Project Controls

Master Specification

PC-RW20 System Safety and Assurance

Document Information	
K Net Number:	11825761
Document Version:	3
Document Date:	October 2020

DEPARTMENT FOR INFRASTRUCTURE AND TRANSPORT

Government of South Australia
Department for Infrastructure and Transport

Document Amendment Record

Version	Change Description	Date
1	Initial issue (formerly RW20)	7/11/2019
2	Reviewed and updated by RSOP	23/04/2020
3	Updated inline with ST-RC-MC-1015	October 2020

Document Management

Contents

PC-RW20 System Safety and Assurance

1 General

1.1 This Part specifies the Requirements for the Systems and Safety Assurance.

1.2 Refer to PC-RW10 "Railways Management Planning" for definitions and referenced documents.

1.3 Contractor must comply with:

a) RSNL — Rail Safety National Law (South Australia) Act 2012 and Regulations.

b) WHS — Work Health and Safety (South Australia) Act 2012 and Regulations.

c) AS15288 — Systems and Software Engineering – System Life Cycle Processes.

d) ISO/IEC 29148 — Systems and software engineering – life cycle processes – requirements engineering.

e) ISO/IEC 26702 — Systems engineering – application and management of the systems engineering process.

f) EN50126 Part 1 — Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability, and Safety (RAM) – Part 1: Basic Requirement and Generic Process.

g) EN50126 Part 2 — Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Guide to the application of EN 50126-1 for safety.

h) EN50128 — Railway applications. Communication, signalling and processing systems. Software for railway control and protection systems.

i) EN50129 — Railway Applications - Communication, Signalling and Processing Systems - Safety Related Electronic Systems For Signalling.

j) IEC 61508 — Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.

k) AS4801:2001 Occupational Health and Safety Management Systems.

l) Major Projects Guideline from the Office of the National Rail Safety Regulator (ONRSR).

m) Meaning of duty to ensure safety so far as is reasonably practicable Guideline (ONRSR)

n) Preparation of a Rail Safety Management System (ONRSR).

o) Safe Work Australia Code of Practice, "Safe Design of Structures.

1.4 Where appropriate, the Contractor must comply with the following Departmental documents:

a) ST-RC-MC1015 — System Safety Standard for New and Altered Assts/Infrastrucutre

b) AM4-DOC-001217 — Systems Engineering Standard

c) PTS-MU-10-EG-PRC-00000023 — Design Lifecycle Management.

d) PTS-MU-10-EG-PRC-00000016 — Design Decision Records Procedure.

e) AM4-DOC-000940 — Asset Management Handover Requirements Standard

f) PC-RW10 — Railways Management Planning.

g) PC-RW50 — Inspection, Testing and Commissioning.

h) PC-RW60 — Asset Management Handover.

2 Systems and Safety Assurance Requirements

General

2.1 The Contractor must have a system, framework and engineering assurance process for assuring Project Activities meet the requirements of AM4-DOC-001217, AS15288, ISO/IEC 29148 and ISO/IEC 26702 for the planning, delivery and operation of the infrastructure and services of the Project.

2.2 The Contractor must progressively provide evidence of the Reliability, Availability, Maintainability and Safety (RAMS), per the requirements of ST-RC-MC1015, EN 50126, EN 50128, EN 50129 and IEC 61508 for railway applications.

2.3 The Contractor must comply with Rail Safety National Law (South Australia) Act 2012 and Regulations.

2.4 The Contractor's safety assurance activities must be delivered following the requirements of EN50126 and meet the minimum Office of the National Rail Safety Regulator (ONRSR) expectations of Major Projects Guideline.
Note: The usage of the Major Project Guideline is a mandatory requirement and is not dependent on ONRSR declaring the project Major for regulatory purposes. The principles included within the Guidance are seen as prudent for a contemporary rail project.

2.5 The Contractors Safety Management System(s) or Integrated Management System must adhere to the National Rail Safety Law (SA) Regulations 2012 and AS4801:2001 Occupational Health and Safety Management Systems. Note the ONRSR publication "Preparation of a Rail Safety Management System".

2.6 The Contractor must adequately resource the assurance process, with the Systems Safety Assurance Lead having minimum of 10 years relevant rail experience.

Systems and Safety Assurance Plan

2.7 The Contractors System Safety Assurance process must be presented in the Systems and Safety Assurance Plan (S&SAP).

2.8 The S&SAP must document how the Contractor will fulfil progressively assure the works.

2.9 The S&SAP must describe the process and techniques to be used for hazard identification and maintained throughout the project lifecycle.

2.10 The S&SAP must describe the methods and techniques to be used in presenting the Safety Case(s) using a best practice tool such as Goal Structuring Notation.

2.11 The S&SAP must outline the overall approach and processes for fire and life safety engineering, following the Building Code of Australia (BCA).

2.12 The S&SAP must describe the method adopted for Safety Integrity Levels (SIL) Apportionment, Allocation and Analysis.

2.13 The S&SAP must outline the Independent Safety Assessment approach and deliverables.

2.14 The S&SAP must describe the Systems Safety resource and provide details on competency levels of those engage to carry out the assurance program.

2.15 The provision of the Contractor's S&SAP constitutes a **Hold Point**.

Hazard Management and Derived Safety Requirements

2.16 The Contractor must put in place a through lifecycle approach to ensure all reasonably foreseeable hazards and safety risks are identified and appropriately managed. All identified hazards must be recorded and maintained in a project hazard log.

2.17 The Contractor must address the hazards identified in the Reference Design Preliminary Hazard Analysis.

2.18 All SFAIRP justifications must be per the ONRSR meaning of duty to ensure so far as is reasonably practicable Guideline.

2.19 Safety requirements derived from hazard controls identified within the project safety hazard log must be recorded in the Requirements Analysis, Allocation and Traceability Matrix (RAATM) while maintaining traceability to the project safety hazard log.

Safety Cases

2.20 The Safety Cases will:

a) be structured in line with the guidance provided in EN 50126:

i) System Definition;

ii) Quality Management;

iii) Safety Management;

iv) Technical Safety (supported by Goal Structuring Notation);

v) Related Safety Cases; and

vi) Conclusion.

b) developed, submitted and updated progressively in order to demonstrate progressive systems safety assurance which aligns to EN50126, EN50128 and EN50129;

c) contain the project safety hazard log, SFAIRP justifications and specifically highlight the residual risk that is to be agreed with the Rail Commissioners operations and maintenance teams; and

d) link closely to the overall Requirements Management Process / RAATM.

2.21 Safety Case(s) must be submitted progressively as follows in a timeline agreed with the Rail Commissioner, to support the Rail Commissioners Rail Accreditation:

a) Gate 4A – Initial Design (30% Design);

b) Gate 4B – Design (70%)

c) Gate 4C – Design Issued for Construction;

d) Gate 4D – Ready for Testing; and

e) Gate 4E – Asset Assurance.

2.22 Provision of a Safety Case shall occur 10 days prior to all Reviews and constitute a **Hold Point**.

2.23 All Safety Cases are controlled Documents (refer to PC-QA1 "Quality Management Requirements").

Independent Safety Assessment

2.24 The Contractor must engage an Independent Safety Assessment (ISA) that:

a) is appropriately independent form the project delivery;

b) is delivered against a documented ISA brief covering the project lifecycle;

c) is performed against a documented ISA plan;

d) is resourced adequately, relevant to the scale and complexity of the task;

e) concludes in a final report with a clear, unambiguous statement as to the assessor's opinion on the safety of the Project plus any limitation on the use of the assets;

f) allows the ONRSR direct access to the ISA through open communication; and

g) considers how the ISA process will support the assurance needs of the Rail Commissioner.

2.25 The ISA Contractor is subject to the prior approval of the Principal, which must not be unreasonably withheld.

2.26 The provision of an ISA Plan constitutes a **Hold Point**.

2.27 Provision of an ISA Design Report (Gate C) and ISA Final Report (Gate E) shall occur ten days before all Reviews and constitute a **Hold Point**.

3 Hold Points

3.1 The following is a summary of Hold Points referenced in this Part:

Document Ref.	Hold Point	Response Time
2.15	Provision of Contractor's Systems and Safety Assurance Plan	10 working days prior to Gate 4A
2.22	Safety Case prior to each lifecycle design review	10 working day prior to Gate 4A, 4B, 4C, 4D, and 4E
2.26	Independent Safety Assessment Plan	10 working days prior to Gate 4A
2.27	Independent Safety Assessment Design (4B) and Final (4E) Reports	10 working day prior to Gate 4C and 4E

4 Records

The Contractor must develop, maintain and supply all records as necessary to provide evidence of compliance with the requirements of this Part in accordance with the requirements of PC-RW60 "Asset Management Handover".