



Published by:

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

© Copyright 2014  
Rail Safety and Standards Board Limited

# GN

**GE/GN8641**  
**Guidance on System Definition**  
Issue One: June 2014  
Rail Industry Guidance Note

## Guidance on System Definition

---

### Issue record

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

### Superseded documents

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

### Supply

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

# Guidance on System Definition

## Contents

Section	Description	Page
<b>Part 1</b>	<b>Introduction</b>	<b>4</b>
G 1.1	Purpose of this document	4
G 1.2	Background	4
G 1.3	Copyright	4
G 1.4	Approval and authorisation of this document	5
<b>Part 2</b>	<b>Guidance on Common Safety Method on Risk Evaluation and Assessment</b>	<b>6</b>
G 2.1	General introduction	6
G 2.2	Guidance documents	8
<b>Part 3</b>	<b>Guidance on System Definition</b>	<b>9</b>
G 3.1	Introduction	9
G 3.2	Role of the system definition within the risk management process	9
G 3.3	Preliminary system definition	10
G 3.4	Content of the system definition	12
<b>Part 4</b>	<b>Guidance on System Definition to Support Hazard Identification</b>	<b>13</b>
G 4.1	General	13
G 4.2	System objective	13
G 4.3	System function and elements	14
G 4.4	System boundary and interfaces	14
G 4.5	Safety measures and safety requirements	17
G 4.6	Assumptions and other contextual information	17
<b>Part 5</b>	<b>Guidance on Final System Definition</b>	<b>19</b>
G 5.1	Final system definition	19
<b>Appendices</b>		
Appendix A	Example of a Preliminary System Definition	20
Appendix B	Template for Documenting the Significance Test	21
Appendix C	Example System Definition	22
<b>Definitions</b>		<b>23</b>
<b>References</b>		<b>25</b>

# Guidance on System Definition

---

## Part 1 Introduction

### G 1.1 Purpose of this document

- G 1.1.1 This document gives practitioner level guidance on the application of the risk management process set out in the 'Common Safety Method on Risk Evaluation and Assessment' (CSM RA). Specifically, this guidance is intended to assist infrastructure managers (IMs) and railway undertakings (RUs) in undertaking system definition.
- G 1.1.2 This document is primarily focussed on the application of the process by practitioners within an RU or IM. Others, who need to apply the process or interact with it in some way, should also find it useful. Further guidance for other actors (for example, manufacturers) may be developed over time.
- G 1.1.3 The CSM RA (Commission Regulation (EC) No 352/2009) has applied since 01 July 2012 to all significant changes to the railway system – 'technical' (engineering), operational and organisational, or if required as the risk assessment process by a Technical Specification for Interoperability (TSI).

### G 1.2 Background

- G 1.2.1 Commission Regulation (EC) No. 352/2009 ('the regulation') established a 'common safety method on risk evaluation and assessment' (the CSM RA). The CSM RA, contained in Annex I to the regulation, sets out a mandatory risk management process for the rail industry that is common across Europe. The CSM RA has applied to all significant changes to the railway system since 01 July 2012. The changes may be of a technical (engineering), operational or organisational nature (where the organisational changes could have an impact on the operation of the railway). The CSM also applies if a risk assessment is required by a technical specification for interoperability (TSI); and is used to ensure safe integration of a structural subsystem into an existing system in the context of an authorisation for placing in service in accordance with the Railway Interoperability Directive 2008/57/EC.
- G 1.2.2 Commission Implementing Regulation (EU) No 402/2013 establishes a revised common safety method for risk evaluation and assessment. The revised CSM RA has been in force since 23 May 2013 (meaning it can be used from that date), and will apply from 21 May 2015 (meaning that it must be used from that date), at which time Commission Regulation (EC) No. 352/2009 is repealed. The principal amendments relate to the acceptability of codes of practice, the documentation provided to an assessment body, the content of the safety assessment report and the recognition and accreditation of assessment bodies.
- G 1.2.3 If a project is expected to continue beyond 21 May 2015, the proposer can continue to use the 2009 regulation, provided the project is at 'an advanced stage of development within the meaning of ... Directive 2008/57/EC'.
- G 1.2.4 All references in this document to 'the regulation' refer to Commission Regulation (EC) No 352/2009, unless otherwise stated.

### G 1.3 Copyright

- G 1.3.1 Copyright in the Railway Group documents is owned by Rail Safety and Standards Board Limited. All rights are hereby reserved. No Railway Group document (in whole or in part) may be reproduced, stored in a retrieval system, or transmitted, in any form or means, without the prior written permission of Rail Safety and Standards Board Limited, or as expressly permitted by law.
- G 1.3.2 RSSB members are granted copyright licence in accordance with the Constitution Agreement relating to Rail Safety and Standards Board Limited.

## Guidance on System Definition

---

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

### **G 1.4 Approval and authorisation of this document**

G 1.4.1 The content of this document was approved by a Multifunctional Standards Committee on 25 March 2014.

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

## Guidance on System Definition

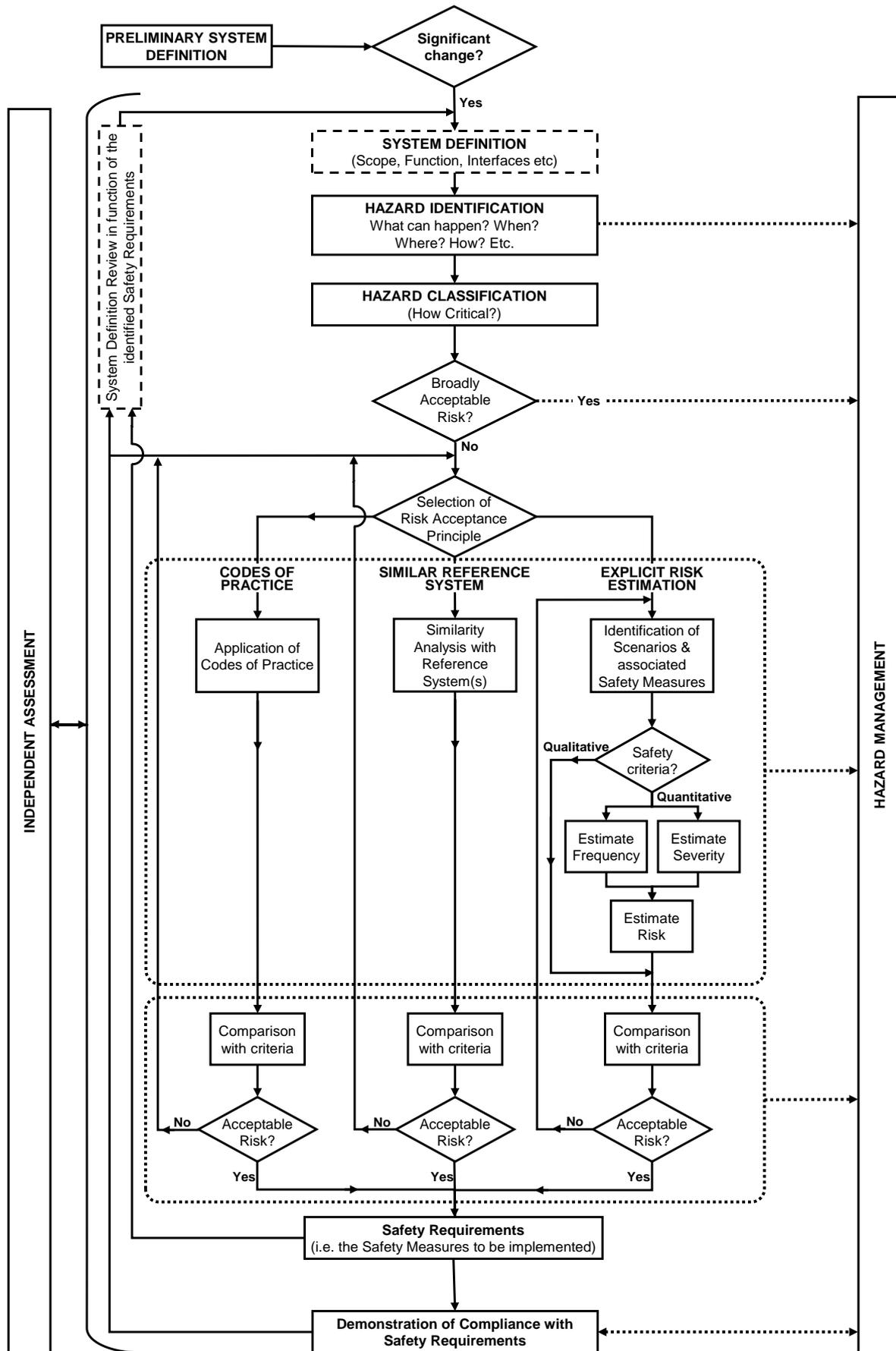
---

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

#### **G 2.1      General introduction**

- G 2.1.1      The CSM RA applies to *'any change of the railway system in a Member State ... which is considered to be significant within the meaning of Article 4 of the Regulation'* that is Commission Regulation (EC) No 352/2009 [the CSM RA itself]. Those changes may be technical, operational or organisational, but are those which could impact the operating conditions of the railway system. The proposer of a change is responsible for applying the risk management process set out in the CSM RA. In many circumstances, proposers will be RUs or IMs. However, a manufacturer may want or need to apply the CSM RA in order to place a new or altered product or system on the market. Once the product is placed on the market, an RU or IM wishing to use the new or altered product or system in a specific application or location will be the proposer of a new change.
- G 2.1.2      Detailed advice on the regulation's requirements, its scope and the significance test that triggers the requirement to apply the risk management process in full, is set out in the Office of Rail Regulation's (ORR's) guidance on the CSM RA. In this section an overview summary of the regulation and its requirements is provided, for the purposes of setting out the context of this guidance and allowing a quick point of reference to the main principles for practitioners.
- G 2.1.3      Figure 1 shows the risk management process defined in the CSM RA. The process essentially consists of the following steps:
- a)      The proposer of a change produces a preliminary definition of that change, and the system to which it relates. It then examines it against the significance criteria in the regulation. If a change is deemed to be significant, then the regulation requires you to apply the risk management process in Annex I and appoint an independent assessment body to assess application of the process. However, the CSM RA risk management process is a sound one and you may choose to apply some or all of it more generally.
  - b)      The CSM risk management process starts with the system definition. This provides the key details of the system that is being changed – its purpose, functions, interfaces and the existing safety measures that apply to it. This system definition will be kept live for the duration of the project.
  - c)      All reasonably foreseeable hazards are identified and their risk is classified and / or analysed.
  - d)      Safety requirements are identified by application of one or more of the three risk acceptance principles to each hazard.
  - e)      A hazard record for the system that is to be changed is produced and maintained. Its purpose is to track progress of the project's risk management process.
  - f)      Before acceptance, the change proposer demonstrates that the risk assessment principles have been correctly applied and that the system complies with all specified safety requirements.
  - g)      The assessment body provides its report to the proposer. The proposer remains responsible for safety and takes the decision to implement the proposed change.

# Guidance on System Definition



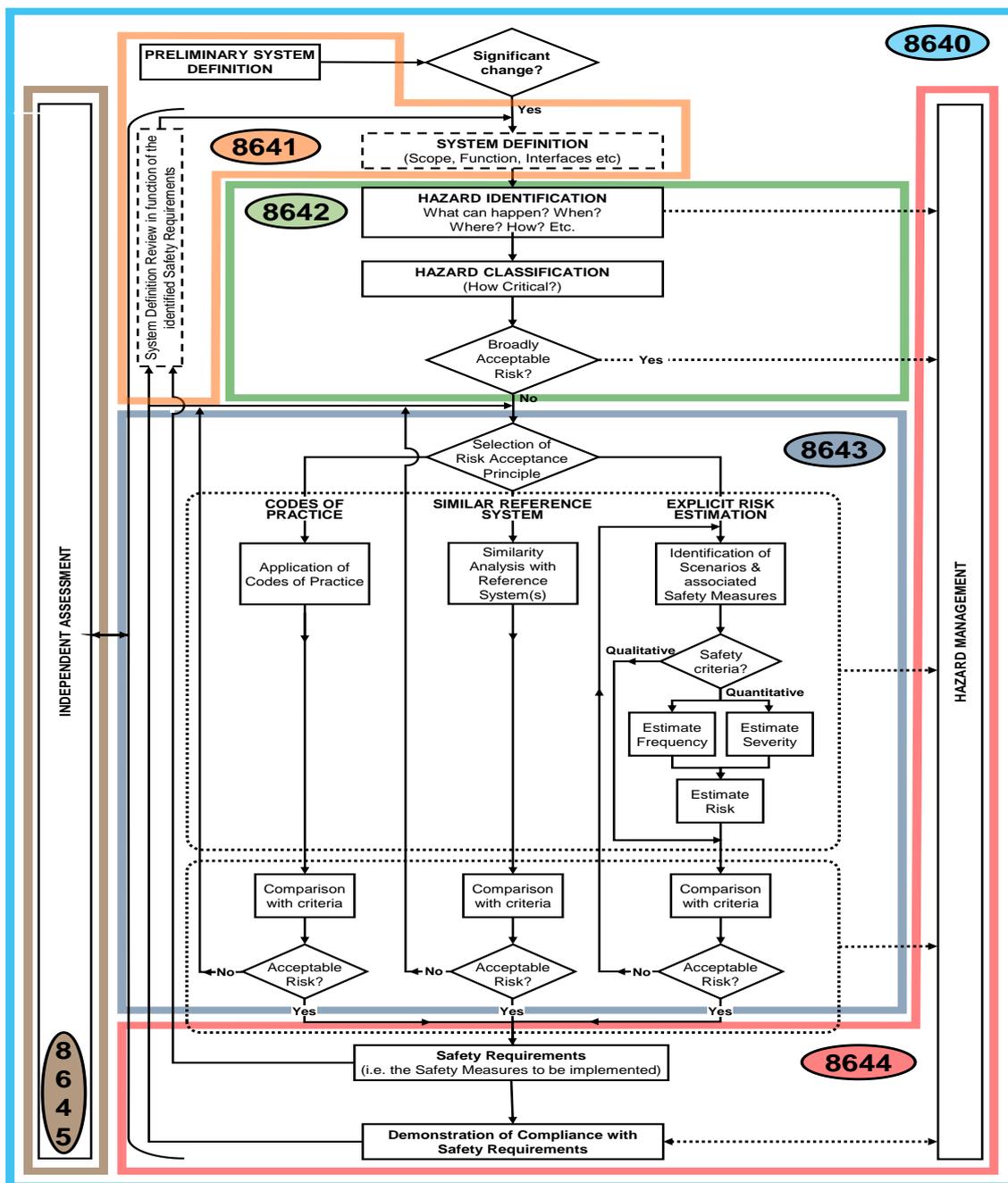
**Figure 1** The risk management and independent assessment process from the CSM RA

# Guidance on System Definition

## G 2.2 Guidance documents

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

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



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

## Guidance on System Definition

---

### Part 3 Guidance on System Definition

#### G 3.1 Introduction

G 3.1.1 The regulation for the CSM RA states that:

*'The risk assessment process is the overall iterative process that comprises:*

- (a) the system definition;*
- (b) the risk analysis including the hazard identification;*
- (c) the risk evaluation.'* (Annex I, clause 2.1.1)

G 3.1.2 Therefore, the system definition required by the regulation is primarily a definition for the purposes of supporting risk analysis and hazard identification. This type of system definition would draw upon the broader project information, but is only one view of it.

G 3.1.3 In order to assess the risk from a change to the railway, it is necessary to draw a boundary round the part of the system that is to be changed. The system definition provides a documented basis for the subsequent hazard identification and risk management work. In particular, it:

- a) Provides a basis and model for assessment.
- b) Provides a better understanding of the interfaces.
- c) Allows for a better understanding of the delivery of a safety requirement. In many cases, the safety of the change will involve actors outside the direct control of the change proposer.
- d) Provides a record of the assumptions on which the safety demonstration ultimately produced is valid.
- e) Provides a record of those things which need to be put in place to deliver a safe change (the safety requirements).

G 3.1.4 The details of a change project are clarified throughout its duration. In order to undertake a robust risk assessment, which is based on sound assumptions, it will therefore be necessary to review the system definition at various stages of the process application.

G 3.1.5 Although not explicitly mentioned in the text of the regulation, a preliminary system definition is needed to carry out the significance test that the regulation requires (see Figure 1). This is recognised in the ORR Guidance (Dec 2012), which states that:

*'In order to assess whether the change is significant or not, the proposer should conduct a preliminary system definition.'* (Clause 3.1)

#### G 3.2 Role of the system definition within the risk management process

G 3.2.1 The system under assessment might comprise:

- a) A change to operational procedures.
- b) An organisational change.

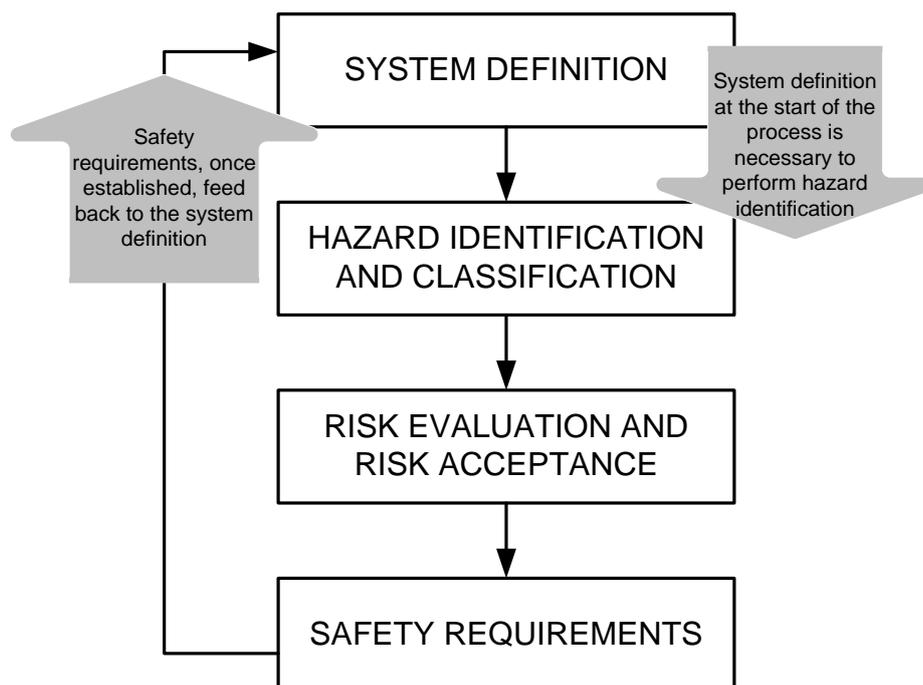
Or

- c) A technical change.

G 3.2.2 Whatever the system's scope, understanding of the reality of the underlying change (and its implications) will gradually develop through the project's life cycle.

## Guidance on System Definition

- G 3.2.3 In some complex projects, many people will be involved. Some will be sub-contracted to the change proposer, who will define the project in the first instance. At the outset, the details of what is to change will not have been fully specified. As the project progresses, however, each of the actors will clarify the detailed aspects of their own work within the bigger project, which will in turn clarify the whole.
- G 3.2.4 The system definition fulfils two roles within a CSM RA assessment. The first is to provide suitable information for the hazard identification and risk analysis. The second is as a repository of the identified safety requirements and project assumptions once the assessment has been completed. These assumptions would, in some cases, encompass application conditions associated with the system's operation.



**Figure 3** Twin purposes of the system definition throughout the life of the CSM RA risk management process

### G 3.3 Preliminary system definition

- G 3.3.1 The ORR Guidance (Dec 2012) states that the:

*'...preliminary system definition' is in effect an analysis of what is being changed and a preliminary risk assessment of that change.* (clause 3.1)

- G 3.3.2 Given its proposed use to support the significance test, the preliminary system definition needs to contain enough information to allow the significance criteria in the regulation to be considered effectively. The regulation states that:

*'When the proposed change has an impact on safety, the proposer shall decide, by expert judgement, the significance of the change based on the following criteria:*

- 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;*

## Guidance on System Definition

---

- (d) *monitoring: the inability to monitor the implemented change throughout the system life-cycle and take appropriate interventions;*
- (e) *reversibility: the inability to revert to the system before the change;*
- (f) *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.’ (Article 4, clause 2)*
- G 3.3.3 The following paragraphs provide guidance on the sort of content that would be necessary to evaluate a project against the stated criteria.
- G 3.3.4 **Failure consequence:** At the early stage of a project, a robust risk assessment may not be available to support the consideration of a), above. However, a preliminary analysis can still be undertaken, which could make use of available information, such as the Safety Risk Model (SRM). The SRM provides a useful checklist of accident types which could help identify hazards. The risk estimates in the SRM are based on observed data and therefore take into account the presence of safety barriers. Alternative sources of information are the generic hazard list in Appendix A of GE/GN8642 or industry ‘bow tie’ models developed by Network Rail. A better understanding of the safety barriers already in place might be obtained by considering controls in place on similar projects. It may be helpful to consider (and review) existing group and company standards that relate to any worst-case consequences identified.
- G 3.3.5 **Novelty:** In order for b), above, to be considered, it is necessary to produce a description of where and when, in implementing the change, it is planned that novel equipment, configurations of equipment or operating practices are to be used. It may also be helpful to identify where there are uncertainties about the exact nature of the solution at this preliminary stage, and where novel systems or processes could be used (for example, where it is known that a certain system is needed but no decision has been made about which particular supplier to source it from). In particular, it is important to understand the overlap between novelty and safety risk, such as where a novel system is planned to be used to deliver some safety-critical functions of the railway.
- G 3.3.6 **Complexity:** There can be technical and organisational complexity. A system – like an engineered system on the railway, say – can be complex in its function or technology and therefore a full description would assess that complexity. In order to understand and assess organisational complexity, some description of the particular organisational structure and contractual arrangements that are to be used to deliver a given change project would also be useful.
- G 3.3.7 **Monitoring:** With respect to d), above, the RSSB document Measuring Safety Performance provides extensive guidance on monitoring safety performance. The key to monitoring is the ability to intervene in time to prevent an accident occurring (see Annex I clause 17 of the ORR Guidance (Dec 2012)). It may be useful to consider the types of monitoring processes used within the IM / RU safety management system, and how they might apply or be adapted to monitor the change. (Note that actors other than the proposer might be best placed to monitor the impact of the change.) A preliminary risk assessment can be used to help identify key safety related processes or functions, whose effectiveness might be considered by monitoring.
- G 3.3.8 **Reversibility:** A description of the wider programme of projects into which the change project fits would help to consider criterion e), above. This is because those projects will be likely to place constraints on the change project. Subsequent work may also depend on the delivery of the change. This includes considering change projects undertaken before the current one is delivered, and those planned for subsequent work. Other issues that might affect the ‘reversibility’ of the project could include the loss of key skills, staff or equipment needed to revert to the previous way of working.
- G 3.3.9 **Additionality:** The description of the wider programme of work might also help with considering the ‘additionality’ described in f), above. The ORR Guidance (Dec 12) suggests that ‘additionality’ should be considered first, as it helps set the scope of the change that is to be assessed.

## Guidance on System Definition

---

G 3.3.10 Early project deliverables, such as a project remit, will provide some of the information needed to develop the preliminary definition. An example of a preliminary system definition relating to an example project for upgrading signalling assets is included in Appendix A.

G 3.3.11 The preliminary system definition can be used to support the judgement of whether or not a change is significant as defined in the regulation. The ORR Guidance (Dec 2012) provides help in making this significance judgement and an example template form to help, which makes reference to the preliminary system definition, is included in Appendix B.

### **G 3.4 Content of the system definition**

G 3.4.1 The regulation 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;*
- g) assumptions which shall determine the limits of the risk assessment.'* (Annex I, clause 2.1.2)

G 3.4.2 As the details of the project emerge and are clarified in various project deliverables over time, the system definition is updated on a rolling basis. The various aspects of the system definition can be elaborated throughout the project, making use of the project information available at each stage, in order to best support the multiple uses shown in Figure 3.

## Guidance on System Definition

---

### Part 4            **Guidance on System Definition to Support Hazard Identification**

#### **G 4.1    General**

G 4.1.1    The regulation states that:

*'The risk management process...shall start from a definition of the system under assessment...'* (Annex I, clause 1.1.1)

G 4.1.2    Therefore, it is useful to consider how the various elements of the system definition set out in G 3.4.1 could be developed to best support risk management. The production of a 'baseline' or reference version of the system definition lets analysis be undertaken on the basis of a clear set of assumptions and provides clarity to the risk management process. This definition can then evolve through application of that risk management process.

G 4.1.3    An example of a consolidated summary definition is set out in Appendix C for a project to introduce driver only operation to a particular passenger train route. The system definition includes information distilled from a range of project documents and outputs which exist to clarify the extent and nature of the changed system and how it is delivered and managed.

G 4.1.4    There is potential for confusion about whether the system definition is a definition of a system or a definition of the change to the system. The regulation implies that the system is defined after the change, as this is what should be made safe. However, in order to make sure that the hazard analysis is complete, all parts of the system that might be relevant to any hazards or risks created by the change should be defined, and some understanding of the nature of the change would be required to allow this judgement to be made.

G 4.1.5    If the change proposer knows where the information used in the definition originally came from, it will help them trace any additional or changed safety requirements that are identified. This is particularly important where documents are specifications of what is going to be delivered. References to key project documentation of this type will therefore help with risk management and the safety demonstration (see GE/GN8644 Guidance on Safety Requirements and Hazard Management and GE/GN8643 Guidance on Risk Evaluation and Risk Acceptance).

G 4.1.6    It may be helpful to those doing risk analysis if additional supporting information, such as photographs or videos, is used to supplement the system definition and aid understanding of it. Information on the use of system definitions to support hazard identification is provided in the accompanying guidance on Hazard Identification.

#### **G 4.2    System objective**

G 4.2.1    The system objective is typically a short statement of the purpose of the changed system. It might include statements about (for example) its reason and function. Depending on the type of change, it is useful to explain the business reason for the change, such as if it is for a specific improvement in capacity, safety or reduction in cost. This information does not directly support the risk analysis exercise, but does provide useful context. Suitable examples would be to:

- a) Facilitate operation to the timetable.
- b) Provide control facilities under failure and emergency conditions and their recovery.
- c) Protect staff during a possession.

## Guidance on System Definition

---

### **G 4.3 System function and elements**

- G 4.3.1 The regulation applies to technical, operational and organisational changes. In order to understand the safety of a system, it is useful to understand not just the technical elements of the system and their function, but also the operational procedures and human actions required. Describing the various functions and procedures in a clear, sequential way, provides a sound basis for a structured hazard identification and risk analysis.
- G 4.3.2 Hazards can often occur during non-standard modes of operation (for example, degraded or emergency working). In order to understand the risks associated with them, it is therefore useful to define these modes of operation for the system under consideration.
- G 4.3.3 The related guidance note on hazard identification provides a description of some hazard identification and analysis techniques and the system representations which they use. There are various techniques for formally describing systems. Details of some of them may be found in Appendix C.

### **G 4.4 System boundary and interfaces**

- G 4.4.1 The regulation requires the boundary of the system to be defined along with its physical and functional interfaces.
- G 4.4.2 A boundary is 'a line which marks the limits of an area; a dividing line' (as defined in the Oxford English Dictionary). In the context of the regulation, a consideration of 'boundaries' tends to occur when referring to:
- The limits of the railway (for example, the boundary between the railway and public areas).
  - Different areas of the railway (for example, the lineside boundary).
  - Organisational or contractual matters, or limits of responsibility (for example, the boundary between an RU's responsibilities and those of a manufacturer delivering a system for them to use).
- G 4.4.3 An understanding of the boundary is important to help to constrain the limits of assessment and the risk assessment and risk management process. To start to analyse a change it is necessary to define an initial understanding of the boundary. Safety requirements should not extend beyond the boundary, although they could reside on the boundary. Assumptions about the nature of the railway or environment beyond the limits of the boundary will need to be made. As understanding progresses, and consideration is given to whether or not these assumptions are true, the understanding of the boundary of the change will improve and the relative position of the boundary might be revised.
- G 4.4.4 An interface is defined in the Oxford English Dictionary as 'a point where two systems, subjects, organizations, etc. meet and interact.' A consideration of interfaces is important, as actions or decisions on one side of the interface might have repercussions on the other.
- G 4.4.5 Identification of the interfaces allows a joint consideration, by appropriate actors from each side of the interface, of how given the change occurring, risk might be impacted on either side of the interface.
- G 4.4.6 Many interfaces across the rail network are understood and well specified, for example in Railway Group Standards or Technical Specifications for Interoperability. In these cases the acceptance of risk could be achieved by using the 'Codes of Practice' risk acceptance principle and implementing the measures from these standards.
- G 4.4.7 There are other interfaces to consider such as:
- Interfaces internal to the change that are under the direct control of the proposer (but might cross internal systems or organisations).
  - Interfaces between the proposers work and another actors work, that are internal to the system under change. Early co-operation is needed to ensure that there is appropriate early consideration of system hazards and resulting safety requirements.

## Guidance on System Definition

---

- c) Interfaces internal to the change that are under the control of another actor. The proposer would need to be confident that these were being considered and that appropriate safety requirements were being developed and put in place.
  - d) Interfaces on the boundary of the change.
- G 4.4.8 Consideration of interfaces that cross the boundary might lead to a realisation that safety measures are needed external to the previous understanding of the boundary. This might be either because inputs to the system under change are potentially hazardous, or because outputs from the system under change have an undesired effect on some external system or process. In either case, additional safety requirements might be necessary and this will cause the boundary of the system definition to be changed.
- G 4.4.9 The regulation says that:
- 'All hazards and related safety requirements which cannot be controlled by one actor alone shall be communicated to another relevant actor in order to find jointly an adequate solution.'* (Annex 1, clause 4.2.)
- G 4.4.10 The regulation also states that:
- '...the risk assessment process shall fall within the responsibility of the proposer. In particular the proposer shall decide, with agreement of the actors concerned, who will be in charge of fulfilling the safety requirements resulting from the risk assessment.'* (Annex 1, clause 1.1.5.)
- G 4.4.11 An understanding of the boundary and interfaces will help the proposer to identify other actors, with whom agreement is, or will be, needed for implementation of safety requirements outside of the proposer's control. Early understanding of the boundary and interfaces enables the key actors to be identified and create the possibility for jointly planning work with them, as the project progresses. This will help to ensure that the requirements that the proposer identifies are able to be put in place in a timely manner, and that the proposer is able to obtain sufficient evidence of their implementation to support its safety demonstration.
- G 4.4.12 The regulation also states that:
- 'When agreement cannot be found between two or more actors it is the responsibility of the proposer to find an adequate solution.'* (Annex 1, clause 1.2.5.)
- G 4.4.13 Hence, the proposer would need to find some other way of managing risk to an acceptable level if:
- a) Other actors do not agree to apply the safety requirements identified for them by the proposer, or they are unable to apply them.
- Or
- b) Appropriate evidence that safety requirements have been met cannot be obtained.
- G 4.4.14 More guidance in the management of risk at interfaces is contained in the supporting document GE/GN8644 Safety Requirements and Hazard Management.
- G 4.4.15 For example, a project proposed by an IM to upgrade life-expired signalling assets in and around a small station might consider some of the interfaces to be:
- a) The interface between a new design and position of signal head and the driver of the trains approaching it. This interface would be between the IM and the RU, and there would be a need for the IM to ensure that the RU had implemented safety requirements around appropriate training and briefing of drivers associated with the new interface. Railway Group Standards define key requirements around such an interface.

## Guidance on System Definition

---

- b) The interface between the track detection equipment and the signalling interlocking. This would be an internal interface for the IM to consider in their analysis.
- c) The electromagnetic emissions from any equipment used might initially be considered to cross the boundary of the change. An initial assumption might be that the levels of emissions would not cause problems for rail and non-rail systems outside the boundary. This assumption would need to be tested and might be dependent on compliance with standards prescribing emission levels, for example.
- d) Similarly it might initially be assumed that emissions from systems external to the change boundary would not impact on the functions of the signalling system, on the basis of compliance with appropriate standards. This assumption would also need to be tested; for example where the signalling system was located near to high power radio transmissions systems.

G 4.4.16 A further example could be for the operational change where an RU wishes to change their dispatch procedures for a number of platforms from driver 'look-back' to the use of platform-mounted cameras and monitors for viewing the train dispatch corridor. In this case some of the interfaces might be:

- a) The interface internal to the system boundary between the RU who is implementing new procedures and the IM who is installing new lineside equipment. The RU and IM need to work together to agree on which systems to put in place and how to go about monitoring their use. Once implemented the RU obtains evidence that the IM had installed the cameras and monitors in accordance with the safety requirements (for example by applying appropriate codes of practice). The IM also provides evidence of the maintenance procedures that are to be applied.
- b) The electrical signal sent from the train detection system to switch on the platform monitors as the train approaches. This is fully under the control of the IM. Evidence that this interface has been managed (including evidence that safety requirements were derived according to the requirements of the regulation and their implementation demonstrated) would need to be passed to the RU as the proposer of the change. The IM would also need to consider if this aspect of the change has any ability to impact on other parts of the railway system (for example the train detection interface with the rest of the command, control and signalling sub-system) and if it was found that it did, this would cause an extension of the boundary of the change.
- c) An interface on the boundary of the system could be sources of light external to the railway that might affect the ability of viewing the monitor. Initially assumptions about the impact of these would be made but these assumptions would need to be tested.

G 4.4.17 For organisational changes, the interfaces and boundaries would include the shared information needed, shared responsibilities or complementary processes and procedures across different organisational structures. These could be internal or external for example:

- a) The interface between a railway undertaking and emergency services, when dealing with an accident.
- b) The interface between a maintenance department and operational department within any transport operator.
- c) The interface between a person planning a possession and the railway undertaking(s) whose services will be affected by it.

## Guidance on System Definition

---

G 4.4.18 In some cases there are interfaces between actors that cross the life cycle stages of an overall project. For example, when new technical systems are being introduced, there is often an initial project to apply the CSM RA risk management process to the technical system itself. The boundary of this change would be closely aligned to the boundary of the technical system. The proposer would need to make assumptions around the operation and maintenance of the technical system, external to that boundary, in order to develop the safety demonstration for this application. A subsequent project, with a separate proposer might involve the putting of that technical system into use. In this case the proposer would consider a wider system boundary, with specific safety requirements addressing operational use and maintenance of the technical system. Many of these requirements would be the implementation of the assumptions of use of the technical system derived from the initial application of the process.

### **G 4.5 Safety measures and safety requirements**

G 4.5.1 The regulation requires the definition of:

*'(f) Existing safety measures and, after iterations, definition of the safety requirements identified by the risk assessment process.'* (Annex I, clause 2.1.2)

G 4.5.2 Where the change relates to some existing part of the railway system, safety measures are likely to be in place already. Documenting these measures will help ensure that the subsequent risk management process considers the extent to which they are still relevant in light of the proposed change.

G 4.5.3 Application of the risk management process generates safety requirements which are identified measures to be put in place in order to ensure that there is an acceptable level of risk. These then become part of the system definition. In addition, any existing safety measures that are necessary to ensure an acceptable level of risk will be recorded in the system definition as safety requirements or assumptions. They are also recorded in the hazard record (further details on the development and use of a hazard record are included in GE/GN8644 Guidance on Safety Requirements and Hazard Management).

### **G 4.6 Assumptions and other contextual information**

G 4.6.1 The CSM on RA states that the system definition should also consider:

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

*g) assumptions which shall determine the limits of the risk assessment.'*  
(Annex I, clause 2.1.2)

G 4.6.2 The system environment characteristics and other assumptions are factors that can control or contribute to hazards or thereby mitigate or exacerbate risk; accordingly, they are inputs to the risk assessment process. Stating assumptions provides a record of the particular circumstances for which the risk assessment and derived safety requirements are valid. In other words, if these assumptions change later, it implies that the risk assessment needs to be reviewed.

G 4.6.3 For example, if a change was being made to the dispatch arrangements for a certain railway route, the change proposer would typically define:

- a) The planned procedure for dispatching trains: as it is through the undertaking of this procedure, or the failure to do so, that risks might arise.
- b) The presence of dispatch-related equipment, and their function (such as door mechanisms and alarms, monitors, cameras or mirrors). This would allow a structured analysis of how effectively these systems support the dispatch arrangements, and consideration of how their failure might lead to a hazard.
- c) The stock type in use, carriage length and numbers of carriages. This would help the risks associated with the dispatch (such as difficulties viewing the whole length of the train on dispatch) to be understood.

## Guidance on System Definition

---

- d) Issues in the environment that might cause risk, such as if a platform were facing east-west, creating the possibility of a dispatcher having their visibility impaired by having to look towards the sun when sending a train out at certain times of the day.
  - e) The known passenger use profile of stations on the route, such as the typical use profile, and potential sources of crowding. This would help the proposer to understand the potential for crowding related risks to arise such as people being pushed towards the train on dispatch, or an increased chance of people being trapped in doors.
- G 4.6.4 There are many factors that might impact upon the safety risk of a change to the railway. There might also be many different combinations of these factors that need to be considered. Typically, a generic definition might be produced and used to assess and identify the risks of the change.
- G 4.6.5 More localised analysis might need to be considered to test the safety requirements and gain confidence in their validity. For example, using the example above, the dispatch risks might be assessed for a route, using general definitions and assumptions. Specific definitions with more targeted information about the specific nature of the dispatch arrangements and characteristics of the particular platforms could then be produced, in order to consider risks in more detail where judged to be necessary.

## Guidance on System Definition

---

### Part 5 Guidance on Final System Definition

#### G 5.1 Final system definition

G 5.1.1 The regulation states that the system definition shall include:

*'(f) existing safety measures and, after iterations, definition of the safety requirements identified by the risk assessment process.'* (Annex I, clause 2.1.2)

G 5.1.2 The system definition therefore develops on a rolling basis and is kept live as work progresses. However, the process of keeping the system definition up-to-date can become more complicated where a number of actors are delivering the project. In such cases an overall system definition is often developed from which more detailed definitions of the sub-systems produced by different actors can be derived.

G 5.1.3 The regulation requires that all hazards and related safety requirements which cannot be implemented by one actor alone are to be communicated to another relevant actor in order to find jointly an adequate solution.

G 5.1.4 Actors in the supply chain to the proposer may undertake their own risk assessment and safety requirements may evolve as a result. Two-way communication between all involved actors is therefore vital. As the project develops, assumptions may change. Ultimately, it is the proposer's responsibility to understand all safety requirements within the scope of their project, and consolidate these into the system definition.

G 5.1.5 It might be that the assumptions in the system definition take the form of safety requirements that others would need to implement (such as ongoing requirements for the maintenance of a technical system). Such assumptions are sometimes referred to as 'application conditions'.

G 5.1.6 Where an IM or RU is using a manufacturer's technical system as part of their project, the manufacturer may not know all the environmental or operational conditions in which the technical system will operate. In these circumstances, if the manufacturer makes assumptions about the safety of the technical system on the basis of the intended or most likely environment of use, then before the system is put into use, the RU/IM will be able to review these assumptions and consider the impact of any differences with the intended environmental and operational conditions. The assumptions would therefore determine the technical system's initial limits of use and be considered 'application conditions'. It should be noted that, in this scenario, the manufacturer may have already applied the risk management process to the technical system.

G 5.1.7 As previously discussed, the information included in the system definition will initially have been defined in a wide array of project documents and deliverables. If the sources of such information are known and understood, it will be easier to feed the safety requirements derived through applying the process back to the actual documents through which they will be specified, implemented and controlled. The ability to link through documents in this way is sometimes referred to as 'traceability'.

G 5.1.8 The process of tracing through safety requirements from their source documentation to the system definition is explained in more detail in GE/GN8644 Guidance on Safety Requirements and Hazard Management.

## Guidance on System Definition

### Appendix A Example of a Preliminary System Definition

<b>Preliminary System Definition</b>	
<b>Target System Overview</b>	To replace signalling assets and equipment in and around xxx station to replace life expired assets and improve ongoing maintenance costs.
<b>Project Overview</b>	<p>Project is to replace outdated signalling equipment and interlocking with modern equivalents. This project will be undertaken in isolation, and led by one contracting entity, with no further engineering work planned subsequently.</p> <p>It is to incorporate:</p> <ul style="list-style-type: none"> <li>- Upgrade of mechanical signal box to Solid State Interlocking and a computer based signalling control system.</li> <li>- Replacement of semaphore signalling system with modern LED equivalents.</li> </ul> <p>Track and point work was recently upgraded and no further work is planned on this.</p> <p>The existing signalling equipment is life-expired and must be replaced. It will not be possible to revert to the previous way of working once the change is implemented; however, there is no option but to replace it. Maintenance practices will be much simplified and reduced, particularly through the use of LED signalling equipment.</p> <p><b>Supporting references:</b> For example, business case, Project remit.</p>
<b>Current System Overview</b>	
	<p>Rural station at the end of a branch line. Has four platforms, although only two regularly used; infrequent service (one to two trains an hour); low-speed services (75 mph maximum).</p> <p>Little or no freight service; two Automatic Open Crossing Locally-monitored (AOCL) level crossings in the area; diesel trains with no electrification in the area.</p> <p>Electromagnetic environment is benign.</p> <p><b>Supporting references:</b> Project remit and specification</p>
<b>Preliminary Risk Analysis</b>	
	<p><b>Relevant hazardous events from SRM</b></p> <p><i>HET01 Collision between two passenger trains:</i> No opportunity for collision when running to timetable because of infrequency of service. SSI functionality not complex. Standard testing and commissioning approaches to be followed. Signal sighting committees to be held.</p> <p><i>HET02: Collision between a passenger train and non-passenger train:</i> Little or no freight services.</p> <p><i>HET10: Passenger train collision with road vehicle on level crossing:</i> There are level crossings, however signalling function is not complex and standard testing and commissioning processes are to be followed.</p> <p><i>HET12/13 derailment of passenger train/freight train:</i> Little curvature – track recently upgraded, and services low speed. Signalling function is not complex.</p> <p><b>Supporting references:</b> SRM risk profile bulletin.</p>
<b>Use of novel equipment or processes</b>	
	<p>Use of solid state interlocking will be new to this location but system has been in use for decades, is mature and very well understood. LED signal heads also well understood, although new to this location.</p> <p><b>Supporting references:</b> -</p>
<b>Monitoring changed arrangements</b>	
	<p>Processes exist within the Railway Undertaking's Safety Management System for reporting back any issues with the signalling system post-implementation. Standard maintenance processes for equipment to be followed.</p> <p><b>Supporting references:</b> Railway Undertaking SMS. IM Maintenance processes.</p>

## Guidance on System Definition

### Appendix B Template for Documenting the Significance Test

<b>Proposed change</b>	Describe the proposed change, for example by referring to Preliminary System Definition (see example in Appendix A)
<b>Significant test questions</b>	<b>Responses</b>
What is the failure consequence associated with the proposed change?	
What is the novelty associated with the proposed change?	
Describe the complexity of the change. How complex is it?	
How possible is it to monitor the change and intervene, if necessary?	
How reversible is the change?	
Additionality: How significant is the change, when also considering other recent non-significant changes?	
Is the change significant (in accordance with the CSM RA): <b>Yes /No</b>	
<b>Rationale for decision:</b>	

## Guidance on System Definition

### Appendix C Example System Definition

<b>System Definition: Generic Overview</b>	
<b>Target System Objective</b>	Changed dispatch arrangements on route XXX to Driver Only Operation (passenger) DOO(P) to facilitate more commercially viable train operations.
<b>Overview of project</b>	<p>Project for a railway undertaking to change the method of working trains on a particular route from driver / guard operation to DOO(P). It is to incorporate:</p> <ul style="list-style-type: none"> <li>- Modification to the rolling stock cab layout.</li> <li>- Changes to procedures for operating trains given that no guard will be present on the train.</li> </ul>
	<b>Supporting References:</b> For example, business case, project remit.
<b>System Function and elements</b>	
<b>Route and Operations</b>	<p>Variable train formations; Route: peak services full and crowded, otherwise moderately busy commuter routes; Some staffed stations, others unstaffed; Moderate passenger numbers; Driver only dispatch procedures.</p>
	<b>Supporting references:</b> Proposed procedures for train dispatch; Proposed procedures for degraded working of trains; Proposed procedures for managing emergency situations; Procedures for support to passengers on trains.
<b>Rolling stock</b>	<p>Train class XXX doors positioned at 1/3 and 2/3 of each carriage and train class YYY doors positioned at end of each carriage; Left-hand-side cab; Door-traction interlock function; Hustle alarm; Door edge detection; Pass-com with emergency brake; Driver can make announcements.</p>
	<b>Supporting references:</b> Technical specification of rolling stock; maintenance procedures for rolling stock.
<b>Stations and infrastructure</b>	<p>Straight platforms; No island platforms; Near and offside platforms; Mostly double-track railway; no level crossings; Signals at all stations; Right Away (RA) at all platforms; No cameras or platform mirrors.</p>
	<b>Supporting references:</b> Station layout plans and information; Scheme plans; procedures for working with infrastructure manager to ensure correct placement and functional performance on Infrastructure manager assets.
<b>System Boundary including other interacting systems/interfaces</b>	
	<p>No technical interfaces currently planned to be changed; Driver interface with lineside signalling; Interface with infrastructure manager to maintain assets in correct condition/position; Interface with emergency services to ensure processes for dealing with emergency situations fit for purpose; Interface with signaller in arrangements for dispatching trains, and other operational issues.</p>
	<b>Supporting references:</b> Proposed arrangements for infrastructure manager management of assets.
<b>Assumptions and other contextual information, including environment</b>	
	<p>Line runs east to west, previous winters with large snow fall, and occasional regular sporting events at some stations cause extreme overcrowding.</p>
	<b>Supporting references:</b> Station plans.
<b>Safety measures and requirements</b>	
<b>Initial</b>	<p>Door-traction interlock function; hustle alarm; door edge detection; pass-com with emergency brake; Driver can make announcements to passengers; Lighting compliant with GI/RT7016; Drivers' training and monitoring processes</p>
	<b>Supporting references:</b> Relevant requirements from TSIs, Railway Group Standards (including the Rule Book), Sectional Appendix, rolling stock technical specifications, TOC operational procedures (including degraded mode; safety management system arrangements; planned operational arrangements for dealing with overcrowding).
<b>Developed</b>	<i>To be determined though application of the risk management process.</i>

# Guidance on System Definition

---

## Definitions

### **Actor**

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

### **Assessment body**

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

### **Assessment report**

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

### **Bow-tie models**

The 'bow tie' approach identifies the direct relationship between objectives, outcomes, hazards, causes and consequences. Controls are used to display what measures are in place to prevent the causes and mitigate the consequences.

### **CSM RA 'the regulation'**

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

### **Hazard**

A system condition that could lead to an accident.

### **Hazard record**

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

### **Infrastructure manager (IM)**

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

*(a) in relation to infrastructure other than a station, is responsible for developing and maintaining that infrastructure or, in relation to a station, the person who is responsible for managing and operating that station, except that it shall not include any person solely on the basis that he carries out the construction of that infrastructure or station or its maintenance, repair or alteration; and*

*b) manages and uses that infrastructure or station, or permits it to be used, for the operation of a vehicle.'* (Part 1, clause 2)

### **Proposer**

As defined in the regulation:

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

### **Railway system**

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

## Guidance on System Definition

---

### **Railway undertaking (RU)**

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

### **Risk analysis**

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

### **Risk assessment**

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

### **Risk evaluation**

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

### **Safety measure**

As defined in the regulation:

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

### **Safety requirement**

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

As defined in the regulation:

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

### **System**

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

# Guidance on System Definition

---

## References

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

RGSC 01	Railway Group Standards Code
RGSC 02	Standards Manual

## Documents referenced in the text

### RSSB documents

GE/GN8640	Guidance on Planning an Application of the CSM on Risk Evaluation and Assessment
-----------	--

GE/GN8642	Guidance on Hazard Identification and Classification
-----------	--

GE/GN8643	Guidance on Risk Evaluation and Risk Acceptance
-----------	---

GE/GN8644	Guidance on Safety Requirements and Hazard Management
-----------	---

GE/GN8645	Guidance on Independent Assessment
-----------	------------------------------------

Measuring Safety Performance	RSSB guide on how to develop and manage safety performance indicators for Britain's railways
------------------------------	--

Safety Risk Model	RSSB Safety Risk Model Risk Profile Bulletin
-------------------	--

### Other references

BS EN 50126-1:1999	Railway applications — The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
--------------------	--

EC No 352/2009	Commission Regulation on a Common Safety Method on risk evaluation and assessment
----------------	---

EU No 402/2013	Commission Implementing Regulation on a Common Safety Method on risk evaluation and assessment
----------------	--

ORR Guidance (Dec 2012)	ORR guidance on the application of the common safety method (CSM) on risk assessment and evaluation (December 2012)
-------------------------	---

R Short (2007)	Combining Different Types of Evidence in Safety Assurance, Asia Pacific Transportation Safety and Security Conference, Beijing
----------------	--

## Other relevant documents

### Other references

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