**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.

**Document Control**

**Identification**

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rollingstock safety assessment</td>
<td>1.0</td>
<td>30 January 2019</td>
</tr>
</tbody>
</table>

**Document History**

<table>
<thead>
<tr>
<th>Publication Version</th>
<th>Effective Date</th>
<th>Reason for and Extent of Change(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>30 January 2019</td>
<td>First publication</td>
</tr>
</tbody>
</table>

**Copyright**

All rights reserved RISSB 2018. The content of this document (except for content explicitly marked as originating from other sources) is owned by RISSB and may not be reproduced or transmitted by any means in whole or in part without written permission from the copyright owner. Current financial members of RISSB may utilise and reproduce the text or diagrams contained herein use within the context of their own rail operations. No photographs contained herein may be reproduced without permission of the relevant copyright holder.
# Table of Contents

1. **Introduction** ............................................................................................................. 5
   1.1 General .................................................................................................................. 5
   1.2 Purpose .................................................................................................................. 5

2. **Scope** ..................................................................................................................... 5
   2.1 Compliance ............................................................................................................ 5
   2.2 Application ............................................................................................................ 6

3. **Referenced documents** .......................................................................................... 6
   3.1 Normative references .......................................................................................... 6
   3.2 Informative references ....................................................................................... 6
   3.3 Definitions and abbreviations .............................................................................. 7

4. **Rolling stock safety assessment** ............................................................................. 10

5. **Project definition** .................................................................................................. 12
   5.1 Determine safety obligations ............................................................................... 12
   5.2 Define scope of work and project requirements ............................................... 12
   5.3 Define acceptance criteria ................................................................................... 13
   5.4 Engineering process ............................................................................................. 13
   5.5 Team .................................................................................................................... 13

6. **Risk management** ................................................................................................ 14
   6.1 Risk identification ............................................................................................... 14
   6.2 Safety assessment methods ................................................................................ 14
   6.3 Interface and operational safety assessment ..................................................... 15
   6.4 Risk control .......................................................................................................... 16

7. **Technical support** ................................................................................................ 16
   7.1 Design safety assurance ...................................................................................... 16
   7.2 Independent assessment ...................................................................................... 16
   7.3 Independent competent person .......................................................................... 16

8. **Change management** ......................................................................................... 17

9. **Records** ................................................................................................................. 17

10. **Accreditation** ...................................................................................................... 18

11. **Rolling stock certification and acceptance** ....................................................... 18

12. **Human factors integration** .................................................................................. 19

13. **Team support** .................................................................................................... 19
   13.1 Competency assessment ..................................................................................... 19
13.2 Interface management ........................................................................................................... 20

14 Supplier management ............................................................................................................... 20

14.1 Assurance ............................................................................................................................. 20

15 Rolling stock engineering lifecycle .......................................................................................... 21

15.1 Specification .......................................................................................................................... 22

15.2 Design .................................................................................................................................... 23

15.3 Supply and assembly .............................................................................................................. 23

15.4 Test and certification .............................................................................................................. 24

15.5 Integration .............................................................................................................................. 25

15.6 Commissioning and acceptance ............................................................................................ 25

15.7 Operation and maintenance .................................................................................................. 25
1 Introduction

1.1 General
The Rail Safety National Law sets a duty on Australian rolling stock operators, associated industry participants (designers, suppliers, etc.) and those who certify and register (owners, rail infrastructure managers, etc.) rolling stock to ensure the rolling stock safety so far as is reasonably practicable (SFAIRP). SFAIRP is further explained by Office of the National Rail Safety Regulator (ONRSR) in the guideline – meaning of duty to ensure safety so far as is reasonably practicable – SFAIRP.

The Work Health Safety Act (WHSA) also places similar duties upon persons conducting a business or undertaking.

As a result, safety has to be looked at more in the entire, integrated lifecycle of rolling stock.

The guideline is to outline major safety assessment aspects to be considered by participants in rolling stock lifecycle and to lead rolling stock providers towards achieving a SFAIRP solution.

1.2 Purpose
This document sets guidance for:

a) providing rolling stock safety assessment awareness in rolling stock lifecycle,
b) preparing and undertaking a safety assessment and safety assurance case toward regulatory compliance,
c) addressing stakeholder responsibilities for safety in the rolling stock lifecycle.

This document is an aid to rail industry describing common practice for the safety assessment of rolling stock and approvals.

2 Scope
This guideline applies to new, modified, repaired and overhauled rolling stock being assessed for use on all Australian railways and covers the complete rolling stock lifecycle.

The guideline does not include the daily management of workplace safety, which is covered by WHS standards. Rolling stock operators must perform any assurance activity identified to ensure the duty of care is accomplished.

Repair in this guideline is limited to only unusual repairs which are not considered in the rolling stock maintenance cycle.

2.1 Compliance
There are only recommendations in this guideline.

This guideline may not be, in and of itself, sufficient to make any claim that safety is managed so far as is reasonably practicable, as described in applicable rail safety legislation.
2.2 Application

The application of this guideline needs to be assessed on a case by case basis depending on complexity, risk and novelty of the change.

Training and development should be considered in support of the guideline implementation.

3 Referenced documents

3.1 Normative references

The following referenced documents are indispensable for the application of this Guideline:

a) A390705 guideline meaning of duty to ensure safety so far as is reasonably practicable – SFAIRP, Office of the National Rail Safety Regulator (ONRSR).

b) A401174 – guideline for preparation of a safety management system, ONRSR.

c) A415539 - guideline – major projects, ONRSR.

d) AS 7470 – Human factors integration in engineering design - general requirements.

e) AS 7501 – Rolling stock certification.


g) EN 50128:2011 – Railway applications. Communication, signalling and processing systems. Software for railway control and protection systems.

h) EN 50129 – Railway applications - communication, signalling and processing systems - safety-related electronic systems for signalling.

i) EN 50388 – Railway applications - power supply and rolling stock - technical criteria for the coordination between power supply (substation) and rolling stock to achieve interoperability.

j) IEC-61133 – Railway applications - rolling stock - testing of rolling stock on completion of construction and before entry into service.

k) ISO 9001 – Quality management systems — requirements.

l) ISO 10007 – Quality management -- guidelines for configuration management.

m) ISO/IEC/IEEE 15288 – Systems and software engineering - system life cycle processes.


p) ISO 55000 – Asset management - overview, principles and terminology.


3.2 Informative references

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

a) Incident investigation reports, ATSB.
3.3 Definitions and abbreviations

For the purposes of this guideline the definitions shall apply. The following definitions are specific to this guideline all other definitions are can be located in the RISSB glossary.

Acceptance for on-track testing certificate: The type certificate issued by a representative of the rolling stock operator following an assessment process on the rolling stock, and on which limitations applying to on-track testing are recorded. This certificate is a condition precedent to any dynamic movement of the rolling stock on a network.

Certificate of standards compliance: The overarching certificate confirming that a unit of rolling stock has been designed, constructed and tested in accordance with the requirements of RISSB Rolling Stock series of standards.

Certification: The process of certifying the compliance of the design and construction of rolling stock against the RISSB rolling stock series of Australian standards and other standards where allowed by the RISSB rolling stock series. Certification culminates with the issuing of the certificate of standards Compliance supported by the design compliance certificate, construction conformance certificate and the acceptance for on-track testing certificate.

Class: A class of rolling stock is a group of vehicles built to the same design within the parameters of the data register.

Construction: The processes of fabrication, manufacture, and assembly (includes installing components, connecting sub-systems), and the required quality control activities, such as Inspection and test plan (ITP), that generate construction records.

Construction conformance certificate: The routine document issued for each unit following a verification process on rolling stock, and on which compliance of the vehicle(s) to the certified design is recorded.

Data register: The list of key characteristics of a particular (class of) rolling stock as listed in the RISSB rolling stock series of Australian standards.

Existing rolling stock: Rolling stock that operates on a railway track in Australia, has a certificate of engineering compliance (certification, previously called registration).

Hazard log: A record keeping tool applied to tracking all hazard analysis, risk assessment and risk reduction activities for the whole-of-life of a rolling stock.

Independent competent person (ICP): A person appointed to critically and capably examine, determine and record compliance of new or modified rolling stock against the AS 7500 series or other applicable standards.
Independent safety assessment: The formation of a judgement, separate and independent from any system design, development or operational personnel, that the safety requirements for the system are appropriate and adequate for the planned application and that the system satisfies those safety requirements.

Independent safety assessor (ISA): A person who carries out independent safety assessment.

Independent verifier (IV): A person who carries out independent design verification. In some projects this may simply be someone who did not undertake the design work itself.

Life expired rolling stock: Worn out or outdated rolling stock that has passed from operational ability and lost all rolling stock attributes and functions necessary to sustain operation.

Modified rolling stock: Rolling stock engineering change on existing rolling stock affecting the engineering parameters (rolling stock data considered critical for operational purposes) or performance of the rolling stock. The declared compliance status for one or more mandatory (MAN) or recommended (REC) clauses in the standards compliance register and project scope are as a consequence affected.

Registration: The process, used by the rail infrastructure manager, by which rolling stock is recorded as a vehicle that can operate on their network.

Network: A railway system under the control of one or more rail infrastructure managers. A track access agreement would be formed between an external Rolling Stock and the rail infrastructure manager (i.e. when the Rolling Stock Operator is not a part of the rail infrastructure manager’s organisation) to allow operation on that network.

ONRSR: The Office of the National Rail Safety Regulator, an independent body corporate established under the Rail Safety National Law (South Australia) Act 2012 to encourage and enforce safe railway operations and to promote and improve national rail safety.

Operator: A person who has effective management and control of the operation or movement of rolling stock on rail infrastructure for a particular railway but does not include a person be reason only that the person drives the rolling stock or controls the network or the network signals.

Owner: The person or body with legal title to the rolling stock.

Rail infrastructure manager: It is a body or organisation responsible by reason of ownership, control or management, for the construction and maintenance of track, civil and electric traction infrastructure, or the construction, operation or maintenance of train control and communication systems, or a combination of these; or a person or body acting on its behalf.

So far as is reasonably practicable (SFAIRP): In relation to a duty to ensure safety, means that which is (or was at a particular time) reasonably able to be done in relation to ensuring safety, taking into account and weighing up all relevant matters, including:

- the likelihood of the hazard or the risk concerned occurring; and
- the degree of harm that might result from the hazard or the risk; and
- what the person concerned knows, or ought reasonably to know, about:
  - the hazard or the risk; and
  - ways of eliminating or minimising the risk.
- the availability and suitability of ways to eliminate or minimise the risk; and
• after assessing the extent of the risk and the available ways of eliminating or minimising the risk—the cost associated with available ways of eliminating or minimising the risk (including whether the cost is grossly disproportionate to the risk).

**Repaired rolling stock:** Rolling stock restored to a good condition in such a way that the declared compliance status for one or more mandatory (MAN) or recommended (REC) clauses in the standards compliance register is as a consequence not affected. For example, OEM component changed over.

**Rolling stock:** Any vehicle that operates on or intends to operate on or uses a railway track, including any loading on such a vehicle, but excluding a vehicle designed for both on- and off-track use when not operating on the track. Rolling stock is a collective term for a large range of rail vehicles of various types, including: a locomotive, carriage, rail car, rail motor, light rail vehicle, train, tram, light inspection vehicle, self-propelled infrastructure maintenance vehicle, trolley, wagon and monorail vehicle.

**Rolling stock operator (RSO):** A organisation who has effective management and control of the operation or movement of rolling stock on rail infrastructure for a particular railway but does not include a person be reason only that the person drives the rolling stock or controls the network or the network signals.

**Rolling Stock Supplier (RSS)** the organisation that supplies the rolling stock to the RSO which may also be the designer, manufacturer, importer, test authority, maintainer or manager of these life cycle stages

**Safety assurance:** An application of safety engineering practices, intended to minimise the risks of operational hazards.

**Safety Case:** A structured argument, supported by evidence, intended to justify that a rolling stock is acceptably safe for a specific application in a specific rail operating environment.

**Safety management system (SMS):** Any system whose primary objective is to achieve safe rail operations. Under co-regulation the accreditation authority has the role of defining the minimum requirement for what must be included in a specific safety management system. Rail transport operators, rail infrastructure managers and rolling stock operators are free to nominate equivalent or superior standards for their safety management system.

**Schedule of standards:** A List of all applicable issued standards against which the rolling stock should be assessed for compliance in accordance with the AS 7501 process.

**Standards compliance register:** A list of compliance and controls against the requirements contained in the AS 7500 series of Australian Standards. See Appendix C in the AS 7501.

**Testing:** The process of verifying that the rolling stock meets design requirements, including but not limited to static factory testing, commissioning and any dynamic operations prior to revenue service.

**Track access agreement:** A formal agreement between a rolling stock operator and a rail infrastructure manager allowing the operator to operate on the rail infrastructure managers’ network under agreed commercial, technical and operational conditions.

**Train:** A single unit of self-propelled rolling stock, or two or more units of rolling stock coupled together, at least one of which is a locomotive or other self-propelled unit.

**Unit:** The smallest number of vehicles that can be considered a single independent entity for the purpose of certification.
Verification checklist: A checklist produced by the supplier listing the features of the design that need to be verified, and how they will be verified. It must be consulted and updated during the production of the construction conformance certificate and the acceptance for on-track testing certificate.


4 Rolling stock safety assessment

New, modified, repaired or overhauled rolling stock may cause a change to the rolling stock operator’s (RSO) business. A rolling stock operator’s responsibility is to assess the change and investigate its safety significance over the entire lifecycle. The change is assessed, implemented and controlled using a safety management process.

An example of a safety management process is presented on Figure 1.

The main aspects of a safety management process are:

- project definition;
- risk management;
- risk identification;
- safety assessment and risk control:
  - analyse risk;
  - evaluate risk;
- technical support;
- team support.

In the project definition phase, safety requirements may be specified along with other requirements. Preliminary risks in the entire rolling stock lifecycle should be identified at the beginning of project. The risks should be registered in a hazard log. The hazard log is maintained for the entire rolling stock lifecycle.

The rolling stock safety assessment is a comprehensive, systematic investigation and analysis of all aspects of risks related to rolling stock associated with major incidents that could potentially occur in the course of operation or work on, with and around rolling stock. There are a number of safety assessment methods available to assess safety in rolling stock.

Risk control is a step of the risk management process that involves dealing with the risk in question.
Figure 1 reflects a generic risk management process and should be tailored to suit project individual requirements as defined by RSO.
# 5 Project definition

Rolling stock project definition is to establish the project context which includes determining safety obligations, defining the scope of work, project requirements, acceptance criteria, engineering process, and the engagement of competent teams of people.

## 5.1 Determine safety obligations

A list of legislation, regulatory policies and recommended documents can be found in this guideline. These references should be considered when manufacturing new and modifying, repairing or overhauling existing rolling stock.

The Rail Safety National Legislation and the additional guidance provided in ONRSR documentation influences the safety assessment and system assurance approach to rolling stock engineering.

Good Practice Handbook – international engineering safety management elaborates on safety assessment methods used in system engineering.

RISSB’s Systems Safety Assurance Guideline is an overarching system engineering guideline that may be read in conjunction with this guideline.

Engineering process phases defined in the international standards do not align:

- **EN50126/IEC 62278** (concept; system definition and operational context; risk analysis and evaluation; specification of system requirements; architecture of apportionment; design and implementation; manufacture; Integration; system acceptance; operational, maintenance and performance monitoring; decommissioning).
- **IEC15288** (stakeholder requirements definition; requirements analysis; architecture definition; implementation; integration; transition; system validation; operation and maintenance; disposal).
- **IEC TR24748** (concept; development; production; verification; validation; utilisation and support; retirement).

RISSB systems safety assurance guideline tailors the phases from EN50126/IEC 62278 that also differs from other standards’ phases and may not be suitable for rolling stock engineering process.

Guideline A401174 provides guidance on the regulatory requirements for a safety management system and provides direction on development of a compliant SMS.

Guideline A401174 may be considered for preparation of a safety management system.

## 5.2 Define scope of work and project requirements

The RSO defines the rolling stock project scope of works. Rolling stock requirements are a vital part of that definition.

AS 7501 Railway rolling stock compliance certificate should be followed for certification of rolling stock along with additional project specific requirements.

System requirement categories that are applicable to rolling stock project are reflected in the RISSB systems safety assurance guideline.
Rolling stock requirements are to be clearly specified and in plain language, allowing a safety assessment against those requirements later on in the rolling stock lifecycle.

### 5.3 Define acceptance criteria

Acceptance criteria to project requirements are determined by the RSO taking into consideration input from other stakeholders.

For major projects, the safety assurance team, if applicable, develop the requirements and establish acceptance criteria on behalf of the RSO.

For smaller projects, acceptance criteria may be defined by an ICP within the RSO’s organisation.

Project documentation should elaborate on the acceptance criteria and establish a plan for meeting the criteria.

Configuration change board (CCB) gates are to be defined in the rolling stock engineering lifecycle which allow an engineering safety assessment. To ensure a progressive approach to safety is taken and aligns with the engineering activities, the RSOs define safety assurance activities expected to be performed for each CCB gate.

Evidence that project requirements in the rolling stock lifecycle have been met are to be provided and stored in a system which will allow an independent assessment if required.

Special computer programs may be mandated by the RSO to assist in the requirements management. The programs should have suitable functionality to allow specification of acceptance criteria, assignment of criteria to corresponding requirements, and should support the attachment of assessing evidence.

### 5.4 Engineering process

Safety is considered in the entire rolling stock lifecycle, i.e. when manufacturing new and modifying, repairing or overhauling existing rolling stock, when rolling stock is in operation and when it is being maintained. Engineering process should be established by the RSO to define rolling stock lifecycle.

The RSOs define and clearly communicate the engineering process phases and tailor it to suit new, modified, repaired or overhauled rolling stock project.

An example of engineering V lifecycle is presented on Figure 2 in section 15 of this guideline.

Configuration change gates should be established by the RSO in lifecycle phases to allow safety assessment points.

### 5.5 Team

Each person in rolling stock lifecycle are to be competent (have suitable or sufficient skill, knowledge, experience and qualified determined by their organization) to conduct the allocated tasks.

An independent competent person is normally appointed by the RSO to examine, determine and record compliance of new, modified, repaired or overhauled rolling stock against the RISSB rolling stock series of Australian standards or other applicable standards. The ICP may need to be accepted by rail infrastructure manager (RIM) prior to commencing its duty.
The independent safety assessor may be engaged by the RSO to carry out the independent safety assessment.

6 Risk management

Risk management consists of three major areas:

- Risk identification.
- Safety assessment (analysing and evaluating risk).
- Risk control.

RISSB’s Systems safety assurance guideline defines and describes in detail, methods and outputs used in risk management.

6.1 Risk identification

The RSO organises a preliminary hazard identification (PHI) that identifies risks associated with the rolling stock project, engineering and the rolling stock lifecycle. All the identified risks are documented in a preliminary hazard list (PHL). The PHL is then registered in a hazard log that is maintain for the entire lifecycle. The PHI may be done as part of the risk assessment.

Sources of data that rolling stock operators use in preliminary hazard identification are as follows:

- Australian Transport Safety Bureau (ATSB) rolling stock operators’ incident safety data.
- Incident logs (assets and injuries).
- RISSB hazard register.
- Lessons learnt from previous projects.

Special attention should be paid to the identification of interface and operational safety risks.

Interface and operational safety are dependent on cooperation between the RIM (the operator and manager of the infrastructure) and the RSO (the operator and manager of the rolling stock).

6.2 Safety assessment methods

Rolling stock safety assessment should include:

- the nature of each major incident and major incident hazard;
- the likelihood of each major incident hazard causing a major incident;
- in the event of a major incident occurring, its potential magnitude and the severity of its potential health and safety consequences;
- the range of control measures considered;
- the control measures the RSO decides to implement.

The methods that can be considered to analyse risk of rolling stock are:

- preliminary hazard analysis (qualitative analysis);
- preliminary event tree analysis (quantitative analysis);
• fault tree analysis;
• Failure mode, effects, and criticality analysis;
• Operating and support hazard analysis;
• Interface hazard analysis;
• system hazard analysis;
• subsystem hazard analysis;
• existing RSO procedures.

The methods are described in greater details in RISSB systems safety assurance guideline and in good practice handbook – international engineering safety management.

Applicability of safety assessment methods to rolling stock projects will depend on the type of project. The methods to be used by project should be decided by RSO and communicated via project documentation.

Analysed risk is evaluated by comparison with acceptance criteria, targets and standards, by demonstration of control adequacy and by estimating risk explicitly.

6.3 Interface and operational safety assessment

A safety interface agreement defines context of rolling stock operation and identifies interface entities, scope and agree obligations.

The RIM and the RSO undertake risk identification and safety assessment individually or jointly or may adopt a safety assessment carried out by independent safety assessor.

Safety assessment methods mentioned in this guideline apply to interface and operational safety assessment.

The RIM and the RSO continuously monitor and review the risks and measures to control the risks for which it is responsible, including progress against the timetable for implementation of risk management measures.

The RSO and the RIM consult each other in relation to the outcome of their monitoring and reviewing of risks and measures. If a risk is considered to be unacceptable following a review, the RSO and the RIM work collaboratively and cooperatively to agree the measures to control the risk so far as is reasonably practicable.

RSOs develop an interface safety management plan and agree the plan with the RIM.

An interface compliance plan will be in place for safe interface and operation.

The following areas may be taken under consideration when assessing interface and operational safety:

• Tests for fitness of purpose of rolling stock.
• Route knowledge obligations.
• Rail traffic crew competencies.
• Use of radio equipment suitable for use on rail infrastructure manager network.
• Adherence to operational noise limits.
• Controls for environmental spills from loading or locomotives.
• Incident response management processes.
• Emergency management capacity and responsibilities.
• Dangerous goods identification, management and reporting.
• Security sensitive dangerous goods identification, management and reporting.
• Adherence to RIM’s network rules and network procedures.

6.4 Risk control

In the safety management process, assessed rolling stock risk is questioned to establish appropriate control measures, set safety requirements and obtain approval. The risk is then monitored and should be evaluated again through the entire rolling stock lifecycle.

7 Technical support

7.1 Design safety assurance

Rolling stock design assurance is a planned and systematic set of activities that ensures rolling stock engineering processes and products conform with rolling stock requirements for safety, reliability, availability, maintainability, standards, procedures and regulations.

In complicated project, the RSO may establish a design assurance team to assist the project in ensuring the processes are developed and followed, and that competent people conduct well defined tasks.

Rolling stock safety assurance activities for each rolling stock project are defined by the RSO in a project plan.

7.2 Independent assessment

To assure safety in rolling stock lifecycle, RSOs or railway manufacturers conducts an independent technical assessment. In some Australian states, independent technical assessment is mandatory.

The independent technical assessment mission provides an authoritative independent opinion on whether or not a project/system will meet its safety requirements.

The independent competent person (ICP) determines whether new, modified, repaired or overhauled rolling stock meet the specified safety requirements and forms a judgement as to whether the rolling stock is fit for its intended purpose in relation to safety. The ICP is independent, qualified and competent specialist and may come from the RSO organisation if the independence criteria is met (i.e. removed from design and design engineering).

7.3 Independent competent person

The RSO appoints an independent competent person to verify that safety and technical critical elements are suitable and remain suitable for the life of rolling stock. The ICP will have the sufficient practical and theoretical knowledge and experience to carry out this function, must be independent from the design process and must be free from any external pressures (e.g. financial, management) which could affect their judgement when carrying out verification activities.
The main objective of ICP is to examine, determine and record compliance of rolling stock against the RISSB rolling stock series of Australian Standards or other applicable standards.

The RSO may need to consult the appointment of ICP with the RIM.

The ICP may not need to be involved when rail accreditation of modified, repaired or overhauled rolling stock remains unchanged.

8 Change management

Change Management procedures should be established in accordance with AS ISO 10007 and applied to relevant changes including:

- changes to configuration items;
- changes to procedures relating to commissioning, operation and maintenance.

Configuration management should be maintained for the whole of asset life. This generally requires cooperation between several different organisations and stakeholders involved in the rolling stock life-cycle and supply chain. Configuration records must be maintained for whole of asset life and made readily accessible to the relevant stakeholders. This is especially important for stakeholders involved in managing ongoing through life support activities such as warranty tasks, corrective maintenance, system fault-finding and optimisation, engineering changes and modifications, obsolescence management and condition monitoring when reference to the product baseline data is essential.

Changes should not be implemented until they have been planned and approved in accordance with Section 5 of the ISO standard.

Change planning includes identification of, and communication with, affected stakeholders and impacts of the proposed changes. The RACI matrix should be established for affected stakeholders.

During and following implementation, compliance with change requirements should be verified, reviewed and validated. Non-conformances arising from the changes should be identified and managed using established techniques such as NCR, CPA, FRACAS, FMECA etc.

9 Records

As part of regulatory requirements rolling stock operator can keep the assessment records. That includes and is not limited to:

- defects recording and corrective action;
- development of a safety argument/case;
- insurance documentation;
- hazardous materials records;
- accident records;
- risk log/assessment;
- equipment/maintenance records;
• configuration management;
• documentation along the project lifecycle (i.e. specify, design, supply and assembly, test and certify, integration, commissioning and acceptance, operation and maintenance, decommissioning).

The way of keeping the records is determined by the RSO. Further guideline on storage and retention of documents and records, exchange of information is given in A401174.

Rolling stock suppliers also are required to keep rolling stock records.

10 Accreditation

Rolling stock operators must have valid rail safety accreditation to be able to operate rolling stock.

The purpose of accreditation by the Office of the National Rail Safety Regulator is to demonstrate that a rolling stock operator has the competence and capacity to manage safety risks associated with its railway operations by implementing its safety management system and to safely manage changes to its operations.

The RSO should review the impact of change on its accreditation and may need to seek variation of its accreditation.

11 Rolling stock certification and acceptance

Operational readiness is a state that is moved toward incrementally by performing tasks and assembling rolling stock throughout the project engineering lifecycle. An operational readiness assessment ensures the rolling stock operating environment can effectively support and accept the changes resulting from the project.

Rolling stock shall obtain the following acceptance before achieving operational readiness:

<table>
<thead>
<tr>
<th>Acceptance Stage</th>
<th>Typical Acceptance by…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Planning, Stakeholder Notifications, RACI matrix</td>
<td>RSO</td>
</tr>
<tr>
<td>Life Cycle Stages (refer to Systems Engineering 'V' Cycle)</td>
<td>IV and CCB</td>
</tr>
<tr>
<td>Safety Management</td>
<td>Safety Management Team or ISA</td>
</tr>
<tr>
<td>Design Certification (AS 7501 plus additional requirements)</td>
<td>IV / ICP</td>
</tr>
<tr>
<td>Construction Certification (AS 7501 + additional requirements)</td>
<td>IV / ICP</td>
</tr>
<tr>
<td>Test Readiness certificate</td>
<td>ICP, RIM</td>
</tr>
<tr>
<td>System Verification Review</td>
<td>IV / CCB</td>
</tr>
<tr>
<td>Network Acceptance and Registration</td>
<td>RIM</td>
</tr>
</tbody>
</table>
The Configuration Change Boards (CCB) should have appropriate stakeholder representation and expertise which may change with the life cycle progression.

Requirements Analysis shall ensure that all relevant requirements and standards are captured prior to rolling stock design and confirmed at the System Requirements Gate Review (SRR).

Note that stakeholders such as the RIM, RSO or RSS may require compliance with standards or specifications in addition to those in the AS 7500 series.

Interim acceptance may be provided to allow on track or other tests to be completed before full authorisation is obtained.

The rolling stock operator must obtain authorisation to travel on the RIM’s network prior to entering service.

12 Human factors integration

Consideration of human factors in all activities related to the development of new, modifying, repairing or overhauling rolling stock is dictated by WHSA.

Human factors are to be considered in specification and design, and then implemented in other lifecycle phases.

Direction on human factors (integration into SMS, generic processes, integration in risk management, change management, design and procurement, job and task design, training of safety workers, safety reporting systems and data analysis and investigation) are described in A401174. It is recommended to follow the guidance as well as standards that provide detailed human factors requirements (e.g. T HR HF 00001 ST).

Rolling stock projects may contain specific requirements for inclusion of a human factor integrator to assist an ICP or safety assurance team where applicable.

13 Team support

13.1 Competency assessment

Competency assessment is the RSO’s responsibility. The RSO develops and maintain a process and system to manage competency of the RSOs project personnel as well as personnel of suppliers. With respect to supplier personnel, the RSO may rely on supplier’s competency assessment system.

ARA’s guideline - National Rail Industry Worker (RIW) introduces a competency system of the Rail Safety Worker and supports the process of the RSOs competency development and maintenance.

The assessment outcome identifies a need for training and development that has an impact on competency of personnel. This may include maintenance and operational personnel and other disciplines.

Competencies requirements should be documented in the project requirements.
13.2 Interface management

Interfaces are a source of uncertainty and can lead to a high safety risk.

Safety requirements associated with the rolling stock systems and sub-systems interfaces should be identified, documented and assessed. Interfaces may be managed in the entire rolling stock lifecycle. Special attention should be paid to integration of those interfaces.

Interface management includes the activities of defining, controlling, and communicating the information needed to enable unrelated objects (including systems, services, equipment, software, and data) to co-function.

RSOs should decide on a project by project basis the need to produce an Interface Management Plan.

14 Supplier management

The RSO should establish and maintain a supplier selection system based on competency assessment, quality and delivery history (this may include supplier auditing and rolling stock inspections during a supplier’s activities).

Interfaces with the RSO should be identified prior to and during rolling stock project were possible. Risks identified at the beginning and during a rolling stock project are submitted to the RSO for safety assessment or if assessed by supplier, assessment methodology and results are also to be submitted to the RSO.

For specific rolling stock components, the RSO may ask suppliers to retain components records for the entire rolling stock lifetime.

Suppliers must cooperate with the RSO to allow third party rolling stock inspections and final inspections. The RSOs highlight the need for inspections as a mandatory requirement on project.

The RSO requires suppliers to prepare and submit to the RSO Inspection Test Plan.

14.1 Assurance

Competency assessment, interface management and supplier management are audited by the RSO. The RIM may have some specific requirements to audit those areas and such requirements may be defined in a track access agreement or other documentation.
15 Rolling stock engineering lifecycle

The RSO, in consultation with the major stakeholders, is responsible for defining the project engineering lifecycle.

Processes on projects to deliver new, modified, repaired or overhauled rolling stock should be structured around the system engineering lifecycle.

All life cycle stages are applicable though the scope of work may vary depending on the scale of the project.

The availability of documentation of older rolling stock may be limited. The RSO, in consultation with relevant stakeholders, should determine on a project by project basis what documentation needs to be recreated and to what extent.

An example of rolling stock lifecycle model is presented in Figure 2. with rolling stock lifecycle stages reflected on the top of picture. Note that in this version of the diagram the term 'Drawings' is used to represent all of the design documentation such as system specifications, design analyses, calculations, verification matrix, inspection and test plans, test instructions etc.

The light blue shapes represent general activity or deliverables in those processes. General requirements specification, concept design and detailed requirements specification are deliverables of the specification process. Static and dynamic tests are activities conducted in the test & certification process.

The thin arrows with some description indicate potential verification and validation activities that should happen to assess and assure rolling stock definition and integration/implementation.

Configuration change/control gates (CCB) are part of safety assurance of rolling stock. They are reflected at the bottom of the V lifecycle model. Gate 0 is a start gate to ensure project is established properly, that the scope of work is defined, processes have been established, and the team has the right competencies to start the project. Gate 1 to Gate 3 are the rolling stock definition gates to assess safety and to assure that requirements are consideration in design. The RSO may apply an extra gate in between gate 3 and 4 to incorporate the primary approval of the standard compliance register. Gate 4 to Gate 7 are the rolling stock integration/implementation gates established to:

- ensure rolling stock is constructed to approved design;
- assess the constructed new, modified, repaired or overhauled rolling stock meets the systems safety assurance requirements and is safe to operate;
- ensure all systems are integrated;
- assess operational readiness;
- ensure competency of operating and maintaining personnel is up to date;
- ensure RSO’s business is procedurally prepared to accommodate the change;
- assess rolling stock engineering evidence is enough to prepare safety assurance report;
- ensure rail accreditation includes the new, modified, repaired or overhauled rolling stock.

Gate 8 is an RSO’s gate established to assess the rolling stock in operation.
15.1 Specification

Rolling stock requirements are documented in the specification phase and applied to the entire rolling stock lifecycle.

Criteria are to be identified and clearly communicated by the delivery team.

The methods of assessment applicable to each rolling stock project are to be clearly defined in the project scope or specification generally termed the 'Systems Engineering Management Plan' or (SEMP).

The delivery team progressively provides evidence that requirements are met to the ICP/IV and safety assurance team.

The ICP/IV and ISA must be independent of the Project Delivery Team. However, the ICP/IV may also act as the Safety Assurance Team / ISA.

Risk identification and assessment is carried out throughout the life cycle stages.

Project plans and reports may include:

- project safety plans;
- system safety plans;
- safety-change management plans;
- project risk register
- risk assurance reports
- preliminary hazard analysis (PHA)
- final hazard analysis (FHA)
- Failure modes, effects and criticality analysis (FMECA)
- event / failure tree analysis
• human factors integration

The safety assurance team may also have inputs to other engineering plans and reports such as:

• quality assurance plans;
• design management plans;
• verification plans;
• manufacturing plans (manufacturing methodology);
• inspection and test plans (ITP);
• rolling stock certification and compliance plans;
• integration plans;
• commissioning and acceptance plans;
• asset management plans;
• transfer to operation plans: and
• maintenance plans.

15.2 Design

Systems Engineering Management Plan (the ‘SEMP’) specifies: design responsibilities, rules of managing design, management systems to be used in design, design process, required design competency and a requirement for verification.

A design process for each project is clearly defined to ensure the design human errors are minimised and removed wherever possible.

Design is conducted to the specification by qualified and competent personnel.

Design is independently assessed (verification), validated and endorsed. The verifier shall be adequately qualified and competent.

The design is reviewed by the verifier before being presented to the CCB.

Designs can be associated with a design report that communicates safety related implications to the next steps of the lifecycle (e.g. additional risk and hazard definition) as well as allowing the ICP to follow the designers process.

Human factors integration is considered in the design and assessed as part of safety in design. The human factor integration is implemented in the remaining steps of the rolling stock lifecycle.

Parts, components, and systems failure rates are assessed during the design process.

A design compliance certificate should be issued by the design authority at the end of the design process including a list of any non-compliances against the specification. The non-compliances will need to be accepted by the RSO.

15.3 Supply and assembly

The design process should be completed prior to supply and assembly.

A manufacturing plan related to the manufacturing process is produced prior to supply and assembly.
Parts, components, and systems to assemble rolling stock are organised in supply step of rolling stock lifecycle.

The rolling stock Supplier (in consultation with the RSO) is responsible for establishing a supplier selection system that conducts competency assessment, quality assurance, and delivery history. For new suppliers, a verification process is conducted before ordering. As part of the supplier selection system, there are periodical supplier audits performed to assess the quality of goods being supplied.

Each part, component, and system is to be manufactured to the approved design and specified requirements, and each should be associated with a clear asset identification label. The presence of those identification labels is to be assessed before assembly.

Suppliers will provide safety management data sheets for hazardous or restricted materials and any other manuals to minimise hazard at Assembly, operation and maintenance.

Suppliers can provide an evidence that parts/components/systems comply with the design. The evidence is attached to the project requirements management system for assurance team to assess compliance.

Assembly is conducted to an approved rolling stock design by competent personnel. The work is organised and conducted in accordance with regulatory requirements.

The RSO and RSS representatives attend/conduct the first article inspection and any subsequent inspections of rolling stock. An ICP/IV may also be involved in rolling stock inspections.

Specific requirements are made for the supplier to keep records for the lifetime of rolling stock’s specific components.

A construction compliance certificate should be issued by the supplier at the end of each portion, including a list of any non-compliances against the specification and production requirements. The non-compliances will need to be accepted by the RSO. Non-compliances may be against the entire design or individual pieces of equipment.

Rolling stock final inspection will be the system safety assurance mandatory requirement.

15.4 Test and certification

Test and certification process follow the detail in project scope. Inspection and test plan (ITP) are developed prior to testing and certification. Due to the nature of each project, the inspection and test plan (ITP) defines the type of tests to be conducted for new, modified, repaired or overhauled rolling stock as well as describes people conducting testing. For test and certification, the RSO, RSS or RIM may decide to follow standards alternative to AS 7501 or additional requirements.

Testing may comprise both type testing (demonstrating compliance of one article against the specification/ITP) or routine testing (testing each article against the specification/ITP).

A testing certificate should be issued by the testing authority for the type testing, including a list of any non-compliances against the specification and production requirements. The non-compliances will need to be accepted by the RSO.

Routine tests normally for part of the supply documentation.

Any deviation from the original system safety assurance is assessed through a change management process. The process of change management can be defined in the change management plan produced.
at specification. Change management identifies any need for training and any new equipment not used in past operations.

15.5 Integration

Integration is a process established to weld together any separated assets, people, processes and considerations the lifecycle of new, modified, repaired or overhauled rolling stock.

Integration assures rolling stock, future rolling stock operators, operators and maintainers are ready to hand over them new, modified, repaired or overhauled rolling stock.

The safety assurance report (safety case) should be put together by the safety assurance team.

15.6 Commissioning and acceptance

The rolling stock registration process is established by the RIM to assess if the rolling stock is acceptable to operate on their network. The RSO should submit the required documentation. Registration documentation usually is for new rollingstock. For modified, repaired or overhauled rollingstock, due to legacy in processes all documentation may not exist. Documentation may only be required for aspects affected by the change.

The change may affect the RSO’s accreditation. The RSO is responsible for submitting a rail accreditation application to the Office of National Safety Regulator (ONRSR) if there are any changes to the accreditation (i.e. new or modified rolling stock is to be operated on the network).

Any project issues related to improvement of rolling stock project needs to be documented in a lesson learnt log.

15.7 Operation and maintenance

All operation and maintenance personnel’s competencies need to be up to date, including the skillset essential to operate and maintain before new, modified, repaired or overhauled rolling stock is handed to operation.

Operation and maintenance procedures are updated to support new, modified, repaired or overhauled rolling stock. That includes any supplier relevant documentation.

Any existing rolling stock issues that arise during operation and maintenance are noted in the lessons learnt register.