Transport Roads & Maritime Services

# Design safety – lifecycle management

An overview of the design safety lifecycle management process under the OneRMS safety management system (OneRMS SMS).

RMS 17.076 **Version 1** **22 March 2017** Objective reference: **A10232585**

# Contents




While the information provided by Roads and Maritime Services (Roads and Maritime) has been compiled with all due care, Roads and Maritime does not warrant or represent that the information is free from errors or omissions, is up to date or that it is exhaustive. Roads and Maritime does not warrant or accept any liability in relation to the quality, operability or accuracy of the information. Roads and Maritime disclaims, to the extent permitted by law, all warranties, representations or endorsements, express or implied, with regard to the information. Users of the information will be responsible for making their own assessment of the information, and Roads and Maritime accepts no liability for any decisions made or actions taken in reliance upon any of the information. Any such decision or action is made or undertaken at the risk of the user of the information. Users wishing to rely on the information should seek their own expert advice.

# Introduction

The design safety lifecycle management framework is a critical element of the OneRMS SMS and the key point in any project where we can eliminate risk.

The Roads and Maritime Services (Roads and Maritime) *infrastructure system* is designed to consider safety including work health and safety and *human factors* during future construction, use, operation, maintenance, modification and demolition.

## Purpose

This framework provides an overview on the design safety lifecycle management process. The purpose of the process is to ensure infrastructure systems are designed so they are safe to construct, use, operate, maintain, modify and demolish. This process supports the implementation of sections 19 (2) and (3) and 22 (2) of the *Work Health and Safety Act 2011.*

## Scope and context

Roads and Maritime workers use this framework for infrastructure design projects, including upgrades. It is tailored according to the nature of the project (size, design-phase and specific needs) by the project-specific Design Safety plan(s).

This framework is used when carrying out design safety activities within Roads and Maritime infrastructure system design projects.

## System requirements

Requirements under this framework can be found in Appendix A. For all system requirements see the *OneRMS SMS manual*.

# Design safety

## 1. Design safety domains

Safety is a key consideration when designing systems and an integral part of the engineering lifecycle management process. Design safety covers domains such as work, health and safety (WHS), system safety and human factors (HF):

- **WHS** covers aspects of health and safety in the workplace. This includes physical, ergonomic, biological, chemical and psychosocial hazards
- **System safety** is a formal engineering design process for hazard identification, evaluation, tracking, elimination or associated risk reduction to an acceptable level throughout the entire lifecycle of a system. This includes chemical, radioactive, biological, environmental, physical, ergonomic, electrical, hardware and software hazards during the system design
- **HF** covers issues such as human performance, error, workload, situation awareness, fatigue, physical layouts, geometry and environment of the workplace, system of work/task analysis, interface design (eg signage, markings, traffic lights, intelligent transport system), lighting, noise, vibration, biomechanics, ingress/egress, and associated safety and effectiveness aspects.

System safety and HF complement each other during the system design process. As described above, they cover most of the design related WHS issues in addition to some other vital safety issues.

Design safety integration ensures WHS, system safety and HF related safety aspects of the infrastructure system are considered during the early system design phase. For more details on the design safety lifecycle process, see *A guide to RMS Design Safety lifecycle management framework*[1].

Phase reviews are carried out to provide assurance design safety related risks within projects have been adequately addressed by adhering to this framework. Phase reviews are carried out by suitably qualified and experienced persons with no prior involvement in the subject design.

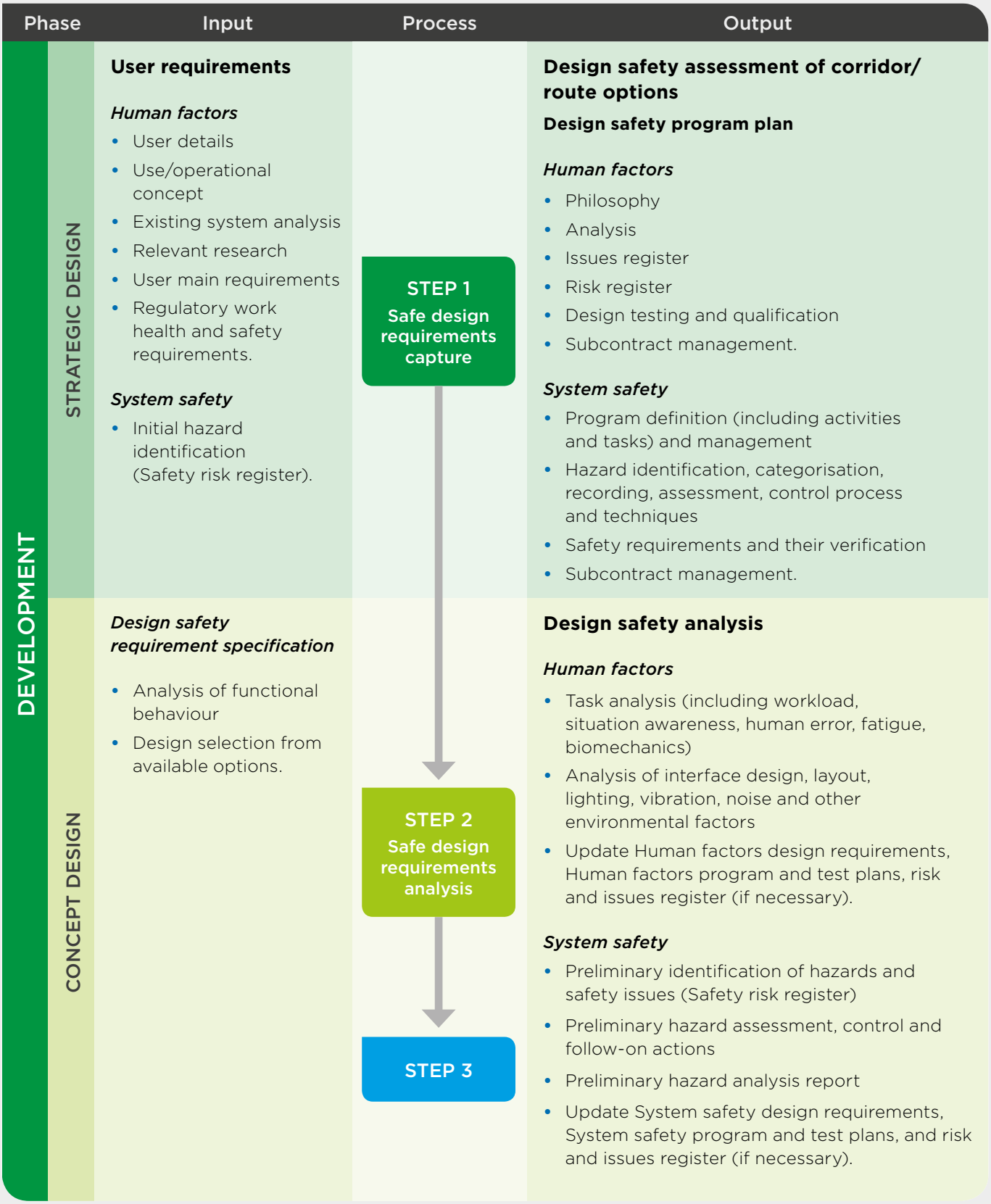
## 2. Design safety lifecycle process

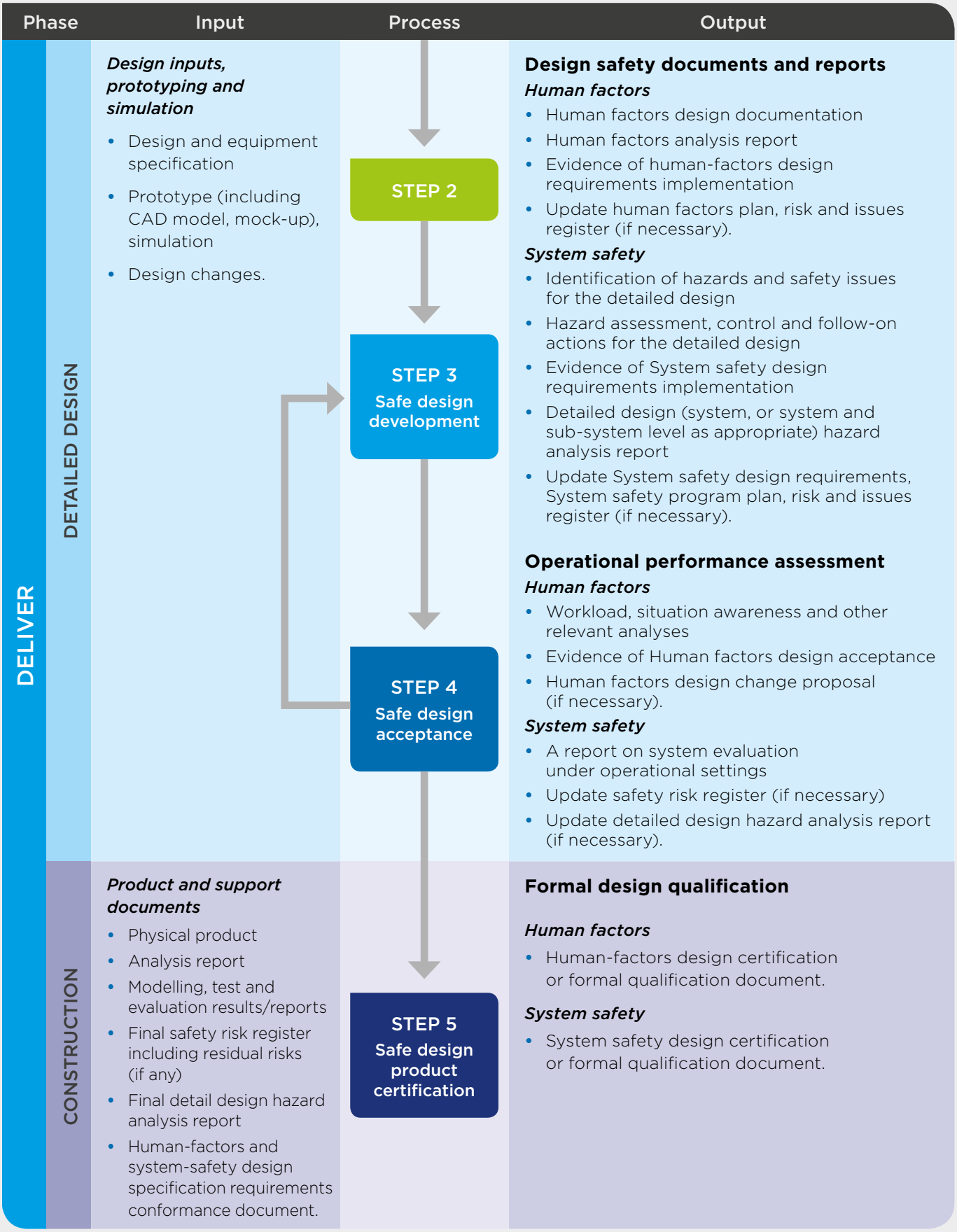
Diagram 1 represents design safety process steps to be carried out during phases of the infrastructure system design project. It shows inputs and outputs relevant to each of these steps.

This process must be tailored according to the nature of the project (size, design-phase and specific needs).

[1] To be developed in 2017

## Diagram 1: Design safety lifecycle process






**Note:**

- Steps 3 and 4 are part of the detailed design phase and are iterative processes
- This activity sequence is a general recommendation. Some design projects may require activities to be undertaken simultaneously or iteratively
- This process aligns with ISO 15288 Systems Lifecycle Processes.

## 2.1 Process activities

| PROCESS | ACTIVITIES INVOLVED |
|---|---|
| **STEP 1**<br>**Safe Design requirements capture** | **Design safety assessment of corridor/route options**<br>• System safety and human factors assessment is carried out as required during the evaluation and selection of corridor/route options.<br>***Human factors***<br>• Explicit and implicit user requirements (include constructor, operator, maintainer, demolisher as well as road users), including those mandated by WHS legislation, to be identified and captured in the human factors planning<br>• Human factors plan to determine the human factors standards, philosophy and methods to be used in the program<br>• Human factors' planning is aligned with overall process (eg risk management, analysis, design, testing and qualification) for the infrastructure design project lifecycle.<br>***System safety***<br>• Initial hazard identification (Safety risk register) is carried out<br>• Scope and objectives of overall system safety program are described<br>• Risk assessment process including hazard severity categories and likelihood being used are explained<br>• Hazard identification, recording, control and transfer methods are explained<br>• System safety design requirements for all phases of the system lifecycle (construction, use, maintenance, modification, and demolition) are described, including the process for their verification. |
| **STEP 2**<br>**Safe Design requirements analysis** | ***Human factors***<br>• An iterative process for determining requirements<br>• The Roads and Maritime functions and design requirements are reviewed to determine their human factors implications<br>• The requirements are used to develop human factors requirements and design option selections<br>• The requirements and their acceptance criteria must be agreed in advance with stakeholders to avoid subjective disagreement over test results<br>• Formation of a user group with valid operational experience and expertise to assist with capturing requirements, conducting analyses and making assessments.<br>***System safety***<br>• Initial safety risk register from Step 1 will be updated to include newly identified hazards related to the conceptual design<br>• Techniques including Fault Tree Analysis (FTA), Failure Mode Effect Analysis (FMEA) and Failure Mode, Effect, and Criticality Analysis (FMECA) could be used as appropriate for the hazard analysis<br>• Appropriate controls for these new hazards are identified and their implementation is formalised by adding relevant new safety design requirements into the *System-safety requirements specification*<br>• Preliminary hazard analysis report is produced describing above activities<br>• For significant safety critical design features, above hazard analysis report further provides additional arguments on why they are safe regardless of the design safety process being followed. |

| PROCESS | ACTIVITIES INVOLVED |
|---|---|
| **STEP 3**<br>**Safe Design development** | ***Human factors***<br>• Ensures the human factors design complies with the identified requirements, standards and philosophies<br>• Identifies any non-compliance and provides justification for any impact on operational performance and safety<br>• Design activities include rapid-prototyping, using Computer-Aided-Design (CAD) models or mock-up designs.<br>***System safety***<br>• Preliminary safety risk register from Step 2 will be updated to include newly identified hazards related to the detail design at system, or both system & sub-system level as appropriate<br>• Techniques including Fault Tree Analysis (FTA), Failure Mode Effect Analysis (FMEA) and Failure Mode, Effect, and Criticality Analysis (FMECA) could be used as appropriate for the hazard analysis<br>• Appropriate controls for these new hazards are identified and their implementation is formalised by adding relevant new safety design requirements into the *System safety requirements specification*<br>• Evidence of system safety design requirements implementation into the detailed design will be produced in the form of a test report<br>• Detailed hazard analysis report is produced describing above safety activities<br>• For significant safety critical design features, detailed hazard analysis report further provides additional arguments on why they are safe regardless of the design safety process being followed. |
| **STEP 4**<br>**Safe Design acceptance** | ***Human factors***<br>• Requires review and assessment of the system prototype or mock-up by internal and external users<br>• Meeting system requirements described in Step 2 is confirmed as acceptance criteria<br>• Non-compliance is resolved through design change, procedural change or formal acceptance of non-compliances<br>• Testing the system prototype or mock-up is conducted as applicable for design acceptance from a 'fit-for-purpose' perspective.<br>***System safety***<br>• Safety risk register including any residual safety risks is updated (if necessary)<br>• The detailed design hazard analysis report is updated to include safety related design changes (if any) as a result of this step. |
| **STEP 5**<br>**Safe Design product certification** | ***Human factors***<br>• Ensures the Roads and Maritime infrastructure has been constructed in accordance with human factors design specification requirements<br>• Represents system acceptance in service (from a human factors perspective).<br>***System safety***<br>• Ensures the Roads and Maritime infrastructure has been constructed in accordance with system safety design specification requirements<br>• Represents system acceptance in service (from a system safety perspective). |

### 2.2 Measures

Design safety acceptance criteria are agreed against specific design requirements.

### 2.3 Verification

Some design safety requirements are verified analytically. Other requirements are verified against acceptance criteria by user assessment or testing.

# Roles and responsibilities

| ROLE | RESPONSIBILITIES |
|---|---|
| **Process owner (PO)**<br>• Director (Chief Operating Officer), JMD | • Ensure the design safety lifecycle management process is deployed in Roads and Maritime design projects. |
| **Divisional Directors** | • Ensure the design safety lifecycle management process is integrated into the relevant Roads and Maritime business unit's design program plan. |
| • Project manager (PM)<br>• Design manager (DM) | • Implement the *Design safety program plan* in Roads and Maritime infrastructure system design projects<br>• Ensure the system users with operational experience or expertise are embedded into the design team throughout the design lifecycle. |
| **Design safety specialist (DSS)** | • To be determined. |

If Roads and Maritime outsources design and/or construction work, the contract should explicitly require the industry partner to undertake design safety activities to cover the intent of this framework.

# Definitions

| Term | Definition |
|---|---|
| **Human factors** | Issues such as human performance, error, workload, situation awareness, fatigue, physical layouts, geometry and environment of the workplace, system of work/task analysis, interface design (eg signage, markings, traffic lights, intelligent transport system), lighting, noise, vibration, biomechanics, ingress/egress, and associated safety and effectiveness aspects. |
| **Infrastructure system** | Roads and Maritime fixed infrastructure systems include:<br>• Hardware elements such as roads, bridges, tunnels, signage, markings, delineations, traffic light, intelligent transport, and smart motorway system's electronic hardware<br>• Software elements of the traffic lights, intelligent transport and smart motorway system's electronics. |

# References

## External references

| Title | Source | Type |
|---|---|---|
| *ISO 15288 Systems Lifecycle processes* | International Organization for Standardization<br>*www.iso.org* | ISO standard |

# Appendices

## A. OneRMS SMS requirements

| Design safety – lifecycle management | | |
|---|---|---|
| **DS1** | **Identify and document safe design requirements** | Roads and Maritime identifies potential infrastructure users and documents their safe design requirements for the infrastructure system design. Based on these requirements, a design safety program plan scopes the project activities.<br>*WHS Act* (sections 19 and 22) |
| **DS2** | **Analyse safe design requirements** | Roads and Maritime analyses the practicability of implementing the documented safe design requirements into the system design. Based on the analysis, a safe design specification for the infrastructure system is developed.<br>*WHS Act* (sections 19 and 22) |
| **DS3** | **Develop safe design** | Roads and Maritime develops a design prototype using the safe design specification.<br>*WHS Act* (sections 19 and 22) |
| **DS4** | **Evaluate safe design** | Roads and Maritime evaluates the design prototype under realistic operational conditions.<br>*WHS Act* (sections 19 and 22) |
| **DS5** | **Certify safe design** | Roads and Maritime confirms that the physical infrastructure system has been constructed in accordance with the safe design specification. It then submits all safe design analysis documents to support safe design certification.<br>*WHS Act* (sections 19 and 22) |

** These requirements ensure, so far as is reasonably practicable, that the infrastructure system is designed to be without risks to the health and safety of persons as required by the WHS Act.*

# Document control

| | |
|---|---|
| **Owner** | Human Factors Specialist |
| **Approval** | General Manager Work Health and Safety |
| **File name** | design-safety-lifecycle-management-framework.pdf |
| **Online location** | Home (*www.rms.nsw.gov.au*) → Safety → Work Health & Safety → OneRMS safety management system → OneRMS SMS manual, frameworks and requirements |
| **Objective ID** | A10232585 |
| **Publication No.** | RMS 17.076 |
| **Template** | Objective ID: A10508605<br>Objective label: WHS procedure template |

## Change history

| Issue | Date | Description of change |
|---|---|---|
| **1.0** | 22/03/17 | First issue |

## Feedback

Contact WHS Branch with feedback on this document at *onermssms@rms.nsw.gov.au*