PROJECT WORKS INFORMATION

Volume 2B – General Requirements

Part 32 – *Contractor's* Engineering Safety Management Requirements (Systemwide)

Document Number: CRL1-XRL-O8-XWI-CRG03-50002

Document History:

Revision:	Date:	Prepared by:	Checked by:	Approved by:	Reason for Issue:
1.0	25-08-11	Ken Harvey	C Bloxsome	M Kilby	Issued for implementation
2.0	16-05-12	Ken Harvey	C Bloxsome	M Kilby	C610 update/peer review
3.0	14-07-16	S James	Chi Wong	J Bates	Review, update of applicable legislation

Contents

Part 32 – Contractor's Engineering Safety Management Requirements

32.1 Introduction

This Part of the Works Information defines the requirements for engineering safety management (ESM) activities to be carried out by the *Contractor* to assure the safety of the Elementary Systems of the *works*

These ESM requirements apply specifically to the design engineering and provision of electrical, electronic and programmable electronic systems and railway mechanical systems. They are not relevant to civil engineering design and construction related activities where the *Contractor* has justified to the *Project Manager* within the *Contractor's* System Safety Plan that operational, maintenance and emergency safety will be adequately assured under the application of the Construction Design and Management (CDM) Regulations.

This document explains the engineering safety deliverables, and level of cooperation required from the *Contractor* to assist the *Project Manager*, the *Employer* or Others to secure safety authorisation to operate the railway in accordance with the applicable railway safety legislation.

32.2 Not Used

Defined Terms (Included in Overall Contract Glossary not in Part 32)

ALARP	As Low as Reasonably Practicable
AsBo	Independent Assessment Body
BS	British Standards
CDM	Construction Design & Management Regulations
CMDL	Contract Master Deliverables List
CSM	Common Safety Method Regulation
DeBo	Designated Body
DOORS	Database Object-Oriented Requirements System
EMC/EMI	Electromagnetic Compatibility/ Electromagnetic Interference
EN	Euro Norm
ESM	Engineering Safety Management
ETA	Event Tree Analysis
FMECA	Failure Modes Effects and Criticality Analysis
FTA	Fault Tree Analysis
HAZID	Hazard Identification
HAZOP	Hazard and Operability Study
IHA	Interface Hazard Analysis
ISA	Independent Safety Assessor
ISwA	Independent Software Assessor
LUL	London Underground Limited
NNTRs	Notified National Technical Rules
NoBo	Notified Body

NR(IL)	Network Rail (Infrastructure Limited)
ORR	Office of Rail and Road
PADS	Parts and Drawings System (NR)
PWHR	Project Wide Hazard Record (i.e. hazard log)
RAM(S)	Reliability, Availability, Maintainability, (Safety)
RIR 2011	Railway Interoperability Regulations
ROGS	Railways and Other Guided Transport Systems (Safety) Regulations
SIL	Safety Integrity Level
TSIs	Technical Specifications for Interoperability

32.3 Not Used

List of Appendices moved to 32.9.

32.4 System Safety

32.4.1 General Engineering Safety Management Requirements

The *Contractor* is responsible for the assurance of the adequacy of safety for the Elementary Systems of the *works.* This shall have regards to:

- normal, degraded and emergency operating modes;
- maintenance of the systems; and
- application conditions and environment of the Crossrail railway.

The *Contractor* shall provide to the *Project Manager* all necessary evidence of safety adequacy to assist the *Project Manager*, the *Employer* or Others to secure safety authorisation to operate the railway in accordance with the relevant railway safety legislation:

- Railway (Interoperability) Regulations 2011 (RIR 2011);
- Railways (Interoperability)(Amendment) Regulations 2013;
- Railway and Other Guided Transport Systems (Safety) Regulations 2006 as amended (ROGS); and
- Railways and Other Guided Transport Systems (Miscellaneous Amendments) Regulations 2013

To facilitate this, the *Contractor* shall be required to make presentations to and secure acceptance of the evidence of engineering safety from the *Project Manager* prior to seeking approval from the appropriate approval bodies

In providing the *works* the *Contractor* shall implement an engineering safety management system consistent with that of the *Employer's* System Safety Plan.

How the *Employer's* System Safety Plan is to be implemented on the Project is explained in the "Crossrail Engineering Safety Management Reference Manual" which will be provided for guidance to the *Contractor* by the *Project Manager* within 4 weeks of the *starting date*.

32.4.2 Engineering Safety Competency

The *Contractor* shall demonstrate to the satisfaction of the *Project Manager* that individuals involved in demonstration of safety adequacy of the Elementary Systems are suitably qualified and experienced.

32.4.2.1 Engineering Safety Manager

The *Contractor* shall appoint an appropriately experienced and competent Engineering Safety Manager who shall be responsible for the management, coordination, quality control and assurance of the *Contractor's* engineering safety management activities. The *Contractor* shall submit the CV of the Engineering Safety Manager to the *Project Manager* for acceptance. The accepted Engineering Safety Manager will serve as the primary interface with the *Project Manager* on engineering safety matters.

32.4.2.2 Competency of Engineering Safety Assessors:

The *Contractor* shall ensure that only qualified and competent professional assessors undertake engineering safety assessment activities. The *Contractor's* engineering safety organisation shall be explained in the *Contractor's* System Safety Plan, and it shall have suitable independence from the design and commercial delivery activities.

The *Contractor* shall maintain an engineering safety staff competency matrix indicating the roles and responsibilities and records of individual's competencies for review by the *Project Manager* upon request.

32.4.3 Demonstration of Safety Adequacy

Demonstration of safety adequacy of the Elementary Systems shall be carried out in compliance with:

- EU/402/2013 EC Commission Regulation – Common Safety Methods for Risk Evaluation and Assessment (CSM Regulation);
- EU/2015/1136 EC Commission Regulation - Amending Common Safety Methods for Risk Evaluation and Assessment (CSM Regulation); and
- ORR March 2015 Guidance on the Application of the Common Safety Method for Risk Evaluation and Assessment (against EU/402/2013);

and, where applicable:

- BS EN 50126 -1: 1999, 'Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)';
- BS EN 50128: 2011, 'Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems';
- BS EN 50129: 2003, 'Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling';
- BS EN 61508 Part 0: 2005 & Parts 1 to 7: 2010, 'Functional safety of electrical/electronic /programmable electronic safety-related systems" – all parts.

The *Contractor* shall prepare Engineering Safety Justifications for the Elementary Systems within the scope of the *works* based on application of the CSM Regulation.

32.4.3.1 Application of Common Safety Methods Regulation (CSM Regulation)

Guidance on how the *Contractor* shall apply the CSM Regulation to the *works* is given in the "Crossrail Engineering Safety Management Reference Manual" which will be provided by the *Project Manager* within 4 weeks of the *starting date*. The approach is summarised below:

The CSM Regulation, and supporting ORR guidance, advises that hazards can be analysed and evaluated by a combination of one or more of the basic principles given below.

A: Application of Codes of Practice

- The *Contractor* shall demonstrate that the Elementary Systems comply with the relevant codes of practice, standards and specifications (e.g. NR, LUL BS, and EN) in accordance with Part 29, Non-compliances are to be identified and safety justified by the *Contractor*.
- If, and where, the RIR 2011 apply, conformance with the relevant Technical Specifications for Interoperability (TSIs) and Notified National Technical Rules (NNTRs) will be advised in the Technical File relating to the Elementary System. In accordance with Works Information Volume 2A – Particular Requirements, Scope of Works the evidence of conformity will be made available by the *Project Manager.*

B: Comparison with Similar Systems (Reference System)

- Where reasonably practicable, the preference is to use railway proven, tried and tested components, Plant and Materials, Equipment and systems (i.e. reference systems). The *Contractor* shall prepare a Product Breakdown Structure, for acceptance of the *Project Manager*, to demonstrate the pedigree of proven use of reference systems prior to their procurement.
- In the event of components, Plant and Materials, Equipment or systems being proposed by the *Contractor* have no obvious proven use (i.e. not a reference system) then the *Contractor* shall advise the *Project Manager*, and the necessary evidence shall be provided by the *Contractor* to secure approval for use from the relevant acceptance bodies in advance of finalising the design. For new, novel, high risk or bespoke design proposals the *Contractor* shall propose in its System Safety Plan, for agreement of the *Project Manager*, where the *Contractor* is to evidence this via preparation of appropriate Product Safety Case(s).

C: Explicit Risk Estimation

- The *Contractor's* design shall be subject to a suitable and sufficient depth of hazard identification, risk estimation and evaluation by the *Contractor* depending on the magnitude of the perceived safety risk, whether the risk is new/novel, and complexity of the system design (e.g. bespoke design). The *Contractor's* estimation and evaluation shall confirm risks are either eliminated or controlled to as low as reasonably practicable (ALARP).
- For the majority of systems the risk estimation and ALARP justification shall follow a recognised risk matrix approach. However, for high risk (e.g. where the unavailability of the system safety function is judged immediately life threatening), new/novel, complex or bespoke design the *Contractor* may be required by the CSM Regulation to undertake a full, in depth, quantitative safety analysis.

- All hazard identification, risk estimation and evaluation will be recorded and monitored to successful resolution by the *Contractor* in the Project Wide Hazard Record (PWHR) relating to the contract.

32.4.4 System Safety Requirements

Outlined below is the process whereby the key system safety requirements are to be demonstrated by the *Contractor.*

32.4.4.1 System Safety Requirements Specification

The *Contractor* is to prepare a System Safety Requirements Specification for acceptance by the *Project Manager*; the document shall be derived from the Works Information as described in Appendix 32A.

The *Contractor* may chose, with prior agreement of the *Project Manager*, to identify safety requirements as part of the overall system requirements traceability strategy for the *works* and not prepare a separate System Safety Requirements Specification. This shall be explained in the *Contractor's* System Safety Plan.

Successful delivery of the identified safety requirements is to be traced by the *Contractor* through to Completion.

32.4.4.2 Project Wide Hazard Record

The outcome of preliminary hazard analysis by the *Employer* is recorded in the preliminary Project Wide Hazard Record (PWHR), which is provided with Works Information Volume 2C – Specifications and Reference Design. The *Contractor* is required to adopt and develop the preliminary PWHR as the principal engineering safety hazard management tool (i.e. hazard log).

The preliminary PWHR is supported on a web based database. The *Contractor* shall use the web based database to maintain the PWHR. On request, the *Project Manager* will provide the *Contractor* with the necessary process procedure, access and training in its use.

32.4.4.3 Safety Integrity Levels

Depending on the depth of application of the Common Safety Method Regulation (2009/352/EC) (CSM Regulation) the *Contractor* may be required under the Regulation to undertake a full quantitative safety analysis in support of explicit risk estimation. Should this be the case, the *Contractor* shall prepare for acceptance of the *Project Manager,* a Safety Integrity Level (SIL) Requirements Report, to recommend the system safety performance requirements against which the quantitative safety analysis will be evaluated. The identification of appropriate SILs is the responsibility of the *Contractor*, and shall be in accordance with the requirements of BS EN 50126 and BS EN 61508.

A preliminary evaluation of the SIL requirements for the Elementary Systems of the *works* is provided with Works Information Volume 2C – Specifications and Reference Design.

32.4.5 Operations and Maintenance

The *Contractor* shall ensure that the *works* are consistent with the mode of operation (normal, degraded and emergency) and maintenance defined by the *Employer's* requirements, and including the Crossrail Concept of Operations.

It is expected the *Contractor* will run appropriate hazard and operability studies (HAZOPs), or similar studies involving the *Project Manager* and Others, to ensure operational and maintenance safety issues are adequately addressed.

32.4.6 System Interfaces

The *Contractor* will prepare an Interface Hazard Analysis (IHA) to confirm the engineering safety implications at internal and external interfaces have been adequately addressed and managed. The IHA will involve the *Project Manager* and Others.

The IHA will take cognisance of the Systems Engineering requirements related to the management of interfaces described in Part 29.

32.5 Safety Deliverables

The required evidence of safety adequacy of the Elementary Systems shall be provided by the *Contractor* via the schedule of safety deliverables listed in Appendix 32A. It is accepted that not all safety deliverables may be relevant to the *works*. The *Contractor* shall include in the System Safety Plan described below a listing of the safety deliverables to be prepared.

Preliminary timescales and responsibilities for preparation and acceptance of the safety deliverables are summarised in Appendix 32C.

32.5.1 System Safety Plan

Within 8 weeks of the *starting date* the *Contractor* shall produce a System Safety Plan, which shall describe the *Contractor's* engineering safety management strategy for the *works* and submit it to the *Project Manager* for acceptance. In the case of the first submission of the System Safety Plan the *Project Manager* replies within 4 weeks of the date of submission. The System Safety Plan shall be prepared by the *Contractor* in accordance with the contents advised in Appendix 32B.

32.5.1 System Software Safety Plan

If significant software development or modification is proposed as part of the *works* then the *Contractor* shall prepare a System Software Safety Plan in accordance with the requirements of BS EN 50128 and submit it to the *Project Manager* for acceptance. The System Software Safety Plan shall list the proposed software safety deliverables for the *works*.

Where there is no proposed software development, or the software development or modification is minimal and not safety significant then the *Contractor* may judge a System Software Safety Plan is not required. This shall be clearly explained in the *Contractor's* System Safety Plan, along with the *Contractor's* processes to assure continuation of software safety.

32.6 Independent Review/Assessment

32.6.2 Independent Safety Assessment

The *Contractor* shall have carried out independent review of Product Safety Cases, where these are prepared, by an Independent Safety Assessor (ISA). An ISA review is required for Engineering Safety Justification(s) prepared by the *Contractor*, unless agreed otherwise by the *Project Manager*. These arrangements shall be described in the *Contractor's* System Safety Plan.

The *Contractor shall* propose an ISA to the *Project Manager* for acceptance.

The findings of the ISA shall be formally reported and made available to the *Project Manager* within 4 weeks of the Independent Safety Assessment being completed.

32.6.2 Independent Software Assessment

If significant software development or modification is proposed as part of the *works* the *Contractor* shall undertake an independent review of software development by an Independent Software Assessor (ISwA) in accordance with the requirements of BS EN 50128. These arrangements shall be described in the *Contractor's* System Software Safety Plan.

The *Contractor* shall propose an ISwA to the *Project Manager* for acceptance.

The findings of the ISwA shall be formally reported and made available to the *Project Manager* within 4 weeks of the Independent Software Assessment being completed.

32.5.2 Independent Assessment Body

In accordance with the CSM Regulation the *Employer* will appoint an Independent Assessment Body (AsBo) to confirm the *Contractor's* engineering safety assurance of the Elementary Systems is in conformance with the principles of the Regulation.

The *Contractor* is to fully cooperate with the AsBo, provide the engineering safety evidence necessary to carry out this assessment, and comply with any improvements to assure the *Contractor's* conformance with the CSM Regulation.

32.7 Programme, Monitoring and Auditing

A preliminary schedule for preparation and the approval route of the required engineering safety deliverables is given in Appendix 32C. The *Contractor* shall integrate the preparation of safety deliverables into the Accepted Programme.

In accordance with Part 29, the *Contractor* is to facilitate fortnightly design progress meetings with the *Project Manager*, where engineering safety management shall be an agenda item. The *Contractor's* Engineering Safety Manager and the *Project Manager's* ESM representative shall attend these meetings, where requested, and if there are significant engineering safety issues to discuss.

The status of engineering safety management activities shall be included in the Contractor's monthly progress report.

The *Contractor* shall ensure that engineering safety management auditing is considered within the overall Quality Assurance auditing programme for the *works* as described in Part 20. These arrangements shall be confirmed in the *Contractor's* System Safety Plan.

32.8 Engineering Safety Relationships

The *Contractor* shall within its System Safety Plan describe how the relationships with the aspects of the Works Information listed below are to be managed and coordinated.

32.8.1 RAM (Reliability, Availability and Maintainability)

The *Contractor* is to explain how the commonality between engineering safety and RAM (Part 30) is to be managed in line with BS EN 50126.

32.8.2 EMC (Electromagnetic Compatibility)

The *Contractor* shall explain how potential safety risks resulting from electromagnetic interference (EMI) (Part 31) are adequately managed and mitigated.

32.8.3 Health & Safety (CDM Regulations)

The *Contractor* shall identify and explain those civil engineering and other elements of the *works* where the operational, maintenance and emergency safety will be assured under the application of the Construction Design and Management (CDM) Regulations (Part 19).

Where operational and maintenance risks are identified within the CDM Risk Register, these shall be included in the PWHR for the *works* and cross-referenced.

32.8.4 Human Factors

The *Contractor* shall explain how any Human Factors analyses (Works Information Volume 2A – Particular Requirements, Scope of Works.) will be accounted for within the engineering safety management activities.

32.8.5 Testing and Commissioning

The *Contractor* shall explain how the safety of the Elementary Systems is to be demonstrated prior to testing and commissioning activities (Part 28).

32.8.6 Interoperability

The *Contractor's* responsibilities regarding application of the Railway (Interoperability) Regulations (RIR 2011) to the central section of the Crossrail Project are described in Works Information Volume 2A – Particular Requirements, Scope of Works.

32.9 Appendices

Appendix 32A Engineering Safety Deliverables

Appendix 32B Content of System Safety Plan

Appendix 32C Programme of Engineering Safety Deliverables

Appendix 32A – Engineering Safety Deliverables

System Safety Plan (SSP) – shall be prepared by the *Contractor* within 8 weeks of the *starting date* in accordance with the contents advised in Appendix 32B to this part of the Works Information. With prior acceptance of the *Project Manager*, the *Contractor* may make reference in the SSP to their existing engineering safety management processes and procedures. These processes and procedures shall be made available to the *Project Manager* with the SSP The SSP shall list the proposed safety deliverables for the contract.

System Software Safety Plan (SSSP) – shall be prepared by the *Contractor* within 8 weeks of the *starting date* and where significant software development or modification is proposed as part of the *works*. The SSSP shall be structured in accordance with the requirements of BS EN 50128. The SSSP shall list the proposed software safety deliverables for the *works*.

Stage Gate ESM Report(s) – where during the *works* it is necessary for the design to undergo a formal design assurance "Design Gate Review" to pass to the next project phase (e.g. 30%, 60%, 90% stages), the *Contractor* shall prepare and update a progressive ESM report to confirm the acceptable status of engineering safety management activities. This report shall be presented as part of the Design Gate Review. The format shall be provided by the *Project Manager* within 4 weeks of the *starting date*.

The report shall be made available to the *Project Manager* for acceptance at least 2 weeks before the particular Design Gate Review.

Safety Integrity Level (SIL) Requirements Report – in certain circumstances the *Contractor* may require to undertake full quantitative safety analysis in support of a Product Safety Case, or where explicit risk estimation is required by the CSM Regulation. Should this be the case, the *Contractor* shall prepare in advance for acceptance of the *Project Manager,* a SIL Requirements Report to recommend the safety performance requirements against which the quantitative safety analysis will be evaluated.

The identification of appropriate SILs is the responsibility of the *Contractor*, and shall be in accordance with the requirements of BS EN 50126 and BS EN 61508.

System Safety Requirements Specification (SSRS) – shall be prepared by the *Contractor* at start of its design activity to define the key safety requirements for the Elementary Systems of the *works*.

The *Contractor* is to derive the system safety requirements from the Works Information and including, but not limited to, the following sources:

- the *Employer's* performance specification(s) typically contained within Works Information Volume 2C;
- relevant codes of practice, standards, specifications and identified non-conformances typically Crossrail New Works Standard Baseline and Works information Volume 2C;
- Project Wide Hazard Record typically contained in Works Information Volume 2C;
- previous knowledge and experience of the *Contractor* regarding the Elementary Systems being prepared in accordance with the Works Information;
- Other specific requirements of the Works Information.

The *Contractor* is to trace the successful delivery of the identified safety requirements through to Completion.

Product Breakdown Structure (PBS) – shall be prepared by the *Contractor* prior to the procurement activity to list the reference systems(s), the related evidence of previous proven use and product approvals for the sub-systems, Plant and Materials, equipment and components of the Elementary System(s) of the Works Information. The pedigree of proven use and safety performance shall be evaluated by the *Contractor* in respect of previous and relevant NR or LUL product approvals, or via cross-acceptance from another recognised railway authority. The *Contractor* shall analyse the safety implications of differences in application and environment of the Project.

It shall include the following:

- Brief description of the significant system(s), Plant and Materials, equipment and components against which the previous approvals is claimed.

  Any previous approval shall be aimed at an appropriate level of safety significant systems, equipment and plant, and not necessarily at individual components.

- Example(s) of where the system(s), Plant and Materials, equipment or components have been previously in use in a similar railway environment.

- Reference to the documentary evidence which proves previous acceptance by a recognised railway authority. This could be a NRIL PADS certificate number, LUL standard equipment drawing, or approval letter from other recognised railway safety authority.

  Where new/novel or bespoke systems are proposed by the *Contractor* this reference may be to a Product Safety Case which has been prepared by the *Contractor* for use on the Project.

- Identification and analysis of any safety significant differences in application or environment relating to the use on the Project.

  Safety significant differences shall be justified by the *Contractor* in the Design Engineering Safety Justification(s) for systems, or in separate risk assessment(s) prepared by the *Contractor*.

  For parts of the *works* installed in tunnels particular emphasis is to be placed by the *Contractor* on the fire performance requirements for the Project.

The format and contents of the PBS will be provided by the *Project Manager* within 4 weeks of the *starting date*.

Evidence referred to in the PBS shall be made available by the *Contractor* for audit by the *Project Manager* prior to contract procurement. At contract completion the evidence shall be handed over to the *Project Manager* with the PBS.

Product Safety Case(s) (PSCs) – shall be prepared by the *Contractor* prior to procurement where it is proposed to use new or novel systems, Sub-systems, Plant and Materials, or Equipment where there is no previous proven use in an equivalent railway environment when compared to the Crossrail Project.

Where required, the *Contractor* is to structure such Project Safety Case(s) in accordance with the requirements of BS EN 50129. The *Contractor* is to identify in the System Safety Plan if, and where, such PSCs will be prepared.

Design Engineering Safety Justification(s) (DESJ) – shall be prepared by the *Contractor* prior to the end of design and before testing and commissioning, to confirm the adequacy of safety of the design of the Elementary Systems of the *works*.

It may be necessary for the *Contractor* to prepare more than one engineering safety justification where the scope of the *works* relates to several Elementary Systems. The Engineering Safety Justification(s) shall contain the relevant evidence of adequacy of safety, or make reference to separate contract deliverables required by the Works Information containing such evidence.

Where there are interfaces with adjacent NR and LU infrastructures the *Contractor* shall prepare a separate Design (Interface) Engineering Safety Justification to enable these interfaces to be safety approved by the adjacent Infrastructure Managers. This shall make reference to the Interface Hazard Analysis undertaken by the *Contractor*.

Guidance on the format and contents of the DESJ will be provided by the *Project Manager* within 4 weeks of the *starting date*.

Engineering Safety Justification(s) (ESJ) – final engineering safety justification(s) shall be prepared by the *Contractor* post testing and commissioning to confirm the adequacy of safety of the *works* following the successful outcome of the testing and commissioning phase. These shall be prepared as an update to the Design Engineering Safety Justification(s) previously accepted by the *Project Manger*.

The ESJ shall clearly define any safety operating constraints and minimum operating requirements for the system(s).

Guidance on the format and contents of the ESJ will be provided by the *Project Manager* within 4 weeks of the *starting date.*

Appendix 32B – Content of System Safety Plan

Listed below are the proposed contents of the System Safety Plan (SSP) to be prepared by the *Contractor*. It is acceptable to implement an alternative structure of headings provided the requirements of the listed contents are addressed. Where appropriate, the *Contractor* may make reference to existing internal processes for engineering safety management; in such instances copies of these references shall be provided to the *Project Manager* with the SSP.

1. **Safety Policy and Strategy** – brief outline of the *Contractors* own safety policy, strategy and arrangements for achieving engineering safety as part of *works*.

   The approach shall be consistent with the ***Employer's*** requirements of the Crossrail Engineering Safety Management - System Safety Plan which will be provided by the *Project Manager* within 4 weeks of the *starting date*.

2. **Scope of the Plan** - what is covered, and what is not covered, by the SSP and with reference to the scope of the Works Information. Any constraints or assumptions relating to the scope of the SSP should be described.

   Explanation should be given of how the relationships between engineering safety, RAM, CDM, EMC/EMI, Human Factors, Interoperability, and Testing & Commissioning activities will be managed by the *Contractor*. Reference shall be made to the *Contractors* documentation, Plans or Strategies for managing these activities.

   Where there is significant software development within the *works*, the *Contractor* shall prepare a System Software Safety Plan (SSSP) in accordance with BS EN 50128. Reference shall be made to this SSSP in the SSP, or justification given by the *Contractor* why such a SSSP is not required, which is to be agreed by the *Project Manager*.

3. **Description of the System** - brief outline of system(s) to be provided by the *Contractor* within the scope of the *works* and covered by the SSP.

4. **Design Safety Organisation** - details of the roles, responsibilities and competencies of those within the ***Contractor's*** organisation responsible for engineering safety. The CV(s) of those persons having responsibility for engineering safety management shall be referred to. The organisation should demonstrate independence between design, commercial delivery and the engineering safety activities. Particular attention shall be given to organisational arrangements at interfaces between contracts and with Others.

5. **Safety Requirements** – a description of how the system(s) safety requirements (including SILs, where appropriate) are to be derived from the Works Information, standards and other sources, and how and where compliance will be demonstrated.

   The *Contractor* is required to prepare a separate System Safety Requirements Specification at start of design for acceptance by the *Project Manager*. Alternatively, the *Contractor* may chose, with prior acceptance of the *Project Manager*, to identify safety requirements as part of the overall system requirements traceability strategy for the *works* and not prepare a separate System Safety Requirements Specification.

6. **Safety Analysis Methodology** – the tools and techniques to be applied during engineering safety assessment will depend on the complexity of the system(s), the perceived magnitude of the safety risks and whether the design is new/novel or bespoke. This section of the SSP shall describe those safety analysis processes the *Contractor* intends to implement with reference to recognised standards, or internal procedures. This may include, but is not limited to:

   - Hazard Management (i.e. Project Wide Hazard Record)
   - Hazard Identification (e.g. HAZOP, HAZID)
   - Interface Hazard Analysis (e.g. IHA)
   - Semi-Quantitative Risk Assessment (e.g. Risk Matrix)
   - Quantitative Risk Assessment (e.g. FMECA, FTA, ETA)
   - Engineering Safety Auditing (internal and external)

7. **Details of Safety Deliverables** – a preliminary list of all safety deliverables shall be provided in the SSP in support of engineering safety assurance and approvals. The list shall be updated as, and when, new safety deliverables are identified.

8. **Safety Justification Strategy** – description of the proposed content of safety justifications supporting engineering safety assurance and approvals. To include:

   - Product Safety Case(s) – in situations where it is necessary to seek pre-approval of new/novel or bespoke design equipment;
   - Stage Gate ESM Reports;
   - System Engineering Safety Justification(s) – Design and Final.

9. **Approval Process** – description of the internal verification, validation and approvals process for the engineering safety deliverables. Explanation shall be given regarding the requirement for, and proposed involvement of, an Independent Safety Assessor.

10. **Safety Approval of Modifications** – explanation of how engineering safety implications of design modifications and value engineering are to be assured and approved throughout the delivery of the *works* (i.e. change control).

11. **Operation and Maintenance Performance** – summary of the process for analysing operation and maintenance performance to ensure realised safety is compliant with *Employer's* requirements and the Crossrail Concept of Operations.

    It is expected the *Contractor* will run appropriate HAZOPs or similar studies, involving the *Project Manager* and Others, to ensure operational and maintenance issues are adequately addressed.

12. **Control of Safety Interfaces** – identification of, and description of the process for, engineering safety management activities at internal and external interfaces.

    The *Contractor* will prepare an Interface Hazard Analysis (IHA) to confirm the engineering safety implications at internal and external interfaces have been adequately addressed and managed. The IHA will involve all relevant interfacing *Contractors*, third parties and the *Project Manager*.

The IHA will take cognisance of the Systems Engineering requirements related to the management of interfaces described in Works Information Volume 2B – Part 29 Design Assurance, Certification and Records.

13. **Procurement of Plant/Equipment** - how it will be ensured by the *Contractor* that the design is fit for purpose, plant/equipment or systems have proven use in the railway environment, or any proposed new/novel plant/equipment or systems are pre-accepted by the *Project Manager* in advance of procurement.

    It is required that the *Contractor* will maintain a Product Breakdown Structure for the Elementary Systems to assure the approval status of the component plant/equipment and systems prior to procurement. The *Contractor* shall programme the *Project Manager's* acceptance of proposed new/novel Plant and Materials, equipment or systems to be consistent with the procurement strategy for the *works*.

14. **Subcontractor Safety Management** – explanation of how the engineering safety management arrangements of Subcontractors and Suppliers will be managed to be compatible with the *Contractor's* System Safety Plan, and the engineering safety management requirements of the *Employer*.

15. **Monitoring and Control** – description of the requirements for periodic engineering safety review and engineering safety auditing (internal and external), throughout the delivery of the *works*.

Appendix 32C – Programme of Engineering Safety Deliverables

Project Phase	**Engineering Safety Deliverables**	***Contractor***	***Project Manager/Employer***	**Approval Body**
8 weeks after *starting date*	System Safety Plan – to establish *Contractor's* ESM approach, agree preliminary list of contract ESM safety deliverables and programme for their delivery	Prepare & Approve	Review & Accept	Endorse
8 weeks after *starting date*	System Software Safety Plan – if required, to confirm the *Contractor's* software development strategy is consistent with BS EN50128	Prepare & Approve	Review & Accept	Endorse
As Required	Such HAZID Reports, Risk Assessments, FTA, ETA, FMECA, OHSA, IHA etc. as necessary in support of Engineering Safety Justifications	Prepare & Approve	Review & Accept	N/A
2 weeks prior to each Design Stage Gate	Stage Gate ESM Report(s) – to confirm a suitable & sufficient depth of engineering safety management to pass design stage gates (e.g. 30%, 60%, 90% Completion)	Prepare & Approve	Review & Accept	N/A
Start of Design	System Safety Integrity Level (SIL) Requirements Report – to determine and agree the requirements, if any, for SILs assigned to system safety functions	Prepare & Approve	Review & Accept	N/A
Start of Design	System Safety Requirements Specification – as per BS EN 50126 (alternatively may be flagged safety related in the overall system requirements specification)	Prepare & Approve	Review & Accept	N/A
Prior to Procurement	Product Breakdown Structure – to confirm the existing proven use of equipment proposed in the system design prior to procurement (i.e. "reference systems")	Prepare & Approve	Review & Accept	N/A
Prior to Procurement	Product Safety Case(s) - as, and if, required owing to the proposed use of new/novel or bespoke equipment and prior to procurement	Prepare & Approve	Review & Accept	Endorse
End of Design	Design Engineering Safety Justification(s) – preliminary document to confirm design is fit for purpose prior to installation, testing & commissioning	Prepare & Approve	Review & Accept	Endorse
Post Testing & Commissioning	Engineering Safety Justification(s) – final document prepared at successful completion of T&C such that the system can be safely brought into service	Prepare & Approve	Review & Accept	Endorse
Award of Contact & final version at Completion	System Project Wide Hazard Record (PWHR) – hazard log to confirm all hazards are successfully resolved such that the system can be safely brought into service	Prepare & Approve	Review & Accept	N/A