Division / Business Unit: Inland Rail
Function: Rail Safety
Document Type: Guideline

Safety in Design

COR-GL-014

Applicability

Inland Rail	SMS

Publication Requirement

Internal / External

Document Status

Version #	Date Reviewed	Prepared by	Reviewed by	Endorsed	Approved
1.0	26 Jul 2017	Health Safety & Environmental Systems Coordinator – Inland Rail	Engineering Manager – Inland Rail	Programme Technical Manager – Inland Rail	Programme Technical Manager – Inland Rail

Amendment Record

Amendment Version #	Date Reviewed	Clause	Description of Amendment
1.0	26 Jul 2017		Initial issue

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this guideline is to detail the ARTC Inland Rail minimum Safety in Design (SiD) requirements and make clear the health and safety responsibilities that will be managed and monitored by Designers.

1.2 Scope

This guideline is for Designers working on ARTC Inland Rail projects. It applies to both internal engineering teams and externally engaged Designers.

1.3 Document Owner

The Programme Technical Manager is the Document Owner and is the initial point of contact for all queries relating to this procedure.

1.4 Responsibilities

The Programme Technical Manager and Programme Delivery Managers are responsible for the implementation of this document.

1.5 Reference Documents

ARTC Project Management Procedure (EGP-20-01)

Safe Design of Structures Code of Practice (July 2012)

AS7470:2016 Human Factors Integration in Engineering Design - General Requirements

RSK-PR-001 ARTC Risk Management Procedure

COR-FM-022 Safety in Design Report

COR-FM-023 Safety in Design Risk Template

1.6 Definitions

The following terms and acronyms are used within this document:

Term or acronym	Description
ARTC	Australian Rail Track Corporation Ltd.
ACT	Refers to: • WHS Act (2011) and associated Regulations • Rail Safety National Law Act (2012) and associated Regulations
Designers	A Service Provider offering Design Services. A person conducting a business or undertaking (PCBU) whose profession, trade, business or agency involves them in expert or professional services that include but are not necessarily limited to the following fields:- architecture, engineering, planning, management, development, safety, access and certification, including managers of these services. A person who alters or modifies a design without consulting the original or subsequent Designer will assume the duties of a Designer
Contractor	Reference to “contractor“ within this document shall, where relevant, be

Term or acronym	Description
	construed to mean any Subcontractor.
Constructor	A Service Provider offering Construction Services
Design	In relation to plant or structure will include: • design of part of the plant or structure • redesign or modify a design.
Hazard	A source of potential harm or a situation with the potential to cause loss.
Hierarchy of Control	A sequence of options which offer you a number of ways to approach the control of hazards. The hierarchy is arranged in order of implementation preference. • Elimination • Substitution • Isolation • Engineering controls • Administrative controls • Personal Protective Equipment (PPE)
Persons Conducting Business or Undertaking (PCBU)	A person conducts a business or undertaking: • Whether the person conducts the business or undertaking alone or with others. • Whether or not the business or undertaking is conducted for profit or gain. This includes a business or undertaking by a partnership or an unincorporated association.
Preliminary Hazard Analysis (PHA)	Systems of work which are foreseeable as part of the construction methodology and the intended use of a structure as a workplace, they should be identified in the preliminary hazard analysis.
Risk	Effect of uncertainty on objectives. An effect is a deviation from the expected, either positive and/or negative. Objectives can have different aspects (such as financial, rail safety, WHS and operation goals) and can apply at different levels (such as strategic, organisational, project and process).
Safety in Design	The integration of control measures early in the design process to eliminate or, if this is not reasonably practicable, minimise so far as is reasonably practicable, risks to health and safety throughout the life of the plant or structures being designed.
SFARIP	So Far As is Reasonably Practicable – The likelihood and consequence of a risk must be weighed against the availability, effectiveness and cost of measures to eliminate or reduce the risk.

2 Safety in Design

2.1 Obligations

A Designers key obligations under the ACT include, but are not limited to, a duty to:

- Identify health and safety risks in relation to their design through consultation across the entire life of the plant or structures being designed
- Manage hazards through the implementation of a systematic risk management process, utilising the Hierarchy of Control in order to mitigate the health and safety risks associated with the design to so far as is reasonably practicable
- Maintain control measures
- Review control measures through consultation
- Communicate Safety in Design information to all parties who interact with the design

All PCBUs have a legal duty to ensure so far as is reasonably practicable, that employees, other workers and other persons (including the public) are not exposed to health and safety risks arising from the business or undertaking.

A PCBU that designs plant or structure must ensure, so far as is reasonably practicable, that the plant or structure is designed to be without risk to the health and safety of various persons who would carry out reasonably foreseeable tasks in relation to the design or are exposed to health and Safety risks arising from that design.

3 Safety in Design Process Overview

3.1 Code of Practice for Safe Design of Structures

The ARTC Project Management Procedure (EPG-20-01) recommends Designers use of the Safe Work Australia Code of Practice for Safe Design of Structures.

The Code provides practical guidance to persons conducting a business or undertaking who design structures that will be used, or could reasonably be expected to be used, as a workplace. This includes architects, building designers and engineers. This Code is also relevant for anyone making decisions that influence the design outcome, such as clients, developers and builders.

This Code applies to the design of ‘structures’ defined under the WHS Act to mean anything that is constructed, whether fixed or moveable, temporary or permanent, and includes:

- buildings, masts, towers, framework, pipelines, roads, bridges, rail infrastructure
- underground works (shafts or tunnels)
- any component of a structure, and
- part of a structure

3.2 What is Safe Design

Safe design (or Safety in Design) means the integration of control measures early in the design process to eliminate or, if this is not reasonably practicable, minimise so far as is reasonably practicable (SFAIRP), risks to health and safety throughout the life of the plant or structures being designed.

The safe design of a structure will always be part of a wider set of design objectives, including practicability, aesthetics, cost and functionality. These sometimes competing objectives need to be balanced in a manner that does not compromise the health and safety of those who work on or use the structure over its life.

4 Provisions and Requirements

4.1 Organisation

4.1.1 Information and Consultation

Consultation between those involved across the project lifecycle aids in design decisions which can eliminate or minimise risks from the construction and operation of structures and plant.

Consultation obligations include interactions with the following key parties:

- Parties who are (or are likely to be) directly affected by a work health and safety matter in relation to the design (or those parties" safety representative)
- Persons who have a safety duty with the design and its outcome
- Persons who commission the construction work
- Persons involved in the operation and maintenance of a building or structure

4.1.2 Meetings and Workshops

The required meetings to be held will be referenced in the applicable section - Meetings and Workshops of the RFT Service Brief document.

4.1.3 Communication and Information on Safety in Design

Designers must give adequate information to those who interact with the design regarding:

- Each purpose for which the plant or structure was designed.
- The results of any calculations, analysis, testing or examination in relation to plant or structures, including any hazardous properties identified by testing. Designers must also provide ARTC-Inland Rail with details of their verification plan, including a register of relevant calculations relating to their design and verification of these calculations.
- The mitigations and actions necessary to ensure that the plant or structure is without risks to health and safety when used for a purpose for which it was designed, including:
    - Construction methods and techniques that were assumed and form the basis of the design (e.g. erection sequences)
    - Operating methods and maintenance techniques that were assumed and form the basis of the design.
    - Consideration of any reasonably foreseeable misuse.
- Residual safety hazards and risks relevant to construction, operation, maintenance, decommissioning, demolition and disposal must be clearly recorded and effectively communicated to those who interact with the design. Information regarding residual risks must include information as to how the residual risk is to be managed. Where the presence of perceived hazards that are significant or unusual and where a designer wound not expect

a competent contractor to immediately recognise the hazard are to be clearly identified on General Arrangement drawings rather than detail drawings, unless the hazard was specific to the detail and the drawing was designed to be used as a construction drawing by a contractor.

A Designer of a plant or structures must also give additional information in relation to Safety in Design, as prescribed by the Regulations. This includes, but is not limited to the following:

- Features that minimise/eliminate Hazardous manual tasks
- Noise emissions and measurement
- Provision of information to the manufacturer

Key parties to whom Safety in Design information should be communicated include:

- Other Designers
- Commissioners
- Constructors (including subcontractors)
- Operators
- Users and the public
- Maintainers
- Demolishers

4.1.4 Documentation

Safety in Design information may be documented in a combination of formats. The type and number of documents will vary depending on the project and would typically entail:

- Drawings featuring design details, including assumed construction methodologies
- Specifications
- Design Reports, including Safety in Design Reports
- Safety in Design Register
- Operations and Maintenance Manuals

Where provided for all Safety in Design information the ARTC-Inland Rail templates are to be used and returned back to ARTC-Inland Rail at the required times.

4.1.5 Competence Standards – Knowledge and Capability

ARTC-Inland Rail seeks to ensure that all people working on our projects are competent to carry out their particular duties and tasks. Competence is achieved through a combination of knowledge, training and experience.

Designers will be required to demonstrate to ARTC-Inland Rail management that their organisations have persons with appropriate health and safety knowledge, technical professional knowledge, and have the capability to manage design hazards through a formal system for the identification, elimination, and minimisation of risks. Designers will need to demonstrate and where requested provide evidence that personnel meet the requirements of the ARTC Competency Matrix- Engineering and Project Management, which can be found on the ARTC Working for Us web portal.

Where Designers are certifying drawings and designs they are to provide a copy of their Rail Industry Worker (RIW) Card relevant to their role for which they are providing design certification.

In addition to core design capabilities relevant to the Designer's role, a Designer should also have:

- Knowledge of work health and safety legislation, codes of practice and other regulatory requirements
- An understanding of the intended purpose of the structure or construction element
- Knowledge of risk management processes
- Knowledge of technical design standards
- An appreciation of construction methods and their impact on the design
- The ability to source and apply relevant data on human dimensions, capacities and behaviours

Many design projects are too large and complex to be fully understood by one person. Various persons with specific skills and expertise may need to be included in the design team or consulted during the design process to fill any knowledge gaps, for example ergonomists, engineers and occupational hygienists.

Designers are required to declare and be able to demonstrate the level of health and safety training that has been completed by their managers and supervisors, relevant to their responsibilities.

4.2 Stages of Safety in Design

Safety in Design (SiD) reviews are required to be conducted at regular pre-agreed milestones throughout design development. SiD reviews should also be conducted following design change or change in design scope. The level of review will be dependent on the scope of change. SiD reviews will be conducted through consultation of the relevant project stakeholders and will typically be facilitated through a series of Safety in Design Workshops. Following all SiD Reviews, a SiD Report together with the ARTC Inland Rail - Safety in Design Risk Template (Doc No: COR-FM-023), must be compiled to communicate the outcomes of the review and other relevant SiD information to the relevant stakeholders using the ARTC Inland Rail – Safety in Design Report (Doc No: COR-FM-022).

Unless otherwise approved by ARTC Programme Technical Manager, ARTC-Inland Rail's Safety in Design templates are to be used for all SiD reviews, record keeping and reporting.

The minimum details and formatting requirements for health and safety information provided by Designers are to detail as per the ARTC Inland Rail - Safety in Design Risk Template.

SiD reviews are to be undertaken as a minimum at the following points in the design development process:

- During Phase 1 Concept Assessment
- During Phase 2 Project Feasibility (Reference Design), required after 30% and 70% design gate reviews
- During Phase 3 Project Assessment (Detailed Design), required immediately after 30% and 70% design submissions. Specific SiD requirements will be established by the ARTC Design Managers and referenced with the corresponding Project Request for Tender documents.

In addition to these design phase reviews, there may be additional safety reviews (i.e. Human Factor Analysis) to be undertaken throughout various project lifecycle phases.

4.3 Participants in Safety in Design Workshops/ Responsibilities

4.3.1 Inland Rail Design Manager

The ARTC Inland Rail Design Manager of a project/s will also fulfil the duty of Inland Rail's SiD Representative. The Design Manager will be responsible for:

- Communicating Inland Rail's SiD Requirements
- Facilitating consultation between all relevant stakeholders of the Project
- Managing the SiD process to ensure it is conducted in line with Inland Rail's policies and procedures
- Import Inland Rail's SiD lessons learnt, where relevant
- Monitoring and reviewing SiD controls through consultation
- Manages the competency assessment and verification of personnel with SiD duties
- Reviewing Designers verification documentation regarding calculations, analysis, testing or examination in relation to plant or structures. Requesting Designers to provide information confirming that calculations, analysis, testing or examination has been conducted and the results have been verified. Typical documentation that should be provided is a calculations register supported by the relevant Designers' verification forms

4.3.2 Designers (Service Providers)

Designers must ensure they conduct risk management in relations to their design and conduct SiD in accordance with Inland Rail's minimum requirements and relevant legislative requirements.

Key Designer SiD obligations include:

- Nominating a SiD representative for their firm. If a Design firm operates across a number of disciplines, then that firm need to appoint a SiD representative per discipline
- Consulting with the relevant project stakeholders throughout the design development
- Conducting risk management in regards to their design, including:
  - Carrying out, or arranging the carrying out of, any calculation, analysis, testing or examination that may be necessary
  - Identifying health and safety risks in relation to their design through consultation
  - Assessing these risks
  - Mitigating risks through the implementation of the Hierarchy of Control
- Communicating to the relevant project stakeholders all SiD information in relation to their design. Including any calculations, analysis, testing or examination in relation to plant or structures, including any hazardous properties identified by testing. Designers must also provide Inland Rail with details of their verification plan, including a register of relevant calculations relating to their design and verification of these calculations
- Schedule and Organise SiD Workshops in line with the lifecycle phases

4.3.3 Inland Rail Project Team

Inland Rail as the "Client" is an essential participant in the design consultation process and has the responsibility to ensure that information such as the purpose and usage of the design is clearly communicated to all persons with design duties. The ARTC Inland Rail Project Manager is the appointed Client Representative. As such the Project Manager's SiD obligations include:

- Consult with Designers, so far as reasonably practicable, about how to ensure that health and safety risks arising from the design during construction, operation, maintenance, decommissioning, demolition and disposal are eliminated or minimised
- Consult with Designers to ensure that the foreseeable purpose and usage of the design outcome is fully communicated
- Provide the Designer with any information has in relation the hazards and risks at the site where the construction work is to be carried out, including previous site investigations, previous incident records and industry specific information
- Communicate any relevant previous hazards or incidences previously exposed to in similar design scenarios or any relevant industry related safety hazards or incidents
- Ensure suitable participants and subject matter experts (including representatives from ARTC Operations and Maintenance teams) are nominated for SiD Workshops

4.3.4 Operators and Maintainers

- Provide expert/informed knowledge of operations and operational and maintenance relate hazards
- Participate in consultation during the design development of a project
- Implement, monitor and review all assigned operational/maintenance phase control measures
- Communicate SiD information to all stakeholders involved with alterations, modification and decommissioning, demolition and disposal of the project
- Implement, monitor and review all assigned operational/maintenance phase control measures

4.3.5 Other Participants

Depending on the design phase additional key stakeholders should be considered for engagement in the SiD Workshops, some of these include:

- WHS and Rail Safety Members
- Construction Team Members
- Suppliers, Manufacturers, Importers and Subcontractors
- Statutory Authorities
- Subject Matter Experts

5 Design Risk Review Process

5.1 Design Risk Assessment Process

Design Risk assessments must be a continual and iterative process as the design proceeds. Designers of both permanent and temporary works must have and apply formal systems covering their risk assessment process.

This is to ensure design solutions are assessed for all reasonably foreseeable hazards that may occur as the structure is built, commissioned, used, maintained, modified, decommissioned, demolished and disposed or recycled.

The system must ensure that it, so far as is reasonable practicable**, Identifies, Assesses, Controls, Reviews and Communicates** all health and safety risks relevant to this lifecycle.

Designers are to ensure all control measures they propose are fit for purpose and must be reviewed and adjusted through consultation. The Hierarchy of Control must be utilised in determining hazard control alternatives. The residual risks for each alternative must be assessed, with the selection of a preferred control measure determined by that which reduces the risk to as low as reasonably practicable.

5.2 Preliminary Hazard Analysis

Designers shall conduct a Preliminary Hazard Analysis (SiD Workshop) at completion of the Design Reference Phase (Phase 2) and as defined in the requirements of Section 4.2. The PHA provides an early high level assessment of the system design / configuration to identify potential hazards, causes and outcomes, and provides a structured mechanism for imitation of appropriate actions to eliminate, mitigate or control the risks. The outputs from the PHA / SID Workshops will be captured through the Inland Rail SiD Risk Template (Doc No: COR-FM-023).

The PHA should be carried out in conjunction with a preliminary Failure Modes, Effects and Criticality Analysis (FMECA), covering both an analysis of individual item failures as well as processes which focus on the interface between operator or maintenance staff and the infrastructure. Some of the failure modes identified within the FMECA will create hazards and will provide inputs to the PHA.

Design engineers have a primary responsibility to ensure that Hazard and Risk analyses are completed as part of each design task and Engineers responsible for verification of design outputs must ensure that the analyses have been completed.

The Hazard Analysis shall be included as part of the design documentation for the project or task and referenced in the ARTC Inland Rail - Safety in Design Report (Doc No: COR-FM-022).

5.3 Detailed Hazard and Risk Analysis

Detailed hazard and risk analysis shall be carried out progressively during Phase 2 (Feasibility Design) and Phase 3 (Detailed Design) of the project, to permit recommendations arising from the analysis to be incorporated into design solutions. The detailed analysis shall follow the structure employed for a Workplace Risk Assessment (WRA), except that the analysis shall be performed at greater depth and, in its final form, shall reflect the final design to be constructed and commissioned.

The detailed analysis is a responsibility of design engineers, supported by specialists from ARTC Operations and Inland Rail Programme personnel. The assessment and analysis of risks shall be

completed using the Inland Rail SiD Risk Matrix and outputs captured in the Inland Rail SiD Risk Template and ARTC Inland Rail – Safety in Design Report (Doc No: COR-FM-022).

5.4 Hierarchy of Control

A primary objective of the hazard and risk analysis process is to ensure that hazards and risks are progressively identified and addressed during the design process and measures introduced to eliminate or mitigate the effect of the hazard wherever possible.

Risk control measures shall be implemented in the following order of preference:

- Elimination of hazard
- Reduction of the hazard through the use of less hazardous equipment, material and/or processes
- Reduction of the risk through engineering controls (e.g. guarding, modification)
- Reduction of the risk through administrative controls (e.g. safe work procedures, signs, training to improve the awareness of hazards and personal judgment regarding actions to reduce the associated risks etc.)
- Reduction of the risk through the use of Personal Protective Equipment (PPE)

Design engineers and specialist staff performing hazard and risk analyses are responsible for identifying and implementing control measures as part of the design task and for providing and/or updating the relevant documentation before the new or altered equipment is introduced into service.

Supporting documentation shall, as a minimum, comprise of the following:

- Operating procedures and instructions
- Process Control Plans (PCP), setting out specific procedures and precautions for performance of maintenance and construction tasks. These will include details of the conditions under which tasks can be safely performed, e.g. isolations, possession, as well as PPE , tools and other equipment to be used and specialist training / competency requirements

6 Additional Design Risk Considerations

6.1 Functional Safety Analysis of software/ Electrical/ Electronic Systems

Infrastructure applications that incorporate software and/or electrical/electronic systems for control of safety functions shall be subject to controls within the ARTC Inland Rail design environment. Similar requirements shall be implemented where the proper operation of a safety system depends on a human interface.

Australian Standards AS 61508.1: 2011 to 61508.7: 2011 provide detailed guidance for establishing requirements for analysis of safety related systems, including the identification of hazards and risks associated with the systems.

Requirements and techniques shall be determined on a case by case basis, including the need for independent assessment and verification of the design.

The results of functional safety analysis for software and/or electrical/electronic shall be documented in a specific report and shall be maintained as part of the design record for the system or equipment.

6.2 Protection of Public

Protection of the public is of paramount concern. Any designs or arrangements must address the safety risks that construction and operational activities present to members of the public.

Where design requires specific measures to protect the public, this information must be clearly detailed in the design information for adoption into the Safety in Design Register.

6.3 Temporary Works

Temporary Works are defined as the works required for execution, completion, maintenance and/or demolition of permanent works which will normally be removed from the site on completion.

Designers are required to demonstrate by calculation, analysis, testing or examination that any temporary structures they specify are capable of performing the duties required.

Design information, including calculations, analysis or testing, must be supplied to ARTC-Inland Rail in sufficient time to allow a review to be carried out by ARTC-Inland Rail.

All temporary works are to be designed in accordance with relevant Codes of Practice.

6.4 Fire prevention, Detection and Emergency Procedures

Designers must consider the impact of their designs in the areas of fire prevention, detection and emergency procedures. This is both during construction and post construction.

Where identified and defined within the scope of work, Designers must ensure that as part of their risk management, they develop drawings that identify Fire Zones, Smoke Zones, Fire Dampers, Fire Collars, Fire Rated Walls, Paths of Travel and locations of all active and passive methods of fire protection.

Design and operational impacts must consider Emergency Response processes, equipment and access requirements and ensure that key emergency response organisations are consulted on the design and the associated operational aspects to ensure an effective response can be achieved in credible scenario event.

6.5 Human Factors

Human Factors must be considered in the design of safety critical systems or operating systems with human – system interfaces requires consideration of a Human Factors Integration Plan. The plan is to ensure user requirements are captured and addressed. Guidance on the content and its formulation of Human Factors integration plan can be found in AS7470:2016 Human Factors Integration in Engineering Design - General Requirements.

6.6 Assumptions, Dependencies and Constraints (ADCs)

The ADCs made against specific hazards identified as part of the SiD review will be tracked throughout the project life cycle in the Project Hazard Log (under the “Assumptions / Dependencies / Constraints” fields). All ADCs will be reviewed as part of the Design Safety Reviews (SiD Workshops). Upon confirmation / resolution of the ADCs by the design team or relevant party, the confirmation / resolution status will be recorded in the Project Hazard Log under the “Assumptions / Dependency / Constraint” field.

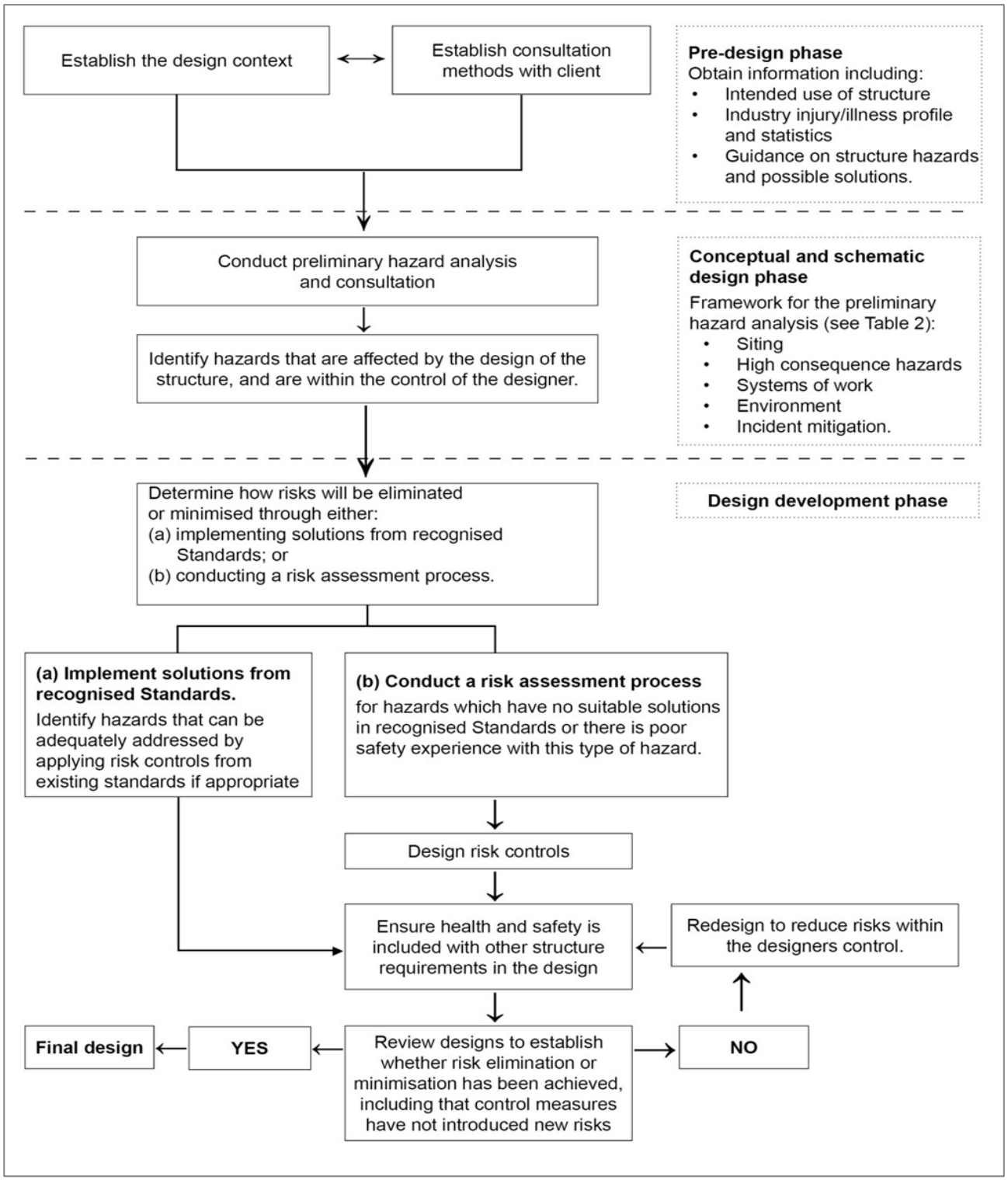
6.7 Transfer of Risks and Ownership

The intent is that controls and mitigations developed through the design development which impact the construction, maintenance, operation or disposal of an asset will be transmitted and accepted by the appropriate owner as the asset is created and moves through its life cycle.

6.8 Requirement Analysis and Allocation Traceability Matrix (RAATM)

Designers shall ensure that the Project Requirements as issued by Inland Rail will be used as the basis for the Requirements Analysis and Allocation Traceability Matrix, and be maintained by the Designer.

Appendix 1 - Safety in Design Process Flow



Reference: Safe Design of Structures – CoP (July 2012)