Standard

System Safety Standard for New or Altered Assets

Version 1.0

Issued date: 20 December 2016
Important warning

This document is one of a set of standards developed solely and specifically for use on Transport Assets (as defined in the Asset Standards Authority Charter). It is not suitable for any other purpose.

The copyright and any other intellectual property in this document will at all times remain the property of the State of New South Wales (Transport for NSW).

You must not use or adapt this document or rely upon it in any way unless you are providing products or services to a NSW Government agency and that agency has expressly authorised you in writing to do so. If this document forms part of a contract with, or is a condition of approval by a NSW Government agency, use of the document is subject to the terms of the contract or approval. To be clear, the content of this document is not licensed under any Creative Commons Licence.

This document may contain third party material. The inclusion of third party material is for illustrative purposes only and does not represent an endorsement by NSW Government of any third party product or service.

If you use this document or rely upon it without authorisation under these terms, the State of New South Wales (including Transport for NSW) and its personnel does not accept any liability to you or any other person for any loss, damage, costs and expenses that you or anyone else may suffer or incur from your use and reliance on the content contained in this document. Users should exercise their own skill and care in the use of the document.

This document may not be current and is uncontrolled when printed or downloaded. Standards may be accessed from the Asset Standards Authority website at www.asa.transport.nsw.gov.au.

© State of NSW through Transport for NSW 2016
Standard governance

**Owner:** Manager Safety and Risk Assurance, Asset Standards Authority

**Authoriser:** Principal Manager Safety, Quality, Environment and Risk, Asset Standards Authority

**Approver:** Executive Director, Asset Standards Authority on behalf of the ASA Configuration Control Board

Document history

<table>
<thead>
<tr>
<th>Version</th>
<th>Summary of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>First issue.</td>
</tr>
</tbody>
</table>

For queries regarding this document, please email the ASA at standards@transport.nsw.gov.au or visit www.asa.transport.nsw.gov.au

© State of NSW through Transport for NSW 2016
Preface

The Asset Standards Authority (ASA) is a key strategic branch of Transport for NSW (TfNSW). As the network design and standards authority for NSW Transport Assets, as specified in the ASA Charter, the ASA identifies, selects, develops, publishes, maintains and controls a suite of requirements documents on behalf of TfNSW, the asset owner.

The ASA deploys TfNSW requirements for asset and safety assurance by creating and managing TfNSW's governance models, documents and processes. To achieve this, the ASA focuses on four primary tasks:

- publishing and managing TfNSW's process and requirements documents including TfNSW plans, standards, manuals and guides
- deploying TfNSW's Authorised Engineering Organisation (AEO) framework
- continuously improving TfNSW’s Asset Management Framework
- collaborating with the Transport cluster and industry through open engagement

The AEO framework authorises engineering organisations to supply and provide asset related products and services to TfNSW. It works to assure the safety, quality and fitness for purpose of those products and services over the asset's whole of life. AEOs are expected to demonstrate how they have applied the requirements of ASA documents, including TfNSW plans, standards and guides, when delivering assets and related services for TfNSW.

Compliance with ASA requirements by itself is not sufficient to ensure satisfactory outcomes for NSW Transport Assets. The ASA expects that professional judgement be used by competent personnel when using ASA requirements to produce those outcomes.

About this document

This standard provides requirements for safety engineering and assurance activities when delivering a new or altered asset to TfNSW.

This standard adopts the requirements of TS 20001 System Safety Standard for New or Altered Assets. TS 20001 will be superseded with the publication of this standard.

The requirements of this standard reflect the full scope of Transport Network assets operated and managed by TfNSW.

This document has been approved by the ASA Configuration Control Board and is a first issue.
# Table of contents

1. **Introduction** .................................................................................................................. 6  
2. **Purpose** .......................................................................................................................... 7  
   2.1. Scope .............................................................................................................................. 8  
   2.2. Application ..................................................................................................................... 8  
3. **Reference documents** ..................................................................................................... 9  
4. **Terms and definitions** ...................................................................................................... 9  
5. **System safety governance** ............................................................................................... 11  
6. **Context of change** .......................................................................................................... 12  
   6.1. Safety impact assessment .............................................................................................. 12  
   6.2. Consider operational context ....................................................................................... 13  
   6.3. Assessment of safety risk ............................................................................................ 14  
   6.4. Initial safety interfaces identification ......................................................................... 14  
   6.5. AEO relationships ....................................................................................................... 14  
7. **AEO system safety requirements** .................................................................................. 15  
   7.1. Competency of personnel ........................................................................................... 16  
   7.2. Human factors integration .......................................................................................... 17  
   7.3. Interface management ............................................................................................... 17  
   7.4. Engineering V-life cycle ............................................................................................. 18  
   7.5. Management of change ............................................................................................. 20  
   7.6. System safety planning ............................................................................................... 20  
   7.7. Safety risk management .............................................................................................. 21  
   7.8. System hazard analysis .............................................................................................. 23  
   7.9. Safety risks in commissioning ..................................................................................... 25  
   7.10. Operational readiness ................................................................................................. 25  
   7.11. Control of safety functions implemented by software ............................................... 26  
   7.12. Type approved products ........................................................................................... 26  
   7.13. Defects recording and corrective action system ......................................................... 27  
   7.14. Safety assurance documentation ............................................................................. 27  
   7.15. Safety argument ........................................................................................................ 29  
8. **Acceptance of new or altered assets** ............................................................................. 33  
   8.1. Acceptance of safety significant changes .................................................................... 33  
   8.2. Acceptance of moderate and minor changes ............................................................... 34  
9. **Specific asset requirements** ............................................................................................. 34  
   9.1. Rail asset specific requirements ................................................................................... 35  
   9.2. Bus asset specific requirements .................................................................................. 36  
   9.3. Maritime asset specific requirements .......................................................................... 36  
   9.4. Road infrastructure asset specific requirements ......................................................... 36  
   9.5. Specific requirements for other asset types ................................................................ 36  

© State of NSW through Transport for NSW 2016
1. Introduction

TfNSW has a varied asset portfolio of fixed infrastructure assets and mobile assets supporting the transport modes. The transport modes, as defined in T MU AM 02001 ST Asset Information and Register Requirements are road, rail, maritime, air and active. These individual assets combine along with the operational processes and personnel to form subsystems, which in turn form the modal transport system. These modal systems do not operate in isolation. They combine to form the NSW Transport Network. Changes to assets, their operational processes or the personnel that operate them directly impact the safety of the subsystem in which they operate, and can also impact the modal transport system and wider NSW Transport Network.

Figure 1 illustrates the relationship of assets, subsystems, modal transport systems and NSW Transport Network.

![Figure 1 - Relationship of assets, subsystems, modal transport systems and NSW Transport Network](image)

TfNSW has a duty to ensure, so far as is reasonably practicable (SFAIRP), the safety of the Transport Network, its assets and their operations.

These duties are necessitated by the following laws:

- *Work Health and Safety Act 2011*
To achieve these duties whenever new assets are introduced, or existing assets are modified, upgraded or removed TfNSW needs to ensure the following:

- operational safety risks are identified, assessed and managed with new or altered system or assets, when operating as an integrated part of the Transport Network
- sufficient evidence is provided to demonstrate a safety argument that the new or altered system or asset has achieved the following:
  - designed to best ensure safety SFAIRP during its operation
  - manufactured or constructed and transitioned into the Transport Network in a manner which best ensures safety SFAIRP
  - reduced all foreseeable safety risks SFAIRP

The AEO contracted to deliver the change to the new or altered system or asset is accountable for conducting activities and providing assurance evidence to demonstrate that these duties have been achieved in accordance with this standard.

All entities involved in the delivery of new or altered systems and assets have a responsibility to manage safety outcomes under their control.

2. **Purpose**

This standard describes the system safety requirements placed upon AEOs delivering a change to the Transport Network. It also provides the requirement for AEOs to provide suitable and sufficient supporting assurance evidence that enables TfNSW and the Transport Network operators to meet their duties under legislation.

TfNSW and the Transport Network operators meet their specific duties under the legislation to ensure that safety is managed SFAIRP by relying on the assurance activities and evidence provided by the AEOs. These assurance activities and evidence enable a determination to be made by the configuration management asset assurance committee (CMAAC) or delegated configuration control board (CCB) that informs the client representative in their role of accepting assets and risks.

Where a transport mode does not have AEOs assigned the supplier is required to assure the engineering service, assets or change to provide evidence that the delivered assets, service or change ensure safety SFAIRP and ensure that the transport network meets, or continues to be safe SFAIRP. As such this document is applicable to non-AEO suppliers and engineering service providers. TfNSW may engage an engineering service provider, in which case the
requirements placed upon the AEOs by this standard shall be applicable by the engineering service provider.

2.1. Scope

This standard sets out the requirements for system safety engineering and assurance activities to be conducted in support of the introduction of new or altered assets into the TfNSW Transport Network.

This standard provides the following:

- safety assurance requirements which the AEO complies to assure the safety of new and altered assets for the Transport Network for its complete life cycle
- requirements that enable a determination to be made by the CMAAC, or delegated CCB, that informs the client representative in their role of accepting assets and risks into the Transport Network through the provision of suitable and sufficient safety argument, supported by evidence

The standard supports the overall TfNSW asset acceptance process, but does not define that process. This standard sets system safety requirements for the engineering services provider to support the TfNSW safety acceptance requirements.

The standard is also consistent with the requirements of the TfNSW safety management system with respect to safety change management and safety risk management.

The requirements in this standard are not criteria that an organisation needs to meet to be authorised as an AEO, they are the requirements that should be followed by an AEO under contract. There are related criteria for authorisation identified in the document T MU MD 00009 ST AEO Authorisation Requirements.

2.2. Application

This standard applies to all changes that affect Transport Network systems or its assets. It applies to all AEOs delivering asset change, their suppliers and other organisations involved in defining, designing, implementing, commissioning and transitioning into the Transport Network new or altered assets or systems, or the decommissioning and disposal of assets. It also applies to changes to assets, changes to the way assets are operated, provision of new assets by operating and maintaining organisations authorised as an AEO.

This standard aligns with CP14005.1 Transport Asset Management Policy by following the life cycle defined and developing details of the requirements for system safety management and assurance.
3. Reference documents

The following documents are cited in the text. For dated references, only the cited edition applies. For undated references, the latest edition of the referenced document applies.

Transport for NSW standards

20-ST-006 Safety Change Management Standard (available on request from standards@transport.nsw.gov.au)
T MU AM 02001 ST Asset Information and Register Requirements
T MU AM 04001 PL TfNSW Configuration Management Plan
T MU HF 00001 ST Human Factors Integration – General Requirements
T MU MD 00004 TI Independent Safety Assessor (ISA) Requirements (Interim)
T MU MD 00005 GU Type Approval of Products
T MU MD 00009 ST AEO Authorisation Requirements
T MU MD 20000 GU Risk Tolerability, Quantified Risk Assessment and its Role in the Assurance of Change
T MU MD 20002 ST Risk Criteria for use by Organisations Providing Engineering Services

Legislation

Marine Safety (Domestic Commercial Vessel) National Law Act 2012
NSW Work Health and Safety Act 2011
Rail Safety (Adoption of National Law) Act 2012

Other references

20-FT-388 Initial Safety Change Assessment (available on request from standards@transport.nsw.gov.au)
ASA Charter
CP14005.1 Transport Asset Management Policy (available on request from standards@transport.nsw.gov.au)

4. Terms and definitions

The following terms and definitions apply in this document:

AEO Authorised Engineering Organisation; a legal entity (which may include a Transport Agency as applicable) to whom the ASA has issued an ASA Authorisation

ASA Asset Standards Authority
CCB configuration change board

client representative the division of TfNSW that represents the client, the Secretary TfNSW

CMAAC Configuration Management and Asset Assurance Committee

competence the identification and application of knowledge, skills and behaviours required to perform tasks to the standards required. Competence is a combination of practical and thinking skills, experience and knowledge and includes a willingness to undertake work activities in accordance with agreed standards, rules and procedures. It embodies the ability to transfer and apply skills and knowledge to new situations and environments

development and implementation the life cycle phases from feasibility to entry to operation in the context of the introduction of new or altered assets to the Transport Network

hazard log the continually updated record of the hazards, accident sequences and accidents associated with a system. It includes information documenting risk management for each hazard and accident (DEF STAN 00-56 (PART 1)/4)

independent safety assessment a series of assessment and audit activities of the safety management, safety engineering and safety assurance activities, processes and deliverables conducted by an ISA.

integrating AEO the AEO responsible for providing the complete operational safety argument, comprising of elements provided either whole by themselves, or including other engineering services providers delivering the change which may or may not be AEOs

IPR independent professional review; an independent SME review of an element of the new or altered asset change. Typically an independent review of an element of the design to support the overall safety argument.

ISA independent safety assessor; an independent ISA AEO with the competency to provide rigorous oversight of safety processes, and assert an opinion of the safety of the new or altered asset (T MU MD 00004 TI)

new or altered assets the changes made to the Transport Network other than those as a result of maintenance activities, including decommissioning and removal of assets from the rail network. Maintenance activities are considered those made by AEOs with authorisation for maintenance activities and conducted under that authorisation scope.

operational safety argument a structured documented safety argument, supported by evidence, providing explicit assurance of the safety of an asset or system for the life of the asset within its intended operational environment

reduce SFAIRP reduce the risk using the hierarchy of controls

• eliminate
• substitute
• engineering controls
• administrative controls
• personal protective equipment (PPE)

residual risk any risk identified and reduced SRAIRP, but not eliminated through the V - life cycle

SFAIRP so far as is reasonably practicable

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 throughout the life cycle of a system or asset

TfNSW Transport for NSW

validation confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

verification confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

5. System safety governance

The requirements in this document shall be followed in order to enable CMAAC or delegated CCB to make a determination of the new or altered asset; this determination informs the subsequent acceptance by client representative.

Where a number of organisations are involved in a change, an integrating AEO shall be nominated. The integrating AEO is accountable for the overall delivery of appropriate safety assurance activities (within design, manufacture, construction and transition) and the operational safety argument to the CMAAC or delegated CCB. All supporting organisations are required to comply with this standard, in support of that argument.

Safety significant changes require an independent safety assessment be completed by an independent safety assessor (ISA). An ISA organisation shall be authorised as an ISA by the ASA. TfNSW may additionally stipulate the appointment of an ISA where the AEO scope does not cover the change activity or if the entity making the change is not an AEO. The ISA assessment provides a professional opinion that the change has been undertaken with an appropriate safety assurance process and confirms the validity of the safety statements and arguments provided by the integrating AEO, demonstrating safety risks have been reduced SFAIRP, supporting the acceptance of the asset of the client representative. Refer to T MU MD 00004 TI Independent Safety Assessor (ISA) Requirements (Interim) for further information on ISA authorisation.
6. **Context of change**

In order to effectively manage the risks associated with the safety change, the operational context, boundaries, interfaces, organisational safety change structure and responsibilities for the change to the new or altered system or asset shall be clearly defined and understood. The initial safety change impact assessment provides the primary input to the change assurance process; this is subsequently supported and enhanced by further risk assessments throughout the life cycle of the change.

6.1. **Safety impact assessment**

The instigator of the change shall complete an impact assessment of the change. This assessment shall identify all risks associated with the change in accordance with the criteria defined in 20-ST-006 Safety Change Management Standard and 20-FT-388 Initial Safety Change Assessment. As shown in Figure 2, the assessment shall define the change as one of the following:

- minor safety change
- moderate safety change
- safety significant change

*Note: By definition, a change to an asset or system will have a safety impact, thus a category of 'no safety change' cannot be applied to changes to assets or systems.*

The risks identified within the safety impact and subsequent risk assessments shall drive the detail and volume of safety assurance activities throughout the engineering V-life cycle.

![Figure 2 - Safety significance of change](image-url)
6.1.1. Changes instigated by TfNSW

TfNSW will complete an impact assessment of the change of introducing new or altered assets to the Transport Network prior to awarding contracts to the development and implementation of the proposed change. The contracted entity delivering the change will be advised of the assessment outcome.

The safety impact assessment is required and defined by the TfNSW safety management system (SMS) document, 20-ST-006. The assessment considers the complexity, novelty and failure consequences of the change. There are three potential levels of change - minor, moderate or safety significant. Throughout this standard, requirements are identified as being applicable to either of the following:

- safety significant or moderate
- minor changes

Where neither is specified, the requirements shall be applied to all changes in proportion to the risks identified with the change.

6.1.2. Changes instigated by maintaining AEOs

When a maintaining AEO instigates a change, a safety impact assessment shall be completed in accordance with the criteria defined in 20-ST-006 and 20-FT-388 to identify key safety risks that need to be addressed during the change process.

The safety impact assessment shall identify the following:

- context of the change
- worst case credible safety outcome associated with the failure of this change

The safety impact assessment shall assess the following:

- complexity of the change
- novelty of the change
- reversibility of the change

The risks identified during the safety impact assessment shall be controlled throughout the change by the planning and application of safety assurance activities in accordance with this standard.

6.2. Consider operational context

Entities delivering change involving new or altered assets to the Transport Network shall recognise that the asset or system will be part of an operating system with interfaces to passengers, operating staff, the general public and other workers. It is therefore essential that
the application of this standard includes consideration of the asset or system in its operating context and not just as a physical system.

6.3. **Assessment of safety risk**

The outcomes of safety risk assessments shall be expressed using the criteria of the owner of the risk.

The owner of the risk will generally be the asset owner. Residual safety risks shall be reported against the appropriate risk owner's risk matrix. In some cases the residual safety risks will be owned by TfNSW, in which case the risks shall be expressed in accordance with the risk criteria used by the organisations providing the engineering services in accordance with T MU MD 20002 ST *Risk Criteria for use by Organisations Providing Engineering Services*.

In order to establish the owner of the residual safety risks, the integrating AEO shall engage all relevant stakeholders, subject matter experts (SMEs) and external expertise.

When conducting safety risk assessments the AEO shall take into account the means of demonstrating SFAIRP within the safety management system (SMS) of the owner of the risk.

6.4. **Initial safety interfaces identification**

The entity instigating the change shall identify safety interfaces, stakeholders, and put in place controls to reduce risk SFAIRP.

6.4.1. **Changes instigated by TfNSW**

When TfNSW instigates a change it shall define the systems safety requirements, identify stakeholders, the contracting arrangements, and engage AEOs with an appropriate capability to assure the change. This organisational safety change structure is defined within the project safety change management plan.

6.4.2. **Changes instigated by maintaining AEO**

When a maintaining AEO instigates a change, they shall identify the stakeholders and manage any contracting arrangements that enable the assurance of the new or altered asset in accordance with this standard.

6.5. **AEO relationships**

The organisational safety change structure will vary according to factors such as the complexity of the change, commercial arrangements, and the relative capabilities of the AEOs. The ASA *Charter* describes the potential contracting arrangements with AEOs.

TfNSW prefers to engage the Authorised Engineering Organisations (AEOs), as their processes have been assessed as appropriate. Where a non-AEO completes the assurance activities they
shall be authorised by TfNSW, meet the requirements of this standard, and additional controls shall be put in place by TfNSW in accordance with 20-ST-006 Safety Change Management Standard.

A single AEO may be appointed. This single AEO can act as an integrating AEO or an integrating AEO may be appointed to provide the operation safety argument for the complete activity, including assuring the assurance activities of other AEOs and suppliers.

For changes assessed as 'safety significant' the integrating AEO is required to develop an operational safety argument for the development and transition of the change into the Transport Network. An independent assessment of the operational safety argument shall be conducted by an authorised independent safety assessor (ISA). TfNSW shall determine the overall safety assurance program including whether to appoint the independent safety assessor either directly or direct the integrating AEO to appoint the ISA.

For changes assessed as 'moderate' or 'minor' the integrating AEO shall lead the safety risk assessment and deliver the assessment of residual safety risks to the CMAAC or delegated CCB where required. The integrating AEO shall ensure that appropriate independent validation of safety related activities are conducted of high risk elements in the development and implementation life cycle; this may include the appointment of an ISA.

7. AEO system safety requirements

The following are the key objectives of system safety:

- to integrate safety into the design and development of new or altered assets such that the delivered systems are safe SFAIRP
- to deliver a documented operational safety argument supported by evidence, demonstrating the safety of the system

The integrating AEO shall plan and implement a program of system safety activities. Where appropriate, the system safety activities should be aligned with the engineering life cycle defined in TS 10504 AEO Guide to Engineering Management. The program shall be proportional to the level of risk and ensure that operational safety is integrated into the designed and delivered system and provide suitable and sufficient assurance of the operational safety of the system throughout its intended life.

AEOs shall have management systems in place to support safety assurance activities for changes to the Transport Network as defined within T MU MD 00009 ST.

Key safety assurance attributes include the following:

- competency management of personnel
- human factors integration
interface management
- engineering V-life cycle
- management of change
- system safety planning
- safety risk management
- system hazard analysis
- management of safety risks in commissioning
- operational readiness
- control of safety functions implemented by software
- defects recording and corrective action
- management of safety assurance documentation
- development of a safety argument

7.1. Competency of personnel

Organisations that develop and implement changes require competent persons to exercise sound, professional judgements and successfully apply a safety assurance approach to the management of change. AEOs shall have a competency management system in place to assure work is performed by suitably competent personnel, that is, personnel designated as being ‘competent’ persons.

Persons deemed to be competent in safety management shall be able to demonstrate the following:
- experience in the technical, operational or organisational field which the person is assessing
- experience and knowledge of application of the tools used in both system safety, and reliability, availability and maintainability management

Persons deemed to be competent in human factors shall meet the requirements of T MU HF 00001 ST Human Factors Integration – General Requirements.

The competence of the safety management resources used should be demonstrated within the operational safety argument.
7.2. **Human factors integration**

Human factors shall be integrated into the design and development process of new or altered assets in order to minimise risk from the possibility of human-system related issues as it requires the following:

- human characteristics are accounted for in the design or re-design of new and existing systems and equipment
- the issues which may cause or contribute to human errors are identified
- activities and the application of controls are conducted to reduce likelihood and consequences of human-system related issues

Human factors integration shall meet the requirements of T MU HF 00001 ST.

7.3. **Interface management**

Poorly managed interfaces are a common source of safety risk. The AEO shall demonstrate its approach for managing interfaces. For 'safety significant' changes this shall be documented in the system safety plan.

The AEO approach for managing interfaces shall include external and internal system interfaces and include identification and management of foreseeable safety risks associated with transition of subsystems into the overall system.

Safety requirements associated with the interfaces shall be identified, documented and implemented. The network architecture provides details of interfaces within the network and, where available, should be used as a source of information when managing the safety of interfaces.

The integrating AEO shall demonstrate that safety at the interfaces are ensured SFAIRP, and all possible activities and actions to ensure the safety of interfaces have been undertaken SFAIRP.

The AEO shall demonstrate that the safety of interfaces have been managed right through to entry to operation, as well as in operational controls and maintenance requirements for the operational life of the asset or system.

Where subordinate AEOs or suppliers require information to meet a particular safety requirement, the integrating AEO shall identify and provide the necessary information to allow interfaces between subsystems or elements of the system to be safely implemented and demonstrated to be safe.
7.4. **Engineering V-life cycle**

System safety activities shall be conducted in alignment with the engineering V-life cycle. The key objective of the system safety activities is to ensure the integration of safety into the design, construction, implementation, commissioning and transition of a change. This can only be achieved if system safety activities are aligned with the engineering life cycle. The alignment also provides progressive assurance, so that there can be confidence that safety in operation has been integrated into the system SFAIRP at each stage of the life cycle.

AEOs shall have processes to plan and complete system safety activities (in conjunction with the systems engineering activities) in place as required by T MU AM 06006 ST *Systems Engineering Standard*. Figure 3 shows engineering V-life cycle including the definition of safety requirements and the verification and validation that those requirements have been achieved.
Figure 3 - TfNSW systems engineering V-life cycle model
7.5. **Management of change**

Change occurs at the following two levels:
- overall change of incorporating new or altered assets into the Transport Network
- changes made within a project delivering new or altered assets

Risk needs to be reduced SFAIRP as part of these changes.

7.5.1. **Overall change**

This standard defines the overall approach to system safety engineering and assurance activities to assure new or altered assets. AEOs shall apply these requirements when incorporating new or altered assets into the Transport Network.

7.5.2. **Change within a project**

Within any project there will be changes that can potentially impact safety. It is important that such changes are managed appropriately and that their impact on safety is understood. Such changes may occur once the design is predominantly complete and implementation is in progress. It may be necessary to change the design to address specific implementation issues. It is important to control change so that the assurance of the designed system remains valid.

The integrating AEO shall establish and maintain a change control system so that the impact of any planned or unplanned change is identified and assessed for its impact on safety.

Where the impact assessment finds it necessary, remedial action shall be taken to ensure the safety of the system. The change control system shall produce evidence to demonstrate that the risk of change has been reduced SFAIRP.

7.6. **System safety planning**

System safety activities shall be planned so that they support the development of a suitably safe system and provide the assurance needed to demonstrate the safety of the system. This plan shall be documented in a manner proportional to the level of risk. A system safety plan is required for ‘safety significant’ changes. The planning of safety activities also supports the application of robust safety management processes for the development and implementation of the new or altered asset.

The planning should define how the hazard identification and management activities support the development of the system through the identification, implementation, verification and validation of safety requirements. It shall ensure that the system safety activities are aligned with the engineering V-life cycle so that system safety is properly integrated into the system engineering.
The planning process should also identify how human factors will be addressed by the engineering of the system, specifying the human factors activities to be undertaken.

The planning process shall include stakeholder consultation and reviews. The review shall note how stakeholders have come to accept that the system is suitably safe at key milestones in the V-life cycle.

It is essential that the planning process addresses stakeholder consultation and reviews, and how key stakeholders review and accept that the system is suitably safe at key milestones in the V-life cycle. The planning process shall also identify the documentation and evidence that will be prepared to assure the safety of the new or altered asset once operational.

7.7. Safety risk management

AEOs and suppliers shall implement a level of safety risk management appropriate to the foreseeable risks of the change, in order to evidence that all safety risks are reduced SFAIRP. This requires the holistic risk and each reasonably foreseeable individual risk be identified and reduced SFAIRP.

Safety risks shall be identified and fully managed and aligned with the V-life cycle. The safety risk management process implemented by AEOs shall address the full intended operational life of the new or altered asset or system.

AEOs shall employ suitable and sufficient hazard identification, hazard analysis and hazard management techniques, and demonstrate this in the operational safety argument or risk summary report. All analysis results shall be documented and referred to as evidence.

7.7.1. Hazard Identification

The integrating AEO shall systematically and continually identify all reasonably foreseeable hazards for the entire system under consideration, including all its functions and interfaces across its full intended life.

Appropriate structured and systematic methodologies should be used, and shall incorporate input from subject matter experts (SMEs) and stakeholders.

Hazard identification shall consider the following:

- the scope and boundary of the system and its operational interfaces
- all system modes of operation including degraded modes
- all potential locations where the system will be operated
- the potential for human error, including human error from an operator, maintainer, passenger or member of the public
- interfaces, both internal and external
• environmental conditions
• all foreseeable failure modes for the system at the module, subsystem and system level, and their impact on safety
• previous performance of the asset
• other potential factors that are safety relevant to the system under consideration

All identified hazards shall be entered into the hazard log for management and assessment.

7.7.2. Hazard management

The integrating AEO shall develop and implement a suitable and sufficient hazard management system that includes a hazard log.

The hazard log is a central repository of identified hazards that facilitates their management throughout the engineering V-life cycle. All hazards not eliminated within development and implementation phase shall be entered into an operational risk register along with their associated controls, in support of the operational safety argument. These residual risks shall be transferred to the risk owner and entered into the operational risk register of the risk owner for ongoing management through the operational life.

An operational risk register is a register of risks that have been identified, but not eliminated during the development and implementation phase, and are thus being transferred to the operate and maintain phase. The register shall include the controls agreed with TfNSW, Transport Authority and the operator.

For 'safety significant' changes the details of the hazard management system shall be documented in the system safety plan.

The integrating AEO shall ensure that all identified hazards are entered into the hazard log and managed appropriately within the log.

The hazard log shall be the primary artefact for providing traceability within the safety risk management process and assurance of the effective management of safety risk. It shall include traceability to all supporting evidence including verification and validation evidence related to each safety requirement.

The hazard log shall be updated and maintained through the development and implementation of entire life cycle phases, to make sure that it accurately reflects safety risk management activities.

Where multiple AEOs or suppliers are required to manage hazards, a hierarchy of hazard logs may be required. The integrating AEO shall develop a suitable and sufficient methodology for management of hazards at each level of the system and subsystems, providing clear tractability to subordinate hazard logs and a demonstration that all safety risks in the top level hazard log are managed to tolerable and SFAIRP. Refer to Figure 4 for a diagram showing relationship
between the Integrating AEO hazard log, operation risk register and subordinate hazard logs from sub-suppliers.

![Figure 4 - Hazard log hierarchy](image)

### 7.8. System hazard analysis

In order to assign and demonstrate appropriate hazard control SFAIRP, it is necessary to understand all the ways that hazards can be caused. A systematic process of identifying the causes shall be undertaken. Identified causes shall be entered into the hazard log and linked to the hazard.

#### 7.8.1. Safety risk assessment

The AEO shall conduct an assessment of the safety risk for each identified hazard against the appropriate risk criteria. This shall include assessing the severity of the consequences if the risk occurs and the likelihood of that consequence occurring.

When assessing the consequences, the worst-case credible consequence shall be used for the risk assessment.

The AEOs shall consider appropriate safety controls for each safety risk so that the safety risks are reduced SFAIRP.
When evaluating the suitability of controls, the hierarchy of controls shall be applied so that safety risk or hazards are eliminated by design where this is reasonably practicable.

Where a hazard cannot be eliminated it shall be controlled to tolerable and SFAIRP in accordance with T MU MD 20000 GU Risk Tolerability, Quantified Risk Assessment and its Role in the Assurance of Change. The hierarchy of controls shall be considered in descending order and in consultation with all impacted parties (including constructors, operators and maintainers).

The integrating AEO shall set up governance arrangements for the review and closure of identified safety risks and hazards. These arrangements shall involve appropriate stakeholders and subject matter experts (SMEs) in the review and closure of hazards.

The setting of the governance arrangements shall be cognisant of where the ownership of the safety risk will reside once the system or asset is in operation, and the acceptability of the residual risk to that ultimate owner.

For 'safety significant' changes the operational safety argument shall demonstrate the effectiveness of the hazard and safety risk management process.

### 7.8.2. Safety requirements and evidence

Safety requirements arise from a number of sources including legislation, requirements placed on an AEO, and the hazard identification and analysis process. The integrating AEO shall have processes for identifying and managing safety requirements throughout the asset life cycle including safety requirements which shall be derived from the hazard analysis.

Deriving safety requirements from the hazard analysis and incorporating them into the system design is a key link between safety and engineering processes. The safety and hazard analysis work shall be programmed in alignment with the engineering activities to ensure that resulting safety requirements are integrated into the design enabling a design solution to be reached that is safe SFAIRP.

The system for identifying and managing safety requirements through the asset life cycle shall be capable of maintaining records to show traceability between each safety requirement and its source. The risk controls arising from the safety risk management process should be treated as safety requirements.

The AEO shall provide complete and objective evidence that each safety requirement and its integrity target has been met, either in the operational safety argument for 'safety significant' changes, or the risk summary report.

The volume of the evidence that each safety requirement has been met shall be commensurate with the degree of safety risk reduction resulting from the safety requirement.

For controls that provide significant risk reduction, or a control that is the single or principal control against a high consequence hazard, diverse evidence of meeting the safety requirement
shall be provided, so that the safety argument is not compromised by uncertainty or errors in individual pieces of evidence. It is preferential not to rely on single-point controls.

7.9. **Safety risks in commissioning**

Where testing and commissioning is conducted in or may impact the live Transport Network, it is necessary to assure the safety of the Transport Network during those activities. The AEO for the testing and commissioning activities shall conduct hazard identification and safety risk assessment for all activities that can affect the integrity or operation of the Transport Network. The approach to managing the identified risks shall be documented within a testing and commissioning safety assurance plan.

The hazards identified as possibly affecting the integrity or operation of the Transport Network during testing and commissioning shall be documented and managed within a hazard log and shown to be reduced SFAIRP.

In order to facilitate a determination of the testing and commissioning activities by the CMAAC or delegated configuration control board, the integrating AEO shall present a testing and commissioning safety assurance plan. The plan shall provide evidence that all foreseeable safety risks associated with the commissioning activities have been identified and reduced SFAIRP.

Before presenting a testing and commissioning safety assurance plan to the CMAAC or delegated CCB, the integrating AEO shall have gained input from stakeholders, and demonstrate that key stakeholders and risk owners support the testing activities based on the assurance provided.

Prior to commencing testing activities, acceptance of the testing and commissioning safety assurance plan shall be obtained from the client representative.

7.10. **Operational readiness**

A key element of assuring the operational safety of a new or altered asset is the demonstration that the operator is ready to operate the asset within the operational environment.

The integrating AEO is accountable for assuring operational readiness. The operator and maintainer will conduct operational readiness activities to ready their network for the new or altered asset. They will ensure adequate resources, training and procedures are in place for safe operation, and provide evidence to the AEO for inclusion in the operational safety argument.

The integrating AEO shall work closely with the operator and maintainer to make sure that the operator and maintainer fully understand what is required for the new or altered asset or system to be operated. The AEO also needs to understand the requirements of the operator and maintainer in terms of information and evidence to support their operational readiness activities.
The AEO shall engage with all relevant stakeholders to gain assurance that the operator and maintainer are operationally ready for the new or altered system to enter operations within the network.

The AEO shall provide evidence of this operational readiness, either in the operational safety argument for 'safety significant' changes or in the risk summary report.

**7.11. Control of safety functions implemented by software**

Software is used in many systems to implement safety functional requirements. Where an AEO is designing or supplying a system that involves software implementing safety related functions, these functions need to be appropriately managed and assured in accordance with an appropriate international standard or equivalent agreed standard with the client representative.

In order to manage and assure the safety of systems that involve software, the AEO shall allocate a safety integrity level (SIL) or equivalent to each safety-related function. During the verification and validation stages, the AEO shall demonstrate that the SIL for each safety-related function has been achieved by suitable means.

**7.11.1. Assurance of safety software integrity compliance**

Throughout the design phase and during the inspection and testing, and commissioning phases, the software development process shall be validated as complying with the required target SIL. Appropriate assurance shall be provided to support the validation of safety integrity level compliance.

The organisation responsible for the software development, or having the software developed for transition into the overall system, shall provide the assurance of safety integrity level.

Where a commercial off-the-shelf system implements safety functions in software, a suitable and sufficient argument shall be developed to provide assurance that these functions are implemented to the necessary level of integrity.

The integrating AEO shall ensure that suitable due diligence of the assurance of functions implemented by commercial software is undertaken to support the operational safety argument to be presented to the CMAAC or delegated CCB.

**7.12. Type approved products**

AEOs of new or altered railway infrastructure assets may use type approved products as part of the demonstration of the operational safety argument.

Type approval of a product provides the following benefits:

- process efficiency (do once and use many times)
- assurance of compatibility to existing networks and interfaces
• assurance of technical compliance with ASA standards
• assurance as part of the assurance and governance plan
• reduction of risk to system reliability, availability, maintainability and safety (RAMS)
• introduction of a new product that provides the same functionality as another type approved product

When an AEO uses the type approval approach and makes a type approval submission, it shall have in place processes to demonstrate type approval in accordance with T MU MD 00005 GU Type Approval of Products.

Note: T MU MD 00005 GU only supports railway infrastructure equipment, component, system and subsystems.

Where type approval is used as part of the operational safety argument, the integrating AEO shall consider the following:

• conditions of the type approval detailed on the type approval certificate
• context in which the type approved equipment is proposed to operate

7.13. Defects recording and corrective action system

The integrating AEO shall operate a defect recording system that captures defects during the development, implementation and early operation of the new or altered asset. Each defect shall be assessed for impact on safety.

Where the impact assessment identifies a safety risk, appropriate remedial action shall be identified, completed and verified to reduce safety risks SFAIRP. The defect recording system shall produce evidence to demonstrate that the risks associated with the identified defect have been reduced SFAIRP.

7.14. Safety assurance documentation

The AEO shall progressively generate safety assurance documentation throughout the engineering life cycle.

The following safety assurance documents as listed in Table 1 are required by this standard:

• System safety plan: This document shall demonstrate the planned approach and define roles and responsibilities to the safety assurance of the change.
• Safety change hazard log: This document shall detail the identified risks, their mitigation controls and associated evidence that those controls have been effective.
• Testing and commissioning safety assurance plan (where activities are to take place in, or have potential to impact the live Transport Network): This document shall demonstrate the
planned approach to reducing safety risks SFAIRP of any testing and commissioning activities in the operational Transport Network.

- Operational safety argument (including operational risk register): This document shall affirm that safety of the Transport Network has been assured SFAIRP during the engineering life cycle, through the evidencing that the identified hazards have been controlled.

The content and detail contained within each safety assurance document shall be proportionate to the level of risk. Where the change is 'safety significant' the documentation shall be provided to support CMAAC gate determination.

Table 1 details the requirements and timing for each of the required safety assurance documents.

<table>
<thead>
<tr>
<th>Document</th>
<th>Change type</th>
<th>Scope</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>System safety plan</td>
<td>Safety significant</td>
<td>Demonstrate the planned approach to safety assurance during the engineering V-life cycle, including roles and responsibilities for those involved with the change. The plan may be supported by sub-plans covering phases of the V-life cycle, such as design and construction.</td>
<td>CM gate 1 and at regular reviews</td>
</tr>
<tr>
<td>ISA plan</td>
<td>Safety significant</td>
<td>Demonstrate the planned approach for conducting the work, setting out the approach to proactive assessment and analysis of the customer’s engineering process and life cycle as it is executed during system development.</td>
<td>CM gate 1</td>
</tr>
<tr>
<td>Hazard log</td>
<td>Safety significant</td>
<td>Evidence of the identified risks, their mitigation controls, and associated evidence that those controls have been effective in reducing risk SFAIRP.</td>
<td>CM gate 1 to gate 6</td>
</tr>
<tr>
<td>ISA summary report</td>
<td>Safety significant</td>
<td>Detailing current independent safety assessment progress, open concerns and overall confidence in the safety assurance activities.</td>
<td>CM gate 1 to gate 6</td>
</tr>
<tr>
<td>Testing and commissioning safety assurance plan</td>
<td>Safety significant</td>
<td>This sub-plan to the system safety plan demonstrates the planned approach to safety assurance within any testing and commissioning activities where those activities are competed within or have an impact with the live operating environment. The content of this plan may be included within the system safety plan, depending on the risk profile and AEO’s approach.</td>
<td>Prior to any testing or commissioning that may impact the live Transport Network</td>
</tr>
</tbody>
</table>
7.15. Safety argument

The culmination of the planned systems safety assurance activities is a safety argument, which provides explicit assurance of the safety of the asset or system for the life of the asset, within its intended operational environment. The safety argument provides the following:

- demonstration that suitable and sufficient safety management activities have been conducted to assure the safety of the change
- demonstration that safety has been ensured SFAIRP
• explicit description and assessment of all residual safety risks (within the operational risk register) that TfNSW or the operator will be exposed to during the operating life of the asset, including demonstration that all safety criteria have been met, and that all safety risks are reduced SFAIRP. The owner of each risk shall be identified.

The safety argument shall be documented within an operational safety argument for ‘safety significant’ or ‘moderate’ changes, or a risk summary report for ‘minor’ changes.

7.15.1. Operational safety argument

For 'safety significant' changes, the integrating AEO shall provide an operational safety argument, which demonstrates the safety of the delivered asset.

The operational safety argument shall demonstrate the following:

• it is a structured argument based on a suitable technique for structuring safety arguments, for example, goal structuring notation (GSN)
• it clearly defines the scope of operations for which safety is demonstrated and clearly defines the operational limitations of the delivered system
• sound safety management and quality management principles have been applied throughout the design, development, implementation and commissioning of the asset
• all reasonably foreseeable safety risks in operation have been identified and reduced SFAIRP, including evidence that the hierarchy of controls has been applied
• explicitly describes all residual safety risks for operation and identify ownership of those residual risks
• arrangements are in place to support and maintain the same level of safety throughout the asset's life
• interfaces between all subsystems have been appropriately managed, and that safety risks at the interfaces have been identified and appropriately managed
• human factors have been considered in the design and development of the system, so that the potential for human error has been minimised SFAIRP, and the asset is suitably operable and maintainable
• foreseeable safety risks with the transition of the asset into the operating Transport Network, and that maintenance and disposal requirements have been identified and will be appropriately managed
• the reliability, availability and maintainability of the new or altered asset has been ensured to be sufficient
• appropriate stakeholder management and input has been conducted to give confidence that all stakeholders requirements will be met
sufficient liaison with the operator has been conducted so that the operator is operationally ready to enter the system into operation

appropriate safety requirements have been defined to adequately control the identified safety risks using supporting evidence

all safety requirements have been verified and validated with reference to supporting evidence

a corrective action process has been applied throughout the design, implementation and commissioning life cycle

7.15.2. Risk summary report

For 'minor' and 'moderate' changes the AEO shall prepare a risk summary report to support a determination of safety by CMAAC.

The risk summary report shall include the following:

- identification of all reasonably foreseeable safety risks in the operational environment
- justification that all reasonably foreseeable safety risks in the operational environment have been reduced SFAIRP
- a statement justifying that all risks identified have been reduced SFAIRP
- explicit descriptions of all reasonably foreseeable safety risks during operation and maintenance, identifying ownership of those risks and the controls in place to manage those risks

7.15.3. Design safety argument

For 'safety significant' and 'moderate' changes a design safety assurance report (SAR) shall be prepared and submitted to CMAAC or the delegated CCB before the final design phase gateway. The design safety assurance report shall document the design safety argument and be supported at the CMAAC or delegated CCB by the ISA.

The design safety argument shall demonstrate that all identified safety risks have been eliminated during the design phase. For those risks that cannot be eliminated, the design safety argument shall have controls identified that reduce the safety risk SFAIRP. Where administrative controls are used, the controls shall have been agreed with the risk owner.

The content of the design safety assurance report shall be as for the operational safety argument but adapted to this stage of the life cycle.

For 'minor' changes risk and controls within the design phase shall be managed within the safety hazard log.
8. Independent safety assessment and due diligence

It is the responsibility of the AEOs to provide suitable and sufficient assurance that the new or altered assets being developed for the Transport Network will be sufficiently safe in operation. This assurance may be supported by an independent professional review of elements of the change by a suitably independent and competent SME, or by an assessment of the complete change by an ISA. The approach to independent safety review shall be defined within the system safety plan.

8.1. Safety significant changes

For 'safety significant' changes, the requirement for the overall independent safety review is met by the appointment of an ISA. An ISA shall be appointed as defined within the safety change management plan.

It is essential that the independent safety assessment process is aligned with a life cycle approach that monitors safety management, safety engineering and safety assurance. The independent safety assessment process shall allow intervention as soon as issues are identified.

The independent safety assessment shall not be limited to an assessment of safety documents. Independent safety assessments shall not be held too close to hold points. This can compromise the assessment due to financial and timescale pressures.

The ISA shall provide a project ISA plan and deliver an assessment report on each occasion that a submission is made to the CMAAC or delegated CCB. The ISA shall provide a summary report at the preliminary design review, a design independent safety assurance report at the final design review, and an operational safety assessment report at the final acceptance. Each report shall support the claim that necessary assurance activities are complete or in progress and that there is a high degree of confidence that the new or altered asset will be able to be demonstrated to be sufficiently safe.

The ASA may decide to conduct additional targeted surveillance activities of the AEO and ISA activities. Where this is the case, the AEO and ISA shall cooperate fully with the ASA.

8.2. Moderate or minor safety changes

The requirement for validation of the assurance for ‘moderate’ or ‘minor’ changes shall be met by the integrating AEO. The integrating AEO shall incorporate the independent professional review into the safety management of the change. This review may be completed by an ISA where substantial risks have been identified, or may be an internal function if an independence and competence assessment can be demonstrated.
The independent validation function shall be applied to the safety management arrangements, the derivation, verification and validation of safety requirements, and the safety risk management process and documentation.

8.3. Independence of assessment

The ISA is accountable for ensuring that the safety assessment undertaken is independent. To be regarded as independent, the assessment body shall not become involved as direct or indirect representatives in the design, manufacture, construction, marketing, operation or maintenance of the system under consideration.

The assessment body shall be an ISA Authorised Engineering Organisation and be free of any pressure or incentive which could affect its judgement or the results of its assessments, in particular, from persons or groups of persons affected by the assessments.

9. Acceptance of new or altered assets

TfNSW has duties specified under legislation to ensure the safety of the Transport Network, through the identification and control of risk SFAIRP. The integrating AEO shall provide an operational safety argument that demonstrates safety risks have been reduced SFAIRP, the structure of which shall be dependent upon the magnitude of the change (minor, moderate or safety significant), the asset type being changed and the risks identified during the change.

TfNSW will also ensure that when developing and transitioning the asset into the Transport Network the risks associated with the safety of the network for the operational life of the asset have been evaluated and controlled SFAIRP. The TfNSW acceptance process considers the safety assurance provided in support of the proposed change and, for significant changes, seeks appropriate due diligence through an independent safety assessment.

The acceptance body of any proposed change within TfNSW is the client representative. The CMAAC or delegated CCB reviews and makes a determination of any configuration change to the Transport Network. In making this determination the CMAAC or CCB confirms that all safety risks have been reduced SFAIRP and are tolerable for operation within the Transport Network.

9.1. Acceptance of safety significant changes

In order to enable the CMAAC to make a determination of a 'safety significant' change, the integrating AEO shall provide to the CMAAC the documents listed in Table 1.

The system safety plan shall meet the requirements detailed within Section 7.6. This system safety plan is submitted to the CMAAC for noting prior to the end of the 'system requirements and concept phase', and at other revisions of the plan.

The operational safety argument shall meet the requirements detailed in Section 7.15.1.
An independent safety assessment of the safety management of the change and of the operational safety argument shall demonstrate support of the validity of the safety argument.

'Safety significant' changes will require the integrating AEO to gain acceptance at intermediate key gateways of the change. The project assurance and governance plan and the system requirement specification both developed by TfNSW, sets out the acceptance arrangements and the delegated authority for acceptance at each intermediate project gateway. This should be in accordance with T MU AM 04001 PL.

9.2. **Acceptance of moderate and minor changes**

To enable the CMAAC or delegated CCB to make a determination of a moderate or minor change, the integrating AEO shall provide a risk summary report that meets the requirements detailed within Section 7.15.2.

10. **Specific asset requirements**

While there are a number of common safety assurance activity requirements across all asset types, there are a number of individual asset types that have specific assurance requirements.

Table 2 maps specific transport assets to sections of this standard that contain applicable requirements.

<table>
<thead>
<tr>
<th>Section</th>
<th>Rail</th>
<th>Bus</th>
<th>Maritime</th>
<th>Road</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 5 System safety governance</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Section 6 Context of change</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Section 6.1 Safety impact assessment</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Section 6.2 Consider operational context</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Section 6.3 Assessment of safety risk</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Section 6.4 Initial safety interfaces identificati</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Section 6.5 AEO relationships</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Section 7 AEO system safety requirements</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Section 7.1 Competency of personnel</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Section 7.2 Human factors integration</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Section 7.3 Interface management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Section 7.4 Engineering V-life cycle</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Section 7.5 Management of change</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Section 7.6 System safety planning</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Section 7.7 Safety risk management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Section 7.8 System hazard analysis</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
The integrating AEO shall provide a safety argument that demonstrates safety is assured SFAIRP. While the SFAIRP requirement is across all modes, the method, evidence of achievement and documentary requirements vary across modes. Section 10.1 to Section 10.5 provides modal specific requirements.

### 10.1. Rail asset specific requirements

Under the Rail Safety (Adoption of National Law) Act 2012, an accredited rail transport operator (RTO) shall request a variation to its accreditation if it 'proposes to vary the scope and nature of the railway operations in respect of which the applicant is accredited'. Consequently the introduction of some new or altered assets to the rail network will also require a change to the operator’s accreditation. In NSW this may require a change to one or more of the following accreditations:

- Country Regional Network
- NSW Trains
• Sydney Light Rail
• Sydney Metro
• Sydney Trains
• TfNSW

TfNSW will advise the integrating AEO if a change to one or more of the above accreditations is required for the change to be implemented. Where a change to an accreditation is required, the integrating AEO is accountable to provide the operator with suitable and sufficient safety assurance to obtain the accreditation change from the Office of the National Rail Safety Regulator (ONRSR). The integrating AEO is also accountable for working with each accredited organisation to ensure that the impact on each accreditation is appropriately coordinated.

10.2. Bus asset specific requirements

New or altered bus assets shall be assured to be safe SFAIRP. The integrating AEO is accountable to provide suitable and sufficient safety assurance evidence, as detailed in this standard, to satisfy TfNSW. This assurance shall demonstrate that the vehicle meets all applicable vehicle standards.

10.3. Maritime asset specific requirements

New or altered maritime assets shall be assured to be safe SFAIRP. The integrating AEO is accountable to provide suitable and sufficient safety assurance evidence, as detailed in this standard, to satisfy TfNSW. For vessels, this evidence shall be supported by an affirmation that the vessel meets the relevant 'class' rules as verified by a classification society (for vessels that fall within classification rules) or through similar and suitable evidence provided by the shipwright.

10.4. Road infrastructure asset specific requirements

New or altered road infrastructure assets associated with projects developed for TfNSW or specified by TfNSW shall be assured to be safe SFAIRP. The integrating AEO is accountable to provide suitable and sufficient safety assurance evidence, as detailed in this standard, to satisfy TfNSW. This assurance shall demonstrate that the infrastructure meets all applicable standards.

10.5. Specific requirements for other asset types

Occasionally, assets beyond those directly referred to in this standard shall be subject to the requirements of this standard. When this occurs TfNSW shall identify the systems safety requirements to be achieved by the AEO within the project safety change management plan. The AEO shall provide suitable and sufficient safety assurance evidence that these requirements have been achieved.