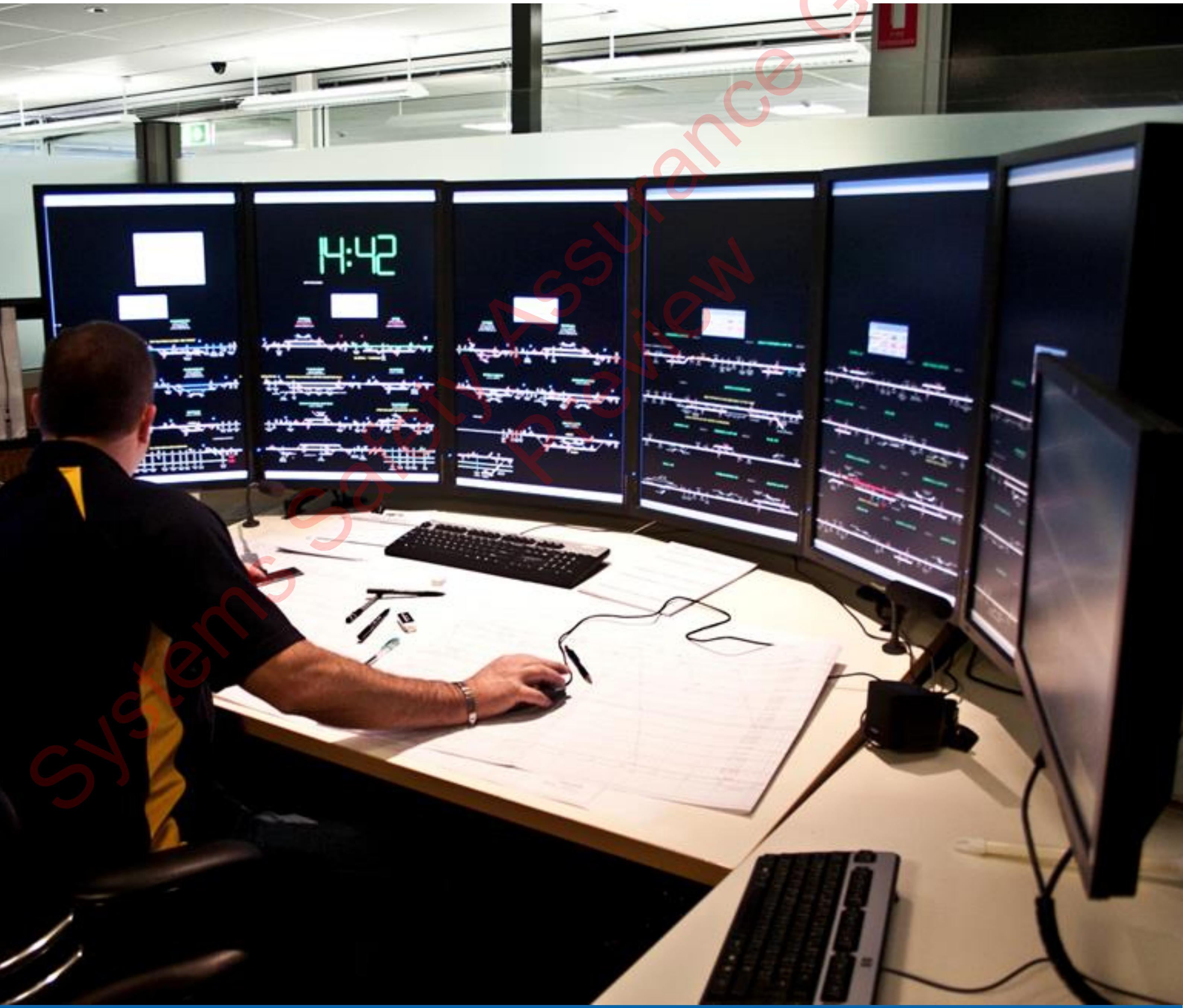
RAIL INDUSTRY SAFETY AND STANDARDS BOARD

ABN: 58 105 001 465

Systems Safety Assurance Guideline



rissb.com.au

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.