also be fitted on rolling stock which assists in protecting both train and infrastructure. Onboard signalling equipment is usually interfaced with rolling stock control equipment to exchange train operational information; and for the purposes of implementing speed control mechanism in response to offboard signalling system inputs.

Rolling stock onboard signalling systems include:

a) automatic train control (ATC);
b) automatic train operation (ATO);
c) automatic train protection (ATP);
d) European Train Control System (ETCS); and
e) communication based train control (CBTC).

2.1.5 Remote condition monitoring systems

Remote condition monitoring systems (RCMS) obtain vast amounts of data for processing and analysing off-board in order to provide railway operators and maintenance staff with vital information to monitor the performance of rolling stock systems. The onboard systems gather data, and report regularly, requiring two-way communications to report data, and to allow configuration changes. None of the monitoring data is used to directly control the train it is installed on.

Data from RCMS can be used for planning, informing operational practices and maintenance scheduling as well as improving computer simulation models for design of components and work practices. They do not directly interact or control the rolling stock or train but may take signals (e.g. speed) as input.

Advances in rolling stock control systems offer enhanced diagnostic and prognostic capability on-board the train in order to provide visualisation of system performance, issues and suggested corrective actions to assist the driver and train crew in performing their duties.

Together this diagnostic information and performance monitoring data may be seamlessly transmitted to support personnel on the wayside, facilitating remote technical support to the driver, prompting timely maintenance interventions and providing a holistic view of fleet performance to ensure service disruptions may be anticipated and therefore minimised or eliminated.

RCMS used on board rolling stock may either be stand-alone systems configured with their own communications links or integrated into the train-wide communication network to utilise a single point device for off-board data transmission.

RCMS usually comprise a combination of sensors, data loggers, GNSS and controlling computers. Examples of remote monitoring equipment installed on rolling stock include:

a) accelerometers (seismic or piezo-electric transducers) to measure vibrations;
b) roll/ pitch/ yaw sensors;
c) motor current transducers and speed sensors;
d) data recorders and data acquisition systems;
e) internet of things (IoT) sensors;
f) strain gauges on springs and couplers;
g) passenger counting sensors;
h) temperature sensors;
i) fuel and engine management systems; and
j) GPS systems.

2.1.6 Signalling systems

Signalling systems are the safety critical systems responsible for the provision of safe movement authority.

A signalling system provides a means to safely regulate the movement of trains on a railway through the use of appropriate technology. The signalling system is an integral part of a safe working system and employs technical equipment to provide safe and efficient control of the movements of a stated quantity of rail traffic over a given network of track. The safe working system includes operating procedures for train movements should the signalling system fail.

The signalling system refers to the whole of the technology established between the signaller and the train or driver, by which control decisions for the safe and efficient movement of the train through the area of control establish a safe route for the train and are communicated to the train and its driver, and by which the signaller receives information on the state of the track and the location of trains on it.

2.1.7 Level crossing monitoring systems

Level crossing monitoring systems detect and record the condition of a level crossing, typically those fitted with protections and warnings for vehicular and/or pedestrian traffic. This includes traffic booms and/or pedestrian gates, with visible and audible alerts.

Level crossing monitoring systems are deployed to comply with safety integrity requirements, or to support improved maintenance practices.

Remote monitoring of level crossing status and live reporting of failure conditions should be provided with the ability to generate automatic notifications and logging for various critical components of the crossing operation, where it is reasonably practicable to implement a communications link. Typically, level crossing monitoring system also monitor and record: availability of primary power supply, battery voltage, timing and operation of visual and audible alerts, train detection systems and associated circuitry and controls that operate, override or test the level crossing system.

2.1.8 Traffic management systems

'Non-vital' control systems used for the control and scheduling of trains. This may also include passenger information systems and those systems that interface with external 'real time' transport information sources.

2.2 Interfacing systems

2.2.1 General

One of the cyber security challenges facing the Australian rail industry is that systems in use are increasingly open, interoperable and harmonised. The changing nature of technology has seen an increasing convergence between OT and IT and so potential exists for interfaces between critical rolling stock systems with remote train control systems or (for example) systems to enhance passenger experience.

When considering cyber security for rolling stock and train control systems, identification of the system boundary is key. It shall be clearly identified what is considered part of (for example) the rolling stock system and what is external to the rolling stock.

It is essential to then identify the interfaces with external systems (such as train control systems) or other external systems used to control, monitor or communicate with rolling stock systems. Therefore, it is important to maintain an enterprise approach to view your systems holistically including where they interface and the nature of any such interfaces. Once this holistic view has been established, the individual systems should be considered in further detail.

2.2.2 Rolling stock and train control system interfaces

There will be many interfaces between rolling stock systems and train control systems. Defining the boundary between a train control system and rolling stock system will be a decision of individual organisations.

2.2.3 Business system interfaces

Business systems include IT systems used to conduct normal business activities of your organisation. In this context they also include systems used for passenger experience, ticketing systems and passenger access systems. These systems will often be connected to the internet which introduces numerous vulnerabilities.

Business systems are considered out of scope for this CoP however it is essential that the interfaces between business systems and rolling stock and train control systems are identified when considering the holistic view of cyber security. It is essential when considering cyber security for rolling stock to identify where systems that would normally be considered as business systems have interfaces with rolling stock systems. Examples of this include passenger information systems and passenger comfort systems (such as onboard Wi-Fi) and these systems may be considered as an internal part of the rolling stock system boundary.

2.2.4 Third party system interfaces

In some cases, there will be interfaces with third party systems; for example, a rolling stock manufacturer may conduct maintenance by connecting their own diagnostic system into your network. Additionally, the manufacturer can provide its own connection point outside of the operator's control (e.g. 3G connection to on-board equipment). This introduces a vulnerability as the security standards to which the third-party supplier operates are not known and there will be limits to what an RTO/RIM is able to affect. It is important to consider the interfaces with third party systems, understand where these interfaces are and the potential vulnerabilities they introduce.

Means of mitigating risks of interfaces with third-party systems include setting standards and requirements through the design process, implementing standards and security requirements in contracts and through security controls in your own systems and networks and requiring mandatory notification of breaches or events affecting the third-party or their supply chain. Trust should not be assumed.

2.3 Conceptual rail control network

There is a broad scope of SuC each of which should be considered in the context of the potential impact on safety and security so that mitigation controls and prioritisation of resources may be allocated appropriately. To achieve a successful defence-in-depth, the SuC should be segmented into clearly differentiated zones based on specific security requirements. The bigger the potential impact on safety and security, the higher the prioritisation of resources for that system and stronger security controls will be required.

To allow the guidance to be generalised, a conceptual model of a modern rail control system has been developed (Figure 1).[3]

[3] *In this model the term ICS is used to refer to all safety-critical control systems, rather than Rail Control System (RCS), as the NIST Publication uses this terminology. For clarity the RCS is a special-purpose ICS, or ICSoS (Industrial Control System of Systems).*

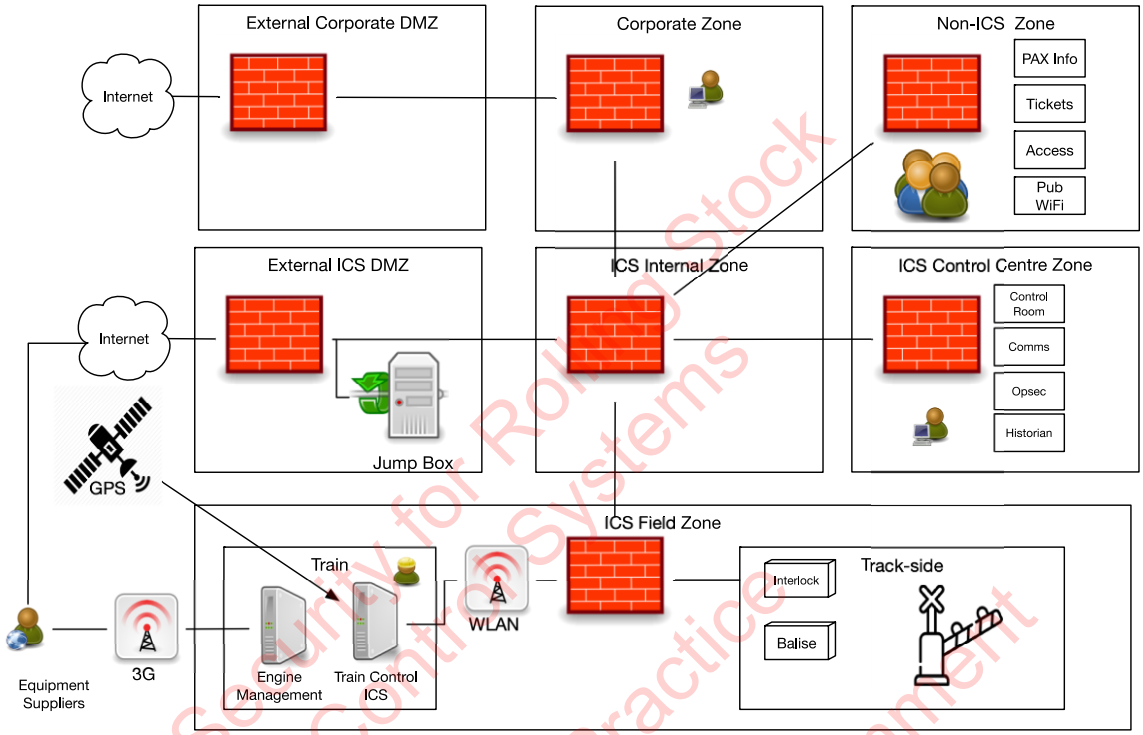


Figure 1 – Conceptual Rail Control System Network

This model is based on a number of specific-purpose network security zones, isolated by firewalls or other network isolation mechanisms, such as data diodes. It assumes that no network is truly physically isolated, because for practical purposes, these networks are accessed for engineering and maintenance purposes making true isolation impractical. The overall design also implements some accepted good-practice, such as network-defence-in-depth and isolation-of-concerns. The model is based on a modern communications-based train control (CBTC) metro-rail system, based on a survey of actual networks in use in Australia by rail operators.

The zones in Figure-1 are described in the following table. IEC 62443 also provides a detailed method of partitioning SuC into zones and conduits.[4]

Zone	Purpose	Considerations
A. External Corporate DMZ	To mediate access to/from the Internet for corporate services.	This zone will have web proxy services, as well as corporate web sites and information services for the public. It is not considered to be within the safety-critical control systems, but delivers services important to the organisation more generally. This appendix does not consider specifically this zone, as it is outside the domain of ICS, however organisations are required to consider risks that connectivity with this zone brings to ICS zone.
B. Corporate Zone	To provide information services to staff of the rail operator,	This zone contains all the regular corporate user desktops, printers and information systems used by the rail operator. Staff in safety-critical functions may have accounts within this corporate zone to

[4] Also see: *Rail and Metro Cybersecurity: Where is the industry now?* https://cyberstartupobservatory.com/rail-cybersecurity-where-is-the-industry-now/

Zone	Purpose	Considerations
	excluding staff using safety-critical systems	access email and corporate services. Significant care should be exercised in providing this access so as not to allow a mechanism for malicious actors to access the safety-critical systems. Better practice is that staff do not use a workstation to access both corporate and safety-critical networks. This appendix does not consider specifically this zone, as it is outside the domain of ICS, however organisations are required to consider risks that connectivity with this zone brings to ICS zone.
C. Non-ICS Zone	To provide information and supporting services to railway users.	There are a range of important but non-ICS systems provided by rail operators to rail users. These include ticketing, public Wi-Fi and passenger information systems. These services need to remain isolated from ICS systems, from each other, and protected from Cyber and cyber-physical attack. For this reason, a zero-trust design is required and assumed for all information systems and devices in this zone.
D. External ICS DMZ Zone	To provide highly mediated access to ICS zone	When external access to ICS systems is required, it needs to be in a safe and controlled manner. Ideally no external access is required, however equipment providers often need on-going access to maintain serviceability and safety of systems. This zone provides a locked-down jump box to facilitate this. It also allows for white-listed data assets to be sent out of the ICS network, to allow remote monitoring and diagnosis.
E. ICS Internal Zone	Provides a central zone that facilitates data flow control and monitoring.	The ICS Internal Zone is the nexus of all of the ICS traffic. All data between zones passes through this zone, allowing monitoring for threats. In this simplified design a common network is used for all types of traffic, although in actual implementation this may be further segmented by type: e.g. control traffic from digital radio.
F. ICS Control Centre Zone	This zone is where central control of ICS systems is done.	This zone contains both the systems and data to do this, and also the operator's workstations and situational displays needed to effect network control.
G. ICS Field Zone	This is an overarching security zone that covers all ICS functions deployed in rolling stock, in stations and trackside	This zone is used to control trains and signalling. In modern Communication-based Train Control Systems, separation of trains is achieved not with physical interlocks but by maintaining a dynamic window of separation using telemetry. For this reason, telemetry and communication security become critical to safe operation.
H. ICS Field Zone - Train	Within the ICS field zone, there are on-train systems that effect train control.	These systems are under the operational control of the Train Driver, or remotely in the case of driverless trains. One area of emerging concern is the presence of direct remote access to engine management and other monitoring systems on trains by Vendors, where these systems share common network infrastructure with ICS systems. While not classified as critical systems, it is a possible weak point for attack.
I. ICS Field Zone – Trackside	This zone includes the network and equipment that is installed along the length of the rail network.	This zone is very important for the safe operation of the railway, and it poses significant challenges to secure. It is very difficult, if not impossible, to physically secure all devices in this zone. For this reason, it is important to have systems that detect tampering and are resilient to device and communication failure.
J. Field Zone – WAN	The WAN connects moving trains to the rest of the ICS field zone.	Communications are essential for telemetry and coordination in a modern CBTC system. These communications shall be immune from communications spoofing and resistant to jamming and Denial-of-service.

2.4 Threats and vulnerabilities

2.4.1 Challenges to rail cyber security

The characteristics of railway infrastructure make them targets for cyber-attacks due to[5]:

a) increased connectivity within both rolling stock and train control systems;
b) a high degree of integration between IT and OT;
c) distributed architecture;
d) long lifecycles of equipment and certification processes. Once a component of the system is certified, it might be obsolete from a cyber security perspective considering the rapidly evolving threat landscape;
e) diversity of supply chain and technology;
f) rail as an industry is typically very safety-orientated and there is a difficulty integrating both cyber security and safety together.

2.4.2 Modes of attack

Cyber systems used on Australian rail networks can be subject to attack through a variety of means, including[6]:

a) remotely, via the Internet or unsecured telecommunications networks;
b) through close access with direct contact with infrastructure (e.g. through a USB port);
c) locally through unauthorised access to physical infrastructure;
d) locally through deliberate misuse by authorised personnel with access to physical infrastructure (insider threat);
e) locally through accidental or negligent actions or behaviour of personnel; and
f) through 3rd parties (including passengers/ customers), as the breadth of technologies, suppliers and interfaces can lead to a lack of cohesiveness in terms of cyber security standards.

2.4.3 Cyber vulnerabilities of rolling stock and train control systems

Vulnerabilities are weaknesses in control systems, information systems, procedures, controls or implementations that can be exploited by a threat actor. Sources of vulnerabilities include[7] :

a) policy and procedure;
b) architecture and design;
c) configuration and maintenance;
d) physical intrusion;
e) communications and networks;
f) increased automation;

[5] Ibid
[6] See: Rail *Cyber Security Guidance to Industry*, Department for Transport (UK), Feb 2016.
[7] Ibid

g) third party/ supply chain interfaces.
h) training and awareness;
i) software development practices;
j) software and firmware defects;
k) legacy/out of support systems.
l) software/technologies introduced into rail networks (are they secure, did they come already compromised from the factory);
m) business information system interfaces;
n) public geolocation and time services e.g. GPS;
o) denial of service conditions e.g. network flooding, interference with radio frequencies;
p) interfaces between different systems and particularly the points where OT and IT converge introduces vulnerabilities;
q) the long Life of Type (LoT) times for systems in use exacerbates existing vulnerabilities with extended periods where new technology and legacy systems are used concurrently, this is of particular concern for rolling stock which has been in service for many years.

2.5 Safety and resilience

AS 7770[8] explains the need to maintain safety and resilience in rail operations during and after an attack. Two essential security goals of rail cyber security are identified:

a) Safety of rail operations shall be maintained so far as is reasonably practical (SFAIRP);
b) Resilience is the ability for the system and services to continue to function during and after a cyber-attack.

The context under which this CoP should be considered is one of safety and resilience. All cyber systems, controls, procedures and practices across the Australian rail network should be designed, initiated, operated and maintained to provide resilience against malicious attack.

Strong emphasis is given to identifying systems and safety impacts formally using safety integrity levels (SIL), and a deliberate bias in controls shall be taken for safety systems in favour of prevention and detection versus remediation and recovery

Measures should be designed to limit the likelihood and impact of both deliberate and non-deliberate attacks in the first instance. For the purposes of this CoP, resilience should be considered to comprise of[9] :

a) reduction of both the consequence and likelihood of attack, through good multi-layered design (defence in depth) and robust operational and maintenance procedures, with consideration given to the defence-in-depth principle, single points of failure and the role of non-cyber related fail safes;
b) capability to detect and respond to potential incidents in a timely manner;

[8] See (Ref A) AS 7770:2018, Section 2.4.
[9] See: *Rail Cyber Security Guidance to Industry*, Department for Transport (UK), Feb 2016 (Ref C).

c) mitigation against disruption and failure once systems come under attack, through development, testing and maintenance of robust contingency and recovery plans;

d) management and monitoring of the effectiveness of systems and procedures, to ensure optimum performance, and early warning of attack;

e) the ability to facilitate investigation by authorities as far as practicable given the need to return the network to normal operation as a priority.

3 Good practice and mitigation

3.1 Overview

The intent of this section is to describe good practice and mitigation strategies that are intended to address threats that could target rail systems in order to prevent or minimise their impact on critical assets and rail operations. This CoP does this by identifying a set of foundational requirements applicable to rail systems.

The requirements identified here are derived from existing standards and frameworks (such as NIST, ISM, ISA/IEC-62443) but this CoP is deliberately not a substitute for other standards and guidance and will not give precise instructions for carrying out security assessments, documenting them, selecting security countermeasures, obtaining security assurances or producing security documents.

This section is supported in further detail by Appendix A which is intended to demonstrate how these requirements may be implemented through a set of baseline controls based on NIST Special Publication 800-53 (Rev 4). Appendix A is an example of one way in which existing publications may be applied. Organisations should utilise controls, counter measures and mitigation strategies that suit their own risk posture, cyber security strategy and business objectives.

There are a number of practices and controls that are applicable to all systems. Train control and rolling stock systems provide an example of where the use of OT can restrict an organisations ability to carry out these good practices as they normally would for IT. This is a good example of where the SFAIRP principle applies. In such cases, an organisation should identify where they need to adapt in order to implement good practices (i.e. through procedural change) or if that is not practicable, identify what alternate controls or practices are in place to mitigate the identified risk.

3.2 Guiding considerations

The following six considerations are intended to provide overarching guidance to establish the context within which this CoP should be considered, they also function as constraints on the CoP provisions themselves[10].

1. **Strategic approach** -This CoP should be considered as part of a comprehensive cyber security risk management system. This CoP takes AS 7770 as the overarching standard and assumes such a comprehensive risk management system is in place.
2. **Do not compromise established methods** - This code of practice is designed to add cyber security considerations to existing Australian rail safety and security regimes. It is

[10] These principles are based on the 9 Principles established in the UKs *Cyber Security Informed Safety Cases for the Rail Industry: Code of Practice*, 15 May 2016, Fraser-Nash-Consultancy for UK Department for Transport

not designed to revise or replace existing standards, procedures, structures or methods. The integration of cyber security presents some challenges to accepted norms within the rail industry and these issues will need to be addressed when faced. However established safety methods, standards and governance structures shall not be compromised.

3. **Consider existing standards** - Applicable industry standards, available good practice and emerging Australian government policy should be considered. There is an increasing range of security best practice guidance available, applicable to both IT and OT (for example ISO/IEC 27001:2013/ NIST SP800 Series).
   Much of the material available is written from an information security perspective and should be carefully interpreted when applied to systems in a safety critical domain such as rail (for example some security techniques to safety critical systems can hinder their operation in an emergency situation). This CoP does not seek to repeat or replace the controls of these existing standards but identifies the good practices under which these existing controls will sit.
4. **Threat context** - This CoP is written in the context of the threat environment. There is a possibility of deliberate, carefully researched attacks against safety-critical systems, attempting to achieve safety-related consequences. This implies the need for a more risk focused approach to its implementation above a compliance focused approach.
5. **System of systems** - The effects of component or subsystem failures shall be assessed for their security and safety impacts on wider railway operations. Therefore, SuC should not be considered in isolation and the knock-on effects of a failure/breach of one system should be considered.
6. **Continual improvement** - The rapidly evolving cyber domain means that nothing should be considered as static. What is considered sufficiently secure today will not necessarily remain so over time as attack vectors change and mitigation strategies evolve. Therefore, as discussed in section 2.5, this CoP is written with the view that the reader seeks to be cyber resilient and not be considered cyber secure and so all procedures, processes and controls shall be continually reviewed, maintained and improved.

3.3 Requirements for cyber security in rolling stock and train control systems

3.3.1 General

Safety and security requirements need to be coherent since both safety risk and security threats may lead to incidents (through deliberate exploitation or accident/ negligence) which can result in serious consequences including damage to equipment, injury to personnel or even loss of life. This should be achieved through a set of foundational requirements for effective cyber security in rolling stock and train control systems and are divided into 8 key areas:

a) Human security.
b) Physical security.
c) Access control.
d) Administration.
e) Data security.

f) Network security.
g) System integrity.
h) Resilience.

3.3.2 Human security

3.3.2.1 Human security general

The human factor is an essential component of a holistic approach to cyber security and it is important that organisations have the human resources to maintain cyber security. *People and process form a significant element of cyber-security controls. Humans are a source of vulnerabilities, in that their knowledge is not complete, and judgement is often imperfect. Attackers use this to gain access to systems.* [11]

For the purpose of this CoP, people are considered in the five primary groups:

a) **Operational staff** – employees involved in the management, maintenance and repair of rail systems.
b) **Users** – employees directly involved in the use of rail systems.
c) **Support staff** – employees that are not directly involved in the use of rail systems but carry out functions in support of rail operations.
d) **Third party administrators** – personnel that are employees of a third-party organisation (i.e. supplier/ vendor/ software developer) that have responsibility for installation or maintenance of rail systems or parts thereof.
e) **Passengers/ customers** – rail users external to the rail organisation that interact with rail systems (such as passenger Wi-Fi and infotainment systems).

3.3.2.2 Human security requirements

The following are requirements for all user groups:

a) **capability and competence** - all personnel should be suitably trained for their roles and responsibilities. Training, education and awareness shall enable all employees to keep up with the rapidly changing threats and risks;
b) **responsibilities** - all personnel should carry out only those tasks that fall within the scope of their official duties, providing such tasks do not violate their established rights of access and do not compromise information security. Access should be limited to only what is required to undertake their responsibilities on a day-to-day basis;
c) **authority** - all personnel should understand the level of his or her authority, the limits of which should be defined in the job description;
d) **duties** - if an employee's official duties change or they are transferred to a different control area, the attributes and means by which they obtain access to the system should be revised. Periodic auditing should be undertaken to assure appropriate privileges are maintained;

[11] (Ref A) AS 7770

e) **vetting** - personnel with privileged (administrative, engineering or technical support) access to systems should be subject to pre-employment screening and periodic background checks;

f) **termination** - on termination of employment, either through the employee's choice or organisational decision, all users have their access rights to the employer's systems revoked and should return all attributes and means associated with relevant systems. Access to information created by the outgoing employee should be provided to other authorised employees in a timely manner;

g) **established procedures** - all personnel shall abide by established policies and not circumvent established procedures;

h) **alterations** - personnel shall not carry out unauthorised alterations to hardware architecture or rail systems software;

i) **approved devices** - personnel shall not use non-approved devices including data storage devices;

j) **approved programs** - personnel shall not run unauthorised programs;

k) acceptable use - personnel should only use approved systems, devices and programs for the intended purpose of that system, device or program and for the execution of their duties and responsibility;

l) **reporting** - personnel should promptly report instances where they believe there has been a compromise to cyber security be it through suspicious activity or personal error. If an employee is responsible for a breach of information security and fails to report this breach to management, or fails to report it in a timely manner, the employee should be identified, and the appropriate disciplinary action taken;

m) **response** - individual users should not search for the cause of any identified or suspected breaches or mistakes themselves nor should they attempt to remove suspicious programs themselves;

n) **third party activity** - all actions carried out by third party personnel in relation to rolling stock systems should be done under the strict supervision of an authorised employee. A record of all actions performed by third party personnel should be documented; and

o) **other actions** - all users shall not carry out any other actions that threaten information security.

3.3.3 Physical security

3.3.3.1 Physical security general

Cyber-attacks and physical attacks are fundamentally different in their nature. However, they are related in that each can facilitate the other. A physical intrusion could allow a cyber attacker into a restricted area to hack into a system. Conversely, a cyber-attack could facilitate access to a restricted area by a physical attacker.

Rail systems may need to be accorded the same level of physical protection as key operational spaces, with security perimeters defined and implemented to protect rail systems and any associated ancillary systems, software or hardware.

Physical and cyber security regimes shall be integrated in order to achieve cyber security objectives.

3.3.3.2 Physical security requirements

It is necessary to have in place physical security which:

(a) prevents unauthorised access to sensitive rail systems, for example:

i. IT equipment accessing, processing or storing sensitive information;

ii. systems utilised to remotely connect to rail systems (i.e. for monitoring/ analytics/ updates);

iii. systems fulfilling safety critical functions; and

iv. security and control systems.

(b) prevents theft of, or damage to:

i. IT equipment, storage media, cables, etc.; and

ii. rail system data, in particular that pertaining to the safe and secure operation of the rail system.

(c) protects the network and communications infrastructure from:

i. accidental damage;

ii. unauthorised access;

iii. deliberate/malicious damage; and

iv. tampering and/or denial of service.

(d) protects utilities, heating, ventilation and cooling systems required to:

i. operate sensitive rail systems;

ii. operate the network and communications infrastructure; and

iii. maintain a safe and secure working environment.

(e) provides accountability for physical access (e.g. record of who entered an area/ accessed equipment and for what purpose).

(f) cabling - cables into buildings and cabinets containing command and control infrastructure need particular protection from physical attacks that might facilitate cyber-attacks i.e. cutting fibre-optic or copper cables and linking them to hardware. You should provide physical security in accordance to cabling;

(g) detect - for track-side control equipment physical security (prevention) is almost impossible, so detection (e.g. tamper detection of enclosures) is essential; and

(h) defence in depth - where it is decided that secure perimeters are needed, these should be designed to prevent unauthorised access or tampering and, depending on the location and criticality. When considering the level and type of protection to be provided, a defence in depth approach is more reliable than a single protective barrier.

3.3.4 Access control

3.3.4.1 Access control general

Access control capabilities are required to reliably identify and authenticate all users (including people, software processes and devices) that are attempting to access systems or assets. The goal of access control is to ensure protection for three of the major principles of information security; confidentiality, integrity and non-repudiation. This may be achieved by protecting the system under consideration from unauthenticated access by verifying the identity of the user seeking access to the system or its components (hardware, data, interfaces).

3.3.4.2 Access control requirements

Access control requirements include:

a) **authorisation** - system owners should create a list of authorised users for each system under consideration. The lists should be built in such a way that each user is uniquely identified and authenticated. Access lists should be securely maintained and reviewed periodically in accordance with organisational policy;

b) **identification** - personnel shall be able to present approved credentials to verify their identity prior to access to the systems being allowed;

c) **authentication** - systems should be protected by authentication methods appropriate to their sensitivity. Effective password policies should be applied across all systems and this should include changing of any default passwords. Multi-factor authentication methods should be used wherever possible;

d) **registration and recording** - every login (logout), operating system loading, initialising or program halt should be registered. Access to sensitive data and use of high-risk transactions/commands should be recorded. Recorded parameters should include date and time of user login (or logout) or system loading (halt), and the results of the login attempt (successful or unsuccessful);

e) **integrity control** - train control systems software should have settings to block unwanted programs from running and unauthorised data storage devices from connecting to the system. Software should not contain software development and debugging tools or tools allowing compiled code modification during information processing;

f) **managing unused interfaces** - where not required for the operation of a system, unused ports should be closed/ disabled and services that are not required should be disabled; and

g) **remote access** - remote access to rolling stock and train control systems, including both access from corporate networks and access from outside the organisation, presents very high cyber security risk and shall be strictly controlled. Rail operators should review and consider adopting all or part of the Australian Cyber Security Centre's Industrial Control Systems Remote Access Protocol (https://www.cyber.gov.au/publications/industrial-control-systems-remote-access-protocol) based on their own risk assessments.

3.3.5 Administration and privilege management

3.3.5.1 Administration and privilege management general

Effective administration/ privilege management is fundamental to ensure data integrity and confidentiality. SuC shall be protected from unauthorised access by verifying that an authenticated user has the necessary privileges to perform the action requested. Actions include reading or writing data/ downloading, updating or deleting files/ accessing restricted networks. This is also referred to as Use Control - the necessary capabilities to enforce assigned privileges of an authenticated user (including people, software processes and devices) to perform the requested action on the system or asset requested and to monitor the use of these privileges[12].

3.3.5.2 Administration requirements

Administration requirements include:

a) **least privilege** - system owners should grant each user (people, software process or device) the necessary privileges to access systems and system component (data, interfaces or networks) and the principle of least privilege should be applied, that is the user should only be given privileges required to complete their assigned task;

b) **privilege restriction** - user privileges could be restricted not only on actions they are trying to perform but also location and date/time. For high-risk privileges, privileges should be granted only when required and then removed. An example of high risk might be Domain Administrator or access to a safety system; and

c) **separation of privilege** - systems should be configured so that they only grant access to resources when more than one condition is met.

3.3.6 Data security

3.3.6.1 Data security general

The confidentiality of data shall be safeguarded to ensure any information type is only made available to those users that are authorised (including people, software processes and devices). Data confidentiality shall be preserved at rest and in transit therefore communications channels and data storage shall have protection against eavesdropping and unauthorised access.

3.3.6.2 Data security requirements

Data at rest requirements include[13] :

a) electronic data storage devices with system and technological software of systems written on them should provide information modification protection to protect information from unauthorised modification or deletion;

b) the procedures for ensuring the protection of data storage devices from unauthorised access should be defined;

[12] "ISA-62443-1-1 - Models and Concepts," in ISA-62443 - Security for Industrial Automation and Control Systems, vol. D6E2, no. September 2016, pp. 3–115

[13] For further detail see Cyrail - http://cyrail.eu/IMG/pdf/cyrail-d21_-_safety_and_security_requirements_of_rail_transport_system.pdf

c) only authorised people should have access to data storage devices. The list of people authorised to access data storage devices should be minimal. People not on the list should never be given access to data storage devices;

d) all removeable data storage devices at the site of systems setup and operation should be registered. Electronic data storage devices should bear labels allowing for their unambiguous identification;

e) the storage locations of data storage devices and their backup copies should be identified. Backup copies should be stored at a separate location to the main storage devices.

f) transporting data storage devices should be controlled to ensure the device remains in hands of authorised people only;

g) data storage devices not intended for future use should be disposed of; and

h) before disposing or transferring an electronic data storage device to be used outside of your systems setup and operation site, such devices should first be sanitised. Steps taken to sanitise the device should be monitored and documented.

Data in transit requirements include:

a) communications should be reliable and encrypted. Internet traffic should use HTTPS or TLS, and for two-way communications such as updating configuration, an encrypted connection such as an IPSEC VPN should be used.

3.3.7 Network security

3.3.7.1 Network security general

Where systems require a network for operation, appropriate measures should be implemented to protect the availability and integrity of that network. This includes the policies and practices to prevent and monitor unauthorised access, misuse, modification or denial and degradation of a network and network accessible resources.

3.3.7.2 Network security requirements

Network security requirements include:

a) **segregation** - physically or electronically segregate on-train networks for passengers from networks used for remote monitoring of rolling stock, train control and railway signalling, particularly where Wi-Fi is used. Vital and non-vital systems should be separated (For example business systems should be separated from systems utilised for train control or signalling);

b) **perimeter protection** - networks should be protected at the perimeter to prevent untrusted and unauthorised system access, to create physical or logical barriers between protected and unprotected networks or to protect individual systems or devices. This may include use of firewalls, VPNs, demilitarised zones (DMZ), content filtering, network address translation, application level gateways and/or application proxies; and

c) **gateway configuration** - for onboard network communications, gateways should be configured to only accept data from known devices (restricting access by encryption, certificates, registered MAC address or similar). Where a system takes data (for

example a speed signal) from rolling stock, the data source and network needs to be restricted to prevent data flowing the other way (for example through isolation by firewalls, permissions or bastion/proxy type services).

3.3.8 System integrity

3.3.8.1 System integrity general

System integrity involves checking the state of the system periodically, monitoring modifications in critical system files by comparing the current state to a baseline state (integrity measurement) and monitoring code executions, such as executables or libraries, in order to detect and avoid system invasions[14].

3.3.8.2 System integrity requirements

System integrity requirements include:

a) **intrusion detection and prevention systems (IDPS)** - tools for detecting and alerting users about information threats to systems accessed remotely should be implemented[15]. A security Information and event management (SIEM) could be used to enable the management of event monitoring and analysis. information on detected intrusions should include;

   i. information on detected network traffic anomalies

   ii. type of detected threats, date and time of threats detection.

   iii. IP addresses of the source and object of the threats.

   iv. port number of the source and object of the threats.

   v. detected threats priority level.

b) **antivirus** - up to date antivirus/ anti-malware should be utilised where available to prevent, detect and remove malicious software (if this is not possible with safety systems, an alternate measure of detection/ isolation should be considered);

c) **patching and updates** - where possible, systems should be patched and updated. Identify and classify all rail systems to determine if they are safety related. All systems that are non-safety systems should be patched and updated. For safety systems, they should be patched and updated where this does not violate the safety case. Identify the current patching and update regime of each system and ensure it is appropriate to maintain configuration with the latest security releases noting that for some systems this could have to be conducted during maintenance cycles. Updates should be restricted to come from specific resources and verified before installation; and

d) **software** - use of unauthorised software should be prohibited. Use of any software obtained through insecure communication channels or via a local computer network should be prohibited. Protection from unauthorised software should include steps to

[14] See http://archive.ibmsystemsmag.com/aix/administrator/security/verify-system-integrity/

[15] Ref H

investigate the causes of unauthorised or altered files being introduced into software applications.

e) **change management** - change management processes should be established to test systems in a realistic test or simulation environment in which changes to the system are verified before putting into production, and which should be used to support security assurance work.

3.3.9 Resilience

3.3.9.1 Resilience general

A resilient system is one that continues or resumes safe operation after an incident. To achieve this security policies, operating procedures, recovery plans and clear communications channels are required to enable effective response to incidents. Incident management capabilities are necessary to respond to security violations by notifying relevant authorities, reporting evidence and taking corrective action in a timely manner.

3.3.9.2 Resilience requirements

Resilience requirements include:

a) **incident management** - measures should be in place for the detection of incidents, analysis, prevention, problem resolution and recovery of systems after incidents;

b) **monitoring** - all cyber security incidents should be monitored and documented on a continual basis;

c) **reporting** - incident reports should be provided to identified recipients according to a prescribed format and reporting frequency;

d) **availability** - measures (and countermeasures) should be in place to guarantee the availability of essential systems and services against degradation and denial. Availability failures (such as power outages/ system upgrades/ hardware failures or denial of service (DoS) attacks) may be prevented using tools or techniques such as redundancy (power, network, hardware), firewall configurations and failover systems[16];

e) **assurance** - periodic testing of availability and security controls, incident management process, and recovery plans should be conducted (e.g. incident simulation, disaster recovery testing or failover testing, control self-assessment and independent assessment, penetration testing.) and;

f) **recovery** - capabilities and services shall be restored to a safe working condition following an attack as soon as possible. Recovery processes shall include:

   i. **recovery plan** – detailed recovery planning shall be conducted and documented. This plan shall include the responses to the most likely and most dangerous courses of action that can affect a system or systems and define and allocate responsibilities;

[16] Ibid

ii. **rehearsal** – the recovery plan should be tested on a regular basis to assess the viability of the recovery plan, identify further gaps and vulnerabilities and ensure responsibilities are known and practised;

iii. **damage assessment** – measures should be in place that enable the analysis of tools utilised by attackers and analysis of monitoring, logging and auditing records in order to determine the systems and resources affected and

iv. **restoration** – the documented and rehearsed recovery plan shall enable the data, systems and services affected by the attack to be restored. Data back-up shall be robust and enable data to be restored in accordance with its priority and in a timely manner.

4 Designing cyber security into rolling stock and train control systems

4.1 Overview

This section discusses designing cyber security in rolling stock and train control systems. It leverages the overarching requirements described in AS 7770 and identifies specific considerations for rolling stock and train control systems. Cyber security is significantly more effective when designed into a system and not bolted on. Security requirements, including cyber security requirements, should be considered from the very start of a design process.

4.2 Principles of effective cyber security design

AS 7770 describes five architecture principles of cyber security control design for RTOs to include in their overall security architecture. These principles provide the overarching guidance for designing cyber security into rolling stock and train control systems[17]:

a) **'If it is not secure, it is not safe'** - states of safety shall be derived from security considerations.

b) **Proportionate response** - measures shall be appropriate to the risk being considered but not hinder controls.

c) **Goal-based security** - establishing goals rather than initiatives ensures more pervasive security and organisational adoption.

d) **Designed-in security** - security should be at every level of design and development and never be a 'bolt on" set of counter measures.

e) **Defence-in-depth** - for each threat there should be multiple independent overlapping controls.

[17] See (Ref A) AS7770:2018, Section 3.1.2

4.3 Cyber security design for train control and rolling stock systems

As part of a product/ system specification, security standards should be defined and stipulate compliance by all entities involved in the design and procurement process.

Mechanisms should be put in place to ensure that security systems are upgraded, updated and maintained throughout their lifecycle. Systems should be disposed of securely to ensure data is effectively deleted and systems still in use should not be compromised.

Five key areas should be considered when procuring new or upgrading existing systems or components[18]:

a) Design.
b) Development.
c) Commissioning of systems.
d) Maintenance.
e) Decommissioning/ disposal.

4.3.1 Design

Systems using modern technologies should be designed with security in mind as an integral part of the system. Security should be considered in every aspect of the system, including specification of requirements, software and application design and the architecture of any communications system.

The design should include a security risk assessment and adequate controls to protect safety and security of people and assets, detect incidents, and enable timely and effective response and recovery. Areas that are likely to be assessed at higher risk include;

a) communications systems;
b) train control and signalling interfaces;
c) power and traction control signalling; and
d) business/corporate systems that interface with rolling stock systems.

Protective measures should enable the system to comply with the requirements for cyber security in rolling stock and train control systems as specified in section 3.3.

Software-defined safety systems should have a comprehensive security assessment and be certified to perform their safety function as expected even in the event of a security incident. Hard-wired safety systems that cannot be compromised or over-ridden should be considered as part of the system architecture where practical.

Confidentiality of system designs should be considered including consideration of how much system design detail should be made publicly available, particularly where there are direct implications for cyber security.

[18] References used to develop this section include *Cyber Security Procurement Language for Control Systems*, Department for Homeland Security (US), September 2009 / *Rail Cyber Security Guidance to Industry*, Department for Transport (UK), Feb 2016 / IEC 62443-2-4, *Security for industrial automation and control systems.*

4.3.2 Development

Recognised secure software development standards exist that should be used when developing software in any environment. Whichever development approach is chosen, it is important to ensure that the following key areas are included:

a) threat modelling / architectural risk analysis;
b) attack surface reduction (the 'attack surface' is the set of interfaces that are exposed to unauthorised users);
c) 'fuzz' testing (using automation to bombard systems with invalid, unexpected, or random inputs to find weaknesses); and
d) static analysis (simplified analysis wherein the effect of an immediate change to a system is calculated without respect to the longer-term response of the system to that change).

A key goal of secure development is to reduce the surface for attack. Effective quality assurance techniques should be considered to ensure that the development of the software is following the secure development process chosen.

Cyber security requirements should be specified in contracts and include the requirement to provide evidence of security features and vulnerabilities in the procured products to clearly define the risk profile of the systems on an individual basis.

The right to audit the development environment and the security of the development, testing, chain of custody and shipping processes should be asserted.

Procurement staff should be sufficiently skilled in cyber security, in order to be able to articulate requirements correctly

4.3.3 Commissioning of systems

Installation of new or upgraded systems, or system components, should not compromise the security already in place. Commissioning of new systems should not increase the attack surface that could be exploited by a threat actor. Commissioning of systems should include:

a) **complete a risk analysis.** A detailed risk analysis shall be conducted to identify any new vulnerabilities that could be introduced as a result of change or integration, the potential impact of any change shall be determined. No changes shall be made without risk analysis and understanding of the impact that they might create from a security angle. The risk analysis shall consider;
    i. changes in threat environment;
    ii. ensuring there is a response plan in place; and
    iii. running exercises to test incident response.
b) **reset/restart mitigations.** Put mitigations in place that allows the equipment to be reset or restarted and returned to previous secure configuration;
c) **malware scanning.** All new equipment and software should be scanned for malware;
d) **suppliers.** The possibility that new equipment and software might contain functionality capable of compromising cyber security should be considered.

Disclosure by the supplier should be required of any functionality in the equipment or software:

i. that allows internet access;

ii. that allows the supplier remote access to the equipment or software, post installation;

iii. that allows the supplier to transmit data to the equipment or that allows the equipment to send data to the supplier;

iv. that allows the supplier to re-program systems;

v. risk based decisions should be made on whether such functions should be enabled and if they are to be enabled, include guaranteed compliance with incoming cyber security standards;

vi. the functionality that should be enabled or disabled in all new equipment and software should be specified in contracts with suppliers;

vii. sources of equipment and software should be considered. Some suppliers have been implicated in facilitating hostile state activity (industrial espionage) through the deliberate supply of infected equipment and software. Some suppliers do not adequately secure their products, allowing non-deliberate infection with malware. Advice from Australian Cyber Security Centre (ACSC) on mitigating the threats posed by suppliers should be sought; and

viii. as a general principle the onus should be put on the supplier to adhere to proscribed security standards or be in breach of contract. However, given the complexity of supply chains, security should not be assumed. RTOs and RIMs should only use products and services from suppliers who are able to provide the appropriate level of assurance, proportionate to the cyber security risk.

e) **conduct testing and evaluation (T&E).** Prior to acceptance into service, thorough T&E should be conducted to ensure the system meets cyber security requirements. Penetration testing is a well-established tool for testing the effectiveness of security systems and should be conducted for all vital systems.

4.3.4 Maintenance

Organisations should keep abreast of new developments in malware and other threats, through engagement with organisations such as the Australian Cyber Security Centre (ACSC).

Systems should be tested on a regular basis for new vulnerabilities or areas that could have become newly vulnerable as a result of a new threat. Planned maintenance schedule should include updating and patching of security software.

Systems should be updated and patched as and when required, fitting this into routine maintenance where it is not possible to patch and update during regular operations and ensuring the safety case of the equipment is not affected.

Systems should be analysed on a regular basis to identify abnormal functioning or indications of suspicious behaviour.

4.3.5 System decommissioning and disposal

Systems should be decommissioned and disposed of securely to limit the possibility of threat actors/ hostile third parties acquiring data or gaining access to systems still in use. Threats may arise from:

a) accidental loss;
b) emergency abandonment (individual, vehicle, facility);
c) espionage (commercial OR state sponsored);
d) insider attack (disgruntled employee (for example)); and
e) theft (from site, vehicle, storage or destruction facility).

Appendix A Application of NIST special publication 800-53 (Rev. 4) to Rail Control Systems

A.1 Background

The US National Institute of Science and Technology (NIST) is the peak laboratory of the Government of the United States of America's Department of Commerce. NIST have taken a leading role in establishing benchmarks and good practice for cyber security of critical infrastructure. Its cyber security framework is increasingly being adopted by critical infrastructure providers within the USA and around the world.

The NIST Special Publication 800-53 (Rev. 4) is a guide to selecting security and privacy controls in government and other organisations. Appendix F is a security control catalogue, that enumerates a normative set of controls that may be considered for implementation within a critical infrastructure provider.

As explained in Section 3.1 of this Code of Practice, the purpose of this appendix (appendix A) is to provide guidance to rail operators who are looking to apply this publication to their rail control systems. In selecting controls to focus on, a 'moderate' baseline has been selected. This is the level most closely aligned to lower-threat critical infrastructure.

A.2 NIST SP800-53 moderate controls

Ref: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Note:

1) The zones described here are referring to the model and zones defined in section 2.3 of the Code of Practice (see Figure 1 and Table 1). Using this model, it is possible to consider the nominal controls, in relation to the logical security zones of a typical railway. Operators may then adjust the recommendation to their particular circumstance.
2) ICS is used to refer to all safety-critical control systems, rather than rail control system (RCS), as the NIST Publication uses this terminology. For clarity the RCS is a special-purpose ICS, or ICSoS (Industrial Control System of Systems.

Control	Description	NW Zones Impacted								Rail-specific guidance
		C	D	E	F	G	H	I	J	
AC-1	Access control policy & procedures	X	X	X	X	X	X	X		The requirement for access control should explicitly address users requiring privileged access. In particular user roles that allow configuration change and operational control of ICS and ICS network zones.
AC-2	Account management	X	X	X	X	X	X	X		Consideration should be given to how common-use logins in control centres will be managed.
AC-3	Access enforcement	X	X	X	X	X	X	X	X	In safety-critical ICS the priority is on safety over confidentiality, however with regards to information that could assist an attacker (e.g. network and ICS design and configuration information), this information should require explicit access on a need-to-know basis to individual user accounts.

Control	Description	NW Zones Impacted								Rail-specific guidance
		C	D	E	F	G	H	I	J	
										In Zone C (Non-ICS) there are specific security and privacy requirements of the users of these services, that will require confidentiality and integrity controls to be implemented.
AC-4	Information flow enforcement	X	X	X	X	X	X	X	X	(See Figure 1 in this code of Practice): • Block all unauthenticated sessions from the Internet to Zone D • Force all sessions from the Internet to terminate in the Jump Box. • Consider use of hardware isolation (data diode) of Zone D and Zone E. • Only accept traffic from the Jump Box Zone D to Zone E • Only allow limited protocols to traverse Zone D and block unauthenticated sessions except where white-listed • Only allow white-listed protocols and authenticated traffic from Zone G to transit zone E
AC-5	Separation of duties	X	X	X	X	X	X	X	X	Deployment of changes should be performed by administrators, not by engineers making the change. Development staff shall not have unsupervised access to ICS systems. Instead use remote desktop sharing. Security operations access should be separated from routine system administration access, and only security operations should be able to modify security logs.
AC-6	Least privilege	X	X	X	X	X	X	X		Devices accessing services should be treated as untrustworthy unless authenticated. Ideally authentication is cryptographic. Services should enforce a least-privilege approach, using a profile of the user or device type.
AC-7	Unsuccessful login attempts	X	X	X	X	X	X	X		This control should be implemented; however, care should be taken so that a hacker may not use this to disable a service or device in a safety-critical ICS.
AC-8	System use notification	X			X					Adapt for local rail operator use e.g. compliance with corporate policies
AC-11	Session lock	X	X							Consider if and where appropriate for your circumstances
AC-12	Session termination	X	X		X					Consider if and where appropriate for your circumstances
AC-14	Permitted actions without ID and authentication	X			X					If common-use logins are in use, positive multi-factor physical access control (e.g. swipe and pin) and video surveillance should be in place, as compensating controls
AC-17	Remote access		X				X			Insecure remote access is a significant risk to ICS. In general, remote access from the Internet should be avoided, and where necessary it should be using an evaluated security solution from a trusted source, exercising least-privilege. This would mean, as a minimum, encrypted VPN with 2FA from a workstation with End-point-protection. Such a

Control	Description	NW Zones Impacted								Rail-specific guidance
		C	D	E	F	G	H	I	J	
										session would have limited access (read only) on assets that are in service. A better model is that all remote access is via a managed remote access solution in Zone D.
AC-18	Wireless access					X	X	X	X	Wireless access needs to be secured to prevent message modification, insertion and denial-of-service. Devices should be authenticated using protocols such as 802.10x.
AC-19	Mobile devices	X				X	X	X	X	Only organisation-owned devices should be used for ICS
AC-20	External information systems	X	X	X	X	X	X	X	X	All access to external information systems from ICS, should be on based a white-list, and subject to a threat & risk assessment. This includes vendor's systems.
AC-21	Information sharing									Unlikely to be relevant to rail operators for ICS data
AT-1	Security awareness & training policy & procedures				X	X		X		Policy should address prioritisation of safety related hazards, and cover training requirements for contractors.
AT-2	Security awareness training				X	X		X		Training should include information on likely threat indicators in ICS context.
AT-3	Role-based security training				X	X		X		Training should be specific to the role of the user, ICS context, and learning-modalities of users, and include information of likely threat indicators.
AT-4	Security training records				X	X		X		
AU-1	Audit & accountability policy & procedures	X	X	X	X	X	X	X	X	Need to align with overall organisational policies.
AU-2	Audit events	X	X	X	X	X	X	X	X	Network and general operating systems security events should be captured. Any security event in the ICS controllers should be captured.
AU-3	Content of audit records	X	X	X	X	X	X	X	X	
AU-4	Audit storage capacity	X	X	X	X	X	X	X	X	Consideration needs to be given to temporary storage of audit record on rolling stock, and later centralisation of audit records.
AU-5	Response to audit processing failures	X	X	X	X	X	X	X	X	Lack of audit records inhibits detection of threats and targeting audit systems is a common mechanism for attackers to avoid detection. Organisation shall have mechanisms to detect and remediate audit failures in systems.
AU-6	Audit review, analysis and reporting	X	X	X	X	X	X	X	X	For critical systems, it is important to have monitoring systems that achieve domain-fusion, giving an integrated view of risk from different domains e.g. control systems and networks, traffic flow and alerts. Regularly testing the power (ability to minimise false-positive and false-negative errors) of these monitoring systems is vital. It is important this information is presented in terms of risk to safety.
AU-7	Audit reduction and report generation	X	X	X	X	X	X	X	X	Audit reporting systems shall be capable of dealing with the significant volume of data generated by ICS systems and OT networks. It should also include protocol-specific analysis to analyse attacks on control systems.

Control	Description	NW Zones Impacted								Rail-specific guidance
		C	D	E	F	G	H	I	J	
AU-8	Time stamps	X	X	X	X	X	X	X	X	Timestamps on log records shall be based on an accurate, reliable and secure time source. Subsystems shall maintain accuracy to within a 100ms of this time source. All time shall be recorded in a consistent time zone – UTC is recommended.
AU-9	Protection of audit information				X					Audit records shall be protected from deletion and modification, by hardware mechanisms. Only privileged security administrators should have access to management of centralised audit databases. Security audit records should be centrally stored, rather than distributed across multiple systems.
AU-11	Audit record retention				X					All audit records should be retained for at least 12 months, and any audit records that have been part of an investigation retained for the maximum period possible, in a format that is portable to new computer hardware and operating systems.
AU-12	Audit generation	X	X	X	X	X	X	X	X	Organisations shall be able to collect and summarise audit info related to an event to facilitate analysis. As attacks are likely to involve both ICS and non-ICS system it is important that this information should be consolidated in a single reporting system.
CA-1	Security assessment and authorisation policy and procedures	X	X	X	X	X	X	X	X	Recommend at least annual review of policy by the board. Recommend at least annual review of procedures by senior executive responsible for OT systems. This may form part of overall security policy & procedures.
CA-2	Security assessments	X	X	X	X	X	X	X	X	Security assessments need to be included in the systems lifecycle. Assessments should be performed by independent assessors, prior to commissioning of systems and periodically through-out its life - the frequency to depend on safety risk. Data for assessments may include: initial or ongoing system authorisations; continuous monitoring; or system development life cycle activities. The overall assessment plan should be adequate to manage risk and approved by the organisation as part of CA-1.
CA-3	System interconnections		X	X			X			All interconnections to ICS zones need to be assessed and authorised before implementation. This requirement should be a contractual obligation of suppliers.
CA-5	Plan of action and milestones	X	X	X	X	X	X	X	X	Allowable time-to-remediate should be based on risk to safety and presence of compensating controls.

Control	Description	NW Zones Impacted								Rail-specific guidance
		C	D	E	F	G	H	I	J	
CA-6	Security authorisation	X	X	X	X	X	X	X	X	It is recommended that this requirement be integrated with general approach to approving systems to operate used in Rail.
CA-7	Continuous monitoring	X	X	X	X	X	X	X	X	Metrics to monitor should be defined as part of system design. Assessments should be on a schedule that reflects risk and be performed by staff independent of the organisational function designing or running the ICS system. Records of the monitoring and assessment program should be centrally maintained, in consistent formats.
CA-9	Internal system connections	X	X	X	X	X	X	X	X	All connections between critical-system components and networks shall be documented and approved, as part of change-control procedures.
CM-1	Change control policy & procedures	X	X	X	X	X	X	X	X	Ensure that there is an integrated policy covering change. Avoid having separate IT and OT policies and procedures in converged or interconnected systems.
CM-2	Baseline configuration	X				X	X	X	X	Minimise variation in configuration of component systems and maintain documented baselines for these. Maintain history of baselines and link change records to standard baseline identifiers.
CM-3	Configuration change control	X	X	X	X	X	X	X	X	
CM-4	Security impact analysis	X	X	X	X	X	X	X	X	A risk-based triage may be used to identify change that required a full impact analysis. Analysis shall be conducted by persons skilled security assessment and knowledgeable about the rail systems under review. Results should include an assessment of a risk to safety.
CM-5	Access restrictions for change	X	X	X	X	X	X	X	X	Changes need to be by approved persons, documented in change records, and supervised by the organisation where this is done by an external party.
CM-6	Configuration settings	X	X	X	X	X	X	X	X	Once the minimum-access is determined for a component, this should be documented and enforced across all instances of this component. Avoid changes to configuration in operating rolling stock.
CM-7	Least functionality	X	X	X	X	X	X	X	X	Where possible use process white listing to enforce least functionality. Deactivate ports/services that are not required for production operation.
CM-8	Information system component inventory	X	X	X	X	X	X	X	X	It is important to maintain these inventories on any safety-critical component. In workstations use end-point protection to detect unauthorised components.

Control	Description	NW Zones Impacted								Rail-specific guidance
		C	D	E	F	G	H	I	J	
CM-9	Configuration management plan	X	X	X	X	X	X	X	X	All rail control systems components, sensors, supporting communications networks and IT services and all gateways should be within the scope of the configuration management plan.
CM-10	Software usage restrictions	X	X	X	X	X	X	X	X	These security zones should only run applications that are approved and licensed by the organisation.
CM-11	User installed software	X	X	X	X	X	X	X	X	Users should not have the ability to install applications on workstations or control systems.
CP-1	Contingency planning policy and procedures	X	X	X	X	X	X	X	X	May be described as a continuity plan or a disaster recovery plan.
CP-2	Contingency plan	X	X	X	X	X	X	X	X	Contingency plans should be in place to ensure continuity of core services under cyber or physical attack, that might include denial-of-service attacks. Consideration needs to be given to the required recovery time for services, particularly allowing for the process of recommissioning compromised devices and systems.
CP-3	Contingency training	X			X		X	X	X	Training of operational staff needs to be part of contingency training.
CP-4	Contingency plan testing	X			X		X	X	X	Testing should include operational staff and include low-probability high-impact cyber-physical attack scenarios. Ensure testing considers peak commuter loads and issues such as maximum time manual fail-safe procedures may be used. In testing of networks, include network service failure within the scope of the testing e.g. name servers, time servers, access-control server.
CP-6	Alternate site storage				X					Consideration should be given to backup storage for control centre and core data logging services.
CP-7	Alternate processing site				X					It is important that alternate data centre and alternate control centre scenarios are considered. Ensure that the time to restore service aligns with community expectations.
CP-8	Telecommunications services	X	X	X	X	X	X	X	X	Critical operations, and other services required to maintain normal operations within a 24-hour period, shall be interconnected by redundant telecommunications services, with divergent paths, technologies and suppliers. Where an active routing design is employed, network monitoring should report on traffic flow and alarm on link failure.
CP-9	Information systems backup	X	X	X	X	X	X	X	X	The backup of information systems needs to include operational systems that record alerts and monitoring data, and all static configurational information. This includes the operating software, licenses and configurations of each device on the network. Snapshots of these should be included in release procedures. This allows a rapid recovery from failure or attack, without the need to manually

Control	Description	NW Zones Impacted								Rail-specific guidance
		C	D	E	F	G	H	I	J	
										reconfigure devices after a restore from a gold master.
CP-10	Information system recovery and reconstitution	X	X	X	X	X	X	X	X	Recovery to an operating state to allow return to operations in a safe and secure manner within the target timeframe is essential. As a secondary consideration a recovery point objective may be needed to ensure attackers do not evade detection or render changes to configurations lost. In an ICS system transaction recovery may be less relevant.
IA-1	Identification and authentication policy and procedures	X	X	X	X	X	X	X	X	The organisation needs a policy that identifies who needs to be identified, and the level and type of identification credentials that are acceptable. The organisation should consider compliance with state, federal or contractual requirements for staff identification.
IA-2	Identification and authentication (organisational users)	X	X	X	X	X	X	X	X	Consideration should be given to how to integrate physical and system access, particularly to operational control systems (control room or rolling stock). If feasible it is preferable to manage identification and access at an individual level using Role-based access control, rather than group logins. If group logins are used, then use of a RFID ID as a secondary factor should be considered.
IA-3	Device identification and authentication	X	X	X	X	X	X	X	X	All devices should be authenticated before they may connect to the network, using protocols such as 802.10. If this is not possible, a compensating control of MAC address white-listing and rogue MAC address scanning should be implemented.
IA-4	Identifier management	X	X	X	X	X	X	X	X	
IA-5	Authenticator management	X	X	X	X	X	X	X	X	IA-5 (1)(a) – refer NIST Special Publication 800-63B. The updated guidance is counter to the long-held philosophy that passwords should be long and complex. In contrast, the new guidelines recommend that passwords should be "easy to remember" but "hard to guess.". In adopting this guidance, privileged users and remote-access users (from outside the operational network) should meet Authenticator Assurance Level 2, and all other users should meet Authenticator Assurance Level 1, as a minimum.
IA-6	Authenticator feedback		X							Organisations may use a compensating control of remote user policy and education to prevent shoulder-surfing. Most operational users access systems from physically controlled environments where this is of minimal risk.
IA-7	Cryptographic module authentication									Where a cryptographic module (hardware security module) or trusted time source is required for correct and secure operation, the devices should be

Control	Description	NW Zones Impacted								Rail-specific guidance
		C	D	E	F	G	H	I	J	
										operated in accordance with manufacturer's policies and procedures.
IA-8	Identification and authentication (non-organisational users)									As a general rule, guest or visitor access to controlled spaces and networks should not be allowed without a staff escort. Where this is required for operational reasons, this control may be applied.
IR-1	Incident response policy and procedures	X	X	X	X	X	X	X	X	It is important that an IR policy and procedures integrates the cyber and operational control organisational elements, and needs to interface with corporate crisis management plans
IR-2	Incident response training	X	X	X	X	X	X	X	X	All staff who are involved in managing an incident need to be trained in the incident response process. This includes senior operations staff.
IR-3	Incident response testing	X	X	X	X	X	X	X	X	It is important that realistic testing of incident response is carried out and involves all parts of the organisation who would be required to response to a real incident. It is recommended that these exercises are facilitated.
IR-4	Incident handling	X	X	X	X	X	X	X	X	Consideration should be given to the physical dimension and impacts of cyber-attack, the challenges of obtaining situational awareness of the issues, and how safety is balanced with preservation of evidence and restoration of service. Consideration should be given to systems to support the incident handling process.
IR-5	Incident monitoring	X	X	X	X	X	X	X	X	
IR-6	Incident reporting	X	X	X	X	X	X	X	X	Reporting is required both internally within the organisation, ONRSR and CERT Australia. It can also require reporting to state-based agencies. Reporting within the organisation should be at a communicated cadence while the incident is in progress and should include: a factual statement of the incident at the point of time, the impact of the incident, and the actions being taken. It should avoid supposition as to actors, their motivations, or state of the network. It should be in plain language understandable by a non-cyber security and non-IT expert. After the event an incident report will provide a more comprehensive analysis of the incident, including causes and lessons learnt.
IR-7	Incident response assistance	X	X	X	X	X	X	X	X	Pre-planning of incident response should include ensuring access to internal and external expertise required to identify the attacker and attack, capture forensic information, and mitigate and restore services. Consideration should be given to how vendor contract and interorganisational MOU enable this to occur. These experts should also be involved in at-

Control	Description	NW Zones Impacted								Rail-specific guidance
		C	D	E	F	G	H	I	J	
										least some of the incident response training and testing.
IR-8	Incident response plan									Incident response plans need to integrate with other organisational plans, such as emergency response plans, crisis management plans, business-continuity plans and general operating procedures of the railway. This is because of the cyber-physical nature of these control systems, and the potential for the cyber to impact the physical and the physical to impact the cyber.
MA-1	System maintenance policy and procedures	X	X	X	X	X	X	X	X	AS 7770 requires all systems to have a maintenance and sustainment plan that addresses security throughout the operational life of the system.
MA-2	Controlled maintenance	X	X	X	X	X	X	X	X	Sanitisation is less of a concern in control systems; however, care should be taken to ensure detailed configuration information is not accidently leaked to hackers.
MA-3	Maintenance tools	X	X	X	X	X	X	X	X	Plugging in external drives or system engineer's laptop computers has the real potential to introduce malware into critical systems. For this reason, such practices should be strictly regulated and technical controls in place on all parts of the supply chain where an attack could originate.
MA-4	Non-local maintenance	X	X	X	X	X	X	X	X	Refer remote access requirements. Weak remote access represents a real and significant threat of ICS.
MA-5	Maintenance personnel	X	X	X	X	X	X	X	X	Social engineering is a common method of gaining access to systems. This control, along with PE-2, reduces the risk that a hacker will gain access to privileged systems and cause damage. A key area of weakness in rail are the track-side systems, where physical access is more easily obtained. In this zone logical authentication and access controls, and detection of unauthorised access attempts, reduce this risk.
MA-6	Timely maintenance	X	X	X	X	X	X	X	X	Managing preventative maintenance and the programmed replacement of components is essential. In particular, continuing to operate systems that are not receiving security updates from manufacturers need to be replaced well in advance of these dates. All systems should inventory their commercial components and the CI databases should track product and version to allow this risk to be managed in a systematic way.
MP-1, MP-2, MP-3, MP-4, MP-5, MP-6	Media protection									In general, there is relatively little confidential information in ICS systems, other than detailed configuration information. Ticketing systems and customer systems will contain significant PII information, however. Even convenience service such as Public Wi-Fi may contain significant sensitive information. The organisation should develop an information classification and release-ability policy that addresses these different information asset classes

Control	Description	NW Zones Impacted								Rail-specific guidance
		C	D	E	F	G	H	I	J	
										and applies the media protection family of controls on this basis.
PE-1	Physical and environmental protection policy and procedures	X	X	X	X	X	X	X	X	Physical access to control centres, network distribution rooms/closets, and track-side equipment are significant considerations for Rail operators. In addition, cross-jurisdictional and cross-organisational issues may make it difficult to set clear policy. Clear and consistent policy on physical access may reduce this risk.
PE-2	Physical access authorisations	X	X	X	X	X	X	X	X	Photo ID with RFID chips should be considered minimum standard. Photo ID should clearly indicate the type of areas that are authorised for access, using a colour and code system.
PE-3	Physical access control	X	X	X	X	X	X	X	X	Doors with electronic locks with RFID strike and PIN should be used to restrict access to building and control rooms. Non-duplicable keys, remote-controlled egress/tamper alarms and CCTV monitoring should be used track-side areas and equipment.
PE-4	Access control for transmission medium	X	X	X	X	X	X	X	X	All communications equipment should be in locked closets or cabinets. Where located in a public area these should be physically resistant to vandalisation. Communications lines external to buildings and accessible to the public should be in conduit that protects the cable from physical damage and access.
PE-5	Access control for output devices									This control is rarely required for rail.
PE-6	Monitoring physical access				X	X	X	X	X	CCTV and remote alarm monitoring, combined with maintenance scheduling and security alert monitoring, provides a means of detecting unauthorised physical access to remote locations.
PE-8	Visitor access records				X					Visitors to the control centre should sign in/out of the building.
PE-9, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-16	Physical environment controls				X					The control centre and data centres supporting it will require a risk assessment to determine the level of physical and environment controls and redundancy required. As general guidance, a government-rated unclassified data centre will have sufficient controls to host these types of systems.
PR-17	Alternate work site				X	X	X	X	X	An alternative site for the control centre, or having multiple control centres geographically separated, should be considered as part of contingency planning. Consideration should also be given to having sufficient remote access capability to allow systems engineering and other support staff to work from home (or a remote office) in a disaster.
PL-1, PL-2, PL-8	Security plans and architecture	X	X	X	X	X	X	X	X	A documented security architecture and plan should be considered mandatory for critical infrastructure and should be in-place prior to commissioning. It should be periodically updated to reflect change.

Control	Description	NW Zones Impacted								Rail-specific guidance
		C	D	E	F	G	H	I	J	
PL-4	Rules of behaviour	X			X	X	X	X	X	Rules of behaviour ('acceptable use') policies address the human aspect of security. Implement practical and pragmatic policies that minimise risk and compliance burden on staff. Ensure it covers all users of systems, not just office staff. Integrate training on this policy with awareness training.
PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8	Personnel security				X	X	X	X	X	Employment processes should include police and background checks for personnel who will have privileged systems access. Personnel risk assessment and reporting should be in place to detect at-risk staff in these positions. Contracts with external parties should include controls to allow management of personnel risk e.g. cleaners, electrical contractors, IT/OT contractors.
RA-1	Risk assessment policy & procedures	X	X	X	X	X	X	X	X	AS7770 requires a formal risk-assessment and approval process to be in place. This is addressed in the body of this Code of Practice.
RA-2	Security categorisation				X	X	X	X	X	All rail systems will be unclassified; however, this control should be adapted to classify safety-critical and non-safety critical systems and networks. Use of the SIL concept in IEC 62443 is recommended for this.
RA-5	Vulnerability scanning	X	X	X	X	X	X	X	X	Vulnerability scanning, including of ICS systems, is highly recommended. The process shall be done in such a way as to not jeopardise safety. For example, scanning of rolling stock systems to be performed only when a unit is not operational. For this reason, automation tools, that include fail-safes to prevent such events shall be used. Accurate systems documentation is required to make this possible. If isolation of operating stock is not possible, then a control group of non-running stock should be used. A partial compensating control would be to use passive detection of intruders using IDS.
SA-1, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-11	System and services acquisition	X	X	X	X	X	X	X	X	This is dealt with at some length in AS7770, its implementation guideline and the main body of this code-of-practice.
SC-2	Application partitioning				X	X	X	X	X	Admin & Engineering interfaces in ICS environments should be separate from user interfaces at an application and network level e.g. the application that is used by despatchers should not be the same application that IT personnel use to configure the despatch system; as the driver of a train should not be able to enter maintenance mode of the train control system using their control panel.

Control	Description	NW Zones Impacted								Rail-specific guidance
		C	D	E	F	G	H	I	J	
SC-4	Information in shared resources	X			X	X	X	X	X	In services used by the general public, this is an essential control. Designers should be aware that this class of vulnerabilities is frequently used to escalate privilege in systems.
SC-5	Denial of service protection				X	X	X	X	X	Denial of service is very important to address in the design of ICS, in particular in CBTC. Communications systems should have sufficient bandwidth and DoS controls to withstand DoS attacks and continue operation, without triggering fail-safes.
SC-7	Boundary protection	X	X	X	X	X	X	X	X	Operators shall implement boundary protection, as part of a defence-in-depth strategy. This shall include network zoning, firewalls, jump-boxes in DMZs, 2FA for external or privileged access, Intrusion detection. They may also implement data diodes to create physical isolation of network zones. Egress of data from ICS is generally not a significant risk in rail and may be managed by white listing.
SC-8	Transmission confidentiality and integrity	X	X	X	X	X	X	X	X	Transmission integrity, non-repudiation and non-impersonation is essential. Cryptographic methods are well suited to this. Confidentiality is more relevant to customer services in Zone C. Confidentially via encryption could, however, make reconnaissance more difficult for attackers, but it also makes detection of attack more difficult for defenders. In balance designers should consider carefully before using channel encryption of network traffic broadly in the ICS system, as it can increase costs and reduce performance and the security profile of the network.
SC-10	Network disconnect	X	X							Only relevant for public access and remote access.
SC-12, SC-13	Cryptographic management									Use approved algorithms, protocol and systems. Manage keys in accordance with approved procedures.
SC-15	Collaborative computing devices	X			X					Use of remotely managed devices may introduce security risks to your organisation, so should be assessed before being connected to your network.
SC-17	Public key infrastructure certificates	X	X	X	X	X	X	X	X	Only approved certificate authorities should be trusted. Avoid use of self-signed certificates in devices or systems.
SC-18	Mobile code				X	X	X	X	X	Mobile code should be avoided where possible in ICS systems and networks. ICS systems should be configured to only run signed executable code.
SC-19	Voice over internet protocol			X	X	X	X	X	X	Voice-over-IP (VoIP) and Radio-over-IP (RoIP) are valuable capabilities for rail. They should, however, be run over separate subnets and interfaces than control and sensor traffic. This is because of the history of security vulnerabilities with these protocols.

Control	Description	NW Zones Impacted								Rail-specific guidance
		C	D	E	F	G	H	I	J	
SC-20, SC-21, SC-22	Secure name / address resolution	X	X	X	X	X	X	X	X	
SC-23	Session authenticity	X	X			X	X	X	X	Mutual authentication of secure sessions is significant and help prevent man-in-the-middle attacks against ICS systems. This is particularly important in code deployment and configuration management systems.
SC-28	Protection of information at rest				X	X	X	X	X	Protection of configuration and logging information is important.
SC-39	Process isolation				X	X	X	X	X	Internal process isolation in hardware (SC-39(1)) and the use of secure computer platforms in ICS controllers is highly recommended. Such a secure platform should include services providing cryptography, communications and operational security (e.g. Host IDS).
SI-2	Flaw remediation	X			X		X	X	X	Flaw remediation is an essential process in managing the security lifecycle of an operating platform. As the platforms age this becomes more difficult, nevertheless, as is stated in AS 7770, if it's not secure, it's not safe. It is important to have a clear policy and management visibly of the current state of flaw detection and remediation with the organisation.
SI-3	Malicious code protection	X	X	X	X	X	X	X	X	The most common technical mechanism used to gain access to secure networks is via targeted malware. Therefore, all points where data is introduced into the ICS network need to include malware scanning and block encrypted data that may not be inspected. In addition, remote access should only be allowed from workstations running end-point-protection. Many VPN clients allow the security of the remote workstation to validated before a VPN connection is granted. Avoid organisation-to-organisation VPN connections or unmanaged remote access, unless the security of these organisations may be independently assured. In ICS devices use of white-listed applications (i.e. a default deny policy) and network services is preferable to running malware detection software.
SI-4	Information system monitoring	X	X	X	X	X	X	X	X	At some point network protection will fail, at which point detection is essential. ICS networks should be designed to include system monitoring and intrusion detection, with care taken to minimise false-positives and false-negatives. This is achieved by strong configuration management and white listing of known services and activities.
SI-5	Security alerts, advisories, and directives	X	X	X	X	X	X	X	X	Alerts from partners, manufacturers and computer emergency response teams (CERTs) need to be received and triaged. Similarly alerts raised by your security operations team need to be shared internally and externally to relevant parties. Consider information sharing initiatives at a sectoral and supply-chain level.

Control	Description	NW Zones Impacted								Rail-specific guidance
		C	D	E	F	G	H	I	J	
SI-7	Software, firmware, and information integrity	X	X	X	X	X	X	X	X	All ICS systems shall perform a security integrity check on start-up and periodically (as defined). This verifies that the device/system is operating in a state of integrity. This may include checksum verification of operational parameters and software.
SI-8	Spam protection	X								Community systems such as public Wi-Fi should include protection of users from locally generated SPAM
SI-10	Information input validation	X			X	X	X	X	X	
SI-11	Error handling	X			X	X	X	X	X	
SI-12	Information handling and retention				X		X	X		Not in general a significant concern for rail control systems, except when the data forms part of forensic investigations. In this case, specific steps shall be taken to preserve this data. Preservation of system configuration data for several years may assist in investigating reliability and security issues.
SI-16	Memory protection	X	X	X	X	X	X	X	X	

RISSB

RAIL INDUSTRY SAFETY AND STANDARDS BOARD

ABN 58 105 001 465

For information regarding s product developed by RISSB contact:
Rail Industry Safety and Standards Board

Brisbane Office
Level 4, 15 Astor Terrace
Brisbane, QLD, 4000

Melbourne Office
Level 4, 580 Collins Street,
Melbourne, Vic, 3000

PO Box 518
Spring Hill, QLD, 4004

T +61 7 3724 0000
E Info@rissb.com.au