# INTERIM ADVICE NOTE 191/16

# SAFETY GOVERNANCE FOR HIGHWAYS ENGLAND

**Summary**
This IAN provides a framework for safety governance on all Highways England activities. It takes cognisance of GD04: Standard for Safety Risk Assessment on the Strategic Road Network.

**Instructions for Use**
This document supersedes IAN 139/11 and IAN 151/11.

# 1.0 Introduction

## 1.1 Background

Highways England is responsible for the operation, maintenance and modernisation of the strategic road network. An important aspect of the work carried out by Highways England is the management of safety risk in an appropriate and cost effective manner. Safety risk can be defined as being the combination of the likelihood and the consequence of a specified hazard being realised. It is a measure of harm or loss associated with an activity. All schemes, projects, programmes, operational activities, policies and other initiatives undertaken by Highways England have to be implemented with an appropriate level of safety governance in order that safety risk is identified, mitigated and managed. These projects and activities include: maintenance, renewals, improvements and upgrades, major schemes, decommissioning, operational management and policy development. (Note: The terms projects and activities are used interchangeably in this document and are used to refer to all terms used above).

The purpose of this IAN is to provide guidance on the selection and implementation of an appropriate safety management system (SMS). The approach to decision making in relation to safety risk is defined within GD04/12: Standard for Safety Risk Assessment.

## 1.2 Scope

This IAN is intended to be read in conjunction with GD04/12 Standard for Safety Risk Assessment on the Strategic Road Network. This Standard sets out the approach which must be applied in all administrative and technical aspects when designing, constructing, operating and maintaining the strategic road network, where safety should be a consideration. The Standard sets out Highways England requirements for managing safety and as such it does not provide legal advice or guidance.

This IAN supports the safety governance and decision making process by setting out how an appropriate SMS is selected and implemented for all projects on the Strategic Road Network (SRN). The term ‘all projects’ includes any project which may impact an individual or groups’ exposure to safety risk. This may include projects which do not directly impact the SRN but have an impact on the way in which operations are carried out or the way in which technology is managed.

IAN 191/16 is relevant at all stages of a project lifecycle, and should be considered and, where appropriate, implemented for projects which include any interventions on the SRN. In addition, as a project moves through the lifecycle, the type of SMS implemented may need to change to adapt to the changing impacts of the project on safety risk.

All aspects of the approach detailed in this IAN are based on existing legislation and Highways England’s stated minimum requirements. Therefore, if any aspects of the safety risk management process described in this document are not met by service providers’ procedures or practice, this indicates a deficiency in the existing processes that must be addressed.

This IAN does not change requirements for the application of existing standards, the Construction (Design and Management) (CDM) Regulations 2015; relevant Health and Safety legislation; the Departures from Standards process; or Road Safety Audits. Following an SMS as set out in this IAN, however, may enhance the meeting of requirements of the aforementioned standards, legislation and processes.

There are four populations that must be taken into account when considering what is reasonably required to manage safety risk exposure. Populations are defined within GD04/12 (Table 1) and are broadly split into three groups:

1. 'Workers'
    a. People **directly** employed by Highways England and who work on the SRN
    b. People in a **contractual** relationship with Highways England

2. 'Users' (including road users, the police and emergency services)
3. 'Other Parties'

### 1.3 Use of this document

This document presents a recognised, tested methodology that is both comprehensive and efficient. It does not prescribe the only way of meeting the requirements for safety governance. Service providers must be able to demonstrate how their own processes and procedures satisfy the requirements. Adherence to the methodology described will help ensure that the necessary evidence is produced and readily available.

All projects must follow the Construction (Design and Management) Regulations 2015 (CDM 2015) and must be able to demonstrate that they have done so. It is not necessary to repeat any risk assessment activity carried out in following this guidance to comply with CDM (2015), neither is it necessary to repeat work carried out under CDM (2015) to comply with GD04/12.

### 1.4 Responsibility for application

It is the responsibility of the Highways England Project Manager to ensure that this guidance is applied, although elements of its application may be delegated to other parties, including Highways England's supply chain, as identified throughout this document.

Specified roles will also be required to undertake approvals at particular points of the SMS application. Roles and responsibilities are discussed further in section 4. In addition GD04/12 provides guidance on developing a Responsible, Accountable, Consulted and Informed (RACI) matrix (GD04/12 Chapter 7).

### 1.5 Document structure

This IAN is presented in two parts with supporting appendices (Part 3):

1) **Part 1** explains how projects should be categorised in order to determine the appropriate level of rigour for safety risk management.

2) **Part 2** explains the main stages of the safety risk management process, via the implementation of the safety activities that make up the SMS. This has three differing levels of appropriate rigour (Type A, B or C), depending on the outcome of the application of Part 1 of the framework.

# PART 1: SAFETY MANAGEMENT SYSTEM (SMS) SELECTION

## 2.0 Selecting the project SMS

The purpose of this section is to support Project Managers in the selection of the SMS type most appropriate to the project. The section explains how projects should be categorised in order to determine the appropriate level of rigour for safety risk management and therefore which SMS type is most appropriate.

### 2.1 Scope of SMS application

Generally, a single type of SMS will be selected for the whole project. However, in some cases, projects may identify a small number of discrete issues or locations that require a more rigorous approach to safety risk management compared with the majority of the project. This situation will require the project to adopt a 'mixed' approach to safety risk management, applying the less rigorous SMS to the majority of the project, but applying the more rigorous SMS to those specific issues or locations that need it.

### 2.2 Types of SMS

A key principle of safety governance is that an **appropriate level of rigour** is applied. This IAN defines three differing types of SMS, Type A, B or C, which apply differing levels of vigour to projects. Detailed information on the key features of each SMS type, and the projects to which each type is likely to be assigned, can be found within Appendix A. A summary is provided below:

1. **Type A SMS – Basic**
   A Type A (Basic) SMS is likely to include the following activities:

   - Completion of a simple hazard analysis to support the production of:
     - Safety plan
     - Combined safety and hazard log report

   The type of projects to which a Type A SMS is likely to apply include:

   - Projects / interventions that are routine, familiar and without operational implications[1]. As such, these will be largely satisfied by the application of existing standards and guidance.

2. **Type B SMS – Moderate**
   A Type B (Moderate) SMS is likely to include the following activities in addition to those undertaken for a Type A SMS:

   - More extensive risk assessment supporting the production of:
     - Safety plan
     - Hazard log
     - Combined safety and hazard log report
     - Combined operations product
     - Maintenance and repair strategy statement

   The type of projects to which a Type B SMS is likely to apply include:

[1] Operational implications can be defined as those aspects which require a change in the way groups or individuals ('Workers') work on the network or a change in the way road 'Users' are expected to behave.

- Projects / interventions that could have some significant operational impacts.
- Those which may lead to an increased level of stakeholder interest (specifically in terms of how safety will be addressed or managed).
- This will include the application of existing standards and guidance.

**3. Type C SMS – Complex**

A Type C (Complex) SMS is likely to include the following activities in addition to those undertaken for a Type A and B SMS:

- Comprehensive risk assessment documentation will be required, supporting the production of:
  - Safety plan
  - Hazard log
  - Combined safety and hazard log report
  - Combined Operations product
  - Maintenance and repair strategy statement.

The type of projects to which a Type C SMS is likely to apply include:

- Complex, infrequent projects / interventions which may have major implications for SRN
- This will include the application of existing standards and guidance.

## 2.3 SMS selection process

The process diagram in Figure 2-1 summarises the main steps involved in the SMS selection process, this must be followed to ensure that project features are assigned correctly. Each step is explained in more detail in the sections that follow.

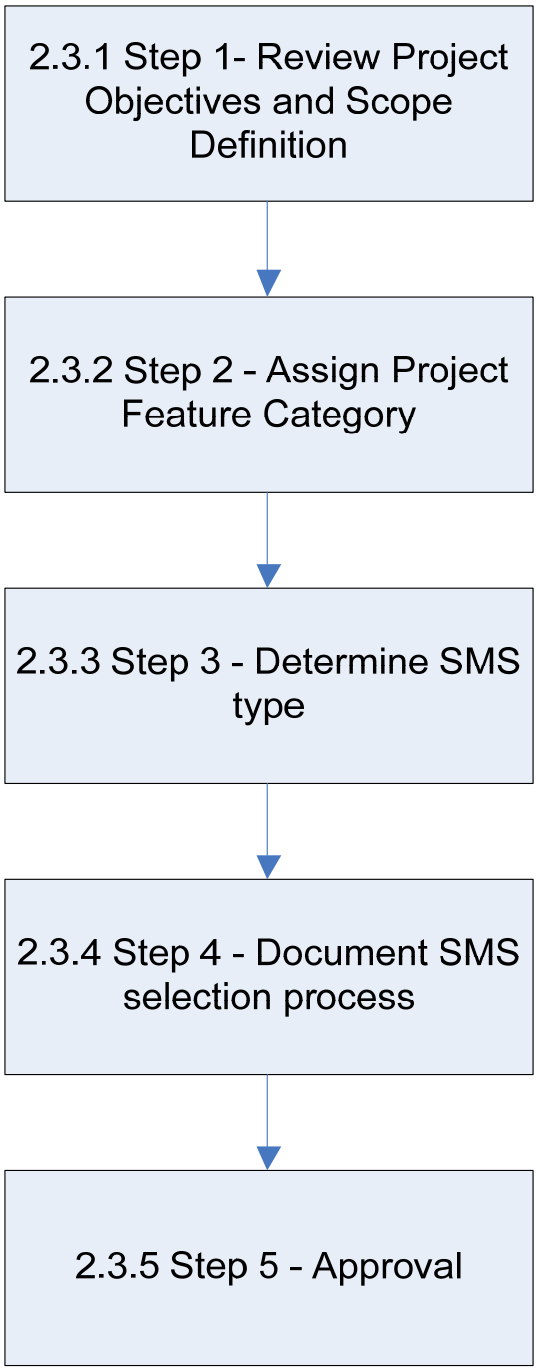



**Figure 2-1 - SMS selection process**

### 2.3.1 Step 1 - Review project objectives and scope

The first step should be to review the project scope (Client Scheme Requirements). The purpose of this step is to gain a thorough understanding of how the individual and composite features of the project work together to achieve the overall project outcomes. Developing this understanding will support the subsequent safety activities by enabling those responsible for undertaking the activities to understand how individual project features contribute towards the achievement of the overall project outcomes.

### 2.3.2 Step 2 - Assign project features

The purpose of step 2 is to review the features of the project and to assign each feature a category according the methodology set out within this section. There are two stages:

a) Review the features against which the project is characterised
b) Assign each of the features against a type (A, B, C)

***Stage a) – Review features***

Table 2-1 sets out the features against which the project is characterised:

**Table 2-1 Project Features and Descriptions**

| | Feature | Description |
|---|---|---|
| **1** | Stakeholder Interest[2] | *Quantity and/or impact of stakeholder groups, interest and resulting influence/impact* |
| **2** | Operational Experience | *Extent of experience to operate and maintain safely, and the location of that experience. Whole life impact* |
| **3** | Technology and/or Infrastructure | *Extent of technological innovation, criticality of application and implications for the level of safety risk* |
| **4** | Standards and Legislation | *Whether relevant standards exist; need for departures; need for changes to legislation; consideration of Highways England guidance* |
| **5** | Impact on organisation[3] | *Structure, responsibility, competency* |
| **6** | Project Scale | *Infrastructure affected and the extent of the roll-out* |

When reviewing Standards and Legislation (Table 2-1, feature 4) only those departures that have an impact on safety risk need be considered. Following this guidance does not affect or modify any existing departures process. Project safety risk assessment work, however, may be used to support the departure process.

***Stage b) - Assign features against a type***

The aim of this stage is to review each project feature and assign a category type (A, B or C).

A simple tool to assist in categorisation is provided in Table 2-2. Applicable characteristics of the project can be circled to establish the category of a project feature.

[2] A stakeholder can be defined as an individual, group or organisation that affects or can be affected by an organisation's actions or one which has an interest in a project or intervention.

[3] 'Organisation' refers primarily to Highways England but may also include those who are commonly referred to as Populations 1 and 2 within GD04/12

Some features within Table 2-2 are defined in terms of a number of sub features e.g. Standards and Legislation is defined in terms of four sub features:

1. Design covered by existing standards or approved codes of practice (ACOP)
2. Departures from standards
3. Changes to legislation
4. Highways England guidance

Where these individual sub-features are themselves different SMS types, it will be up to the project manager to decide the appropriate type for the feature overall. This decision will take account of the implications for the approach to safety risk management of choosing a higher or lower sub feature type.

Further guidance on project feature categorisation can be found in Appendix A. Any assumptions must be clearly stated and documented. As further information becomes available SMS selections shall be reviewed.

## Table 2-2 - Project features and SMS categories

| Feature | Sub Feature | Type A | Type B | Type C |
|---|---|---|---|---|
| **1. Stakeholder Interest** | | | | |
| | Number of stakeholders | Single or few | Several or Single or few | Many or Key or Several |
| | Impact | Limited | Limited or Significant | Limited or Significant or Major / critical |
| **2. Operational Experience** | | | | |
| | Extent | Widespread | Limited or Some | None in UK nor overseas |
| | Where | UK | UK or Overseas only | |
| **3. Technology and/or Infrastructure** | | | | |
| | Technology experience (consider degree of innovation and criticality of application) | Widespread | Used in different application or Applied in part | Not previously applied |
| | Level of safety risk that introduced technology affects | Low | Medium | High |
| **4. Standards and Legislation** | | | | |
| | Design covered by existing standards | All | Mostly | No or New standard |
| | Safety related departures from standard | None/No significant | Some/Few significant | Many Significant or Some Critical departures |
| | Changes to legislation | None | Minor changes only | Moderate or Significant |
| | Highways England Guidance (in the form of | Existing/not applicable | Relevant new guidance available | Major development in relevant guidance |
| **5. Impact on Organisation -** (consider structure, responsibility, competency, whole life impact) | | | | |
| | | No changes | Minor changes/responsibility transfer | Significant change or responsibility transfer |
| **6. Project Scale** | | | | |
| | Infrastructure affected | Single/small location | Major location/implications | Widespread/national implications |
| | Extent of roll-out | None/minimal | Moderate | National potential |

### 2.3.3 Step 3 - Determine SMS selection type

Once each of the project features have been identified and a category assigned to each of them, an overall SMS Type can be determined for the project. Table 2-3 provides guidance on how to determine the SMS type.

**Table 2-3 - Determining SMS Selection Type**

| Project Feature Classifications | SMS Type | Comments |
|---|---|---|
| All type A | Type A | Where all project features are classified as type A then the entire SMS will be of type A |
| All type B | Type B | Where all project features are classified as type B then the entire SMS will be of type B |
| All type C | Type C | Where all project features are classified as type C then the entire SMS will be of type C |
| 3 or more type B, remainder type A | Type B | Where three or more project features are classified as type B and the remainder are type A, then the entire SMS will be of type B |
| 3 or more type C | Type C | Where three or more project features are classified as type C then the entire SMS will be of type C |
| Equal distribution of categorisation across features | Type A/B | Where there is an equal distribution of features then the decision shall be governed by the relative importance of the categorisation, i.e. a decision may still be a type A with two type B features. In this instance then the overall decision type would be type A but the two features that were identified as type B would require a greater rigour of analysis assessment and evaluation. |
| | Type B/C | Where there is an equal distribution of features then the decision shall be governed by the relative importance of the categorisation, i.e. a decision may still be a type B with two type C features. In this instance then the overall decision type would be type B but the two features that were identified as type C would require a greater rigour of analysis assessment and evaluation. |

### 2.3.4 Step 4 - Document SMS selection process

The results of the SMS selection process should be documented in the safety plan. A template for the safety plan can be found on the MP Project Control Framework within the Product Matrix (Specification Requirements and Design) and on the Highways England Supply Chain portal.

### 2.3.5 Step 5 - Approval

The choice of SMS must be agreed in principle before work to implement the SMS begins. Formal approval of the SMS selection will be through approval of the safety plan. Guidance on approval is provided in Section 4.0.

# PART 2: IMPLEMENTATION OF THE SMS

## 3.0 Safety Management System Activities

### 3.1 SMS activities and project lifecycle

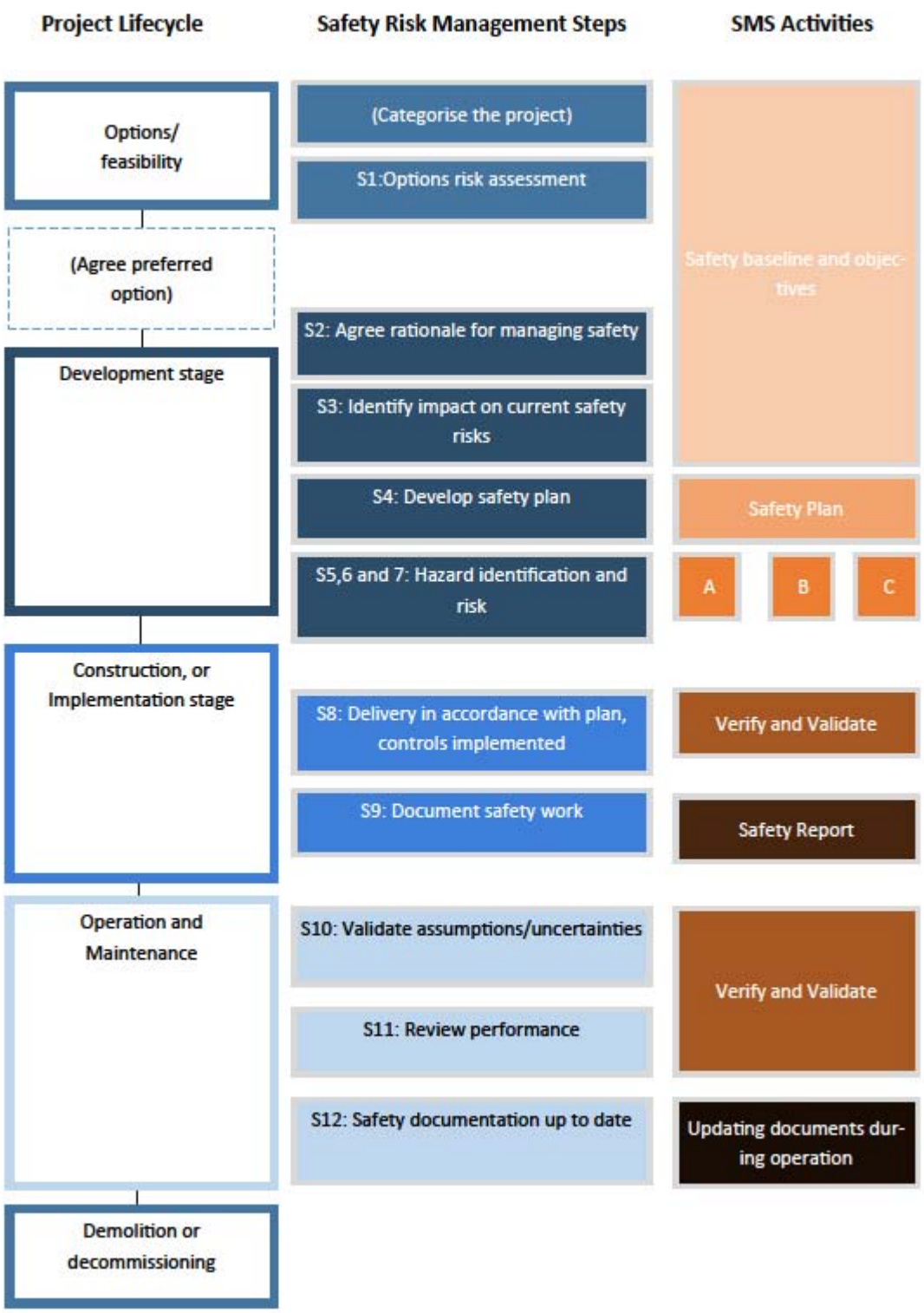
The purpose of this section is to provide guidance to Project Managers on the implementation of the chosen SMS and how the implementation stages relate to a projects lifecycle. This section explains the main stages of the safety risk management process and provides a summary of activities and responsibilities in respect of implementation.

The SMS is an ongoing and live system and as such should be regularly reviewed, reassessed and managed throughout the lifecycle of any project or intervention.

The appropriateness of the SMS type selected should also be regularly re-assessed whenever there is a significant change to the scope of the project, or to the detail of proposed operational regime, technology or infrastructure. Re-assessments of the SMS type should be documented in updates to the safety plan.

The general alignment of safety risk management, the SMS activities and a generic project lifecycle is shown in Figure 3-1.

**Figure 3-1—General guidance on the alignment of safety risk management and the project lifecycle**



## 3.2 Summary of SMS activities

Table 3-1 summarises the SMS activities for type A, B and C projects. Any omission must be justified to demonstrate that an appropriate level of safety risk management has been employed.

**Table 3-1 - Summary of SMS activities**

| Safety Risk Management Steps | SMS Activity | Description of activity | Reason for carrying out the activity |
|---|---|---|---|
| Categorise the Project<br>Step 1 – Options risk Assessment<br>Step 2 – Agree Rationale<br>Step 3 – Identify impact | Safety baseline & objectives | Document a suitable baseline for intervention.<br>Document objectives to cover relevant populations and align with wider Highways England safety and risk objectives.<br>(Guidance on safety baselines and objectives can be sought from the Client Scheme Requirements.) | Allow the effect of the intervention to be measured. A safety baseline is required to measure the achievement of the safety objective.<br>Have a clear understanding of the rationale to be pursued for managing safety for the different populations affected by the intervention. |
| Step 4 – Develop safety plan | Safety plan | Document a clear plan of how safety risk will be managed for all populations at project level throughout the project lifecycle.<br>Establish roles and responsibilities by using a RACI matrix (detailed in GD04/12).<br>Define the specific safety risk activities that will be undertaken for the project. | Supports the planning of safety activities and demonstrates that a defined SMS approach is being used.<br>Provides a means of communicating to and educating stakeholders as to how the project will achieve its safety objectives. |
| Step 5,6,&7 Hazard identification and risk assessment | Type A project - Risk assessment | Identify and document potential hazards associated with the project to all populations. Conduct safety risk assessment as reasonably required.<br>The project must also record details of any residual risks, and provide clear guidance on how these will be managed / monitored into the future. | Supports the identification and documentation of the hazards that will affect the project; enabling them to be appropriately safety risk assessed and subsequently mitigated.<br>The project must ensure any residual risks are handed over to the appropriate owner within Highways England for ongoing management. |
| | Type B project - Risk assessment | As above, and conduct additional, appropriate safety risk assessments as reasonably required, including use of a hazard log.<br>Projects must consider use of sensitivity analysis. | As above. The hazard log provides additional detail and rigour to the risk assessments and ensures that project options are informed by risk assessment.<br>Sensitivity analysis on risk scores will help focus design resources on areas where significant safety improvements are required. |

| Safety Risk Management Steps | SMS Activity | Description of activity | Reason for carrying out the activity |
|---|---|---|---|
| | Type C project - Risk assessment | As above, and conduct additional hazard analysis and appropriate safety risk assessment for all populations as reasonably required, which may include:<br>• Preliminary hazard analysis (PHA)<br>• System hazard analysis (SHA)<br>• Sub-system hazard analysis (SSHA)<br>• Interface hazard analysis (IHA)<br>• Operation and support hazard analysis (OSHA)<br>Further detail on Type C Risk Assessments can be found in Appendix E. | Supports the identification of hazards arising from various sources and interfaces during the project, enabling the project to be thoroughly risk assessed and subsequent mitigations proposed. The management of these hazards will be consolidated in a hazard log. |
| Step 8 – ensure delivery as per plan<br>Step 10 – validate assumptions<br>Step 11 – Review performance | Verification & validation | Verify that the project has implemented any identified safety requirements and ensure that all planned safety activities have been adequately undertaken in accordance with GD04/12.<br>Validate assumptions and meeting safety objectives. This will require post operational monitoring.<br>If any activities have not been completed, or have been completed but not in accordance with the safety plan, then this situation will be reported to the Highways England Project Manager. Mitigation measures will be developed, implemented and recorded in the combined safety and hazard log report (and safety plan as necessary). | To demonstrate that the project has done what it set out in the safety plan.<br>Validate that the project design satisfies its safety objectives.<br>It is important to make it clear what has been done to mitigate issues where activities have not been completed as planned, or outcomes are not as expected. |
| Step 9 – document combined safety and hazard log report | Combined safety and hazard log report | Document all project SMS activities undertaken. Include evidence showing that the project has developed appropriate safety objectives and demonstrate how these objectives have been achieved. | To demonstrate that the appropriate level of safety management has been undertaken to assess the expected safety performance.<br>For all Highways England projects the term ‘combined safety and hazard log report’ is used to refer to the document that is produced at the end of the SMS, summarising the evidence showing that the safety objective has been achieved. The term ‘Safety Case’ has a legal definition in particular industries. By adopting the term ‘combined safety and hazard log report’, flexibility is available for the content of the document and confusion with the existing term is avoided. |
| Step 12 – Keep safety documentation up to date | Updating safety documentation during operation | Update safety documentation to reflect any changes made once the project has commenced operation. | Maintains documentation as a record of project status and records ongoing achievement of safety objectives.<br>This activity demonstrates that the project still meets all of the necessary safety requirements and that appropriate safety risk management of the project is continuing during operation. |

The templates for the safety plan and combined safety and hazard log report can be found on the MP Project Control Framework within the Product Matrix (Specification Requirements and Design) and on the Highways England Supply Chain portal.

An indicative list of existing risk assessment tools and methodologies is provided in Appendix C and Appendix D.

## 4.0 Project safety ownership, approval and acceptance arrangements

Throughout the lifecycle of a project, ownership and accountabilities in relation to the SMS should be clearly identified and documented. Ownership is likely to transfer during the whole life cycle of a project or activity. When this occurs, responsibility for continuing to apply the appropriate approach to project safety risk management also transfers to the new owner. GD04/12 provides guidance on the roles, responsibilities and competence in relation to SMS and provides guidance on the development of a Responsible, Accountable, Consulted and Informed (RACI) matrix. Table 5 and 6 within GD04/12 also provide guidance on definitions and an example of RACI roles through the project lifecycle.

## 4.1 Acceptance and approval requirements

All project SMS deliverables must be formally accepted and approved by the relevant parts of Highways England.

- SMS deliverables require consultation before acceptance and approval can take place. This is required to gain an understanding of whole life considerations and agreement from across Highways England. This will be a project specific consideration.
    - All projects should define the roles that must be consulted to enhance and support the acceptance and approval process.

- Acceptance and approval shall be undertaken by competent persons (refer to GD04/12).
- Acceptance and approval shall be appropriately recorded (see Appendix B).
- An acceptance and approval process shall also apply to any changes introduced to project safety documentation after operation has commenced, and this shall be identified and documented.

## 4.2 Acceptance and approval roles

### 4.2.1 Type A SMS

Safety risk decisions will be reviewed and agreed in writing by the Project Team and Highways England Project Manager.

### 4.2.2 Type B SMS

Safety risk decisions will be referred to the Project Safety Control Review Group (PSCRG). The PSCRG (with the authority of the senior managers who ultimately sign off the safety products) will decide whether or not to endorse the recommendation(s) or will comment on the safety implications. This will be documented in the minutes of the PSCRG.
Type B issues will be monitored by the National Safety Control Review Group (NSCRG) and may be raised where an issue of consistency across schemes arises.

**Major Projects Directorate (MPD) Smart Motorways (SM)**
At present SM all lane running projects are likely to be assessed as requiring a type B SMS.

### 4.2.3 Type C SMS

Decisions relating to a type C issue shall be referred to the NSCRG. The NSCRG will consider the issue, together with the recommendation and provide their response to the Project Team. This must be documented.

Further information on approval roles can be found in Appendix B.

## 4.3 Consultation

Consultation should include all parties involved in design, construction, operation, maintenance and safety decision-making.

**Type A safety risk decisions:**
The following roles are consulted (refer to GD04/12 Figure 9):

1. Specialist Technical / Coordinator in the field impacted upon by the safety risk decision
2. Specialist Technical / Coordinator of general safety related good practice and current legislative requirements.

**Type B safety risk decisions:**
The following roles are also consulted:

1. Safety specialist / Team Leaders in safety(refer to GD04/12 Figure 9)
    a. The Project Safety Control Review Group (PSCRG). Detailed requirements for the formation of this group are described within the document: 'NSCRG and PSCRG Remit for Organisation and Governance' (CHE 375/16).

**Type C safety risk decisions:**
The following roles are also consulted:

1. Professional Roles (refer to GD04/12 Figure 9)

In addition to the above, the NSCRG must be consulted.

## 5. Handover and updating safety documentation during operation

### 5.1 Objective

Safety documentation should be kept up to date and the ownership regularly reviewed throughout the lifecycle of the project. Doing this enables safety related changes and decisions to be documented during operation to show safety objectives continue to be met.

### 5.2 Requirements

The following safety documentation should be updated throughout project operation:

| | Type A SMS | Type B SMS | Type C SMS |
|---|---|---|---|
| Safety Plan | ✓ | ✓ | ✓ |
| Combined Safety and Hazard Log Report | ✓ | ✓ | ✓ |
| Hazard Log | | ✓ | ✓ |
| Combined Operations Product | | ✓ | ✓ |
| Maintenance & Repair Strategy Statement | | ✓ | ✓ |

The above list is indicative and not exhaustive, as other safety documentation may also require updating.

### 5.3 Triggers to update documentation subsequent to commencement of operation

1. **Identification and implementation of new functionality**. Either a change to existing or introduction of new functionality may be required. This may include a change in the way the scheme or technology operates which results in a change in the behaviour required by road users or those involved in the operation of the scheme. These changes will need to be subject to hazard analysis and reflected in the relevant safety documentation.

2. **Identification of new hazards**

    - It is possible that new hazards may be identified that are not captured within the project hazard log. Details of any new hazard must be communicated immediately to and discussed with the Safety Risk & Governance Team.

    - Any changes to assumptions or risk calculations need to be assessed for impact on the safety objectives and documented within the hazard log. A hazard log change record will need to be maintained.

3. **Organisational and governance changes.** Any organisational and governance changes that affect safety need to be captured in the safety plan and the combined safety and hazard log report.

4. **Transfer of safety responsibility**. When a transfer in ownership of project safety work occurs, the combined safety and hazard log report must be updated to reflect where safety responsibility will be held.

5. **Validation of meeting project safety objectives**. This will generally occur prior to a project being handed over into business as usual (as it requires a long enough period of operation to gather evidence to demonstrate likely delivery of the safety objectives). The safety documentation will be updated once this validation has been achieved.

## 6.0 References

### 6.1 Normative

Construction Design and Management Regulations 2015
Health and Safety At Work etc Act 1974
(DMRB) GD04/12: Standard for Safety Risk on the Strategic Road Network

### 6.2 Informative

Cost Benefit Analysis (COBA) manual
Managing the accidental obstruction of the railway by road vehicles

WebTAG
Transport Statistics Great Britain
Reducing Risks Protecting People (R2P2)
Design Manual for Roads and Bridges
Highways Act 1980

Road Traffic Act 1988

Aiming for Zero

Information for Managing Safety on the Highways Agency Network (IMSHAN)

Management Arrangements for Health and Safety

## 7.0 Abbreviations

| Abbreviation | Definition |
|---|---|
| ACOP | Approved Codes Of Practice |
| CDM (2015) | Construction Design and Management Regulations 2015 |
| DMRB | Design Manual for Roads and Bridges |
| FMEA | Failure modes and effects analysis |
| FWI | Fatality weighted index |
| GD04 | DMRB GD04/12 Standard for Safety Risk Assessment on the Strategic Road Network |
| GSN | Goal structured notation |
| IAN | Interim advice note |
| IHA | Interface hazard analysis |
| IMSHAN | Information for Managing Safety on the Highways Agency Network |
| NSCRG | National Safety Control Review Group |
| OSHA | Operation and support hazard analysis |
| PCF | Project control framework |
| PHA | Preliminary hazard analysis |
| PSCRG | Project Safety Control Review Group |
| SHA | System hazard analysis |
| SMS | Safety management system |
| SRN | Strategic Road Network |
| SSHA | Sub-system hazard analysis |
| TM | Traffic Management |

## 8.0 Glossary of frequently used terms

| Term | Explanation |
|---|---|
| Agency | The Highways Agency (now Highways England) |
| Hazard | A source of potential harm. |
| Hazard analysis | The process by which potential hazards and accident sequences relevant to a project are analysed. |
| Hazard identification | Formal process by which hazards are identified. |
| Interface hazard analysis | A type of hazard analysis that focuses on both equipment and organisational interfaces. |
| Operation and support hazard analysis | A type of hazard analysis that focuses on the processes and procedures associated with the project. |
| Preliminary hazard analysis | A type of hazard analysis that focuses on hazards that will affect the project, based on the interaction of the project and its environment |
| Project Director (Consultant) | Person responsible for the team delivering the project, on behalf of an organisation, in partnership with Highways England. |
| Project Executor | Person or organisation executing the project. |
| Project feature | Property of the project that can be expected to affect safety management requirements. |
| Project lifecycle | The series of stages that any project goes through including: options stage; development; construction/implementation; operation; demolition. |
| Project Manager | Person representing Highways England interests on the project and to whom the Project Director/Consultant reports. |
| Project safety risk management | The process of managing safety risks associated with projects. |
| Project team | The group responsible for executing the project. |
| Qualitative | An expression in terms of a description of characteristics rather than an exact numerical measurement. |
| Quantitative | An expression using numerical values. |
| RACI matrix | A tool that breaks down roles and responsibilities in relation to a process or activity. RACI stands for Responsible, Accountable, Consulted, Informed. |
| Risk | The combination of the likelihood and consequence of a specified hazard being realised. |
| Risk analysis | Systematic process for understanding the nature of, and estimating the level of risk. |
| Risk assessment | The overall process of risk identification, risk analysis and risk evaluation. |
| Risk evaluation | Process of comparing the level of risk against risk criteria. |
| Risk management | The overall process of risk assessment, plus processes for assigning ownership of risks, taking actions to control them and then monitoring and reviewing progress. |
| Safety baseline | Level of safety against which the project Safety Objectives are set and measured. |
| SMS activities | Activities that comprise the project SMS, fulfilled to ensure compliance with GD04/12. |
| Safety management system | A system that ensures compliance with GD04/12 and appropriate consideration of safety for all Highways England projects. Also outputs products that align with the HA PCF process. |
| Safety objective | What the project expects to achieve in terms of safety. |

| Term | Explanation |
|---|---|
| Sub-system hazard analysis | A type of hazard analysis that focuses on hazards that can arise from the detailed design of the project system, by systematically examining the design of each sub-system. |
| System | Any collection of equipment, people and procedures that work together to achieve a common goal. This may include:<br>1. The carriageway and associated infrastructure (lighting, barriers, markings, drainage, etc.)<br>2. The telematics equipment<br>3. People involved in operations and maintenance, and the procedures by which they work |
| System hazard analysis | A type of hazard analysis that focuses on hazards that can arise from the project system design. |
| TM worker | Person whose job it is to install or remove traffic management. |
| Type A project feature | A project feature requiring a basic level of safety management to be applied. |
| Type B project feature | A project feature requiring a moderate level of safety management to be applied. |
| Type C project feature | A project feature requiring rigorous safety management to be applied. |
| Users | Defined in GD04/12. |
| Validation | Safety risk management activity that checks that any significant design assumptions or uncertainties are validated. Where appropriate, it also uses performance data to demonstrate actual safety performance. |
| Verification | Safety risk management activity that checks that any activities or measures necessary for the project to fulfil its safety objectives are completed. |
| Workers | Defined in GD04/12. |

# PART 3 – APPENDICES

## APPENDIX A: Guidance on project feature categorisation

### A1.0 Indicative characteristics of an SMS

Once each of the project features has been categorised the appropriate SMS can be selected. Indicative levels of safety risk management for each SMS category are given below.

**Type A** SMS applies to projects that:

- Highways England has extensive experience of delivering and operating.
- Are uncontroversial and fall completely, or almost completely, within the scope of existing standards, legislation, practice and procedures (a small number of minor safety-related departures would be allowed in this instance).
- Have limited impact on the network as a whole.
- Meet Highways England's 'usual' requirements for approvals and documentation.

**Type B** SMS applies to projects with:

- Some innovation or uncertainty in terms of how the safety risk is managed or affected.
- An increased level of stakeholder interest (specifically in terms of how safety will be addressed or affected).
- Some aspects falling outside of existing standards, legislation, practice or procedures (and therefore requiring more significant safety risk related departures)
- Some implications for competence or roles and responsibilities within Highways England or the suppliers.
- Moderate implications for the overall Highways England network.

For projects such as those described above to be categorised as type B, they would need to have some track record of successful implementation elsewhere e.g. either elsewhere in the world, or elsewhere in the UK, but under different circumstances.
Other examples of type B projects would be those that involve established techniques or designs, but where circumstances result in local combinations of relatively significant safety-related departures that required more extensive risk assessment in order to ensure that residual risk levels are tolerable.

**Type C** SMS applies to projects that:

- Are delivering something completely new that has never been done before (either in the UK or Overseas).
- Are likely to have significant stakeholder interest in safety terms.
- Are, for the most part, not covered by existing standards, practice or procedures.
- May require new legislation or significant amendments to existing legislation.
- Will require many significant safety risk related departures, either in terms of numbers of departures or in terms of the extent of the departures.
- Involve significant changes to roles and responsibilities and required competences within Highways England or its Supply Chain.
- Have widespread or national implications for the Highways England network.

### A2.0 Assigning project features

Table A-1 provides guidance on the indicators for categorising the defined project features outlined in Section 4.0. This guidance will assist in producing an overall SMS type for the project, when used in conjunction with the content of Section 4.0.

**Table A-1: Project features and SMS type indicators**

| Project Feature | Feature Questions to be Considered | Feature Requirement | Indicators for Selecting Type A, B or C |
|---|---|---|---|
| **1. Stakeholder Interest**<br>The degree of interest that an individual or group have in the success of the project. Stakeholders can be both internal and external | • Which groups/individuals can be considered as stakeholders?<br>• How many stakeholders are there?<br>• What kind of influence does each of the stakeholders have?<br>• Which stakeholders have the most influence?<br>• Are there any key stakeholders on which project 'go ahead' depends? | The projects needs to demonstrate to stakeholders that safety issues, as they perceive them, are well understood and will be fully addressed | **Type A**<br>Projects where few stakeholders are expected to have a significant impact (i.e. none of whom are 'key') and there are no significant issues or strongly opposing views to be addressed.<br>**Type B**<br>Projects that have only a single or a few stakeholders but their impact may be significant. Alternatively it will represent a project that has several stakeholders but the amount or types of issues involved are limited.<br>**Type C**<br>A project where stakeholder impact will be significant, either owing to the large number involved, the impact of the project on key stakeholders, or conflicting needs arising that will need to be addressed. |
| **2. Operational Experience**<br>The degree of knowledge available from operating or running a similar project | • Is there operational experience available from previous projects?<br>• How similar is the operating environment of the previous project?<br>• Is the experience local to this project or to somewhere else in the UK?<br>• If there is no relevant UK experience, is there relevant experience overseas? | The projects needs to demonstrate that the risks associated with the operation that will be introduced are sufficiently understood and mitigated | **Type A**<br>Projects for which there is significant operational experience and will therefore be less likely to require major safety studies or risk assessments. Previous safety studies should be available, and some project features might have been codified in a standard.<br>**Type B**<br>Projects for which there is either limited operational experience in the UK, or some overseas which is deemed sufficiently similar to the project in question to be relevant. In this case, some additional safety work is likely to be required. There may also be local and site specific issues to take into account that could affect the relevance of the available operational experience.<br>**Type C**<br>Projects for which there is no previous experience. These projects will need a more robust SMS to support the more detailed safety analysis work that will be required. |

| Project Feature | Feature Questions to be Considered | Feature Requirement | Indicators for Selecting Type A, B or C |
|---|---|---|---|
| **3. Technology**<br>Measure of technical novelty the project brings | • Has the technology associated with the project been applied elsewhere?<br>• If so, how was the technology applied elsewhere?<br>• How effective has the technology been?<br>• Are previous risk assessments associated with the technology available?<br>• Will there be any modifications to the technology for the proposed project that have not yet been applied on previous projects? | Where technology novel or new to the highway is used, its operation must be understood and appropriately tested to ensure that risk levels are not adversely affected | **Type A**<br>A project where the technology involved is currently in widespread use or limited/no technology will be introduced by the project. Re-examination is unlikely to be needed.<br>**Type B**<br>There may be some experience of the technology, but from use in either another application or perhaps from overseas in which case some additional work may be required to demonstrate that safety can be assured for the intended application.<br>**Type C**<br>Those that will use a new technology for which there is no previous experience in the UK or elsewhere and extensive safety assessments are likely to be required. |

| Project Feature | Feature Questions to be Considered | Feature Requirement | Indicators for Selecting Type A, B or C |
|---|---|---|---|
| **4. Standards and Legislation**<br>Consideration as to the applicability of current standards and legislation and to whether new standards or changes in legislation will be required | • Is the project covered by existing standards?<br>• Will the project require significant safety related departures from existing standards?<br>• In order to implement the project will a change need to be made to existing legislation? What is the extent of this change?<br>• What legislation (if any) imposes additional safety related duties on the project?<br>• Has legislation affecting this project changed?<br>• Have any safety related projects standards that affect this project changed?<br>• Is there any available Highways England guidance on the project? | A project needs to demonstrate that the interventions it will introduce and the means by which it will deliver these interventions are covered by standards and legislation | **Type A**<br>Work is substantially or entirely covered by existing standards. No changes in legislation will be required and there will be no safety related departures from standards.<br>**Type B**<br>The design will be largely or entirely covered by existing standards however there may be some minor changes to existing legislation required and/or a few significant safety related departures may be needed.<br>**Type C**<br>Represent more novel projects that are not covered by existing standards. Any project that does not conform to existing legislation, or may require new legislation, will be classified as 'type C', as it is likely that a strong case for safety would need to be made to support a change to legislation. It will also be needed when new legislation is created that imposes additional safety related duties on a project which did not previously exist.<br>While the number of safety departures from standard may affect the characterisation the nature and type of a given departure is the most important element in determining characterisation. A large number of safety departures that can be addressed straightforwardly will have less impact on feature type than a single safety departure that requires a detailed risk assessment to support it. |

| Project Feature | Feature Questions to be Considered | Feature Requirement | Indicators for Selecting Type A, B or C |
|---|---|---|---|
| **5. Impact on the Organisation**<br>The effect that the project will have on the current Highways England organisational arrangements and in particular and changes in roles and responsibilities. | Will the project have an impact on the organisation of Highways England operations?<br><br>Will the project have an impact on the maintenance activities carried out on affected infrastructure?<br><br>Will the project require changes to organisational structure or changes to the safety organisation?<br><br>Will any new responsibilities be required?<br><br>What are the competency requirements for the project?<br><br>Are they currently covered?<br><br>Will new staff need to be recruited?<br><br>Will the project have a different impact on the organisation as it progresses through the life cycle?<br><br>What will these changes be? | A project needs to demonstrate that the impact of the project on the organisation are fully understood and accounted for.<br><br>The use of a RACI matrix, as outlined in Chapter 7 of GD04/12, will aid in this process. | **Type A**<br><br>Projects and they have no impact on the organisation of Highways England.<br><br>**Type B**<br><br>Projects where minor organisational changes will occur. However, new roles and responsibilities and organisational arrangements would need to be defined, as would competency, training requirements, recruitment needs and the way that responsibility would be transferred when the new roles are introduced.<br><br>**Type C**<br><br>Projects requiring major changes in organisational arrangements and more particularly a change in core safety roles and responsibilities. Demonstration that they will deliver an adequate safety performance will also be required. |

| Project Feature | Feature Questions to be Considered | Feature Requirement | Indicators for Selecting Type A, B or C |
|---|---|---|---|
| **6. Project Scale**<br>Consideration of the size of the project to be implemented | What infrastructure will be affected by project implementation?<br><br>Will the project have a local/regional/national impact?<br><br>Is the project a Pilot or Trial?<br><br>Does the project involve the wider roll-out of a previous Pilot/Trial/local project?<br><br>Is there potential for wider roll-out of the project? | A project needs to ensure that adequate safety measures are taken in proportion to the scale of the project. | **Type A**<br><br>Projects that involve either a single or limited number of locations, or where the affected infrastructure/interventions are limited in nature.<br><br>**Type B**<br><br>For projects which are concerned with larger, major locations with larger implications. There will only be a moderate scale roll-out.<br><br>**Type C**<br><br>A large project is likely to affect a large number of people and will therefore be associated with a large potential impact on risk. For these large projects, more comprehensive risk analysis may be justified. |

## A3.0 Additional consideration for categorising project features

### Categorising stakeholder interest

When categorising the type of stakeholder interest:

1. Consider both internal (Highways England or other Project Team) and external stakeholders (e.g. emergency services, local authorities, other roads groups such as the AA or RAC, members of the public living nearby)

### Categorising operational experience

When categorising the type of operational experience:
1. Categorise the project to reflect Highways England's corporate experience - not just that of the Project Team
2. Consider if there are any local issues that may affect the relevance of previous experience

### Categorising technology and/or infrastructure

When categorising the type of technology and/or infrastructure:

1. Consider the level of novelty or innovation that the project will introduce and what level of safety risk this is managing, or will potentially introduce
2. As with operational experience, consider Highways England's corporate experience - not just that of the Project Team
3. Consider if there are any local issues that may require modifications to the technology or infrastructure that have not been applied on previous projects

### Categorising standards and legislation

When categorising the type of standards and legislation (and particularly the feature concerned with safety-related departures from standards) 'significant' departures are likely to include those that:

1. Result in a considerable increase in safety risk to one population, potentially bringing the level of risk for that group close to the intolerable limit
2. Potentially affect a number of different populations, resulting in a material increase in the level of collective safety risk
3. Are based predominantly on judgement and risk assessment (e.g. to predict the impact of the departure on road user behaviour), resulting in a relatively uncertain assessment of the impact on safety risk

Less 'significant' departures are likely to include those that are concerned with technical solutions that are:

1. Very closely equivalent to those present in current standards, but that may not yet be documented or codified (e.g. with a revised version of the current standard currently in development), or
2. Strongly based in ongoing research, or reflecting the outputs of recent relevant research studies

‘Critical’ departures will be those without which, the entire project becomes impossible.

### Categorising impact on the organisation

When categorising the type of impact on the organisation:

1. Consider whether the project will require any change to the current organisation, roles and responsibilities or competence of Highways England
2. Will the project require new staff to be recruited?

### Categorising project scale

When categorising the type of project scale:

1. Consider the extent of Highways England network, the number of road users affected by the project and value of project
2. Take care to differentiate between pilots and trials that might only affect a relatively localised part of the network and any implementation projects that might follow; only categorise the project for the true extent of the network that it will directly affect

## APPENDIX B: Approvals

Type A safety management requires no more than a 'business as usual' approach as long as it can be demonstrated that this satisfies all aspects of legal compliance. Consequently, Type A approvals will not require any additional effort beyond Highways England Project Manager/Senior Responsible Owner and Senior Users existing involvement in decision making and approvals.

Responsibility for final approvals for Type B *safety issues* lies with the Asset Operational Development Group Manager. The decision must be informed by discussion with a project stakeholder group that includes PSCRG members and representatives of end users affected by the activity. Type B safety issues should be approved on a case by case basis.

Type C decisions will require consideration by the NSCRG who will accept or reject the proposed solution. Referrals to NSCRG will be informed by documented discussion with the relevant subject matter experts. Type C safety issues must be approved on a case by case basis.

## APPENDIX C: Examples of risk assessment tools and methodologies

Examples of existing Agency risk assessment tools and methodologies are:

1. The Safety Risk Model (SRM) and annual Information for Managing Safety on the Highways England Network (IMSHEN) Reports managed by Highways England's Safety Risk and Governance Team

2. Regional Intelligence Unit reports

3. Design Manual for Roads and Bridges (DMRB) HD 22/02 "Managing Geotechnical Risk"

4. Design Manual for Roads and Bridges (DMRB) HD 41/03 "Maintenance of Highway Geotechnical Assets"

5. *Road Restraints Risk Assessment Process* (RRRAP) part of Design Manual for Roads and Bridges (DMRB) TD19/06 "Requirements for Road Restraint Systems"

6. *Passively Safe Gantry Risk Model (PSGRM) part of IAN 85/06 "Design of Passively Safe Portal Signal Gantries"*

7. Design Manual for Roads and Bridges (DMRB) BD 78/99 "Design of Road Tunnels"

8. Area Management Memorandum (AMM) 130/10 "Priority Drainage Assets"

9. Area Management Memorandum (AMM) 129/10 'Lane restrictions at barrier repairs'

10. Area Management Memorandum (AMM) 107/09 'Road Safety Data Types and their Uses'

11. Generic ALR hazard log spreadsheet

12. MPI-19-112013, Road Worker Safety Assessment Tool

13. IAN142/11, Temporary Barrier Decision Tool (TBDT)

Acknowledging that risk assessment tools and methodologies are increasing with time, this list is not exhaustive; however it provides an indication of the types of documentation available.

## APPENDIX D: Methodologies for quantifying project safety risk

### D1.0 Overview

This section outlines some of the different risk assessment methodologies that can be used as a means of quantifying the risks associated with a particular project. In choosing or deriving a risk assessment methodology there are a number of requirements to take into account, including:

1. Proportionate analysis based on the Type of SMS applicable to the project.
2. The methodology should be consistent with the way any safety objectives are expressed.

### D2.0 Risk assessment techniques

This section lists the majority of the most frequently used risk assessment techniques for quantifying safety risk. The information given is intended to provide awareness that such techniques exist but not to teach their application. For this level of instruction please refer to other sources of information.

1. **Quantitative risk assessment.** As defined within Annex A of GD04/12.

2. **Semi-Quantitative risk assessment.** As defined within Annex A of GD04/12.

4. **HAZard and OPerability study (HAZOP).** Detailed within the guidance on undertaking an OSHA (7.10.10)

5. **Fault Tree Analysis (FTA).** This is a top down analysis approach, which begins with a high level event such as a hazard or accident, and then breaks it down into lower level causes until the required level of detail is reached. Combinations of events are joined by logical ‘or’ or ‘and’ operators, helping to provide an understanding as to what the minimum set of events is that can lead to a hazard or accident.

6. **Event Tree Analysis (ETA).** This involves a bottom up analysis approach that begins with a base event and then explores the consequences of this event. It is particularly appropriate for determining the range of consequences that may arise from a hazard and the most likely of these consequences. Once the base event has occurred, each possible outcome is considered, and then these are further separated by considering the occurrence of additional events.

7. **Failure Modes and Effects Analysis (FMEA).** This technique is also bottom up. Failure of a system element is considered and the consequences of this failure are examined until either a hazard occurs or it becomes clear that no hazard will occur. A system element in this context can be either equipment or a procedure step.

### D3.0 Example of a quantitative risk assessment methodology

This section describes a quantitative risk assessment methodology used previously to assess the acceptability of existing and new types of equipment on the SRN. It has also been used to assess the risks associated with alternative design options and with departure applications.

The risk assessment includes the following steps:

1. Hazard identification
2. Describe associated risks and who they affect
3. Estimate risk (defined as the product of the consequences and the likelihood of the risk being realised)
4. Assess the tolerability of risk
5. Assess the reasonableness of risk controls
6. Record findings

### D3.1 Hazard identification

This includes the use of:

1. Generic checklists
2. Hazard logs from previous, similar projects
3. Creative thinking techniques, e.g. brainstorming

Within this, it may be helpful to structure hazard identification around the following matrix:

**Table D-1 Hazard identification matrix**

| | Construction | Normal Operations | Planned Maintenance | Emergency Situation | Demolition |
|---|---|---|---|---|---|
| Users | | | | | |
| Workers – contractual relationship | | | | | |
| Workers – directly employed | | | | | |
| Other Parties | | | | | |

There will not necessarily be specific hazards associated with every user for every stage in the project life cycle (so there won't always be a something within every cell of the matrix). However, basing the hazard identification on this matrix will ensure that no users/life cycle stages are systematically missed as part of the hazard identification process.

In general, checklists and/or existing hazard logs will be applied first, subsequently followed by brainstorming. Particular attention must be given to any hazards that are introduced, changed or removed by the project.

Note that hazard identification must focus on the significant risks associated with the project; it must not look to identify trivial, generic hazards that will be well known and addressed by established standards or design/construction practices.

### D3.2 Associated risks and who they affect

For each hazard identified in the previous step, identify the associated risks and who they affect (i.e. road users, construction workers etc.).

Depending on the purpose of the risk assessment, it may be necessary to split certain groups down further than this e.g. 'Users' to car drivers, LGV drivers, HGV drivers, motorcyclist, NMUs, vehicle recovery workers and emergency services; 'Workers' to TM operatives; maintenance workers and Traffic Officers.

### D3.3 Estimate risk

Risk is estimated using the following equation:

*Risk = consequence x likelihood*

Depending on the purpose of the risk assessment, the final risk measure may be required to reflect collective or individual risk, as defined in Chapter 5 of GD04/12.

- **Collective risk** measures provide a measure of the safety risk affecting a particular population (e.g. road users, road workers).
- **Individual risk** measures then provide a measure of the safety risk for a particular individual – usually a hypothetical 'most exposed' individual from a particular population

This will need to be taken into account when the consequence and likelihood measures are chosen for the risk assessment.

### D3.4 Collective risk

Collective risk is expressed in terms of the rate of Fatalities and Weighted Injuries (FWIs), where a FWI is defined as:

*(No. of fatalities) + (0.1 x No. of serious casualties) + (0.01 x No. of slight casualties)*

The 'rate' unit then depends on whether the risk is proportional to time, to the distance travelled on the network, or to the number of 'transits' of a particular network feature.

- Risk proportional to time – this typically applies where exposure to a risk is proportional to time spent travelling or working on the network.

  *Where risk is proportional to time, the units of risk will be the number of FWIs/yr.*

- Risk proportional to distance travelled – this typically applies to risks associated with a particular route or feature that is continuous along a significant length of the network (where 'significant' is defined as lengths in excess of 1km).
  *Where risk is proportional to the distance travelled, units of risk will be no. of FWIs/vehicle km.*

- Risk proportional to number of transits – this typically applies to risks associated with a particular network feature or discrete 'point' on the network e.g. a junction, structure or discrete feature or object at the side of the road.
  *Where risk is proportional to the number of vehicle transits, units of risk will be no. of FWIs/vehicle transit.*

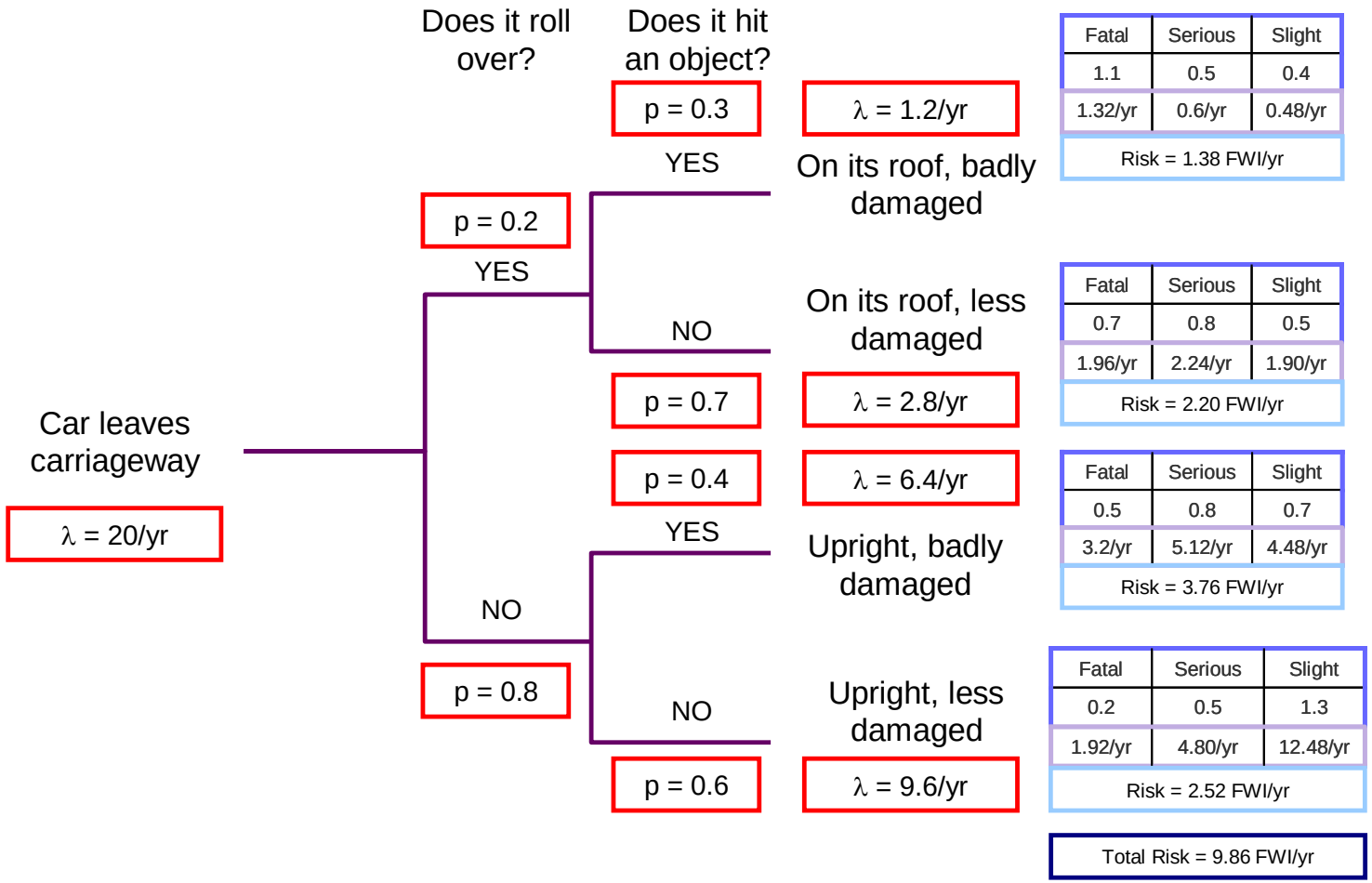
### D3.5 Individual risk

Individual risk is only usually calculated in order to compare the value obtained with risk tolerability criteria established by the HSE. These criteria are expressed in terms of the annual probability of death of an exposed person; therefore the units of individual risk calculated in any risk assessment will generally be in these same units.

For simple risks, values of consequences and likelihood within the risk equation can be estimated directly; the risk calculation can then be produced in a simple spreadsheet.

For more complex risks, it may be necessary to estimate risk using an event tree, such as the one given in Figure G-1.

**Figure D-1 Example of an event tree**



Ideally, estimates of consequences and likelihood within the risk assessment must be based on direct data. However, this may not always be available. In such cases, expert estimates will be used to inform the risk assessment.

Sources of direct data include:

- HAPMS/HAMIS (for validated Stats19 data)
- Agency Accident and Incident Reporting System (AIRS – for supply chain safety data)
- Agency Information Reporting and Investigation System (IRIS – for Traffic Officer and other Highways England staff safety data)
- Reported Road Casualties in Great Britain (published by DfT)
- Highways England project managers (for traffic data)
- Highways England - Safety Risk Model

Expert estimates should be obtained through a process of elicitation. This could involve either an individual expert, or a group of experts. The process will generally involve a discussion of the data to be determined.

The expert estimates of the data will then be recorded along with the basis for this (including any assumptions or constraints/conditions that may affect the value for the data) and who the 'experts' were (to establish their competence to make the judgements they had made).

### D3.6 Assess tolerability

Depending on the purpose of the risk assessment, there may be a need to assess the tolerability of a risk. Because the methodology is quantitative, it must be possible to compare the estimated risk values with absolute tolerability criteria, as defined within Chapter 5 of GD04/12.

Safety risks greater than the maximum tolerable risk limit will not be accepted. Where the safety risks are demonstrably below the minimum acceptable risk limit, i.e. broadly acceptable, then no additional safety risk controls will be implemented. The only exception is if there are obvious existing good practices that have not been implemented.

### D3.7 Criteria to assess the reasonableness of risk controls

Risk controls may be considered reasonable wherever:

1. Costs of preventing a fatality do not exceed the established Value of Preventing a Fatality (VPF) figure.

2. Costs, time or resources to deliver the controls do not impact the ability to deliver other safety measures that have a higher Benefit-Cost Ratio (BCR).

3. The controls do not have an unreasonable impact on the performance of the network, as measured against criteria other than safety e.g. Journey Time Reliability, carbon emissions

### D3.8 Record findings

The purpose of this step is to make sure that the application of the risk assessment process is auditable in the future – to record what was done, why and on what basis.

Detail recorded for a risk assessment must include:

1. The conclusions/findings of the risk assessment
2. Detail of any calculations made under each of the steps in the process
3. Any assumptions/decisions underpinning the assessment
4. Any data sources
5. Who did the risk assessment

The last point is important as it could be needed in the future to demonstrate that the risk assessment was undertaken by a competent person.

## D4.0 Example of a semi-quantitative risk assessment methodology

This risk assessment methodology has been used previously on type C SMS projects. This methodology allows a semi-quantitative assessment of the risk from each identified hazard to be made.

## D4.1 Types of hazards

The first step in the methodology is to decide whether each identified hazard is an 'Event' type or a 'State' type:

- An Event (E) is a hazard which occurs momentarily, e.g. a vehicle carries out a high-risk lane change. Usually it is not meaningful to talk of how long such a hazard exists for.

- A State (S) hazard is one which is present for a period of time e.g. vehicle stopped on hard shoulder – the longer it is present, the greater the risk. Such hazards will have a measurable duration and can persist for long periods.

It is important to distinguish between these two types of hazards as the risk scores are evaluated differently depending on the choice. Both types of hazard are assessed based upon the following properties:

### 1. 'E' Hazards

Event hazards are evaluated by adding together a score for each of the following three factors:

- The frequency at which the hazard is expected to occur
- The probability that the hazard causes an incident
- The severity of the incident

### 2. 'S' Hazards

State hazards are evaluated by adding together a score for each of the following three factors:

- The likelihood that the hazardous state is present
- The rate at which incidents occur if the hazardous state is present
- The severity of the incident, which is the same as for event hazards

The definitions and descriptions of the elements that make up both event and state hazards are summarised in Table D-2.

**Table D-2 Components of hazards**

| | Component Description | Hazard Type | |
|---|---|---|---|
| | | Events | States |
| **Component 1** | How often the hazard is likely to occur | Frequency | Likelihood |
| **Component 2** | A measure of whether or not an incident will be caused by the hazard | Probability | Rate |
| **Component 3** | The severity of the incident consequences | Severity | Severity |

In order to determine what overall scores will be assigned for Event and State Hazards, the project must decide on the scale it will use to score each factor. A logarithmic scale of scoring is used in order to cover the necessary range of values and then present them in a manageable form. An increase of 1 in a score therefore represents a factor increase of 10 in risk. The tables which follow are examples of the values that each of the event and state factors may be assigned.

**Table D-3 Example of classification of event hazard frequencies**

| Frequency Classification | Nominal Value: Occurrences/year mile | Occurrences/year/ entire project | Frequency of occurrence | Index Value |
|---|---|---|---|---|
| Very frequent | 1,000 | | | 6.0 |
| | 316 | | | 5.5 |
| Frequent | 100 | | | 5.0 |
| | 31.6 | | | 4.5 |
| Probable | 10 | | | 4.0 |
| | 3.16 | | | 3.5 |
| Occasional | 1 | | | 3.0 |
| | 0.316 | | | 2.5 |
| Remote | 0.1 | | | 2.0 |
| | 0.0316 | | | 1.5 |
| Improbable | 0.01 | | | 1.0 |
| | 0.00316 | | | 0.5 |
| Incredible | 0.001 | | | 0.0 |

Each project would complete columns 3 and 4 in the above table, based on the length of scheme being considered, with column 3 being the product of the nominal number of occurrences per year per mile and the overall scheme length (miles), and column 4 being the inverse (i.e. 1 divided by the value of column 3, remembering to correct to get the right units e.g. per year, per day, per hour etc.). Having such numbers available has been found to be helpful when evaluating the frequencies of hazard occurrence.

**Table D-4 Example of likelihood classification of state hazard**

| Likelihood Classification | Interpretation | Nominal value per mile of motorway | Expected number of occurrences present on scheme | Index Value |
|---|---|---|---|---|
| Very frequent | | 1 | | 6.0 |
| | | 0.316 | | 5.5 |
| Frequent | | 0.1 | | 5.0 |
| | | 0.0316 | | 4.5 |
| Probable | | 0.01 | | 4.0 |
| | | 0.00316 | | 3.5 |
| Occasional | | 0.001 | | 3.0 |
| | | 0.000316 | | 2.5 |
| Remote | | 0.0001 | | 2.0 |
| | | 0.0000316 | | 1.5 |
| Improbable | | 0.00001 | | 1.0 |
| | | 0.0000031 | | 0.5 |
| Incredible | | 0.000001 | | 0 |

Table D-4 requires completion for dealing with State hazards in the same way that Table D-3 did for Event hazards. Column 2 is again the product of the length of scheme in question and column 3. Typical entries will include ‘x occurrences present at any one time’ and ‘present for x days per year’, where ‘x’ is calculated each time.

To give an example, if a scheme has a length of 10 miles, then the value to enter for an ‘occasional’ hazard will be 10 x 0.0001 = 0.001 occurrences on the scheme at any one time (entry in column 4). To calculate how many days of the year this event is likely to be present, this result is multiplied by the number of days in the year, i.e. 0.001 x 365 = 0.365, or about 9 hours. The entry in column 2 would therefore read ‘Present for approximately 9 hours per year’.

The figures in D-5 are used for hazards of both types, Event and State, to estimate the frequency/likelihood of an accident occurring once a hazard has occurred/is present.

**Table D-5 Example of hazardous events and states probability and rate classifications**

| Classification | Interpretation | Index value |
|---|---|---|
| Certain | It is certain that this hazard, if it occurs, will cause a collision | 4 |
| Probable | It is probable that this hazard, if it occurs, will cause collision | 3 |
| Occasional | This hazard, if it occurs, will occasionally cause a collision | 2 |
| Remote | There is a remote chance that this hazard, if it occurs, will cause a collision | 1 |
| Improbable | It is improbable that this hazard, if it occurs, will cause a collision | 0 |

Table D-6 shows the consequence values that are used as the final part of the risk evaluation of each hazard.

**Table D-6 Example of severity classifications for hazardous events and states**

| Severity classification | Interpretation | Index value | Person outside of vehicle | Stationary vehicle | Motorcycle | Car | Large Vehicle (LHV, HGV, Bus) |
|---|---|---|---|---|---|---|---|
| Severe | The proportion of collisions that are fatal is expected to be higher than average by at least a factor of 10 | 2.0 | Involved | Involved | Involved | Speed differential approx 60 mph | Speed differential approx 50 mph |
| Higher than average | The proportion of fatal collisions is expected to be higher than average by a factor between 3 and 10 | 1.5 | No involvement | No involvement | No involvement | Speed differential approx 50 mph | Speed differential approx 40 mph |
| Average | The distribution of collisions (i.e. ratio of damage-only to fatal) is expected to be similar to the motorway average | 1.0 | No involvement | No involvement | No involvement | Speed differential approx 40 mph | Speed differential approx 30 mph |
| Lower than average | The proportion of fatal collisions is expected to be lower than average by a factor between 3 and 10 | 0.5 | No involvement | No involvement | No involvement | Speed differential approx 30 mph | Speed differential approx 20 mph |
| Minor | The proportion of collisions that are fatal is expected to be lower than average by at least a factor of 10 | 0.0 | No involvement | No involvement | No involvement | Speed differential < 20 mph | Speed differential < 10 mph |

Once the three elements of a hazard have been assessed then they need to be added up. While risk is usually calculated by multiplying together its constituent elements, adding is appropriate in this instance because of the logarithmic scale that is being used.

**Risk index for hazardous event**
*= hazard frequency index + incident probability index + incident severity index*

**Risk index for hazardous State**
*= hazard likelihood index + incident rate index + incident severity index*

Event hazards will have a prefix ‘E’ e.g. E08
State hazards will have a prefix ‘S’ e.g. S08

Given the score ranges specified, hazard scores will range from 0-12.

## D4.2 Notes on risk scores and ranking

- Despite the use of numbers, the risk score is at best semi-quantitative and does not provide an absolute measure of risk, even approximately.

- The methodology is designed to place each hazard into one of a number of bands, so that it can be seen clearly which hazards are considered to present the greatest risk and resources can be allocated proportionately.

- This approach also facilitates the calculation of risk changes that a project brings about, thus enabling an assessment to be made as to whether a project has achieved its safety objective.

- In order to complete such an assessment, each hazard must be reviewed and the impact that the project has on its score considered. By adding together the impact of all such risk changes, the overall change in risk that the project brings is calculated.

- This ‘before and after’ analysis requires that the change to a given hazard, as a result of implementing a project, is quantified to some degree.

- The smallest risk change so far provided in this risk assessment method is 0.5, which, given the logarithmic scale being used, represents a factor of 3. As the number of hazards that will experience a risk change of this size is likely to be few or none, some finer scale is needed to measure risk changes.

- An approach that provides a finer level of granularity in assessing risk change is shown in Table D-7.

**Table D-7: Measuring before and after risk changes**

| Change in risk score (logarithmic) | Absolute change in risk |
|---|---|
| 0.5 | 216% increase in risk |
| 0.4 | 150% increase in risk |
| 0.3 | 100% increase in risk (i.e. doubling of risk) |
| 0.2 | 60% increase in risk |
| 0.1 | 25% increase in risk |
| 0.0 | No change in risk |
| -0.1 | 20% decrease in risk |
| -0.2 | 35% decrease in risk |
| -0.3 | 50% decrease in risk (i.e. risk is halved) |
| -0.4 | 60% decrease in risk |
| -0.5 | 70% decrease in risk |

Using the changes in risk scores listed in Table D-7, a hazard's before and after scores can be assessed. It is normal to assess the initial hazard score as if the project were implemented, and then to consider the change to the hazard score that the scheme brings. Therefore a hazard may be assessed as an E08 with the scheme implemented, and a change of -0.1 as a result of implementation, meaning that it's before score was E08.1.

By assessing each hazard in turn in the way described above, total before and after risk scores can be calculated and compared.

## APPENDIX E: Hazard analysis methodologies for type C SMS

### Type C risk assessment

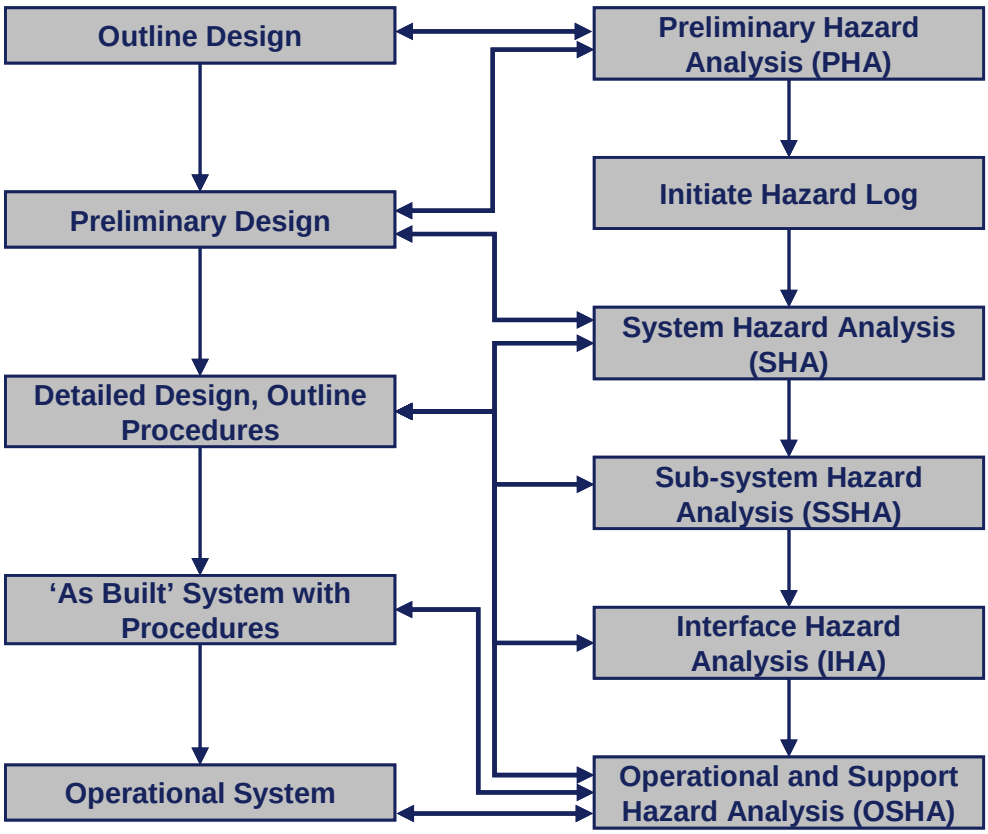



**Figure 5-1: Project SMS Hazard Analysis Activities and Design**

Appendix E describes the use of recognised forms of hazard analysis that may be used as a form of risk assessment for projects with a type C SMS.

Each analysis involves the systematic examination of the project or project elements and its/their environment, with a view to identifying potential hazards, their causes and appropriate mitigations.

It will be acceptable to omit SSHA and IHA if, having completed PHA, SHA and OSHA, it can be shown that:

- The project design promotes confidence that no new hazards will be revealed through more detailed examination.
- All necessary interfaces have been analysed in sufficient depth, in respect of equipment to be deployed and of organisations involved.

Any omissions must be justified in the project safety report.

Where available, any pre-existing hazard analyses will be taken into account, and where still applicable, need not be repeated. These may be analyses undertaken as part of meeting legislative requirements (e.g. CDM (2007); the departures procedures; or a similar project.

## E1 Selection of methodology

Figure E-1 below helps to distinguish the difference between the preliminary, system and sub-system hazard analysis activities:

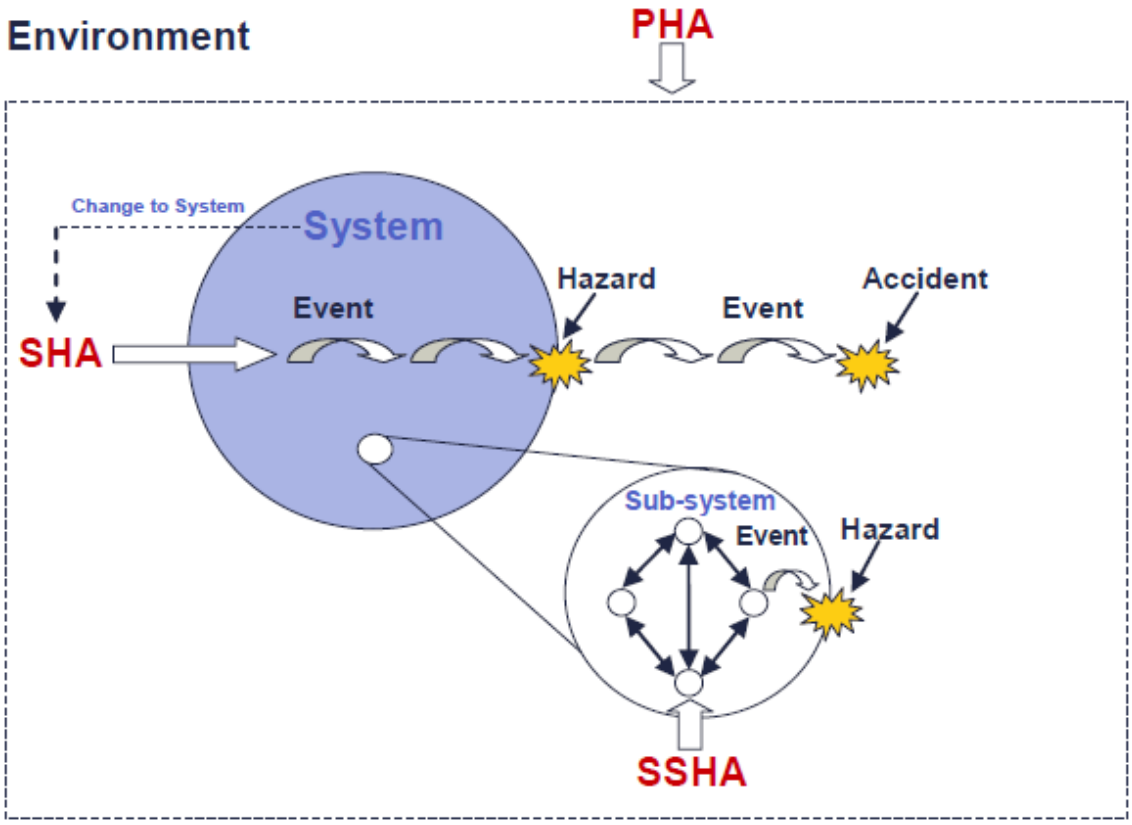



**Figure E-1 Differences between hazard analysis activities**

As shown in Figure E-1 the PHA is a preliminary examination of the whole project. The PHA is the first type of hazard analysis activity that is carried out. It identifies as many of the hazards as possible that can affect the project, through consideration of the main functions and operations that the project will provide i.e. the general suite of hazards that occur when the project operates in its proposed environment.

Figure E-1 also shows that the SHA examines internal aspects of a project. The SHA is a more detailed assessment of the project. It considers all of the events that could occur within the project that may lead to a hazard.

The SSHA develops a further level of detail on the SHA. The SSHA examines detailed internal aspects of design. It includes analysis of the project sub-systems and identifies each of the events that could occur within the sub-systems that may lead to a hazard.

The following sections detail recognised forms of hazard analysis that may be used as a form of risk assessment for projects with a type C SMS.

## E2 Preliminary hazard analysis (PHA)

### E2.1 Objective

To identify all reasonably foreseeable hazards that can arise from the project interacting with its environment, after establishment of project concept and before detailed design.

### E2.2 Pre-requisite data

- The main functions that the project will deliver.
- The main operational changes that it will deliver (including project maintenance).
- The environment in which they will operate.
- Design sketches and drawings.
- Any applicable historical data from related projects that is available.

### E2.3 Process

**1. Define the project – determine the project model**

The first stage of the PHA involves describing what is meant by the project. The project description is based on the known design and operational features. Hazard identification is based on this description.

The project model will provide a list of project characteristics that can then be used as the basis for PHA discussions. The type of information that a project model would contain is given below in Table E-1.

**Table E-1: Example - project characteristics that are used to create the project model**

| **A selection of the assumed features that may form the basis of the PHA for an example project** | |
|---|---|
| **Design characteristics:**<br>Additional running lane<br>Hard Shoulder<br>Lay-bys<br>Lane spacing<br>Lighting<br>CCTV cameras<br>Gantry spacing<br>Gantry design<br>Emergency Refuge Areas (ERA)<br>Speed limits<br>Safety barriers<br>MIDAS spacing<br>Central reserve details<br>Cable cabinets<br>Compliance<br>Emergency Roadside Telephones (ERT) | **Operational characteristics:**<br>Worker safety<br>Highways England staffing<br>Traffic flows<br>Incident management<br>Resilience/diversion rates<br>Reliability of technology |
| Each characteristic is then expanded to provide detailed information. For example, the ERA spacing feature would include how far apart they are to be spaced (e.g. at 1km intervals) and their position in relation to the road itself. Speed limits would include a detailed description of the speed limit throughout the whole project location (e.g. 70pmh for 2 km, 50mph for 4km etc).<br><br>These features and details are then used to supply the subsequent steps of the PHA with the required project detail. Each feature will be systematically examined in the discussion at the workshop to investigate the hazards that are applicable to the project. | |

**2. Identify applicable hazards from existing work**.
Hazards already identified during safety risk assessments carried out on related projects can be incorporated into the PHA.

Collisions and hazards already identified from previous projects will be reviewed to check that they are still applicable to the current project and to modify them as required.

Modifications to existing hazards may include changes to the risk score and the removal/addition of mitigations.

Factors to take into account when reviewing existing hazards and collisions will include differences in the road environment that apply to the current project, any mitigations that may no longer be applicable, new mitigations that may be available and data that may be available to refine the risk score.

**3. Conduct workshops to review existing hazards and identify other applicable hazards**.
Identification of new hazards will be achieved through examination of the project functions and operations in a workshop environment. Attendees will be drawn from:

- Highways England Project Manager
- Maintenance Service Providers
- Health and safety representatives
- Operators
- Safety experts
- Technology specialists
- Specific designers of pertinent areas
- Suppliers

In the workshops, each function and operational aspect of the project will be examined systematically to identify:

a) The collisions that could arise from these functions and operations.
b) The hazards, which if they occurred, would give rise to these collisions occurring.

Each hazard will be identified as either sufficiently mitigated or in need of further mitigation.

The identification of further mitigations is not a formal part of the PHA process, but any that are identified must be recorded.

Any actions required to better understand the hazards will be noted for addressing during a subsequent hazard analysis activity

**4. Initial risk assessment of each hazard**.

Once all of the preliminary design hazards have been determined a ‘risk score’ is to be assigned to each of them. This activity involves assigning a frequency and consequence to each hazard. Each project will need to establish its own approach to scoring safety risks.

**5. Apply rationalisation and organisation of the hazards into the Hazard Log**.
Each of the identified hazards, collisions and causes will be entered into a project hazard log. Hazards will be linked to the relevant collision and the safety risk score associated with each hazard recorded.

This rationalisation will inform whether the project meets the tolerability requirements for each population required by Chapter 5 of GD04/12.

Each hazard entry will have:

- A full description
- The consequences of the hazard, noting the collisions which can result if the hazard occurs
- A safety risk assessment (a score assigned to each hazard) including an explanation for the score given (where possible this must be based on data rather than expert judgement, but it is to be expected that data will not be available for all cases)
- The assumptions underlying the safety risk assessments
- Known mitigation measures for the hazard
- A list of future actions to be undertaken including outstanding questions or further investigations to be carried out, actions which will be managed through subsequent safety risk assessment.

A version of the Hazard Log corresponding to the completion of the PHA will be retained for future audit requirements.

**6. Documentation of PHA results**
The main activities undertaken in the PHA and the main results arising will be documented in the PHA report. This report will provide an audit trail to show how the PHA was carried out and what it produced.

### E2.4 Deliverable

- The PHA report and
- Consolidation of hazards into the hazard log.

Guidance for the PHA report is detailed in Table E-2. The format must be tailored to reflect the nature of the project being analysed. The areas in grey are not essential, however, may be a useful addition and should be considered for inclusion.

## Table E-2: PHA report guidance

| Section Reference | |
|---|---|
| **1. Introduction** | *This section gives an introduction to the need for the PHA, its objectives and scope, and how the outputs will be used.*<br>**1.1 Project overview**<br>**1.2 Previous applicable projects**<br>*Outputs from previous PHAs can be used as input for the project but these must be reassessed. This section needs to reference any equivalent previous projects.* |
| | **1.3 Outputs from the PHA**<br>*An indication could be given of how the outputs will be used, e.g. how they will feed into the Hazard Log, the operational safety requirements report, the operational plan, operational procedures, maintenance requirements, maintenance plan, safety and maintenance procedures, etc* |
| | **1.4 Structure of the PHA**<br>*The structure of the report could be outlined, including any techniques used to determine the structure. An overview of the safety argument could be given.* |
| **2. Objective and scope of PHA** | **2.1 PHA objective**<br>*A brief statement is required on the objective of the PHA, e.g. "to conduct an initial examination of the project scheme and its environment to establish the hazards that could potentially arise from use of the proposed design and to carry out an initial risk assessment of these hazards".*<br><br>**2.2 PHA scope**<br>*The scope of the PHA will be defined, e.g. "the PHA covers all of the preliminary design features (both physical and operational) of the project at the time the PHA was conducted". This will be accompanied by a list of all of the pertinent design features, with a brief description of each.* |
| **3. PHA methodology** | *The method used to conduct the PHA.*<br><br>**3.1 Activities carried out**<br>*This section will include a brief overview of the PHA activities. These are likely to include the following:*<br><br>***3.1.1 Initial identification of hazards***<br>*An outline will be provided of the hazard review conducted once an initial set of features has been agreed for the project scheme, the outputs of this, and how these were used.*<br><br>***3.1.2 Rationalisation and organisation of the hazards into a hazard log***<br>*This will explain how all the hazards identified by the initial identification process were entered into the hazard log, and any grouping system used.*<br><br>***3.1.3 Initial analysis and risk assessment***<br>*This will provide details of the analysis conducted for each hazard, including initial cause and consequence analysis, initial risk estimation, identification of possible mitigation measures and an initial comparison with what is present currently on the motorway.* |

| Section Reference | |
|---|---|
| | ***3.1.4 PHA workshops***<br>*Any workshops conducted to complete the identification and assessment of the identified hazards will be explained, with a list of workshop attendees provided and details of the approach adopted by the workshops.*<br><br>**3.2 Risk assessment methodology**<br>*This section will provide a summary of the approach to risk assessment.* |
| | **3.3 Definitions**<br>*A list of the definitions applicable to the PHA report will be provided, e.g. definitions of terms such as "hazard", "risk" and "incident". The definition supplied here will apply to any subsequent hazard analyses.* |
| | **3.4 The hazard log**<br>*The hazard log will be briefly introduced, with detail on the type of system being used by the project in question. Further information should be provided on:*<br><br>• *The structure and content of the log- e.g. the hierarchy of collisions, hazards, causes and sub-causes within the log*<br>• *The usage of the hazard log* |
| | **3.5 Current status of analysis**<br>*An overview may also be given of the current status of analysis, e.g. the current state of the hazard log and scheme design development* |
| | **3.6 Task plans**<br>*This section is relevant if a set of task plans will be developed and traced through the hazard log to mitigate particular hazards. A list of the known plans and their status will be provided.* |
| **4. Identification of higher risk hazards** | *This section will list those hazards with the highest risk scores. The highest-scoring hazards of both types will be recorded separately. Such hazards have the largest influence on the overall risk level of the project, and their mitigation has the greatest potential for reducing risk. The key issues arising for the project scheme from these hazards will also be explored.* |
| **5. Next steps in safety analysis process** | *This section describes the future activities of the safety programme for the project scheme, in order to show how the outputs of the PHA will flow into these other activities*<br><br>**5.1 Future risk assessment activities**<br>*The analyses to be conducted after the PHA will be listed, e.g. SHA, SSHA, IHA, and OSHA*<br><br>**5.2 Other outstanding issues to be analysed**<br>*This section will include a description of any further issues that will be analysed.* |
| **6. Conclusion** | *This will summarise the findings so far, and explain the rationale for why, at this stage, the PHA provides confidence that the risk that will be presented by this project scheme is well understood* |

### E2.5 Approval requirements

The PHA report will be subject to the approval process outlined in Section 4.0, once delivered as part of a PCF product.

## E3 System hazard analysis (SHA)

### E3.1 Objective

- To identify the hazards that can arise from the project design through systematic examination of the design and its potential failure modes.

### E3.2 Pre-requisite data

- Outputs from the PHA.
- The latest design sketches and drawings.
- Diagrams (e.g. flow diagrams) describing any proposed sequences of activities/functions/operations.
- Any additional applicable historical data from related projects that is available.

### E3.3 Process

The process for conducting an SHA is outlined below.

1. **Further develop the project description used in the PHA by adding in additional design details.** This description will act as a basis for conducting the SHA so it is important that it is as accurate a reflection as possible of the design intentions at this point in time

2. **Identify any new hazards from existing work that may now be applicable to the design.** Additional hazards that have already been identified on other Highways England projects may now be applicable depending on the new design features to be implemented.

3. **Conduct a set of SHA workshops to review existing hazards and identify all other applicable hazards.** These workshops will be similar in nature to those carried out as part of the PHA and will analyse the design that the project will deliver.

    - Attendees to the workshops will include those listed for PHA, with particular emphasis on specific designers of pertinent areas.

    - Each design element of the project must be examined systematically to identify the potential collisions and associated hazards that apply to them.

    - Collisions and hazards from previous projects now identified as relevant will be reviewed and any project specific features taken into account.

    - Each hazard will be identified as either sufficiently mitigated or in need of further mitigation. Where this is the case, either further mitigations will be identified and recorded or an action recorded to identify further mitigations.

    - Any actions required to better understand hazards will be noted for later attention

4. **Carry out assessment of the risk associated with new hazards and refine any from the original set of hazards.**

5. **Conduct ongoing analysis of issues arising from the workshops.** Not all issues will be resolved in the course of the workshops and specific risk assessments and other studies are expected to be needed. These activities will commence as soon as the workshops are complete although they do not need to form part of the SHA Report.

6. **Capture of all information arising from the SHA in the hazard log.** The hazard log will be the main repository of all information that arises in the course of conducting the safety analysis work so the output from each analysis activity must be added.

   For the SHA, the new information will take the form of new hazards, updates to existing hazards, additional mitigations and revisions to risk assessments. Any issues that require further investigation will be documented in the hazard log.

   This rationalisation will inform whether the project meets the tolerability requirements for each population required by Chapter 5 of GD04/12.

7. **Documentation of SHA results.** The main activities undertaken and results arising will be documented in the SHA report. This report will provide an audit trail to show how the SHA was carried out and what it produced. It is acceptable to document some analysis that contributes to the SHA in separate reports, where combining them would be impractical.

### E3.4 Deliverable

- The SHA report. The outline content for the SHA report is the same as the PHA, summarised in Table 7-8.
- Consolidation of hazards into the hazard log.

### E3.5 Approval requirements

The SHA report will be subject to the approval process outlined in Section 4.0, once delivered as part of a PCF product.

## E4 Sub-system hazard analysis (SSHA)

### E4.1 Objective

- To complete the safety analysis of the design, identifying any additional hazards that can arise from the detailed project design.

- Where an SSHA is assessed as not being necessary, the decision will need to be documented and then included in the Safety Report.

### E4.2 Pre-requisite data

- Outputs from PHA
- Outputs from SHA
- The latest design sketches and drawings (these will have been updated since those used in the PHA and SHA)

- Data describing the project subsystem components in detail
- Diagrams (e.g. flow diagrams) describing any proposed sequences of activities/functions/operations
- Additional applicable historical data from related projects (especially with respect to the project subsystems)

### E4.3 Process

By the time that the SSHA is undertaken, detailed design will be advanced but will not be complete. The process for conducting an SSHA is outlined below.

1. **Define the sub-system design components.** The first stage of the SSHA is to clearly define the project sub-system components that are to be analysed. The design will need to be sufficiently advanced to allow this to be possible

2. **Review any existing analysis work for its applicability to the SSHA.**

3. **Conduct SSHA workshops and/or analysis processes.** Once the set of sub-system components have been agreed, analysis can take place through two approaches, which may be combined. These are:

    1) **Holding of workshops**
    The attendance will be similar to those held as part of the SHA. The workshops will be used to analyse detailed design components and sub-systems.

    2) **Detailed safety analysis**
    Detailed design components may be analysed using a desk based method such as FMEA.

    It will be a project specific decision as to how the SSHA will be carried out. The approach will be justified in the SSHA report.

4. **Carry out assessment of the risk associated with new hazards and refine any from the original set of hazards.**

5. **Capture of all information arising from the SSHA in the hazard log**. The hazard log will be the main repository of all information that arises in the course of conducting the safety analysis work so the output from each analysis activity must be added.

    For the SSHA, the new information will take the form of new hazards, updates to existing hazards, additional mitigations and revisions to risk assessments. Any issues that require further investigation will also be documented in the hazard log.

    This rationalisation will inform whether the project meets the tolerability requirements for each population required by Chapter 5 of GD04/12.

### E4.4 Deliverables

- The SSHA report and any other detailed analysis reports that are necessary.
- Where a workshop approach is used, the report will be similar in content to the PHA and SHA reports.
- Consolidation of hazards into the hazard log.

### E4.5 Approval requirements

The SSHA report will be subject to the same approval requirements of the SHA and PHA outlined elsewhere, once delivered as part of a PCF product.

## E5 Interface hazard analysis (IHA)

### E5.1 Objective

- To complete the analysis of project related interfaces, whether technical (i.e. system or sub-system interfaces) or organisational.
- May be omitted if PHA. SHA and OSHA cover all system interfaces.
- The IHA examines sub-system and system interfaces for:

    1. Possible combinations of dependent and independent failures (both system and organisational) that can cause hazards to the project scheme users or personnel
    2. Ways in which any proposed design changes to the interfaces may create new hazards
    3. Organisation interfaces involved in project operation and maintenance

### E5.2 Pre-requisite data

The following is useful input data for an IHA:

- The outcome from the PHA, SHA (SSHA if applicable) and if available, the OSHA
- The latest design sketches and drawings
- Any data describing the project elements
- Diagrams (e.g. flow diagrams) describing any proposed sequences of
- activities/functions/operations
- Organisational charts of proposals for safety and project organisation
- Any applicable historical data from related projects

### E5.3 Process

The IHA takes place after the PHA and SHA have been completed. It may take place before or after the OSHA. During these other analyses it is possible that all the project related interfaces will be examined. Only when this is not the case is it necessary to perform an IHA.

1. **Define the interfaces to be examined and the flows across these interfaces.** The IHA will only be needed if interfaces can be identified that have not yet been analysed.

2. **Analyse the flows between interfaces.** The method of analysis will be to consider each type of information that can flow across an interface and the failure modes that apply to this information transfer. The analysis will be carried out either through additional workshops or as a desk-based exercise. Where a desk-based exercise is selected, the results must be reviewed sufficiently widely to demonstrate that appropriate expertise has been used in completing the activity. Where a workshop is used, similar attendance to that used for the SHA workshops is required.

3. **Carry out assessment of the safety risk associated with new hazards and refine any from the original set of hazards.** Risk scores will be assigned to all new hazards.

4. **Capture of all information arising from the IHA in the hazard log.** For the IHA, the new information will take the form of new hazards, updates to existing hazards, additional mitigations and revisions to risk assessments. Any issues that require further investigation will be documented in the hazard log.

   This rationalisation will inform whether the project meets the tolerability requirements for each population required by Chapter 5 of GD04/12.

5. **Documentation of IHA results in IHA report.** The main activities undertaken in the IHA and the main results arising will be documented in the IHA report. This report will provide an audit trail to show how the IHA was carried out and what it produced.

### E5.4 Deliverable

- The IHA report. The IHA report, if needed, will be similar in format to the PHA and SSHA reports.
- Consolidation of hazards within the hazard log.

### E5.5 Approval requirements

The IHA report may be subject to the same approval requirements as the PHA, SHA and SSHA, outlined in Section 4.0, once delivered as part of a PCF product.

## E6 Operation and support hazard analysis (OSHA)

### E6.1 Objective

- To Identify and analyse those hazards that are associated with the project processes and procedures carried out by people.
- Primarily concerned with the procedural interactions that people have with the project systems rather than the functions of the project (e.g. 'Worker' exposure to the SRN during maintenance).
- Procedures associated with construction that are addressed through existing legislation should not be repeated.

### E6.2 Pre-requisite data

The following data should be available prior to conducting the OSHA:

- Engineering descriptions/diagrams of the proposed system.
- Engineering descriptions/diagrams of the support equipment.
- Draft procedures and operating manuals.
- PHA, SHA, SSHA outputs.
- Personnel capabilities/competencies.
- Proposed resource requirements.
- Any relevant human factors engineering data and reports.
- Details of any historical data containing information about collisions or mistakes that have occurred due to human error (this data may be available from projects that are similar and are currently in operation).

### E6.3 Process

An OSHA examines the procedurally controlled aspects of the project system.

Broadly, these include:

- System production and deployment (installation) procedures
- System testing (commissioning) procedures
- Equipment storage prior to installation
- Operation of the system
- Maintenance
- Training

An OSHA is based on the descriptions of the project system operational regimes and maintenance processes that are available at the time it is conducted.

The process for conducting an OSHA is outlined below:

1. **Carry out preparation for hazard analysis workshop**. Process flow charts modelling maintenance and operational processes will be developed. If procedures have not been developed for a particular activity, then outline procedures will need to be developed for the workshop, based on best available information

**2. Review any existing analysis work for its applicability to the OSHA**

**3. Conduct workshops**. Workshop attendees must consist of key stakeholders and members of the project. Between them they will have:

- Maintenance or operations expertise, or knowledge of existing procedures.
- Knowledge of the safety activities that have already been carried out for the project.
- Knowledge of user behaviour (this will depend on the project).
- Experience of the system equipment that may be introduced.
- Knowledge of the project design.

The OSHA workshop must focus on:

- Identifying hazards associated with the procedures that are examined.
- Changing steps in any of the current processes to account for these hazards.
- Creating new steps in existing processes and procedures as required.
- Creating new processes or procedures, in the form of flow charts for those that do not currently exist, taking into account the known hazards that can affect these procedures.

The following may be used when approaching an OSHA workshop:

1. **HAZOP**
   - An OSHA may be conducted using a HAZOP (HAZard and Operability) study to systematically examine each project procedure.
   - An example of this method of capturing information is shown in Table E-3. To support the analysis it is recommended flowcharts describing the procedures to be examined are developed.

2. **OSHA guidewords**
   - Each step in the process flowcharts must be examined and it is useful to use guidewords in this process.
   - Guidewords are a predefined list of words which aid the thought process by steering the workshop in a particular direction. They are words that describe a deviation from the design intent.
   - A list of guidewords that may be used in an OSHA is given in Table E-4.
   - At the start of the HAZOP process, the project must agree that the guidewords set are sufficient for the intended purpose, and on the interpretation of each guideword with respect to the project. If a guideword is not considered relevant to a step, it should not be included in the OSHA records.
   - A guideword may also lead to several recommendations or questions, and this must be represented in the records.

**Table E-3- Example of recording results for an OSHA conducted as a HAZOP**

| Item no. | Procedure step | Guideword | Interpretation | Cause of hazard | Consequence/ implication | Hazard | Mitigation | Question/ Recommendations |
|---|---|---|---|---|---|---|---|---|
| 1 | Maintainer informs operator when equipment will be taken out of service | No | Maintainer does not inform operator before taking equipment out of service | Maintainer unaware of need, forgets, or does not think it is important to inform the operator | When an incident occurs, the operator is unable to use signals and signs to protect it, as they are no longer available | Refer to 'system failure' items in hazard log | Operator is likely to realise that the COBS is under maintenance as there will have been fault alarms | Ensure appropriate procedures are in place for maintainers to gain access to the project highway |

**Table E-4 List of some commonly used guidewords and their meaning**

| Guideword | Meaning |
|---|---|
| No | Not part of the intended procedure step is carried out |
| Late | Procedure step happens later than expected |
| Less | Quantitative Decrease |
| More | Quantitative Increase |
| Part Of | Qualitative Decrease |
| As Well As | Qualitative Increase |
| Reverse | Logical Opposite of the Intent |
| Other Than | Complete Substitution |

4. **Carry out assessment of the risk associated with new hazards and refine any from the original set of hazards.** Risk scores will be assigned to all new hazards.

5. **Capture of all information arising from the OSHA in the hazard log**. For the OSHA, the new information will take the form of new hazards, updates to existing hazards, additional mitigations and revisions to risk assessments. Any issues that require further investigation will also be documented in the hazard log.

   This rationalisation will inform whether the project meets the tolerability requirements for each population required by Chapter 5 of GD04/12.

6. **Documentation of OSHA results in OSHA report.**
   The main activities undertaken in the OSHA and the main results arising will be documented in the OSHA report.

   This report will provide an audit trail to show how the OSHA was carried out and what it produced.

   The OSHA is expected to produce a series of follow up actions that will need completion before an agreed set of procedures is available for a project. The OSHA report will document these actions; however resolution will be documented in the hazard log and in separate reports if necessary.

### E6.4 Operational procedures

The operational processes which must be considered include the operational regimes and incident management processes that are to be used for the operation of the project system.

### E6.5 Maintenance procedures

This part of the OSHA can be conducted by considering a selection of the equipment which will be used in the project system. The selected equipment must provide coverage of all the issues relating to the project equipment and infrastructure. The rationale for selecting specific items could include:

- **Equipment uniqueness**, i.e. equipment with unique maintenance requirements

- **Equipment access**, i.e. equipment with restricted access (the restriction in this case may be temporal, e.g. access to equipment may be restructured to prevent maintenance being carried out when the highway is in operation)

- **Maintenance location**, i.e. equipment for which consideration must be given to the location of maintenance personnel, e.g. on the hard shoulder

Each item of equipment must be examined with respect to how it will be maintained, with the organisations involved in this maintenance considered, along with the associated interfaces and any required information flows between these organisations.

A guideword approach can be used for the information flow (more information on application of guidewords is given previously in this document). For the selected equipment items, a generic flowchart for the operational management of access and the actions of those with maintenance must be produced.

### E6.6 National procedures

The OSHA provides the opportunity to identify the following:

- Activities occurring under hazardous conditions; their time periods; and the actions required in order to minimise risk over their time period
- Changes needed in functional or design requirements for system hardware/software, facilities, tooling, or support/test equipment to eliminate or control hazards or reduce associated risks
- Requirements for safety devices and equipment, including personnel safety equipment
- Warnings, cautions and special emergency procedures (e.g. egress or recovery)
- Requirements for packaging, handling, storage, transportation, maintenance and disposal of hazardous materials
- Requirements for safety training and personnel certification
- Potentially hazardous system states under operator control

The implementation of a project with a type C SMS may affect at least some, if not all of the above, which could affect Highways England's National Procedures. Before the project can be put into operation any effect on National Procedures will need to be identified and appropriate amendments made and agreed.

### E6.7 Recommendations

- The output of the OSHA will result in a list of recommendations; these must be tracked in the hazard log and task plans developed in order to address them. It may be advisable to prioritise these using hazards and urgency ratings in order to make their implementation more manageable.

- The hazard rating could have a scale ranging from ‘low risk hazard’ to ‘high risk hazard’, and the urgency rating could have a scale ranging from ‘latest’ (e.g. the recommendation does not need to be implemented until the project is decommissioned) to ‘earliest’ (e.g. the recommendation must be carried out immediately).
- Recommendations can then be prioritised based on the combination of these two factors. In addition to grouping based on prioritisation, recommendations may also be grouped in a manner that facilitates the development of task plans and their subsequent implementation.
- These must be recorded and tracked in the hazard log. It is likely that questions will arise during the OSHA, which cannot be answered immediately, and it may be the case that resolving these will produce more recommendations.
- These questions must be recorded and each assigned to a project member to investigate the answer and then, if necessary, formulate recommendations. This process must be recorded and tracked in the hazard log.

### E6.8 Deliverable

- The OSHA report. Guidance for an OSHA report is summarised in Table E-5.
- Specific maintenance and operational safety requirements that must be achieved to meet the project safety objectives. These requirements must be reflected in maintenance and operations plans for the project.
- Consolidation of hazards within the hazard log.

**Table E-5: Guidance for an OSHA report**

| Section Heading | Section Detail/Breakdown |
|---|---|
| **1. Introduction** | *This section gives an introduction to the need for the OSHA, its objectives and scope, and how the outputs will be used*<br><br>**1.1 Project overview**<br>*From PHA report.*<br><br>**1.2 OSHA objectives**<br>*A brief statement is required on the objectives of the OSHA, e.g. "to confirm that, within the scope of the OSHA, all equipment associated with the project has been reviewed to check that the required operation and maintenance procedures exist and the relevant aspects of all procedures that will be used by this project have been analysed"*<br><br>**1.3 OSHA scope**<br>*Scope needs to define the particular project design features to be analysed, and the associated operational related issues studied by the OSHA.* |
| | **1.4 Outputs from the OSHA**<br>*An indication will be given of how the outputs will be implemented e.g. how they will feed into the hazard log, the operational safety requirements report, the operational plan, operational procedures, maintenance requirements, maintenance plan, safety and maintenance procedures, etc*<br><br>**1.5 Structure of the OSHA**<br>*The structure of the report will be outlined, including any techniques used to determine the structure, such as Goal Structuring Notation.*<br><br>*An overview of the safety justification will be given.* |

| Section Heading | Section Detail/Breakdown |
|---|---|
| | **1.6. Overview of the SMS**<br>*The principal safety activities that will be undertaken throughout the Project Lifecycle will be shown. A figure is a helpful way of achieving this. An indication of which activities have been carried out thus far, and how the OSHA outputs will feed into other work An indication will also be given of the other types of hazard analyses that are being undertaken for the project, e.g. PHA, SHA, etc., and where the OSHA fits into this. There will be an indication of the scope of the OSHA in relation to the other hazard analyses, i.e. the two areas it is principally concerned with are operation and maintenance.* |
| **2. OSHA methodology** | **2.1 Activities carried out**<br>*The main points regarding the methodology will be summarised, including:*<br><br>• *When the OSHA was conducted.*<br>• *How the workshop team was chosen, the names and roles of those included, and which workshop meetings each attended.*<br>• *The method used to represent the process, e.g. the analysis could be based on a series of process flowcharts, each of which models either the maintenance or the operation process.*<br>• *How the results of the OSHA were recorded*<br>• *How the maintenance processes were considered, including which items of project equipment were selected for detailed study of their maintenance, the criteria by which these were chosen, and how maintenance was reviewed. There will also be a note on how different organisations involved in maintenance and associated interfaces were considered, and how any required information flows between these organisations were examined.*<br>• *How the operational processes were considered, including a list of all the operational regimes and management processes that were examined in the OSHA.*<br><br>**2.2 Approach to analysing the results**<br>*If the recommendations rising from the OSHA were prioritised, such as by using a combination of hazard and urgency ratings, the methodology for this will be explained.* |
| **3. Main Findings** | *This section summarises the key findings from the OSHA and provides a high-level breakdown of the recommendations into categories such as priorities for action.* |

| Section Heading | Section Detail/Breakdown |
|---|---|
| | **3.1 Summary of key findings**<br>This will produce a high-level summary of the key findings, such as the number of recommendations produced, a broad overview of the topics these mainly relate to, the main areas for further work and the number of questions raised during the analysis.<br>**3.2 Priorities of recommendations**<br>*The results of the prioritisation of recommendations will be given, e.g. the number of recommendations within each priority bracket. Some brief discussion may be added to indicate which issues have resulted in high-priority recommendations, etc.*<br>**3.3 Grouping of recommendations**<br>*If there are numerous recommendations, it is likely that these will have to be grouped in order to develop the Task Plans to address the recommendations and their implementation. Any such categories will be listed, with an explanation of the rationale behind the groupings given, and any categories of priority highlighted. A table may be used to represent this information, with the name of the group, the name of the subgroup, a description of the grouping, and the number of recommendations assigned to that group.* |
| **4. Issues for further analysis** | **4.1 Future risk assessment activities**<br>*This section will outline any future risk assessment activities that are to occur with a rough estimate of the timescale involved*<br><br>**4.2 Other issues to analyse**<br>*Any other issues to analyse that have not been mentioned previously will be outlined* |
| **5. Conclusion** | *This section should provide details of the work which will be conducted using the outputs of the OSHA, including the formulation of task plans for addressing the recommendations, and the way in which this will be carried out and progress tracked* |

### E6.9 Approval requirements

The OSHA report may be subject to the same approval requirements as all aforementioned risk assessments, outlined in Section 4.0, once delivered as part of a PCF product.

## APPENDIX F: Validation and verification

### F1 There are four types of verification that can be applied:

1. **Inspection** - Typical techniques include desk checking, walkthroughs, software reviews, technical reviews, and formal inspections

2. **Analysis** - Mathematical verification of the test item, which can include estimation of execution times and estimation of system resources

3. **Testing** - Given input values are traced through the test item to assure that they generate the expected output values, with the expected intermediate values along the way

4. **Demonstration** - Given input values are entered, and the resulting output values are compared against the expected output values

### F2 V-Lifecycle

The main elements of a typical testing process that may be used are illustrated in the V-Lifecycle of Figure F-1 below. This may be used as part of any type C verification and validation activity.

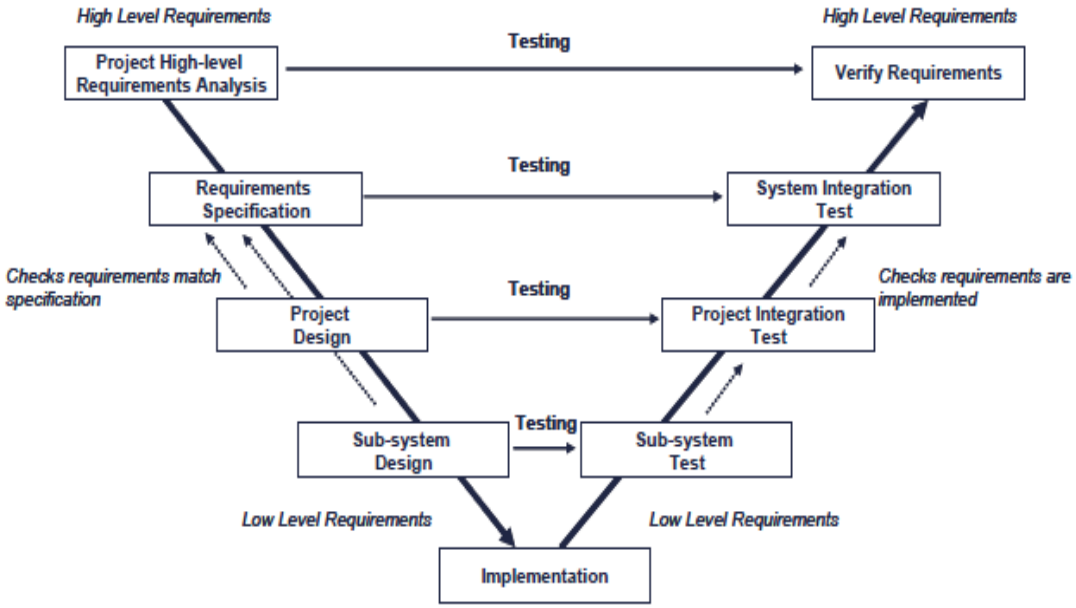



**Figure F-1: V-Lifecycle**

- The left branch of the ‘V’ shows the successive development of safety requirements from the projects high-level requirements down to the low level requirements.

- The right branch of the ‘V’ shows the successive testing activities required in order to verify the design.

- The V-lifecycle makes clear that testing activities are linked to those of design and development, i.e. what is designed must be checked with regards to the relevant requirements.

- It is important to note that testing activities will not only consider the physical design aspects but also consider procedural and operational aspects too. It is possible to envisage a further V-lifecycle which covers these aspects.

Each of the process steps are described briefly below:

1. **Project high-level requirements analysis and requirements specification.** The V-lifecycle begins with the definition of the high level requirements for the project. At this stage it will be possible to specify the demonstration and acceptance criteria for the high level safety requirement for the system.

2. **Project design and sub-system design.** The objectives of these stages are to create an overall project design and subsequent subsystem designs that conform to the safety requirements that have been specified. The aim of the verification activities is to demonstrate that the design matches the specified requirements.

3. **Sub-system, project integration and system integration test.** The objectives of these stages are to test the sub-systems, project as a whole and the entire system to check that the specified requirements have been implemented.

## APPENDIX G: Goal structured notation

Goal structure notation (GSN) is a graphical argumentation notation. It is used to represent each element of the safety report and the relationships between each element. Use of GSN also enables a systematic approach to be taken when assessing the impact of changes to the safety report. GSN is a key tool for use in the presentation of information and evidence in the safety report.

The GSN for a safety report consists of four elements:

1. **Requirements** – the overall safety objectives that must be addressed in order to demonstrate project safety. In the GSN, these form high-level goals/claims.

2. **Evidence/solutions** – information from the examination and test of the system.

3. **Strategy/argument** – how the evidence indicates compliance with the goals. In the GSN, the strategy/argument is expressed through the structuring of goals supported by sub goals.

4. **Contextual information** – the background on which the argument is based. In the GSN, this can be represented as context, assumptions, justification and models.