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:	Application of Safety Integrity Levels (SILs) in Australian Rail Projects
Date of suggestion:	February 2019
Reason for suggestion:	The Australian Rail Industry is undergoing unprecedented change, and the both industry and the regulator have an expectation that appropriate Safety Integrity Levels will be allocated and demonstrated for new and altered systems. There are a number of different approaches to SIL analysis and demonstration, which are documented in a variety of standards and guidelines, but there is no standardised approach - for example the requirements for a given SIL are not consistent among the different functional safety standards. Furthermore none of the current functional safety standards adequately addresses how SIL analysis fits within the SFAIRP framework prescribed within Australia by the Rail Safety National Law. The consequential uncertainty arising from these two issues is an ongoing source of contention between customers, suppliers, and regulators within the Australian Rail Industry, and has been the cause of significant delays in a recent major rail project. This subject was discussed by the Working Group which developed the RISSB System Safety Assurance Guideline in 2018, however it was considered too big an issue to address within the scope of that document, and more appropriate for consideration for a separate and dedicated RISSB guideline.
Railway discipline area:	Infrastructure, rolling stock, train control, and safety

Objective:

What: A guideline to establish recommended standardised approaches for the analysis and demonstration of SILs for Australian Rail Projects

For whom: Delivery Agencies, Rail Operators, Suppliers and Contractors

Why: To deliver appropriate safety assurance for rail projects, and to reduce the potential for disputes regarding the approach to be applied.

Scope:

The guideline is to provide a standardised approach to applying SIL aspects of functional safety standards in the Australian Rail Context. The scope includes:

- Identifying those functional safety standards (or elements thereof) that should be followed for SIL analysis and demonstration by projects in the Australian Rail Industry.

- The scope of rail systems for which SIL analysis is appropriate (e.g. should it be applied to depot equipment not involved in the movement of rolling stock?)
- The nature of safety functions for which SIL analysis/demonstration is appropriate (e.g. should functions implemented only by mechanical and/or physical systems be included?)
- At what stage of a project should SIL allocation be done? And who should do it – customer or supplier?
- The methods for analysing on-demand versus continuous safety functions.
- Methods for demonstrating that allocated SILs and/or THRs have been achieved (e.g. what needs to be demonstrated for which systems)
- The process for recognition and application of rail systems with pre-existing SIL certification from other jurisdictions.
- The relationship between SIL analysis/demonstration and SFAIRP determination, and how to demonstrate that the allocated SIL levels form part of a SFAIRP solution.

It is not anticipated that the Standard will provide guidance on the Tolerable Hazard Rates (THRs) that should be established for SIL analysis, however it should clarify the process and responsibility for setting THRs, and provide guidance, or at least principles, on how to set these. For example what is a 'hazard' in this context (is it the 'crash event' or the ultimate fatality event?). A SIL needs to be set at the 'lowest functional level' – what does that actually mean?

Hazard identification:

1	Failure of safety-related systems	6	
2	2.1 Loss of accreditation	7	
3	2.1.9 The failure to follow appropriate risk management processes	8	
4	2.1.23 The lack of effective change control systems	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

Providing a standardised approach to SIL analysis/demonstration will provide a baseline methodology which can be expected to meet required standards of safety assurance.

The application of a consistent approach will enhance the ability of stakeholders to undertake and demonstrate effective due diligence, review and approval of safety assurance documentation due to increased familiarity with the approach being applied.

Use of a consistent approach to SIL analysis/demonstration will mitigate the risk of misinterpretation of safety assurance documents at project interfaces.

Interoperability / harmonisation

The use of a standard approach across the Australian Rail Industry will increase opportunities for cross-acceptance of safety assurance arguments, and support the overall safety assurance of related projects being delivered by different delivery agencies.

Financial

The availability of an accepted standard approach to SIL allocation and demonstration should reduce compliance costs for members of the rail industry, increase the pool of practitioners available to perform SIL analysis activities, and reduce the potential for project delays arising from safety assurance activities ending up on the critical path for the commissioning of new projects.

Environmental

Not applicable

Impacts:

This is a highly specialised subject, with a limited number of capable and experienced practitioners within the Australian Rail Industry. Care will be needed to ensure that the Development Group has an adequate number of competent resources to ensure the quality of the guideline produced.

Reference / source materials:

#	Reference / source material	Available from
1	EN50126/128/129	SAI Global
2	Major Projects Guideline	ONRSR
3	IEC 61508	SAI Global
4	TMU MD 20001 ST (System Safety Standard for New or Altered Assets)	TfNSW (Asset Standards Authority)
5	System Safety Assurance Guideline	RISSB
6	State of the art analysis and review of results from previous projects (D4.1)	MODSafe
7	Analysis of Common Safety Requirements Allocation for MODSafe continuous Safety Measures and Functions (D4.2)	MODSafe

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).