GN

GE/GN8644
Guidance on Safety Requirements and Hazard Management

Issue One: June 2014
Rail Industry Guidance Note

Published by:

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

Guidance on Safety Requirements and Hazard Management

Issue record

Issue	Date	Comments
One	June 2014	This guidance was developed as part of the RSSB research project T955 and provides guidance on the application of the Common Safety Method on Risk Evaluation and Assessment required by Commission Regulation (EC) No 352/2009.

Superseded documents

This Rail Industry Guidance Note does not supersede any other Railway Group documents.

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) when applying the CSM RA to formulate safety requirements, comply with them, demonstrate compliance and manage hazards.

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 05 March 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.

Guidance on Safety Requirements and Hazard Management

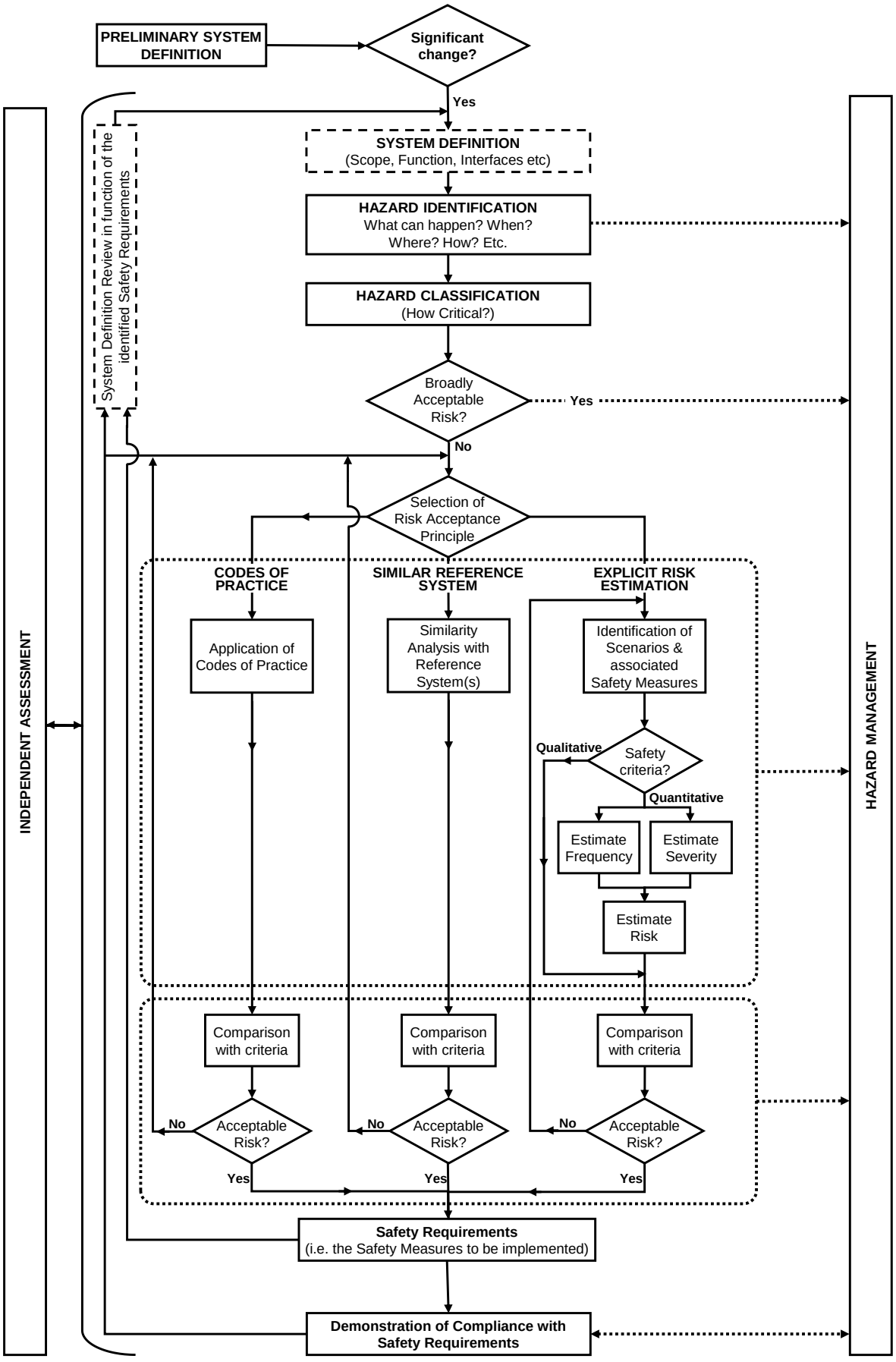

Figure 1 The risk management and independent assessment process from the CSM RA

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).

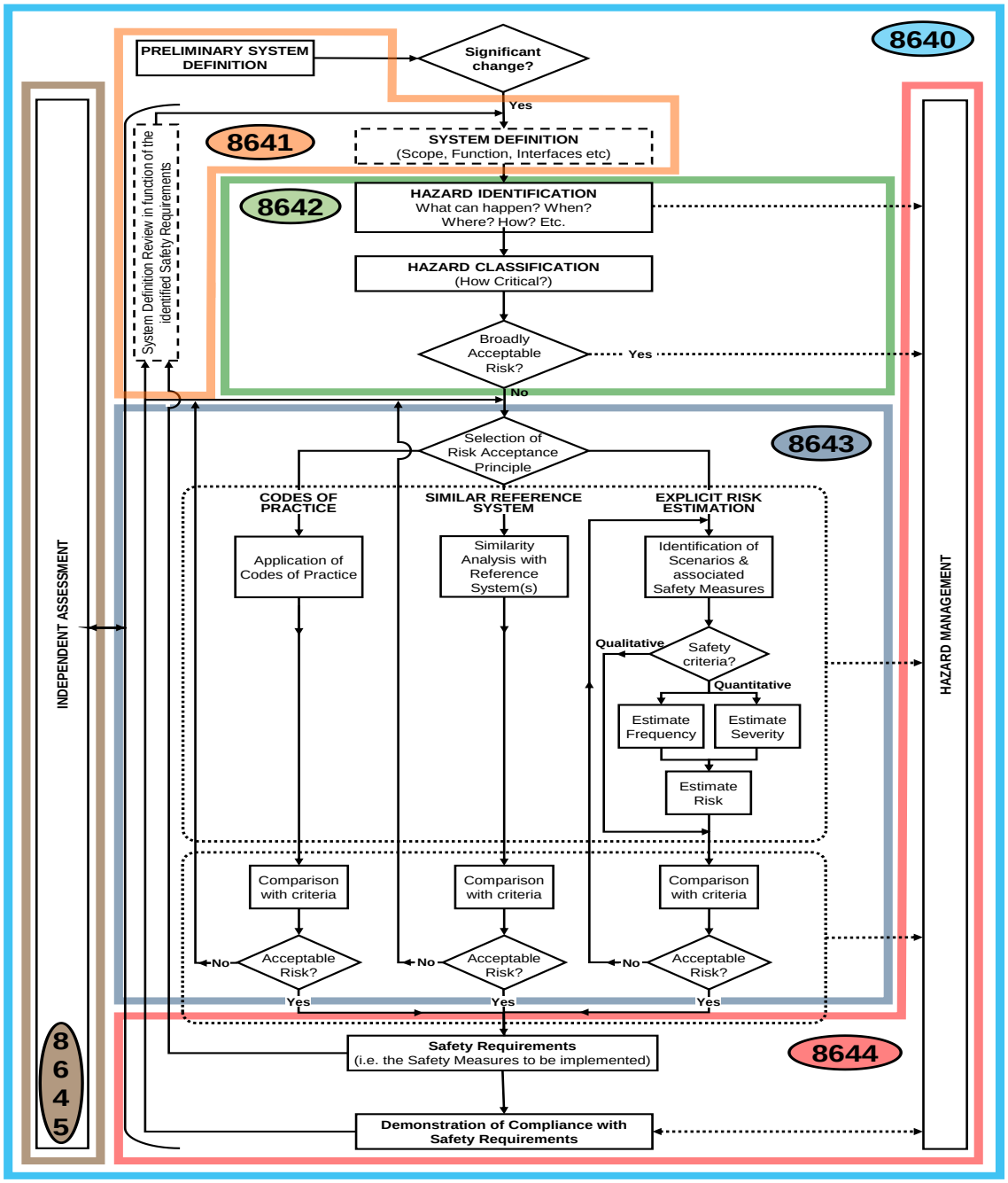

Figure 2 The set of guidance notes on the application of the CSM RA, and the process elements to which they relate

Part 3 Guidance on Safety Requirements and Hazard Management

G 3.1 Introduction to safety measures and safety requirements

G 3.1.1 The concepts of 'safety measures' and 'safety requirements' are key to the application of the risk management process. Safety measures are defined in the regulation as:

'a set of actions either reducing the rate of occurrence of a hazard or mitigating its consequences in order to achieve and/or maintain an acceptable level of risk.'
(Article 3, clause 10)

G 3.1.2 In the regulation in general, safety measure is a broad term, encompassing measures that are in place prior to the proposed change, new measures which might be considered for application, and also the safety measures that become formal safety requirements following the application of risk acceptance principles (see GE/GN8463).

G 3.1.3 The formal definition and use of safety requirements in the regulation is less clear:

''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 3)

G 3.1.4 However, in places in the regulation safety requirements are strongly implied to be a type of safety measure. For example, the regulation states:

'The application of these risk acceptance principles shall identify possible safety measures which make the risk(s) of the system under assessment acceptable. Among these safety measures, the ones selected to control the risk(s) shall become the safety requirements to be fulfilled by the system.' (Annex I, clause 2.1.6)

G 3.1.5 Also, the diagram describing the risk management process describes safety requirements as 'safety measures to be implemented'.

G 3.1.6 Any change often has technical, organisational and operational aspects and therefore safety requirements may be very different in nature. Safety requirements may include requirements on the technical system, but also requirements on the operational and maintenance arrangements.

G 3.1.7 Where the change affects organisational arrangements, the safety requirements are likely to be concerned with features of those arrangements, training, communications and transitional arrangements.

G 3.1.8 Some safety requirements may have to be met by other actors. For example, if an RU is introducing a new fleet of electric trains which will implement regenerative braking for the first time on a route, then the IM may have to make adjustments to the power supplies and to its operational maintenance arrangements to make the change acceptably safe. The regulation states that:

'Prior to the safety acceptance of the change, fulfilment of the safety requirements resulting from the risk assessment phase shall be demonstrated under the supervision of the proposer.

'This demonstration shall be carried out by each of the actors responsible for fulfilling the safety requirements, as decided in accordance with point 1.1.5.'
(Annex I, clauses 3.1 and 3.2.)

G 3.1.9 It is therefore the proposer's responsibility to demonstrate that all safety requirements have been met, regardless of who is actually responsible for fulfilling them.

G 3.2 Introduction to hazard management

G 3.2.1 The regulation states:

'The iterative risk assessment process can be considered as completed when it is demonstrated that all safety requirements are fulfilled and no additional reasonably foreseeable hazards have to be considered.' (Annex I, clause 2.1.7)

G 3.2.2 The risk management process in Annex I of the regulation can be regarded as a process of identifying all hazards and then moving them all to closure. A hazard is closed when there is demonstrable evidence that the safety requirements have been met.

G 3.2.3 The hazard record is used to track progress towards the closure of hazards. There is a an established practice in safety management of maintaining documents to track the progress of hazards in this way. Other names that have been used for such documents are hazard log and risk register. The hazard record is fundamentally the same as these and, if an IM or RU has existing processes and tools for tracking hazards, it may find that minimal change to them is needed to align with the requirements of the regulation.

G 3.2.4 The hazard record is a key output once the application of the risk management process is complete as it provides evidence that safety requirements have been met, and hence that the hazards have been closed.

G 3.3 Documenting safety requirements

G 3.3.1 The regulation requires that the safety requirements be recorded in the system definition and referenced in the hazard record. The regulation also requires that the system definition be kept up to date as the project proceeds so the phrase 'system definition' should not be thought to refer to a document which is frozen early in the project. Guidance on the format and structure of a system definition is given in GE/GN8641.

G 3.3.2 Some parts of the system definition may be formatted as a document but this does not imply that the safety requirements may not be stored in a database. Where a project is complex, and there are a significant number of safety requirements, storing them in a database may significantly reduce the overheads involved in managing them, and may help to keep the safety requirements up to date as the project proceeds.

G 3.3.3 The extent to which existing safety measures need to be formally documented as safety requirements is not clear in the regulation. A proportionate, risk-based approach to documenting these as safety requirements is suggested. For example, if existing management or monitoring arrangements are in place to ensure that certain safety measures are in place (for example, through a duty holder's safety management system), then it may be that the safety measures need only be documented by reference to the existence of these arrangements.

G 3.3.4 If safety requirements are being stored in a database, then storing existing safety measures in a separate table within the same database may make it easier to obtain a full picture of all the safety measures in place.

G 3.3.5 Safety requirements may include any of the following:

a) Requirements to implement features of functions of technical systems associated with the change.

b) Requirements to deliver minimum levels of integrity for functions of technical systems.

c) Requirements on the operational arrangements, such as provision of user manuals, provision of driver training, updates to operational procedures and restrictions on use.

d) Requirements on the maintenance arrangements, such as provision of tools, spares, special equipment and maintainer training, and inclusion of certain checks within maintenance procedures.

e) Any temporary restrictions introduced for an initial period of operation to control risk while assumptions about the behaviour of the system are being confirmed.

G 3.3.6 Safety requirements may include measures taken by other parties, as set out in G 3.1 above.

G 3.3.7 If one or more codes of practice are being used as a basis for controlling a hazard, then clause 2.3.5 of Annex I of the regulation requires that the use of these codes of practice shall be registered as safety requirements. Adding a requirement that 'the system shall conform to <code of practice>' would comply with the regulation. It may, however, facilitate more efficient implementation if the requirements in the individual clauses of the code of practice are entered as individual safety requirements, for example where the scope of the code of practice is very broad or where alternatives are permitted.

G 3.3.8 A good requirement should be accurate, unambiguous, achievable and testable. Where a requirement actually specifies more than one thing which may be checked at different times, it should make it easier to manage the requirement if that requirement is split into multiple requirements. It may save time to keep a note of the reasons for introducing a requirement, in case a need should arise to consider changing it in the future. This may be done by storing with a requirement the cross-references to documents containing the rationale for the requirement. Systematic cross-referencing of this sort is often referred to as 'traceability' and some databases can assist with the process of storing and maintaining traceability.

G 3.4 Complying with safety requirements and demonstrating compliance

G 3.4.1 The regulation requires that:

'Prior to the safety acceptance of the change, fulfilment of the safety requirements resulting from the risk assessment phase shall be demonstrated under the supervision of the proposer' and that 'This demonstration shall be carried out by each of the actors responsible for fulfilling the safety requirements […].' (Annex I, clauses 3.1 and 3.2)

G 3.4.2 The proposer is responsible for ensuring that compliance with all safety requirements is demonstrated, and for gathering together the necessary evidence that this is the case, but not necessarily for producing such evidence.

G 3.4.3 Compliance with a safety requirement may be demonstrated by testing, inspection, analysis or some combination thereof.

G 3.4.4 It may save time and money if the proposer of a change plans out, at a high level, how compliance with a safety requirement will be demonstrated shortly after the proposer writes down the safety requirement, because this planning may reveal imprecision in the requirement, or problems with demonstration, at an early stage when the issues are easier to correct (see GE/GN8640).

G 3.4.5 Compliance with some safety requirements may be demonstrated by standard project processes. To avoid introducing unnecessary activities it is advisable to review these processes and take account of all existing demonstration activities before introducing new ones.

G 3.4.6 When a proposer's suppliers carry out demonstration on its behalf, then the proposer should agree with them what sort of records they provide to it so that it can carry out the supervision which the regulation requires. It may agree with them that they will provide it with copies of the detailed records. However, where these records are extensive and the supplier can show that they have robust demonstration processes, the proposer may agree with them that they will just supply a summary of the results recorded in a 'certificate of compliance' or similar.

G 3.4.7 Demonstration records should record the versions of the items that were tested, inspected or analysed so that, when a change is made to the system, it is possible to work out what demonstration activities should be repeated. A demonstration activity should be repeated if the change might affect its outcome.

G 3.4.8 The regulation also requires that:

'The approach chosen for demonstrating compliance with the safety requirements as well as the demonstration itself shall be independently assessed by an assessment body.' (Annex I, clause 3.3)

G 3.4.9 Complete and sufficient evidence is needed in order to support this assessment. There are other good reasons for keeping good records, including helping to diagnose problems that occur in the field.

G 3.4.10 The proposer and the assessment body should agree in advance the level of visibility of demonstration activities that are required. In some cases audit activity might encompass the witnessing of some tests and in others review of the records alone will be deemed sufficient (see GE/GN8645).

G 3.5 Managing safety requirements

G 3.5.1 Where a safety requirement is implemented and compliance with it is demonstrated as planned, then there is little further management required. However, it will probably assist the management of the project if the proposer of a change (and, where necessary, its suppliers) tracks the progress towards demonstrating compliance with the safety requirements. This may be achieved in a table which shows how compliance with each requirement will be demonstrated and whether compliance has been achieved.

G 3.5.2 A hazard record produced according to the template set out in Appendix A may be used for this purpose. Alternatively, if the safety requirements have been stored in a database, then additional tables within the same database may be used to record the status of compliance with the safety requirements.

G 3.5.3 Issues of three types may arise after safety requirements have been formulated:

a) The safety requirements are found to be inadequate.

b) It is found that one or more safety requirements will not be implemented.

c) A safety requirement is based upon an assumption that requires confirmation.

Each issue is treated in turn.

G 3.5.4 The regulation requires that:

'Any inadequacy of safety measures expected to fulfil the safety requirements or any hazards discovered during the demonstration of compliance with the safety requirements shall lead to reassessment and evaluation of the associated risks by the proposer […]. The new hazards shall be registered in the hazard record […].' (Annex I, clause 3.4)

G 3.5.5 If the proposer finds out that the safety measures are inadequate, it is necessary, in order to put things completely right, to go back to the point in the risk management process where the inadequacy was introduced and restart the process there, updating the hazard record, safety requirements and other outputs, as necessary.

G 3.5.6 Safety requirements may be formulated on the basis of assumptions. The regulation requires that these should be recorded in the system definition. If safety requirements are stored in a database, then it may make sense to store assumptions in another table in the same database so that links between the two tables may be easily maintained. A hazard record produced according to the template set out in Appendix A may also be used to support tracking of assumptions.

G 3.5.7 The regulation requires that:

'For the system under assessment, any actor who discovers that a safety measure is non-compliant or inadequate is responsible for notifying it to the proposer, who shall in turn inform the actor implementing the safety measure.

'The actor implementing the safety measure shall then inform all the actors affected by the problem either within the system under assessment or, as far as known by the actor, within other existing systems using the same safety measure.

'When agreement cannot be found between two or more actors it is the responsibility of the proposer to find an adequate solution.' (Annex I, clauses 1.2.3, 1.2.4 and 1.2.5)

G 3.5.8 If it is found that one or more intended safety requirements will not be implemented, then the proposer should co-ordinate the parties involved to agree a resolution which may result in new hazards and / or new safety requirements, and should repeat the relevant parts of the risk evaluation process to confirm that the risk associated with all hazards is acceptable.

G 3.5.9 Where the validity of a safety demonstration is dependent on the assumptions made, the validity of these assumptions needs to be checked.

G 3.6 The hazard record

G 3.6.1 The regulation requires that:

'The proposer in charge of the risk management process required by this Regulation shall maintain a hazard record […].' (Annex I, clause 1.1.3)

G 3.6.2 Sometimes risks may be managed by multiple actors and, therefore, the proposer's hazard record may be supported by other hazard records maintained by other actors. The co-ordination arrangements needed in order to deal with this are set out in G 3.8.

G 3.6.3 Further detail is set out in clauses 4.1.1 and 4.1.2 of Annex I of the regulation, which requires that one or more hazard records should be maintained to track hazards, safety measures and assumptions throughout the project before being handed over to the IM or RU in charge of the operation of the system under assessment at the end of the project.

G 3.6.4 A hazard record contains information about each record and may be considered as a very large table with a row for each hazard and columns for the different sorts of information that is kept for each hazard. A template in Appendix A sets out suggestions for a set of column headings.

G 3.6.5 The table may be maintained using a database, spreadsheet or word processing tool. The former is recommended where there are more than a few dozen hazards.

G 3.6.6 The hazard record contains information that will continue to be useful to managing the hazards after the change is complete.

G 3.6.7 Where actors have been maintaining separate hazard records, then the records will usually be handed over to the proposer at the appropriate point in the project.

G 3.6.8 It is normal within RUs and IMs that project organisations are organisationally separate from the departments that carry out railway operations. Typically, at the end of a project, the proposer's project organisation hands over its hazard record, after incorporating information from any suppliers' hazard records to other parts of the proposer's organisation.

G 3.6.9 When a hazard record is handed over to another party, it may assist the recipient if information which was relevant to the project but is not relevant to the rest of the asset life cycle is removed first, for example the names of the people who took actions may be of no value to the recipient.

G 3.6.10 The regulation states:

'…once the system has been accepted and is operated, the hazard record shall be further maintained by the infrastructure manager or the railway undertaking in charge with the operation of the system under assessment as an integrated part of its safety management system.' (Annex I, clause 4.1.1)

G 3.6.11 The hazards in the project hazard record will need to be integrated into a safety management system. Therefore, consideration should be given to structuring the records in such a way as to facilitate this integration. This supports transfer of knowledge and understanding of the risks into the operational railway.

G 3.7 Managing hazards

G 3.7.1 Hazards can be considered to progress through a 'life cycle' or a series of states. An example hazard life cycle is shown in Figure 3. The ovals represent the states and the arrows depict possible transitions between states.

G 3.7.2 The meaning of each state is as follows:

a) Open: the initial status assigned immediately after a hazard has been identified.

b) Controlled: the risk evaluation process has been completed and safety requirements have been established which are sufficient to control risk to an acceptable level.

c) Cancelled: the potential hazards have been determined not to be an actual hazard or to be wholly contained within another hazard so no further action is necessary.

d) Transferred: the hazard has been transferred to another actor who now takes the lead in delivering the associated safety requirements for controlling the risk of the hazard. The proposer retains responsibility for managing the hazard.

e) Closed: compliance with all safety requirements related to the hazard has been demonstrated and any other actions associated with the hazard have been satisfactorily completed and so no further action is required.

G 3.7.3 Sometimes, as set out in the next section, it may require activity from more than one actor to move a hazard from 'Open' to 'Closed'.

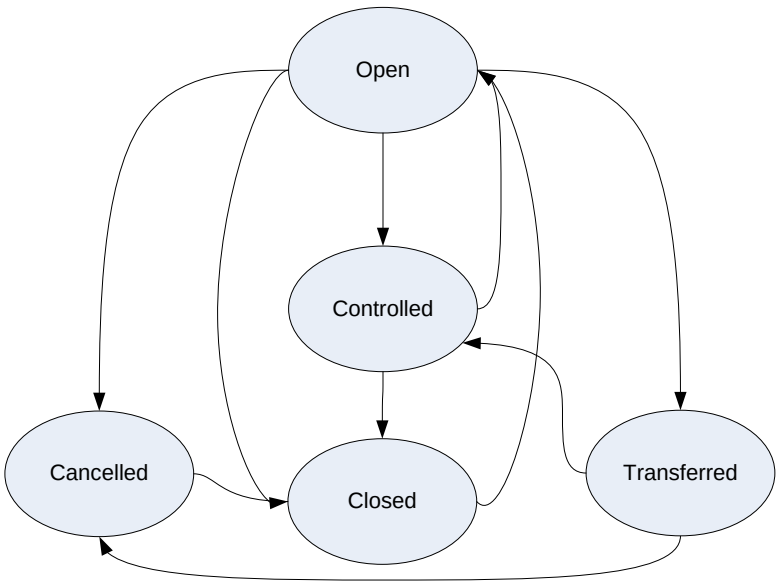

Figure 3 An example hazard life cycle

G 3.7.4 There is a 'Transferred' state in this life cycle because sometimes risks may be managed by multiple actors managing multiple hazard records. The co-ordination arrangements needed in order to deal with this are set out in G 3.8.

G 3.7.5 The information in the hazard record is essential to the management of risk and therefore care should be taken to ensure that it is accurate. Typically, only a small number of people will have permission to update the hazard record.

G 3.7.6 Maintaining a log of the changes made to the hazard record and the reasons for each change, and archiving previous versions of the hazard record, is beneficial because it makes it easier to diagnose and correct any errors that are made when updating the hazard record. If a database is being used to hold the hazard record, then it may be possible to maintain a change history using the database tools journal facility. If not, it may be maintained as a separate part of the hazard record.

G 3.7.7 An up-to-date version of the hazard record should be made available to all the actors responsible for controlling the hazards.

G 3.8 Involving others

G 3.8.1 Railways are strongly interconnected networks of systems and it is often the case that a proposer of a change will not be able to make that change safe through its own efforts alone. Generally, other actors will need to take action as well.

G 3.8.2 The regulation requires that:

'For each interface relevant to the system under assessment and without prejudice to specifications of interfaces defined in relevant TSIs, the rail-sector actors concerned shall cooperate in order to identify and manage jointly the hazards and related safety measures that need to be handled at these interfaces. The management of shared risks at the interfaces shall be coordinated by the proposer.' (Annex I, clause 1.2.1)

G 3.8.3 In order to discharge these responsibilities, the proposer of a change should set up arrangements for:

a) Exchanging information about hazards and related safety requirements (where identified) with other actors involved in the change.

b) Ensuring that information that should be passed to another actor is passed on promptly.

c) Ensuring that information passed to it by another actor, and which requires action, is acted upon promptly.

G 3.8.4 In the railway industry there are a number of clearly defined roles and responsibilities and therefore some organisational interfaces that typically arise. In all cases the responsibility for the necessary co-ordination remains with the proposer. The regulation requires that:

'All hazards and related safety requirements which cannot be controlled by one actor alone shall be communicated to another relevant actor in order to find jointly an adequate solution. The hazards registered in the hazard record of the actor who transfers them shall only be 'controlled' when the evaluation of the risks associated with these hazards is made by the other actor and the solution is agreed by all concerned.' (Annex I, clause 4.2)

G 3.8.5 Ultimately it is the IM or RU that implements the change on the railway. Co-ordination of arrangements to meet safety requirements associated with the operation and maintenance of the railway is typically between these actors. The proposer may need another actor, typically another RU or IM, at a shared interface, to implement the safety requirement. In this case the proposer should:

a) Make the other actor aware of the relevant hazards identified and agree with them any additional safety measures needed to control the hazard risk.

b) Enter the relevant information in the hazard record, and system definition.

c) Maintain an appropriate dialogue with the other actor for the duration of the project.

d) Gather evidence that the safety measures have been met, at appropriate points in the project life cycle.

G 3.8.6 A manufacturer of a technical system might also be a proposer. There are two broadly different approaches.

G 3.8.7 Firstly, the design and engineering of the system might be quite separate from the requirements of a specific project. Based on certain operational assumptions, the manufacturer would apply the risk management process to derive safety measures outside of their direct control. Actors who then wish to use the system being manufactured would need to implement those measures (these are sometimes referred to as application conditions). The operational environment assumed would tend to be based on commercial considerations and the potential use of the system. A subsequent application of the regulation would then be required by the RU or IM as proposer. The RU or IM putting the system into use would:

a) Consider the appropriateness and sufficiency of each safety requirement to their project.

b) Implement the safety requirement.

c) Supervise the demonstration of compliance with the safety requirement.

d) Keep the system definition and hazard record up-to-date (that is, include any additional hazards or hazard causes associated with the requirement, as appropriate).

G 3.8.8 Secondly the RU or IM might have a stronger influence on the design of the technical system, and work with the manufacturer to develop a system as an integrated part of its change project. In this case, one or more safety requirements and / or hazards would be passed to the manufacturer. In this instance, the proposer should:

a) Instruct the manufacturer to implement the necessary parts of the risk management process, including maintaining a hazard record.

b) Agree the transfer of the safety requirements, and reflect that in the system definition and hazard record.

c) Discuss the transfer of hazards with the supplier and jointly agree an adequate solution.

d) Supervise the demonstration of compliance with the safety requirements.

e) Keep the system definition and hazard record up-to-date.

G 3.8.9 There are variations in the above arrangements; however, the same principles of communication and co-ordination hold. For example, suppliers to RUs and IMs may deliver a wide range of services, not just that of providing technical systems.

G 3.8.10 Even where the change being made includes the introduction of a technical system, then the ‘system’ referred to will include other things that need to change at the same time, such as operational and maintenance arrangements. Safety requirements may include requirements on the technical system, such as a requirement for a certain braking performance and reliability when introducing a new train, and also the following:

a) Requirements on the operational arrangements, such as provision of user manuals, provision of driver training, use of particular operational procedures and restrictions on use.

b) Requirements on the maintenance arrangements, such as provision of tools, spares, special equipment and maintainer training, and inclusion of certain checks within maintenance procedures.

c) Any temporary restrictions introduced for an initial period of operation to control risk while assumptions about the behaviour of the system are being confirmed.

G 3.9 Forthcoming changes to the regulation

G 3.9.1 A revised CSM RA has been published 'European Commission. Regulation 402/2013 on the common safety method for risk evaluation and assessment', which came into force on 23 May 2013. Therefore, a proposer may use the revised CSM RA if they wish. The revised CSM RA will apply from 21 May 2015; this is the date on which the revised CSM RA must be used.

G 3.9.2 The revised regulation introduces an output that is produced by the proposer at the end of the CSM RA process. This is a declaration by the proposer that the risks are acceptable, the revised regulation requires a:

'*Declaration by the proposer*

'Based on the results of the application of this Regulation and on the safety assessment report provided by the assessment body, the proposer shall produce a written declaration that all identified hazards and associated risks are controlled to an acceptable level.' (402/2013 Article 16)

Appendix A Hazard Record Template

G A.1 Introduction to the hazard record template

G A.1.1 The regulation places the following requirements on the contents of a hazard record:

'The hazard record shall include all hazards, together with all related safety measures and system assumptions identified during the risk assessment process. In particular, it shall contain a clear reference to the origin and to the selected risk acceptance principles and shall clearly identify the actor(s) in charge of controlling each hazard.'
(Annex I, clause 4.1.2)

G A.1.2 Section G.A.2 shows an example of the typical contents of the hazard record. Not all the elements will need to be completed for all hazards (for example, if a hazard is broadly acceptable, then information on safety requirements is not necessary).

G A.1.3 The asterisks below identify those hazard record fields that are mandatory.

G A.2 The hazard record template

Hazard identifier		A unique identifier for the hazard. The identifier should not be changed or reused. If the hazard record is maintained in a database, this may be assigned automatically.		
Hazard title *		A short description of the hazard, which is meaningful enough to convey the essential nature of the hazard to the reader.		
Hazard description *		A longer description of the hazard, which is sufficiently precise that one could take any potential state of the system and its environment and say whether the hazard was exhibited or not.		
Hazard consequence		The ultimate accident consequences of the hazard. It is important to also document the critical events that will result in the escalation of the hazard consequences, as safety requirements to minimise the rate of occurrence of these events might be necessary (as well as mitigation of accident consequences).		
Hazard causes		Each hazard might have a number of different causes. Many safety requirements would map to the hazard at the causal level.		
Origin *		The activity that resulted in the identification of the hazard.		
	Broadly acceptable	'Yes' or 'No'. Where the answer is yes, a justification of the reasons for the decision.		
	Risk ranking	The overall results of ranking the hazard, including the hazard frequency and consequence. For guidance on classifying hazards, see GE/GN8642.		
State*		An indication of the state of the hazard towards closure. A suggested list of status would be open, controlled, cancelled, closed or transferred. These are defined in section G 3.7. The state of the hazard will be related to status of the individual safety requirements.		
Risk evaluation principle(s) *		The risk acceptance principle or principles being used to accept the hazard. It might be that principles need to be associated to specific causes.		
Risk evaluation documents		References to any documents containing further information about the risk evaluation of this hazard.		
Existing safety measures*		A list, possibly empty, of existing safety measures that act to control the risk associated with this hazard.		
Safety requirements *		Details (see below) of any safety requirements associated with the hazards.		
	Requirement	A reference, typically, identifier and title, to a safety requirement (which will be defined in the system definition, see GE/GN8641).		
	Actor Responsible *	The 'actor', which will typically be an organisation / person assigned responsibility for managing the hazard. This will be the proposer unless and until transferred to another actor, as set out in clause 1.2.2 of Annex I of the regulation.		
	Demonstration method	The means by which compliance with the safety requirement has been demonstrated or will be demonstrated, typically, by reference to a test or survey activity.		
	Demonstration state *	An indication of whether or not compliance with the safety requirement has been demonstrated.		
	Demonstration evidence	References to any documents, such as test reports, containing further information about the demonstration of this safety requirement.		
Assumptions *		System assumptions identified during the risk assessment process.		
Other actions		Details (see below) of any actions that have been taken to progress the hazard but which are not concerned with implementing safety measures, for example, actions to confirm assumptions.		
	Action	A description of the action.	**Responsible**	The person responsible for completing the action.
	Target date	The target date for completion of the action, if not complete.	**Status**	An indication of whether or not the action has been completed.
Notes		Any other information about the hazard considered useful to the users of the hazard record.		

Definitions and Abbreviations

Actor

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

Code of Practice

As defined in the regulation:

'A written set of rules that, when correctly applied, can be used to control one or more specific hazards.' (Article 2, clause 19),

The set of rules may be made up of specific clauses from one or more standard, relevant to the control of that hazard.

CSM RA '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.

ESM

Engineering Safety Management.

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 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 Integrity Level (SIL)

One of a number of defined discrete levels for specifying the safety integrity requirements of functions and systems.

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, clause 10)

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.

Technical system

As defined in the regulation:

means a product or an assembly of products including the design, implementation and support documentation; the development of a technical system starts with its requirements specification and ends with its acceptance; although the design of relevant interfaces with human behaviour is considered, human operators and their actions are not included in a technical system; the maintenance process is described in the maintenance manuals but is not itself part of the technical system (Article 3, clause 22)

TSI

Technical Specification for Interoperability.

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 of an Application of the Common Safety Method on Risk Evaluation and Assessment
GE/GN8641	Guidance on System Definition
GE/GN8642	Guidance on Hazard Identification and Classification
GE/GN8643	Guidance on Risk Evaluation and Risk Acceptance
GE/GN8645	Guidance on Independent Assessment

Other references

(EC) No 352/2009	Commission Regulation on a Common Safety Method on risk evaluation and assessment (2009)
(EU) No 402/2013	Commission Regulation on a Common Safety Method for risk evaluation and assessment (2013)
ORR Guidance (Dec 2012)	ORR guidance on the application of the common safety method (CSM) on risk assessment and evaluation (December 2012)
ROGS 2006	Railways and Other Guided Transport Systems (Safety) Regulations 2006

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