

# RISSB Product Proposal (and Prioritisation)

Primary information	
Type of product being suggested:	Code of Practice
Title of product being suggested:	System Safety Assurance for Australian Rail Industry
Date of suggestion:	14/2/19
Reason for suggestion:	<p>The Australian Rail Industry lacks a dedicated code of practice to provide a “best practice” baseline for managing System Safety across the lifecycle of new or modified assets.</p> <p>Due to the lack of such a baseline there is wide variety in the approach and standard of System Safety programs and evidence resulting in high cost and time commitments both in development and assurance of rail assets. Further, this lack of consistency may lead to lower quality of System Safety programs and assurance placing additional risk to rail employees and the public.</p>
Railway discipline area:	Safety
Objective:	
<p>Provide a clear “best practice” baseline for System Safety programs that addresses Australian legislative requirements and is readily scalable for the scope of rail projects undertaken within Australia. This code of practice should provide a detailed outline of how to manage System Safety of new or modified rail assets integrated into the rail network.</p> <p>This code of practice should provide detailed processes which outline safety-related activities and deliverables to ensure safety, SO far As Is reasonably Practicable (SFAIRP), throughout the asset lifecycle from design, commissioning, operation, maintenance and disposal.</p>	
Scope:	
<p>The System Safety Assurance code of practice is to describe how safety-related risks may be identified and eliminated or minimised SFAIRP throughout the design, commissioning, operation, maintenance and disposal of rail assets including rollingstock, track and supporting infrastructure. Further, this code of practice should provide guidance on the evidence required to provide an effective Safety Argument in support of State endorsement of any change to the rail network.</p> <p>The code of practice is to outline how developers may:</p> <ul style="list-style-type: none"> <li>- Assess criticality of new or modified assets and identify key risks associated with any change to a transport network;</li> <li>- Integrate the System Safety program with Systems Engineering effort ensuring sufficient assurance is provided throughout the engineering lifecycle to support design development and commencement of operation;</li> <li>- Undertake hazard identification, assessment, management and approval process in a consistent and documented manner;</li> <li>- Propose and implement hazard controls;</li> <li>- Identify and manage Safety Related Application Conditions (SRACs)</li> <li>- Develop and manage hazard logs and operational risk registers to track and manage safety-related risks; and</li> <li>- Develop of deliverables to provide a sufficient Safety Argument.</li> </ul>	

This code of practice is intended to provide a scalable process intended to support designers, manufacturers, transport operators and State entities in demonstrating and assuring that new or modified rail assets are safe in accordance with the Australian legislative framework.

**Hazard identification:**

1	All hazards associated with operation of rail systems.	6	
2		7	
3		8	
4		9	
5		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**

This code of practice will provide detailed processes for the management of System Safety within the rail industry, ensuring that:

- Safety is considered through the design process;
- Safety-related risks are eliminated or minimised in accordance with Australian legislation; and
- A sufficient Safety Argument is developed in a manner which is readily understood enabling greater appreciation of risks and obligations for implementing effective risk controls throughout the asset lifecycle.

This will ensure that a greater focus is placed on effective risk control actions providing both an effective demonstration that risks are eliminated or minimised SFAIRP and therefore provide a significant improvement to safety of transport employees and the public.

**Interoperability / harmonisation**

The code of practice will provide detailed processes for:

- Scoping of System Safety program in a risk-based manner to ensure effort is commensurate with the change;
- Risk identification, assessment, management and approval; and
- Safety Argument and deliverables.

By driving consistency across these areas there are significant gains to be made both in terms of supporting the development of Safety Arguments and the assurance by State entities of changes to rail assets.

### **Financial**

A consistent approach to the management and demonstration of System Safety will reduce the time required to develop safety programs, ensure that effort is directed toward implementing effective controls to eliminate or minimise risks and improve the quality of safety-related deliverables.

This will result in both a significant reduction in time and cost to address safety across rail assets and improvement of safety for rail employees and the public reducing ongoing costs of managing the rail network.

### **Environmental**

Not applicable.

### **Impacts:**

Will require significant effort to engage stakeholders, including both state transport authorities, transport operators and suppliers of rail assets.

Will have significant impact of management of safety and transition from use of extant CENELEC standards.

Will require significant specialist input including System Safety professionals and software specialists.

### **Reference / source materials:**

#	<u>Reference / source material</u>	<u>Available from</u>
1	RISSB SSA guidance	<a href="https://www.rissb.com.au/">https://www.rissb.com.au/</a>
2	TfNSW: <ul style="list-style-type: none"><li>- System Safety Standard for New or Altered Assets</li><li>- Guide to Transport for NSW Framework for Assuring the Safety of Rail Assets and Infrastructure</li></ul>	<a href="https://www.transport.nsw.gov.au/">https://www.transport.nsw.gov.au/</a>
3	CENELC standards (EN50126, EN50128 and EN50129)	
4	MIL-STD-882E	<a href="http://everyspec.com/MIL-STD/MIL-STD-0800-0899/MIL-STD-882E_41682/">http://everyspec.com/MIL-STD/MIL-STD-0800-0899/MIL-STD-882E_41682/</a>
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).