OFFICE OF RAIL AND ROAD

Common Safety Method for Risk Evaluation and Assessment

Guidance on the application of Commission Regulation (EU) 402/2013

01 September 2018

Contents

1. Introduction

Background

1.1. Commission Implementing Regulation (EU) 402/2013 (the Regulation on a common safety method (CSM) for risk evaluation and assessment [or "the CSM RA"]) is part of a wide-ranging programme of work by the European Union Agency for Railways (the Agency) and the European Commission (the Commission) to bring about a more open, competitive rail market while seeking to ensure that safety levels are maintained, and, if reasonably practicable, improved. In the past, safety requirements may have been used as a barrier to open competition across the EU. The intention of the CSM RA is to harmonise processes for risk evaluation and assessment and the evidence and documentation produced during the application of these processes. By applying a common process, it will be easier for an assessment undertaken in one EU Member State to be accepted in another with the minimum of further work. This is referred to as mutual recognition. The Intergovernmental Organisation for International Carriage by Rail (OTIF) has adopted risk assessment requirements (UTP GEN-G) equivalent to the CSM RA. Mutual recognition therefore extends to contracting states of OTIF.

1.2. The CSM RA is a framework that describes a common mandatory European risk management process for the rail industry and does not prescribe specific tools or techniques to be used. The processes are intended to complement requirements in other legislation, for example on interoperability or safety certification, and not to duplicate them. The broad principles of how these requirements fit together are explained in the following paragraphs.

Interface between the CSM RA and national requirements in Great Britain

1.1 There is other domestic legislation in Great Britain that requires *suitable and sufficient* risk assessments to be undertaken, such as the Management of Health and Safety at Work Regulations. As far as possible, courts will read and interpret domestic legislation in a way that is compatible with European law. To prevent conflict arising, ORR should interpret national law in a way which is consistent with European law. In order to ensure there is conformity across Europe, every effort must be made to interpret and apply national law in line with European law. The Courts' guiding principle is that European and domestic requirements are compatible unless a conflict is clear. Where a provision of European law conflicts with a national law provision and cannot be reconciled, European legislation will take precedence over domestic requirements and a court must set aside the conflicting national law provision.

1.2 ORR is of the view that there is no conflict between the domestic requirements for a risk assessment to be *suitable and sufficient* and the level of risk assessment required by the risk management process of the CSM RA. In practice, therefore, when any significant safety related change of a technical, operational or organisational nature is proposed to the mainline railway, compliance with the risk management process of the CSM RA should produce a suitable and sufficient risk assessment for that change.

1.3 Under the Health and Safety at Work etc. Act 1974 and relevant health and safety regulations, duty holders have a responsibility to undertake a suitable and sufficient assessment of risks for the **entirety** of its operations and make arrangements for the effective planning, organisation and control of protective and preventative measures.

1.4 The starting point for anyone proposing any change in relation the mainline railway system is the CSM RA. The CSM RA applies when any technical, operational or organisation change is being proposed to the railway system. A person making the change (known as 'the proposer') needs to firstly consider if a change has an impact on safety. If there is no impact on safety, the risk management process in the CSM RA need not be applied and the proposer must keep a record of how it arrived at its decision.

1.5 If the change has an impact on safety the proposer must decide on whether it is significant or not by using criteria in the CSM RA (see Annex 1 of this guidance). If the change is significant the proposer must apply the risk management process. If the change is not significant, the proposer must keep a record of how it arrived at its decision.

If the change is not significant

1.6 In cases where a change is not significant, it will fall to the proposer of the change to consider domestic legislative requirements, such as those set out in regulation 19 of the Railways and Other Guided Transport Systems (Safety) Regulations 2006 (ROGS) and regulation 3 of the Management of Health and Safety at Work Regulations 1999 (MHSWR), which require a suitable and sufficient risk assessment to be undertaken. It is possible to adopt the approach of the risk management process of the CSM RA even when there is no legal requirement to do so (for example, when a change is not significant) in line with the organisation's safety management system. Following the CSM approach correctly in these circumstances is likely to mean that domestic safety legislation is complied with.

1.7 The Rail Safety and Standards Board (RSSB) in its publication Taking Safe Decisions has suggested applying the risk management process of the CSM RA even if a change not significant. This is to avoid the need to have duplicate risk assessment processes.

1.8 So, even though it is not mandatory to apply the risk management process if a change is not significant a proposer may choose to apply it. In these circumstances some elements of the risk management process (such as the need for independent assessment) can be omitted.

If the change is significant

1.9 In cases where a change is determined to be significant, the risk management process of CSM RA must be carried out by the proposer. The framework of the risk management process is based on the analysis and evaluation of hazards using one or more of the following risk acceptance principles:

- application of codes of practice;
- comparison with similar systems (reference systems); and
- explicit risk estimation.

1.10 Although the risk management process of the CSM RA must always be complied with, it can complement existing domestic legislation. The CSM RA applies the same principles as set out in Regulation 3 of the MHSWR but sets out a more formalised process with an independent evaluation of the risk assessment process by an assessment body (which can be carried out by an in-house service if it meets the criteria in the regulation). The CSM RA also includes additional elements requiring:

- agreements with other duty holders or 'actors' (in European terms) involved in managing or affected by the risk in their risk management process and associated safety management responsibilities; and
- cooperation arrangement between 'actors' in how shared risks will be managed.

1.11 It is very likely that the change being proposed will impact on other interfaces in relation to the railway system which domestic legislation such as MHSWR and CDM Regulation (see below) will also require the proposer to assess safety risk. Whilst it is possible to carry out separate risk assessments under each piece of legislation, in these cases it is likely to be more efficient to produce a single, broadly scoped, risk assessment in accordance with the CSM RA that addresses the risks for the whole operation as a result of the proposed change. The scope of the risk management process should be recorded in the System Definition.Conflict should not arise between domestic and European legislative provisions in relation to risk assessments. The CSM RA, ROGS, MHSWR and CDM Regulation requirements seek to achieve the same result: a robust risk assessment and controls to maintain or reduce risk. ORR therefore considers it to be unnecessary for duty holders to produce separate risk assessment and evaluation processes to comply with domestic and European requirements. Compliance with the CSM RA should simultaneously deliver compliance with regulation 19 ROGS and regulation 3 MHSWR in respect of

the change and impact on other interfaces, as the purpose of the CSM RA is to deliver a thorough and competent risk assessment process.

1.12 Significantly, a court is likely to interpret domestic legislation in such a way as to determine that a risk assessment which is CSM RA compliant is suitable and sufficient for the purposes of the domestic requirements.

1.13 If a proposer of a change applies one or more of the three risk acceptance principles in the CSM RA regulation correctly for all identified hazards, and implements suitable control measures, this should mean that the risk has been reduced to an acceptable level for the change being effected. One of the purposes of the CSM RA is to ensure that a high level of safety will be maintained, and where reasonably practicable, improved.

Designing in risk control

1.14 It is essential that duty holders' risk assessment and evaluation processes, whether European or domestic, consider risk control from the initial design stage. Where the change is likely to be significant this will require the CSM RA to be considered early enough in the process to influence the client requirements before pre-construction information is finalised. A case study on designing in risk control can be found in Annex 5.

Purpose of this guidance

1.15 This guidance summarises and explains the main requirements of the CSM RA, to whom it applies, and specific points on compliance in the UK.

1.16 This is the fourth issue of this guidance. It has been updated to reflect the coming into force of amendments made to the CSM RA by Commission Implementing Regulation (EU) 2015/1136, which was adopted by the European Commission on 13 July 2015. The amendments are concerned with 'risk acceptance criteria', which are now called 'harmonised design targets'. The term 'harmonised design targets' has been introduced to distinguish the acceptance of risks associated with technical systems from the acceptance of operational risks and of the overall risk at the level of the railway system.

1.17 Regulation (EU) 402/2013 came into force on 23 May 2013 and started to apply from 21 May 2015. It amended the original Regulation (EC) 352/2009, which came into force on 19 July 2010 and has been applicable from July 2012 to all significant changes which impact on safety. Those amendments were mostly concerned with the accreditation and recognition of assessment bodies. Regulation (EC) 352/2009 was repealed on 21 May 2015 but its provisions continue to apply in relation to projects that were at an advanced stage of development on that date. We believe it is unlikely that proposers will claim that any further projects were at an advanced stage

on 21 May 2015. The amendments to Regulation (EU) 402/2013 made by Regulation (EU) 2015/1136 came into force and started to apply on 3 August 2015. This guidance will continue to be updated as further revisions to the CSM RA come into force or if there are changes to other related legislation or processes that impact on how the CSM RA should be applied.

1.18 The full (consolidated) text of the CSM RA is available on the Commission's website. As a Commission Regulation, it applies directly and does not need to be transposed into UK law. The CSM RA primarily applies to railway undertakings (RUs), infrastructure managers (IMs) and entities in charge of maintenance (ECMs) but also applies to project entities and manufacturers in certain circumstances (see paragraphs 2.17 - 2.18).

1.19 The Agency has also produced guidance on the application of the CSM RA. This is in two parts: the first is intended as further explanation ('Guide to the Application of the CSM'); and the second is a collection of examples of risk assessments, processes and applications that were used in some Member States prior to the introduction of the CSM RA. The main aim of the second part is to illustrate the types of tools and techniques that may be used to apply the CSM RA. In addition the Agency has produced guidance on harmonised design targets.

1.20 The Railway and Other Guided Transport Systems (Safety) Regulations 2006 (as amended) (ROGS) require RUs and IMs to develop safety management systems (SMS) to manage the risks associated with their activities and to meet specific criteria. One of the criteria for the SMS is that it must apply the relevant parts of CSMs. (In addition to the CSM RA, there is one other CSM applicable to RUs and IMs (the CSM for Monitoring). Please see ORR's website or Taking Safe Decisions for further details.) ORR will check compliance with CSMs when we examine applications from duty holders for safety certificates or authorisations and when we subsequently supervise those duty holders.

1.21 The Railways and Other Guided Transport Systems (Miscellaneous Amendments) Regulations 2013 removed from ROGS the requirement for a written safety verification scheme by RUs or IMs in certain circumstances. This was to prevent duplication following the introduction of the CSM, which achieves a similar outcome.

More information

Commission Regulation (EC) 352/2009

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:108:0004:0019:EN:PDF

Commission Regulation (EU) 402/2013 (consolidated with Regulation (EU) 2015/1136)

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02013R0402-20150803&qid=1486726327105&from=EN

Commission Implementing Regulation (EU) 2015/1136

http://www.era.europa.eu/Document-Register/Pages/Commission-implementing-R.aspx

The Agency's guidance to the application of the CSM

http://www.era.europa.eu/Document-Register/Documents/guide-for-application-of-CSM-Ver-1-1.pdf

The Agency's collection of examples of risk assessments and some possible tools

http://www.era.europa.eu/Document-Register/Documents/collection_of_RA_Ex_and_some_tools_for_CSM_V1.1.pdf

The Agency's guidance on harmonised design targets

http://www.era.europa.eu/Document-Register/Pages/Commission-implementing-R.aspx

RSSB guidance: Taking Safe Decisions

http://www.rssb.co.uk/risk-analysis-and-safety-reporting/risk-analysis/taking-safe-decisions

2. Applying the CSM RA

When does the CSM RA apply?

2.1 The CSM RA applies when any technical, operational or organisational change is being proposed to the railway system. A person making the change (known as 'the proposer') needs to firstly consider if a change has an impact on safety. If there is no impact on safety, the risk management process in the CSM RA need not be applied and the proposer must keep a record of how it arrived at its decision.

2.2 If the change has an impact on safety the proposer must decide on whether it is significant or not by using criteria in the CSM RA (see Annex 1 of this guidance). If the change is significant the proposer must apply the risk management process (see Chapter 3). If the change is not significant the proposer is not obliged to apply the risk management process but it is strongly recommended to use the process to manage non-significant safety risks. The proposer must keep a record of how it arrived at its decision.

2.3 This process is summarised in Figure 1.

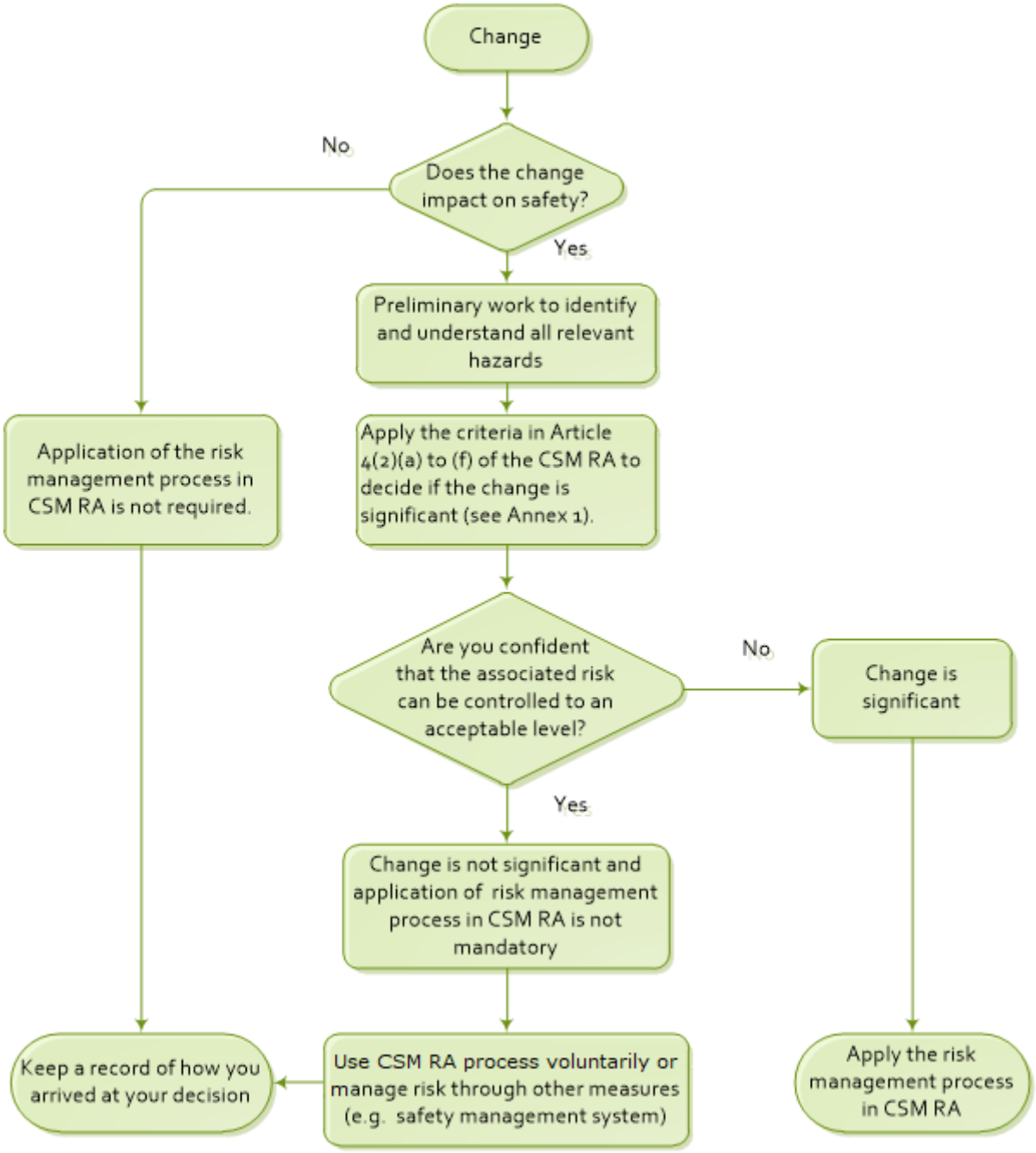
2.4 In addition to technical, operational or organisational changes, application of the CSM RA may be required

- by a Technical Specification for Interoperability (TSI) when structural sub-systems falling within the scope of the Railways (Interoperability) Regulations 2011 (as amended) (RIR) are constructed or manufactured, or upgraded or renewed; or
- when placing in service a structural sub-system to ensure that it is integrated into the existing system in a safe manner.

2.5 Structural sub-systems (as described in Directive 2008/57/EC) are:

- rolling stock;
- infrastructure;
- command control and signalling; and
- energy.

Figure 1: Applying the CSM RA for technical, operational or organisational change



What are technical, operational and organisation changes?

Technical changes

2.6 Technical changes are changes to a structural sub-system such as new rolling stock or a station rebuild. Technical changes should also be reviewed to determine whether they introduce changes to the operation of the sub-system under consideration.

Operational changes

2.7 Operational changes are:

- changes to the operation of a structural sub-system;
- changes to the operation of the railway system; or
- changes to the operating rules of the railway system.

2.8 Operational changes are often the result of technical changes to a sub-system. Indeed, technical changes are frequently made for the purpose of delivering a desired operational change. In these cases, the technical change and its effect on

- the operation of the sub-system;
- the wider railway system; or
- the operating rules of the railway,

must be considered and assessed together.

2.9 For example, a change of the command, control and signalling (CCS) system from fixed marker signals (for example TVM) to a cab-based system (for example ETCS) is a significant safety-related technical change that should be assessed in accordance with the risk management process of the CSM RA. Such a change will also involve changes to the operation of the CCS sub-system and changes to the wider operating rules. These operational changes must be assessed together with the significant safety-related technical changes as part of the risk management process of the CSM RA.

2.10 Of course, changes to

- the operation of a sub-system; or
- the operation of the railway system; or
- the operating rules of the railway system,

can also be introduced without a related technical change. If these changes are safety-related, the proposer should consider whether they are significant or not. Only if they are significant should the risk management process of the CSM RA be applied to them. If the change is not significant, the proposer must keep a record of how it arrived at its decision.

Organisational changes

2.11 Organisational changes are changes to the organisation of an actor in the railway system which could impact on the safety of the railway system. The ‘actor’ is most

likely to be an IM or a RU, but it could be an ECM or any other organisation that affects the safety of the railway system.

2.12 An example could be a change to the Safety Management System (SMS) - moving from a structure and culture based on a large number of prescriptive standards to a risk-based system relying on trained and competent staff using a small number of key principles. This could be a significant safety-related change and should be assessed using the CSM RA.

2.13 Further guidance on organisational changes can be found in Annex 4.

Who has duties under the CSM RA?

2.14 The CSM RA places duties primarily on the proposer of a change. Proposers are those in charge of projects who wish to implement a change to a technical, operational or organisational aspect of the railway system.

2.15 In many circumstances, proposers will be RUs or IMs. This aligns with the Safety Directive 2004/49/EC which places the main responsibilities for safety on these two key players. An ECM will also become a proposer in relation to changes to its maintenance system or if it is responsible for the modification of vehicles.

2.16 However, the CSM RA allows other bodies to act as the proposer. This could apply, for example, to project entities and manufacturers who lead projects where they are required to engage a Notified Body (NoBo) or a Designated Body (DeBo), or an applicant for an authorisation for placing in service under RIR.

2.17 In some circumstances a manufacturer or client will act as the proposer at the start of a project,for example if they want to market a new or altered product and/or there is no RU or IM in place. For manufacturers once the product is placed on the market, that ‘change’ is complete and an RU or IM wishing to use the new or altered product in a specific application or location will then be the proposer of a new change for CSM RA purposes. The RU or IM’s risk assessment will focus on such matters as route-specific technical compatibility and safe integration and will not need to repeat the manufacturer’s risk assessment. In projects where a client is undertaking the initial design and development work the client will carry the obligations under CSM RA initially and once an RU or IM is appointed the RU and/or IM will then take on the outcomes of the client’s initial CSM RA work and incorporate that into their ongoing CSM RA duties.

2.18 It may be advisable to ensure that the obligations on the manufacturer/client to apply CSM RA, in particular the requirement to appoint an independent Assessment Body (see chapter 4), before handing the product/project over to the RU/IM is included in the commercial contractual arrangements between the two parties.

2.19 The proposer must ensure that risks introduced by its suppliers and its service providers, including their subcontractors are also managed through application of the CSM RA. This may require participation in the risk management process of the CSM RA through contractual arrangements coordinated by the proposer.

Where on the railway system does the CSM RA apply?

2.20 The CSM RA has the same scope as the mainline railway as defined in ROGS. Therefore, the CSM RA does not apply to a railway if

a) ORR determines under regulation 2A (1) of ROGS that it falls within one or more of these categories:

- metros and other light rail systems;
- networks that are functionally separate from the rest of the mainline railway system and intended only for the operation of local, urban or suburban passenger services, as well as transport undertakings operating solely on these networks; or
- heritage, museum or tourist railways that operate on their own networks; or

b) ORR determines under regulation 2A(2) of ROGS that heritage vehicles that operate on the mainline railway and comply with national safety rules are part of a non-mainline operation; or

c) it is privately owned infrastructure that exists solely for use by the infrastructure owner for its own freight operations.

2.21 Rail systems that fall under (a) and (b) above are contained in an Approved List on our website.

2.22 The CSM RA also does not apply to RUs operating vehicles (for example On-Track Machines) within a possession. If vehicles operate within a possession and subsequently leave the possession to operate on the mainline railway the CSM RA will apply. The risks arising from operating OTMs within a possession can be managed through other measures, such as the Management of Health and Safety at Work Regulations 1999.

2.23 In circumstances where the CSM RA is not a formal legal requirement (for example if the rail system is on the Approved List), the risk management process it describes can nevertheless be used for the management of change (see also paragraphs 1.8 to 1.10).

How does the proposer determine the significance of a change?

2.24 If a proposed change has an impact on safety, the proposer must determine the significance of the change by examining the criteria in Article 4(2) of the CSM RA (see Annex 1 of this guidance). Note that the assessment body (see Chapter 4) assesses the application of the risk management process of the CSM RA but cannot question the proposer's significance decision.

2.25 If a change is deemed to be non-significant, application of the risk management process of the CSM RA is not mandatory and the change should be managed under the change management processes as described in the proposer's SMS or by carrying out a risk assessment which is required as part of compliance with other legislation, such as the Management of Health and Safety at Work Regulations 1999. However, there is nothing to prevent the proposer voluntarily applying the CSM RA risk management process for a non-significant change.

2.26 ORR, or the safety authority in another EU Member State, may check the process that RUs or IMs have used to determine whether or not to apply the CSM RA. Proposers, therefore, must document their decisions, particularly in relation to the test for significance.

2.27 The CSM RA contains six criteria which should be examined to determine 'significance'. These are:

- **failure consequence**: credible worst-case scenario in the event of failure of the system under assessment, taking into account the existence of safety barriers outside the system;
- **novelty used in implementing the change**: this concerns both what is innovative in the railway sector, and what is new just for the organisation implementing the change;
- **complexity of the change**;
- **monitoring**: the inability to monitor the implemented change throughout the system life-cycle and take appropriate interventions;
- **reversibility**: the inability to revert to the system before the change; and
- **additionality**: assessment of the significance of the change taking into account all recent safety-related modifications to the system under assessment and which were not judged as significant.

2.28 The CSM RA gives no order or priority on how to use the "significance" criteria, nor any thresholds to evaluate and make the decision. To help proposers work through

the process, a UK industry proposal for how to determine significance is included at Annex 1. This approach is only one way of applying the criteria and is not mandatory.

Additionality

2.29 Additionality can be described as considering other changes that have been made since the entry into force of the CSM RA (23 May 2013) or since the last application of the risk management process (whichever is later), which, when combined with the change being considered, could become significant. If there are other safety-related changes that have been made 'recently', the test for significance should be made for all the changes as a whole rather than for just the individual change being considered.

2.30 Annex 1 suggests that additionality should be considered first as this defines the scope of the change that is to be assessed. It also proposes a method of addressing how far back to look when examining a series of changes.

2.31 Breaking down a significant change into a series of smaller changes, which individually are not significant so that the risk management process is then not applied to the overall significant change, is not permitted by the CSM RA.

Novelty and complexity

2.32 If a proposed change is novel or complex there could be an increase in the likelihood that, once implemented, the changed structural sub-system, operation or organisation will not behave as predicted and that unforeseen hazards will arise. Classifying such changes as significant and applying the risk management process, including the requirement for an independent assessment, will provide additional assurance and should help to identify measures to mitigate any potential increase in the risk.

3. Applying the risk management process of the CSM RA

What does the risk management process involve?

3.1 The risk management process is contained in Annex I of the CSM RA. The main phases are illustrated in Figure 2 and further details are set out below. The process illustrated is not static or linear as the proposer may undertake iterations of all or part of the process. The proposer should also integrate the process into the project lifecycle, rather than carrying it out in isolation. The process begins with a system definition and ends when the proposer is content that for each hazard the identified safety requirements and measures have been complied with by applying defined risk acceptance principles (see paragraphs 3.26 to 3.52). If the proposer decides to change the system definition throughout the process, it may need to start again from the beginning.

3.2 An assessment body must carry out an independent assessment of the risk management process and the results obtained from carrying it out.

3.3 The processes required by Annex I of the CSM RA will be familiar to many in the UK and are probably already in use in their risk management systems. The key requirements are examined below. Potential proposers who need to comply with the risk management process should review their current processes and procedures and make any necessary adjustments.

What are the main phases of the risk management process?

Preliminary system definition

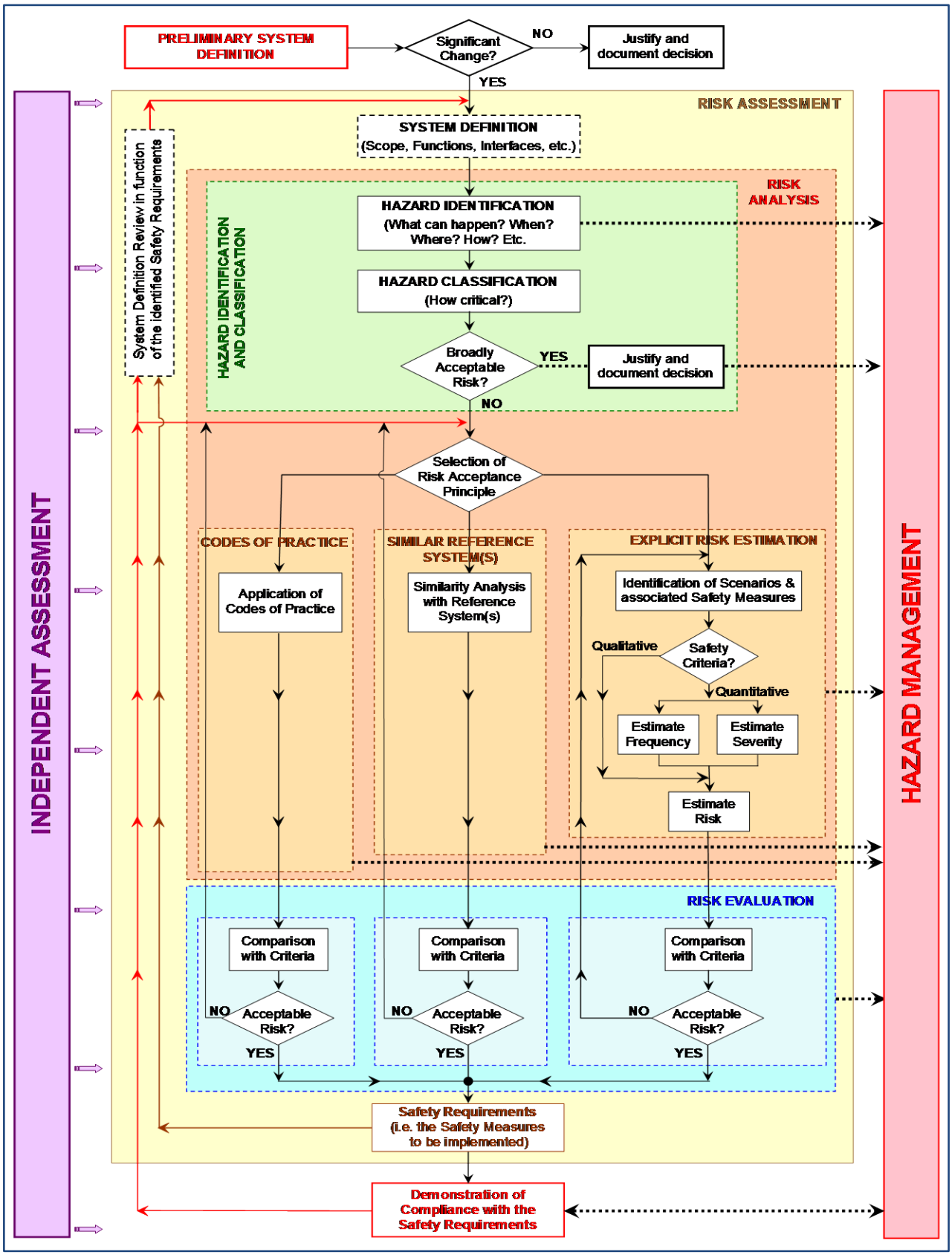
3.4 In order to assess whether the change is significant or not, the proposer should conduct a preliminary system definition. This 'preliminary system definition' is in effect an analysis of what is being changed and a preliminary risk assessment of that change. The 'preliminary system definition' should

- give a clear statement on what is being changed and the scope of the change; and
- address the information described in paragraph 3.10(a) to (d) to the extent necessary to enable the proposer to determine the significance of the change.

System definition

3.5 The risk assessment process starts with the system definition (which can use information from the preliminary system definition). This provides the key details of

Figure 2: Risk management process and independent assessment



the system that is being changed - its purpose, functions, interfaces and the existing safety measures that apply to it. In most cases, the hazards which need to be analysed will exist at the boundary of the system with its environment.

3.6 The definition is not static and during iterations of the risk management process, it should be reviewed and updated with the additional safety requirements that are identified by the risk analysis. It therefore describes the condition (or expected condition) of the system before the change, during the change and after the change.

3.7 The system definition may change due to factors other than the specification of safety requirements, such as

- changes in scope;
- changes in client requirements;
- increasing design definition; and
- implementation of changes proposed by contractors and suppliers.

3.8 Such changes may necessitate iteration of the risk management process.

3.9 Equally, changes to the system definition for other reasons may require the proposer to repeat all or part of the process and discuss with the assessment body the implications.

3.10 The risk management process states that the system definition should address at least the following issues:

a) system objective, e.g. intended purpose;

b) system functions and elements, where relevant (including e.g. human, technical and operational elements);

c) system boundary including other interacting systems;

d) physical (i.e. interacting systems) and functional (i.e. functional input and output) interfaces;

e) system environment (e.g. energy and thermal flow, shocks, vibrations, electromagnetic interference, operational use);

f) existing safety measures and, after iterations, definition of the safety requirements identified by the risk assessment process; and

g) assumptions which shall determine the limits for the risk assessment.

3.11 The system definition needs to cover not only normal mode operations but also degraded or emergency mode.

3.12 Consideration of interfaces should not be restricted to physical parameters, such as interfaces between wheel and rail. It should include human interfaces, such as the user-machine interface between the driver and driver displays in the cabs of rail vehicles. It should also include interfaces with non-railway installations and organisations. For example, the interface with road users at level crossings.

3.13 Operational rules and procedures, and staff competence should be considered as part of the system environment. This is in addition to the more usual issues such as weather, electromagnetic interference, local conditions such as lighting levels, etc.

3.14 A good test of whether the system definition is complete and sufficient is if the proposer can describe the system elements, boundaries and interfaces, as well as what the system does.

3.15 The description can effectively serve as a model of the system and should cover

- structural issues (how the system is constructed or made up); and
- operational issues (what it does, and how it behaves normally and in failure modes).

3.16 The existing safety measures, which may change as the risk assessment process progresses, can be added after the structural and operational parts of the model are complete.

3.17 For some projects, the proposer may not know all the environmental or operational conditions in which the altered or new system will operate. In these circumstances, they should make assumptions on the basis of the intended or most likely environment. These assumptions will determine the initial limits of use of the system and should be recorded. When the system is put into use, the proposer (who may be different to the original proposer) should review the assumptions and analyse any differences with the intended environmental and operational conditions.

Hazard Identification

3.18 The purpose of the hazard identification is to identify all reasonably foreseeable hazards which are then analysed further in the next steps.

3.19 The hazard identification should be systematic and structured, which means taking into account factors such as

- the boundary of the system and its interactions with the environment;
- the system's modes of operation (i.e. normal/degraded/emergency);
- the system life cycle including maintenance;
- the circumstances of operation (e.g. freight-only line, tunnel, bridge, etc.);
- human factors;
- environmental conditions; and
- relevant and foreseeable system failure modes.

3.20 While the risk management process does not require that any specific tools should be applied, many of the more well-known techniques will be relevant, including

- structured group discussions;
- checklists;
- task analysis;
- hazard and operability studies (HAZOPs);
- hazard identification studies (HAZIDs);
- failure mode and effects analysis (FMEA);
- fault trees; and
- event trees.

3.21 Whichever technique is used, it is important to have the right mixture of experience and competence while maintaining impartiality and objectivity. Correct hazard identification will underpin the whole risk management process and give assurance that the risks will be managed in the project.

3.22 The risk management process uses the term 'broadly acceptable'[1] to identify those hazards which need not be analysed further. In this context, 'broadly acceptable' applies to those hazards where the risk is, to all intents and purposes, insignificant or negligible. This could be because the hazard is so unlikely to arise that there are no feasible control measures that could be used to control the risk it creates or where there is a credible failure mode but the consequences are negligible. An example of a very low frequency, very high severity event is a 'meteorite impact; and an example of a high frequency, very low severity event is a 'paper cut'. By screening out the 'broadly acceptable' hazards at this stage, the risk analysis can focus on the more important hazards to manage. It is unlikely that many hazards will be screened out in this way.

3.23 The level of detail of the hazard identification depends on the system that is being assessed and needs to be sufficient to ensure that relevant safety measures can be identified. If, following a high level hazard identification, it can be successfully demonstrated that the hazard can be controlled by application of one of the three risk acceptance principles required by the risk management process (see paragraph 3.26), then no further hazard identification is necessary unless it is required as part of the application of the explicit risk estimation principle. If it is not possible to have sufficient confidence at this stage, then the high level hazard may be broken down in to its component parts allowing further analysis of the causes and consequences and identification of relevant measures to control the risks arising. The risk management

[1] 'Broadly acceptable' in the Regulation does not have the same meaning as it has in the HSE tolerability of risk framework (see 'Reducing Risks, Protecting People')

process continues until it can be shown that the overall system risk is controlled by one or more of the risk acceptance principles.

3.24 Hazard identification is still necessary for those changes where the hazards are to be controlled by the application of codes of practice or by comparison to reference systems. Hazard identification in these cases will serve to check that all the identified hazards are being controlled by relevant codes of practice or by adopting the safety measures for an appropriate in-use system. This will also support mutual recognition and transparency. The hazard identification can then be limited to verification of the relevance of the codes of practice or reference systems, if these completely control the hazards, and identification of any deviations from them. If there are no deviations, the hazard identification may be considered complete.

3.25 The purpose of risk analyses and evaluation is to identify those safety requirements and measures that are necessary to control the risks arising from the identified hazards.

Risk acceptance principles

3.26 Hazards can be analysed and evaluated using one or more of the following risk acceptance principles:

- the application of codes of practice;
- a comparison with similar systems (reference systems); or
- an explicit risk estimation.

3.27 In the UK, you can choose any of these three risk acceptance principles. However, if a proposer is seeking mutual recognition in another EU Member State, they should check whether there is a notified national rule restricting the choice of risk acceptance principle. If there is, only the required principle(s) must be applied.

3.28 Individual hazards can be closed out by the application of one or more of the three principles. FHowever, it is likely that different principles will be used for different hazards. Any risk assessment conducted under the CSM RA should always be proportionate to the extent of the risk being assessed.

3.29 The CSM RA has been introduced to ensure that levels of safety are maintained or improved when and where necessary and reasonably practicable, in accordance with the requirements of the Railway Safety Directive (2004/49/EC). Applying one or more of the three risk acceptance principles correctly for all identified hazards and implementing suitable control measures should mean that the risk acceptance criteria (see 3.47) has been met. In these circumstances, ORR will not normally require further evidence that the residual risk is acceptable.

Codes of Practice

3.30 Standards and rules have to meet all the following criteria to be used as a code of practice for the risk management process:

- be widely accepted in the railway sector or otherwise justified to the assessment body;
- be relevant for the control of the specific hazard; and
- be available to an assessment body so that it can:
  - assess the suitability of the how the CSM RA is applied and the results of applying it; or
  - mutually recognise any safety assessment report on the same system (see paragraph 4.9).

3.31 Standards and rules that are widely accepted in the railway sector include

- TSIs or other mandatory European standards, for example those used in other EC verifications;
- notified national safety rules;
- notified national technical rules (NNTRs); and
- Euro standards or ISO standards.

3.32 Domestic or UK standards can also be used where they meet the requirements in paragraph 3.30 and are not in conflict with mandatory standards. In particular, Railway Group Standards (RGSs) and Rail Industry Standards (RIS) are widely acknowledged in the UK railway industry. There are a number of other domestic standards that are available to all railway actors that could be considered as codes of practice in certain circumstances such as

- ATOC standards for passenger rail services or passenger rail vehicles;
- Rail Industry Company Standards;
- codes of practice relating to plant produced by the Mechanical and Electrical Engineers Networking Group for the rail industry; or
- relevant British Standards issued by the British Standards Institution; or
- other rail industry standards.

This list is not exhaustive.

3.33 It is also possible to use standards or codes of practice from other sectors, for example aviation and maritime, but these have to be justified and be acceptable to the assessment body (see paragraphs 3.65 - 3.80). The proposer will have to

demonstrate that they are effective in controlling the risks from the relevant hazards in a railway context.

3.34 To be satisfied that a code of practice is relevant for the control of the specific hazards in the system, the proposer needs to

a) know what the hazards are;

b) be able to demonstrate that the code(s) of practice are relevant to the hazards; and

c) be able to demonstrate that application of the code(s) of practice control the hazards.

3.35 In evaluating whether a code of practice controls one or more of the hazards, proposers will need to check, with the support of other affected parties, that it covers the intended application of the system under assessment.

3.36 Deviations from codes of practice are possible where the proposer can demonstrate that at least the same level of safety will be achieved. Mandatory standards such as TSIs and Railway Group Standards include a process for deviating from them.

3.37 Most non-mandatory standards do not have a process for deviating from them. If one or more conditions of the code of practice are not fulfilled but there are residual hazards in the system under assessment that the code of practice is relevant to, the proposer may have to conduct an explicit risk estimation on those hazards. Alternatively, other codes of practice or reference systems could be used.

Reference systems

3.38 Reference systems can be used to derive the safety requirements for the new or changed system. For an existing system to be used as a reference system, a proposer needs to demonstrate that as a minimum:

- it has already been proven in use to have an acceptable safety level and would therefore still qualify for approval in the Member State where the change is being introduced; and
- the system being assessed is used under similar functional, operational and environmental conditions and has similar interfaces as the reference system.

3.39 For technical changes, it is unlikely that evidence of in-service history alone can prove that a high integrity system has an acceptable safety level, given the low failure rates required of such systems. Evidence that sufficient safety engineering principles have been applied in the development of the reference system will need to be confirmed for each new application. Therefore, when a technical system under assessment is compared with a similar reference system, the new technical system

under assessment must comply with the same safety requirements of the old one since they are both used to demonstrate the acceptance of the risk associated with the reference system. ‘Safety requirements' include:

- the redundancy of the architecture used for the reference system;
- the engineering principles; and
- the application of safety and quality processes commensurate with the safety integrity level expected for the technical system under assessment.

Proven in use to have an acceptable safety level

There needs to be robust monitoring of the return of experience of the reference system to demonstrate that it has been ‘proven in use to have an acceptable safety level’. This is the ‘risk monitoring’ part of the risk management process. It aims to check that the failure rate actually achieved by the reference system is not worse than the value used during the predictive risk assessment. It is therefore necessary to monitor the achieved failure occurrence of the reference system and verify that, when failed, the reference system is not in an unsafe state. The number of ‘unsafe’ failure occurrences; the number of items of the reference system already in use; and the number of operating hours per day are all needed to determine the failure rate achieved by the reference system.

3.40 The proposer must use the support of other affected parties to analyse whether one; several; or all hazards are appropriately covered by a similar reference system. If the reference system meets the requirements in paragraph 3.39, and those in paragraph 3.40 for technical changes, the hazards and associated risks covered by that system are considered as acceptable. If there are deviations, the safety requirements can still be used for the hazards that are covered by the reference system, providing the same level of performance can be demonstrated. This may involve further risk assessment and evaluation. If the same performance or better cannot be reached, additional safety measures need to be identified by applying one of the other two risk acceptance principles.

Explicit risk estimation

3.41 Explicit risk estimation is an assessment of the risks associated with hazard(s), where risk is defined as a combination of the rate of the occurrence of the hazard or hazardous event causing harm (the frequency) and the degree of severity of the harm (the consequence).

3.42 The estimation can be qualitative, quantitative or a combination of the two. The choice will be determined by factors such as the availability of quantitative data and

confidence in such data. Any analysis should be proportionate to the potential risks. Any risk assessment should follow a systematic and structured process.

3.43 A typical risk assessment process in the UK rail industry for the type of projects that are likely to be significant would be

- identifying the hazardous events which have the potential to cause injury or death to
  - passengers;
  - workers; or
  - members of the public who are directly or indirectly exposed to the technical, operational, or organisational change being assessed;
- identifying the precursors (i.e. the component, sub-system or system failures, physical effects, human error failures or operational conditions), which can result in the occurrence of each hazardous event;
- identifying the control measures that are in place to control or limit the occurrence of each precursor that cannot be eliminated;
- estimating the frequency at which each precursor and hazardous event can occur;
- estimating or analysing the consequences in terms of injuries and fatalities that could occur for the different outcomes that may follow the occurrence of a hazardous event;
- estimating the overall risk associated with each hazardous event;
- identifying any additional control measures required to ensure that risk is reduced so far as is reasonably practicable; and
- providing clear and comprehensive documentary evidence of the methodologies, assumptions, data, judgements and interpretations used in the development of the risk assessment and the analysis of its results (The results may also need to be accompanied by sensitivity and uncertainty analyses, particularly where the assessment is quantitative and where different safety measures need to be evaluated).

3.44 Explicit risk estimation can be used where

- a proposer is unable to address the hazards identified in the hazard identification stage of the risk management process via a code of practice or comparison with a reference system;
- deviations are necessary from codes of practice or reference systems; or
- a proposer needs to analyse the hazards and evaluate design principles or safety measures.

3.45 The CSM RA does not impose any specific tools and techniques to be used in an explicit risk estimation but:

- The methods used must correctly reflect the system under assessment and its parameters (including all operational modes); and
- The results obtained must be sufficiently accurate to provide a robust basis for decision-making (minor changes in input assumptions or perquisites must not result in significantly different requirements).

3.46 Proposers may find the Rail Industry Guidance Note on risk evaluation and risk acceptance (GE/GN8643) useful for explicit risk estimation.

Risk acceptance criteria for explicit risk estimation

3.47 Risk acceptance criteria are used to judge whether the risk is sufficiently reduced to allow the proposer to accept and implement the change. Risk acceptance criteria can be based on domestic or European legislation. Depending on the risk acceptance criteria, the proposer can evaluate the acceptability of the risk for each associated hazard either individually or collectively. If the estimated risk is not acceptable, the proposer must identify and implement additional safety measures to reduce the risk to an acceptable level. For the UK, this will mean that risks should be reduced 'so far as is reasonably practicable' (see ORR SFAIRP guidance).

3.48 An important exception relates to when hazards arise as a result of failures of the functions of a technical system. In these cases the proposer can choose to use harmonised design targets if the system has the potential to lead to either catastrophic or critical accidents. However, if the proposer wants the acceptance of the change to be mutually recognised in another Member State the use of the harmonised design targets is mandatory.

A **catastrophic accident** is one that typically affects a large number of people and results in multiple fatalities. In cases where a failure has a credible potential to lead directly to a catastrophic accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be highly improbable (i.e. an occurrence of failure at a frequency less than or equal to 10-9 per operating hour).

A **critical accident** is one that typically affects a very small number of people and results in at least one fatality. In cases where a failure has a credible potential to lead directly to a critical accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be improbable (i.e. an occurrence of failure at a frequency less than or equal to 10-7 per operating hour).

3.49 The harmonised design targets can be used for the design of electrical, electronic and programmable electronic (E/E/PE) technical systems. But they cannot be used for

- the design of purely mechanical technical systems;
- controlling hazards arising from the purely mechanical part of a technical system; or
- overall quantitative targets for the whole railway system of an EU Member State.

3.50 Please see the guidance published by the Agency on its website, which gives more details on how harmonised design targets should be applied.

3.51 It is possible for an EU Member State to notify a national rule to the Agency which would require a more demanding design target than the harmonised design targets. The UK has no such national rule and at the time of publication, our understanding is that no other Member State had notified a rule.

Hazard record

3.52 The proposer has to create and maintain a hazard record for the system (or part system) that is to be changed. Its purpose is to track progress of the risk assessment and risk management process for the project. The CSM RA requires that it contains certain information but does not mandate any particular format.

3.53 The hazard record should concentrate on key issues. To aid transparency and consistency, it needs to contain the safety measures relating to the identified hazards and the assumptions taken into account in the definition of the system. It needs to include details of the risk assessment principles used and the actors in charge of controlling each hazard.

3.54 When the change has been 'accepted' by the proposer, and is successfully embedded in the system, the hazard record should be integrated by the IM or RU operating the system into its SMS. This may be examined by the national safety authority (NSA) as part of its inspection of a duty holder's SMS.

3.55 The hazard record itself should be updated if

- other significant changes occur that affect the system;
- a new hazard is discovered;
- there are new accident and incident data; or
- assumptions about the system are changed.

3.56 The hazard record, if kept updated, may also be of value where the system is later used as a reference system.

3.57 There may be more than one hazard record if there are several bodies participating in the change. If separate hazard records are maintained during the project, the proposer is responsible for co-ordinating the production of an overall record.

Other documentation

3.58 The CSM RA places some minimum requirements on proposers to document certain information to assist the assessment body. These are

- a description of the organisation and the experts appointed to carry out the risk assessment process;
- the results of the different phases of the risk assessment and a list of all the necessary safety requirements to be fulfilled in order to control the risk to an acceptable level;
- evidence of compliance with all the necessary safety requirements; and
- all assumptions relevant for system integration, operation or maintenance, which were made during system definition, design and risk assessment.

Demonstration of system compliance

3.59 The proposer 'accepts' the change in the system and is responsible for its safe integration and operation in the wider railway system. This means ensuring that the system is designed, validated and accepted against the safety measures identified to control the hazards. Before acceptance, the proposer needs to demonstrate that the risk assessment principles have been correctly applied and that the system complies with all specified requirements. The proposer has overall responsibility for coordinating and managing the demonstration that the safety requirements are met. Other organisations involved will need to demonstrate that they have met the safety requirements and implemented safety measures at the lower level for the part of the system which they are responsible.

3.60 The proposer allocates the safety requirements to each part of the system that was defined in the system definition, but these can also be transferred to other organisations. If that happens, it should be recorded as such in the hazard record. Contracts may be required to reflect these agreements.

3.61 Many hazards, and the risks arising, will be at shared interfaces and cooperation will be needed to ensure that such risks are properly assessed and controlled.

3.62 The demonstration of compliance can involve further activities including causal analyses, testing, etc. It is also possible that new hazards may be identified during

the validation phase which will need to be analysed further. Where a non-compliance with safety requirements is discovered, then the proposer must be notified. The proposer must then further notify others who are affected and responsible for the same or similar subsystems so that they can take the appropriate action.

Independent assessment

3.63 The CSM RA requires an independent assessment of

- how the risk management process is applied; and
- the results from the risk management process.

3.64 An assessment body must carry out the independent assessment.

3.65 The proposer is able to choose (subject to certain restrictions) the assessment body, unless there is a national rule in an EU Member State that requires certain bodies or persons to be used. There is no such national rule in the UK.

3.66 The proposer is required to appoint an assessment body at the earliest appropriate stage of the risk assessment process. However, ORR recommends that the assessment body is involved from the beginning of the project so that it can monitor the development of the hazard record, consider other relevant material (such as a safety plan) and possibly ask to observe tests. This may also include the detailed design stage or the manufacturing stage of the project.

3.67 The assessment body must meet the criteria set out in the CSM RA (included in this guidance at Annex 2). It must be either accredited, recognised, or an NSA. However, if the proposer does not require the significant change to be mutually recognised in one or more other EU Member State the CSM RA allows the proposer to appoint an assessment body meeting relaxed criteria agreed by the NSA. ORR has developed relaxed criteria for the UK and these are set out in Annex 3 of this guidance. A proposer (or assessment body) wishing to use the relaxed criteria may do so without further recourse to ORR. However, the proposer must provide ORR with details of any assessment body it engages which makes use of the relaxed criteria. See paragraphs 3 – 7 of Annex 2 for further details on the relaxed criteria.

3.68 The proposer can appoint an assessment body external to the organisation or an in-house assessment body. Factors that enable the proposer to demonstrate that an in-house assessment body is independent include

- different line management;
- no involvement with the development of the safety measures associated with the system under assessment; and
- freedom from undue commercial influence or bias.

3.69 The assessment body can be made up of more than one organisation.

3.70 The scale and complexity of any given project may determine whether an external or in-house assessment body is used. For more complex projects, or those where the proposer is unfamiliar with the technical analytical skills needed for the assessment, access to external independent assessment may be needed.

3.71 The process for taking the decision about use of internal or external assessment bodies should be recorded. Relevant factors include

- evidence to satisfy the proposer that the assessment body is independent and competent;
- absence of financial pressure or incentives on the assessment body (noting that the proposer cannot control financial pressure or incentives from third parties);
- checks that the assessment body has civil liability insurance, if it is an external organisation; and
- appropriate policies relating to confidentiality rules, if the assessment body is an external organisation.

3.72 At the conclusion of the independent assessment, the assessment body produces a safety assessment report and this should facilitate the proposer's review of the management of the safety system. If the proposer disagrees with any part of the safety assessment report it must keep a record of this with clear justification for its disagreement.

Declaration by the proposer

3.73 When the proposer receives the safety assessment report at the end of the risk management process it must produce a written declaration confirming that all identified hazards and associated risks are controlled to an acceptable level.

3.74 If the change to the system requires an authorisation for placing in service the proposer's declaration will be accepted by the

- NoBo when delivering a conformity certificate (unless it justifies and documents its doubts about the assumptions made or the appropriateness of the results from the assessment); and
- NSA in its authorisation decision (unless it can demonstrate the existence of a substantial safety risk).

3.75 If the change to the system does not require an authorisation for placing in service, then the proposer's declaration must be kept as part of its records.

Avoiding duplication of assessment processes

3.76 There are a number of assessment processes required under different laws:

- assessment of conformity with TSIs (by a NoBo);
- assessment of conformity with NNTRs (by a DeBo);
- assessment of safety certificates for RUs (by an NSA);
- assessment of safety authorisations for IMs (by an NSA);
- independent assessment under the CSM (by an assessment body); and
- assessment of the system of maintenance of ECMs (by a certification body}.

3.77 ORR's position is that there should not be duplication when these processes are carried out, and there are opportunities for businesses to avoid duplication by being aware of the following points:

- A NoBo can act as an assessment body as long as it meets the criteria in the CSM RA. So, if the significant change concerns sub-systems that are covered by TSIs, it is possible to appoint a NoBo that meets the criteria for independent assessment so that it can carry out the CSM assessment as well as the assessment of conformity with TSIs. Similarly it is possible to appoint a DeBo that meets the criteria for independent assessment so that it might carry out the CSM assessment as well as the assessment of conformity of NNTRs.
- If ORR has issued a safety certificate or authorisation, then the assessment body does not need to examine the general processes for risk assessment during the application of the CSM RA, but should look only at how the processes are applied for the specific change. However, if the assessment body finds that there are issues with the general processes for risk assessment these should be reported to the NSA and the proposer.
- If the proposer does not have a safety certificate, safety authorisation, or ECM certificate, then quality management systems may give the assessment body assurance about the general processes for change management and risk assessment within the proposer's organisation.
- If the proposer does not have a safety certificate or safety authorisation, the proposer should as far as possible apply equivalent change management and risk assessment processes to those of the duty holder (IM or RU) who is likely to introduce that significant change onto the railway system.

3.78 The CSM RA allows, but does not oblige, NSAs to act as an independent assessment body when a significant change also concerns

- an authorisation for placing a structural sub-system or vehicle into service; or

- an update or revision of a safety certificate or safety authorisation.

3.79 ORR does not intend to act as an assessment body in these circumstances.

Further information and references

ORR guidance

ORR guidance on assessing whether risks on Britain's railways have been reduced so far as is reasonably practicable

http://orr.gov.uk/__data/assets/pdf_file/0007/2140/rgd-2009-05.pdf

Agency guidance

Agency explanatory note on the CSM RA assessment body

http://www.era.europa.eu/Document-Register/Documents/ERA-GUI-01-2014-SAF%20EN%20V1.0.pdf

Industry guidance

RSSB guidance: Taking Safe Decisions

http://www.rssb.co.uk/risk-analysis-and-safety-reporting/risk-analysis/taking-safe-decisions

RSSB guidance on preparing and using company risk assessment profiles

http://www.rssb.co.uk/risk-analysis-and-safety-reporting/risk-assessment-guidance

RSSB guidance on the management of change (including six complementary Rail Industry Guidance Notes)

http://www.rssb.co.uk/improving-industry-performance/management-of-change

RSSB guidance on the use of cost-benefit analysis when determining whether a measure is necessary to ensure safety so far as is reasonably practicable

http://www.rssb.co.uk/Library/risk-analysis-and-safety-reporting/2014-guidance-safety-related-cba.pdf?web=1

GE/GN8640 – Guidance on planning an application of the common safety method on risk evaluation and assessment

http://www.rssb.co.uk/rgs/standards/GEGN8640%20Iss%201.pdf?web=1

GE/GN8641 – Guidance on system definition

http://www.rssb.co.uk/rgs/standards/GEGN8641%20Iss%201.pdf?web=1

GE/GN8642 – Rail Industry Guidance Note on hazard identification and classification

http://www.rssb.co.uk/rgs/standards/GEGN8642%20Iss%202.pdf?web=1

GE/GN8644 – Rail Industry Guidance Note on safety requirements and hazard management

http://www.rssb.co.uk/rgs/standards/GEGN8644%20Iss%201.pdf?web=1

GE/GN8645 - Guidance on independent assessment

http://www.rssb.co.uk/rgs/standards/GEGN8645%20Iss%201.pdf?web=1

EN 50126:1999 Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS) applicable to electro and electro-mechanical subsystems

http://shop.bsigroup.com/ProductDetail/?pid=000000000030228795

4. The role of the assessment body

What is the role of the assessment body?

4.1 The assessment body is appointed by a proposer to carry out independent assessment of

- how the risk management process in the CSM RA is applied; and
- the results obtained from the risk management process.

4.2 This could involve a sample or vertical audit to check

- the correct application of the processes to the specific change (but not the question of whether the change is significant or not);
- adequate definition of the part of the system that is being changed ;
- robust process for hazard identification and that the hazard identification appears to be complete;
- justified classification of hazards associated with a broadly acceptable risk;
- correctly applied risk acceptance principles (see paragraph 3.26);
- satisfactory demonstration of compliance with safety requirements;
- the hazard record contains the right information about: the hazards and their associated safety measures; and the responsibilities of the main parties involved for those hazards; and
- hazards and the associated safety measures are closed and validated.

4.3 To carry out the independent assessment, the assessment body must

- ensure that it has a thorough understanding of the significant change based on the documentation provided by the proposer;
- conduct an assessment of the processes used for managing safety and quality during the design and implementation of the significant change, if those processes are not already certified by a relevant conformity assessment body; and
- conduct an assessment of the application of those safety and quality processes during the design and implementation of the significant change.

4.4 Once the assessment body has completed its assessment as described in paragraph 4.3 it must deliver the safety assessment report as described below.

4.5 The proposer is required to appoint an assessment body at the earliest appropriate stage of the risk assessment process. However, ORR recommends that the

assessment body is involved from the beginning of the project so that it can monitor the development of the hazard record, consider other relevant material (such as a safety plan) and possibly ask to observe tests. This may also include the detailed design stage or the manufacturing stage of the project. The assessment body must ensure that its involvement in these activities does not jeopardise its independence. The assessment body's role in oversight does not remove the responsibility of the proposer for overall safety. In all cases **the proposer remains responsible for safety and takes the decision to implement the proposed change**.

4.6 The Agency has published on its website an explanatory note on the CSM RA assessment body.

Safety assessment report

4.7 At the conclusion of the assessment, the assessment body produces a safety assessment report and this should support the proposer in taking the decision on the safety of the system. If the proposer disagrees with any part of the safety assessment report it must keep a record of this with clear justification for the disagreement.

4.8 If the change to the system also requires an authorisation for placing in service, then the safety assessment report should also be submitted to the NSA with the technical file and other documentation. The NSA will take this into account in considering the authorisation. If there is an authorisation for placing in service and the proposer disagrees with any part of the safety assessment report it must keep a record of this on the technical file with clear justification for the disagreement.

4.9 Where an assessment body has delivered a safety assessment report, that report must be mutually recognised by any other assessment body, providing the system is used under the same conditions and equivalent risk acceptance criteria are applied.

4.10 In accordance with Annex III of the CSM RA the safety assessment report must contain as a minimum the following information:

a) identification of the assessment body;

b) the independent assessment plan;

c) the definition of the scope of the independent assessment as well as its limitations;

d) the results of the independent assessment, including in particular:

   i) detailed information on the independent assessment activities for checking the compliance with the provisions of the CSM RA; and

   ii) any identified cases of non-compliance with the provisions of the CSM RA and the assessment body's recommendations; and

e) the conclusions of the independent assessment.

5. Miscellaneous requirements for specific duty holders

Railway undertakings and infrastructure managers

5.1 RUs and IMs should undertake periodic audits of the application of the CSM RA as part of their SMS arrangements

5.2 As part of their annual safety report to ORR, RUs and IMs must include

- a summary of experience in applying the CSM RA; and
- a summary report on the decisions related to significance of change.

Entities in charge of maintenance

5.3 All ECMs should undertake periodic audits of the application of the CSM RA as part of their maintenance system as referred to in regulation 18A of ROGS.

5.4 As part of their annual maintenance report to the certification body, ECMs responsible for freight wagons must include a summary of experience in applying the CSM process.

5.5 ECMs responsible for vehicles that are not freight wagons must also share their experience with the Agency, which will coordinate the sharing of this information with NSAs.

Supervision by national safety authorities

5.6 ORR, or the safety authority in another EU Member State, may check the process that

- RUs;
- IMs; and
- ECMs not responsible for freight wagons but registered in the national vehicle register,

have used to determine how to apply the CSM RA. Proposers must therefore keep a record of how they have arrived at their decisions, particularly in relation to the test for significance.

5.7 The process that freight wagon ECMs use may be checked by ORR, or another certification body, as part of its surveillance activities.

Annex 1: Determining the significance of a change

1. When a proposed change has an impact on safety, the CSM RA requires the proposer to decide, by expert judgement, the significance of the change based on stated criteria (Article 4[2]).

2. These criteria are:

   - **failure consequence**: credible worst-case scenario in the event of failure of the system under assessment, taking into account the existence of safety barriers outside the system;
   - **novelty** used in implementing the change: this concerns both what is innovative in the railway sector, and what is new just for the organisation implementing the change;
   - **complexity of the change**;
   - **monitoring**: the inability to monitor the implemented change throughout the system life-cycle and take appropriate interventions;
   - **reversibility**: the inability to revert to the system before the change;
   - **additionality**: assessment of the significance of the change taking into account all recent safety-related modifications to the system under assessment and which were not judged as significant.

3. The CSM RA does not prescribe how to use the criteria, or the priority or weighting given to any of them. The method described here may be useful to proposers and provide some structure for taking these decisions.

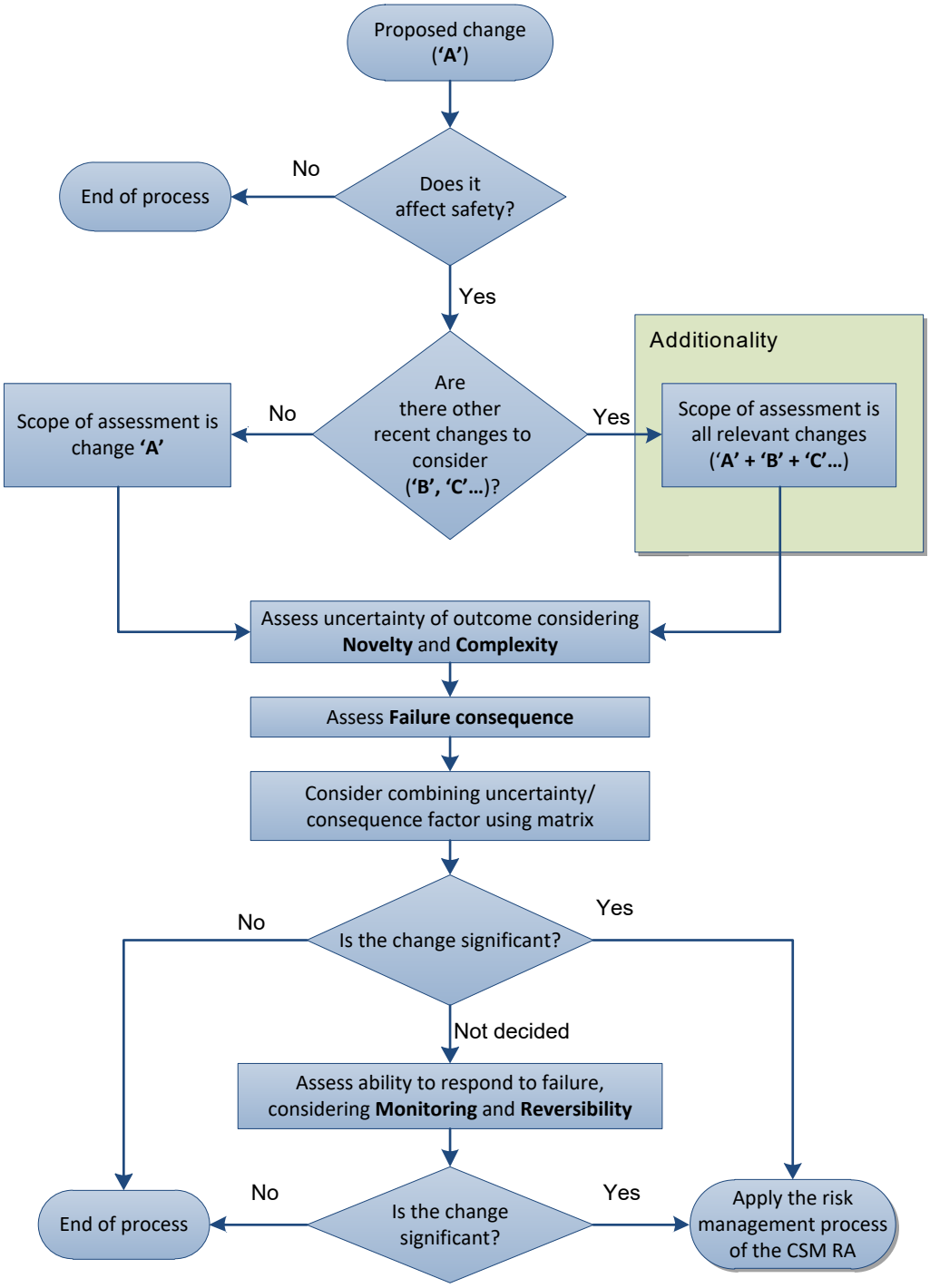
Methodology for using the criteria

4. It is likely that the proposer will need to undertake some preliminary work to identify and understand the relevant hazards before applying the significance test. A good overall understanding of all the hazards will help with identifying the most appropriate risk acceptance principle.

5. For a significant change the proposer must produce “a written declaration that all identified hazards and associated risks are controlled to an acceptable level”. The proposer must also be confident that risk is controlled to an acceptable level if a change is not significant.

6. Taking the criteria together, it would be reasonable to conclude that a change is not significant if the proposer

Figure 3: A proposed approach to applying the criteria for determining significance



- is confident that it has identified all significant hazards (i.e. those that give rise to non-negligible risk); and either
- knows how it will control the associated risk to an acceptable level; or
- is confident that it will be straightforward to identify and implement the measures required to control the associated risk to an acceptable level.

7. If the proposer choses to apply the criteria more explicitly, it is possible to group and sequence the criteria in a way that assists their application. Figure 3 shows a flowchart, which illustrates a proposed application of the criteria.

Additionality

8. Additionality is considered first, as this defines the **scope** of the change that is to be assessed.

9. When a change 'A' is proposed, other recent changes (B, C, …) should be considered and, if necessary, included within the scope of the change subject to the test of significance (that is, if necessary, the change whose significance is to be decided is A + B + C …)

10. Additionality can be described as considering other changes that have been made since the entry into force of the CSM RA (23 May 2013) or since the last application of the risk management process (whichever is later).

11. This would achieve the intention of the CSM RA (which refers to '**recent**' safety-related changes), whilst being practical and not imposing an arbitrary time limit.

Novelty and complexity

12. Novelty and complexity can be thought of as measures of the **uncertainty of outcome** or the likelihood that the proposed change, once implemented, will or will not behave as predicted. Clearly, the more novel and the more complex a change is, the higher the likelihood that it may behave in an unpredicted, and possibly undesirable, way. Therefore, the more novel and the more complex a change is, the more significant it is likely to be.

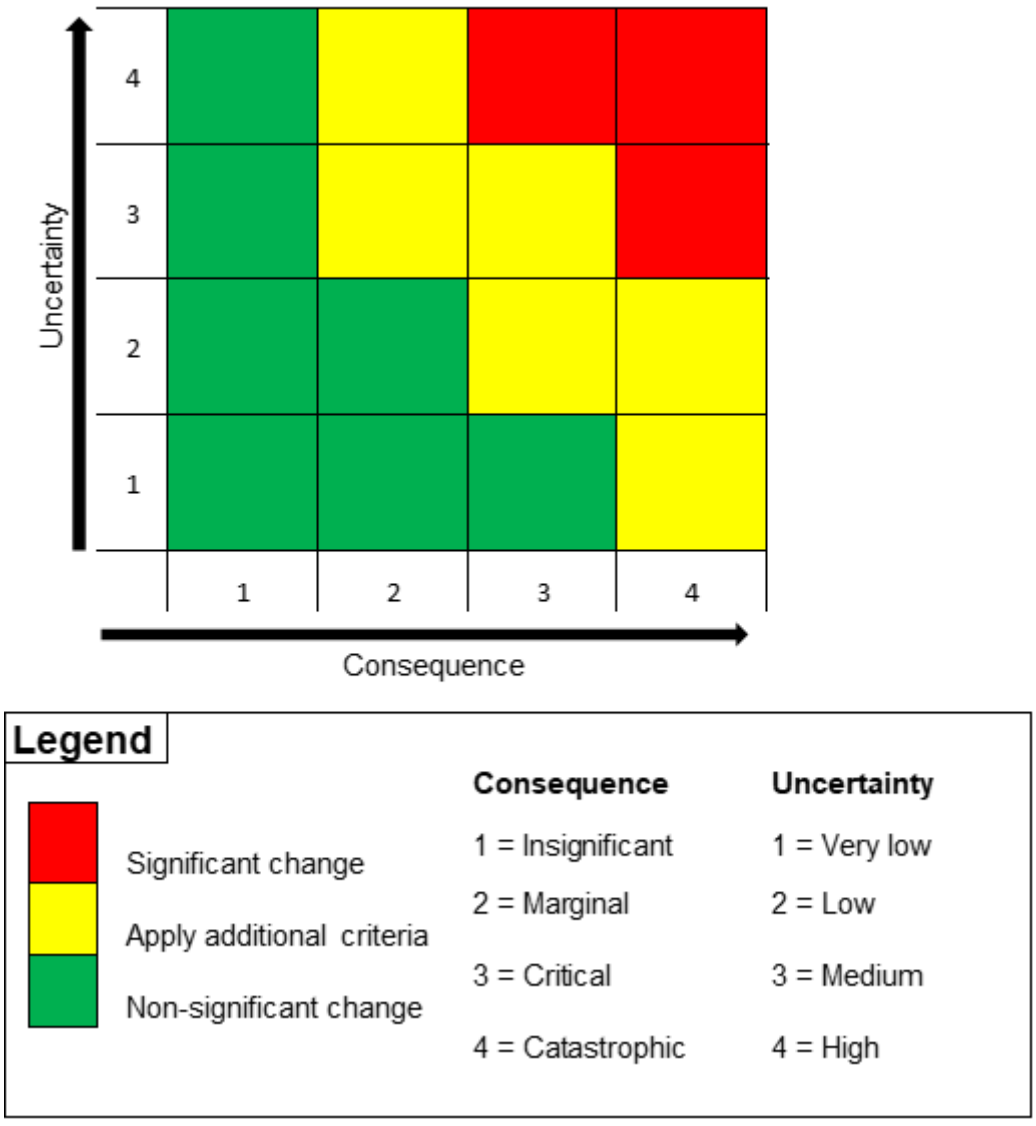
Failure consequence

13. Failure consequence (or **consequence of failure**) is straightforward. This is asking the question "What is the worst that could happen if the system behaves in an undesirable way following the introduction of the proposed change?"

Combining uncertainty of outcome and consequence of failure

14. Risk is usually understood to be *likelihood* x *consequence*. Similarly, *'uncertainty of outcome'* x *'consequence of failure'* can be thought of as a factor measuring the potential scale of a change with respect to safety. The 'uncertainty of outcome' is judged by reference to novelty and complexity.

Figure 4: Combining uncertainty of outcome and consequence of failure



Judging significance

15. It is possible to develop a simple matrix, to assist in making a judgement about whether a proposed change is 'significant' (high uncertainty, high consequence) or 'non-significant' (low uncertainty, low consequence) or where the additional criteria (ability to monitor and reversibility) need to be applied to make a final decision.

Monitoring and reversibility

16. Monitoring and reversibility are additional criteria that should be considered where the decision about whether the change is 'significant' or 'non-significant' cannot be made on the basis of the '*uncertainty of outcome* x *consequence of failure*' test.

17. The criterion in relation to monitoring is 'the inability to monitor the implemented change throughout the system life-cycle and take appropriate interventions'. In essence, this is asking the question "Can I see what is going on and react in time?"

18. But a more complex question to ask when thinking about monitoring as a criterion is "Is it possible and practicable to introduce a system of monitoring that gives sufficient warning early enough to permit effective intervention to prevent or mitigate any hazard arising from the change I have made?" Note that it is not sufficient, for example, to simply install monitoring equipment. Supporting operational procedures are necessary to take note of, and react to, warnings generated by the equipment.

19. Reverting to the system before the change is one possible intervention, though one that is not usually available in the case of engineering change. It should therefore be thought of in the wider sense of:

    The ability (or otherwise) to intervene in a timely manner to prevent or mitigate any hazard arising from the change you have made, when such intervention is indicated by the monitoring arrangements.

20. If it is not possible to adequately monitor the effects of a change so as to be able to 'take appropriate interventions'; or if it is impossible to reverse the effects of a change, it is likely that the change should be considered significant.

21. An example of a possible matrix is shown in Figure 4. Others (3 x 3 or 5 x 5 for example) are possible.

Annex 2: Criteria for assessment bodies

1. The assessment body must be either

   - accredited by a national accreditation body; or
   - recognised by a recognition body (see paragraph 8 below); or
   - the national safety authority (NSA).

2. In the UK the national accreditation body (the United Kingdom Accreditation Service) has been asked to establish an accreditation scheme.

3. Alternatively, a proposer may appoint an assessment body that meets the relaxed criteria in the CSM RA (Article 12) if a significant change does not need to be mutually recognised in one or more other EU Member State. (Mutual recognition is explained in paragraph 13 of Annex 4.) The benefit of this is where the appointment of an accredited or recognised assessment body would be less economical. For example, it could be used for changes that affect only the domestic market (parts of the railway system where international trains would never operate). However, the downside is that using the relaxed criteria does not contribute to establishing mutual trust in the same way that accreditation and recognition does. It does not provide the same level of assurance for the different parts of the railway system concerning the independent assessment of the application of the risk management process and the results obtained. The safety assessment report of an assessment body using the relaxed criteria cannot therefore benefit from mutual recognition enjoyed by accredited or recognised assessment bodies (see paragraph 13).

4. An assessment body making use of the relaxed criteria must meet at least the competency, independence and impartiality requirements in Annex II of the CSM RA when the risk assessment for a significant change is not to be mutually recognised. Other requirements may be relaxed in agreement with the NSA in a non-discriminatory way. ‘Non-discriminatory’ means that any assessment body fulfilling the same relaxed criteria and requirements should be allowed to be appointed on the considered significant change.

5. ORR has developed, in consultation with industry, the relaxed criteria set out in Annex 3 of this guidance. An assessment body, or a proposer selecting an assessment body, may use the relaxed criteria without further recourse to ORR. It is for

   - the assessment body to satisfy itself that it meets the relaxed criteria; or
   - the proposer selecting an assessment body to satisfy itself that the assessment body meets the relaxed criteria.

6. ORR will not provide an approval role in a proposer's decision to appoint an assessment body meeting the relaxed criteria. However, the proposer must provide ORR (rogsguidance@orr.gsi.gov.uk) with details of any assessment body it engages which makes use of the relaxed criteria. We will publish details of the assessment body on our website. The proposer's determination of whether or not an assessment body meets the relaxed criteria in Annex 3 may be checked by ORR as part of its supervision role (see Chapter 5).

7. Even if a proposer does not require a significant change to be mutually recognised in one or more other EU Member State, it may decide to choose an accredited or recognised assessment body over using the relaxed criteria.

8. An assessment body may be accredited or recognised for one, several or all of the areas of competence listed in Box 2.

Box 2: Accreditation and recognition

1. The assessment body has to be accredited or recognised for the different areas of competence within the railway system, or parts of it, for which an essential safety requirement exists. This includes the area of competence involving the operation and maintenance of the railway system.

2. The assessment body has to be accredited or recognised for assessing the overall consistency of the risk management and the safe integration of the system under assessment into the railway system as a whole. This must include competence of the assessment body in checking the following:

Organisation

The arrangements necessary to ensure a coordinated approach to achieving system safety through a uniform understanding and application of risk control measures for sub-systems.

Methodology

Evaluation of the methods and resources deployed by various stakeholders to support safety at sub-system and system level.

Technical aspects

The technical aspects necessary for assessing the relevance and completeness of risk assessments and the level of safety for the system as a whole.

9. The CSM RA allows for recognition of an assessment body by the EU Member State or NSA as follows:

   - recognition by the Member State of:

- an entity in charge of maintenance (ECM);
- an organisation or part of it;
- or an individual;

- recognition by the NSA of the ability of:
  - an organisation or part of it; or
  - an individual

  to conduct independent assessment through the assessment and supervision of the SMS of an RU or an IM;
- recognition by the NSA as ECM certification body of the ability of:
  - an organisation or part of it; or
  - an individual
  - to conduct independent assessment through assessment and surveillance of the system of maintenance of an ECM; or
- recognition by a recognition body designated by the Member State of the ability of:
  - an ECM;
  - an organisation or part of it; or
  - an individual

  to conduct independent assessment.

10. In any of the cases above the person acting as assessment body must be sufficiently independent from the project that it is engaged in (see paragraphs 3.64 to 3.72).

11. ORR, an NSA in another EU Member State, or an ECM certification body has to accept accreditation, or recognition by a EU Member State, as proof of the ability of:

    - an RU to act as an assessment body when granting a safety certificate;
    - an IM to act as an assessment body when granting a safety authorisation; or
    - an ECM to act as an assessment body when granting an ECM certificate.

12. ORR has to accept accreditation or recognition in another EU Member State as proof of the ability of an organisation to act as an assessment body under the CSM RA. This includes when the CSM RA is used when authorising the placing into service of a sub-system.

Can all assessment bodies work EU-wide?

13. The safety assessment report of any assessment body accredited or recognised in an EU Member State in accordance with the requirement of the CSM RA must be recognised across the EU. This also extends to contracting states of OTIF (see the Agency's explanatory note on the CSM RA assessment body).

14. An assessment body accredited in an EU Member State in accordance with the requirements of the CSM RA can carry out independent assessment in the whole of the EU (and in OTIF contracting states).

15. An NSA recognised by its Member State as an assessment body under the CSM RA cannot provide independent assessment in another EU Member State, unless there is a bilateral agreement between the two Member States.

16. An assessment body using relaxed criteria cannot provide independent assessment in another EU Member State.

Annex 3: Relaxed criteria where a significant change is not to be mutually recognised

Introduction

1. Article 12 of the CSM RA requires that where the risk assessment for a significant change is not to be mutually recognised, the proposer shall appoint an assessment body meeting at least the competency, independency and impartiality requirements of Annex II. The other requirements of paragraph 1 in Annex II (see Box 3) may be relaxed in agreement with the national safety authority in a non-discriminatory way.

Box 3: Paragraph 1 of Annex II of the CSM RA

Paragraph 1 of Annex II says the following:

"The assessment body shall fulfil all the requirements of the ISO/IEC 17020:2012 standard and of its subsequent amendments. The assessment body shall exercise professional judgment in performing the inspection work defined in that standard. The assessment body shall fulfil both the general criteria concerning competence and independence in that standard and the following specific competence criteria:

(a) competence in risk management: knowledge and experience of the standard safety analysis techniques and of the relevant standards;

(b) all relevant competences for assessing the parts of the railway system affected by the change;

(c) *competence in the correct application of safety and quality management or in auditing management systems."*

2. The objective is to avoid unnecessary costs being incurred by a proposer when engaging an assessment body in a risk assessment for a significant change that would never require mutual recognition in one or more other EU Member State.

3. The logic, therefore, is that it is the requirements of ISO/EN17020:2012 which are to be relaxed, and also paragraphs 2, 3 and 4 of Annex II of the CSM RA.

4. ISO/EC 17020:2012 contains the following elements:

- Section 1: Scope;
- Section 2: Normative References;
- Section 3: Definitions;
- Section 4: General Requirements
- Section 5: Structural Requirements;

- Section 6: Resource Requirements
- Section 7: Process Requirements:
- Section 8: Management System Requirements:
- Annex A: Independence Requirements for Inspection Bodies
- Annex B: Optional Elements of Inspection Reports and Certificates.

5. Sections 1, 2, 3 and 5 are largely administrative and are concerned with what the standard covers and what the relevant definitions are, as such they may be relaxed within the terms of Article 12.

6. Some elements of Sections 7 and 8 may be relaxed provided that the requirements in paragraph 1(a) – (c) of Annex II of the CSM RA are met.

Sections of ISO/IEC 17020:2012 which must be fulfilled

7. Section 4 (General Requirements) covers independence and impartiality; Section 6 on Resource Requirements deals with the competence aspects of employing the correct personnel; and Annex A deals with independence requirements for inspection bodies. These sections of the standard cannot therefore be relaxed.

8. Using the principles outlined below, it is possible to create a proportionate assessment structure which meets industry needs for assessing a significant change where mutual recognition is not required.

Principles

(i) Facilities and Equipment

The assessment body shall have directly available to it, or should be able to access, all facilities and equipment required to carry out a proper assessment.

This means that the assessment body shall either have, or be responsible for, all the facilities and equipment needed to carry out an assessment, including anything which is required to be calibrated before use, or it shall have the ability to contract for such services as are required to carry out a full and proper assessment. In this latter case the assessment body or its parent organisation will have to conduct all necessary checks to make sure that the services provided by third parties meet the required quality.

(ii) Sub-contracting

An assessment body should carry out the assessments it is contracted to undertake. However, in some cases sub-contracting of specialist activities may be allowed.

This means that for this form of assessment the expectation is that the designated in-house assessment body would carry out assessments for the purposes of an

assessment of a significant change that does not require mutual recognition. However, in some circumstances sub-contracting of specialist functions may be appropriate. If this route is taken the sub-contractor's roles and responsibilities should be clearly specified and the assessment body should satisfy itself that the contractor is competent to carry out the specified duties.

(iii) Assessment Methods and Procedures

The assessment body should use assessment methods appropriate to the scale and extent of the change being assessed.

The assessment body should clearly set out the methods used and the reasoning behind the decision. The assessment body shall have documented instructions for carrying out assessments safely.

(iv) Handling samples and Items

The assessment body shall have in place appropriate procedures and processes for handling assessment samples and items.

There shall be appropriate documentation which allows for the accurate identification of samples and other items which are required as part of the assessment.

(v) Safety Assessment Reports

All safety assessment reports should be produced in a retrievable format and be in line with the format set out in the CSM RA.

If the report includes any information derived from work by sub-contractors this should be clearly specified.

(vi) Management Requirements

An assessment body should have in place an organisation and management structure appropriate to the scale and extent of the change being assessed.

This means having an organisation which allows the proper fulfilment of safety assessment functions. The organisation should be clearly set out and the relationships between the various functions involved described. There should be a designated competent manager in charge of the assessment team, with competent staff in that team and having appropriate job descriptions for the roles involved. There should be a robust document control system in place.

Annex B of ISO/IEC 17020:2012

9. Annex B of the standard concerns inspection reports. As these are optional they could be omitted from the reports of an assessment body engaged in the risk assessment of a significant change which is not to be mutually recognised.

Annex 4: Guidance on organisational change

Purpose

1. This Annex provides high-level guidance on the application of the CSM RA when assessing significant organisational changes.

What is a significant organisational change?

2. It is a requirement of the CSM RA that, when making any technical system, operational or organisational changes which could impact on the safety of the operational railway system, consideration should be given to whether or not the change is 'significant' by applying the six criteria described in the CSM RA.

3. The reasons for the decision that a change is, or is not, significant must be documented. The documentation of this assessment is particularly important where it is decided that a change is not significant, as this may be required to be reviewed should the change be implicated in a safety incident in the future.

4. It is not possible to define explicitly what a significant organisational change is in terms of a particular type of change. A change that is significant for one company/circumstance may not be significant for another company/circumstance. Each change has to be assessed individually in the context in which it is being applied.

5. The first consideration is whether the organisational change is within the scope of the CSM RA – could it impact on the operational or maintenance processes of the railway system?

6. The second consideration is whether the change affects safety, either directly or indirectly. If the organisational change does not affect safety then no further consideration needs to be given in relation to the application of the CSM.

7. If an organisational change does affect safety, one method for assessing whether a change is significant is offered in Annex 1 of this guidance.

Assessing the change

8. The CSM RA presents three 'risk acceptance principles' by which the hazards associated with a significant change can be analysed and evaluated. These are:

   a) the application of codes of practice;

   b) a comparison with similar systems (reference systems); and

   c) an explicit risk estimation.

9. The most likely acceptance principle to be applied to significant organisational change is explicit risk estimation. This can be qualitative. Quantitative risk assessment of the proposed organisational change is not necessarily required.

10. Risk assessment associated with significant organisational changes is not an exact science; it is about managing and organising people, therefore a qualitative or semi-quantitative risk ranking method for assessing organisational changes should meet the requirements of the CSM RA.

11. Most companies already have structured safety validation processes for organisational changes within their existing SMSs which are likely to meet the requirements of the CSM RA. In broad terms for significant organisational changes this would include:

    a) definition of the extent of the change being made;

    b) preparation of disposition statements indicating where the safety responsibilities are transferred from one job description to the job description of the new role;

    c) checking that the new job roles specify the correct competency levels for the safety functions that have been transferred;

    d) carrying out a risk assessment commensurate with the scale of the change to determine the potential impact of the change and that adequate mitigation measures have been put in place;

    e) recording and maintaining the outputs of the risk assessment in a hazard record;

    f) establishing the go-live criteria that need to be achieved before the organisational change is implemented; and

    g) documentation of records relating to (a) to (f) above.

Risk Acceptance criteria

12. The quantitative risk acceptance criteria defined in paragraph 2.5.4 of Annex I of the CSM RA only apply to significant changes relating to technical systems and therefore do not have to be considered in the context of significant organisational changes.

Mutual recognition

13. One of the main principles introduced by the CSM RA is that of mutual recognition. This principle is designed to reduce industry costs by not having to redo risk assessment work when the change can be applied to more than one company in any EU Member State, i.e. once a significant change has been assessed and subject to an independent assessment by an assessment body, the change should be acceptable anywhere in the EU Member States without additional assessment providing the same application conditions apply.

Independent Assessment

14. The CSM RA requires that all significant changes, including organisational changes, are independently assessed by an assessment body, which produces a safety assessment report.

15. The role and requirements of an assessment body are described in Chapter 4 of this guidance. The key to a successful independent assessment is getting the assessment body involved at the early stages of the risk assessment process, including attendance at some or all of the workshops/safety review meetings, as long as independence is maintained and they don't become involved in the design of the change. This will ensure that the assessment body has a good insight into the risk assessment process and the development of the hazard records. Early feedback from the assessment body can help in the development and refining of the risk assessment process being used.

16. The assessment body is required to review the adequacy of the risk assessment process used and determine if the conclusions of the assessment are reasonable based on the results obtained from the assessment. The assessment body does not sign off that the change being made is acceptable from a safety risk perspective. This remains the responsibility of the proposer of the change.

Documentation

17. All stages of the application of the CSM RA should be documented and the hazard record established for use through the implementation of the change.

Risk assessment process

18. There is no defined methodology currently available for risk assessment of organisational change. A qualitative risk assessment based on a structured workshop process and the management of a hazard record derived from the workshops should be adequate to meet the requirements of the CSM RA.

19. This Annex provides an overview of an approach that could be used, based on the risk assessment work that was done for the review of the organisational changes associated with the establishment of the South West Trains/Network Rail Wessex Alliance.

20. The purpose of the workshops would be to identify whether the organisational changes could introduce safety concerns/issues and consider the measures that need to be put in place to control/mitigate any increase in risk. The extent of the workshops depends on the scale of the change, the number of people affected and their role in influencing safety.

21. The workshop(s) will enable individuals who will be affected by the change to better understand the objectives of the change and provide proactive input to the consideration of the safety implications of the change and any additional mitigating measures. The method should involve:

    a) clearly defining the change being made;

    b) identifying who is affected by the change and needs to be consulted including:

        i) staff;

        ii) representative bodies e.g. trades unions;

        iii) interface organisations; and

        iv) other stakeholders

    c) facilitating the structured workshop(s) involving representatives of the groups that could be affected by the change;

    d) the independent assessor attending some or all or the workshops; and

    e) development and maintenance of a hazard record, including the measures to be taken to mitigate the risk from each identified hazard and the current status of the implementation of the control measures.

22. The workshop(s) should be structured into topic areas that could be influenced by the organisational change rather than just a general brainstorming of the issues. The topic areas could include the potential influences on:

    a) the way the SMS is implemented and managed;

    b) the different risk areas such as train accident risk, station risk, on-train risk and infrastructure risk;

    c) management of risk interfaces:

        i) incident/emergency management (on-track, at station, on-train);

        ii) degraded operations - for example, failed train and station safety (e.g. platform-train interface); and

        iii) safety reporting, safety meetings, risk reviews, accident investigation, etc.;

    d) communications;

    e) safety decision making;

    f) operational strategy; and

    g) maintenance strategy.

Identification of safety concerns

23. Attendees should be asked to brainstorm the safety concerns they perceive against each of the topic areas in relation to the proposed organisational changes. The use of post-it notes can be useful here to ensure that each attendee has the opportunity to note down their own perceived issues. This will assist the facilitator in the collation of similar safety concerns into agreed safety concern statements.

24. Given the difficultly in assigning meaningful likelihood and consequence rankings to each safety concern for organisational changes, a simple high, medium and low vulnerability ranking can be considered such as:

    a) High = Major concern – potential for significant degradation in safety;

    b) Medium = Some concern – potential for some degradation in safety; and

    c) Low = Minimal concern – unlikely to significantly affect safety but should be reviewed.

25. As each topic area is reviewed, participants should write their perceived safety concerns and associated vulnerability ranking onto individual post-it notes and place them on a flip chart/wall poster for the topic area divided into the high, medium and low vulnerability rankings.

26. Once all the post-it notes have been put on the relevant category poster the comments should be collated by the workshop facilitator and discussed by the group to produce agreed safety concern statements, including the overall perceived vulnerability ranking for each statement.

Identification of control measures

27. Having identified the safety concerns into agreed safety concern statements and their associated vulnerability rankings, the project team can develop a ranked hazard record. The relevant control/mitigation measures required to address each hazard can then be identified.

28. This can either be done in the workshop environment (if there are not too many safety concerns raised) or as a separate exercise by the project team and fed back to the participants for review.

29. The hazard record containing

    - the agreed safety concern statements with their associated vulnerability rankings;,
    - control/mitigating actions;
    - actions required;

- person(s) responsible for the actions; and
- the status of the actions

can then be managed throughout the implementation phase to ensure the identified control/mitigation measures are put in place.

30. A requirement that the actions from the hazard record relevant to the development and start-up phases are completed should be part of the go-live criteria necessary to be addressed before the organisational change is implemented.

Annex 5: Case study on designing in risk control

1. Given the current investment in electrification, we have taken the example of a route to be electrified for the first time (thereby creating a new energy subsystem) in order to illustrate how the CSM RA and relevant domestic legislation fit together.

1. The process of risk assessment using the CSM RA and the subsequent identification and application of the relevant statutory provisions to a new electrification project can be illustrated as follows:

   Step 1 Significant Change – a proposer decides to electrify its network, applies the CSM RA and recognises it is a significant change. A plan or company process for applying the CSM RA where there is a significant change is essential. A plan is likely to address all the steps below at some stage in the process, however it should require the application of the hierarchy of control set out in Regulation 4 MHSWR early enough to influence the client requirements before pre-construction information is finalised.

   Actions required: – a proposer complies with the CSM RA process and as part of the risk analysis identifies the relevant statutory provisions. The initial risk analysis should identify what information the proposer needs to collect to give to the designer, in particular regarding the future maintenance requirements of the structure as a whole and its use once electrified. In relation to an electrification project, the risk assessment should match the output requirements of the project specification in terms of train paths, speeds, effect on the asset with the asset maintenance requirements to keep the infrastructure in efficient working order (e.g. under Provision and Use of Work Equipment Regulations 1998 (PUWER)) without working on or near live conductors. By ensuring the CSM risk assessment addresses regulation 3 of MHSWR, the proposer will be able to demonstrate it has met the absolute requirements in the legislation. Particular attention should be given to the elimination of hazards by design.

   Step 2 Legislation – identification of the relevant statutory provisions, these will include European legislative requirements as well as HSWA and regulations enacted under it.

   Actions required:– one method of demonstrating compliance could be production of a methodology for identifying relevant statutory provisions, which is wide enough to capture regulations that influence design but might not necessarily be fulfilling a direct safety function. For example, Railways Interoperability Regulations 2011, Supply of Machinery (Safety) Regulations 2008 etc.

Below is a non–exhaustive list of statutory provisions that may be applicable to a new electrical traction system during the detailed design / construction phase / life time operation / decommissioning / dismantling:

(i) Electricity at Work Regulations 1989 (directly related to system design and use)

(ii) Railway Safety (Miscellaneous Provisions) Regulations 1997 (prevention of third parties affecting railway operations and prevention of inadvertent contact)

(iii) Workplace (Health, Safety and Welfare) Regulations 1992 (future use of the modified structure as a workplace)

(iv) PUWER (virtually all the equipment will be work equipment whether part of the electrical system or not)

(v) Confined Spaces Regulations 1997 (may need to be considered as part of the original infrastructure or may need to be designed out of the new one)

(vi) Manual Handling Operations Regulations 1992 (most recent example is 33kg lids for the only specified cable ducting being installed – CDM-C should make sure suppliers / designers can identify safe means of installing)

(vii) Personal Protective Equipment Regulations 1992 (may be appropriate if risks cannot be effectively controlled at any time)

(viii) Work at Height Regulations 2005 (for the future maintenance and use of the structure and during construction phase)

(ix) Supply of Machinery (Safety) Regulations 2008 (for any new machinery as defined that is being installed)

(x) Control of Asbestos Regulations 2006 (to be considered where existing infrastructure is being disturbed)

(xi) Railways and Other Guided Transport Systems (Safety) Regulations 2006 (the requirements for risk assessments under ROGS exclude the assessment of health risks)

(xii) Railway Interoperability Regulations 2011 (the risk assessment must apply consideration of interoperability)

(xiii) Construction (Design and Management) Regulations 2007 (specific duties in managing construction but also application of part 4)

(xiv) Control of Substances Hazardous to Health Regulations 2002 (requires risk assessment if hazardous substances are involved)

(xv) Control of Lead at Work Regulations 2002 (for work on existing structures)

Step 3 Level of Duty – once the relevant statutory provisions have been identified, the proposer will need to identify what the relevant legal duties are and whether they are absolute or subject to the test of reasonable practicability.

Step 4 Approved Codes of Practice – once legislative requirements have been identified, requirements set out in codes of practice that support the regulations should be identified. This step is key when the risk acceptability evaluation takes place under the CSM RA, as application of codes of practice is one of the risk acceptance principles. If all the legislation is not considered by the proposer, then the codes of practice are unlikely to be identified or applied.

Step 5 Guidance – as set out in Step 4, the proposer should identify relevant guidance, specifically that issued by HSE / ORR on what good practice in meeting the relevant statutory provisions looks like. There may also be other guidance to be considered which is specific to a project. For example, for an electrification project, ORR's level crossings guidance for designers is for the highest practicable conductor height to be in place at level crossings.

Step 6 Existing industry standards – a CSM RA approach to risk assessment, which is informed by specific duties, is likely to minimise the risks arising during the project. For example, on a new electrical subsystem, there is a risk of inadvertent contact with energised conductors. There is no Railway Group Standard providing guidance on specific duties, e.g. fencing the railway infrastructure to secure compliance with the Railway Safety (Miscellaneous Provisions) Regulations 1997 or the duty to ensure an electrical system is safe and does not give rise to danger at all times in accordance with the Electricity at Work Regulations 1989. Identifying these legislative measures as part of the CSM RA approach, will minimise risk as advice can be given to designers on what they need to achieve when designing the control measures.

Step 7 Client and future operator's strategic aims – scoping the CSM RA risk assessment broadly from the outset of a project, will ensure that provisions such as "*General principles of prevention*" set out in Schedule 1 to the MHSWR are applied at the outset of the risk assessment process. This can enable the proposer to use the opportunity to introduce strategic aims into the design of a new sub system. For example, the electrical asset policy includes some significant policy safety statements that should be considered at the outset of an electrification project.

2. An approach to CSM RA risk assessment which identifies relevant statutory provisions, codes of practice etc. should ensure duties are met under both European and domestic legislation, whilst avoiding duplication of work. A broadly scoped risk assessment under CSM RA will identify hazards relevant to the entirety of the project, not just the system change. This will negate the need for risk assessments on the

same hazards under different legislation. Consideration of CSM RA at the outset of a project should produce a compliance matrix which systematically identifies all hazards (which could be linked to specific legislative provisions). For example, when scoping a risk assessment for a new electrical subsystem the client will need to undertake a HSG85 (Electricity at Work – Safe Working Practices) style assessment of individual maintenance tasks compared to electrical risk, which will determine when, where and how often electrical isolations are needed and indicate to the designer the future demands for isolations on the subsystem so that sufficient switches, points of isolation and integral earths can be provided in the design.

Annex 6: Glossary of terms and acronyms

Accreditation	An attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity.
Actors	All parties which are, directly or through contractual arrangements, involved in the application of the CSM RA.
Advanced stage of development	When the proposer considers that the planning/construction stage of a project has reached a point where a change in the technical specifications would not be viable on economic, contractual, legal, social or environmental grounds.
Agency, The	European Union Agency for Railways
Assessment body	The independent and competent external or internal individual, organisation or entity which undertakes investigation to provide a judgement, based on evidence, of the suitability of a system to fulfil its safety requirements.
ATOC	Association of Train Operating Companies (now Rail Delivery Group)
Code of practice	A written set of rules that, when correctly applied, can be used to control one or more specific hazards.
DeBo	Designated Body
Designated Body	A person appointed under regulation 31 of RIR as a designated body.
ECM	Entity in charge of maintenance

Entity in charge of maintenance	Any person or organisation that is responsible for the safe maintenance of a vehicle and is registered as an ECM in the national vehicle register. This can include people or organisations such as transport undertakings, infrastructure managers, a keeper (usually the owner of a rail vehicle) or a maintenance organisation
ETCS	European Train Control System
Functional sub-systems	Traffic operation and management; maintenance; and telematics applications for passenger and freight services.
Hazard	A condition that could lead to an accident.
Hazard identification	The process of finding, listing and characterising hazards.
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.
IM	Infrastructure Manager
Interfaces	All points of interaction during a system or subsystem life cycle, including operation and maintenance where different actors of the rail sector will work together in order to manage the risks.
Interoperability constituent	Any elementary component, group of components, subassembly or complete assembly of equipment that is incorporated or intended to be incorporated into a sub-system upon which the interoperability of the rail system depends directly or indirectly; and the concept of a "constituent" covers both tangible objects and intangible objects such as software.
ISO/IEC 17020:2012	An international standard which specifies requirements for the competence of bodies performing inspection and for the impartiality and consistency of their inspection activities.

National accreditation body	The sole body in a Member State that performs accreditation with authority derived from the State.
National vehicle register	A database of vehicles authorised or operated in Great Britain under RIR.
NNTRs	Notified National Technical Rules
NoBo	Notified Body
Notified Body	A body which is responsible for assessing the conformity or suitability for use of the interoperability constituents or for appraising the 'EC' procedure for verification of the sub-systems
Notified national rule	Any national rule notified by Member States under Council Directive 96/48/EC, or Directive 2001/16/EC of the European Parliament and of the Council and Directives 2004/49/EC and 2008/57/EC.
NSA	National safety authority
Proposer	One of the following: (a) a railway undertaking or an infrastructure manager which implements risk control measures in accordance with Article 4 of Directive 2004/49/EC; (b) an entity in charge of maintenance which implements measures in accordance with Article 14a(3) of Directive 2004/49/EC; (c) a contracting entity or a manufacturer which invites a notified body to apply the 'EC' verification procedure in accordance with Article 18(1) of Directive 2008/57/EC or a designated body according to Article 17(3) of that Directive; (d) an applicant for an authorisation for the placing in service of structural sub-systems.
RAC	Risk acceptance criteria The terms of reference by which the acceptability of a specific risk is assessed; these criteria are used to determine that the level of a risk is sufficiently low that it is not necessary to take any immediate action to reduce it further.

Recognition	An attestation by a national body other than the national accreditation body that the assessment body meets the requirements set out in Annex II to the CSM RA to carry out the independent assessment activity specified in Article 6(1) and (2).
Reference system	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.
RDG	Rail Delivery Group (formerly Association of Train Operating Companies
RGS	Railway Group Standard
RIR	Railways (Interoperability) Regulations 2011
Risk	The frequency of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm.
Risk acceptance criteria	The terms of reference by which the acceptability of a specific risk is assessed; these criteria are used to determine that the level of a risk is sufficiently low that it is not necessary to take any immediate action to reduce it further.
Risk acceptance principle	The rules used in order to arrive at the conclusion whether or not the risk related to one or more specific hazards is acceptable.
Risk analysis	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 estimation	The process used to produce a measure of the level of risks being analysed, consisting of the following steps: estimation of frequency, consequence analysis and their integration.

Risk evaluation	A procedure based on the risk analysis to determine whether an acceptable level of risk has been achieved.
Risk management	The systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risks.
ROGS	Railways and Other Guided Transport Systems (Safety) Regulations 2006
RSSB	Rail Safety and Standards Board
RU	Railway Undertaking (also referred to as Transport Undertaking under ROGS)
Safe integration	The action to ensure that incorporating an element of a system into a bigger system does not create an unacceptable risk for the resulting system.
Safety	Freedom from unacceptable risk of harm.
Safety assessment report	The document containing the conclusions of the assessment performed by an assessment body on the system under assessment.
Safety management system	The organisation and arrangements established by an infrastructure manager or a railway undertaking to ensure the safe management of its operations.
Safety measures	A set of actions either reducing the frequency of occurrence of a hazard or mitigating its consequences in order to achieve and/or maintain an acceptable level of risk.
Safety requirements	The safety characteristics (qualitative, quantitative, or both) necessary for the design, operation (including operational rules) and maintenance of a system in order to meet legal or company safety targets.
SFAIRP	So far as is reasonably practicable
SMS	Safety management system
Structural sub-systems	Rolling stock; infrastructure; command control and signalling; and energy.

Sub-system	The whole, or, as the context requires, part of a subdivision of the rail system as specified in sections 1(a) and 1(b) of Annex II to Directive 2008/57/EC - namely structural sub-systems and functional sub-systems and includes a structural or functional sub-system that is intended to become the whole or part of a subdivision of the rail system.
System	Any part of the railway system which is subjected to a change whereby the change may be of a technical, operational or organisational nature.
Technical specification for interoperability	A specification adopted in accordance with Directive 2008/57/EC by which each subsystem or part subsystem is covered in order to meet the essential requirements and ensure the interoperability of the rail system
The Agency	European Union Agency for Railways
Systematic failure	A failure that occurs repeatedly under some particular combination of inputs or under some particular environmental or application conditions.
Systematic fault	An inherent fault in the specification, design, manufacturing, installation, operation or maintenance of the system under assessment.
Technical system	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.
TSI	Technical specification for interoperability

TVM	Transmission Voie-Machine (*English: track-to-train transmission*). A form of in-cab signalling used on high speed railway lines originally deployed in France.

© Crown copyright 2017

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at orr.gov.uk

Any enquiries regarding this publication should be sent to us at orr.gov.uk