INTEGRATION
ENGINEERING SAFETY MANAGEMENT

Requirements for the Creation, Format and Provision of a Design Engineering Safety Justification (DESJ)

Document Number: CRL1-XRL-O8-GPS-CR001-50025

Current Document History:

Revision:	Effective Date:	Author(s) ('Owner' in eB *)	Reviewed by: ('Checked by' in eB *)	Approved by:	Reason for Issue:
1.0	18/05/2016	Stephen James	Chi Wong	Jeremy Bates	First Issue

Revision Changes:

Revision	Status / Description of Changes
1.0	First revision.

Contents

1 Introduction

The following details the mandatory format of a Design Engineering Safety Justification (DESJ). This is equally applicable to an Engineering Safety Justification (ESJ).

This is applicable across all contracts, although not all parts will be applicable to each contract.

Additionally, this document is part of the Crossrail Engineering Safety Management Reference Manual (Ref 1) and its accompanying procedure Crossrail Process and Format for Overall Safety Justifications (Ref 2).

2 Purpose

DOCUMENT STRUCTURE

Executive Summary (1 Page – where possible)
The Executive Summary should contain a brief précis of the paper, its content and the outcome of the deliberations e.g. "All safety hazards evaluated through series of workshop sessions and closed……. This safety justification therefore demonstrates that Contract XXX works have accomplished a suitable level of safety."

3 Scope

Overview
State what this Safety Justification covers. Provide the parameters under which the safety will be assured. Explain the processes used and what the outcome is e.g. to demonstrate an acceptable level of safety has been achieved within the design.

Context
Provide a brief description of the Crossrail project together with timescales.

Scope
Provide the physical parameters of the safety justification, together with the Objectives of the (D) ESJ

Safety Justification Reviews
Provide details of the number of reviewers and their involvement through the various versions (the initial version will only have current details, but the history will build up through the issue of subsequent versions).

Structure of this Safety Justification
Provide an outline of the document structure, together with a resume of what each part contains.

References
Refer to where the references may be found (at the rear of the document)

4 Terms & Definitions

4.1 System Definition

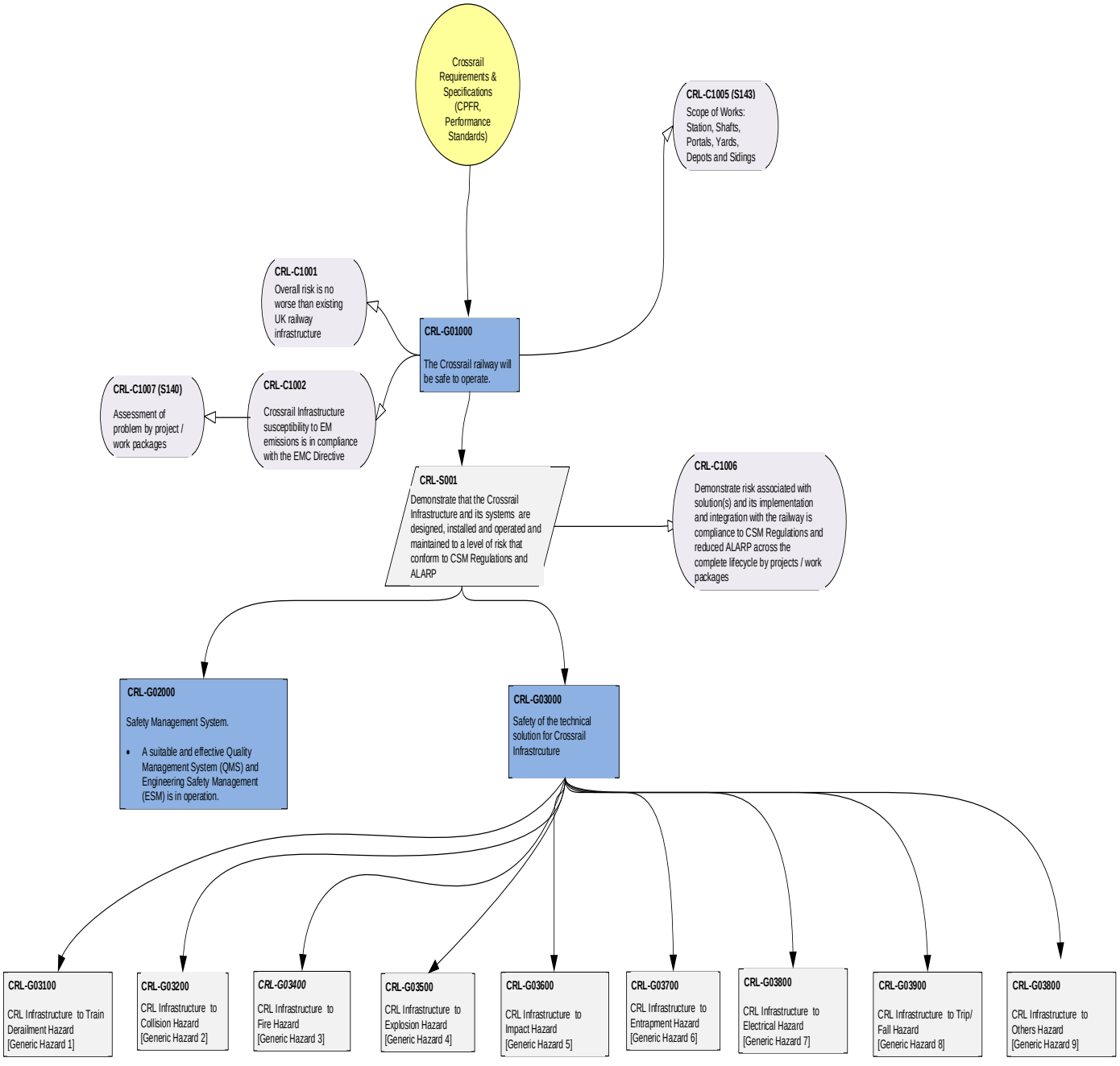
System Description

Provide a description of the system in question, together with the components that come together to form the "whole".

This could be the various components of "Systemwide" e.g. track, signalling, communications etc., or, in a Shaft or Portal structure could be ventilation, LV power, fire alarm system etc.

Safety targets for the system / components should be stated, together with any SIL determinations.

This may be represented diagrammatically using GSN, as per the following example:



4.2 Safety Management System

Quality Management Report
Overview
Detail the Quality Management components that have been provided and the manner in which they are delivered. Refer to appropriate Assurance Plans etc.
Provide details of audits undertaken, together with outcomes. The relevance of the QMS to this justification should be stated.

Safety Management Report
Overview
Refer to the current approved version of the Contractor's System Safety Plan, which is a Contract safety deliverable *[versions prior to current document to be identified].*
Provide confirmation as to the adequacy of the implementation of the Contractor's System Safety Plan via reference to internal/external reviews and audits of engineering design, and including Suppliers and Sub-contractors [versions prior to current with brief description of the changes per version].
Provide a listing of (or signpost to) the legislation and standards that are applicable to this justification.

Safety Organisation
Capability to identify the safety related tasks to be carried out and how the competence and capability of those individuals carrying out those tasks is initially demonstrated and continually assessed so as to remain current.

4.3 Technical Safety Assessment

Safety Claim for System Level

This should include a statement that the DESJ is designed to confirm / demonstrate that the "system" (details from the earlier section on scope) are "safe"

Safety Claim for Sub-System Levels

This should include a statement that the DESJ is designed to confirm / demonstrate that the "system" (details from the earlier section on scope) are "safe"

Safety Claim for Product Acceptance / Approval

This should be based upon the PWHR outputs, Product Breakdown Structures and demonstration of product acceptability to CRL (including the use of the Product Acceptance Procedure for new / novel products), and RAB(C) acceptance.

Outline of the overall safety argument to include the following inputs-

- High Level Requirements derived from CSM, RIR, RSSB, ORR etc.
- Strategy adopted to meet this
- RA Principles drawn from Engineering Safety Management Plan
- Definition of the Safety requirements and where these are drawn from e.g.
- Conceptual from CPFR and Performance Specification
- Emergent from PWHR, HAZOPS
- Specific identified through the design process

- How the Safety requirements will be implemented
- Compliance with the CPFR and Performance Specification (through V&V activities)
- Process for (agreement and) transfer of requirements with others
- HRP Process
- IHA Process
- Asset and Maintenance strategy

Demonstration of the safety argument-

This is based upon the core hazards as identified in the CRL document "Projectwide Hazard Record Process" CRL1-XRL-O8-GPS-CR001-50013. A full listing of the hazards from the above document is provided, however, this section should be tailored to cover those applicable to the DESJ in question. To provide a consistent document it is proposed that each hazard is identified, but that a n/a is placed against those that are not applicable to the DESJ rather than delete them.

Each of the applicable hazards should provide a safety argument based upon the following inputs:

Specific derived Safety Requirements from the following sources and how the requirements are met.

- CPFR
- Standards
- PWHR
- Strategies e.g. Fire strategy
- RA's e.g. Fire Risk Assessment
- Asset and Maintenance Plan
- Specific SIL Requirements

Demonstration of the mitigation for the particular hazard from the following.

- PWHR
- HAZOPS
- HAZIDS

Provision of any certification and how this applies

- Design completion certificates.
- What these demonstrate

Validation / Verification activities carried out through the phase, the outcomes and issues

- Details of Audits undertaken, outcomes and status
- Details of Checks undertaken, outcomes and status

Dealing with interfaces

- How the interfaces identified, both internal and external
- List of external interfaces
- List of internal interfaces
- Interface requirements and how they have been met
- Outputs from IHA, HRP, SIRP, MIRP etc., Inc. any outstanding issues
- Summary of the issues involved, how these were dealt with, and outcomes e.g. provision of O&M Manuals, Training etc.

Conclusion

Specific conclusion and demonstration that the safety argument for the particular hazard has been accomplished.

- **Related Safety Activities and its Documentation**
  - Providing and demonstrate that it fulfils the necessary safety functions.
  - Identification and demonstration of SIL Requirements
  - Generic Product Safety Case, Generic Application Safety Case or Product Safety Case (new or novel)
  - Fulfilment of SRAC's
  - EMC Issues
  - Human Factors
  - RAM
  - NoBo TSI Compliance

- **Outstanding Issues**
  Summary of Assumptions, Evidence that all assumptions have been satisfactorily closed out as part of the design acceptance process, Dependencies & Restrictions placed upon the design and the requirements / timescales for resolution.

- **Overall DESJ Conclusion** i.e. that the "system" in question has been demonstrated as being "safe" through the application of the approach above.

4.4 Appendices (located in accordance with CRL document format)

4.5 Related Safety Cases / Justifications (if required)

- Hierarchy of (D) ESJ's

4.6 Document Control

- Abbreviations
- Documents referenced as evidence
- Documents provided for information only

Example of Technical Safety Assessment using the Project Wide Hazard Record Process – generic hazard list, see diagram 1.

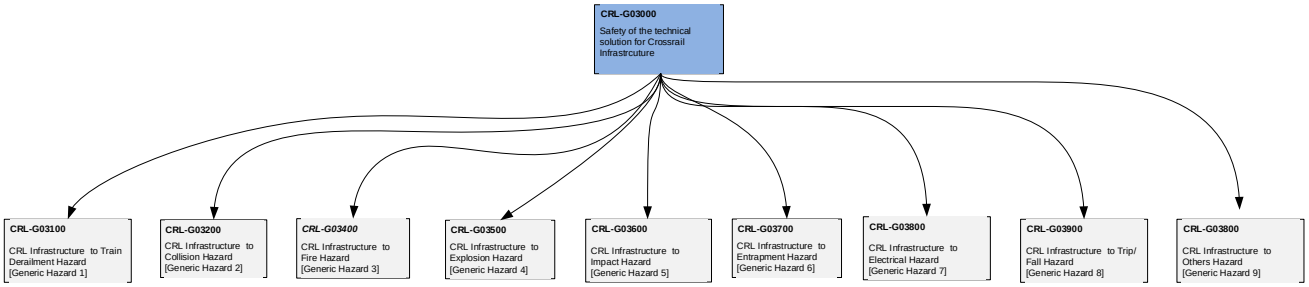


Diagram 1

The following is the listing of generic hazards from PWHR:

- **Potential for Derailment Hazard**
  - Der 1 Potential vehicle derailment due to a fault / failure of rolling stock
  - Der2 Potential vehicle derailment due to fault / failure of infrastructure
  - Der3 Potential vehicle derailment due to over speed
  - Der4 Potential vehicle derailment due to object on track
- **Potential for Collision Hazard**
  - Col1 Potential collision between rail vehicles
  - Col2 Potential collision between vehicle and object dropped / left on the track
  - Col3 Potential collision between vehicle and rail structure
  - Col4 Potential impact between vehicle and object falling from vehicle
- **Potential for Fire Hazards**
  - Fir1 Potential fire in vehicle / station / trackside / depot etc.
  - Fir2 Person(s) exposed to smoke in vehicle / station / depot etc.
- **Potential for Explosion Hazards**
  - Exp1 Explosive device
  - Exp2 Potential for explosion exists
- **Potential for Impact Hazards**
  - Imp1 Potential impact between rail vehicles and person (s)
  - Imp2 Potential impact between vehicle and person (s) falling from or being dragged / crushed by vehicle
  - Imp3 Impacts of person (s) with heavy object (s)
  - Imp4 Person (s) struck by flying objects
  - Imp5 Person (s) exposed to pointed or sharp objects
- **Potential for Entrapment hazards**
  - Ent1 Person (s) becoming trapped
  - Ent2 Potential for person (s) to become trapped by / caught in equipment / machinery
- **Potential for Electrical Hazards**
  - Ele1 Person (s) exposed to hazardous voltages on vehicle / track / station
  - Ele2 Person (s) exposed to arcing
- **Potential for Trip / Fall Hazards**
  - Stf1 Person (s) fall from height
  - Stf2 Slip / trip / fall hazard present
- **Potential for Other Hazards**
  - Oth1 Flooding
  - Oth2 Evacuation
  - Oth3 Station congestion
  - Oth4 Unauthorised access
  - Oth5 Lack of communication
  - Oth6 Structural failure
  - Oth7 Manual handling
  - Oth8 Exposure to noise
  - Oth9 Potential heat exhaustion due to exposure to abnormally high temperatures
  - Oth10 Person (s) exposed to hazardous materials
  - Oth11 Person (s) exposed to hot object / surface / fluid
  - Oth12 Trespass and illegal acts
  - Oth13 Road traffic accident
  - Oth14 Asphyxiation

(Note that the list is not exhaustive)

Additional information on derivation of Safety Acceptance Criteria
Three types of safety acceptance criteria are applied in the Technical Safety Report through the application of the Common Safety Methods, namely:

Deterministic Criteria:
Deterministic criteria that define specifically what must be done. Such criteria include compliance with specific standards, such as LU Standards or British or European Standards, compliance with specific safety requirements and implementation of hazard mitigations identified in the System Hazard Log or Change Safety Analysis processes;

Reference Systems:
The use of a similar reference system using the same products / configurations and applications and has the same functional, operational and environmental conditions (together with interfaces); and

Explicit Risk Estimation.
The ALARP (As Low As Reasonably Practicable) principle is applicable throughout, but the means of justifying it may vary with the novelty of safety risk from one part of the system to another. For major new constituents of the overall system, such as the new signalling system, specific ALARP analyses have been performed. In other areas, particularly where existing systems or procedures are continuing in use without change, it has generally been concluded on the basis of expert judgement that adherence to existing best practice is sufficient.

Example for a simple Safety Argument:
Potential for 'Structural Failure'

- The core hazards related to Structural failure is: Core Hazard Oth6 'Potential for structural failure'.
- The portfolio safety sub-goals that contributes to Structural failure risk is shown in table below:

Ref. (GSN Ref)	Goals
SI-G04119	The risk due to structural failure is reduce ALARP

Table X Structural Sub Goals

- This safety sub-goal is concerned with the demonstration that the risk of structural failures is acceptable.

Derivation of Safety Acceptance Criteria

- The safety acceptance criteria as per the CSM regulations are applied throughout the analysis for all generic hazards.
  - COP xxxxxxx
  - Reference System xxxxxx
  - ERE xxxxx

[Project/System Level]: Changes introduced by the scope of work has no impact on structures. Structural failure would be a second order event consequence. All mounting arrangements are reviewed and agreed with the appropriate civils engineer.
[Sub-System Level]: The Legacy Signalling (OS1) HAZID [D21], Engineering Safety Case for the Legacy Signalling System [S4] and Legacy Compliance Submission [L1-8] demonstrated that the structural supports for Signalling equipment are fit for purposes.

Conclusion
The potential risk for structural failure from the portfolio safety sub-goals are considered to be comparable.

5 Reference Documents

Ref:	Document Title	Document Number:
1.	Crossrail Engineering Safety Management Reference Manual	CRL1-XRL-O8-GML-CR001-50001
2.	Crossrail Process and Format for Overall Safety Justifications	CRL1-XRL-O8-GPS-CR001-50012
3.		
4.		

6 Standard Forms / Templates

Ref:	Document Title	Document Number:
A.	None	
B.		