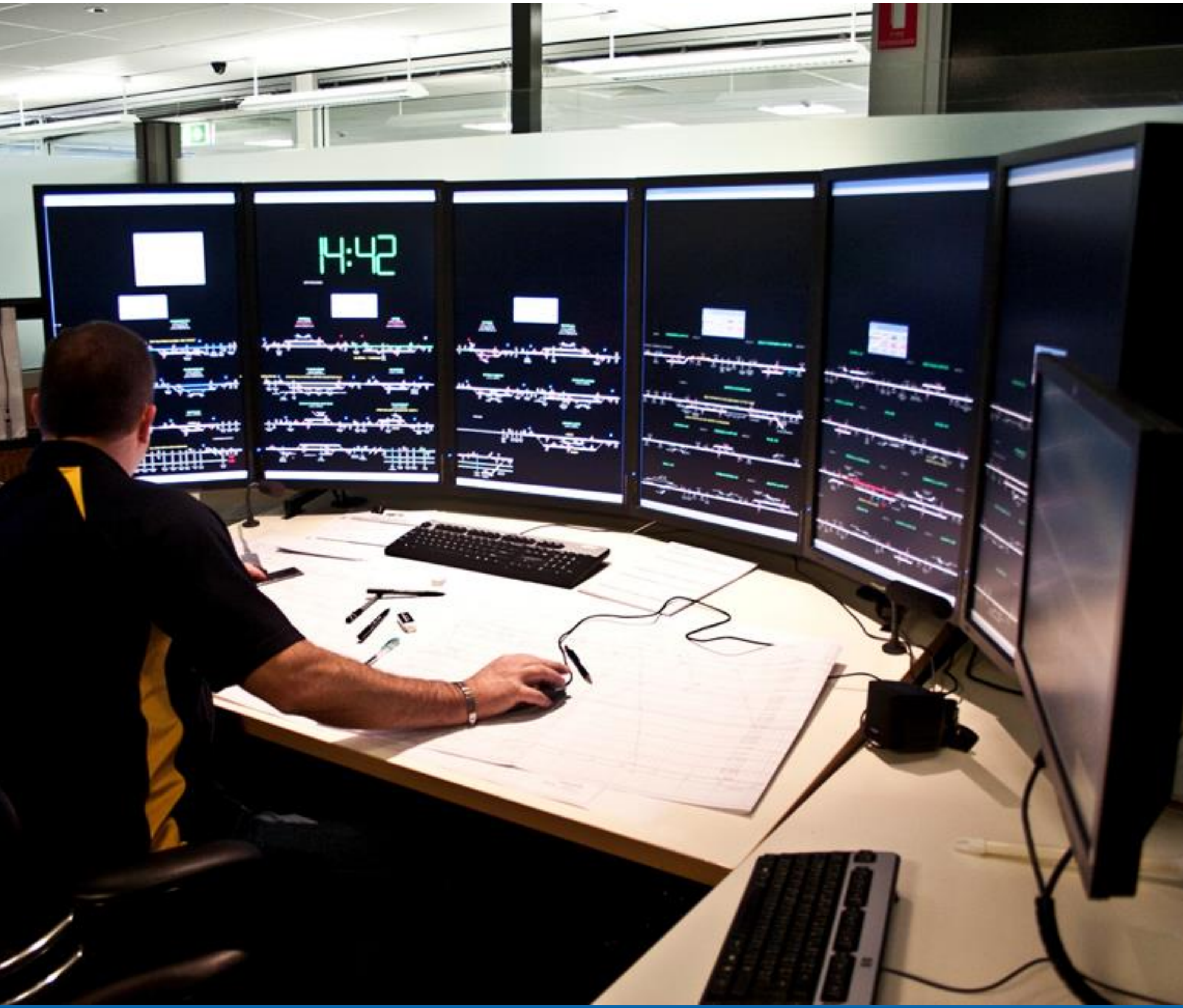
RAIL INDUSTRY SAFETY AND STANDARDS BOARD

ABN: 58 105 001 465

Systems Safety Assurance Guideline



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

Document title	Version	Date
Systems Safety Assurance	1.0	September 18, 2018

Document history

Publication version	Effective date	Page(s) affected	Reason for and extent of change(s)
1.0	September 18, 2018	All	First publication

Copyright

Table of contents

1 Introduction

1.1 Introduction

System safety assurance (SSA) provides the necessary governance, processes and objective evidence by which all interested parties satisfy themselves that a given product, service, system or organisational change can be safely integrated, operated and maintained into the transport network, so far as is reasonably practicable (SFAIRP).

1.2 Aim and purpose

This guideline aims to create a harmonised, uniform and consistent approach for managing the safety of existing and future Australian railway network assets and systems.

The purpose of this guideline is to assist rail organisations in the establishment and running of assurance activities within their business. The assurance activities will be scalable and tailorable to meet the complexities of a proposed change of product, service, system or organisational change.

1.3 Scope

This document applies to organisational, operational and asset change and provides guidance on:

- why do SSA?
- key SSA considerations;
- important organisational matters relevant to SSA; and
- the SSA process.

This guideline outlines high-level, structured safety assurance processes that:

- can be applied throughout the change;
- can be tailored to fit the size and complexity of the change;
- ensure regulatory and legal requirements are met; and
- ensure existing standards may be applied.

The guideline provides a SSA lifecycle model to safely design, deliver, construct, commission, operate, maintain, modify, and dispose of railway assets, systems and operations. The guideline applies to new and modified railway infrastructure and equipment, including rolling stock, electrical, telecom, signalling and civil infrastructure. It applies to significant changes to operation and maintenance of existing systems. While specifically concerned with safety, it is also relevant to assuring prevention of environmental and asset damage, cybersecurity and reliability, availability and maintainability (RAM).

The guideline does not include the daily management of workplace safety which is covered by WHS standards, including during construction.

1.4 Who this guideline applies to

This guideline is intended to be used by those managing changes in the rail industry. This can include:

- executives and senior managers in order for them to understand the requirements of SSA management and the duty of care that which applies to an organisation; and
- designers, engineers, safety and assurance managers, project managers, contractors and suppliers and procurement authorities who need a detailed understanding of SSA principles in the Australian rail context.

The guideline is applicable to all sectors in the rail industry including light rail and heritage operators.

1.5 How to use this guidance

This guideline provides detail to support rail organisations in addressing SSA obligations. Each organisation needs to carefully consider the applicability of this guideline and supporting documents and their impact on the entire system and its whole of life management to identify solutions that represent the best value for money to the industry whilst managing safety.

1.6 Definitions and abbreviations

New definitions and abbreviations that are not part of the standard ‘RISSB Glossary of Terms’ but identified as part of the development of this guideline, are included below.

Accreditation: the purpose of accreditation of a rail transport operator in respect of railway operations is to attest that the rail transport operator has demonstrated to the regulator the competence and capacity to manage risks to safety associated with those railway operations (RSNL Section 61).

Asset management: The set of coordinated activities that an organisation uses to realise value from assets in the delivery of its outcomes or objectives (ISO 55000:2014).

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

Audit: systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.

Availability: ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided (EN 50126-1:2017 adapted from IEC:60050-821:2017).

CCB: configuration control board.

Certification: the process of issuing a certificate to indicate conformance with a standard, a set of guidelines or some similar document.

Change configuration board: an entity that approves configuration changes in the railway assets and systems which they are delegated to manage.

CHAZop: computer/control hazard and operability study.

Configuration management: coordinated activities to direct and control the configuration of an asset.

COTS: commercial off the shelf.

Design (verb): a process to define the architecture, system elements, interfaces, and other characteristics of a system or system element (ISO 15288:2015).

Design (noun): result of the process of design (ISO 15288:2015).

ETA: event tree analysis.

FFA: functional failure analysis.

FMEA: failure modes and effects analysis.

FMECA: failure modes, effects and criticality analysis.

FTA: fault tree analysis.

GSN: goal structuring notation.

HAR: hazard analysis report.

Hazard: a condition that could lead to an accident (EN 50126-1:2017).

Hazard analysis: the process of identifying hazards and analysing their causes, and the derivation of requirements to limit the likelihood and consequences of hazards to a tolerable level (EN 60050-821:2017 and adopted by EN 50126-1:2017).

Hazard log: a document in which hazards identified, decisions made, solutions adopted, and their implementation status are recorded or referenced (EN 60050-821:2017 and adopted by EN 50126-1:2017).

Hazard management: process typically involves:

- Hazard identification - Identification of reasonably foreseeable hazards.
- Assessing the hazard risks - Assessment of the level of risk associated with exposure to, or unintentional release of, the hazard.
- Hazard mitigation and controls - Development of risk control measures and their implementation.
- Hazard monitoring and review - Evaluation of the control measures and their modification, if necessary, to ensure effective control of risk (Hazard Management Procedure; Government of South Australia; April 2011 referenced in SAI Global Effective hazard identification and management 2012).

HAZops: hazard and operability studies.

HF: human factors.

HFI: human factors integration.

IHA: interface hazard analysis.

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

ISA: independent safety assessor.

ISAR: independent safety assessor's report.

Lifecycle: a series of identifiable stages through which an item goes, from its conception to disposal (EN 60050-821:2017 and adopted by EN 50126-1:2017).

Lifecycle model: framework of processes and activities concerned with the lifecycle that may be organized into stages, which also acts as a common reference for communication and understanding (ISO 15288:2015).

Maintainability: ability to be retained in, or restored to, a state to perform as required, under given conditions of use and maintenance (EN 50126-1:2017 adapted from IEC:60050-192:2015).

OCD: operational concept document.

OHS: occupational health and safety.

ONRSR: Office of the National Rail Safety Regulator.

Operational concept: verbal and graphic statement of an organization's assumptions or intent in regard to an operation or series of operations of a system or a related set of systems (ISO 15288:2015). Note: sometimes known as a concept of operations.

OSHA: operating and support hazard analysis.

PHA: preliminary hazard analysis.

PHAR: preliminary hazard analysis report.

PHI: preliminary hazard identification.

PHL: project hazard log.

Railway asset: an item or thing that has potential or actual value to a rail transport operator (ISO 55000:2014).

Railway authority: the body with the overall accountability to a safety authority for operating a safe railway system (EN 50129:2003).

RAM: reliability, availability and maintainability.

RAMS: reliability, availability, maintainability, and safety (EN 50126-1:2017).

RBD: reliability block diagrams.

Reliability: ability to perform as required, without failure, for a given time interval, under given conditions (EN 50126-1:2017 adapted from IEC 60050-192:2015)

Requirement: statement that translates or expresses a need and its associated constraints and conditions (ISO 15288:2015).

RIM: rail infrastructure manager.

Risk: a combination of expected frequency of loss and the expected degree of severity of that loss (EN 50126-1:2017).

Risk analysis: the systematic use of available information to identify hazards and to estimate the risk (IEC Guide 53:2014, IEC 60050-903:2013 and adopted by EN 50126-1:2017).

Risk assessment: the overall process comprising a risk analysis and a risk evaluation (IEC Guide 73:2014, IEC 60050-903:2013 and adopted by EN 50126-1:2017).

Risk evaluation: the procedure based on the risk analysis to determine whether the risk SFAIRP has been achieved (IEC Guide 53:2014, IEC 60050-903:2013 and adopted by EN 50126-1:2017).

Risk management: the systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risk (EN 50126-1:2017).

Risk tolerability: risk which is accepted [by an entity] in a given context based on the current values of society (ISO Guide 51:1999 and adopted by EN 61508.4:2018). Note that where there are perceived to be other reasonably practicable risk controls available, Australia's RSNL may require a higher level of risk reduction than such an entity's risk tolerability.

RSNL: Rail Safety National Law.

RSO: rolling stock operator.

RTO: rail transport operator.

Safety: a measure of the degree of freedom from risk or conditions that can cause death, physical harm (adapted from Stephenson, 1991).

Safety assurance report: forms part of the safety case which should be supported by an independent assessment where required, a hazard log and control output data (evidence all the chosen safety control measures/treatments have been implemented). These in turn are supported by a wide range of evidence which the organisation uses to demonstrate safety of rail assets.

Safety case: a documented demonstration that the product (e.g. a system, subsystem or equipment) complies with the specified safety requirements (IEC 60050-821:2017 and adopted by EN 50126-1:2017).

Safety critical system: a safety-related system of high criticality (Storey, 1996).

Safety integrity: probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time (EN 61508.4: 2018).

Safety integrity level: discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest (EN 50126-1:2017 and EN 61508.4: 2018

Safety-related system: a system by which the safety of equipment or plant is assured (50126-1:2017 and Storey, 1996).

SAR: safety assurance report.

SDD: safety design documents

SE: systems engineering.

SiD: safety in design.

SFAIRP: so far as is reasonably practicable.

SHA: system hazard analysis.

SIL: safety integrity level.

SME: subject matter expert.

SRAC: safety requirement application conditions.

SMS: safety management system.

SRS: safety requirement specification.

SSA: systems safety assurance.

SSAMP: SSA management plan.

SSA practitioner: systems safety assurance practitioner (or safety expert) – engineer with SSA process expertise and knowledge of RAMS, human factors and WHS safety issues. SSA practitioner responsibilities will typically be to ensure SSA processes are adequate and will rely on SMEs for specialised technical knowledge.

SSHA: subsystem hazard analysis.

Subsystem: the part of a system, which is itself a system (IEC 60050-192:2015 and adopted by EN 50126-1:2017)

Systems: an integrated set of elements, subsystems, or assemblies that accomplish a defined objective. These elements include products, (hardware, software, firmware), processes, people, information, techniques, facilities, services and other support elements (INCOSE, 2015).

Systems engineering: an interdisciplinary approach and means to enable the realisation of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with the design synthesis and system validation while considering the complete problem: operations, cost and schedule performance, training and support, test, manufacturing and disposal. SE considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs (INCOSE, 2004 and 2015).

System safety assurance: all planned and systematic actions necessary to afford adequate confidence and demonstrate that a product, a service, an organisation or a functional system achieves acceptable or tolerable safety. In the railway industry risks to safety must be eliminated or reduced so far as is reasonably practicable (SFAIRP), (adapted from RC Commission Regulation 2096/2005).

System safety: a sub-discipline of systems engineering that applies scientific, engineering and management principles to ensure adequate safety, the timely identification of hazard risk, and initiation of actions to prevent or control these hazards throughout the lifecycle and within the constraints of operational effectiveness, time and cost (Stephenson, 1991).

THR: tolerable hazard rate.

Validation: confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled (ISO 15288:2015, modified from ISO 9000:20005).

Verification: confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (ISO 15288:2015, modified from ISO 9000:20005).

WHS: work health and safety.

2 System safety assurance: Requirements

2.1 Why SSA?

Procurers, delivery agencies and rail transport operators (RTO) have a duty of care (safety duty) defined within legislation to ensure that all reasonably foreseeable safety hazards are eliminated, or if not reasonably practicable to do so, minimised SFAIRP. In particular:

- general duty of care to employees and rail workers is imposed by the federal Work health and safety (WHS) Act (2011);
- duty of care to all persons encountering rail assets is outlined within the rail safety national law (RSNL) (2012); and
- the safety duty is a legal obligation which cannot be transferred to another entity by any rail authority.

Within this guidance, the goal is to ensure that:

- each foreseeable risk has been eliminated or minimised SFAIRP; and
- that the system as a whole is safe SFAIRP, the declaration of which is justified, documented and approved.

More information is provided around SFAIRP in Section 2.3, 3.2.1, 4.2.6.6, 4.2.6.9 and 4.5.

SSA forms part of the management of change requirements of the accredited rail transport operators' (RTO) safety management system (SMS). This guideline encourages the application of SSA as a coherent group of activities undertaken throughout the system lifecycle.

Whilst the law does not explicitly require the assurance through the lifecycle approach, it is an established as good practice where the change is more novel and complex. This is evidenced by a number of rail industry standards and guidance material, including the Office of the National Rail Safety Regulator (ONRSR) Major Projects Guideline.

SSA:

- facilitates the provision of a safe system;
- is necessary for all parties involved in delivery of systems to achieve due diligence;
- provides a structured approach to identification, assessment and control of hazards and the demonstration that rail assets are safe to undertake commission, operation and disposal; and
- is used to improve safety of rail employees, passengers and the public and to justify that the risks associated with rail operation have been duly addressed.

In this manner, an effective SSA program seeks to:

- protect employees, passengers and the public from risks to health and safety; and
- provide organisations the evidence to demonstrate that they have undertaken their duty of care to all persons who encounter the rail assets.

SSA should be applied to all changes that have a potential safety impact, including changes to services, the addition or modification or disposal of assets, the introduction of new technologies and the construction and delivery of major projects.

2.2 SSA considerations

SSA involves a range of contextual considerations as outlined in Figure 1. These include both legal and organisational requirements as well as safety objectives, interactions with ONRSR, application of industry standards, data and new technology. This guideline addresses each of the matters included in Figure 1.

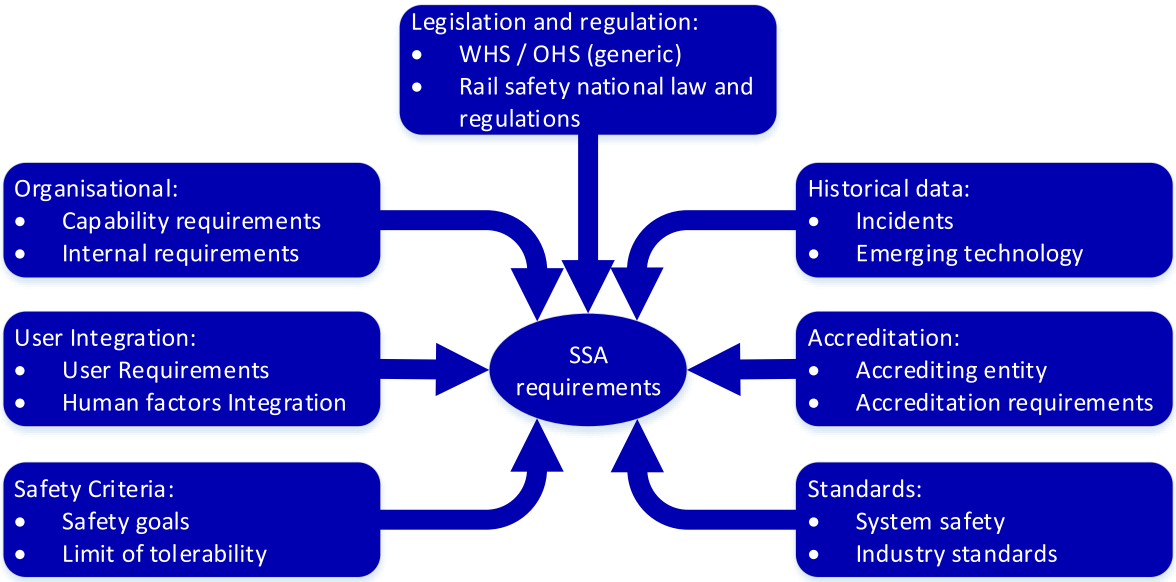


Figure 1- The range of inputs to SSA

SSA is most effective to influence the safety outcomes when applied throughout the change lifecycle. In principle, this requires system safety activities to be linked to safety requirements development early in the change through to verification and validation of those requirements. For asset changes, SSA links to systems engineering (SE) standards to achieve this purpose. SSA needs to integrate with other activities through the project lifecycle such as design management, SE, RAM and human factors integration (HFI).

2.3 SSA process outline

The SSA document hierarchy described within the following sections provides a framework for the development of a safety argument, that a given system is safe SFAIRP and that the process for making this argument meets necessary standards and legislation. This chapter provides guidance for the SSA management plan (SSAMP) which outlines the process for developing the safety case.

The SSA process may be broken down to the following elements, shown in Figure 2:

- SSA procedure: This guidance may be used to provide an SSA procedure, suitably modified for the project. For some organisations, specific SSA procedures may be applicable to specific projects.
- SSAMP: The documented management plan for SSA within an individual project, this may be used to support one or more individual systems.

- Safety case: The structured argument and supporting evidence to demonstrate that a particular system is deemed to be safe SFAIRP.

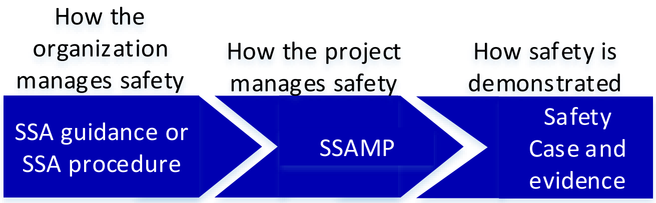

How the organization manages safety
How the project manages safety
How safety is demonstrated
SSA guidance or SSA procedure
SSAMP
Safety Case and evidence

Figure 2 - SSA document hierarchy

The SSA process:

- involves a range of considerations and documents;
- is iterative as assumptions and estimations used early in the project lifecycle may require modification when further information is available;
- is most effective in improving safety of rail systems when applied throughout the change lifecycle; and
- should be linked to requirements development from the earliest stage of the project through to verification and validation of those requirements.

For asset changes, SSA links to SE standards to achieve this purpose.

The safety case should incorporate a safety assurance report (SAR) which should be supported by an independent safety assessment where required, a hazard log and control output data (evidence all the chosen safety control measures/treatments have been implemented). These in turn are supported by a wide range of evidence which the organisation uses to demonstrate safety of rail assets. The safety case is discussed in more detail in section 4.6

The SSA process involves a wide range of inputs and outputs as shown in Figure 3. More detail on each of the elements of the SSA process framework is provided in Chapters 3 and 4 (including a description of the acronyms).

This guideline is based on the principles of managing rail assets within a lifecycle, and as such, draws on the systems and development lifecycles as described in Appendices A and B.

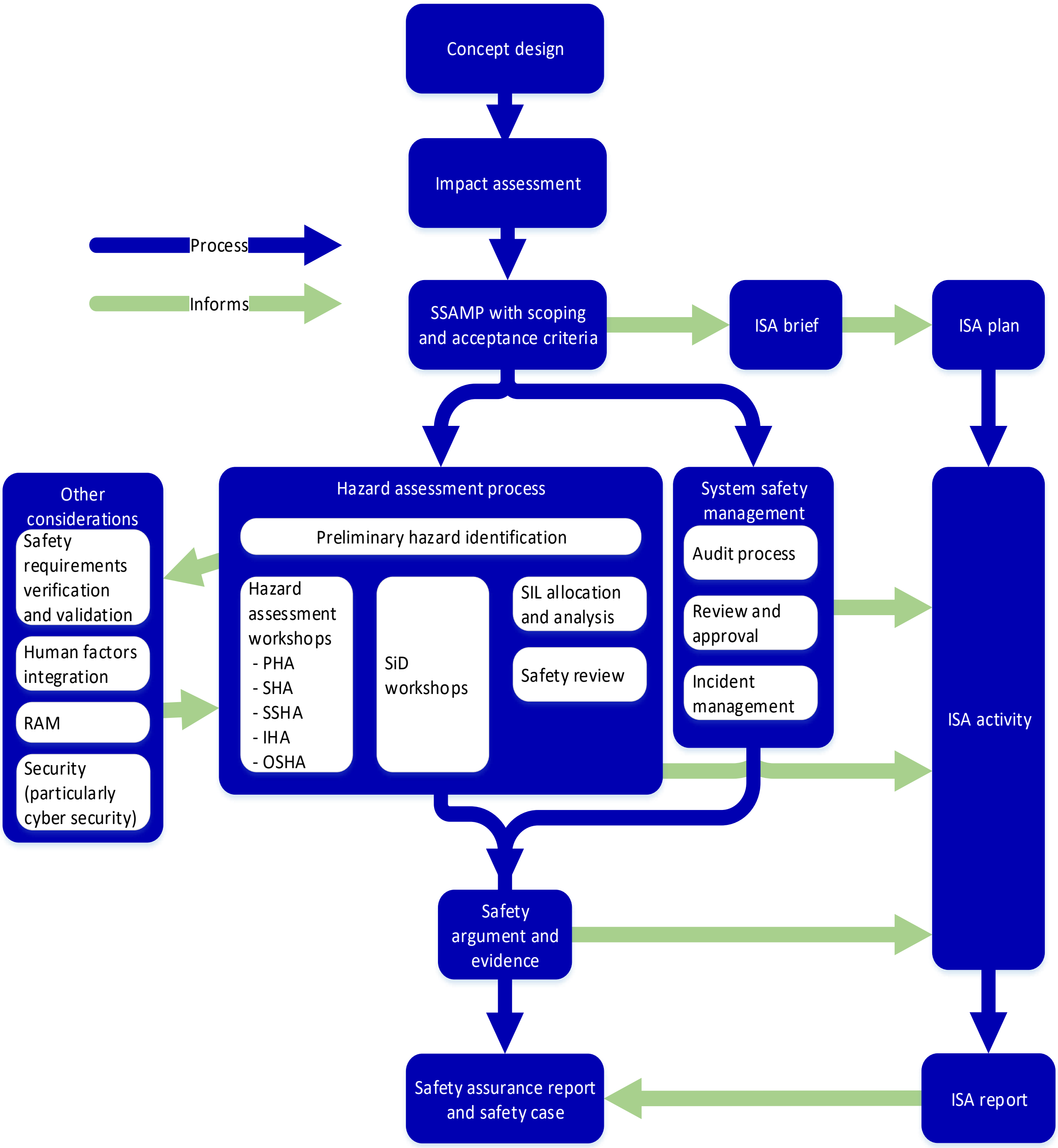

Concept design
Impact assessment
Process
Informs
SSAMP with scoping and acceptance criteria
ISA brief
ISA plan
Other considerations
Safety requirements verification and validation
Human factors integration
RAM
Security (particularly cyber security)
Hazard assessment process
Preliminary hazard identification
Hazard assessment workshops
- PHA
- SHA
- SSHA
- IHA
- OSHA
SiD workshops
SIL allocation and analysis
Safety review
System safety management
Audit process
Review and approval
Incident management
ISA activity
Safety argument and evidence
Safety assurance report and safety case
ISA report

Figure 3 - SSA framework

3 System safety assurance: Organisational matters

In undertaking SSA, all rail organisations need to take into account a number of considerations relating to legal matters, governance, organisational structure, qualifications, management of SSA and auditing.

3.1 Organisational legal status

The relevant railway authority is responsible for the effective, efficient and safe use of their railway assets and systems throughout their whole lifecycle including:

- planning: identifying the demand/need for new or altered assets and planning for their design, construction and use;
- acquisition: design and constructing new assets, or altering/modifying existing assets; and
- operation and maintenance: deploying the assets for use in delivering transport services.

ONRSR uses the term accredited entity which is used interchangeably with RTO. RTOs are categorised into two further categories depending upon whether they have above or below rail management responsibilities:

- Rolling stock operator (RSO) – an organisation that has effective management and control of rolling stock.
- Railway infrastructure manager (RIM) – an organisation that has effective management and control of rail infrastructure.

A railway authority is described in EN 50129:2003 as "*the body with the overall accountability to a safety authority for operating a safe railway system*".

For projects within the scope of a single RTO, the RTO will normally be the railway authority for the project. Projects which involve more than one RTO should ensure that the identity and areas of responsibility of the railway authority(ies) are clearly identified early in the project lifecycle and documented in the SSAMP.

3.2 Organisational responsibilities

It is important to understand responsibilities under SSA and an organisation should define these responsibilities in appropriate safety documentation, e.g. a SSAMP.

Statutory obligations apply to all entities which have a role in the concept, development, design, commissioning, operation and disposal of rail assets. In addition to the regulations cited within the following sections, there may be legislation applicable within individual jurisdictions or for specific rail applications. It is the responsibility of the organisation to identify applicable legislation within SSAMP documentation and ensure that the safety case demonstrates compliance.

3.2.1 RTOs responsibilities

Section 52 of the RSNL places a duty on RTOs to ensure SFAIRP the safety of the transport network and their operations.

To achieve these duties whenever new railway assets or systems are introduced, or existing railway assets or systems are modified, upgraded or removed RTOs need to ensure the following:

- Operational safety risks are identified, assessed and managed with new or modified systems 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 ensure safety SFAIRP during its operation.
    - Manufactured or constructed and transitioned into the transport network in a manner which ensures safety SFAIRP.
    - All reasonably foreseeable safety risks are eliminated or minimised SFAIRP.
- Disposal: arranging for the safe disposal of assets.

3.2.2 Designers, manufacturers and suppliers' responsibilities

Section 53 of the RSNL imposes duties on designers, manufacturers and suppliers who carry out functions or services in connection to railway infrastructure or rolling stock including contracted infrastructure or rolling stock maintainers and others providing engineering or technical services. Such parties are therefore regulated under the RSNL, even though they may not be accredited RTOs. Therefore, all those responsible for delivering new or modified railway assets or systems are accountable for conducting activities and providing SSA evidence to demonstrate that these duties have been achieved in accordance with the RTO's SMS.

It is important that responsibilities for the planning, oversight and delivery of railway infrastructure and contracting for the delivery of railway services are defined. As part of this responsibility there should be an organisational chart that outlines safety governance and SSA responsibilities for existing, new and modified railway assets and systems. Of most concern in the SSA domain is the management of change, which occurs at two levels:

- Overall change that incorporates new or modified assets into the railway network.
- Changes made within a project delivering new or modified assets.

Regardless of these two levels, all safety risks need to be reduced SFAIRP as part of these changes.

3.2.3 Assurance levels

In undertaking SSA, organisations should note there are generally three levels to assurance of change - as depicted in Figure 4:

- ***Level 1 (design)***: The processes by which design, development, implementation and testing and commissioning are conducted as well as the associated system safety activities. This is effectively the SMS and engineering management system of the delivery organisations. This may include auditing for compliance to management systems and processes internal to the delivery organisations. It also includes design checking etc. within the delivery organisation.
- **Level 2 (review):** At this level independent audits and checks are made of the delivery organisations. This may be by the procuring/lead delivery organisation of

its appointed suppliers or for the principal contractor by the RTO. It also includes independent safety assessment, independent design checks, independent professional review and the independent validator required under EN50126:2017 clause 7.

- **Level 3 (accept):** At this level are the activities undertaken by the RTO or asset accepting organisation. This includes the Tier 1 configuration management process and a configuration change board (CCB) (see section 4.7) as well as all due diligence activities undertaken by the RTO/asset acceptor[1]. Due diligence activities would normally be conducted in a risk-based manner focussing on the highest levels of risk to delivery, cost and safety.

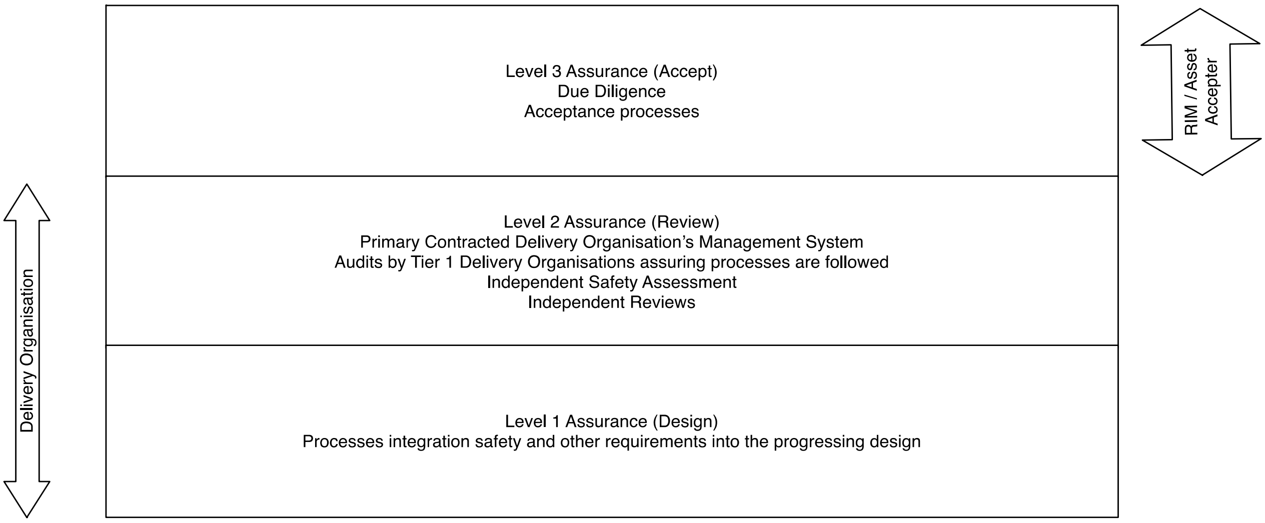

Level 3 Assurance (Accept)
Due Diligence
Acceptance processes
Level 2 Assurance (Review)
Primary Contracted Delivery Organisation's Management System
Audits by Tier 1 Delivery Organisations assuring processes are followed
Independent Safety Assessment
Independent Reviews
Level 1 Assurance (Design)
Processes integration safety and other requirements into the progressing design
Delivery Organisation
RIM / Asset Accepter

Figure 4 - Assurance levels

3.3 SSA stakeholders

Rail infrastructure projects tend to be large, complex, tasks undertaken across several stakeholder organisations responsible for different elements of the project lifecycle. The scope of SSA tasks undertaken by an organisation should be clearly outlined within their SSAMP (see section 4.1.1.6), typical stakeholder organisations may include the following:

- Network authority: Typically, a state entity responsible for oversight over rail operators and the overall architecture of the network.
- Delivery authority: Responsible for managing selection, procurement and delivery of transport assets. Typically, a state entity, the delivery authority, is responsible to ensure that the rail system delivered is safe SFAIRP, as designed.
- Supplier: Responsible for manufacture and supply of a rail system, the supplier is required to ensure that a rail system as designed is safe SFAIRP.
- RTO: Responsible for safe operation and maintenance of transport assets. The RTO is required to seek accreditation from the rail safety regulator.
- Rail safety regulator: ONRSR is the regulator for rail transport within Australia and provides information and accreditation to support rail transport operation

[1] Refer to section 3.4 for detail about configuration management.

3.4 Organisational structure

While the form of organisation arrangements may vary, it is essential that the senior safety specialist in any organisation or project has provision for direct reporting to the relevant executive officer (e.g. project director) on safety matters, and the opportunity to provide timely input into all decisions that may impact on the safety of railway assets or operations.

In terms of structure the following other key personnel should have clearly documented accountabilities and responsibilities for their role in SSA:

- An executive officer with ultimate accountability for the configuration of the railways assets and systems, assurance and legal compliance. This executive officer discharges accountability by authorising (through delegation) competent people to lead:
    - A railway asset and system requirements team for:
        - the identification, selection, development, publication and maintenance and control of a suite of requirements documents on behalf of the railway assets and systems owner, i.e. configuration management requirements in a documented plan;
        - delegating authority to operate within the framework; and
        - approving the railway asset or system configuration management plan; and
    - A configuration change management and assurance team to set and manage the framework for configuration management of new and modified railway assets and systems.

The railway asset and system requirements team leader then become accountable through delegation of responsibility, normally through contractual arrangements, to:

- authorised suppliers who the railway asset and system configuration team can delegate authority to for making decisions on configuration; and
- subcontractors who can who the railway asset and system configuration team can delegate authority to for making decisions on configuration change.

There should be sign off on the risk that has been accepted in the change as being assessed SFAIRP, including who made this assessment and how they have reached this conclusion.

3.5 Personnel with safety duties: Qualifications and competence

SSA requires competent persons to exercise sound, professional judgements and successfully apply a safety assurance approach to the management of change. In broad terms the following levels within an organisation should be qualified as indicated:

- Executive/decision board – need awareness but no specific qualification, they must rely on recommendations;
- Managers – need to be aware of SSA issues, however when supported by practitioners does not require in-depth knowledge (if expected to undertake SSA tasks need to be as SSA lead);

- SSA practitioners – qualifications/experience required;
- 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;
- Understanding of the Australian legal and regulatory framework for managing railway safety; and
- Junior SSA practitioners – minimal qualifications required if work is reviewed by SSA lead.

A competency management system should be in place to assure work is performed by suitably competent personnel.

The competence of the safety management resources used should be demonstrated within the high-level argument of the safety assurance report (competence and qualification should be recorded in safety documentation). The person leading the SSA process should be suitably qualified (e.g. a degree in an appropriate engineering discipline) and have relevant experience. SE qualifications and experience are desirable.

It should be noted that it takes time for organisations to develop the right rigour and people in the SSA process and that as a result there will be differing maturity levels amongst the project participants. As such, the planning for SSA must take into account these varying maturity levels.

4 SSA: Process details

This chapter and the appendices provides detail on many of the activities outlined in the SSA framework (Figure 3).

4.1 Impact assessment

An initial impact assessment (also called a *criticality assessment* or *assessment of significance*) is undertaken to define the criticality of the project and inform the scope of the SSAMP. This can be achieved by undertaking an assessment of significance, that considers complexity, failure consequence, reversibility, novelty of technology, additionality (accumulation of insignificant changes leading to significant change), ability to monitor the change and intervene throughout its lifecycle and novelty of the project.

Note: Most engineering organisations will have an extant SE process which includes conduct of an impact assessment. If this does exist it is recommended to employ output form the extant plan. If this plan is not available, this section provides guidance on how this may be achieved.

The impact assessment should be undertaken as depicted in Figure 5, the output of which is used to support identification of key activities and justification for tailoring of guidance/standards proportionate to the project.

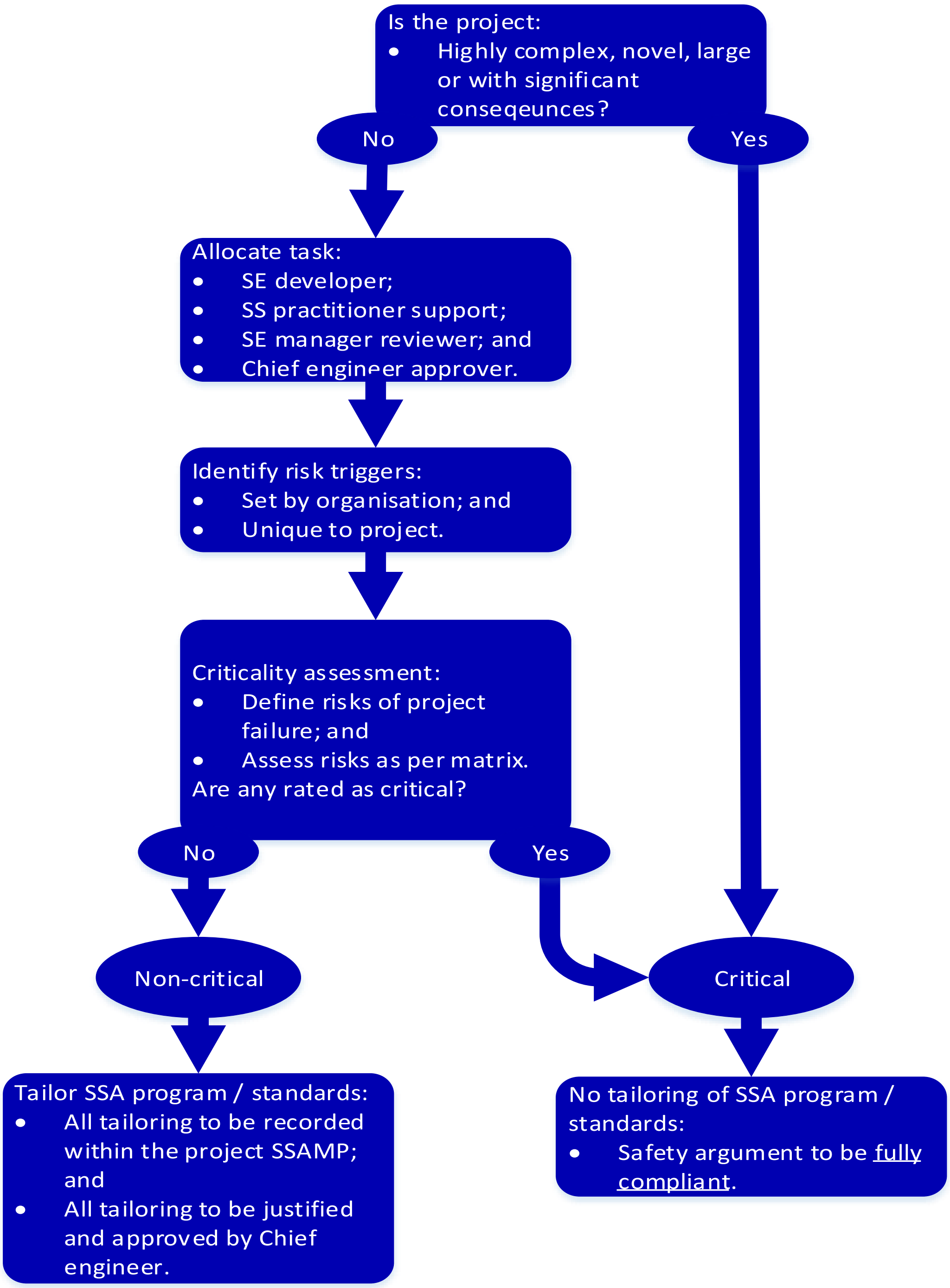

Is the project:
• Highly complex, novel, large or with significant conseqeunces?
No
Yes
Allocate task:
• SE developer;
• SS practitioner support;
• SE manager reviewer; and
• Chief engineer approver.
Identify risk triggers:
• Set by organisation; and
• Unique to project.
Criticality assessment:
• Define risks of project failure; and
• Assess risks as per matrix.
Are any rated as critical?
No
Yes
Non-critical
Critical
Tailor SSA program / standards:
• All tailoring to be recorded within the project SSAMP; and
• All tailoring to be justified and approved by Chief engineer.
No tailoring of SSA program / standards:
• Safety argument to be fully compliant.

Figure 5 – Example: Impact assessment process

The following is a list of sources of information that can be used in the impact assessment process:

- Similar or related railway assets or systems.
- Safety.
- Reliability.
- Availability.
- Maintainability.
- Economy.

- Service life (stating how this will be accepted).
- Industry and other standards and norms (themselves functional).
- Train service quality management.
- Targets (train paths provided, delays, recovered energy, efficiency, costs).
- Public perception.
- Additionally, for adapting existing railways while traffic continues to run, the quality of the service provided (operated and supported by staff of stated competence) during the staged introduction of new railway assets or systems.

Other consideration that may help include:

- how the railway asset or system will be used and maintained;
- the people who will use and maintain the railway asset or system and other stakeholders impacted by that; and
- the interfaces between the railway asset or system and other technical systems.

4.1.1 Planning an impact assessment

An impact assessment should be undertaken by a system engineer or SSA practitioner with sufficient knowledge to identify and advise on key risks and approved by the chief engineer (or equivalent). Planning for the impact assessment should include identification of who will write the impact assessment, who will be consulted, who will review the impact assessment and who will approve the impact assessment.

The impact assessment is comparable to a simplified risk assessment, with the following considerations:

- As a preliminary scoping document this does not require the level of consultation and review anticipated for the risk assessment process.
- The developer should consult with an SSA practitioner and applicable subject matter expert (SME) prior to progressing the document for review.
- As this assessment is to inform scoping, it should consider impact of the project process being insufficient rather than risk assess the system itself.
- As a preliminary document with limited input and assessment the impact assessment relies on significant assumptions (which should be explicitly stated) and lacks data, all assessments should therefore be conservative.

4.1.2 Identify project risks

Key risks resulting from insufficient project scope should be identified and assessed in terms of their impact on the capability of a system and implementation of change. Identification of key risks may be undertaken in any manner, however is commonly undertaken using a set of key risk ‘triggers’ which may include the following:

- Technology maturity – capability of the technology may not be well understood, in particular there may be a lack of knowledge regarding management of unique risks;
- Complexity of change – highly complex changes may result in significant delay and many interfaces resulting in complex or unforeseen risks;

- Technical specialisation – requirement for highly specialised systems and operators may impact availability to safely install and operate systems;
- Interfaces – multiple interfaces or interfaces with high risk assets;
- Potential consequences – high cost or critical consequences;
- Reversibility – ability to use extant systems in the event of failure or inability to commence services; and
- As part of the impact assessment process, the developer should consult to ensure they have captured key foreseeable risks and add risks as deemed appropriate.

4.1.3 Assess criticality

Once risks have been identified, these should be assessed to identify if the project is deemed as 'critical', which is achieved using a simplified risk assessment matrix. An example of a criticality assessment matrix is included at Table 1.

Table 1- Example Impact Assessment matrix

<table>
<tr><td colspan="5">Likelihood</td></tr>
<tr><td colspan="2">Unlikely</td><td colspan="3">Unlikely to occur in the event of failure</td></tr>
<tr><td colspan="2">Possible</td><td colspan="3">May occur in the event of failure</td></tr>
<tr><td colspan="2">Likely</td><td colspan="3">Will occur in most circumstances</td></tr>
<tr><td colspan="5">Consequence</td></tr>
<tr><td colspan="2">Insignificant</td><td colspan="3">Minor injury not requiring treatment</td></tr>
<tr><td colspan="2">Major</td><td colspan="3">Non-life threatening injury</td></tr>
<tr><td colspan="2">Catastrophic</td><td colspan="3">Life threatening injury or death</td></tr>
<tr><td colspan="2" rowspan="2"></td><td colspan="3">Consequence</td></tr>
<tr><td>Insignificant</td><td>Major</td><td>Catastrophic</td></tr>
<tr><td rowspan="3">Likelihood</td><td>Unlikely</td><td>Non-Critical</td><td>Non-Critical</td><td>Critical</td></tr>
<tr><td>Possible</td><td>Non-Critical</td><td>Critical</td><td>Critical</td></tr>
<tr><td>Likely</td><td>Non-Critical</td><td>Critical</td><td>Critical</td></tr>
</table>

Note: The example is suitable for an organisation undertaking non-complex tasks. Where the organisation is undertaking a wide variety of highly critical tasks it may be beneficial to classify a criticality rating (for example, (C1 – C4) to provide better direction to engineering tasks.

Once each identified risk has been assessed:

- If any risk is deemed to be critical, then the project is deemed as critical.
- If no risk is deemed critical, then the project is deemed non-critical.

Similarly, if the project is employing a criticality scale, the project is deemed the same criticality as the highest risk assessed. Before completing the SSA checklist, the developer should seek review and agreement from the chief engineer (or equivalent).

The criticality assessment should determine the need for an independent safety assessor (ISA), considering the factors listed in Section 4.1, as well as the organisational capability, maturity and experience of the supplier and of the RTO.

4.1.4 Allocate SSA tasks

An outline of required tasks is to be developed, informed by the criticality assessment. It is recommended that organizations have a list of standard SSA tasks which may be tailored by removing or adding tasks deemed appropriate for the project. A simplified example is presented in Appendix C.

When allocating SSA tasks the following must be considered:

- Any task not undertaken should be justified and approved.
- All decisions should be documented and recorded.
- Where there is uncertainty SSA tasks should be included.
- If there is scope for significant risk to personnel or public, the assessment must be deemed critical.

Note: Where an organisation does not have an established set of SSA activities, this may be developed from applicable standards and this guidance document. Regardless of the source, justification of tailoring must be included, and the list should subsequently be approved by the chief engineer (or equivalent).

4.1.5 System safety assurance management plan

The output of the impact assessment is used to draft the system safety assurance management plan (SSAMP). The SSAMP should be scoped according to the information available and the organisation of the project. It may be split into smaller plans that cover particular stages of the SE lifecycle, activities to be carried out by particular disciplines or the entire project.

The SSAMP should provide an outline of all safety management processes as deemed applicable for the project and describe the key deliverables to demonstrate that the system or product is safe SFAIRP. The SSAMP should include details regarding the following:

- Scope and purpose of the system and safety program.
- The allocation of safety responsibilities and accountabilities.
- The definition of the system or product and project scope.
- Legislation, standards and codes of practice adopted for the project and how their requirements will be achieved.
- The safety objectives and targets for the system or product.
- SSA organization.
- Hazard identification, including all applicable SSA tasks.
- Hazard estimation and evaluation.
- Establishing and maintaining safety requirements.
- Validation of safety requirements.
- Managing HF and reliability, availability, maintainability and safety (RAMS) and how this is integrated.
- Managing hazards, controls, assumptions, constraints, dependencies and application conditions.

- Approach to allocating and demonstrating safety integrity levels (SIL) /functional safety integrity requirements.
- Monitoring and control of the safety program (including audit program with internal/external auditing).
- Liaison with the ONRSR and other key stakeholders.
- The format of the safety assurance report suite of documents that will be prepared and the authorities who will authorise the relevant supporting documents.
- Configuration management.
- Quality management.
- Safety management of subsystems.
- Type approval process.
- ISA tasking and management.
- Plan for certification, accreditation and acceptance.

SSA tasks identified within the SSAMP should be aligned to systems engineering tasks undertaken within the project, enabling deliverables to support project assurance tasks.

The SSAMP should be a ‘living’ document throughout the SSA program and is therefore open to update and review.

4.2 System safety assurance: Hazard management

Hazard management is a core SSA activity and should be embedded in the organisation’s SMS. Hazard management is not the same as risk management, although risk analysis methods may be used to assess safety hazards.

The following section includes a description of hazard management related tasks that may be undertaken throughout the SSA process. Tasks are to be undertaken in accordance with the SSAMP. When undertaking SSA activities it is critical to ensure that these contribute to the overall systems engineering lifecycle, therefore these activities must inform the overall project deliverables.

4.2.1 Hazard assessment

Hazard assessment is at the core of all SSA processes and must be undertaken on all safety risks in a consistent manner with the goal of assuring that the system, as a whole, is safe SFAIRP. Risk analysis methods (following ISO 30100:2018 for example) may be used to assess safety hazards, accordance with the organisation’s risk management processes.

Hazard assessment requires the identification, assessment, control and ultimately acceptance of risks to safety as shown in Figure 6. Note this section outlines common hazard assessment tasks with important outputs. Further information relevant to hazard management is provided in Appendix D.

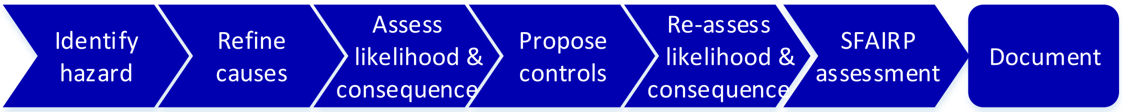


Figure 6 - Simplified hazard assessment concept

A hazard is "*a condition that could lead to an accident*", (EN 50126-1:2017). It is not an internal fault, nor an external event, which may be potential causes, nor it the accident itself, nor is it the measure of risk. Hazards should be described with respect to the system under investigation.

4.2.1.1 Preliminary hazard identification

Note: PHI may be undertaken as part of the concept development and impact assessment process. If this is done, then the SSAMP should include the output of the PHI and a list of any derived requirements as an annex.

Preliminary hazard identification (PHI) may be performed early in the design cycle when the design is at a conceptual stage. The intent of the PHI is to:

- guide the design process by considering risks associated with the conceptual system, enabling elimination or reduction of hazards; and
- identify any applicable derived requirements to inform the requirement management/documentation process.

The PHI process applies to all projects and is generally a brainstorming process to identify possible risks with the system concept and refine causes of those risks (

Figure 7). The PHI should provide a list of derived requirements and a preliminary hazard list that also feeds into the hazard log.

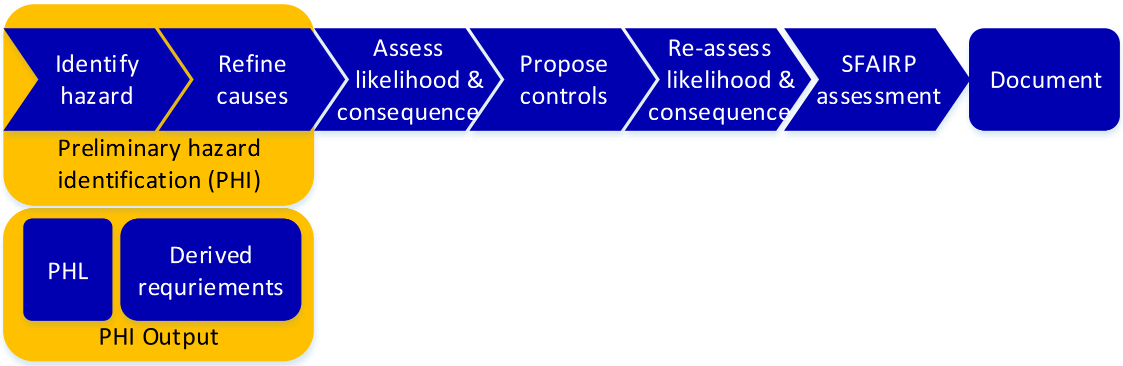

Identify hazard
Refine causes
Assess likelihood & consequence
Propose controls
Re-assess likelihood & consequence
SFAIRP assessment
Document
Preliminary hazard identification (PHI)
PHL
Derived requirements
PHI Output

Figure 7 –Hazard assessment: PHI

Sources of information include:

- system concept and operational environment, what the anticipated system is, the intent of the system, what environment it will operate within and how this would interact with the public and passengers;
- historical data for similar systems: what risks/incidents have occurred in similar systems and how these systems have interfaced (successfully and unsuccessfully) with other elements of transport systems; and
- technology and domain-specific analyses and checklists.2

The preliminary hazard analysis (PHA) should be undertaken as a workshop with appropriate stakeholders including technical SMEs, SSA practitioners and project managers to ensure completeness of the resultant hazard log. While it is possible for the PHI to be blended with the PHA (see the following section) using system techniques such as hazard and operability study (HAZop), it is recommended that these processes are separate.

PHI Output: The following documents should be retained as supporting evidence to development of SARs and for auditing/control of the SSA process:

- Preliminary hazard list.
- Initial hazard log.
- PHI records including an attendance list, meeting minutes and any subsequent action items.

4.2.1.2 Preliminary hazard analysis

The Preliminary Hazard Analysis (PHA) is undertaken to refine and assess hazards based on the concept design and functional requirements of the system to identify safety implications and evaluate trade-offs and design alternatives. This provide a 'high-level' assessment using a conceptual system before detailed design is carried out to identify safety implications and evaluate design alternatives.

The PHA is performed using a system model that defines:

- scope and boundary of system;
- operating modes;
- system inputs, outputs and functions;
- the preliminary internal structure; and
- outputs from the PHI.

Note: PHA requires sufficient detail to employ a systematic method of failure analysis, such as functional failure analysis (FFA) or event tree analysis (ETA) see ISO 62502:2011.

The PHA is generally a brainstorming process to refine identified risks, identify additional risks and undertake an initial risk assessment. These are used to validate the derived requirements, develop the hazard log and produce a PHA report (Figure 8).

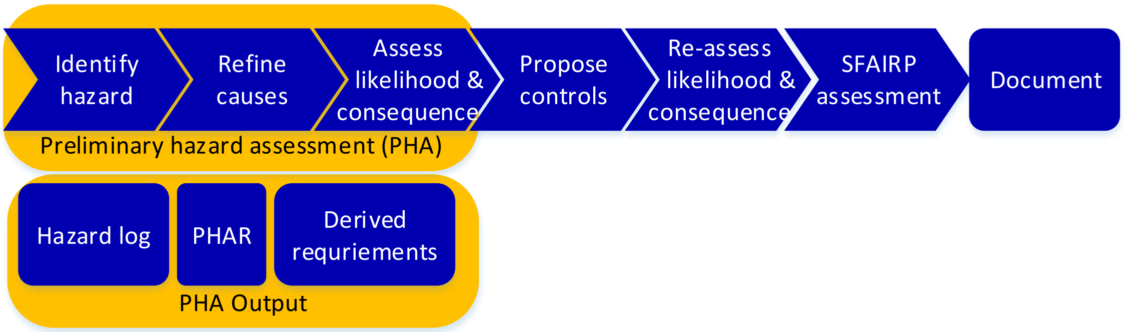


Figure 8 - Hazard assessment: PHA

The PHA should include identification of hazards which relate to complete system behaviour, considering hazards associated with:

- all operational modes and circumstances;
- degraded function;
- loss, inappropriate activation and incorrect application of each system function; and

- externally initiated hazards.

Where possible, the hazard effects, causes, and proposed control or mitigation measures should be considered.

PHA Output: The following documents should be retained as supporting evidence to development of SARs and for auditing/control of the SSA process:

- Hazard log.
- PHA records including an attendance list, meeting minutes and any subsequent action items.
- Preliminary hazard analysis report (PHAR.
- Documentation of any applicable update to requirement documentation.

4.2.1.3 System hazard analysis

The system hazard analysis (SHA) is undertaken when the system design is sufficiently developed to assess the system as a whole. The SHA provides a 'low-level' assessment of the design, considering actual hardware and software components in addition to interactions between these components. The SHA should not be undertaken to make significant changes to the configuration, however should provide a clear outline of controls in place to ensure safety of people and provide a safe SFAIRP assessment of the system.

Note: SHA requires systematic methods to analyse failures, such as:

- hazard and operability studies (HAZops), see ISO 61882:2016;

- fault tree analysis (FTA), see ISO 61025:2007; or

- failure mode effects (and criticality) analysis (FME(C)A), see ISO 60812:2006.

As the SHA requires significant detail on the system, this should be undertaken during detailed design phases resulting in no configuration changes (or minor only). The SHA (Figure 9) should assess risks associated with how the system is to be operated and therefore should provide:

- confirmation of implemented design controls;
- recommendations in relation to administrative controls;
- any safety related application conditions (SRACs); and
- SFAIRP assessment for all hazards.

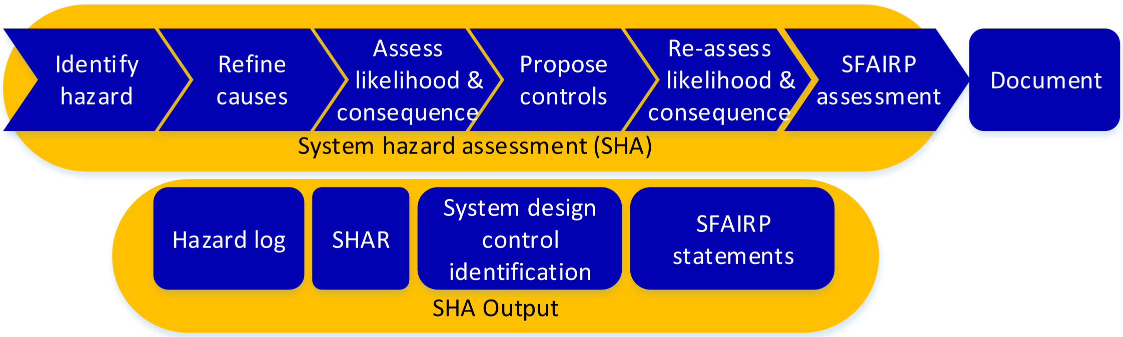

Identify hazard
Refine causes
Assess likelihood & consequence
Propose controls
Re-assess likelihood & consequence
SFAIRP assessment
Document
System hazard assessment (SHA)
Hazard log
SHAR
System design control identification
SFAIRP statements
SHA Output

Figure 9 - Hazard analysis: SHA

The SHA should always be undertaken via workshop with all applicable stakeholders and SMEs present in order to support the SFAIRP assessment, with all decisions documented to provide evidence of the assessment process.

For SHA a systematic method should be used to analyse systematic failures, such as hazard and operability studies (HAZops, refer ISO 61882:2016 - Hazard and operability studies (HAZOP studies). Application guide), fault tree analysis (FTA, refer ISO 61025:2007 Fault tree analysis (FTA) and failure mode effects analysis (FMEA, refer ISO 60812:2006 Analysis techniques for system reliability. Procedure for failure mode and effects analysis [FMEA]) sometimes combined the consideration of criticality – FME(C)A. HAZops can also be adapted computer applications by considering additional flows associated with data flows and interconnections and in this case the acronym becomes CHAZops.

It can often be difficult to decide what sort of techniques to use. Table 2 shows some of the indicative techniques that can be used. The choice of technique(s) should be based on the purpose of the analysis - known/unknown causes and consequences.

Table 2 - How to determine the technique to use based on purpose of the analysis

	Known Consequences	Unknown Consequences
Known Causes	Verification FME(C)A, ETA	Consequence Analysis FME(C)A, ETA
Unknown Causes	Causal Analysis FTA	Exploratory Analysis HAZops

There are four different types of analysis and a number of tools, some sit across each combination of known/unknown cause and consequence:

- When there are unknown causes and unknown consequences, the approach needs to be exploratory in nature and HAZop is a good tool, HAZop is suitable for PHI and PHA, but it works best in SHA.
- When there are known causes and known consequences, PHA would have already been done, and so FME(C)A and ETA are good tools to use in this verification area. ETA is a good tool in PHA.
- When there are known consequences and unknown causes, some PHA would have already been done to identify consequences, but the causes are unknown in terms of what components are going to lead to those hazards. In this causal analysis area FTA is a good tool.
- When there are unknown consequences and known causes, experience with the component may tell if they will fail in a certain way, e.g. a switch has two failure modes – stuck on and stuck off. In other more complex components, there is a set of failure rates associated with them. If the causes are known but not the consequences, then in the consequence analysis area FMEA and ETA are good tools.

Reliability block diagrams (RBD) can be used to assess the reliability of the system. The RBDs of the function of the system can be developed in either parallel or series:

- Series means that both of them have to be operating correctly for the system to be operating correctly.
- Parallel means only one of them needs to be operating correctly for the system to be operating correctly.

Having developed the system as an RBD a reliability figure can be given to each component in the system, then using probability theory the reliability of the system as a whole can be calculated.

SILs have been discussed where they were studies on high-level functions. The process is repeated at a low-level component level.

SHA Output: The following documents should be retained as supporting evidence to development of SARs and for auditing/control of the SSA process:

- Updated hazard log.
- SHA records including an attendance list, meeting minutes and any subsequent action items.
- System hazard analysis report (SHAR).

The SHAR should include:

- identification of hazard causes of the system, including what the components are that fail or even the combination of failing components;
- further justification of the preliminary and system risk and integrity level assignments made;
- details of risk assessments carried out to date;
- an updated set of safety requirements as component level and safety requirements are looked at;
- SILs assignation in the same way as discussed for high-level functions, e.g. how much integrity these components are going to need to have; and
- risk apportionment to various components so riskiest and those that have to be most reliable can be identified.

It is important to note that even if the SHA process determines that the project is not one of highest safety criticality, a record should be kept as evidence for due diligence process.

Note: the risk assessment techniques mentioned here are the most common used for PHA and SHA, however there are many more techniques available in:

- SA/SNZ HB 436:2013 Risk management guidelines – Companion to ISO 3100:2009, and
- ISO 31010:2009 Risk management – Risk assessment techniques.

4.2.2 Additional hazard analysis activities

Additional hazard analysis activities may be required depending on the scope or complexity of the system under consideration to examine subsystems, interfaces and operational characteristics. The organisation may also impose additional activities as deemed appropriate.

While the following sections provide less detail on these activities, the process and output are similar to the PHA and SHA discussed above.

4.2.2.1 Subsystem hazard analysis

The subsystem hazard analysis (SSHA) is undertaken for a system made up of multiple interdependent subsystems or components, therefore it is typically undertaken during the detailed design phase.

The purpose of the SSHA is to examine, in isolation, the operation and interaction with subsystems/components to identify and assess hazards related to normal operation, complete/partial failure, unintended operation or degraded operation of individual subsystems/components. This should provide data on any controls that may be implemented on the subsystem level (Figure 10).

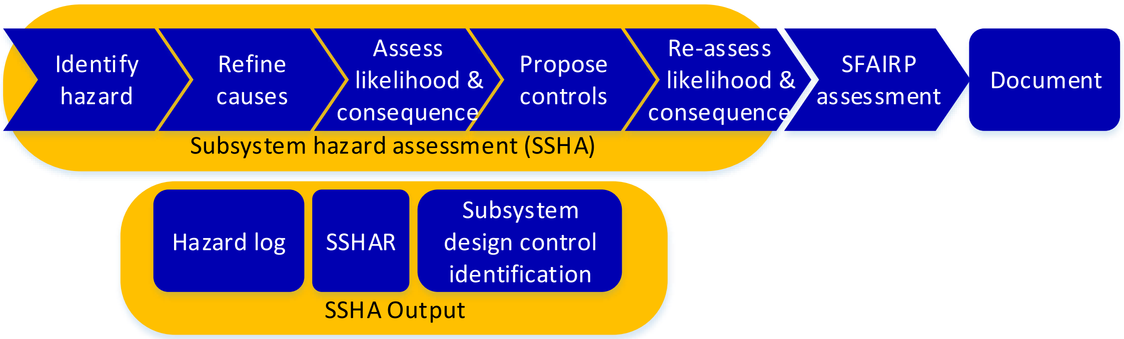

Identify hazard
Refine causes
Assess likelihood & consequence
Propose controls
Re-assess likelihood & consequence
SFAIRP assessment
Document
Subsystem hazard assessment (SSHA)
Hazard log
SSHAR
Subsystem design control identification
SSHA Output

Figure 10 - Hazard assessment: SSHA

To avoid repetition, where it is identified that the hazard affects the system as a whole, these hazards should be managed within the SHA process.

4.2.2.2 Interface hazard analysis

The interface hazard analysis (IHA) is typically undertaken when a system design is mature to identify hazards associated with interfaces of the system to other rail or transport assets. An IHA is therefore typically undertaken following the SHA and is chiefly undertaken to identify controls which require some interaction with other systems or entities. (Figure 11)

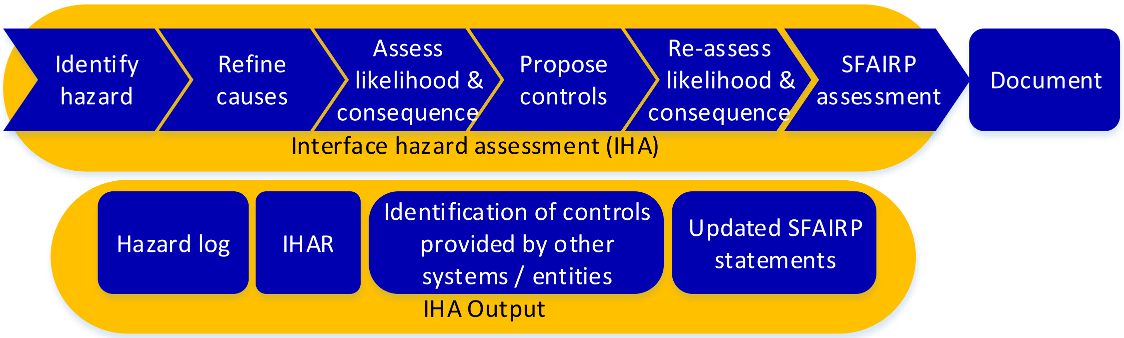

Identify hazard
Refine causes
Assess likelihood & consequence
Propose controls
Re-assess likelihood & consequence
SFAIRP assessment
Document
Interface hazard assessment (IHA)
Hazard log
IHAR
Identification of controls provided by other systems / entities
Updated SFAIRP statements
IHA Output

Figure 11 - Hazard assessment: IHA

As the system may not be able to affect the design of other systems or entities, the IHA typically allocates responsibilities to other parties and provides recommendations/SRACs necessary to ensure that the system is safe SFAIRP.

4.2.2.3 Operating and support hazard analysis

The operating and support hazard analysis (OSHA) is typically undertaken when a system design is mature to identify hazards associated with how the system is operated and the systems, processes and facilities required to support the system. An OSHA is therefore typically undertaken following all other hazard assessment activities and is chiefly undertaken to validate the safe operation/support of the system and identify applicable administrative controls necessary throughout the operational life of the system (Figure 12).

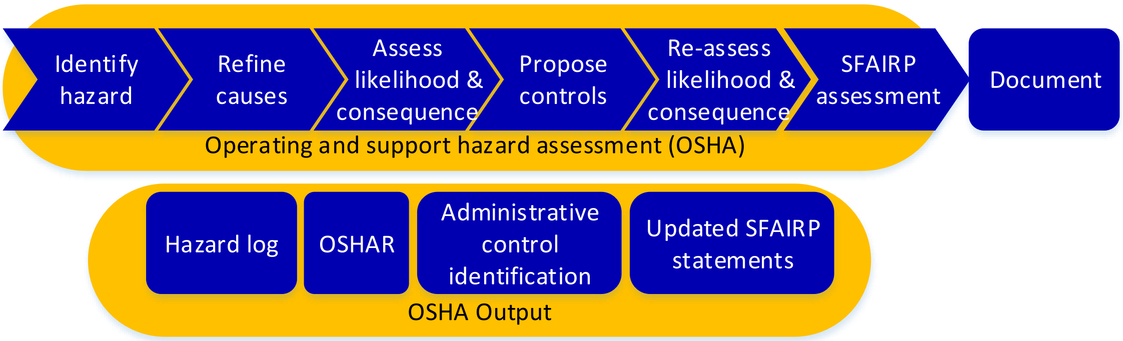

Identify hazard
Refine causes
Assess likelihood & consequence
Propose controls
Re-assess likelihood & consequence
SFAIRP assessment
Document
Operating and support hazard assessment (OSHA)
Hazard log
OSHAR
Administrative control identification
Updated SFAIRP statements
OSHA Output

Figure 12 - Hazard assessment: OSHA

4.2.3 Hazard analysis documentation

Hazard analysis documentation includes a range of reports and processes as outlined below:

4.2.3.1 Hazard analysis report

Hazard analysis reports (HAR) should be developed using the output of each hazard analysis workshop (sections 4.2.1.1 and 4.2.2) in accordance with the SSAMP. These assessments are subsequently used as supporting evidence in the SAR.

The HAR provides an outline of the system and background, highlights any key risks and provides a summary of the risk assessment at the time of writing. This should include:

- a brief description of the system and its environment;
- an overview of the systems functions and safety features;
- the safety objective of the system;
- justification of the preliminary risk and integrity level assignments made;
- target failure rates;
- details of risk assessments carried out to date;
- sources of any data used in the analysis; and
- a bibliography of all documents used.

The above is then used to guide decisions on the design process and acceptance of the system. Along with the PHL, HARs form part of the SAR.

4.2.3.2 Project hazard log

The project hazard log (PHL) should be a 'living' document which should be progressively updated during hazard identification and assessment activities. Further, the PHL should be managed by SSA Practitioners and updated as required.

The hazard log should include sufficient detail to define the hazard, identify applicable controls and provide an argument that the hazard has been eliminated or reduced SFAIRP. In general, the PHL should include the following details:

- Hazard identification:
  - unique identifier for each hazard;
  - hazard source (traceability of source of hazard);
  - hazard title;
  - systems (and subsystems) to which hazard applies;
  - causes;
  - hazard description (a concise statement of how the hazard occurs and affects people);
  - hazard owner
  - potential consequences; and
  - applicable assumptions, constraints and dependencies.
- Control measures:
  - unique identifier for each control;
  - control title;
  - type of control (see hierarchy of controls in Section 4.2.6.9);
  - control description (outline he control and how this affects the hazard);
  - control status (proposed, implemented, transferred or rejected);
  - control owner; and
  - applicable references.
- Post control hazard assessment:
  - post-control risk assessment;
  - SFAIRP statement;
  - any applicable references; and
  - hazard Status (open, managed, cancelled or transferred).

PHLs should clearly articulate any assumptions, constraints, or dependencies which underpin the assessments documented in the hazard log.

Even if the project is deemed not of high safety criticality, the PHL a record should be kept as evidence for due diligence process.

4.2.4 Safety in design workshops

Where the design of a system is well understood and there are little (if any) novel elements to a design it is appropriate to simplify the hazard assessment process by undertaking the safety in design (SiD) workshop approach, however this approach must be adequately justified within the SSAMP.

Note: SiD workshops are undertaken when a design is known, non-complex and has little or no novel elements. Examples include commission/construction of additional track, stabling or procurement of additional assets of an extant rail fleet.

The justification for undertaking an SiD approach should be clearly outlined within the SSAMP.

When undertaking an SiD process:

- SiD workshops should be broken down to support major milestones within the SE lifecycle, with an SAR developed following the SiD workshop to support progress of the project;
- it is anticipated that the majority of risks should be sourced from extant hazard logs, the SiD workshop should only consider additional risks (or changes to extant risks) that are affected by the project scope; and
- the SiD workshops should consider if the extant controls are sufficient (SFAIRP) and where appropriate identify additional controls.

Where an SiD process identifies that additional controls are necessary to ensure that a design is safe SFAIRP above that of the extant systems, an outcome of the SiD process should be a requirement to consider implementation of the control into extant systems.

4.2.5 Safety review

The SSA program should be reviewed periodically throughout the design process to validate conduct of the SSAMP and to review the SSAMP itself and should take into account both SSA management outputs as well as external events that may affect or inform the SSA process. The safety review may include any system safety activity as indicated in Figure 13.

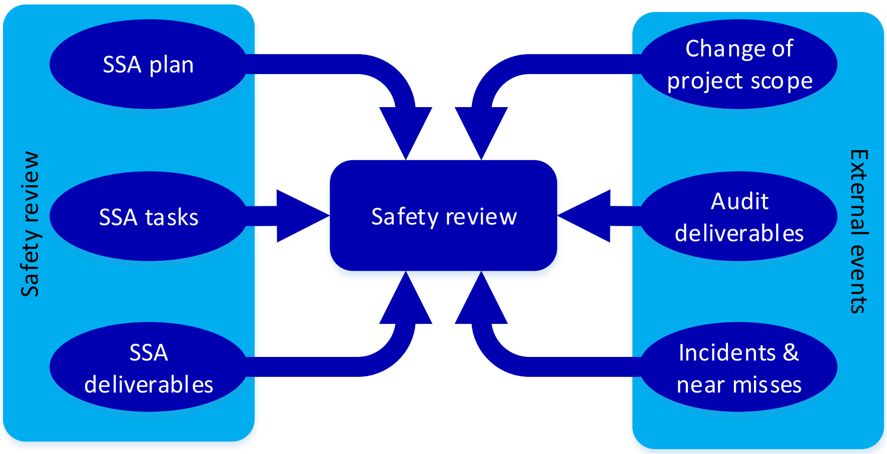


Figure 13- Safety review considerations

As part of this review the following should be considered:

- Criticality/SSAMP scope: The scope of tasks should be reviewed to ensure that these are sufficient to meet the safety integrity of the project. This may require additional tasks to be undertaken or identify that some tasks are not necessary.
- Conduct of SSA tasks: Adherence to the SSAMP should be assessed, including quality and applicability of documentation produced.

The output of these safety reviews should include:

- formal record of the review and any recommendations;
- update to the SSAMP; and
- any modification to the PHL.

4.2.6 Other issues related to hazard management

4.2.6.1 Hazard analysis – qualitative or quantitative

Hazard analysis may be qualitative (descriptive), semi-quantitative (using ordinal scales), quantitative (using ratio scales) or a combination of these depending on the circumstances. The approach to hazard assessment should be clearly identified and justified within the SSAMP, the most common approach is to use qualitative methods however where appropriate quantitative methods provide greater certainty. Table 3 outlines some differences in qualitative and quantitative hazard analysis.

Table 3 - Qualitative vs quantitative hazard analysis

Qualitative	Quantitative
• Relies mainly upon expert judgment and past experience.	• Relies upon failure.
• Requires less effort/time to complete; and • Does not require significant data to undertake.	• Can provide greater precision; and • Clear demonstration that hazards meet the tolerable hazard rate (THR).
• Results may not be as precise; • Requires significant workshop time and discussion.	• Requires detailed data on failure/hazard rates; • Is only effective when systems and interfaces are clearly defined and may be modelled accurately; and • Requires analytical methods for hazard assessment (FMECA etc).

During the PHI and PHA the system is typically conceptual, due to the lack of data. Qualitative methods are better used when identifying the PHL. During later design stages (such SSHA, SHA and IHA) there is more detailed data available and quantitative assessments may be completed.

When considering the use of qualitative methods, considerations should include:

- hazards which may lead to a major or catastrophic consequence may require a greater level of analysis;
- their appropriateness to highly novel systems or products; these may require a quantitative approach due to a lack of prior experience/knowledge; and
- SILs required and that the approach is capable of arriving at THRs.

The quantitative approach should only be considered if a higher level of confidence is required, it is generally not justified unless:

- the significance of the decision to be made is substantial;
- the data to support the analysis is available and reliable; and
- the decision makers are able to use quantitative results.

If these requirements are not satisfied then qualitative analysis is typically more appropriate, noting that where critical risks exist these may be assessed qualitatively to support the hazard assessment.

4.2.6.2 Safety vs reliability

Safety is defined as a "*measure of the degree of freedom from risk or conditions that can cause death, physical harm, or equipment, or property damage*" (Stephenson, 1991).

Reliability is "*ability to perform as required, without failure, for a given time interval, under given conditions*", (EN 50126-1:2017 adapted from IEC 60050-192:2015), and the following should be noted:

- Systems can be reliable but not safe.
- Systems can be safe but not reliable.
- A system needs to be safe under all foreseeable circumstances.

Reliability and safety risk has often been confused, they are not synonymous, reliability is about componentry whereas safety risk cannot be defined or measured without considering the environment.

There are six key techniques to make systems more reliable:

- Parallel redundancy – two or more components operating simultaneously, such that if one fails the other still performs.
- Standby sparing – as above but may be an auto or manual switchover.
- Safety factors and margins – overdesigning to withstand stress – most appropriate for mechanical devices.
- Derating – operational stress ratings of components is reduced – most appropriate in electrical components.
- Screening – components eliminated where tests show they may fail in an unacceptable time.
- Time replacements – replacement before failure.

Reliability engineering cannot replace systems safety, while sometimes they can support each other, sometimes they have opposing goals.

4.2.6.3 Safety vs availability

Safety and availability are inter-linked in the sense that a weakness in either or mismanagement of conflicts between safety and availability requirements may prevent achievement of a dependable system. Reliability is defined as the "*ability to perform as required, without failure, for a given time interval, under given conditions*", (EN 50126-1:2017 adapted from IEC 60050-192:2015). The inter-linking of railway RAMS elements, reliability, availability, and maintainability and safety is shown in Figure 14.

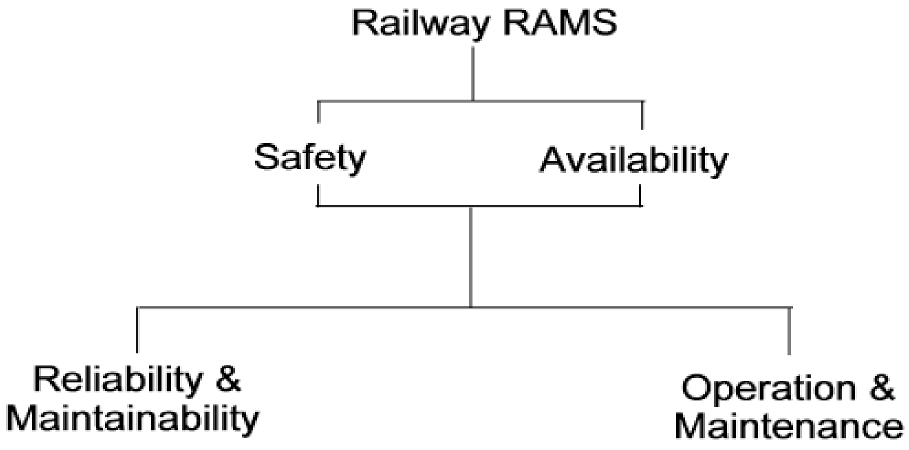


Figure 14 - Interrelation of railway RAMS elements (EN50126-1: 1999)

Attainment of in-service safety and availability targets can only be achieved by meeting all reliability and maintainability requirements and controlling the ongoing, long-term, maintenance and operational activities and the system environment.

Failures in a system, operating within the bounds of an application and environment, will have some effect on the behaviour of the system. All failures adversely affect the system reliability whereas only some specific failures will have an adverse effect on safety within the particular application. These links are shown in Figure 15.

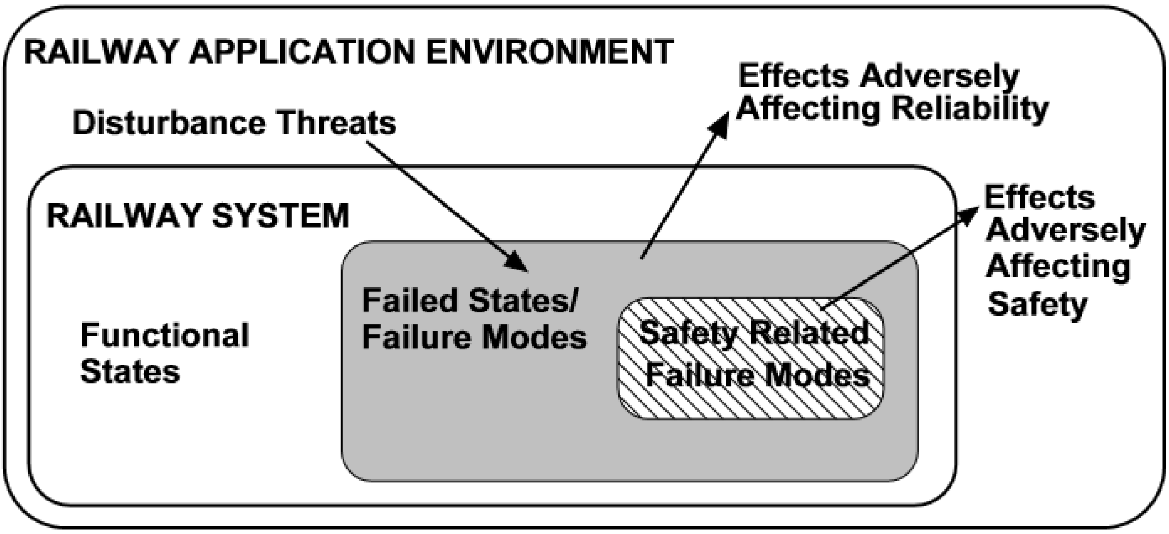

RAILWAY APPLICATION ENVIRONMENT
Disturbance Threats
Effects Adversely Affecting Reliability
RAILWAY SYSTEM
Effects Adversely Affecting Safety
Functional States
Failed States/ Failure Modes
Safety Related Failure Modes

Figure 15 - Effects of failures within a system

4.2.6.4 Systems and boundaries

A system is defined as an integrated set of elements, subsystems, or assemblies that accomplish a defined objective. These elements include products, (hardware, software, firmware), processes, people, information, techniques, facilities, services and other support elements (INCOSE, 2015).

Before undertaking any SSA work, the system boundaries need to be defined because safety is a whole of system issue. Then thought needs to go into possible failures, i.e. the cessation of required function or performance of undesired function/s, within the system boundary. This can cause the system to enter into a hazardous state, which when interfacing with co-effectors (i.e. an external event within the environment in which a system operates) can cause an accident.

4.2.6.5 Software

Railway technology employs software-intensive systems, where many system functions are implemented in software, for applications at all levels of safety criticality.

Writing software for safety-critical and safety-related applications is different from business applications. With software, it is easy to introduce unmanageable complexity and unpredictable component behaviour. The behaviour of software is not continuous; behaviour can change radically with small changes in input values. Failures are systematic, rather than random, due to latent errors in the design. Multiple redundant systems are vulnerable to common failure mode.

Safety development is about improving the correctness of the software design, rather than the reliability of the equipment. The objective is to produce software with zero faults. The more rigorous the methods used, the more likely the goal will be achieved. Standards for safety-related systems recommend or require methods for software at different levels of criticality. For example, EN 50128:2011, Annex A has tables of recommended practises addressing these issues, at different SILs.

RTOs and application developers should determine, justify and uphold an appropriate software development standard.

Given the stringent requirements and additional costs of safety-related software, developers should consider restricting safety functions to smaller, more readily verified components, while other components undertake the bulk of functionality.

Commercial, off-the shelf software (COTS) should not be used without due certification and consideration of the safety functions of the application. This includes, for example, regular business operating systems which are not suitable for real-time systems at the highest levels of criticality. Similar considerations apply to firmware, custom digital electronic hardware etc, which also encapsulate complex design logic.

4.2.6.6 Hazard assessment process

There are many approaches used to assess hazards, this section does not intend to provide definitive guidance on these processes. Table 4 shows a simple outline which may support other hazard assessment techniques.

Table 4 – Other hazard assessment techniques

	Detail
Risk Identification	Formal risk identification activities are discussed in detail at section 4.2 and 4.10, however hazards may be identified at any stage throughout the system lifecycle. Regardless of their source, hazards are to be assessed, controlled and accepted in the same manner. Potential risk sources may be: • SME recommendation; • User/operator recommendation; • Incident reports; and • Design process.
Refine Causes	Once risks have been identified it is important to review the causal events to validate that the risk exists and to identify other means by which the risk may eventuate. Prior to continuing to risk assessment, it is recommended that the list of risks is reviewed to ensure that each risk is unique to avoid duplication of effort.
Assess Likelihood & Consequences	Risks are to be assessed prior to identification of any control actions to provide a baseline of risks.
Propose Controls	Controls should be identified and assessed through hazard assessment working groups, further detail of control assessment is included below.
Re-assess Likelihood & Consequences	Once controls have been identified the likelihood and consequences are to be re-assessed to define the status of the hazard.
SFAIRP Assessment	Each hazard is to be assessed within working groups to make the claim that they are minimised SFAIRP. Further detail of SFAIRP assessment is included below

4.2.6.7 Hazard assessment working group

The hazard assessment working groups (see sections 4.2.1, 4.2.2 and 4.2.4) require a diverse team to generate and review hazards associated with the design, construction, operation, maintenance and disposal of trail assets. Depending on the requirements of the assessment, the working group should include:

- customer(s);
- designers;
- engineers (SMEs and system engineers);
- manufacturers;
- user(s) (operators and maintainers);
- project managers; and
- SSA Practitioners.

The output from the working group should consist of any update to the hazard log, workgroup minutes and any action items as a result of unresolved issues. The working group chair is responsible to provide all attendees copies of meeting documentation and preparation of any subsequent hazard analysis reports.

4.1.1.1 Hazard control strategies and types of failures

In SSA there are four main categories of risk reduction strategies, given in the order that they should be applied:

- Hazard elimination.
- Hazard reduction.

- Hazard control.
- Damage limitation.

There needs to be differing control strategies depending on whether the failures are random or systematic, i.e.

- Random failures (associated with hardware component failures – gather right data may be able to predict probability of failure in a given time) can be mitigated by:
    - using the most reliable components available, noting that manufacturers will often supply known failure rates in the product specification;
    - applying redundancy to achieve overall reliability;
    - performing preventative maintenance to replace components before faults arise; and
    - executing on-line or off-line diagnostic checks.

In theory systematic failures (associated with software faults – not random so not easy to predict their impact of system reliability) can be eliminated, but in practice it is too costly, therefore, instead, focus effort on the most critical areas by:

- identifying safety requirements using hazard analysis.
- assessing risk in system and operational context, then look to:
    - elimination or reduction of errors using quality development processes by verifying compliance with safety requirements and
    - integrating and test against safety requirements.

4.1.1.2 Control application and SFAIRP assessment

RTOs have a duty under the RSNL to identify all reasonably foreseeable safety risks, to eliminate the risk if reasonably practicable or, if it is not reasonably practicable to eliminate a risk, the safety risk must be reduced SFAIRP.

For each hazard, all potential safety controls should be identified and documented in a hazard log. Controls should be identified against the hierarchy of controls, where possible these should rely on the most effective controls practicable (see figure 16).

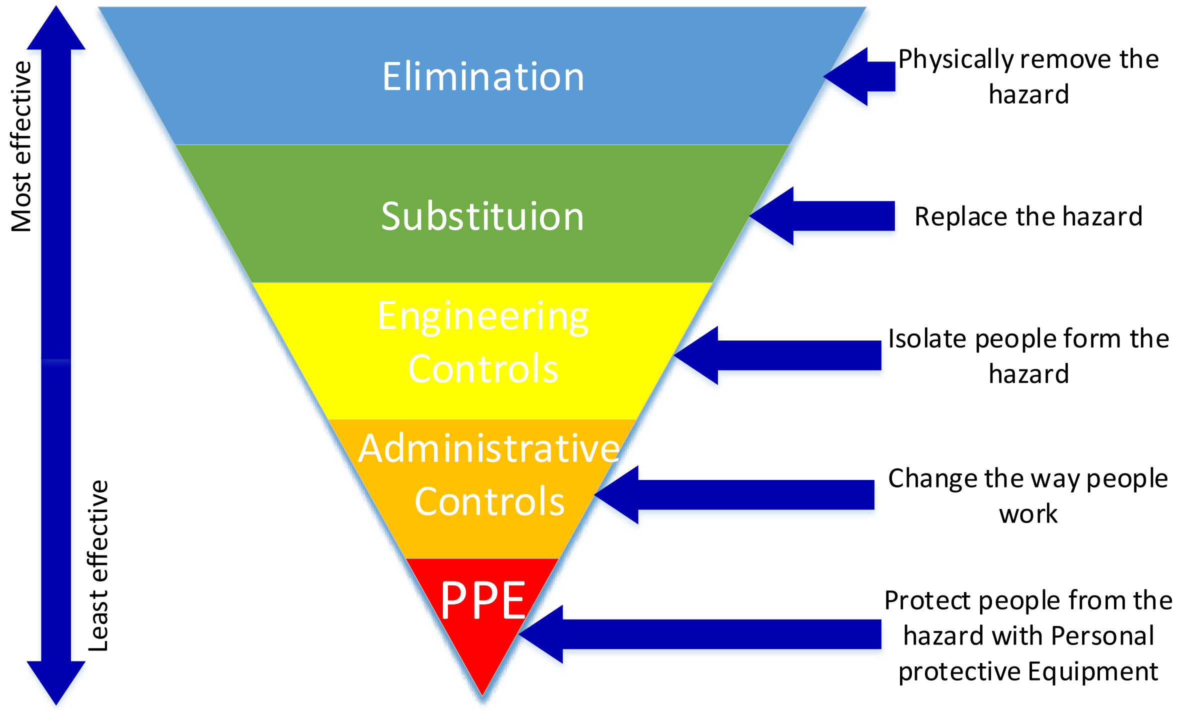

Most effective
Least effective
Elimination
Substituion
Engineering Controls
Administrative Controls
PPE
Physically remove the hazard
Replace the hazard
Isolate people form the hazard
Change the way people work
Protect people from the hazard with Personal protective Equipment

Figure 16 – The hierarchy of controls (National Institute for Occupational Safety and Health, DART, USA May 2018)

All controls should be identified and discussed through design review and hazard assessment workshops. The hazard log should contain sufficient information to:

- identify the control;
- outline how the control affects the hazard;
- identify the responsible party for that control;
- demonstrate if the control is proposed, implemented or rejected; and
- where applicable justify why a control is rejected.

Controls need to be applied until there are no more reasonably practicable controls available that will reduce the risk any further, with the rationale recorded for rejecting any controls not implemented in the hazard log. The assertion that a hazard has been mitigated SFAIRP should be validated during hazard assessment activities and recorded within the hazard log.

There is no prescriptive rule that can be used to determine whether or not a control is reasonably practicable. Instead, there are a number of principles that should be considered, including what can be done, should be done, unless it is reasonable in the circumstances to do less. Specific reference is made to the ONRSR Guideline: Meaning of duty to ensure safety so far as is reasonably practicable – SFAIRP and RISSB Guideline – Safe Decisions.

A potential control may generally be considered to be reasonably practicable if any one of the following applies:

- It is required by law.
- It is readily commercially available.
- It is recommended by reputable standards, codes of practice, or guidance.
- It has been implemented in similar situations elsewhere.

- Professional judgement considers it to be reasonably practicable.
- The cost is relatively low.

A potential control is generally considered to be not reasonably practicable if:

- it would introduce other safety risks that outweigh the safety benefits;
- it prevents the implementation of an alternative, more effective control;
- it would be ineffective in reducing the risk;
- it would prevent the organisation/system from achieving its required function; or
- the costs of implementing the control are grossly disproportionate to the safety benefits.

When considering whether or not the cost of implementing a control for a new-build project is grossly disproportionate, the cost that must be considered is the cost that would have been incurred had you decided to implement the control at the start of the project.

The following arguments are not generally considered sufficient to claim that a control is not reasonably practicable:

- The control will not be accepted by a stakeholder group (e.g. unions, customers, rail operator, ONRSR etc).
- It would conflict with the preference of, or a decision made by, an executive or political authority.
- There are insufficient funds available to implement the control.
- The time required to implement the control is inconsistent with the project schedule.
- It is outside the current scope of the project or a project contract.
- It would detract resources away from dealing with a higher priority risk.
- It does not comply with local practice.

The following arguments are not generally sufficient by themselves to claim that the risk of a hazard has been reduced SFAIRP:

- The system meets the minimum requirements of a standard.
- It is as safe as systems in use elsewhere.
- It is as safe as the system it is replacing.
- Key stakeholders are willing to accept the current level of risk.
- The system uses ‘type approved’ equipment (see AS/RISSB 7659:2012 Rail equipment type approval).

4.3 Independent safety assessment

Where deemed necessary by impact assessment an ISA should be appointed to provide judgement and form recommendations, separate and independent from the organisation in accordance with the SSAMP. Factors which determine the decision to engage an ISA include the scale, safety criticality and novelty of the system, and the experience and maturity of the Supplier and RTO.

To ensure this requirement is met, a documented ISA brief and plan appropriate to the scale of the change being assessed should be created and implemented. Independent safety assessment is an investigative activity, aimed at producing an informed judgment on the level of safety achieved, rather than an audit of activities undertaken.

An ISA is appointed to assess that:

- safety requirements are appropriate and adequate for the planned application;
- safety management is appropriate and sufficient to ensure that SSA activities are adequately undertaken;
- all safety related issues have been identified and are appropriately managed;
- SSA activities are being undertaken in accordance with documented processes; and
- the safety argument and evidence are complete and robust and demonstrates that the system meets its safety objectives and is safe SFAIRP.

Independent safety assessment is a significant body of work in its own right. The ISA should be engaged early in the system development lifecycle, with agreed objectives and assessment plan.

The level of independence of the ISA should be determined by impact assessment. The ISA will generally be fully independent of the supplier. The ISA should also be independent of the procuring RTO, or at least the RTO's project management line. This provides a buffer against pressure to accept an unready product. To be effective, access and a good working relationship between the ISA and supplier should be established.

This independent judgement provides an additional level of assurance to give the asset and assurance acceptor confidence in the validity of the safety argument presented and the development of the progressive assurance. The ISA will generally present their judgement to the CCB of other acceptance authority at relevant assurance gates to support the decision-making process.

An independent safety assessment is a team-based activity. It is led by a lead assessor that is suitably qualified and experienced in system safety supported by a team of SMA with competence in disciplines relevant to the assessment scope. For example, an ISA for a signalling project would require a signalling SME and potentially a testing and commissioning SME in order to ensure an appropriate assessment of the engineering arrangements and activities are conducted. Quality and competence of staffing is important in getting best value from an ISA.

Independent safety assessment should be conducted in a risk-based manner with the majority of effort focussed in the areas of highest risk.

Independent safety assessment activities include safety management and other audits, reviews of safety management and safety engineering arrangements, document assessments, witnessing of project activities, technical interviews and vertical slice analysis.

Independent safety assessment outcomes should be reported in independent safety assessment reports making a clear recommendation based on the judgement reached linked to the evidence witnessed by the assessment activities.

The assessment may undertake product and process reviews as part of the assessment:

- Process-focused reviews to check how things are being done, looking for objective evidence that evidence that the plans for safety are being followed.
- Product- focused reviews to check what is being produced, looking for objective evidence that the safety requirements are being met.

The frequency and rigour for each type of review, and the degree of independence of the reviewer, will depend on the extent of the risk and novelty and on how complicated the project is.

The assessment activities should include:

- interviews with project personnel;
- examination of project documents;
- observation of normal working practices, project activities and conditions;
- re-work of parts of the safety analysis work to check accuracy, concentrating on particularly critical areas or where the assessor has reason to suspect a problem (for assessment only); and
- demonstrations arranged at the assessor's request.

The output of the independent safety assessment will be an independent safety assessment report (ISAR). The plan should be brief and should include:

- a statement of the assessment requirements, according to the assessment remit, but taking into account any agreed amendments;
- identification of any dependencies on the project or others, such as access to project personnel or documents;
- identification of the assessor or assessment team, including qualifications, experience and level of independence;
- identification of individuals to be interviewed;
- management arrangements for reporting findings and reviewing, endorsing and distributing;
- assessment reports;
- assessment timescales, including the expected date of issue of assessment reports; and
- communication channels, and the access rights of key stakeholders to ISA documentation and personnel.

In the case of an audit the ISAR should record the evidence for compliance or non-compliance with the plans for the SSA program activities.

4.4 Human factors integration

HFI is the process that considers HF within an integrated approach to the project lifecycle. It involves applying a systematic and scientific approach to the identification, tracking, and resolution of issues related to human-system interactions. Effective HFI ensures the balanced development of both the technological and human aspects of the system and delivers the desired safety and operational capability.

HFI can have a direct impact on SSA so it is critical that relevant HFI is integrated and issues and safety requirements are transferred into the SSA process. Evidence of HFI will form part of the safety case.

It important that HF is integrated with SSA through the whole lifecycle, including requirements development, hazard management, design development and verification and validation activities. HF requirements are an input the design development stage and are typically associated with ensuring a design meets the physical, functional or performance needs of its identified end users. HF requirements will be verified and validated as part of the HF activities in line with other systems engineering processes.

HFI deliverables may include:

- HF integration plan;
- HF issues register;
- HF assurance report; and
- verification/validation of derived requirements.

More detailed guidance is provided by international standards and guidelines and the following RISSB products:

- AS/RISSB 7470:2016 Human factors integration in engineering design - General requirements;
- Guideline - Integration of human factors in engineering design; and
- Guideline – Human factors integration to the project lifecycle (currently under development).

HF incorporates a number of different domains and resource areas including cognitive psychology, physical sciences and ergonomics, organisation design, human-machine interface design/useability and human reliability assessments. When HF advice is required it is important to use a person with an appropriate competency for the required task.

4.5 Applying SIL methods in a SFAIRP environment

Safety integrity is specified as discrete levels (1 to 4 in EN50129:2003) that provide a measure of confidence in the integrity of the safety function. In deriving SILs, the tolerable hazard rate (THR) for each hazard is apportioned to system functions and the sub-systems that perform those functions. The THR is then translated to a SIL.

As the allocation of a SIL requirement is intended to meet an explicit level of tolerability (i.e. THR), meeting the resulting SIL levels will not, by itself, demonstrate the achievement of SFAIRP. At best, SIL analysis can identify the minimum SIL rating for any system element or safety function that would enable a system to meet a pre-determined safety target.

In order to satisfy SFAIRP it is necessary to also consider whether it would be reasonably practicable to implement SIL ratings that are higher than the minimum derived from the SIL analysis (and/or other risk controls) – particularly if products which could deliver higher ratings are readily available in the marketplace or have been implemented in other comparable systems. EN 50129:2003, especially Annex 5.1 and 5.2 defines an approach which may be useful for rail transport applications. Consistent application of EN 50129-2003 would help overcome the lack of harmonisation between functional safety standards and ensure all definitions are clearly defined within the SSAMP and approved prior to use.

Due to the potential sensitivity associated with establishing THRs amongst some stakeholders, and the potential for significant cost and schedule impacts if they are not agreed when required by the project life cycle, the SSAMP should either clearly articulate any THRs to be applied in the project, or else clearly identify the authority, procedure and schedule for their determination.

4.6 The safety case

The safety case is "*a documented demonstration that the product (e.g. a system, subsystem or equipment) complies with the specified safety requirements*", (IEC 60050-821:2017 and adopted by EN 50126-1:2017).It comprises a safety assurance report (SAR) along with supporting documents and evidence as shown in Figure 17. It is a means of documenting the safety justification of the system and is a record of all the safety activities associated with the system, throughout its life.

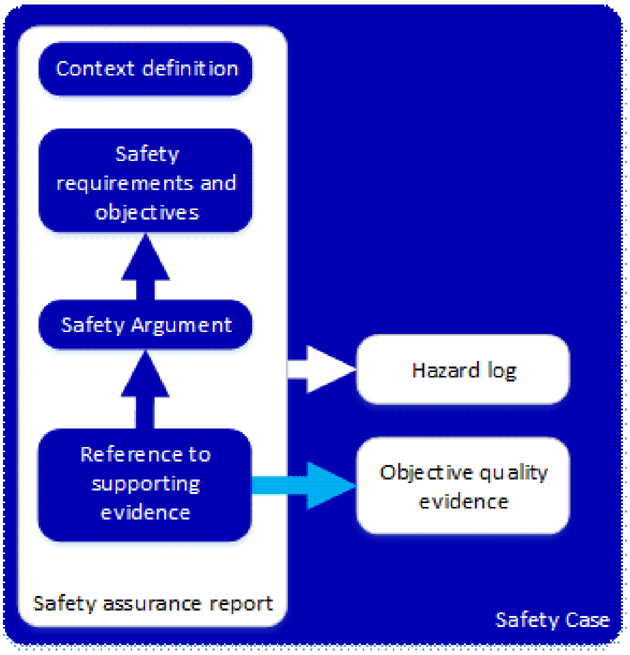

Context definition
Safety requirements and objectives
Safety Argument
Reference to supporting evidence
Hazard log
Objective quality evidence
Safety assurance report
Safety Case

Figure 17- The safety case

The SAR is a rigorous argument of why the system is safe SFAIRP and should communicate a clear, comprehensive and defensible argument that a system is acceptably safe to operate in a particular context. The SAR should be seen as a roadmap whereby the contextual and supporting evidence is analysed, and meeting the safety requirements is demonstrated, i.e. it provides traceability to all the relevant safety-related information. Preparation of the SAR is started early in the process and many other documented outcomes flow into it. It should include:

- the safety argument – a high level summary with appropriate sign-off that controls are in place that make risks SFAIRP;
- safety requirements and objectives – records overall goals and strategies;

- contextual information - this is helpful for all the intended audiences, but in particular for auditors and evaluators. It should include:
    - a specification of the safety requirements;
    - standards, codes and other criteria;
    - project and development constraints; and
    - supporting documents – these provide the building blocks upon which the SAR is built and contains the outputs of processes such as PHI, PHL and SHA.

A SAR will normally include a vast amount of data that can be easily lost if not structured appropriately. Most SARs are developed using word processing and spreadsheets, and the documents and the audit trail become cumbersome. More recently computer tools have been developed to manage the process though visibility and consistency of information.

Goal Structuring Notation (GSN) is a graphical method which may be used to document and communicate the safety argument within a SAR. GSN has a number of advantages over traditional text-based argument formats, in that it can be readily understood by stakeholders who are not safety professionals and provides an explicit structure to the safety argument which can make it easier to establish the 'completeness' of the argument. Further guidance on GSN is available in the GSN Community Standard V1, (November 2011).

Regardless of the above, the SAR still needs to be structured to be able to manage the information that gives the safety justification. A compounding issue is the input of multiple disciplines, i.e. software, hardware, analogue electronics, electrical engineering, mechanical engineering, pneumatics, hydraulics, HF and psychology. As such gathering and representing views on interactions and safety issues is complex and difficult.

At each stage of the SAR development the 'proof' in a safety assurance report must be carefully justified and assumptions made explicit, without this it is flawed. The production of the safety assurance report in a coherent argument is one of the most difficult and demanding aspects of creating a safety-critical system.

Change is inevitable and so the safety assurance report should be seen as a 'living-breathing' document and changes need to be managed in the safety assurance report for, but not limited to: user requirements, design solutions, acceptance of risk. The challenge is to efficiently maintain consistency, completeness and correctness of the safety assurance report in the presence of such change.

It is important that underlying assumptions, constraints, and dependencies relating to safety cases and risk assessments are explicitly articulated, as they provide critical contextual information that needs to be considered when evaluating the applicability of any assessment, or the acceptability of a reported risk.

These three elements can be described as follows:

Assumptions:

- a statement that can't be proven but is believed to be true (and is expected to remain true for the life of the system without further management); and

- the associated risk assessment cannot be relied upon unless the assumption is actually true.

Constraints:

- a limiting condition that is accepted on the operation of the system;
- it is the boundary condition for the safety argument. If we operate the system outside of a constraint, the safety argument may no longer be valid; and
- constraints are something the system operator will need to be mindful of for the life of the system; but
- constraints are not really suitable for conditions that require active management, monitoring and ongoing maintenance – those conditions should be implemented as controls in the hazard log.

Dependencies:

- an action or activity that has not yet been finished but will generally be completed before the system enters service;
- closure of the dependency may result in further amendments or additions to the risk assessment; and
- the risk assessment therefore can't be considered finalised until all dependencies have been closed out.

All assumptions, constraints, and dependencies should be clearly described in the SAR, and formally accepted by the relevant RTO prior to a system commencing operation.

4.7 Assurance and acceptance requirements

The safety argument established within the key stages of the SSA process such that it should be considered a progressive assurance process. The key documents that are produced as outputs at various stages form supporting evidence and appendices to the safety assurance report, being the principle assurance argument.

Acceptance is paramount and demonstrated through sign-off by the various responsible managers for their safety statements associated with their competency domains. These positions should be authorised to sign-off through a formal delegation by the accountable person.

The safety argument is then given authority by an overarching sign-off by an executive officer with formal accountability to do so.

Configuration authorities (also known as CCB) should be established by RTOs to facilitate the configuration management, assurance and staged acceptance of railway assets and systems for which they are delegated to manage within the full systems engineering lifecycle. CCBs can be run at sub-contractor, supplier or rail authority level.

4.8 Accreditation and variation

One of the uses for the safety case is to support an application for accreditation or a variation to accreditation. It needs to provide evidence of the process followed and controls put in place to ensure safety SFAIRP.

The purpose of accreditation or approval for a variation by the ONRSR is to demonstrate that a RTO has the competence and capacity to manage safety risks associated with its railway operations by implementing its SMS and to safely manage changes to its operations.

Although accreditation comes at the end of the project, planning for it is important, including robust verification and validation iterations, need to be commenced at an early stage. The process involves convincing an independent body of the matters identified in this guideline and it would be wise to ensure early liaison with that body to ensure communication channels are opened to foster a common understanding of all parties in the process.

This early liaison will define what standards are to be used as criteria documents, any variations and any internal criteria or other good practice that can be considered to demonstrate appropriate safety and integrity levels moving into operation and maintenance phase of the project and beyond.

As part of the SSAMP a verification plan needs to be developed and approved by any regulatory bodies who will be involved in the accreditation process. The verification plan should contain elements from the SSAMP to give enough context and then also the agreed criteria (including standards), development methods to be used and the documents to be provides as part of the certification. Should there be any deviations from standards then a justification also needs to be documented in the verification plan. This plan needs to be developed early in the process and signed by all parties and doing such should alleviate any unnecessary and expensive rework. However, that’s not to say that as the project unfolds the verification plan will not be updated as change is generally inevitable in large complex system development that could impact on certification.

Having previously said accreditation comes at the end of the project, i.e. a signed certificate, the process is continuous throughout the project with data and documents provided at key stage gates. This will then trigger reviews with the accrediting body with advice given on levels of satisfaction given by the certifying body at those stage gates.

It should be noted that accreditation may be conditional, i.e. it will impose certain operational constraints.

5 References

The reference material below has been drawn on to create this guideline or is a handy further reference on the subject of systems safety assurance.

A Guide to Hazard and Operability Studies, Chemical Industries Association, 1992

AS 61508.4: 2018, Functional safety of electrical/electronic/programmable electronic safety-related systems - Definitions and abbreviations

AS/RISSB 7470:2016 Human factors integration in engineering design - General requirements

AS/RISSB 7659:2012 Rail equipment type approval

BS 5760: Part 5 1991, Reliability of systems, equipment and components: Part 5 Guide to failure modes, effects and criticality analysis

Def(Aust)5679, Issue 2, 2008, Safety engineering for defence systems

Design and safety assessment of critical systems, Bozzano and Villafiorita, 2011

EN 50126-1:2017, Railway Applications - The specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 1: Generic RAMS process

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

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

EN 50129:2003, Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

EN 60812:2006, Analysis techniques for system reliability. Procedure for failure mode and effects analysis (FMEA)

EN 61882:2016, Hazard and operability studies (HAZOP studies). Application guide

EN 62502:2011, Analysis techniques for dependability. Event tree analysis (ETA

Engineering a safer world, Leveson, 2009

Engineering requirements, Hull et al, 2002

Engineering Safety Management, issue 4, ‘Yellow Book 4’, note withdrawn

GSN Community Standard V1, November 2011

Hazard Analysis Techniques for System Safety, Ericson, 2005

Hazard Management Procedure; Government of South Australia; April 2011 referenced in SAI Global Effective hazard identification and management 2012

HB 436:2013: risk management guidelines - Companion to AS/NZS ISO 31000:2009

Human factors in systems engineering, Chapanis, 1996

IEC 60050-192:2015, International electrotechnical vocabulary - Part 192: Dependability

IEC 60050-821:2017, International electrotechnical vocabulary - Part 821: Signalling and security apparatus for railways

IEC 60050-903:2013, International electrotechnical vocabulary - Part 902: Conformity assessment

IEC Guide 73:2014, Risk management - Vocabulary

INCOSE:2015, INCOSE systems engineering handbook: A guide for system life cycle processes and activities

International engineering safety management, 2013

Introduction to systems engineering, Sage and Armstrong, 2000

ISO 10007:2003, Quality management systems. Guidelines for configuration management

ISO 15288:2015, Systems and software engineering - System life cycle processes

ISO 31000:2018, Risk management. Guidelines

ISO 55000:2014, Asset management - Overview, principles and terminology

ISO 9000:20005, Quality management systems - Fundamentals and vocabulary

ISO Guide 51:1999, Safety aspects - Guidelines for their inclusion in standards

National Institute for Occupational Safety and Health, DART, USA May 2018

NUREG 0492, The Fault Tree Handbook, 1981

ONRSR Guideline, 2016, Major projects guideline

ONRSR Guideline, 2016: Meaning of duty to ensure safety so far as is reasonably practicable – SFAIRP

Rail safety national law, 2012

RC Commission Regulation 2096/2005

RISSB Guideline – Human factors integration to the project lifecycle (currently under development)

RISSB Guideline, 2016: Safe decisions

RISSB Guideline, 2017 - Integration of human factors in engineering design; and

Safety-critical computer systems, Storey, 1996

System engineering management, Blanchford and Blyler, 2016

System safety, Stephenson, 1991

System safety, Vincoli, 2006

Systems engineering: Coping with complexity, Stevens et al, 1998

Systems safety and computers, Leveson, 1995

TfNSW, 2016, Guide to Transport for NSW Framework for assuring the safety of rail assets and infrastructure

TfNSW, 2016, System safety standard for new or altered assets

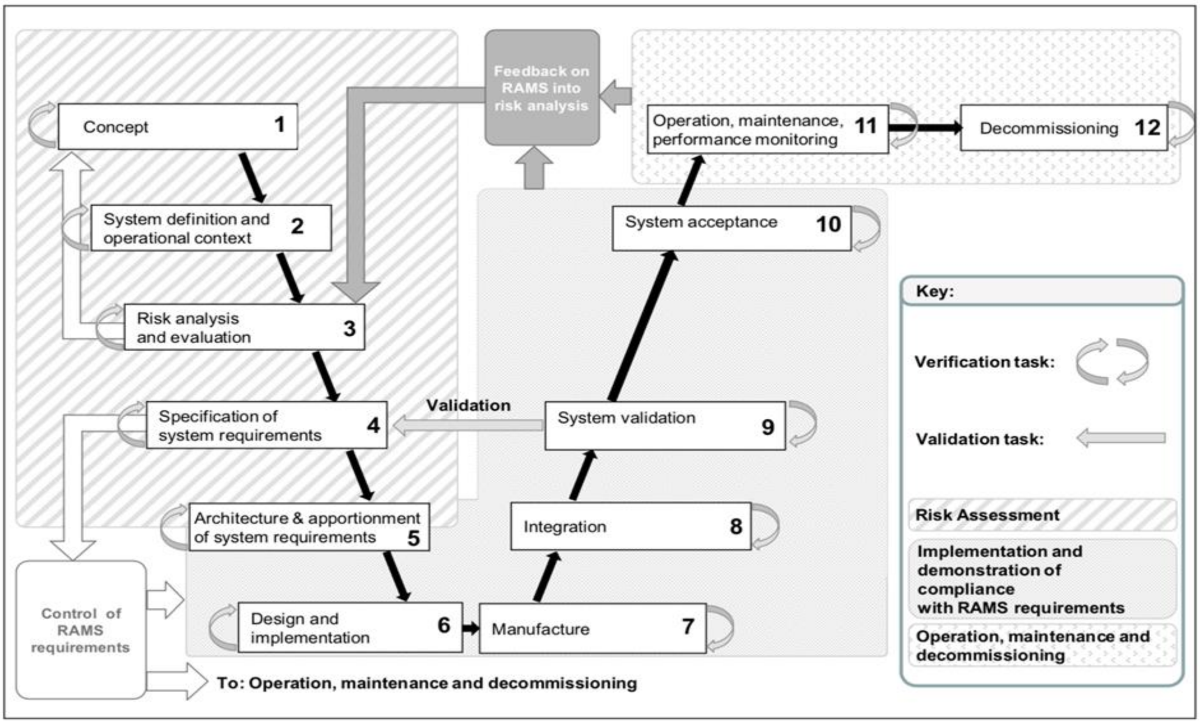
The Goal Structuring Notation – A Safety Argument Notation, Kelly and Weaver, 2004

UK Ministry of Defence, DEF-STAN 00-56, Safety Management Requirements for Defence Systems, Issue 4, June 2007

Work health and safety act, 2011

Appendix A Systems lifecycle model

Figure 18 is a systems lifecycle model from EN 50126 that provides a structure for planning, managing, controlling and monitoring all aspects of a system from concept to decommissioning.



Concept 1
System definition and operational context 2
Risk analysis and evaluation 3
Specification of system requirements 4
Architecture & apportionment of system requirements 5
Design and implementation 6
Manufacture 7
Integration 8
System validation 9
System acceptance 10
Operation, maintenance, performance monitoring 11
Decommissioning 12
Feedback on RAMS into risk analysis
Validation
Control of RAMS requirements
To: Operation, maintenance and decommissioning
Key:
Verification task:
Validation task:
Risk Assessment
Implementation and demonstration of compliance with RAMS requirements
Operation, maintenance and decommissioning

Figure 18 - Systems lifecycle model (EN 50126-1: 2017)

The top-down branch (left side) is generally called ‘development’ and is a refining process ending with the manufacturing of system components. The bottom-up branch (right side) is related to the assembly, the installation, the hand-over and then the operation and maintenance of the whole system.

As can be seen verification is required at each stage to verify that “*demonstrate that the requirements of each lifecycle phase have been fulfilled*” (EN 50126-1:2017), and the inputs are then used to the validation process. The validation process at stage 4 assures “*that system requirements (including RAMS requirements) have been properly specified applying the requirements defined in this standard and any additional specific requirements defined by applicable legal framework*” (EN 50126-1: 2017). The validation process at stage 9 assures “*that the system under consideration meets the specified requirements for the intended use or application*” (EN 50126-1: 2017).

Other lifecycle models are widespread in the use of systems safety assurance; however, a simplified development lifecycle model is most commonly used. That said, the reliability, availability, maintainability and safety (RAMS) process should be noted as being part of the overall process. RAMS is a process that is used to reduce the incidence of failures and/or the consequences throughout the lifecycle, and thus minimise the residual risk resulting from these errors.

Appendix B Development lifecycle model

Figure 19 is an adapted development lifecycle model and depicts the overarching system and lifecycle process in the front square-corner boxes and the deliverables in the rounded-corner boxes behind. There is a slight change in terminology when compared to the system lifecycle, but these are the models accepted by and used in industry.

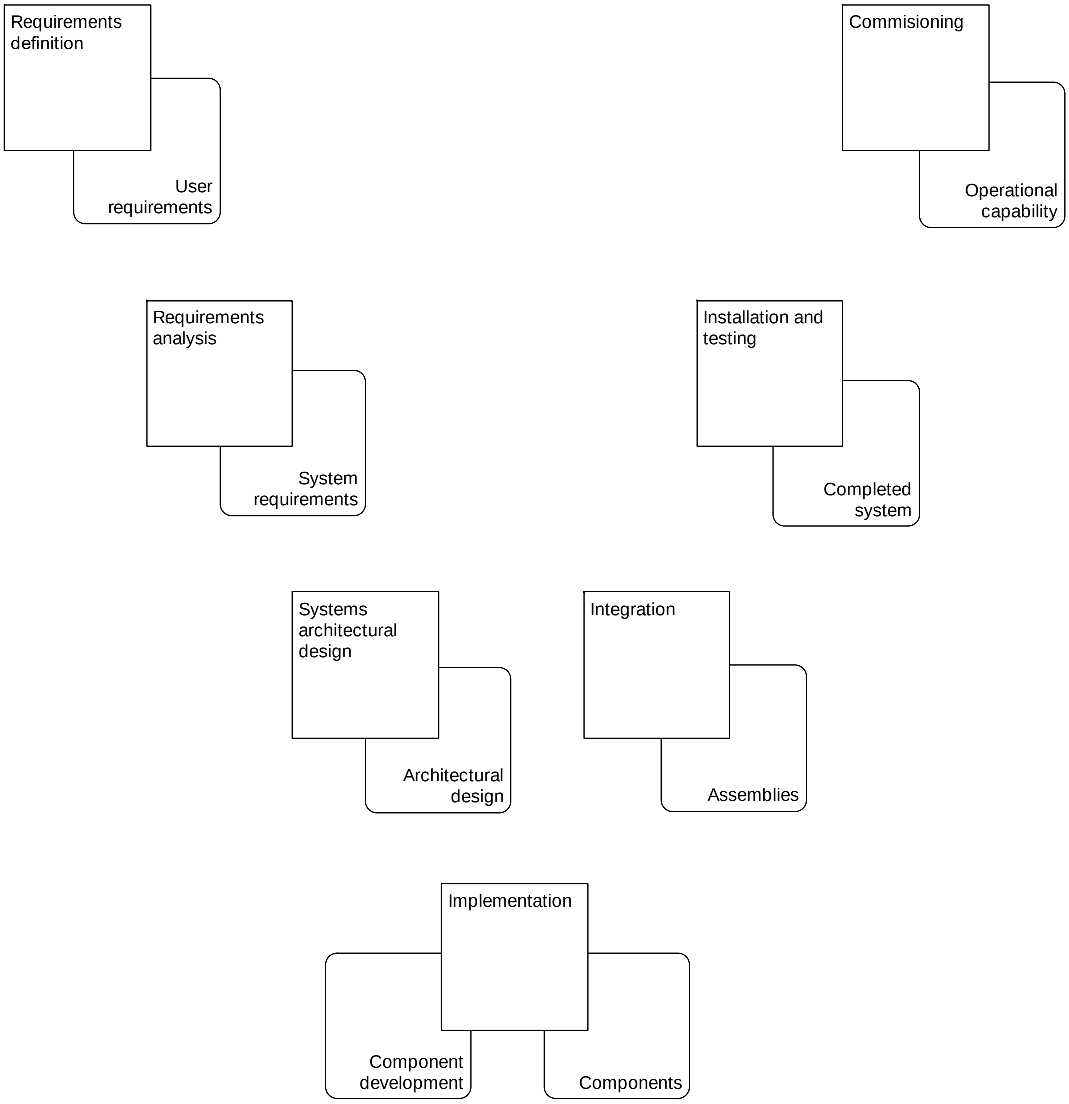


Figure 19 – Development lifecycle process and deliverables model

Figure 19 is a simplified model and omits the traditional elements normally represented on top of the 'V' and elsewhere:

- Verification and validation processes, because they are usually depicted in the model as being a linear step associated with one leg of the model or towards the end of the lifecycle process. In practice the validation processes are continuous, and the verification process is iterative all the way through the lifecycle process, and

- The operations, maintenance and disposal process.

In terms of this simplified development lifecycle model, assurance is depicted as a progressive process, working down the left-hand side:

- the requirements definition - working with the customer and understand different stakeholder requirements and specify them in a set of user requirements and an operational concept document (OCD), and then
- the requirements analysis- working on converting the user requirements into a technical view of an operational solution and specify them as a set of system requirement specifications (SRS), and then
- the architectural design - generating a number of architecture alternatives and select the one that best frames user requirements and system requirements and specify them as the architectural design (at a systems and subsystems level, some know these as system design documents (SDD)) to give a consistent view, and then
- the implementation process - creating/fabricating system elements or components conforming to the user requirements, architectural design and interfaces.

Working up the right-hand side of the model:

- the integration process – synthesising a set of system elements into a system or assembly that satisfies system requirements and architecture design, and then
- installation and testing – working a complete system at customer locations to ensure the asset/system works with the customers equipment and the external systems and then gradually transition it into operation, so it generally includes training the operators, iron out bugs that come up, and satisfying the regulators' needs, and then
- commissioning – asset or system goes into operation and maintenance (to sustain the operational capability of the asset/system) phase to give operational capability that should match the initial user requirements.

The downwards left-hand side of the V model is about architecture decomposition and definition, the upwards right-hand side of the V model is about architecture integration and verification. As you work along the V model it's from the highest level of system requirement to the lowest level of detail. The V is supposed to represent the validation and verification process in a continuous iterative manner.

So, as can be seen the system safety activities ensure that safety is woven into the design, implementation, commissioning and transition stages of a change, be that a new asset or a modification to an existing asset. It's important to recognise that at any time in the operations and maintenance phase of an asset or system any modification will start the process back in the requirements definition phase.

The systems engineering (SE) process is defined in INCOSE 2015 as: "*an interdisciplinary approach and means to enable the realisation of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with the design synthesis and system validation while considering the complete problem: operations, cost and schedule performance, training and* *support, test, manufacturing and disposal. SE considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs*". The technical process and outputs of the INCOSE 2015 approach map closely to the development lifecycle model. There are also other aspects such as enterprise processes, agreement processes and project-enabling processes. All these processes are collectively known as systems engineering management. EN 15288 is also a handy reference for the SE process.

The enterprise processes "*are used to establish and evolve plans, to execute plans, to assess actual achievement and progress against the plan and control execution through to fulfillment*", INCOSE, 2015.

The agreement processes "*define the activities necessary to achieve an agreement between two parties*", INCOSE, 2015.

The project-enabling processes "*help ensure the organisation's capability to acquire and supply products or services throughout the initiation, support and control projects*", INCOSE, 2015.

Appendix C SSA task allocation: Sample scoping table

Table 6 - Example scoping

System Safety Assurance Task	Non-critical	Critical	Planned?	Justification
System Safety Assurance Management Plan (SSAMP)	M	M	Y / N	
Preliminary Hazard Identification (PHI)	M	M	Y / N	
Preliminary Hazard Analysis (PHA)	M	M	Y / N	
System Hazard Analysis (SHA)	R	M	Y / N	
Subsystem Hazard Analysis (SSHA)	NR	R	Y / N	
Interface Hazard Analysis (IHA)	R	M	Y / N	
Operating & Support Hazard Analysis (OSHA)	R	M	Y / N	
Hazard Log	M	M	Y / N	
Preliminary Design Review (PDR)	R	M	Y / N	
Detailed Design Review (DDR)	NR	R	Y / N	
Critical Design Review (CDR)	R	M	Y / N	
Safety Assurance Report (SAR)	M	M	Y / N	
Independent Safety Assessment (ISA)	R	M	Y / N	

M: Mandatory R: Recommended NR: Not required

	Name & position	Signature & Date
Author:		
Reviewer:		
Approver:		

Note: The example above is suitable for an organisation undertaking non-complex tasks. The SSA tasks should be modified to represent the range of SSA tasks deemed applicable for the scope of works undertaken.

Appendix D Functional failure analysis (FFA)

There is no reference guide for FFA although it is a well-accepted multi-industry process for PHA.

A FFA is a system safety and reliability analysis technique. Its purpose is to identify the consequences of system functional failures, and so identify those functional failures that are hazardous or adversely impact availability.

FFA is very similar to FMEA, another technique used in SHA. However, FFA is done on functions rather than components, so it is useful in very early stages of in the system development lifecycle when the operational concept is being explored and before system architecture has been decided. So, to complete an FFA, you need a high-level model of the functions of the system.

Because components, technologies, etc. may not have been decided yet, detailed failure modes are not known, but functional failure modes can (and should) be postulated. For each system function, consider cause and effects of:

- loss of function (omission failure);
- provision of function when not required (commission failure), and
- incorrect value of function (error).

Environmental and operational contributing factors also are important to take into consideration before appropriate hazard controls but into place.

The advantages of FFA include it:

- is a simple concept.
    - can be applied at system level, before selection of specific technologies, and
    - considers hypothetical failure modes, which can’t be done in HAZops dues to the system design and guidewords.

The disadvantage is that in software, single functions may be too complex to have confidence in the completeness of analysis, i.e. it does not have the same granularity as HAZops.

The outcomes often influence the choice of safety features, guide further risk assessment and assist with SIL determination

If the system architecture has been defined it would generally be more appropriate to move straight into a SHA using a failure modes and effects analysis.

Table 7 is a template for a FFA process.

Table 7 – Template FFA process

Function	Failure Mode	Causes	Effects	Comments

RISSB

RAIL INDUSTRY SAFETY AND STANDARDS BOARD

ABN 58 105 001 465

For information regarding a product
developed by RISSB, contact:

Rail Industry Safety and Standards Board

Melbourne Office
Level 4, 580 Collins Street,
Melbourne, Vic 3000

Brisbane Office
Level 4, 15 Astor Terrace
Brisbane, QLD, 4000

PO Box 518
Spring Hill, QLD, 4004

T +61 6270 4523
F +61 6270 4516
E info@rissb.com.au