RISSB
RAIL INDUSTRY SAFETY AND STANDARDS BOARD
ABN: 58 105 001 465

RISSB Product Proposal (and Prioritisation)

Primary information

Type of product being suggested:	Guideline
Title of product being suggested:	AS.7770 Rail Cyber Security Reference Architecture
Date of suggestion:	February 2019
Reason for suggestion:	The Rail Cyber Security Implementation Guideline (already under development) is focussed on the management implications and the process through which organisations need to proceed in order to adopt / become compliant with the standard AS.7770. The implementation guideline is under development by a DG at the time of writing. Members of the DG have noted that a “best practice / reference architecture” would be valuable to provide guidance to a technical audience on the design and implementation of cyber security systems that contribute to the mitigation of cyber risks across both IT and OT domains.
Railway discipline area:	Safety

Objective:

1. To provide a common reference architecture for cyber security system planners and managers so that best practices that align to AS.7770 can be adopted when implementing technologies in the IT and OT domains.
2. Provide a common reference model for collaboration between Rail organisations in their discussion on design, implementation and effectiveness of cyber security technologies in both IT and OT domains.

Scope:

Cyber Security Reference Architecture comprising:

- IT and OT technologies – the commonalities and differences, using an OSI (or similar) taxonomy addressing each of the applicable layers: Physical (inc EM), Data-Link, Network, Transport, Session, Presentation, Application
- Examples and or catalogues of typical technologies used (overall and within layers)
- A conceptual architecture illustrating:
  - A model implementation including specific highlighting of key interfaces and management / control boundaries between traditionally IT and OT technologies
  - A model deployment of cyber security technologies at interfaces, boundaries, between layers and systematically
  - The key cyber technology components required in the model for prevention, detection and response to cyber threats.

Hazard identification:

1	Failure to effectively implement controls results in vulnerabilities that allow	6	Failure to embed cyber security concerns in the systems lifecycle results in a reliance on compensating controls, an unmaintainable security

	attackers to successfully compromise systems.		profile for the life of the system, and system vulnerabilities that can be exploited by attackers.
2	Failure to ensure supply chain partners effectively implement controls provides a vector for attackers to successfully compromise systems.	7	
3	Failure to protect rail control systems from other systems allows attackers to compromise safety.	8	
4	Failure to design resilience to cyber-attack into systems results in routine attacks disabling services.	9	
5	Lack of good security architecture results in poor investment of cyber security budget, resulting in a weak security posture.	10	

Definitions

i A ***Guideline*** is a set of informative guidance. It is not normative but informative.

A ***Code of Practice*** is a set of descriptions. It is the “how” one can meet a higher-level requirement (either of a Standard, or a piece of Legislation). It is normative, but by its nature can contain several options about how to achieve compliance with the higher-level requirement. It can also have some informative guidance within it if it is more practical than writing a separate guideline.

A ***Standard*** is a set of requirements only. It is the “what” must be done to be claim compliance to the standard. It is normative. It can also contain optional and/or supplementary requirements, but they still should be worded as requirements.

Benefits:

Safety

Rail cyber-attack has the potential to result in any of the following outcomes:

- Loss of life.
- Serious injury to passengers and staff.
- Other threats to safety, including injury.
- Disruption to network operations.
- Economic loss to operators, suppliers and the wider Australian community.
- Reputational damage to rail organisations and government.
- Loss of and /or corruption of commercial, sensitive and operational information.
- Physical damage to infrastructure.

Ensuring that rail systems are protected from/and are resilient to cyber-attacks provides assurance to rail transport operators, customers and the community.

Interoperability / harmonisation

This product which will support the national standard (AS7770) will provide a model / reference architecture which will specifically assist system interoperability (and security thereof)

Financial

The cost of a major cyber-attack on the national rail network would eventuate in a high cost on the Australian economy whether it be delays to peak metro services. port or transportation of goods. Innovation and technology will continue to evolve and be taken on in rail and therefore the investment need to be protected.

Environmental

Potential of rail incidents specifically involving dangerous goods and bulk commodities.

Impacts:

Minimal impacts as this would be supporting AS7770.

Reference / source materials:

#	Reference / source material	Available from
1	AS7770 Rail Cyber Security Standard	RISSB
2		
3		
4		
5		

Definitions

ii ***Interoperability*** is the ability of a process, system or a product to work with other process, systems or products (aka compatible systems through managed interfaces).
iii ***Harmonisation*** - the act of bringing into agreement so as to work effectively together (aka uniformity of systems).