GN

GE/GN8643
Guidance on Risk Evaluation and Risk Acceptance

Issue Two: June 2014
Rail Industry Guidance Note

Published by:

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

Guidance on Risk Evaluation and Risk Acceptance

Issue record

Issue	Date	Comments
One	September 2012	This document gave guidance on reducing risk (previously found in the Yellow Book Issue 4) and identifies where the guidance is out-of-date or should be treated with caution.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Superseded documents

The following Rail Industry Guidance Note is superseded, either in whole or in part as indicated:

Superseded documents	Sections superseded	Date when sections are superseded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/GN8643 issue one Guidance on Reducing Risk	All	07 June 2014

GE/GN8643 issue one Guidance on Reducing Risk, is withdrawn as of 07 June 2014.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 evaluating risk and in deciding whether or not to accept risk, when applying the CSM RA.

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 08 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 acceptance 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.

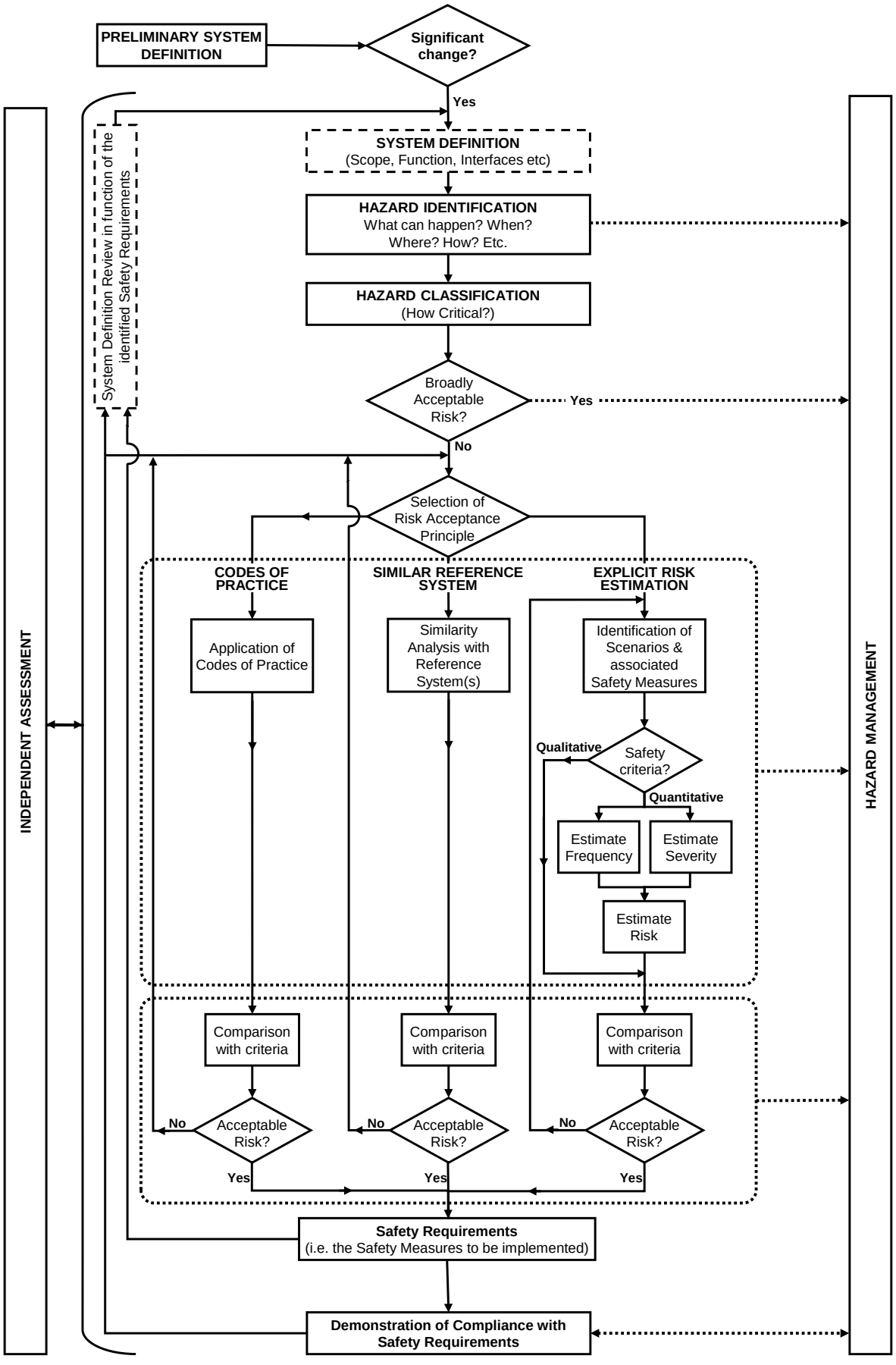

Figure 1 The risk management and independent assessment process from the CSM RA

Guidance on Risk Evaluation and Risk Acceptance

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 in to 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).

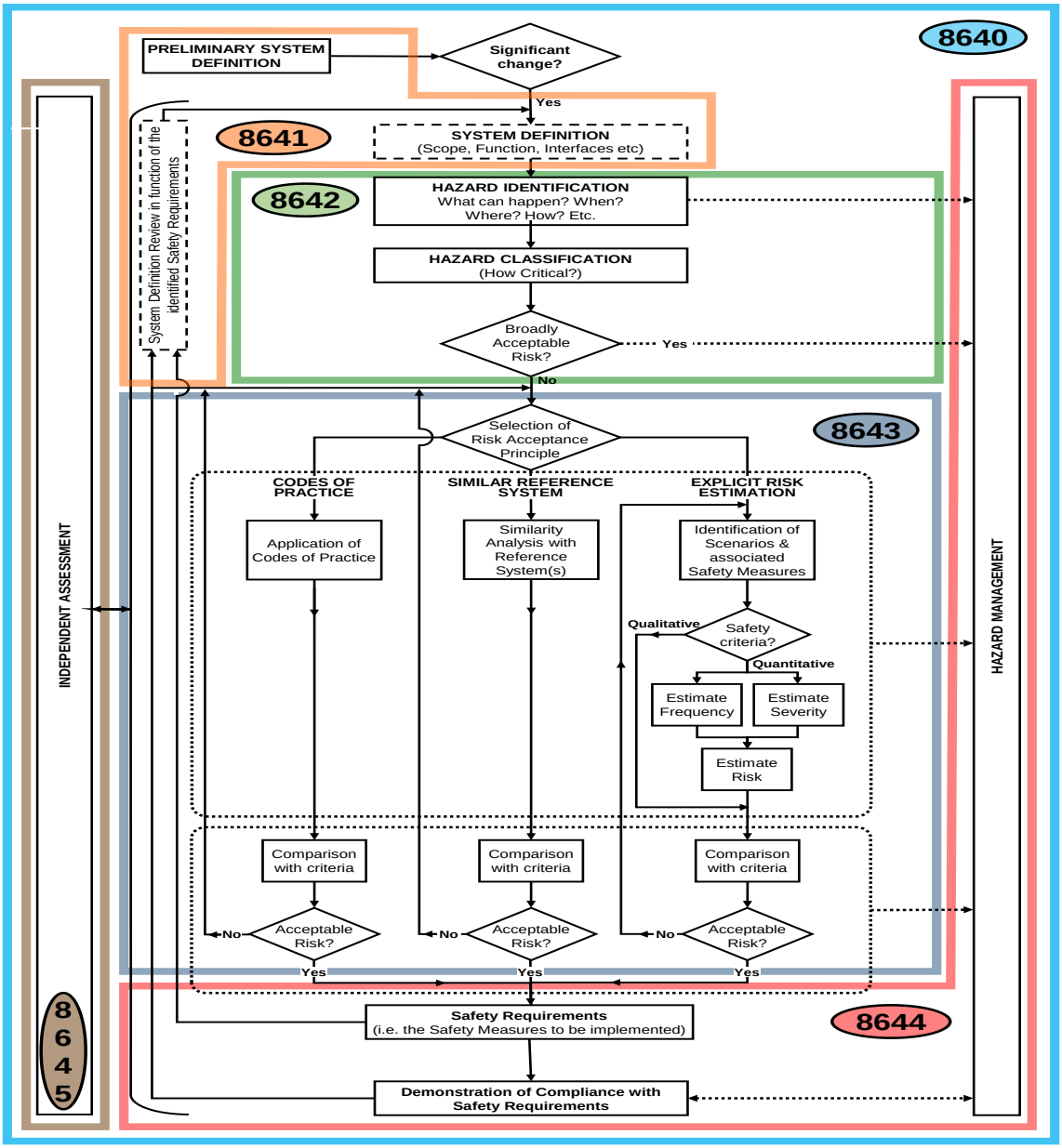

Figure 2 The set of guidance notes on the application of the CSM RA, and the process elements to which they relate

Part 3 Guidance on Risk Evaluation and Risk Acceptance

G 3.1 Introduction

G 3.1.1 The part of the risk management process being treated in this document takes as its starting point a classified list of hazards and delivers:

a) A set of safety requirements, which define the safety measures that will be put in place to control risk (and which will be documented in the system definition and the hazard record).

b) An updated hazard record, containing information as set out in the regulation:

'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)

c) A decision that the risk will be acceptable if all the safety requirements are met.

G 3.1.2 The CSM RA defines three risk acceptance principles:

a) Application of codes of practice.

b) Comparison with reference system(s).

c) Explicit risk estimation.

G 3.1.3 Annex I, clause 2.1.4 of the regulation requires that the acceptability of the risk associated with a significant change is evaluated using one or more of these risk acceptance principles. This is done by evaluating the risk associated with each hazard of the system. The risk associated with the change is acceptable when the risk associated with each hazard is acceptable.

G 3.1.4 The process may need to be partially repeated if the project changes or new information comes to light. For further guidance on this topic see GE/GN8644.

G 3.1.5 For further guidance on identifying and classifying hazards see GE/GN8642.

G 3.1.6 For further guidance on formulating safety requirements and maintaining a hazard record see GE/GN8644.

G 3.1.7 Guidance is provided for the case where the proposer of a change is able to implement all safety requirements themselves. Section G 3.6 gives guidance on how to adjust the process when the proposer needs other actors to implement safety requirements.

G 3.2 Selecting a risk acceptance principle

G 3.2.1 If it has been concluded that the risk associated with a hazard is classified as 'broadly acceptable' (see GE/GN8642), then the risk associated with the hazard is accepted without further analysis. The ORR Guidance (Dec 2012) records the ORR's opinion that, for the majority of hazards, this would not be the case.

G 3.2.2 For every other hazard, one or more of the following risk acceptance principles is applied:

a) Application of codes of practice.

b) Comparison with reference system(s).

c) Explicit risk estimation.

G 3.2.3 Different principles may be used for different hazards and the regulation does not state an order of preference for application of risk acceptance principles. However, it may be preferable to think first about where clauses within codes of practice are also safety requirements for a project, as in many cases processes will already be in place to demonstrate compliance with these requirements. A more efficient and joined up application of safety and interoperability processes will result.

G 3.2.4 Even where the application of safety measures taken from codes of practice is not sufficient to accept a risk, their application may be useful in defining safety measures which are tried and tested and which will allow the risk to be accepted by using another principle in addition.

G 3.2.5 Where it is applicable, the 'comparison with reference system(s)' principle provides an efficient method of reaching clear decisions about the acceptability of hazard risk. This is because most hazards are not unprecedented and there is therefore likely to be good understanding and experience of such hazards. Also, application of this principle leads to discussions about the similarity of the railway in different locations and circumstances rather than more abstract debates about levels of risk. It is often simple to establish that the hazards and operating circumstances are sufficiently similar that measures which are proven to be safe in one environment could be safely adopted elsewhere. It will, therefore, generally make sense to use this principle in preference to explicit risk estimation wherever appropriate reference systems exist.

G 3.2.6 There are no restrictions on the use of the 'explicit risk estimation' principle, which would be likely to be used either to support application of the other principles, or when neither of the other two principles is applicable.

G 3.2.7 Advice is provided on the application of each principle in the following sections.

G 3.3 Applying the 'application of codes of practice' risk acceptance principle

G 3.3.1 The regulation defines a code of practice to mean:

'a written set of rules that, when correctly applied, can be used to control one or more specific hazards.' (Article 3, Definitions, 19).

G 3.3.2 The regulation places other requirements that codes of practice must meet before they can be used for risk evaluation. It requires that they must:

'(a) be widely acknowledged in the railway domain. If this is not the case, the codes of practice will have to be justified and be acceptable to the assessment body;

(b) be relevant for the control of the considered hazards in the system under assessment;

(c) be publicly available for all actors who want to use them.' (Annex I, clause 2.3.2)

G 3.3.3 'Widely acknowledged in the railway domain' is a broad definition that may cover documents described as standards, procedures or rule books, for example:

a) Technical Specifications for Interoperability (TSIs).

b) National Technical Rules and National Safety Rules (including Railway Group Standards).

c) Rail Industry Standards.

d) British Standards, Euronorms and other international standards.

e) Network Rail company standards.

f) ATOC standards.

This is not an exhaustive list.

G 3.3.4 'Relevant' in G 3.3.2b) is taken to mean that the code of practice has been successfully applied to control the identified hazards of a system effectively in similar situations.

G 3.3.5 It is not necessary that a code of practice is available free of charge to meet criterion G 3.3.2c). It is sufficient to be publicly available for purchase by the actors who want to use it. The requirement for public availability has changed in the 2013 regulation. See section 3.7 below.

G 3.3.6 The documents in G 3.3.3 are a source of safety measures. In many cases the proposer would only be concerned with the subset of those safety measures that it determined to be safety requirements using the code of practice risk acceptance principle. Therefore, the safety requirement might reference only a specific clause or set of clauses of the code of practice.

G 3.3.7 There are several ways in which safety measures within codes of practice may control causes and/or consequences of hazards (either singly or together), including the following:

a) They may place constraints on the design of some equipment which will make it less likely to exhibit a hazard.

b) They may require the provision of protective measures which prevent failures from leading to accidents.

c) They may require interfaces between humans and machines to be designed in a way that makes it less likely that people will make mistakes.

d) They may require operational procedures that control the effects of hazards or prevent them from occurring.

G 3.3.8 Use of some codes of practice will be mandatory. Where safety measures from mandatory codes of practice control hazards, it is sensible to consider them early in the risk management process and see if they can be used to support the 'application of codes of practice' risk acceptance principle, as this can reduce the effort involved in applying the risk management process.

G 3.3.9 If the 'application of codes of practice' risk acceptance principle is being used to control a hazard, a broad range of types of code of practice should be considered in order to maximise the chances of finding the combination that is most effective.

G 3.3.10 The regulation states:

'*The proposer, with the support of other involved actors […] shall analyse whether one or several hazards are appropriately covered by the application of relevant codes of practice.'* (Annex I, clause 2.3.1)

G 3.3.11 The phrase '*appropriately cover*' is not defined in the regulation but it is considered here to primarily mean that the codes of practice are being used within their intended scopes. Where standards are used outside of their original intent, consideration is needed as to whether the safety measures are sufficient to control the risk associated with the hazard.

G 3.3.12 Codes of practice are rarely written just to control hazards – they are normally also written to deliver other benefits such as efficiency, interoperability and reliability. Moreover, where a code of practice does control hazards, it may not say which requirements within it are safety related and which hazards they control. It may be necessary to assemble a group of people with expertise in the area to decide whether relevant codes of practice *'appropriately cover'* a hazard or not.

G 3.3.13 When applying this principle, the simplest case is when safety measures from the codes of practice appropriately cover the hazard, as set out above, and the codes of practice are fully complied with. In this case:

a) Enter the safety measures within the codes of practice as safety requirements for the hazard in the hazard record.

b) Record the reasons for believing that the safety requirements from the codes of practice appropriately cover the hazard in the hazard record.

c) Enter these safety requirements in the system definition.

G 3.3.14 If nothing changes to undermine the validity of the conclusion that the codes of practice appropriately cover the hazard, and if the codes of practice are actually complied with, then following the codes of practice builds the necessary risk control into the system, and the risk associated with the hazard is accepted without further analysis.

G 3.3.15 The regulation also allows a hybrid approach. If safety measures from codes of practice cover most but not all of the risk associated with a hazard, then the principle may still be used, provided that one or more of the other principles is used for the parts of the risk which are not covered.

G 3.3.16 Figure 3 summarises the options described above as a flowchart.

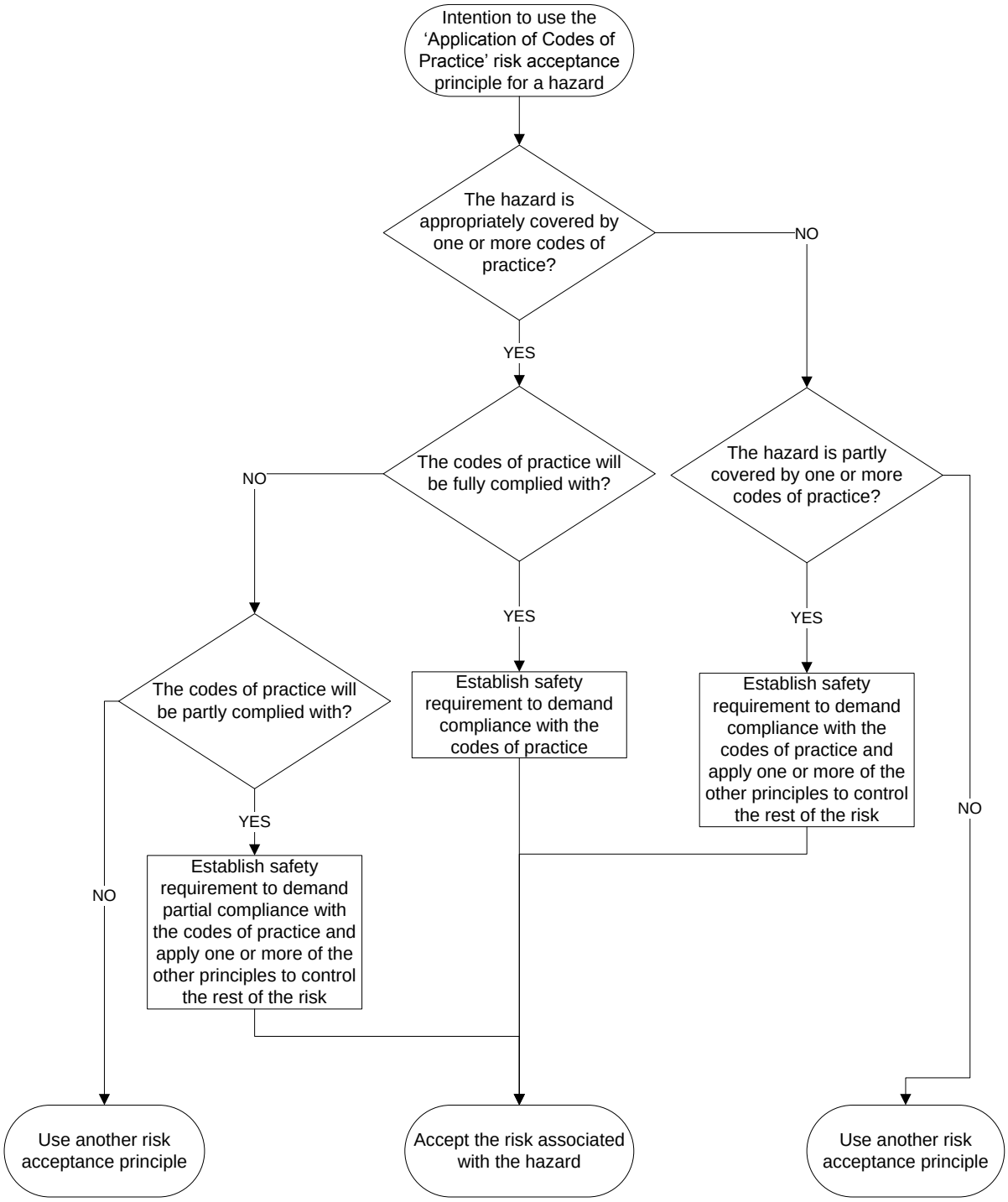

Figure 3 Applying the 'application of codes of practice' risk acceptance principle

G 3.3.17 If a fault in a safety measure in a code of practice is discovered which undermines its ability to control a hazard that it appears to be designed to control, then it is advisable to bring the fault to the attention of the organisation issuing the code of practice so that it may be corrected. It may be possible to use the hybrid approach described in the previous paragraph to restore adequate control of the hazard. If not, it will be logically necessary to conclude that the code of practice no longer 'appropriately covers' the hazard and to use other codes of practice or other risk acceptance principles.

G 3.4 Applying the 'comparison with reference system(s)' risk acceptance principle

G 3.4.1 The idea behind the 'comparison with reference system(s)' principle is straightforward: one compares a new system against an existing 'reference system' which is known to be associated with a level of risk which would be acceptable. The similarity of the reference system to the new system is considered, and if the systems are sufficiently similar that there is no additional risk associated with the new system, then the risk from it is considered acceptable. The safety measures from the reference system will be adopted by the new system as safety requirements.

G 3.4.2 The regulation defines minimum requirements that a reference system must meet:

'(a) it has already been proven in-use to have an acceptable safety level and would still qualify for approval in the Member State where the change is to be introduced;

(b) it has similar functions and interfaces as the system under assessment;

(c) it is used under similar operational conditions as the system under assessment;

(d) it is used under similar environmental conditions as the system under assessment.' (Annex I, clause 2.4.2)

G 3.4.3 It is necessary to check that a system meets these requirements before it may be used as a reference system. Point 3.2.3 (a) states that it is not enough that a system is in actual use; it must be the case that it would qualify for approval if it were to be introduced today. It is not entirely clear what this means in practice however it could be taken to mean that the proposer needs to consider whether the reference system is still representative of good practice, and is not based on out-moded technology.

G 3.4.4 The regulation describes the process of applying this principle in the following three steps:

'(a) the risks associated with the hazards covered by the reference system shall be considered as acceptable;

(b) the safety requirements for the hazards covered by the reference system may be derived from the safety analyses or from an evaluation of safety records of the reference system;

(c) these safety requirements shall be registered in the hazard record as safety requirements for the relevant hazards.' (Annex I, clause 2.4.3)

G 3.4.5 To put these steps into practice, the safety measures in place on the reference system that control the hazards in question are identified, and safety requirements on the new system are formulated that provide equivalent safety measures.

G 3.4.6 The regulation also allows another approach. It states:

'*If the system under assessment deviates from the reference system, the risk evaluation shall demonstrate that the system under assessment reaches at least the same safety level as the reference system. The risks associated with the hazards covered by the reference system shall, in that case, be considered as acceptable*.' (Annex I, clause 2.4.4).

This allows the level of risk associated with the hazards in question for the reference system to be established, and then safety requirements for the new system put in place to control the risk to a level which is no greater.

G 3.4.7 One way of carrying out this approach is to perform the following steps:

a) Identify all differences between the systems under assessment and the reference system which might affect risk.

b) Identify all differences between the operational and environmental conditions which might affect risk.

c) Assess for each difference in both lists whether it would make the risk associated with the system under assessment higher or lower than the risk associated with the system under assessment.

d) Consider each hazard to which the 'comparison with reference system(s)' principle is being applied and, if the results of the previous step demonstrates that the risk associated with the hazard is no greater in the system under assessment than in the reference system, then the risk associated with that hazard may be accepted. In this case the level of risk met by the reference system sets the risk assessment criteria for the system under assessment.

G 3.4.8 In practice, these points can be considered effectively once the hazards of the system have been identified, by asking a group of experts at a workshop whether there is any reason why the system in hand would be less safe than the reference system.

G 3.4.9 It will generally be easier to apply the principle if the people doing the assessment have access to a record of safety management activities carried out on the reference system and, ideally, if the hazard analysis actively involves some of the people who carried out these activities. It may facilitate this if RUs and IMs form long-term arrangements with other RUs and IMs that operate similar systems, in order to share information about these systems.

G 3.4.10 The regulation also describes a hybrid approach. It states:

'If the same safety level as the reference system cannot be demonstrated, additional safety measures shall be identified for the deviations, applying one of the two other risk acceptance principles.' (Annex I, clause 2.4.5)

G 3.4.11 Therefore, if the 'comparison with reference system(s)' principle is not sufficient to demonstrate an acceptable level on its own, it may still be used, provided that one or more of the other principles is used for the parts of the risk which are not covered. See Appendix A for an example of this.

G 3.4.12 Figure 4 summarises the options described above as a flowchart.

Guidance on Risk Evaluation and Risk Acceptance

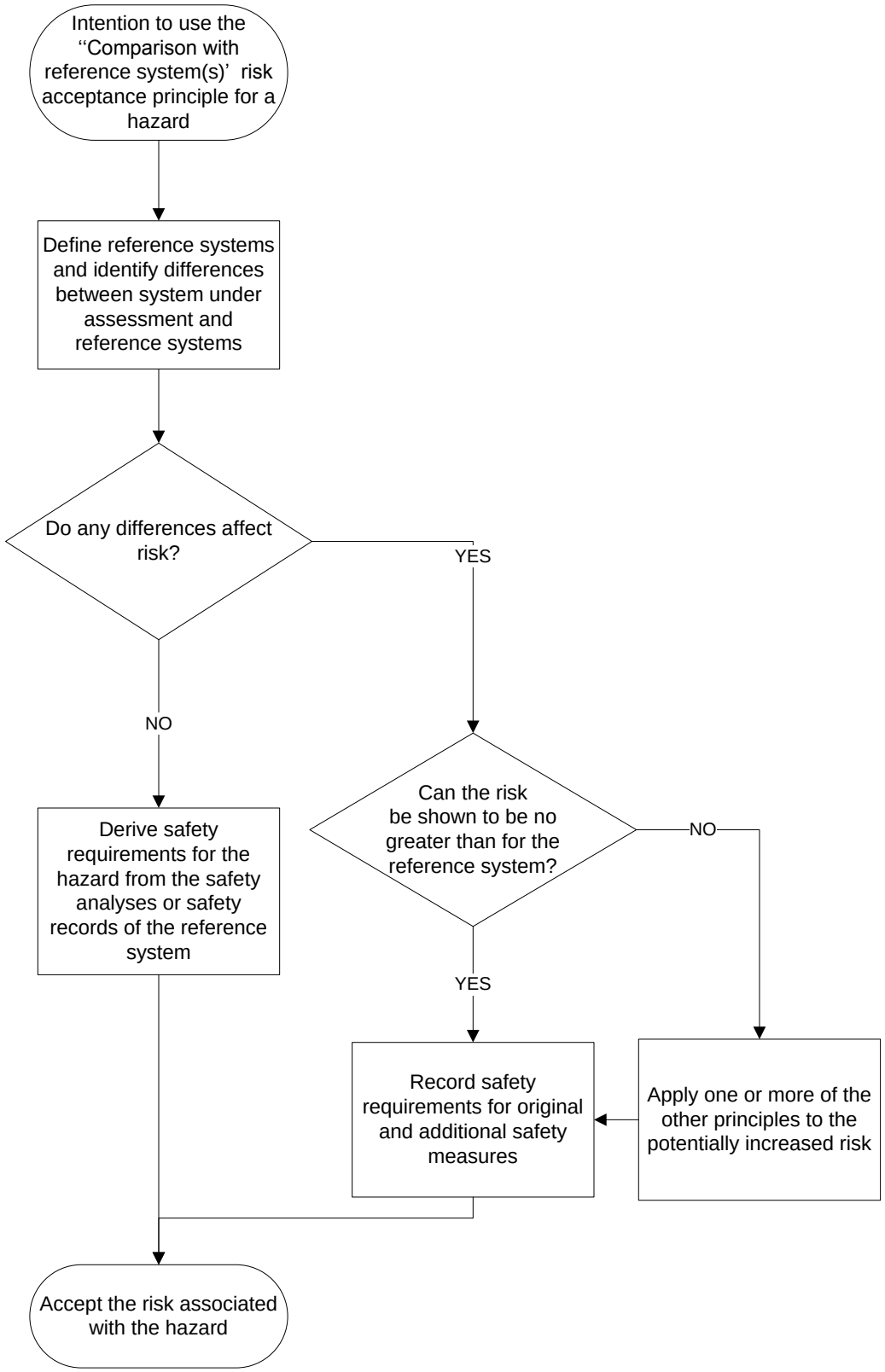

Figure 4 Applying the ‘comparison with reference system(s)’ risk acceptance principle

G 3.5 Applying the 'explicit risk estimation' risk acceptance principle

G 3.5.1 The 'explicit risk estimation' principle is generally used when it has been decided not to apply either of the other principles.

G 3.5.2 The regulation provides the following introduction to the principle:

'When the hazards are not covered by one of the two risk acceptance principles […], the demonstration of the risk acceptability shall be performed by explicit risk estimation and evaluation. Risks resulting from these hazards shall be estimated either quantitatively or qualitatively, taking existing safety measures into account.

'The acceptability of the estimated risks shall be evaluated using risk acceptance criteria either derived from or based on legal requirements stated in Community legislation or in notified national rules. Depending on the risk acceptance criteria, the acceptability of the risk may be evaluated either individually for each associated hazard or globally for the combination of all hazards considered in the explicit risk estimation.'

*'If the estimated risk is not acceptable, additional safety measures shall be identified and implemented in order to reduce the risk to an acceptable level.' (*Annex I, clauses 2.5.1 and 2.5.2)

G 3.5.3 In the UK, the ORR has stated in clause 3.41 of the ORR Guidance (Dec 2012) that the risk acceptance criterion to be used is that risk should be reduced 'so far as is reasonably practicable'. This criterion is sometimes referred to as the 'ALARP principle', where ALARP stands for 'as low as reasonably practicable'. The 'explicit risk estimation' principle is the only risk acceptance principle that explicitly invokes the ALARP principle. There was already considerable experience in the UK of explicitly evaluating risk using the ALARP principle before the regulation was introduced and this experience remains applicable in this context. RSSB's publication 'Taking Safe Decisions' gives guidance on taking decisions in a manner that is consistent with the ALARP principle.

G 3.5.4 The ALARP principle is not associated with a threshold of acceptable risk, below which risk can be accepted and above which it cannot. Instead, it requires demonstration that no reasonably practicable options to reduce risk further exist.

G 3.5.5 The risk management process allows risks to be evaluated either qualitatively or quantitatively. Either approach can be applied to support an ALARP test.

G 3.5.6 Quantitative risk evaluation generally requires significant effort and significant statistical data and is not always required. It is often possible to reach robust decisions using qualitative methods, which are discussed in the next section.

G 3.5.7 Hazards of railway systems are rarely unprecedented and previous experience can often be used to reach robust decisions more quickly than working from first principles. GE/GN8642 advises linking the hazards of the system to a generic list of hazards. If this has been done, then it may be possible to draw upon repositories of risk information, such as the Safety Risk Model, to assist with the risk evaluation.

G 3.5.8 For a straightforward hazard, the 'explicit risk estimation' principle may be applied qualitatively in the following manner:

a) Identify the causes of the hazard, and document as a table or short explanation.

b) Identify the possible consequences of the hazard and the factors that affect those consequences, and document as a table or short explanation.

c) Identify the existing safety measures which control the hazard.

d) Identify the practical additional safety measures which might be implemented to control the hazard further.

e) Review the additional safety measures, discard those that are judged not to be reasonably practicable and set safety requirements to implement those that are judged to be reasonably practicable.

G 3.5.9 Proceeding through these steps will lead to a robust decision, provided that:

a) There are people with sufficient experience and knowledge involved in each step.

And

b) There is consensus that the hazard is understood such that the results of each step can be reliably obtained from experience and knowledge.

G 3.5.10 The process of performing quantitative risk estimation to support risk acceptance using the ALARP principle is well-established and straightforward to explain. Carrying out the analysis and calculations that underpin the process is, however, a laborious and specialist task.

G 3.5.11 Because the process involves balancing the benefits and costs of safety measures and because a safety measure may affect the risk associated with several hazards, it is normally carried out for all hazards of a system together, or at least for a related group of hazards.

G 3.5.12 The 'explicit risk estimation' principle may be applied quantitatively in the following manner:

a) Identify the causes of the hazard.

b) Identify the possible consequences of the hazard.

c) Identify the existing safety measures and further safety measures which control the hazard and which it has been decided to implement. This is the baseline case.

d) Use the information from the previous steps to create a logical description of the causal chains which may result in an accident, usually using one or more specialist notations and computer programmes. Estimate the likelihood of the events in these chains and derive the frequency with which accidents occur.

e) Use these frequencies to quantify the risk associated with the baseline case as a statistical estimate of the harm incurred per year. That harm may include both fatalities and injuries, and conventions exist, which are set out in GE/GN8642, for combining these into a single number. One such convention results in a measure called 'Fatalities and Weighted Injuries' or FWI for short. Risk is then measured in FWI per year.

f) Identify all practical additional safety measures which might be implemented to control the hazard further.

g) For each safety measure, repeat steps 4 and 5, allowing for the effects of this safety measure, in order to estimate the reduction of risk resulting from the safety measure. The decrease in risk is compared with the increase in cost. Industry-standard benchmarks exist for deciding whether the option is reasonably practicable or not (see RSSB's publication 'Taking Safe Decisions').

h) Set safety requirements to implement those safety measures which were originally planned and those additional safety measures which were found to be reasonably practicable.

G 3.5.13 Any quantitative estimates of risk should clearly state what hazards they concern. Where the risk is associated with a number of identical systems (for example, a fleet of trains), any statement of risk level should make clear whether it relates to one item or the whole population.

G 3.5.14 In order to produce accurate quantitative estimates of risk, it is necessary to have accurate estimates of the probability of equipment failures and other events. Equipment suppliers may be able to provide some of these estimates. The Safety Risk Model published by RSSB may also be helpful.

G 3.5.15 No analysis of risk can ever be completely accurate, but the uncertainty can generally be reduced by further data collection or analysis. Risk analysis is used to support decision making and it follows therefore that risk analysis should be refined until a robust decision can be taken but no further. If uncertainty cannot be reduced further, the degree of uncertainty can be taken into account using techniques such as sensitivity analysis. When controlling risk, it is a generally accepted principle that, where there is an uncertainty about a risk, one should err on the side of caution. This typically means using an estimate at the higher risk end of the plausible range.

G 3.5.16 Significant uncertainty is often associated with the risk of multi-fatality accidents because there is usually limited data available to extrapolate from, and because the severity of such accidents may depend upon many factors. As explained in 'Taking Safe Decisions', this uncertainty justifies a conservative approach to the estimation of risk of multi-fatality accidents.

G 3.5.17 Clauses 2.5.4 to 2.5.6 inclusive of Annex I of the regulation define an alternative risk acceptance criterion, for a functional failure of a technical system. The RUs and IMs are considered to be unlikely to employ this criterion but may interface with suppliers that have applied this criterion. Additional guidance on its use is given in Appendix B.

G 3.5.18 Other EU states use different risk acceptance criteria. This will not be relevant to most changes made by UK IMs and RUs, but a proposer of a change should bear this in mind if it plans to seek recognition of its risk acceptance decision in another EU state, or if it plans to use a reference system from a different EU state. See GE/GN8645 for guidance on mutual recognition. Annex D of EN 50126-1:1999 sets out some risk acceptance criteria used in other EU states.

G 3.6 Involving others

G 3.6.1 For the changes within the scope of the guidance in this document, the proposer will be an IM or RU, and the proposer has overall responsibility for the risk management process. Moreover, the regulation specifically allocates to the proposer responsibility for certain aspects of the part of the process discussed in this document, including:

a) Choosing the risk acceptance principles to apply, see clause (11) of the preamble to the regulation.

b) Ensuring that risks are managed, see Article 5, point 3 of the regulation.

c) Deciding who will be in charge of implementing each safety requirement, see clause 1.1.5 of Annex I of the regulation.

d) Co-ordinating the management of risk at interfaces, see clause 1.2.1 of Annex I of the regulation.

e) Resolving conflicts regarding the management of risk. See clause 1.3.5 of Annex I of the regulation.

G 3.6.2 However, the regulation recognises that the proposer will often have to delegate parts of the risk management process, see Article 5, point 3 and clauses 1.1.5 and 1.1.6 of Annex I.

G 3.6.3 Where delivery of the change is being led by a prime contractor or supplier, it will probably make sense to delegate much of the day-to-day operation of the risk management process to the contractor or supplier. If a proposer does this, it should bear in mind that the contractor or supplier will rarely, if ever, be responsible for delivering the whole system, as this is likely to include changed operational and maintenance procedures for which the proposer will be responsible. It will seldom make sense to attempt to delegate aspects of the proposer's core business.

G 3.6.4 In the end, delivering a safe system always requires teamwork. Some IMs and RUs have formed integrated safety teams with their suppliers and reported success.

G 3.6.5 This teamwork is likely to extend to other parties, such as other IMs and RUs at interfaces. The regulation states '…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.'(Annex 1, section 1.2.)

G 3.6.6 However the proposer leads this process. The regulation states:

The management of shared risks at the interfaces shall be coordinated by the proposer. (Annex 1, section 1.2.1)

G 3.6.7 As a project progresses, practical issues may arise or new information may come to light, which will mean the need to reconsider the appropriateness of the safety requirements initially derived. The process for determining safety requirements remains the same, and the risk acceptance principles need to be reapplied.

G 3.6.8 On large or complex projects it may be the case that unresolved non-compliances remain when the proposer needs to implement the change. If this is the case, then the proposer should consider the effect of the non-compliance and put in place alternative safety measures, such as restrictions on operation, in order to restore risk to an acceptable level. Any changed or additional safety requirements would be registered in the hazard record and recorded system definition.

G 3.7 Forthcoming changes to the regulation

G 3.7.1 A new version of the regulation has been published 'European Commission. Regulation 402/2013 on the common safety method on risk evaluation and assessment', which will come into force on 21 May 2015. Differences between the new version and the version which was current at the time of writing this guidance note and which are relevant to this guidance note are as follows:

a) Clause 2.3.2 of Annex I provides additional clarification of the meaning of the requirements that codes of practice must meet in order to be used in the 'Application of codes of practice' risk acceptance principle. In particular the statement in the 2009 regulation that codes of practice must:

*'…be publicly available for all actors who want to use them.' (*Regulation 352/2009 Annex I, 2.3.2 c);

has been replaced by the statement that:

*'Upon request, [codes of practice] must be available to assessment bodies for them to either assess or, where relevant, mutually recognise, in accordance with Article 15(5), the suitability of both the application of the risk management process and of its results.' (*Regulation 402/2013, Annex I, 2.3.2c).

This change is likely to have the practical effect that proposers will feel more able to use the codes of practice risk acceptance principle in relation to their internal standards, systems and processes without fear of inadvertently giving away commercially valuable information to others. However, this reduced transparency might also make it harder for a proposer to use a reference system argument for accepting a system that has been used and accepted elsewhere. It might also make it difficult for new entrants to a market to use a reference system argument based on the application of similar safety requirements to those already in place for those operating in the member state.

b) Clause 2.4.4 of Annex I makes clear that, when the 'comparison with reference system(s)' acceptance principle is being used to evaluate a system and that system deviates from one reference system, it is legitimate to use another reference system to show that the deviation does not increase risk.

c) Clause 5.2 of Annex I adds requirements that the evidence retained regarding application of the risk management process will include evidence of compliance with the necessary safety requirements and documentation of assumptions.

Appendix A Example Risk Evaluation – Introduction Driver Only Operation with Passengers

This appendix contains a simplified, hypothetical example of the application of risk acceptance principles to illustrate particular points made in this guidance document.

G A.1 Introduction and background

G A.1.1 A railway undertaking operating passenger services (the proposer) is considering changing from driver and guard operations to Driver Only Operations with Passengers (DOO (P)).

G A.1.2 The operator already runs empty coaching stock without guards and there are several other operators already using DOO (P) with similar rolling stock and service conditions. Details on the evaluation of risk performed by these operators are available.

G A.1.3 The system to be considered includes the train, train staff, station platforms and train dispatch procedures. The system includes staff at some stations but most are unstaffed.

G A.1.4 The hazards associated with the change include but are not limited to:

a) H1: Doors closed with person or object attached to person not clear.

b) H2: Train dispatched with person trapped in doors.

G A.2 Risk evaluation and acceptance for hazard H1: doors closed with person or object attached to person not clear

G A.2.1 In the foreseen new system, safety measures to control this hazard include:

a) Sensitive edges on the doors, which are designed to cause the doors to reopen if they close upon someone or something.

b) A ‘hustle alarm’ which warns passengers that the doors are about to close.

c) Provision of station lighting to a level defined in Railway Group Standards.

d) A procedural requirement for the driver to observe the closure of the doors and the provision of mirrors, where required, to ensure that the driver can observe all doors.

G A.2.2 Similar arrangements are operated by other operators, with similar numbers of passengers and similar rolling stock. Informed by this, the proposer judges that the systems encompassing these arrangements meet the requirements in clause 2.4.2 of Annex I of the regulation for application as a reference system.

‘(a) it has already been proven in-use to have an acceptable safety level and would still qualify for approval in the Member State where the change is to be introduced;

(b) it has similar functions and interfaces as the system under assessment;

(c) it is used under similar operational conditions as the system under assessment;

(d) it is used under similar environmental conditions as the system under assessment.’
(Annex I, clause 2.4.2)

G A.2.3 A comparison of the proposed arrangements with the arrangements in use elsewhere performed at a workshop, including experts in train design and railway operations, reveals that the sensitive door edges are different on the trains under consideration from those in the reference systems, and this is the only difference. However, the sensitive door edges meet the requirements of the relevant TSI, which is considered to meet the requirement for a suitable code of practice in clause 2.3.2 of Annex I of the regulation and to cover the risk.

Guidance on Risk Evaluation and Risk Acceptance

G A.2.4 It is concluded that:

a) The risk for the change in question has been shown to be no higher than that associated with the reference systems.

And

b) This risk is covered by an appropriate code of practice.

G A.2.5 The risk is therefore accepted on the basis of the 'comparison with reference system(s)' risk acceptance principle supported by the 'application of codes of practice' risk acceptance principle.

G A.2.6 Figure 5 reproduces the flowchart from section G A.2.4, with the options taken highlighted in blue.

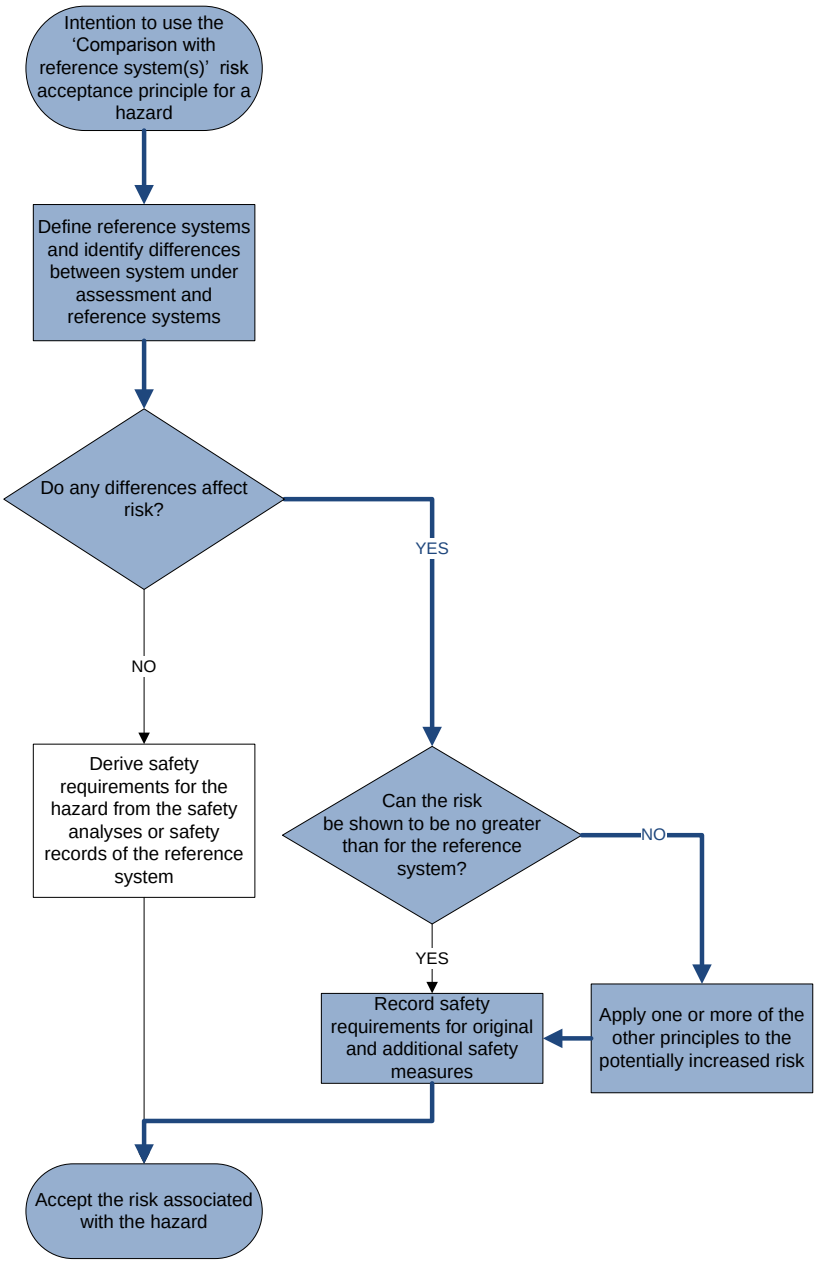

Figure 5 Applying the 'comparison with reference system(s)' risk acceptance principle

G A.3 Risk evaluation and acceptance for hazard H2: train dispatched with person trapped in doors

G A.3.1 This hazard is similar to hazard described in G A.2 but is concerned with the act of dispatch.

G A.3.2 In the foreseen new system, safety measures to control this hazard include:

a) A procedural requirement for the driver to confirm that all doors are closed and clear before moving off, and the provision of mirrors, where required, to ensure that the driver can observe all doors.

b) Emergency alarms by each door, which are available for use by passengers and which result in an immediate brake application if used.

c) Provision of station lighting to a level defined as acceptable for DOO (P) in Railway Group Standards (a level which is higher than that required for stations where DOO (P) is not employed).

G A.3.3 For most stations, the logic used to close the previous hazard is applicable and is actually applied.

G A.3.4 However, the trains are operated at two stations which have sharply curved platforms. At these stations, the view that the driver has of the rear doors of the train is not considered to be as good as in the reference system due to the available locations to position the mirrors. It is agreed to perform an explicit risk estimation of the risk at these stations.

G A.3.5 A baseline risk estimation is performed and two potential additional measures are identified:

a) Ensuring that these stations are manned through the operational day, that is, in effect, abandoning DOO (P) at these stations.

And

b) Changing passenger access to the platform so that passengers only arrive from an access point at the front of the train.

G A.3.6 Data on the risk associated with these options are available from local operational statistics.

G A.3.7 From these data, the risk reduction for the two options is estimated. These reductions are compared with the costs, using the methodology described in ‘Taking Safe Decisions’. It is concluded that option (a) above is not reasonably practicable but that option (b) is reasonably practicable, and safety requirements are established to require its implementation at the two stations concerned.

G A.3.8 As no further reasonably practicable safety measures can be identified, the risk at these stations is accepted using the ‘explicit risk estimation’ principle, which in the UK is the ALARP principle.

G A.3.9 The overall risk across all stations is therefore accepted on the basis of the ‘comparison with reference system(s)’ risk acceptance principle supported by the ‘explicit risk estimation’ risk acceptance principle.

G A.3.10 The options taken when traversing the flowchart from section G A.2.4 are the same as for hazard H1, and as shown in Figure 5. However, the supporting risk acceptance principle employed is different.

Appendix B Applying the 'Explicit Risk Estimation' Risk Acceptance Principle (Quantitative Using the 10^{-9} Criterion)

G B.1.1 The regulation states in Annex I:

'2.5.4. Where hazards arise from failures of technical systems not covered by codes of practice or the use of a reference system, the following risk acceptance criterion shall apply for the design of the technical system:

For technical systems where a functional failure has credible direct potential for a catastrophic consequence, the associated risk does not have to be reduced further if the rate of that failure is less than or equal to 10^{-9} per operating hour.

2.5.5. Without prejudice to the procedure specified in Article 8 of Directive 2004/49/EC, a more demanding criterion may be requested, through a national rule, in order to maintain a national safety level. However, in the case of additional authorisations for placing in service of vehicles, the procedures of Articles 23 and 25 of Directive 2008/57/EC shall apply.

2.5.6. If a technical system is developed by applying the 10^{-9} criterion defined in point 2.5.4, the principle of mutual recognition is applicable in accordance with Article 7(4) of this Regulation.

Nevertheless, if the proposer can demonstrate that the national safety level in the Member State of application can be maintained with a rate of failure higher than 10^{-9} per operating hour, this criterion can be used by the proposer in that Member State.' (Annex I, clauses 2.5.4, 2.5.5 and 2.5.6)

G B.1.2 Annex I clauses 2.5.4 to 2.5.6 of the regulation define an alternative risk acceptance criterion to the national risk acceptance criteria for technical systems. The criterion defines a tolerable hazard rate where, in certain circumstances, the risk associated with a failure of a technical system does not have to be reduced further if the rate of that failure is less than or equal to 10^{-9} per operating hour. The regulation does allow national governments to request a more demanding criterion, but the UK has not opted to do this (see clause 3.46 of the ORR Guidance (Dec 2012)).

G B.1.3 The ORR Guidance (Dec 2012) (see paragraph 3.45) explains that the ALARP risk acceptance principle may still be applied to technical systems if the proposer chooses, as this would maintain the national safety level in the member state in accordance with Annex 1, clause 2.5.6 of the regulation).

G B.1.4 10^{-9} per operating hour is a very low rate, corresponding to less than one failure, on average, every 10,000 operating years. Nevertheless, some specialist manufacturers do have the capability to justify claims of delivering such a rate and it may also be able to demonstrate achievement of that rate from field statistics for equipment that has been installed in large quantities. The regulation requires mutual recognition for risk evaluations using this criterion.

G B.1.5 A UK RU or IM may be offered technical systems for which such claims have been made and endorsed by a recognised acceptance body. If the applicable requirements in the regulation have been applied, then these claims may not be called into question and should be taken as valid for the RU's or IM's application if the functional, operational and environmental conditions are the same.

G B.1.6 However, there are obstacles that stand in the way of the use of this criterion:

a) There is currently disagreement about the interpretation of this criterion where a function is replicated on a system. An example would be a door control system fitted to each of 48 doors on a train. It is not agreed whether the criterion requires a failure rate less than or equal to 10^{-9} per operating hour for the train as a whole or for each door. The former interpretation would be 48 times more stringent than the latter one.

b) The system that the RU or IM is evaluating will generally extend beyond the technical system at its heart. So, if an RU wishes to bring a new train into service, it will need to evaluate the risks of a system that includes operational and maintenance procedures as

well as the train. Even if the doors fail at a rate less than or equal to 10^{-9} per operating hour, this does not mean that door incidents will occur at this rate because they may also be caused by operator error.

G B.1.7 UK RUs and IMs who are considering using this criterion in their own risk evaluation should, therefore, read the detailed requirements in the regulation very carefully and consider taking specialist advice.

Definitions and Abbreviations

Actor

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

ALARP

As Low As Is Reasonably Practicable.

Note: The Health and Safety at Work etc. Act 1974 places duties on employers in the UK to ensure safety 'so far as is reasonably practicable' (SFAIRP). When these duties are considered in relation to risk management the duty is sometimes described as a requirement to reduce risk to a level that is 'as low as is reasonably practicable' (ALARP). These terms therefore express the same concept in different contexts and should be considered to be synonymous.

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.'

Configuration item

An item subject to configuration management.

Configuration management

A discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, to control changes to those characteristics, to record and report change processing and implementation status and to verify compliance with specified requirements.

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.

DOO (P)

Driver Only Operation with Passengers.

FWI

Fatalities and Weighted Injuries.

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.

Reference system

As defined in the regulation:

'means a system proven in use to have an acceptable safety level and against which the acceptability of the risks from a system under assessment can be evaluated by comparison.' (Article 3, clause 20)

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.

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)

SFAIRP

So far as is reasonably practicable (see ALARP).

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 CSM on Risk Evaluation and Assessment
GE/GN8641	Guidance on System Definition
GE/GN8642	Guidance on Hazard Identification and Classification
GE/GN8644	Guidance on Safety Requirements and Hazard Management
GE/GN8645	Guidance on Independent Assessment
Measuring Safety Performance	RSSB guide on how to develop and manage safety performance indicators for Britain's railways
Safety Risk Model	RSSB Safety Risk Model Risk Profile Bulletin

Other references

BS EN 50126-1:1999	Railway applications — The specification and demonstration of Reliability, Availability, Maintainability and Safety (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
GD-0001-SKP	Taking Safe Decisions – how Britain's railways take decisions that affect safety
ORR Guidance (Dec 2012)	ORR guidance on the application of the common safety method (CSM) on risk assessment and evaluation (December 2012)

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