Master Specification
Part PC-RW20

System Safety and Assurance

July 2025

Government of South Australia
Department for Infrastructure and Transport

Build.
Move.
Connect.

Document Information

Document Information	
K Net Number:	1185761
Document Version:	0
Document Date:	09/07/2025

Document Amendment Record

Version	Change Description	Date
0	Initial issue	09/07/2025

Document Management

Contents

PC-RW20 System Safety and Assurance

1 General

a) This Master Specification Part sets out the requirements for systems and safety assurance for Rail Infrastructure including:

i) the documentation requirements, as set out in section 2;

ii) the systems and safety assurance requirements, as set out in section 3; and

iii) the Hold Point requirements, as set out in section 4.

b) The systems and safety assurance for Rail Infrastructure must comply with:

i) the Reference Documents, including:

A. AM4-DOC-001217 Systems engineering standard;

B. AS 15288 Systems and software engineering – System life cycle processes;

C. Building Code of Australia (BCA);

D. EN 50126-1 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Generic RAMS Process;

E. EN 50126-2 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Systems Approach to Safety;

F. EN 50128 Railway applications. Communication, signalling and processing systems – Software for railway control and protection systems;

G. EN 50129 Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling;

H. IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems;

I. IESM Application Note 4 – Independent Assessment;

J. ISO/IEC/IEEE 24748-4 Systems engineering – application and management of the systems engineering process;

K. ISO/IEC/IEEE 29148 Systems and software engineering – Life cycle processes – Requirements engineering;

L. Office of the National Rail Safety Regulator (ONRSR) Guideline - Major Projects;

M. Office of the National Rail Safety Regulator (ONRSR) Guideline - Safety Management System;

N. Office of the National Rail Safety Regulator (ONRSR) Guideline - Meaning of duty to ensure safety so far as is reasonably practicable; and

O. ST-RC-MC-1015 System Safety Standard for New or Altered Assets / Infrastructure; and

ii) Laws including:

A. Rail Safety National Law (South Australia) Act 2012; and

B. National Rail Safety Law National Regulations 2012.

c) This Master Specification Part applies to Rail Infrastructure and at the interface with other infrastructure, where applicable. Where the Contract Documents require systems and safety

assurance of any other infrastructure, the process must be undertaken in accordance with PC-EDM6 “Systems Engineering Management”.

d) System and safety assurance for Rail Infrastructure must be undertaken at each design gate as set out in PC-EDM1 “Design Management” and PC-RW30 “Design”.

e) The gate referenced in this Master Specification Part are references to gates contemplated by PC-RW10 “Railway Management Planning”.

2 Documentation

2.1 Systems and Safety Assurance Plan

a) The Contractor must prepare a Systems and Safety Assurance Plan, in accordance with ST-RC-MC-1015 System Safety Standard for New or Altered Assets / Infrastructure, which:

i) documents how the Contractor will progressively assure the Works;

ii) describes the process, techniques and management to be used for hazard identification and maintained throughout the project lifecycle;

iii) describes the methods and techniques to be used in presenting the safety cases using a best practice tool, such as goal structuring notation;

iv) outlines the overall approach and processes for fire and life safety engineering, following the Building Code of Australia (BCA);

v) describes the method adopted for Safety Integrity levels (SIL) apportionment, allocation and analysis;

vi) outlines the independent safety assessment approach and deliverables; and

vii) describes the systems safety resource and provide details on competency levels of those engage to carry out the assurance program.

b) The Systems and Safety Assurance Plan must be developed in compliance with:

i) the gate details in PC-RW10 “Railway Management Planning”; and

ii) the design management process in PC-EMD1 “Design Management” and PC-RW30 “Design”.

c) The Systems and Safety Assurance Plan must be prepared, submitted and updated in accordance with the requirements of PC-PM1 “Project Management and Reporting”, except that the Systems and Safety Assurance Plan must be initially submitted within 10 days of Commencement Date. Submission of the Systems and Safety Assurance Plan will constitute a **Hold Point**. The Contractor must not progress past gate 4A until the Hold Point is released.

d) Failure by the Contractor to achieve an agreed Systems and Safety Assurance Plan by gate 4A will result in a “prohibit work from proceeding” status being applied to the gate.

3 Systems and safety assurance requirements

3.1 General

a) The Contractor must implement a system, framework and engineering assurance process for assuring that the Works meet the requirements for the planning, delivery and operation, (including informing of rail operators) of the Rail Infrastructure as per the requirements of:

i) AS 15288 Systems and software engineering – system life cycle processes;

ii) ISO/IEC/IEEE 29148 Systems and software engineering – Life cycle processes – Requirements engineering;

iii) ISO/IEC/IEEE 24748-4 Systems engineering – application and management of the systems engineering process; and

iv) AM4-DOC-001217 Systems engineering standard.

b) The Contractor must progressively provide evidence of safety for Rail Infrastructure as per the requirements of:

i) EN 50126-1 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Generic RAMS Process;

ii) EN 50126-2 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Systems Approach to Safety;

iii) EN 50128 Railway applications. Communication, signalling and processing systems – Software for railway control and protection systems;

iv) EN 50129 Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling;

v) IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems; and

vi) ST-RC-MC-1015 System Safety Standard for New or Altered Assets/Infrastructure.

c) The Contractor's safety assurance activities for Rail Infrastructure must comply with the requirements of:

i) EN 50126-1 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Generic RAMS Process;

ii) EN 50126-2 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Systems Approach to Safety; and

iii) the minimum requirements of the Office of the National Rail Safety Regulator (ONRSR) Guideline - Major Projects available at https://www.onrsr.com.au/industry-information/latest-news/onrsr-major-projects-guideline-review-and-update.

d) In addition to the requirements of PC-WHS1 “Work Health and Safety”, the Contractor’s Safety Management Systems or integrated management system for Rail Infrastructure must comply with:

i) National Rail Safety Law National Regulations 2012; and

ii) Office of the National Rail Safety Regulator (ONRSR) Guideline Safety Management System.

e) The Contractor must adequately resource the rail system safety and assurance process.

f) In addition to the requirements of PC-PM3 “Contractor’s Personnel and Training“, the Contractor must nominate a rail systems safety assurance lead in the Key Personnel. The systems safety assurance lead must have a minimum of 10 years’ relevant rail experience.

3.2 Systems and safety assurance plan

a) The Contractor’s rail system safety assurance process must be presented in the Systems and Safety Assurance Plan as per the requirements in section 2.1.

b) The Contractor must update and resubmit the Systems and Safety Assurance Plan throughout the project life cycle in accordance with the requirements of PC-PM1 “Project Management and Reporting” including if major changes to the Project or assurance requirements occur.

3.3 Hazard management and derived safety requirements

a) The Contractor must implement a through lifecycle approach for Rail Infrastructure to ensure all reasonably foreseeable hazards and safety risks are identified and appropriately managed.

b) The Contractor must record all identified hazards and maintain them in a Project safety hazard log which must be submitted as an appendix to the safety cases at each gated design review as required in section 3.4.

c) Without limiting section 3.3b), the Contractor must address the hazards identified in the Reference Design preliminary hazard analysis, including those raised by the Rail Commissioner, Principal and other rail transport operators, within the project safety hazard log.

d) The project safety hazard log required by section 3.3b) must include all SFAIRP justifications in accordance with the ONRSR Guideline - Meaning of duty to ensure safety so far as is reasonably practicable.

e) Safety requirements derived from hazard controls identified within the project safety hazard log section 3.3b) must be recorded in the requirements analysis, allocation and traceability matrix (RAATM), as set out in PC-RW30 “Design”, while maintaining traceability to the project safety hazard log.

3.4 Safety cases

a) The Contractor’s safety cases must:

i) be structured in accordance with:

A. EN 50126-1 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Generic RAMS Process; and

B. EN 50126-2 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Systems Approach to Safety; and include

I. system definition;

II. quality management;

III. safety management;

IV. technical safety, supported by goal structuring notation;

V. related safety cases; and

VI. conclusion;

ii) be developed, submitted and updated progressively to demonstrate progressive systems safety assurance which aligns to:

A. EN 50126-1 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Generic RAMS Process;

B. EN 50126-2 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Systems Approach to Safety;

C. EN 50128 Railway applications. Communication, signalling and processing systems – Software for railway control and protection systems; and

D. EN 50129 Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling;

iii) contain the project safety hazard log section 3.3b), SFAIRP justifications and specifically highlight the residual risk that must be agreed with the Rail Commissioner and other rail transport operators where appropriate by a hazard transfer form; and

iv) link closely to the overall requirements management process and RAATM.

b) Safety cases must be submitted to support the Rail Commissioner's and other rail transport operators' rail accreditation requirements at the following gates":

i) Gate 4A with the Preliminary Design Documentation;

ii) Gate 4B with the Detailed Design Documentation;

iii) Gate 4C with the Issued for Construction Design Documentation stage;

iv) Gate 4D ready for testing; and

v) Gate 4E testing complete.

c) The Contractor must provide the safety cases to the Principal, 10 Business Days prior to all gated reviews. Submission of the safety cases will constitute a **Hold Point** and the relevant gated review cannot proceed unless this Hold Point is released.

d) All safety cases are controlled Documents as per the requirements of PC-QA1 "Quality Management Requirements" or PC-QA2 "Quality Management Requirements for Major Projects" as applicable.

3.5 Independent safety assessment

a) Where required in the Contract Documents, or if deemed appropriate by the Rail Commissioner's management of change process, the Contractor must undertake an independent safety assessment (ISA) in accordance with IESM Application Note 4 – Independent Assessment and this section 3.5.

b) In addition to the requirements of PC-PM3 "Contractor's Personnel and Training", and where required in the Contract Documents, the Contractor must engage an ISA Contractor and must nominate them in the Key Personnel.

c) The Contractor must prepare a brief for the preparation of the ISA and provide to the Principal for approval. This constitutes a **Hold Point**. Provision of the ISA Plan in accordance with section 3.5d) must not proceed until the Hold Point is released.

d) The Contractor must provide an ISA Plan in accordance with IESM Application Note 4 – Independent Assessment. The provision of an ISA Plan constitutes a **Hold Point** and must occur with 10 Business Days of Contract Commencement. The independent safety assessment must not proceed until this Hold Point is released.

e) The independent safety assessment must:

i) be appropriately independent from the project delivery;

ii) be delivered against the approved ISA brief approved in accordance with section 3.5c);

iii) be performed against the ISA plan approved in accordance with section 3.5d);

iv) be resourced adequately, relevant to the scale and complexity of the task;

v) conclude in a final report with a clear, unambiguous statement as to the ISA Contractor's opinion on the safety of the Project plus any limitation on the use of the Works;

vi) allow the ONRSR direct access to the ISA Contractor through open communication; and

vii) consider how the ISA process will support the assurance needs of the Rail Commissioner.

f) The Contractor must submit the ISA report 10 Business Days before the gate 4C review, as outlined in PC-RW30 "Design", which constitutes a **Hold Point**. The Gate 4C review cannot take place until this report is submitted.

g) The Contractor must submit a final ISA report 10 Business Days before the gate 4E review, as outlined in PC-RW30 "Design", which constitutes a **Hold Point**. The Gate 4C review cannot take place until this report is submitted.

4 Hold Points

Table PC-RW20 4-1 details the review period or notification period, and type (documentation or construction quality) for each Hold Point referred to in this Master Specification Part.

Table PC-RW20 4-1 Hold Points

Section reference	Hold Point	Documentation or construction quality	Review period or notification period
2.1c)	Submission of the Systems and Safety Assurance Plan	Documentation	10 Business Days
3.4c)	Provision of safety cases to the Principal prior to nominated gated reviews (Gates 4A, 4B, 4C, 4D and 4E)	Documentation	10 Business Days
3.5c)	Provision of a brief for the ISA	Documentation	10 Business Days
3.5d)	Provision of the ISA Plan	Documentation	10 Business Days
3.5f)	Provision of the ISA report (Gate 4C)	Documentation	10 Business Days
3.5g)	Provision of the final ISA report (Gate 4E)	Documentation	10 Business Days