Australian STANDARD®

Rail industry – System safety

RISSB
RAIL INDUSTRY SAFETY AND STANDARDS BOARD

Safety Standard

Please note this is a RISSB Australian Standard® draft

Document content exists for RISSB product development purposes only and should/shall not be relied upon or considered as final published content.

Any questions in relation to this document or RISSB's accredited development process should/shall be referred to RISSB.

RISSB Office

Phone:
(07) 3724 0000
Overseas: +61 7 3724 0000

Email:
info@rissb.com.au

Web:
www.rissb.com.au

This Australian Standard® AS 7474 Rail industry – System safety was prepared by a Rail Industry Safety and Standards Board (RISSB) Development Group consisting of representatives from the following organisations:

Asset Engineering Services,
Indic Consulting, Kiwi Rail,
MTM,
Public Transport Authority WA,
Rail Control Systems Australia,
Sydney Metro,
Abbott Risk Consulting,
Marling Group,
MottMac,
Queensland Rail,
Rio Tinto,
Transport for NSW,
Calibre Group,
Majestic Safety Assurance,
Network Rail Consulting,
Rail Assurance Consulting,
SMEC,
Department of Transport Victoria,

The Standard was approved by the Development Group and the Safety Standing Committee in Select SC approval date. On Select Board approval date the RISSB Board approved the Standard for release.

This standard was issued for public consultation and was independently validated before being approved.

Development of the Standard was undertaken in accordance with RISSB's accredited process. As part of the approval process, the Standing Committee verified that proper process was followed in developing the Standard

RISSB wishes to acknowledge the positive contribution of subject matter experts in the development of this Standard. Their efforts ranged from membership of the Development Group through to individuals providing comment on a draft of the Standard during the open review.

I commend this Standard to the Australasian rail industry as it represents industry good practice and has been developed through a rigorous process.

Deb Spring
Exec. Chair / CEO
Rail Industry Safety and Standards Board

Keeping Standards up-to-date

Australian Standards developed by RISSB are living documents that reflect progress in science, technology and systems. To maintain their currency, Australian Standards developed by RISSB are periodically reviewed, and new editions published when required. Between editions, amendments may be issued. Australian Standards developed by RISSB could also be withdrawn.

It is important that readers assure themselves they are using a current Australian Standard developed by RISSB, which should/shall include any amendments that have been issued since the Standard was published. Information about Australian Standards developed by RISSB, including 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. Members are encouraged to use the change request feature of the RISSB website at: http://www.rissb.com.au/products/. Otherwise, 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.

Notice to users

This RISSB product has been developed using input from rail experts from across the rail industry and represents good practice for the industry. 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.

AS 7474:2020

Rail industry – System safety

Document details

First published as: AS 7474:2019

ISBN Enter ISBN.

Document history

Publication Version	Effective Date	Reason for and Extent of Change(s)
2020	Select Board approval date	

Approval

Name	Date
Rail Industry Safety and Standards Board	Select Board approval date

Copyright

Published by SAI Global Limited under licence from the Rail Industry Safety and Standards Board, PO Box 518 Spring Hill Qld 4004, Australia

This Standard was prepared by the Rail Industry Safety and Standards Board (RISSB) Development Group AS 7474 Rail industry – System safety. Membership of this Development Group consisted of representatives from the organisations listed on the inside cover of this document

This paragraph is used to indicate if this Standard supersedes other documents in whole or in part. … only change this paragraph if it is applicable

Objective

The objective of this Standard is to define the minimum requirements for System Safety in the rail industry.

Standard Compliance

There are two types of control contained within Australian Standards developed by RISSB:

1. Requirements.
2. Recommendations.

Requirements – it is mandatory to follow all requirements to claim full compliance with the Standard. Requirements are identified within the text by the term 'shall'.

Recommendations – do not mention or exclude other possibilities but do offer the one that is preferred. Recommendations are identified within the text by the term 'should/shall'.

Recommendations recognise that there could be limitations to the universal application of the control, i.e. the identified control is not able to be applied or other controls are more appropriate or better.

For compliance purposes, where a recommended control is not applied as written in the Standard it could be incumbent on the adopter of the Standard to demonstrate their actual method of controlling the risk as part of their WHS or Rail Safety National Law obligations. Similarly, it could also be incumbent on an adopter of the Standard to demonstrate their method of controlling the risk to contracting entities, or interfacing organisations where the risk may be shared.

Controls in RISSB Standards address known railway hazards are addressed in an appendix.

Contents

Appendix Contents

1 Scope and general

1.1 Scope

This Standard identifies and defines the minimum requirements for system safety and its application to eliminate or minimize the safety risk so far as is reasonably practicable. This applies to changes to the system including the introduction of new or altered assets, or changes to the operation of the railway.

This Standard will apply throughout the system lifecycle phases including planning, design, build, installation, testing & commissioning, operation, maintenance, and disposal.

The RISSB System Safety Guideline provides additional information on the application of this Standard.

1.2 Normative references

The following are referred to in the text in such a way that some or all of their content constitutes requirements of this document:

- Rail Safety National Law (South Australia) Act 2012
- Rail Safety National Law National Regulations 2012
- Rail Safety National Law (NSW) No 8a
- Rail Safety (National Uniform Legislation) Act 2012 No 27 (NT)
- Rail Safety (National Uniform Legislation) Regulations 2015 (NT)
- Rail Safety National Law (Tasmania) Act 2012 No 38
- Rail Safety National Law Application Act 2013 No 22 (VIC)
- Rail Safety National Law (ACT) Act 2014
- Rail Safety National Law (WA) Act 2015
- Rail Safety National Law (WA) Regulations 2015
- Rail Safety National Law (Queensland) Act 2017
- Rail Safety National Law (Queensland) Regulation 2017

NOTE: Other reference documents, for informative purposes, are listed in a Bibliography at the back of this Standard.

1.3 Terms and definitions

For the purposes of this document, the following terms and definitions apply:

(a) ***assurance***
confidence in achieving a goal being pursued with a declaration intended to give that confidence (EN 50126-1:2017)

(b) ***hazard***
a source or a situation with a potential to harm someone (death, injury or illness) or damage property or the environment

(c) ***independent safety assessment***
The independent process to determine whether the system/product meets the specified safety requirements and to form a judgement as to whether the system/product is fit for its intended purpose in relation to safety (EN 50126-1:2017).

(d) ***individual risk***
individual risk is the probability of fatality per year to which a hypothetical individual is exposed from the operation of the railway. Individual risk is a useful notion when organizations are seeking to understand their risk profile and to prioritise and target safety management effort

(e) ***risk***
risk is a product of the estimated likelihood of an event and the consequence of that event. The expression of risk can be either qualitative or quantitative

The above definition is consistent with ISO 31000 which includes the notion of consequences and likelihood in determining the risk of an event occurring.

(f) ***safety objective***
objectives focused on safety outcomes that are developed as part of the project management processes that support System Safety. Safety objectives should be developed appropriate to the nature and scope of each specific system, or sub-system, for which they are set

(g) ***system safety***
the concurrent application of a systems-based approach to safety engineering and of a risk management strategy covering the identification and analysis of hazards and the elimination, control or management of those hazards through the life cycle of a system or asset.

General rail industry terms and definitions are maintained in the RISSB Glossary: https://www.rissb.com.au/products/glossary/

1.4 Abbreviations

(a) ***ISA***
independent safety *assessment*

(b) ***ONRSR***
Office of the National Rail Safety Regulator

(c) ***RSNL***
Rail Safety National Law

(d) ***RTO***
rail transport operator

(e) ***SFAIRP***
so far as is reasonably practicable

2 Key requirements of system safety

2.1 Introduction

System safety is the application of a structured multi-disciplinary approach that provides the necessary governance, processes and objective evidence by which an organization can assure themselves that a given new or altered product, service, or system can be safely integrated, operated and maintained into the transport network, so far as is reasonably practicable (SFAIRP). The approach should be scaled to be commensurate with the complexity of the change and associated level of risk.

System safety shall commence when the need for change is identified and shall continue throughout all of the lifecycle phases of the change.

Clauses 52, 53 and 56 of the RSNL define the safety duties of organizations and individuals to ensure that all reasonably foreseeable safety hazards are identified and eliminated, or if not reasonably practicable to do so, minimised SFAIRP.

The safety duty is a legal obligation which cannot be transferred to another entity or person.

System safety shall:

(a) identify all reasonably foreseeable hazards associated with the change;

(b) evaluate and eliminate or control hazards, so that cumulative risks to safety are reduced so far as is reasonably practicable;

(c) identify, implement, verify and validate resulting safety requirements;

(d) demonstrate that the design and implementation of the change to the system ensures safety so far as is reasonably practicable;

(e) communicate residual risk to the relevant stakeholders;

(f) be conducted by persons who have relevant experience and/or qualifications;

(g) ensure that all parties involved in the changes to systems demonstrate due diligence.

It is important to note that all requirements under this Standard should be applied commensurate with the scale and level of risk of the system or change being assured.

Organizations conducting system safety shall have a procedure that describes how system safety is undertaken.

2.2 System safety outcomes

The following outcomes shall be produced to make up a body of evidence that demonstrates that the safety of the system has been assured:

(a) System safety process.

(b) Change impact assessment;

(c) Document(s) that describe the safety objectives and system safety activities that are planned to be undertaken.

(d) Hazard log/ risk register.

(e) A change that is demonstrated to be as safe as is reasonably practicable.

(f) An argument (supported by evidence) that the change is demonstrably safe for its intended purpose.

(g) Safety objectives and safety requirements have been met.

(h) Residual safety risks have been effectively communicated to affected stakeholders.

(i) A list of application conditions for system operation.

Where appropriate, a post implementation review should be conducted to ensure the residual risk of the performance of the system is consistent with the body of evidence.

Figure 1 – Example of a typical system safety framework

As part of any framework, system safety shall also take into account the interfaces from a safety perspective and evaluate these and any potential dependencies that will impact or be impacted.

In relation to the framework, organizations shall first establish the correct level of assurance required for the system, and/or subsystems. The layers of assurance generally apply to projects requiring system safety with responsibilities allocated at each layer, namely:

(a) Layer 1 – What processes are in place - process integration at design (Design)

(b) Layer 2 – How to check that the work is being done against process – such as management system compliance, audit, independent safety assessment & independent reviews (Review)

(c) Layer 3 – Overview and authorities - satisfying a due diligence and acceptance processes; (Accept)

(d) Layer 4 – Handover from the delivery entities to the rail transport operator(s) for operations and maintenance. (Handover)

Depending on the project structure, layers may be applied by multiple or different project parties.

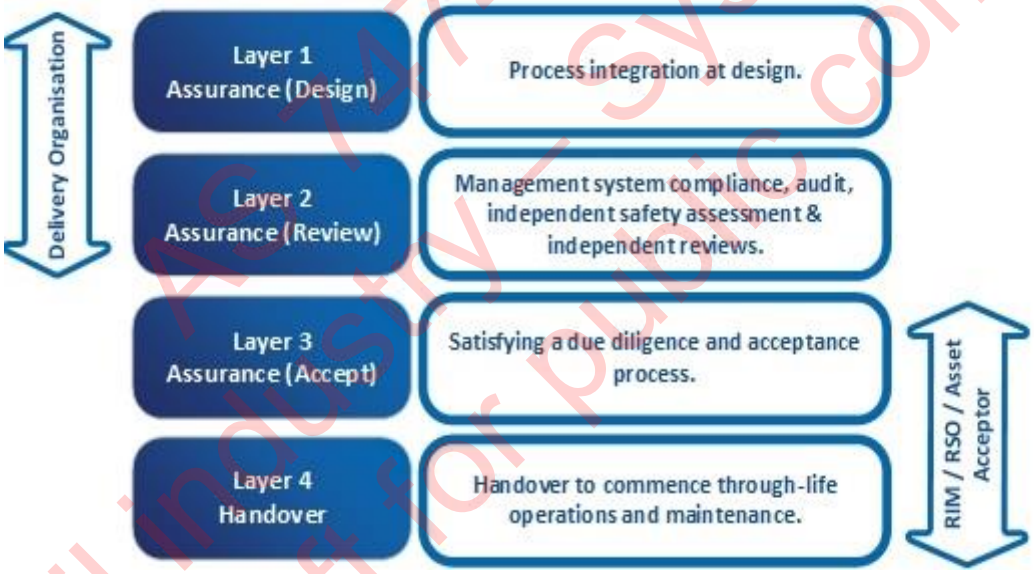

Figure 2 – Assurance layers

2.2.1 System safety process

For some organisations, specific system safety processes can be applicable to specific projects, and not to others. Regardless of the specifics of the processes, they should take systematic, structured and auditable approach.

The approach taken shall meet the requirements of the RTO's applicable systems of work.

Depending on the level of the system safety, the process shall include documentation of the following:

(a) Conceptual articulation of design.

(b) Interface definition.

(c) Hazard assessment and analysis.

(d) Impact assessment and analysis.

(e) Determination of need for Independent Safety Assessment, and its scope.

(f) Consideration integration of human factors.

(g) Evidence and assurance.

(h) Acceptance.

2.2.2 System safety management planning activities

A plan shall be developed at the project outset prior to the commencement of any system safety activities. The plan shall provide details of the safety objectives, scope and methodology as appropriate to the proposed change to ensure that the project requirements can be met. It shall be commensurate with the scale and level of risk associated with the change.

The plan shall provide an outline of all safety management processes, applicable to the project, and describe the key deliverables to demonstrate that the safety of the system is ensured so far as is reasonably practicable.

The plan shall be integrated into the system lifecycle to assist with the definition of safety objectives and the management of key risks. The plan shall be reviewed and updated during the project lifecycle phases to ensure the validity of the safety approach planned for each phase of the project lifecycle.

2.2.3 Demonstration of system safety

An initial safety argument shall be established at the start of the system safety process, that demonstrates that the system will be safe so far as is reasonably practicable.

This argument shall identify the supporting evidence to be captured to assure the safety of the system.

The plan shall define how the evidence will be generated.

The plan and argument shall be reviewed and updated throughout the project lifecycle.

The evidence shall be collected throughout the project lifecycle to support the argument.

The completed body of evidence together with the argument, shall demonstrate that the system is assured to be safe, so far as is reasonably practicable.

2.2.4 Independent safety assessment (ISA)

The demonstration of system safety may be subject to an appropriate level of independent safety assessment. It should be commensurate with the level of safety risk associated with the proposed project defined changes.

An ISA brief shall be developed to reflect the requirements of the system safety plan.

The assessor shall develop an ISA plan that will meet the objectives of the brief.

The ISA activities shall be conducted in accordance with the ISA plan.

The assessor shall report the findings of their assessment.

Appendix A Hazard register

This standard has a broad scope, as the context of the system safety can vary significantly. This means that the range of hazards potentially arising as part of the process of system safety may be all encompassing.

Where high level references of hazards are noted here, the user should review the details of the RISSB Hazard Register when constructing their own risk matrix.

Hazard number	Hazard	Heading number(s)
2.1	Loss of Accreditation	Throughout the Standard
3.0	Security	Throughout the Standard
4.0	Environment	Throughout the Standard
5.0	Rollingstock	Throughout the Standard
6.0	Infrastructure	Throughout the Standard
7.0	Human Factors	Throughout the Standard
8.0	Operations	Throughout the Standard
9.0	Signals Infrastructure	Throughout the Standard
10.0	Degraded Working	Throughout the Standard

Appendix B Bibliography

The following referenced documents are used by this Standard for information only:

a) AS 7470 - Integration of Human Factors in Engineering Design – General Requirements.

b) AS 7472 Railway Operations – Management of Change.

c) European CENELEC Standards.

d) iESM Handbook.

e) ISO 31000 – Risk Management.

f) ONRSR Guideline - Asset Management.

g) ONRSR Guideline - Major Projects

h) ONRSR Guideline - Meaning of the duty to ensure Safety So Far As Is Reasonably Practicable.

i) ONRSR Guideline - Preparation of a Rail Safety Management System.

j) ONRSR Policy - Compliance & Enforcement Policy.

k) ONRSR Policy - Notification of Change.

l) ONRSR Policy - Safety Improvement.

m) RISSB Guideline - Integration of Human Factors in Engineering Design;

n) RISSB Guideline - System Safety;

o) RISSB Guideline – Security Handbooks (Volumes 1 and 2);

p) RISSB Guideline - Rail Cyber Security;

q) RISSB Standard - AS7473: 2020 Complex Systems Integration

r) RISSB Standard - AS 7770:2018 Rail Cyber Security.

s) RISSB Guideline – Safe Decisions

About Rail Industry Safety and Standards Board

The Rail Industry Safety and Standards Board is a not for profit company limited by guarantee. Wholly owned by its funding members, RISSB is required to apply the whole of its income and assets to achieving the objects listed in its constitution.

RISSB is responsible for the development and management of Standards, Rules, Codes of Practice and Guidelines for the Australian rail industry.

For further information, visit www.rissb.com.au

RISSB Australian Standards Development Process

The Standards development process is rigorous and transparent.

Authors work with RISSB's Standards Development Managers and Development Groups to ensure that products are acceptable to industry. Standing Committees oversee this work and ensure that proper governance and process is followed. The products are exposed to the public and industry for comment and validated by an independent validator.

Once agreed by the Development Groups, Standing Committees and Validator, the drafts are passed to the RISSB Board for approval.

The same process is used in developing other RISSB products, although Guidelines are not exposed to the public for comment or validated, given their non-binding nature.

Standards Development and Accreditation Committee

RISSB is accredited by the Standards Development and Accreditation Committee (SDAC), and all Standards produced by RISSB since 31 July 2007 are published as Australian Standards.

The Standards Development and Accreditation Committee audits RISSB annually to ensure that RISSB's processes are in accordance with SDAC accreditation requirements.

Sales and distribution

Australian Standards developed by RISSB are sold and marketed through SAI Global. For further information, please visit www.saiglobal.com.

Financial members of RISSB are granted access with membership.

RISSB
RAIL INDUSTRY SAFETY AND STANDARDS BOARD

ABN 58 105 001 465

For information regarding the development of Australian Standards 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 3274 000
E Info@rissb.com.au

For information regarding the sale and distribution of Australian Standards developed by RISSB contact:

SAI Global Limited
Phone: 13 12 42
Fax: 1300 65 49 49
Email: sales@saiglobal.com
http://infostore.saiglobal.com/store

ISBN: Enter ISBN.