PART RW20

RAILWAYS – SYSTEM AND SAFETY ASSURANCE

CONTENTS

1. GENERAL
2. SYSTEMS AND SAFETY ASSURANCE REQUIREMENTS
3. HOLD POINTS
4. RECORDS

1. GENERAL

.1 This part specifies the requirements for the Systems and Saftey Assurance.

.2 Refer to Part RW10 for definitions and referenced documents.

.3 Contractor must comply with:

RSNL:	Rail Safety National Law (South Australia) Act 2012 and Regulations
WHS:	Work Health and Safety (South Australia) Act 2012 and Regulations
AS15288	Systems and Software Engineering – System Life Cycle Processes
AS10007	Quality Management System – Guidelines for Configuration Management
ISO/IEC 29148	Systems and software engineering – life cycle processes – requirements engineering
ISO/IEC 26702	Systems engineering – application and management of the systems engineering process
EN50126 Part 1	Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability, and Safety (RAM) – Part 1: Basic Requirement and Generic Process
EN50126 Part 1	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
EN50128	Railway applications. Communication, signalling and processing systems. Software for railway control and protection systems
EN50129	Railway Applications - Communication, Signalling and Processing Systems - Safety Related Electronic Systems For Signalling
IEC 61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems
ISO 10007	Guidelins for Configuration Management

.4 Where appropriate, the Contractor must comply with following DPTI documents:

PTS-MU-10-EG-PLN-00000017	PTSOM Systems Engineering Management Plan
PTS-MU-10-EG-PRC-00000023	Design Lifecycle Management
PTS-MU-10-EG-PRC-00000016	Design Decision Records Procedure
PTS-MS-05-AM-PRC-00000091	Asset Management Technical Data Requirements for Projects
Part RW10	Railways Management Planning
Part RW50	Inspection, testing and commissioning
Part RW60	Asset Handover

2. SYSTEMS AND SAFETY ASSURANCE REQUIREMENTS

GENERAL

.1 The Contractor must have a system, framework and engineering assurance process for assuring Project Activities which meets the requirements of ISO/IEC 15288, ISO/IEC 29148 and ISO/IEC 26702 for the planning, delivery and operation of the infrastructure and services of the Project.

.2 The Contractor must progressively provide evidence of the reliability, availability, maintainability and safety of the Works, in accordance with the requirements of EN 50126, EN 50128, EN 50129 and IEC 61508 for railway applications.

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

SAFETY MANAGEMENT

.4 The Contractor must adopt a safety by design approach and develop, implement and document a safety assurance process for the Project Activities which meets the requirements of EN50126, EN 50128 and EN 50129 for railway applications for the planning, delivery and operation of the infrastructure and services of the Project.

.5 The Contractors Safety Assurance process must be defined and detailed in the Systems and Safety Assurance Plan.

.6 The provision of the Contractors Systems and Safety Assurance Plan constitutes a **HOLD POINT**.

.7 The Contactor's safety assurance activities must be delivered in accordance with the requirements of EN50126 and meet the minimum ONRSR expectations of Major Projects Guideline from the Office of the National Rail Safety Regulator (ONRSR).
Note: The usage of the Major Project Guideline is 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.

.8 The contactor must undertake a quantitative risk assessment in relation to its operational protocols to ensure the safe operation of Assets during Operational and Maintenance Activities.

.9 The Contractor must analyse and set the upper limit for individual or collective risks of equivalent fatality which must be recorded within the Systems and Safety Assurance Plan.

.10 The Contractor must demonstrate effective management and control to ensure the safe management of the contractors Activities over the Term through implementation of, but not limited to;

(a) progressive project reviews;

(b) independent verification reviews;

(c) Independent safety assessment reviews;

(d) identification and involvement of stakeholders and accredited party/s;

(e) risk is managed so far as is reasonably practicable (SFAIRP)

(f) integration of a positive safety culture; and

(g) executive communication, reporting and business wide communication.

.11 The Contractor must:

(a) ensure that people carrying out verification reviews have a suitable level of independence from the personnel involved in preparing Design Documentation and that any inspection and test plans verify and validate the Design Documentation and inspection and test plans for the various components of the Works;

(b) provide the Rail Commissioner with all relevant safety information and conditions in relation to the use of the Works; and

(c) ensure that training is provided to enable Activities to be carried out safely;

.12 Safety requirements must be taken into account in all aspects of the Contractor's Activities with input from involved and affected parties.

.13 Without limiting the requirements in the WHS Legislation, the Rail Safety National Law and the Rail Safety Regulations, the Contractor must consider and address all safety issues, hazards and risks and requirements relating to safety during the project lifecycle of the Works and in the development and production of the Project Documents, including:

(a) all safety issues, hazards and risks arising out of or in connection with the Contractor's Activities, including public and community safety during the Delivery Activities;

(b) safety goals and objectives and generic hazards associated with Project Activities;

(c) safety issues, including generic issues, and hazards and risks associated with Project Activities;

(d) all applicable safety standards and codes of practice to be applied to the design input for each design package, hazards and risks which cannot be eliminated, managed or mitigated by the design and the measures to be adopted in the construction, operation, maintenance, handover and decommissioning phases to manage and mitigate these hazards and risks;

(e) hazards and risks that require the development of specific procedures in the construction, operation, maintenance and decommissioning phases to eliminate the risks to safety and, where elimination of a risk to safety is not reasonably practicable, reduce those risks so far as is reasonably practicable;

(f) hazards and risks associated with working in a rail corridor ;

(g) safety issues related to the on-going repair, maintenance, upgrading and decommissioning;

(h) issues relating to working adjacent to or with live utility services, including high voltages or pressures, overhead clearances, dangerous excavations, contaminated ground or groundwater and asbestos materials;

(i) hazards and risks identified as part of the risk management process and resultant changes and management measures in the Project Documents and Project Activities;

(j) safety implications of Project Activities including but not limited to:

.1 competencies and condition of personnel;

.2 positioning of site access and egress points;

.3 location of site facilities and accommodation;

.4 location of traffic / pedestrian routes;

.5 working on or adjacent to the road network; and

.6 safe work at height requirements.

.14 Safety in design principles and processes must be included in the design development and other key stages throughout the Contractor's Activities, incorporating the requirements of all relevant codes and standards, including Safe Work Australia Code of Practice, "Safe Design of Structures". The outcomes of Contractor's risk assessment activities must be considered as part of the safety in design process.

.15 The Rail Commissioner must be provided an opportunity to participate in the various safety in design processes.

HAZARD MANAGEMENT AND DERIVED SAFETY REQUIREMENTS

.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 managed in a project hazard log.

.17 The Contractor must as a minimum address the hazards identified in the Reference Design Preliminary Hazard Analysis into the Contractor's own Hazard Log to the extent applicable to the Design.

.18 The Contractor must document in the Systems and Safety Assurance Plan the hierarchy it will follow with regards to hazard controls and eliminate risks so far as is reasonably practical (SFAIRP). It should be noted that the SFAIRP will need to be in accordance with the ONRSR Major Project Guideline.

.19 All elements of the Works that include software, electrical / electronic systems (i.e. hardware) and which have an associated safety function must have a safety integrity level (SIL) determined and documented in accordance with the requirements of EN 50126 and IEC 61508.

.20 Safety requirements derived from hazard controls identified within the project safety hazard log must be recorded in the Project Project requirements analysis, allocation and traceability management (RAATM) register while maintaining traceability to the project safety hazard log.

.21 The project safety hazard log must have considered Preliminary Hazards Assessment (PHA), interface hazards assessment, human factors hazards.

SAFETY MANAGEMENT SYSTEM(S)

.22 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”.

PROGRESSIVE SAFETY ASSURANCE

.23 For the Contractors Activities Safety Case(s) must be developed, submitted and updated progressively in order to demonstrate progressive safety assurance which aligns with EN 50126, EN 50128 and EN 50129 for railway applications and the Rail Safety National Law (SA).

.24 The Contractor must prepare a framework to demonstrate how the requirements of the safety standards such as EN 50126, EN 50128 and EN 50129 for railway applications will be assured.

.25 The Contractor must demonstrate the level of progressive assurance for compliance with the requirements of EN 50126, EN 50128 and EN 50129 for railway applications. This must be performed by independent peer review and an Independent Safety Assessment.

.26 The Contractor must provide within the Safety Case(s) the safety arguments of the Project and describe the safety argument using a best practice tool, such as Goal Structuring Notation.

.27 All solutions and controls identified by the Contractor in order to satisfy the safety arguments identified in assurance activities must be supported by robust and traceable evidence that is referenced against the associated requirement in the RAATM register.

.28 The Contractor will detail the process and delivery of the Safety Case(s) in the Systems and Safety Assurance Plan.

SYSTEMS AND SAFETY ASSURANCE PLAN

.29 The, Safety and Systems Assurance Plan must document how the Contractor will fulfil each of the mandatory requirements for systems assurance and systems safety assurance for the Works and the Temporary Works and be consistent with the Rail Safety National Law Act 2012 (SA) and the Preparation of a Rail Safety Management System Guideline issued by the Office of the National Rail Safety Regulator.

.30 The Contractor must provide within its Systems and Safety Assurance Plan details of how it will progressively provide assurance that safety requirements will be met. As a minimum this must be demonstrated by Safety Case(s) submitted progressively as follows in a timeline agreed with the Rail Commissioner, to support the Rail Commissioners Rail Accreditation:

(a) Gate 4A – Initial Design;

(b) Gate 4B – Design Issued for Construction;

(c) Gate 4C – Ready for testing; and

(d) Gate 4D – Asset Acceptance (prior to handover).

.31 The Systems and Safety Assurance Plan must describe the process and techniques to be used for hazard identification and management throughout the project lifecycle;

.32 The Systems and Safety Assurance Plan must describe the processes and techniques to be used in presenting the safety argument using a best practice tool such as Goal Structuring Notation;

.33 The Systems and Safety Assurance Plan must outline the overall approach and processes for fire and life safety engineering, in accordance with the Building Code of Australia (BCA);

.34 The configuration management requirements of Systems and Safety Assurance Plan must fulfil each of the mandatory requirements for configuration management listed in AS ISO 10007 for the Works.

Safety Cases / Safety Assurance Statements

.35 The Contractor must show progress systems and safety assurance via a series of Safety Case(s) at Design Lifecycle Reviews and Safety Assurance Statements against subsystems (if appropriate).

.36 These documents will form part of the overall assurance demonstration provided to the Office of the Notational Rail Safety Regulator (ONRSR) to ensure continued / changed Rail Accreditation.

Safety Assurance Statement

.37 The purpose of the Safety Assurance Statement is to provide assurance that the hazards and risks identified as part of the Hazard Identification and Risk Assessment process, and the controls identified to prevent or protect against them, have been appropriately addressed by the design.

Safety Cases

.38 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 ENS50126, EN50128 and EN50129;

(c) supported by Goal Structuring Notation (GSN);

(d) contain the project hazard log, SFAIRP justifications and specifically highlight residual risk that is to be agreed with DPTI Rail operations and maintenance; and

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

.39 Provision of a Safety Case shall occur 10 days prior to all Reviews and constitute a **HOLD POINT(s).**

.40 All Safety Cases are Controlled Document (refer Part G20 “Quality System Requirements”).

Independent Safety and Assurance Assessor

.41 The Contractor must engage an Independent Safety and Assurance Assessor that:

(a) is appropriately independent form the project delivery;

(b) is delivered against a documented Independent Safety Assessor brief covering the project lifecycle;

(c) is delivered against a documented Independent Safety Assessor plan;

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

(e) produces documented reports containing remedial actions categorised by safety risk;

(f) 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;

(g) allows the ONRSR direct access to the Independent Safety Assessor though open communication; and

(h) considers how an Independent Safety Assessor can support the assurance needs of the Rail Commissioner

.42 The Independent Safety Assessor is subject the prior approval of the Principal prior approval, which must not be unreasonably withheld.

.43 Within the Safety Management Plan, the Contractor must include the Independent Safety Assessor arrangements, the Independent Safety Assessor assessment activities, the Independent Safety Assessor's proposed interactions with the Contractor and the Independent Safety Assessor's deliverables to the Principal.

3. HOLD POINTS

CLAUSE REF.	HOLD POINT	RESPONSE AND DELIVERY GATE
2	Provision of Contractor’s Systems and Safety Assurance Plan	10 working days prior to Gate 4A
2	Safety Case prior to each lifecycle design review	10 working day prior to Gate 4A, 4B, 4C, and 4D

4. RECORDS

.1 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 Part RW60 “Asset Handover”.