GN

GE/GN8642
Guidance on Hazard Identification and Classification

Issue Two: June 2014
Rail Industry Guidance Note

Published by:

RSSB
Block 2
Angel Square
1 Torrens Street
London
EC1V 1NY

Guidance on Hazard Identification and Classification

Issue record

Issue	Date	Comments
One	September 2012	Original document: This document gives guidance on identifying hazards and assessing risk (previously found in the Yellow Book Issue 4) and identifies where the guidance is out-of-date or needs to be treated with caution.
Two	June 2014	Supersedes and replaces issue one. This document has been revised throughout and gives guidance on hazard identification and classification associated with the application of the Common Safety Method on Risk Evaluation and Assessment required by Commission Regulation (EC) No 352/2009.

Superseded documents

The following Rail Industry Guidance Note is superseded, either in whole or in part as indicated:

Superseded documents	Sections superseded	Date when sections are superseded
GE/GN8642 issue one Guidance on Identifying Hazards and Assessing Risk	All	07 June 2014

GE/GN8642 issue one Guidance on Identifying Hazards and Assessing Risk, is withdrawn as of 07 June 2014.

Supply

The authoritative version of this document is available at www.rgsonline.co.uk. Uncontrolled copies of this document can be obtained from Communications, RSSB, Block 2, Angel Square, 1 Torrens Street, London EC1V 1NY, telephone 020 3142 5400 or e-mail enquirydesk@rssb.co.uk. Other Standards and associated documents can also be viewed at www.rgsonline.co.uk.

Contents

Part 1 Introduction

G 1.1 Purpose of this document

G 1.1.1 This document gives practitioner level guidance on the application of the risk management process set out in the 'Common Safety Method on Risk Evaluation and Assessment' (CSM RA). Specifically, this guidance is intended to assist infrastructure managers (IMs) and railway undertakings (RUs) in hazard identification and classification.

G 1.1.2 This document is primarily focussed on the application of the process by practitioners within an RU or IM. Others, who need to apply the process or interact with it in some way, should also find it useful. Further guidance for other actors (for example, manufacturers) may be developed over time.

G 1.1.3 The CSM RA (Commission Regulation (EC) No 352/2009) has applied since 01 July 2012 to all significant changes to the railway system – 'technical' (engineering), operational and organisational, or if required as the risk assessment process by a Technical Specification for Interoperability (TSI).

G 1.2 Background

G 1.2.1 Commission Regulation (EC) No. 352/2009 ('the regulation') established a 'common safety method on risk evaluation and assessment' (the CSM RA). The CSM RA, contained in Annex I to the regulation, sets out a mandatory risk management process for the rail industry that is common across Europe. The CSM RA has applied to all significant changes to the railway system since 01 July 2012. The changes may be of a technical (engineering), operational or organisational nature (where the organisational changes could have an impact on the operation of the railway). The CSM also applies if a risk assessment is required by a technical specification for interoperability (TSI); and is used to ensure safe integration of a structural subsystem into an existing system in the context of an authorisation for placing in service in accordance with the Railway Interoperability Directive 2008/57/EC.

G 1.2.2 Commission Implementing Regulation (EU) No 402/2013 establishes a revised common safety method for risk evaluation and assessment. The revised CSM RA has been in force since 23 May 2013 (meaning it can be used from that date), and will apply from 21 May 2015 (meaning that it must be used from that date), at which time Commission Regulation (EC) No. 352/2009 is repealed. The principal amendments relate to the acceptability of codes of practice, the documentation provided to an assessment body, the content of the safety assessment report and the recognition and accreditation of assessment bodies.

G 1.2.3 If a project is expected to continue beyond 21 May 2015, the proposer can continue to use the 2009 regulation, provided the project is at 'an advanced stage of development within the meaning of ... Directive 2008/57/EC'.

G 1.2.4 All references in this document to 'the regulation' refer to Commission Regulation (EC) No 352/2009, unless otherwise stated.

G 1.3 Copyright

G 1.3.3 In circumstances where Rail Safety and Standards Board Limited has granted a particular person or organisation permission to copy extracts from Railway Group documents, Rail Safety and Standards Board Limited accepts no responsibility for, nor any liability in connection with, the use of such extracts, or any claims arising therefrom. This disclaimer applies to all forms of media in which extracts from Railway Group Standards may be reproduced.

G 1.4 Approval and authorisation of this document

G 1.4.1 The content of this document was approved by a Multifunctional Standards Committee on 28 January 2014.

G 1.4.2 This document was authorised by RSSB on 09 May 2014.

Part 2 Guidance on Common Safety Method on Risk Evaluation and Assessment

G 2.1 General introduction

G 2.1.1 The CSM RA applies to *'any change of the railway system in a Member State … which is considered to be significant within the meaning of Article 4 of the Regulation'* that is Commission Regulation (EC) No 352/2009 [the CSM RA itself]. Those changes may be technical, operational or organisational, but are those which could impact the operating conditions of the railway system. The proposer of a change is responsible for applying the risk management process set out in the CSM RA. In many circumstances, proposers will be RUs or IMs. However, a manufacturer may want or need to apply the CSM RA in order to place a new or altered product or system on the market. Once the product is placed on the market, an RU or IM wishing to use the new or altered product or system in a specific application or location will be the proposer of a new change.

G 2.1.2 Detailed advice on the regulation's requirements, its scope and the significance test that triggers the requirement to apply the risk management process in full, is set out in the Office of Rail Regulation's (ORR's) guidance on the CSM RA. In this section an overview summary of the regulation and its requirements is provided, for the purposes of setting out the context of this guidance and allowing a quick point of reference to the main principles for practitioners.

G 2.1.3 Figure 1 shows the risk management process defined in the CSM RA. The process essentially consists of the following steps:

a) The proposer of a change produces a preliminary definition of that change, and the system to which it relates. It then examines it against the significance criteria in the regulation. If a change is deemed to be significant, then the regulation requires you to apply the risk management process in Annex I and appoint an independent assessment body to assess application of the process. However, the CSM RA risk management process is a sound one and you may choose to apply some or all of it more generally.

b) The CSM risk management process starts with the system definition. This provides the key details of the system that is being changed – its purpose, functions, interfaces and the existing safety measures that apply to it. This system definition will be kept live for the duration of the project.

c) All reasonably foreseeable hazards are identified and their risk is classified and / or analysed.

d) Safety requirements are identified by application of one or more of the three risk acceptance principles to each hazard.

e) A hazard record for the system that is to be changed is produced and maintained. Its purpose is to track progress of the project's risk management process.

f) Before acceptance, the change proposer demonstrates that the risk assessment principles have been correctly applied and that the system complies with all specified safety requirements.

g) The assessment body provides its report to the proposer. The proposer remains responsible for safety and takes the decision to implement the proposed change.

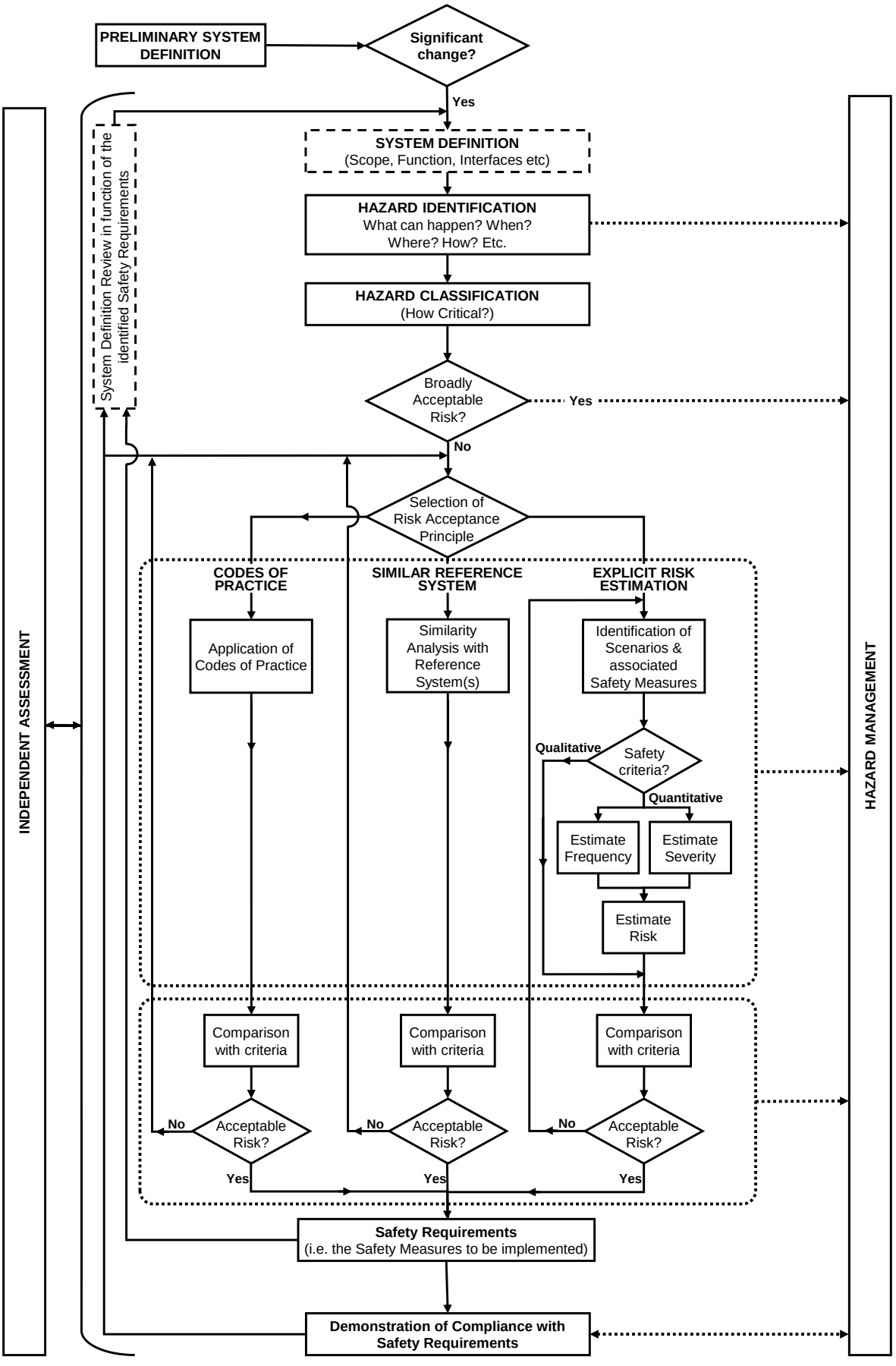

Figure 1 The risk management and independent assessment process from the CSM RA

Guidance on Hazard Identification and Classification

G 2.2 Guidance documents

G 2.2.1 This guidance forms part of a suite of six documents that address the different elements of the risk management process. The guidance notes are numbered below and Figure 2 shows how each one fits into the whole:

- Guidance on Planning an Application of the Common Safety Method on Risk Evaluation and Assessment (GE/GN8640).
- Guidance on System Definition (GE/GN8641).
- Guidance on Hazard Identification and Classification (GE/GN8642).
- Guidance on Risk Evaluation and Risk Acceptance (GE/GN8643).
- Guidance on Safety Requirements and Hazard Management (GE/GN8644).
- Guidance on Independent Assessment (GE/GN8645).

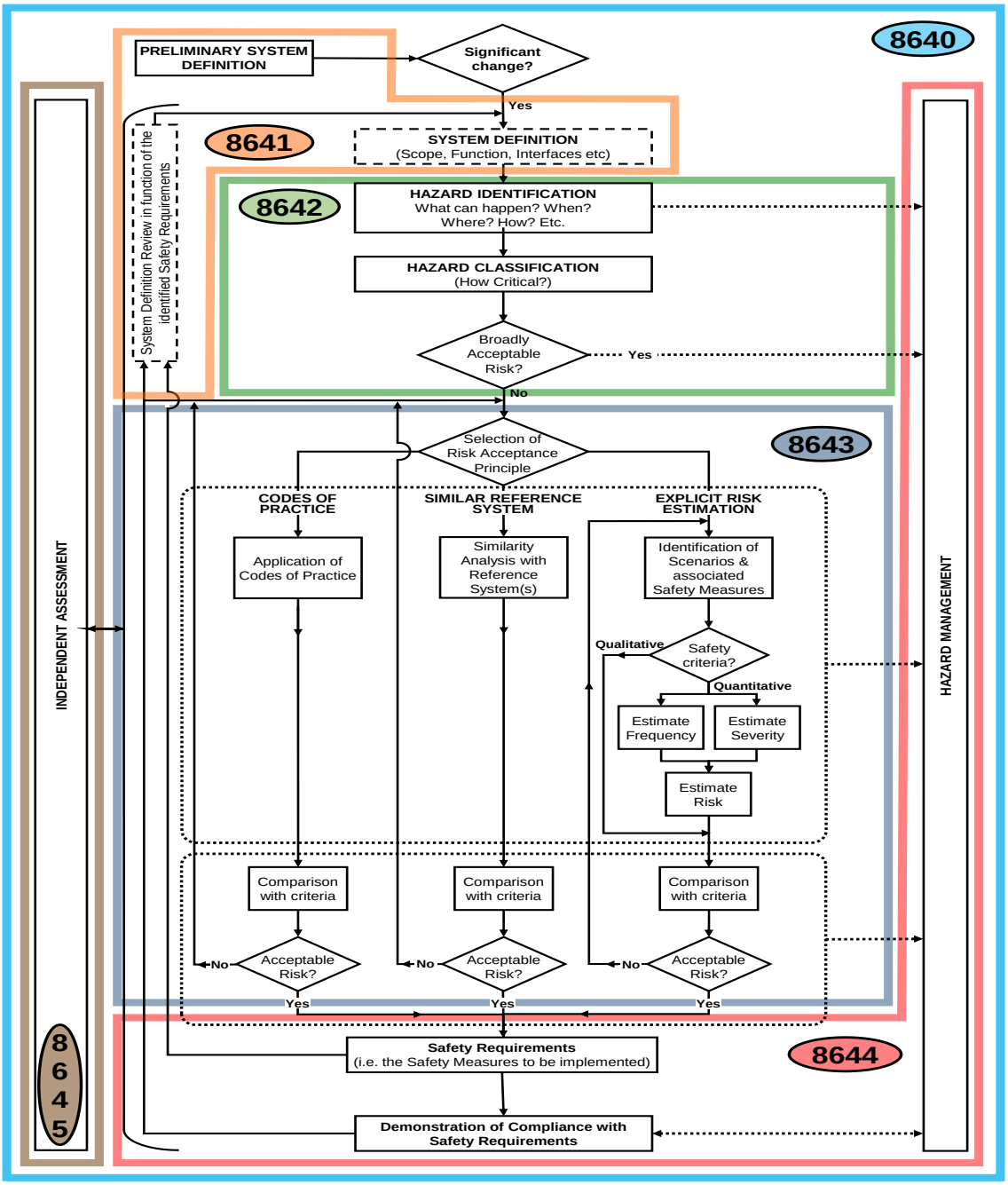

Figure 2 The set of guidance notes on the application of the CSM RA, and the process elements to which they relate

Part 3 Guidance on Hazard Identification

G 3.1 What is a hazard?

G 3.1.1 The regulation defines a hazard as 'a condition that could lead to an accident'.

The Safety Directive defines an accident as:
'accident' means an unwanted or unintended sudden event or a specific chain of such events which have harmful consequences; accidents are divided into the following categories: collisions, derailments, level-crossing accidents, accidents to persons caused by rolling stock in motion, fires and others; (Directive 2001/14/EC)

The Safety Directive defines a serious accident as:
'serious accident' means any train collision or derailment of trains, resulting in the death of at least one person or serious injuries to five or more persons or extensive damage to rolling stock, the infrastructure or the environment, and any other similar accident with an obvious impact on railway safety regulation or the management of safety; 'extensive damage' means damage that can immediately be assessed by the investigating body to cost at least EUR 2 million in total (Directive 2001/14/EC)

G 3.1.2 Therefore a hazard is a condition that could lead to harm to people, assets or the environment.

G 3.1.3 Hazards can be expressed in various ways and at various levels of abstraction. The way a hazard is expressed has implications for the way it is understood; therefore hazards need to be described very carefully.

G 3.1.4 There is currently no universally agreed list of generic hazards for the railway system, although various lists and models do exist and are used by the GB mainline railway, and other railways.

G 3.1.5 An example list of generic railway system hazards relating to rolling stock operation is presented in Appendix A.

G 3.1.6 As hazards are conditions, they could have a number of different causes. For example the hazard 'train fails to stop at an intended location' could be caused by, amongst other things, brake failure, poor adhesion conditions or driver error. A robust and efficient approach to hazard definition is one where a clear distinction is made between hazards and causes. This helps to ensure that:

a) The number of hazards is kept to a manageable level.

b) A more effective link between the hazards and the accident outcomes can be made.

c) Individual causes can be effectively mitigated by lower level decision makers or actors in the project, while still allowing an understanding of overall system safety.

G 3.2 What is hazard identification?

G 3.2.1 Hazard identification is a vital step in risk assessment and risk management processes. It describes the process of systematically identifying hazards so that they – and the risk they create – can be controlled effectively. If hazards can be eliminated, for example by a changed design, then there is no further risk to control. This, therefore, is the preferred approach to hazard closure where possible. However, in many cases, hazards cannot be eliminated; thus the risk they create should be controlled to an acceptable level.

G 3.2.2 The regulation states that:

The proposer shall systematically identify, using wide-ranging expertise from a competent team, all reasonably foreseeable hazards for the whole system under assessment, its functions where appropriate and its interfaces. (Annex I, clause 2.2.1)

G 3.3 Approaches to hazard identification

G 3.3.1 There are various approaches to the systematic identification of hazards. Approaches are desk-based (typically involving an individual working alone to apply some structured analysis process), workshop based, or some combination of the two.

G 3.3.2 The approach or combination of approaches selected should be matched to the complexity and novelty of the proposed change. Further guidance related to technical systems is also available in Annex A of CLC/TR 50126-2:2007.

G 3.4 Desk-based approaches

G 3.4.1 There are various desk-based approaches to hazard identification. Perhaps the simplest is to review available data in order to identify which failures, incidents and hazards have occurred to similar systems in similar operational circumstances to those being analysed, using this information to infer what the relevant hazards for the system in question might be.

G 3.4.2 Desk-based analysis processes are typically variants of failure mode and effect analysis (FMEA). FMEA is a structured process to identify the potential failure modes of the elements of a system, the causes of these failures, and their effects. Failure modes are identified for each component, and the effects of each failure mode on larger assemblies and the whole system are identified. Some of these effects may include hazards. Failure modes, effects and criticality analysis (FMECA) are an extension of FMEA, in which the criticality of the failure effects is also considered.

G 3.4.3 FMEA and FMECA are rigorous and thorough, if applied by a competent analyst who understands both the technique and the system under analysis. However, they can be time consuming. Further guidance on both techniques is provided in BS EN 60812:2006.

G 3.4.4 A Functional Hazard Analysis (FHA) is a systematic, comprehensive examination of functions to identify and classify failure conditions of those functions according to their severity. For the analysis of a change to the railway, it may be appropriate to apply the FHA at system level. This would involve a high-level, qualitative assessment of the defined functions of the system (as specified in the system definition). The system-level FHA is undertaken to identify and classify the failure conditions associated with the system-level functions. FHA involves less work than FMEA/FMECA and can be started earlier, because a specification, and not a design, is all that is required. However, FHA is not good at finding hazards that are not easily characterised as the failure of a function (such as electromagnetic interference or fuel leakage).

G 3.5 Workshop-based approaches

G 3.5.1 The wording of the regulation quoted in G 3.2.2 implies a workshop-based approach to hazard identification, and there needs to be some collective approach to consideration of hazards, as this helps to ensure completeness. Appendix D gives general guidance on how to plan and undertake workshops, and how to use the outputs from them in the context of the regulation.

G 3.5.2 RUs and IMs commonly use workshop-based approaches to support hazard identification. The technique of a workshop helps to ensure the completeness of hazard identification by drawing on the collective experience and understanding of all the workshop attendees. There are various different approaches that can be applied, ranging from a structured Hazard and Operability (HAZOP) type study to a more informal ‘brainstorming’ exercise.

G 3.5.3 The HAZOP technique was initially developed to analyse chemical process systems, but was later extended to other types of systems and industries. A HAZOP is a qualitative technique for analysing a defined system by applying 'guide words' like 'no', 'more' or 'less than'. The guide words are applied to some attribute or intention of the system, in order to consider how it might fail and what the consequences of that failure might be. For example, if a point motor were being analysed, the guide words might be applied to the force exerted by it. As with FMEA, this is a thorough and systematic approach, but it can be time-consuming, and relies on there being a clear formal definition of the system and its elements. Guidance on undertaking HAZOPs may be found in BS IEC 61882:2001.

G 3.5.4 A more common approach is to undertake a structured brainstorming exercise. This can take on a variety of forms, but is typically a variation of the HAZOP approach, involving the analysis of a given system, set of functions and / or procedures using a checklist of some type. The checklist might be a set of potential causes of hazards, a list of known hazards, or a list of different operational scenarios and circumstances relevant to the system. An example of a checklist is given in Annex B to CLC/TR 50126-2:2007.

G 3.5.5 A typical way of conducting a workshop for the operational railway is to use a structured checklist approach to analyse the functions and operation of the railway for different 'phases of mission'. These 'phases of mission' might include 'train start-up', 'normal operation' or 'degraded mode working', for example.

G 3.5.6 To support this analysis, a description of the various functions and human actions that would need to occur would be produced. The workshop process then steps through these functions and actions in sequence, and uses an appropriate checklist(s) to identify hazardous deviations from the intended function or action. Various causes and consequences are then recorded. This approach is essentially a hybrid combination of task analysis and functional hazard analysis.

G 3.5.7 The outputs from an analysis of the type set out in G 3.5.5 to G 3.5.6 would be causes of the generic hazards. In order to structure these causes, and link them to the generic hazard list, it might be necessary to create sub-hazards. These sub-hazards would in effect be sub-types of the generic hazard to which they are linked.

G 3.5.8 The workshop process may incorporate the classification of hazards. Guidance in the classification of hazards in accordance with the requirements of the regulation is included in Part 3 of this document.

G 3.6 Human Factors assessment

G 3.6.1 Human Factors assessments can be particularly appropriate to the analysis of hazards associated with railway operations and the analysis of procedures. They can be either desk-based or workshop-based and can also be supported by observations at sites if systems are already in operation.

G 3.6.2 Although not a hazard identification method in itself, task analysis can be used as a way to describe tasks before they are systematically assessed by identifying potential deviations from procedure, as well as the causes and consequences of these deviations. Task analysis is a systematic method for describing a task in terms of its goals, operations and plans. The goal is what the system is required to achieve. The operations describe the actions or decisions performed by people interacting with the system, while the plans describe the conditions under which the operations are performed. Task analyses are often presented as written descriptions of the operations in a numbered sequence, or in the form of a flowchart.

G 3.6.3 To perform task analysis a certain level of data is required, such as the general operating procedure including job descriptions, process diagrams and / or the operating manual. If feasible, observation at site and input from staff may also be appropriate.

G 3.6.4 The benefit of a task analysis is that it provides an exhaustive description of operators' tasks. This type of analysis can be used as a basis for identifying (and potentially quantifying) human errors, analysing causal and contributory factors and consequences. The approach used to identify human errors is similar to the structured HAZOP process, in that it uses guide words to determine what errors could occur for each step identified in the task analysis.

G 3.6.5 Further guidance on task analysis can be found in Hierarchical Task Analysis (Shepherd, 2001). Further guidance on human error identification and quantification can be found in RSSB research project T270 (Railway Action Reliability Assessment: A technique for quantification of human error in the rail industry).

Part 4 Guidance on Hazard Classification

G 4.1 Requirements and approach

G 4.1.1 Hazard classification has a very particular meaning in the context of the regulation. It is based on an initial assessment of the risk associated with each hazard and is carried out as part of a hazard identification process.

G 4.1.2 However in related standards, such as BS EN 50126, classification has a broader use as an initial stage of risk assessment, incorporating the use of a risk matrix. Although not required by the regulation, guidance on this broader approach to hazard classification is provided in Appendix C: Classification using a risk matrix, should a project consider that it would benefit from use of this approach.

G 4.2 Meeting the requirements in the regulation

G 4.2.1 The regulation states that:

'To focus the risk assessment efforts upon the most important risks, the hazards shall be classified according to the estimated risk arising from them. Based on expert judgement, hazards associated with a broadly acceptable risk need not be analysed further but shall be registered in the hazard record. Their classification shall be justified in order to allow independent assessment by an assessment body.' (Annex I, clause 2.2.2)

G 4.2.2 Classification of hazards allows the proposer to focus subsequent risk assessment work on the most important risks, by discounting those hazards which need no further consideration at an early stage of the project. The actual classification of a hazard is made on the basis of expert judgement. In practice this is usually undertaken via the collective opinion of the attendees at a hazard identification workshop. A record of who attended the hazard identification workshop, or otherwise took part in the classification, will help demonstrate that the requirement to apply expert judgement has been met.

G 4.2.3 The regulation states that:

'As a criterion, risks resulting from hazards may be classified as broadly acceptable when the risk is so small that it is not reasonable to implement any additional safety measure. The expert judgement shall take into account that the contribution of all the broadly acceptable risks does not exceed a defined proportion of the overall risk.' (Annex I, clause 2.2.3)

G 4.2.4 A judgement that the risk is 'broadly acceptable' is needed. The ORR Guidance (Dec 2012) states:

'The Regulation uses the term 'broadly acceptable' to identify those hazards which need not be analysed further. In this context, 'broadly acceptable' applies to those hazards where the risk is, to all intents and purposes, insignificant or negligible. This could be because the hazard is so unlikely to arise that there are no feasible control measures that could be used to control the risk it creates (eg. earthquakes if in a low vulnerability area) or where there is a credible failure mode but the consequences are negligible. By screening out the 'broadly acceptable' hazards at this stage, the risk analysis can focus on the more important hazards to manage. It is unlikely that many hazards will be screened out in this way.' (Clause 3.15)

G 4.2.5 'Hazard Classification' as described in the regulation should therefore be thought of as a filtering exercise to remove those hazards that are judged to be of broadly acceptable risk.

G 4.2.6 The regulation also states that:

'The expert judgement shall take into account that the contribution of all the broadly acceptable risks does not exceed a defined proportion of the overall risk.' (Annex I, clause 2.2.3)

G 4.2.7 Given that the broadly acceptable risks are by definition very low, and that it would not be expected that many hazards would be discounted in this way, it is likely that the contribution of all broadly acceptable risks would be insignificant compared to the overall risk.

G 4.3 Broader approach to hazard classification

G 4.3.1 The broader approach to hazard classification referred to in section 3.2 might be beneficial in order to prioritise those hazards which:

a) Need to be considered in project option selection and decision making early in the project, when design options are still readily available or not cost prohibitive, in order to ensure that the project is doing all it can to reduce risk to an acceptable level.

b) Are likely to require significant project resources to control.

c) Need greater consideration of whether or not safety requirements reduce risk to an acceptable level. In general, the higher the risk of the hazard the more consideration will need to be given to the sufficiency of its associated safety requirements.

G 4.3.2 This need might therefore be associated with projects that are large in scale (such as a major engineering project) as this would tend to imply that there were a large number of hazards to consider and prioritise. Such projects might also incorporate sub-projects of various scale, type and novelty requiring a top level understanding of where the risks were greatest.

G 4.3.3 The use of such an approach might also be helpful where there is significant novelty, and as a starting point for risk assessment work to be undertaken later in the application of the risk management process. Further guidance to support the use of risk classification matrices in this way is given in Appendix C.

Appendix A Example Generic Hazard List: Rolling Stock Related Hazards

G A.1 Purpose of the generic hazard list

G A.1.1 The rolling stock related generic hazard list in this appendix is intended to:

a) Help start the hazard analysis process and avoid repetitive work.

b) Support a structured approach to hazard management.

c) Improve the efficiency and reduce the cost of safety analysis work.

G A.1.2 The regulation applies to changes to the railway system in its broadest sense. As a hazard is a 'state' of the railway the hazards contain no causal information. The scope of potential application of the list is very large and the causes of each hazard could be technical, operational and organisational in nature.

G A.2 Limitations on the use of the example

G A.2.1 It is stressed that, although these hazards relate to rolling stock, they are not defined at the level of the technical system (eg the rolling stock). Functional failures associated with rolling stock would be considered to be causes of these 'Railway System' level hazards. For example, 'Brake failure' would be one of the causes of RSH-35 'train fails to stop at intended location'. However, another cause of RSH-35 could be 'driver error' and this is external to rolling stock as a technical system.

G A.2.2 The example list is incomplete and should not be considered to be definitive. If anyone using this list identifies errors or omissions within it, then any feedback or suggestions would be welcomed.

G A.3 Example generic hazard list: rolling stock

Example generic hazards: rolling stock	Code
Projectile originating from train movement	RSH-1
Driver confused or distracted	RSH-2
Driver incapacitated	RSH-3
Person trapped inside train in an emergency	RSH-4
Driver or other staff member trip, slip or fall hazard entering or leaving cab	RSH-5
Excessive electromagnetic emissions from system	RSH-6
System has insufficient immunity from electromagnetic interference	RSH-7
Gap between train and platform	RSH-8
Gap between train and walkway	RSH-9
Excessive pressure in train	RSH-10
Exposure to arcing	RSH-11
Exposure to raised electrical potential	RSH-12
Exposure to biological / toxic substances	RSH-13
Exposure to corrosive / reactive substances	RSH-14
Exposure to noise	RSH-15

Guidance on Hazard Identification and Classification

Example generic hazards: rolling stock	Code
Exposure to vibration	RSH-16
Exposure to surfaces / liquids at extreme temperatures	RSH-17
Exposure to pressurised system / explosion	RSH-18
Exposure to exterior door closing / opening	RSH-19
Exterior door open whilst train moving	RSH-20
Exterior door opens off platform / wrong side	RSH-21
Potential for trap / cut hazard	RSH-22
Exposure to fire / smoke	RSH-23
Exposure to interior door closing/opening	RSH-24
Gauge infringement (train)	RSH-25
Insufficient warning of presence of train	RSH-26
Failure of train wheelset, bogie, or suspension	RSH-27
Detraining hazard	RSH-28
Person trapped in train doors	RSH-29
Potential for train surfing	RSH-30
Structural collapse of interior system / equipment	RSH-31
Person exposed to sudden train movement	RSH-32
Aerodynamic force created by train movement	RSH-33
Defective track	RSH-34
Train fails to stop at intended location	RSH-35
Train moves in wrong direction	RSH-36
Unauthorised train movement	RSH-37
Train not detected by railway infrastructure	RSH-38
Train overspeeds	RSH-39
Train unstable	RSH-40
Unwarranted train division	RSH-41
Potential for slip / trip / fall	RSH-42
Person too close to moving train	RSH-43
Person exposed to extreme temperature in train interior	RSH-44
Lack of adequate ventilation in train	RSH-45
Potential for manual handling injury	RSH-46
Inadequate structural integrity of train	RSH-47
Potential for assault	RSH-48
Rail vehicle falls/moves during maintenance	RSH-49
Pollution of environment	RSH-50
Potential for injury carrying out maintenance activities	RSH-51
Rail system functions cannot be correctly operated during emergencies	RSH-52
Inadequate life saving equipment provided	RSH-53
Exposure to contaminated food or water	RSH-54

Example generic hazards: rolling stock	Code
Cab ergonomics not optimized	RSH-55
Object on track	RSH-56
Driver fails to maintain proper lookout	RSH-57
Train overloaded	RSH-58

Appendix B Definition of Fatality and Weighted Injury (FWI)

G B.1 Background / introduction

G B.1.1 In order to quantify, compare and understand the impact of safety related incidents and risk the GB railway industry has adopted, by industry agreement, the scheme set out in the table below for relative weighting of different types of injury.

G B.1.2 This weighting was determined as an output of RSSB research project T440. This research made use of studies of what members of the public believe that it would be sensible for the industry to pay to put in place measures to prevent the occurrence of different types of risk. When the research was undertaken, definitions of different types of injury were taken from the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 1995, which was the key piece of legislation underpinning industry reporting at that time.

G B.1.3 Although the RIDDOR regulations have been updated since this work was undertaken the FWI definition still makes use of the definitions provided in RIDDOR 1995. This is to ensure that the FWI metric remains consistent over time, allowing changes in safety loss and risk to be monitored and compared over time.

Injury degree	Definition	Weighting	Ratio
Fatality	Death occurs within one year of the accident.	1	1
Major injury	Injuries to passengers, staff or members of the public as defined in schedule 1 to RIDDOR 1995. This includes losing consciousness, most fractures, major dislocations, loss of sight (temporary or permanent) and other injuries that resulted in hospital attendance for more than 24 hours.	0.1	10
Class 1 minor injury	Injuries to passengers, staff or members of the public, that are neither fatalities nor major injuries, and are defined as reportable in RIDDOR 1995[1] amended April 2012, and workforce injuries, where the injured person is incapacitated for their normal duties for more than three consecutive calendar days, not including the day of the injury.	0.005	200
Class 2 minor injury	All other physical injuries.	0.001	1000
Class 1 shock / trauma	Shock or trauma resulting from being involved in, or witnessing, events that have serious potential of a fatal outcome, for example train accidents such as collisions and derailments, or a person being struck by train.	0.005	200
Class 2 shock / trauma	Shock or trauma resulting from other causes, such as verbal abuse and near misses, or personal accidents of a typically non-fatal outcome.	0.001	1000

Table G B.1 Definition of Fatality and Weighted Injury

[1] RIDDOR refers to the *Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995*: a set of health and safety regulations that mandates the reporting of, *inter alia*, work-related accidents.

Appendix C Classification Using a Risk Matrix

This appendix provides guidance in the classification and use of a risk matrix.

G C.1 Principles

G C.1.1 The main advantages of using a risk matrix for hazard classification are that it:

a) Is an easily understandable representation of relative risk levels.

b) Can be applied relatively quickly.

c) Is readily understandable by those whose inputs and opinions are needed to apply it, who may not be risk specialists themselves.

d) Enables the combination of frequency and consequences to be represented in an intuitive visual way.

G C.1.2 Some rigour in the quantitative aspects of a risk matrix is desirable to support their use within an efficient and effective process.

G C.1.3 Risk in the context of safety can be defined as a measure of the fatalities and weighted injuries (FWIs) that are estimated to occur per year. It can be calculated as the product of how often an event is likely to occur per year (the event frequency) and the consequences (injuries, fatalities or incidents of shock / trauma) that could arise should an event occur, that is:

Frequency of an accident (resulting from a hazard)

for example, events / year

x

The consequences of the accident

for example, expected FWIs / event

=

Collective Risk

for example, expected FWIs / year

G C.1.4 The definition of FWIs is set out below in table G B.1.

G C.1.5 A risk matrix is two-dimensional, with the frequency of the accident resulting from the hazard occurring on one axis and the consequence of the accident (see Table G C.1). The risk is then expressed as a combination of the accident frequency and consequence as a result of the occurrence of the hazard. When used to support an application of the risk management process in Annex 1 of the regulation, the assessment would assume the presence of the safety requirements described in the system definition, as these would already have been specified. The risk matrix provides a reasonably quick and easy way to represent risk and consequently has been relatively widely used in many safety-critical industries.

G C.2 Calibration of a risk classification matrix

G C.2.1 As risk classification matrices are used for ranking and comparing the risk of different hazards, the matrix must be calibrated so that relative risk of different hazards is preserved across the various risk classifications. In the example of Table G C.1 this is achieved by having the same factor difference (a factor of 5) between each frequency and consequence category. The benefit of doing this is that similar rankings in different parts of the matrix equate to similar levels of risk; hence, hazards can reasonably be compared or aggregated.

Guidance on Hazard Identification and Classification

			Consequence (FWI)				
			Class 1 Minor injury / multiple Class 2 injuries	Multiple Class 1 minor injuries / more severe injury	1-2 Major injuries	Multiple major / single fatality	Multiple fatalities
Frequency			**1**	**2**	**3**	**4**	**5**
	Once in	**No/year**	**0.008**	**0.04**	**0.2**	**1**	**5**
5	**12 days**	**31.25**	6	7	8	9	10
4	**2 months**	**6.25**	5	6	7	8	9
3	**9 months**	**1.25**	4	5	6	7	8
2	**4 years**	**0.25**	3	4	5	6	7
1	**20 years**	**0.05**	2	3	4	5	6

Table G C.1 Example of a quantified, calibrated risk matrix

G C.2.2 The rankings are then added rather than multiplied, as this ensures that each number in the matrix equates to a similar level of risk. In other words, hazards ranked as the same risk classification equate to similar levels of risk regardless of the particular frequency or consequence category. For example:

Risk classification '7' could be estimated in the following two ways, each of which calculates the same FWI per year:

Risk classification '7' = Frequency category '5' + Consequence category '2'

= 31.25 events / year * 0.04 FWI / event

= 1.25 FWI / year

OR

Risk classification '7' = Frequency category '4' + Consequence category '3'

= 6.25 events / year * 0.2 FWI / event

= 1.25 FWI / year.

G C.2.3 When developing and calibrating a risk matrix of this type, the range of frequencies and consequences presented needs to be appropriate to the scale of risks associated with the set of hazards being classified. For example, the risk matrix shown in Table G C.1 would not be suitable for assessing the risk associated with a hazard which was estimated to lead to an accident on a weekly basis, as its most frequent category assumes a rate of occurrence of once every 12 days.

G C.2.4 When assigning frequency and consequence rankings to hazards, the classification is based on an assessment of the frequency with which a particular type of accident would occur as a result of the occurrence of the hazard, and the typical consequences associated with that accident. Therefore, in order to estimate the 'frequency' categorisation consideration is needed of both how likely the hazard is to occur (through consideration of its various causes), and how often the hazard would result in the occurrence of the accident.

G C.2.5 If the analyst specifies a large number of sub-hazards, or analyses individual hazard causes instead of hazards, this might lead to a flawed perception that hazard risk is not significant.

G C.2.6 The classification would typically be based on the credible worst case accident associated with the hazard, and its typical consequences. For some accidents, however, different outcomes can lead to significantly different consequences.

G C.2.7 For example, if the hazard were a broken rail, then the most significant resulting accident would be a derailment. The average consequences for this would typically only be a number of minor injuries, due perhaps to passengers falling over inside the train, whereas in extreme cases derailments can lead to multiple fatalities. It is recommended that in such cases, to get a better understanding of the risk associated with the hazard, two or more separate rankings of the hazard should be considered, as follows:

a) The first ranking should relate to the frequency and consequence of the typical (most frequent) outcome.

And

b) The second risk ranking should relate to the frequency and consequences of the realistic worst case outcome, if appropriate.

G C.2.8 This is shown diagrammatically in Figure G C.1, where it is assumed that, for a section of the railway, four 'broken rail' derailments occur every year. The classification uses the example matrix shown in Table G C.1. The ranking is based on the frequency and consequence of each outcome, given that the hazard has occurred.

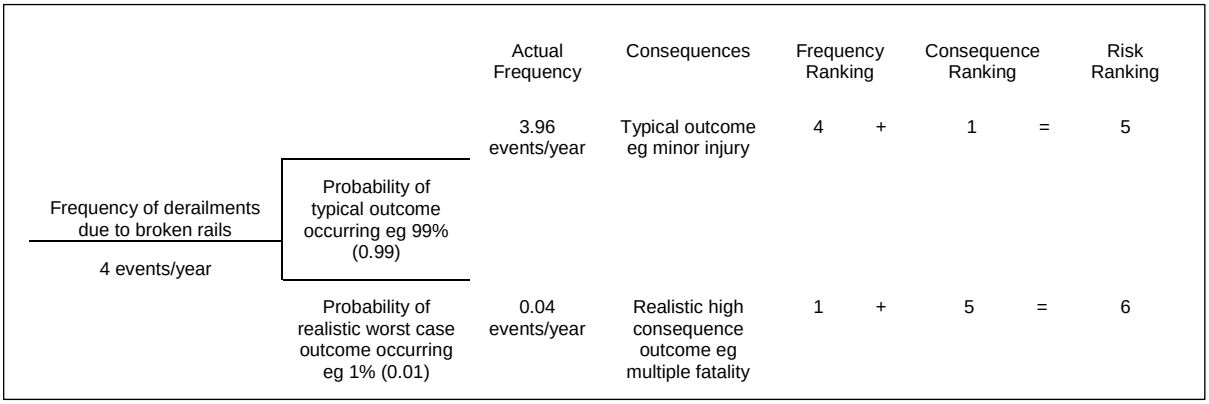

Figure G C.1 Example of risk classification for events with the potential for significantly different outcomes

G C.2.9 The overall classification for 'broken rail' as a hazard is therefore '6'. In the example shown in Figure G C.1, the outcome associated with the multi-fatality accident dominates the risk classification for the hazard, as it is approximately a factor of 5 higher.

G C.2.10 For some hazards, it may also be that a number of different types of outcomes are possible. For example, a failure of train brakes might lead to a collision or a derailment. In such cases, and where risks are potentially significant, a more detailed risk assessment may be needed using structured techniques such as fault tree analysis (BS EN 62502: 2011) or event tree analysis (BS EN 61025:2007).

G C.2.11 There may be a tendency to overestimate risk in a workshop environment when using the risk estimates from a risk classification matrix to support the optioneering of different safety measures. Safety measures often impact on a number of different hazards. As decisions about which safety measures to apply can involve trade-offs of risk, it is not always obvious whether the 'credible worst case' risk estimate or the 'most probable' risk estimate will err on the side of caution regarding the safety measures being considered.

Guidance on Hazard Identification and Classification

G C.2.12 For frequent, probable or even occasional events, the experience of individuals may well be a sufficient basis for an accurate judgement. To arrive at a classification involving the terms ‘remote’, ‘improbable’ or ‘incredible’ requires an extensive knowledge of data on failures and incidents and of historic accident rates, together with at least an appreciation of how the probability of unlikely events or combinations of events can be estimated.

G C.2.13 In order to support the understanding of the risk estimates made, and ensure that the estimates can be understood and interpreted at a later date, it is important to capture and record the rationale and basis of each risk classification. For example, the risk classification might state that a hazard classified using the matrix in Figure 2 as risk classification 6 (Frequency 5, Consequence 1) on the basis of historical accident data, or risk classification 5 (Frequency 1, Consequence 4) on the basis of personal experience and judgement of workshop attendees in the absence of data.

Appendix D Hazard Identification Workshops

G D.1 Introduction

G D.1.1 The wording of the regulation quoted in section G 3.2.2 implies a workshop-based approach. This appendix provides general guidance on how to plan, and undertake workshops and how to use the outputs from them in the context of the regulation.

G D.2 The key roles

G D.2.1 When undertaking a hazard identification workshop, there are key roles to be filled. The workshop chair is the person who will guide the workshop, and the application of the methodology that is to be followed. The workshop chair's role is to ensure that the workshop process that is to be followed (see section G D.4) is applied completely and at the right depth. There may be a tendency for HAZOP workshop attendees to digress from the process, or for discussions to become unfocussed. HAZOP chairing is a skill that has to be learnt over time, and selection of the chair is therefore critical to success.

G D.2.2 The workshop secretary's role is to record the discussion in an appropriate format (see G D.3.4). It would be expected that, prior to taking on a role as a workshop chair, an individual would have had extensive experience in the role of workshop secretary.

G D.2.3 The remaining attendees are the technical experts whose expertise is needed to analyse the hazards of the system. A common mistake is not to include relevant stakeholders from outside the organisation. The selection of technical experts is made with reference to the competencies needed to understand the safety issues and is therefore dependent on the system definition.

G D.3 Planning the workshop

G D.3.1 In order to plan for the workshop, a number of activities need to be undertaken. A checklist to help undertake the correct activities in set out in G.D.5.

G D.3.2 The hazard analysis should be based on a clear description and understanding of the system that is to be analysed and the precise change to be considered. Further guidance on system definition, for the purposes of supporting the application of the risk management process is given in GE/GN8641. It should be borne in mind that the purpose of the system description set out here is to support a systematic hazard analysis which identifies all 'reasonably foreseeable' hazards. The way in which the system is described and presented is therefore closely linked to the analysis process to be followed.

G D.3.3 When the scope of the analysis is understood, it should be possible to specify the ideal technical, operational or organisational competencies that need to be represented at the workshop. Specifying the competence requirements will provide a set of criteria to identify who should attend the workshop. In addition to the particular technical and operational competencies needed, expertise in safety analysis and conducting of hazard identification workshops is required (although it would be expected that these competencies would be met by the workshop chair and secretary).

G D.3.4 In order to undertake the analysis, the workshop secretary and chair should prepare a template file (typically a set of structured tables in a spreadsheet) to use to record the output of the analysis. The table structure should be closely aligned with the process to be followed at the workshop. For example, the order of the fields should follow the order of questions that will be asked of the attendees. Guide words might also be included as drop-down lists in the spreadsheet.

G D.3.5 It is advised that the workshop methodology, and the use of the proposed recording template, are trialled ahead of the workshop. If a methodology is not tested and refined in this way, it is possible that the analysis will prove unworkable in practice, either because the exercise does not actually elicit the required information or proves too complex or time-consuming. The trial could be as simple as the chair and secretary running through some example analysis, or it might involve a full 'dress rehearsal', with a sub-set of the experts attending, prior to launching into a programme of workshops. Work might also be done to fill record sheets in beforehand, getting the attendees to review them before they arrive.

G D.3.6 The trial exercise should help to determine appropriate timings for the exercise. In general no more than two consecutive days of workshops is recommended, as the hazard identification process can lead to mental fatigue. Undertaking a workshop over a full working day is also not recommended, unless there is plenty of time for comfort breaks.

G D.3.7 Pre-work might also include the use of available safety data to pre-populate part of the recording template. In any case, it is recommended that some analysis of available safety data be undertaken before the workshop and that the results of this analysis and / or the raw data are brought to the meeting in an appropriate format to support the analysis process. This is particularly important if the workshop process is to encompass hazard classification, as estimates of hazard frequency and consequence are very prone to error if not calibrated against some known data points.

G D.3.8 The work described above would result in a briefing note for the workshop. An outline of the essential contents of a briefing note is set out in Appendix D.

G D.4 Conducting the workshop

G D.4.1 Following introductions, and outline of the agenda, there should be a description of the system and / or change to the railway that is to be analysed. Typically, one or more of the technical experts in attendance would provide this, supported by the briefing note material and additional presentation materials. The objective of this technical briefing is not to describe the system and / or change at great length, but to bring the understanding of the key issues to the forefront of the attendees' minds to prepare them for the task at hand. There may be one or more of these technical briefings planned throughout the course of the day.

G D.4.2 Once the technical briefing is complete, the workshop chair should take the attendees through the methodology that is to be followed. It is useful to have a pre-prepared example, perhaps developed in the trial exercise, in order to explain the method clearly.

G D.4.3 The chair should then guide the attendees through the workshop process, while the secretary supports the process and records the output. It is common practice for the secretary's notes to be presented on a screen at the workshop, as they are produced to give the attendees a chance to review the notes being taken and edit them in real time.

G D.4.4 Typically, a workshop does not follow a linear path. Initially, progress might be slow as the experts get to grips with the workshop process being applied. However, progress generally increases to a point where it is very rapid. At some point in the day, though, the attendees may begin to lose motivation and find it hard to make further progress. Because of the mentally tiring nature of the work, comfort breaks are essential. These need to be planned to maximise the progress made though out the whole day. If energy levels are flagging, impromptu breaks may also be needed.

G D.4.5 A common problem is that often hazard identification workshops will identify a very significant number of hazard causes without specifically linking them to hazards or sub-hazards. In these circumstances a significant amount of post-workshop rationalisation would be required to link the identified causes to sub-hazards and hazards. Applying a structured approach to hazard identification and management at the outset of the project as outlined here, will minimise the chances of this happening.

G D.5 Checklist for preparing and running a hazard identification workshop

G D.5.1 To support the preparation of a hazard identification workshop the following checklist may be useful:

a) Before the workshop:

i) Is the scope of the hazard identification understood and documented?

ii) Are there clear objectives of the exercise?

iii) Is there an identified and competent hazard identification chair and secretary?

iv) Is there an identified person to provide the technical brief for the exercise?

v) Has the methodology been planned and tested?

vi) Have sheets for recording the output been prepared?

vii) Have the required competencies been documented?

viii) Has an appropriate venue been found with the necessary facilities?

ix) Has the availability of the attendees been checked? (generally no more than eight attendees is recommended).

x) Has the briefing note been circulated in sufficient time? (at least one week in advance) – See G.D.6 for a template.

b) On the day:

i) Has the venue been set up correctly and are the necessary facilities in place?

ii) Is there a mechanism to record attendance?

iii) Are their sufficient comfort breaks planned, including refreshments?

c) After the workshop:

i) Have the records been rationalised into a clear record of discussion and hazard identification outputs?

ii) Has the report been sent to all attendees?

iii) Does a review of attendees and their competencies meet the competence requirements specified? If not, what action needs to be taken?

G D.6 Workshop briefing note

G D.6.1 The minimum contents of the hazard identification workshop briefing note are:

a) Date and starting time of workshop.

b) Venue of workshop, including directions to the venue.

c) List of attendees.

d) Scope and boundaries of workshop (with exclusions).

e) Technical briefing material.

f) Workshop methodology, with associated agenda and timings.

g) Contact details of organisers.

Definitions

Actor

Any party which is, directly or through contractual arrangements, involved in the application of the risk management process.

Assessment body

An independent and competent person, organisation or entity which undertakes investigation to arrive at a judgment, based on evidence, of the suitability of a system to fulfil its safety requirements.

Assessment report

The document containing the conclusions of the assessment performed by an assessment body on the system under assessment.

Hazard

A system condition that could lead to an accident.

Hazard record

The document in which identified hazards, their related measures, their origin and the reference to the organisation which has to manage them are recorded and referenced.

Infrastructure manager (IM)

As defined in the ROGS 2006: *'infrastructure manager' means the person who—*

'(a) in relation to infrastructure other than a station, is responsible for developing and maintaining that infrastructure or, in relation to a station, the person who is responsible for managing and operating that station, except that it shall not include any person solely on the basis that he carries out the construction of that infrastructure or station or its maintenance, repair or alteration; and
(b) manages and uses that infrastructure or station, or permits it to be used, for the operation of a vehicle'. (Part 1, clause 2)

Proposer

As defined in the regulation:

''proposer' means the railway undertakings or the infrastructure managers in the framework of the risk control measures they have to implement in accordance with Article 4 of Directive 2004/49/EC, the contracting entities or the manufacturers when they invite a notified body to apply the 'EC' verification procedure in accordance with Article 18(1) of Directive 2008/57/EC or the applicant of an authorisation for placing in service of vehicles.' (Article 3, clause 11)

Railway system

The totality of the subsystems for structural and operational areas, as defined in Directives 96/48/EC and 2001/16/EC, as well as the management and operation of the system as a whole.

Railway undertaking (RU)

As defined in Directive 2001/14/EC, and any other public or private undertaking, the activity of which is to provide transport of goods and/or passengers by rail on the basis that the undertaking must ensure traction; this also includes undertakings which provide traction only.

Risk analysis

The systematic use of all available information to identify hazards and to estimate the risk.

Risk assessment

The overall process comprising a risk analysis and a risk evaluation.

Risk evaluation

A procedure based on the risk analysis to determine whether the acceptable risk has been achieved.

Safety measure

As defined in the regulation:

'A set of actions that either reduce the rate of occurrence of a hazard or mitigate its consequences in order to achieve and / or maintain an acceptable level of risk.' (Article 3, clause10)

Safety requirement

As used in this guidance: A characteristic of a system and its operation (including operational rules) necessary in order to deliver acceptable risk.

As defined in the regulation:

''safety requirements' means the safety characteristics (qualitative or quantitative) of a system and its operation (including operational rules) necessary in order to meet legal or company safety targets.' (Article 3, clause 9)

System

That part of the railway system which is subject to a change.

The regulation

The Common Safety Method on Risk Evaluation and Assessment. Commission Regulation (EC) No 352/2009 of 24 April 2009 on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of Directive 2004/49/EC of the European Parliament and of the Council.

References

The Catalogue of Railway Group Standards gives the current issue number and status of documents published by RSSB. This information is also available from www.rgsonline.co.uk.

RGSC 01	Railway Group Standards Code
RGSC 02	Standards Manual

Documents referenced in the text

RSSB documents

GE/GN8640	Guidance on Planning an Application of a CSM on Risk Evaluation and Assessment
GE/GN8641	Guidance on System Definition
GE/GN8643	Guidance on Risk Evaluation and Risk Acceptance
GE/GN8644	Guidance on Safety Requirements and Hazard Management
GE/GN8645	Guidance on Independent Assessment
GD-0001-SKP	Taking Safe Decisions – how Britain's railways take decisions that affect safety
Research project T270	Railway Action Reliability Assessment: A technique for quantification of human error in the rail industry
Research project T440	The weighting of non-fatal injuries: Fatalities and weighted injuries
Research project T955	Hazard analysis and risk assessment for rail projects

Other references

BS EN 60812:2006	Analysis techniques for system reliability. Procedure for failure mode and effects analysis (FMEA)
BS EN 61025:2007	Fault tree analysis (FTA)
BS EN 61508-1:2010	Functional safety of electrical/electronic/ programmable electronic safety-related systems. General requirements
BS EN 50126-1:1999	Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
BS EN 62502:2011	Analysis techniques for dependability. Event tree analysis (ETA)
BS IEC 61882:2001	Hazard and operability studies (HAZOP studies). Application guide
CLC/TR 50126-2:2007	Railway applications – the specification and demonstration of reliability, RAMs
EC No 352/2009	Commission Regulation on a Common Safety Method on risk evaluation and assessment
EU No 402/2013	Commission Implementing Regulation on a Common Safety Method for risk evaluation and assessment
ORR Guidance (Dec 2012)	ORR guidance on the application of the common safety method (CSM) on risk assessment and evaluation (December 2012)
Shepherd (2001)	Hierarchical Task Analysis, Taylor and Francis: London
S.I. 1995/3163	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (subsequently amended)

Other relevant documents

Other references

ERA/GUI/02-2008/SAF	European Railway Agency Collection of examples of risk assessments and of some possible tools supporting the CSM Regulation