Rail Industry Standard
RIS-0745-CCS
Issue: One **Draft:** 1h
Date: May 2022

Client safety assurance of high integrity software-based systems for railway applications

Synopsis

This document sets out requirements for safety assurance of high integrity software-based systems for railway applications.

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.

RSSB members are granted copyright licence in accordance with the Constitution Agreement relating to Rail Safety and Standards Board Limited.

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 documents may be reproduced.

Published by RSSB

© Copyright 2022
Rail Safety and Standards Board Limited

Issue record

Issue	Date	Comments
One	03/09/2022 [proposed]	Original document.

Superseded documents

The following Railway Group documents are superseded, either in whole or in part as indicated:

Superseded documents	Sections superseded	Date when sections are superseded
GEGN8650 issue one, Guidance on high-integrity software-based systems for railway applications	All	September 2022 [proposed]

Supply

The authoritative version of this document is available at www.rssb.co.uk/standards-catalogue. Enquiries on this document can be submitted through the RSSB Customer Self-Service Portal https://customer-portal.rssb.co.uk/

Contents

List of Figures

List of Tables

Part 1 Purpose and Introduction

1.1 Purpose and introduction

1.1.1 This document sets out requirements and guidance for the role of the client in managing safety assurance of high integrity software-based systems used in railway applications. It identifies the activities undertaken as part of the safety management of the development, installation, and maintenance of high integrity software-based systems. The document is intended for use by a client when procuring and utilising high integrity software-based systems.

1.1.2 The term client refers to the group of people within the client's organisation who are collectively responsible for the procurement and the use of a safety-related software-based system. The requirements in this standard could be discharged by anyone from within such a group. The client organisation might change over the course of the system lifecycle. Within the client organisation, a project could be established to manage the safety assurance of the high integrity software-based system, and would typically include a project manager, project engineer and project sponsor.

1.1.3 The Health and Safety at Work, etc. Act (HASAW) places legal responsibilities on organisations regarding the management of safety. The Management of Health and Safety at Work regulations reinforce HASAW, placing duties on employers and employees to manage health and safety.

1.1.4 The Railways and Other Guided Transport Systems (Safety) Regulations (ROGS) require transport operators to maintain a safety management system. This standard can be adopted by a client organisation under their safety management system (SMS), to assist the management of risks relating to high integrity software-based systems.

1.1.5 Common Safety Method for Risk Evaluation and Assessment (CSM RA) provides a standard approach for proposers of a technical, operational or organisational change that affects safety to evaluate and assess risk. If a change is significant, the proposer is responsible and accountable for applying the CSM RA process.

1.1.6 In many circumstances, the proposer will be a railway undertaking (RU) or infrastructure manager (IM). Other types of proposers include an entity in charge of maintenance (ECM) who is responsible for the maintenance and modification of rail vehicles.

1.1.7 When a high integrity software-based system is procured, the client organisation could be the RU or IM who would be the proposer of the change for CSM RA purposes.

1.1.8 This standard is structured as follows:

a) Part 1 sets out the purpose and scope;
b) Part 2 provides an introduction of how the increasing use of software-based systems provides opportunities and challenges, as well as an agreed approach to control the risk from software failures. It describes how this standard relates to existing standards and legislation, especially the close relationship with a suite of railway software standards (BS EN 50657:2017, BS EN 50128:2011,

BS EN 50126-1:2017, and BS EN 50126-2:2017). The standard is structured to align with the 12-phase lifecycle set out in BS EN 50126-1:2017 which is illustrated in Figure 1. Figure 2 depicts a summary of how the requirements in this standard link into an overall process for assuring the safety of a high integrity software-based system;

c) Part 3 sets out generic requirements and guidance that apply throughout the system lifecycle;
d) Part 4 sets out requirements and guidance for client activities within the specific lifecycle phases identified in Figure 1 of this document;
e) Appendix A contains checklists that supports some of the requirements in Part 3 and Part 4;
f) Appendix B contains a set of case-studies illustrating the potential causes and consequences of software failures; and
g) Appendix C provides guidance on the specification of high integrity software requirements.

1.2 Scope

1.2.1 RIS-0745-CCS issue one covers high integrity software-based systems, specifically those systems that deliver functions assessed to have a safety integrity level (SIL) greater than basic integrity (BI), or performance level (PL) at b, c, d and e as set out in the BS EN ISO 13849 series, and where the functionality of the system is primarily delivered through the execution of software.

1.2.2 RIS-0745-CCS issue one applies to all systems used in railway applications, primarily infrastructure, trains, and their operation to deliver a service.

1.2.3 The requirements set out in this standard apply to:

a) the development of a generic product or system where the development is commissioned by a client, excluding systems for which there is no client distinct from the supplier (for example, generic products being developed by a supplier for the market).
b) the application of a generic product or system to a new specific circumstance beyond its existing approval.
c) changes made to an existing system procured and accepted against the requirements in this standard.

1.2.4 A high integrity software-based system includes the software that implements the system behaviour, configuration data that defines the behaviour in a specific application, and the processes used to generate the configuration data. It is important that the safeguards to assure that the software is correct are extended to cover the configuration data as well.

1.3 Application of this document

1.3.1 Compliance requirements and dates have not been specified because these are the subject of internal procedures or contract conditions.

1.3.2 If you plan to do something that does not comply with a requirement in this RIS, you can ask a Standards Committee to comment on your proposed alternative. If you

want a Standards Committee to do this, please submit your deviation application form to RSSB. You can find advice and guidance on using alternative requirements on RSSB's website www.rssb.co.uk.

1.4 Health and safety responsibilities

1.4.1 Users of documents published by RSSB are reminded of the need to consider their own responsibilities to ensure health and safety at work and their own duties under health and safety legislation. RSSB does not warrant that compliance with all or any documents published by RSSB is sufficient in itself to ensure safe systems of work or operation or to satisfy such responsibilities or duties.

1.5 Structure of this document

1.5.1 This document sets out a series of requirements that are sequentially numbered. This document also sets out the rationale for the requirement, explaining why the requirement is needed and its purpose and, where relevant, guidance to support the requirement. The rationale and the guidance are prefixed by the letter 'G'.

1.5.2 Some subjects do not have specific requirements but the subject is addressed through guidance only and, where this is the case, it is distinguished under a heading of 'Guidance' and is prefixed by the letter 'G'.

1.6 Approval and authorisation of this document

1.6.1 The content of this document will be approved by Control Command and Signalling Standards Committee on [31 May 2022] [proposed].

1.6.2 This document will be authorised by RSSB on [29 July 2022] [proposed].

Part 2 Overview

2.1 Software-based railway systems

Guidance

G 2.1.1 Software provides opportunities to transform the railway by delivering functionality that would have been unthinkable with mechanical and simple electrical systems. This greater use of software-based systems allows for the processing, storage and retrieval of large volumes of data at speed and in different forms. It reduces the need for bespoke hardware solutions, and enables the adaptation of system behaviour during development or after deployment. As these opportunities are taken, the amount of software in the operational railway grows. Alongside this growth, however, come challenges such as increased complexity and hazards arising from interconnected systems, and cyber-security risk.

G 2.1.2 Many of these new software-based railway systems have failure modes that could contribute to hazards, or impact on service provision. There are multiple causes for these failure modes, including defects ('bugs') in the software, errors in configuration or input data, and incorrect use arising from poor interface design. Controlling the safety risk associated with software defects involves an extension to the approaches used to control the safety risk associated with older technologies because the way in which software fails is different.

G 2.1.3 Older technologies tend to fail as result of wear and tear but software does not wear out. The defects in software are the result of mistakes made by the people who specified, designed, coded and tested the software, and the failure modes that they produce are repeatable. The software will fail again in the same way if the circumstances under which the software first failed are reproduced. The internal operation of software-based systems is not immediately visible, and defects could remain undiscovered for extended periods of time while the system appears to operate correctly until the right combination of events trigger the fault.

G 2.1.4 A number of case study examples illustrating the potential causes and consequences of software failure are given in Appendix *B*.

G 2.1.5 It is generally not possible to confirm the behaviour of software-based systems by testing all possible combinations of input. The risk of hazardous software failures is therefore controlled using proven and rigorous techniques for specifying, designing, coding, analysing and testing the software. The purpose of such an approach is to introduce fewer defects and find more of those that are introduced, so that they can be removed. However, applying the full range of these techniques tends to use more resources, and might not always be efficient for systems that are less critical to safety.

G 2.1.6 The extent to which functions of a system relate to safety is often expressed in terms of the SIL as set out in BS EN 61508 and associated standards, or PL as set out in the BS EN ISO 13849 series. Further details on how SILs are determined and used are provided in the suite of railway software standards (BS EN 50657:2017, BS EN 50128:2011, BS EN 50126-1:2017, and BS EN 50126-2:2017). For each SIL, the suite of railway software standards provides guidance on the techniques to be used for controlling the risk in the design of safety-related software-based systems. Further

information about Performance Levels (including the relationship between PL and SIL) is set out in the BS EN ISO 13849 series.

G 2.1.7 Software-based systems operate on hardware and the risk of hazardous failures arising from that hardware remain. As such, safeguards to control the risk of hardware systems failing are also applied.

G 2.1.8 Software-based systems are often highly configurable and include a significant amount of configuration data that defines the environment in which the system will run and its desired behaviour. These data have many of the characteristics of software:

a) defects in data are the result of mistakes made by people when specifying, coding and testing the data;
b) defects in data will produce repeatable failures, some of these failures could be hazardous; and
c) mitigation of the safety risk associated with these defects includes taking more care when specifying, coding and testing the data.

G 2.1.9 A system, whether it contains software or not, does not have to fail in order to exhibit a hazard. If there is a flaw in its specification leading to circumstances where what is specified is not safe, then a hazard can arise while the system appears to behave correctly. It is also important to consider how the system needs to behave in the domain of application because with a system that contains software, much of its behaviour will be embodied in the software. Fundamental to this, is ensuring the system specification is correct and complete.

G 2.1.10 It is not sufficient for an organisation which is procuring a safety-related software-based system simply to require the supplier to follow the suite of railway software standards because there are activities in the process that the procuring organisation has to carry out in order to exercise appropriate due diligence as part of safety management. This RIS describes those activities and provides guidance on how to approach them.

G 2.1.11 The suite of railway software standards places a reduced set of requirements on the design and development of systems that have a basic integrity. However, many of the activities set out in this standard could be beneficial even at basic integrity because they represent general good practice (for example supplier selection in *3.2.2*, and change control in *3.5* of this document), or might reduce development costs and timescales by ensuring that the system is well understood early in the lifecycle (for example lifecycle concepts in *4.2.2* and usage scenarios in *4.4.1* of this document).

2.2 Relationship with existing standards and legislation

Guidance

G 2.2.1 There are two alternative European standards which define a process for producing safety-related software for railway applications and which define the techniques that can be used for a defined SIL:

a) BS EN 50657:2017, Railways Applications - Rolling stock applications - Software on Board Rolling Stock

b) BS EN 50128:2011, Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems.

G 2.2.2 The two standards contain very similar requirements but are applicable to different sorts of systems. A new standard is under development, prEN50716:2021, which is intended to supersede both BS EN 50128:2011 and BS EN 50657:2017.

G 2.2.3 There is a two-part European standard which defines a process for engineering the system that will contain the safety-related software and includes processes for defining SILs:

a) BS EN 50126-1:2017, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), Part 1: Generic RAMS Process
b) BS EN 50126-2:2017, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), Part 2: Systems Approach to Safety.

G 2.2.4 For brevity the standards BS EN 50657:2017, BS EN 50128:2011, BS EN 50126-1:2017, and BS EN 50126-2:2017 are referred to as the suite of railway software standards in this document. They have been specifically identified here due to their close alignment to the scope of this standard. The requirements in this standard support compliance with the suite of railway software standards but do not replace or overrule any part of them.

G 2.2.5 The Supply of Machinery (Safety) Regulations 2008 as amended by the 'Product Safety and Metrology etc. (Amendment etc.) (EU Exit) Regulations 2019' applies to the safety-related software within control systems used by on-track machines and on-track plant. Requirements for control systems on these machines are set out in RIS-1530-PLT and RIS-1720-PLT.

G 2.2.6 BS EN 61508 set out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic elements that are used to perform safety functions. BS EN50126 forms part of the railway sector specific application of BS EN 61508.

G 2.2.7 The focus of this standard is on ensuring that the software within high integrity software-based railway systems does not cause hazards. This software will run on programmable electronic hardware and it is equally important to ensure the hardware does not cause hazards.

G 2.2.8 If the design artefacts and process outputs that are set out by the suite of railway software standards exist, this standard places no new requirements for the creation of those artefacts (for example a validation plan).

G 2.2.9 In general, the overlap between the requirements in this standard and those in the suite of railway software standards exists in order to:

a) clarify the responsibility of the client organisation in meeting the requirements of the suite of railway software standards; and
b) provide the client organisation with increased confidence that the requirements of the suite of railway software standards have been met by requiring further specific activities.

G 2.2.10 Other domain-specific standards could apply for a specific project such as:

a) BS EN 50155:2021, Railway applications - rolling stock - electronic equipment
b) BS EN 50129:2018, Railway applications - communication, signalling and processing systems - safety related electronic systems for signalling
c) BS EN 50159:2010, Railway applications, communication, signalling and processing systems - safety-related communication in transmission systems.

G 2.2.11 Additionally, obligations under general legislation and standards would apply. Relevant legislation would include Health and Safety at Work Act, etc. Act 1974, the Management of Health and Safety at Work Regulations 1999, the Railways (Interoperability) Regulations 2011, the Railways and Other Guided Transport Systems (Safety) Regulations, and Regulation (EU) 2015/1136 on the Common Safety Method for Risk Evaluation and Assessment (CSM RA).

G 2.2.12 The CSM RA regulation sets out a harmonised risk management process used to assess the impact on safety from technical, operational and organisational changes to the railway system. Guidance on CSM RA is set out in GEGN8646. If the technical changes related to introducing the software or system are significant, as defined in article 4 of the CSM RA, then an independent assessment of the risk assessment is undertaken for CSM RA as set out in *3.6* of this document.

G 2.2.13 Some of the requirements of this standard overlap with the requirements of legislation and of other standards, particularly the CSM RA. If the CSM RA applies to a project then it is efficient to align the safety assurance activities set out in the safety assurance strategy with those for the CSM RA.

2.3 Applying and adapting this standard

Guidance

G 2.3.1 Projects for the development, installation, testing and commissioning, maintenance, upgrade, renewal and the subsequent operation of high integrity software-based systems could be established by many different organisations, for many different purposes, and under many different management arrangements.

G 2.3.2 The client organisation could change over the course of the system lifecycle. This change could be as a result of a transfer of responsibility to a different group of people within the same organisation, or to a different organisation. The transition from system design lifecycle stages to system operational use is a typical point where such a change of client organisation might take place. The relationship between this RIS and the system lifecycle is described further in *2.4* of this document.

G 2.3.3 For infrastructure projects managed by an infrastructure manager (IM), the initial system design could be procured by a centralised project team before the accepted system is transferred to multiple regional teams for roll-out, operation, and maintenance. For the purposes of this standard the client organisation changes in the same way; from procurement team initially to the regional team for later lifecycle stages.

G 2.3.4 The anticipated changes to the organisations, and their roles and responsibilities, through the lifecycle of the system, and a description of how safety assurance

responsibilities are handed over when these changes occur are set out in the safety assurance strategy described in *3.1.1* of this document. The safety assurance strategy includes a description of the organisations involved in the system lifecycle (including the client organisation) and the division of responsibilities between those organisations.

G 2.3.5 To accommodate the different management arrangements, the requirements in this RIS are written using two different phrasings:

a) 'The client shall [take some defined action]'. The action defined in such a requirement cannot be delegated; the client organisation carries it out. The requirements of this form of wording cover areas that could not reasonably be wholly delegated. These are: defining the safety assurance strategy; selecting suppliers; placing contract terms on suppliers; assessing client competence; delegating change control responsibility; reviewing the outcome of system validation; and assessing compliance gaps for system acceptance; and
b) 'The client shall require that [some defined action is taken]'. In this case, it is possible for the client organisation to delegate the defined action to another organisation provided that it retains accountability for the performance of this action.

G 2.3.6 The client's role in safety assurance is defined at the level of the whole system under consideration. Where the system contains subsystems the safety assurance strategy defines how the assurance responsibilities are allocated. This allocation generally falls into one of three delivery models:

a) Prime contractor: the client has appointed a prime contractor to undertake the development and delivery of the full system. The client documents the approach to safety assurance of the prime contractor's activities in the safety assurance strategy. Delivery of the assurance for subsystem design and development is defined in the safety assurance strategy and is usually the responsibility of the prime contractor.
b) Separate contracts for subsystem supply and integration: the client appoints the subsystem suppliers and an integrator. The client sets the scope of each supplier and documents the approach to safety assurance in the safety assurance strategy.
c) Client system integrator: the client takes on some of the system development activities. The safety assurance strategy will set out the responsibilities of the suppliers and client as well as describe how the client will carry out development activities. This standard only defines the activities for the client's safety assurance role; it is expected that in the client system integrator scenario, the client will commit to carrying out development activities in compliance with the suite of railway software standards in the same way as would be required by contract terms on an external supplier as set out in *3.3.1* of this document.

2.4 Relationship with system lifecycle

Guidance

G 2.4.1 The process for assuring the safety of a system which is defined in the suite of railway software standards is structured around a system lifecycle with 12 phases, shown in Figure *1*.

G 2.4.2 General requirements, which are not specific to any phase are provided in *Part 3*.

G 2.4.3 This system lifecycle is used to structure the requirements in this standard. Requirements for the client action during the specific phases shown in green in the figure are set out in Part 4 of this document. In some cases requirements for client action during early lifecycle phases demand consideration of the approach to later lifecycle phases (e.g. the development of lifecycle concepts in Phase 2 demands consideration of the approach to lifecycle phases 8, 9, 11 and 12).

G 2.4.4 This standard contains no specific requirements for the client action during Phase 1 because it is an exploratory phase, and all relevant requirements are better associated with Phase 2. It might, nonetheless, save time if those responsible for Phase 1 bear in mind the requirements that will have to be met in the following phase.

G 2.4.5 This standard contains no specific requirements for the client to act during phases 6, 7, and 8 (software design integration) because client involvement in these phases is set out as a general requirement in *3.4* of this document to approve phased deliverables.

G 2.4.6 This standard contains no specific requirements for the client to act during Phase 12 because the activities during that phase are considered to be out of scope. However, it is necessary to consider how the decommissioning phase impacts the system design, and this is covered by the production of lifecycle concepts during Phase 2.

G 2.4.7 For complex systems where the system architecture decomposes functions across multiple subsystems, it is possible for these different subsystems to be at different phases of the lifecycle. The requirement set out in *3.1.1* of this document states that the lifecycle relationships are documented within the safety assurance strategy. A specific requirement relating to the re-use of pre-existing subsystems or software elements is set out in *4.5.2* of this document. This is a particular example of differences in the lifecycle phase.

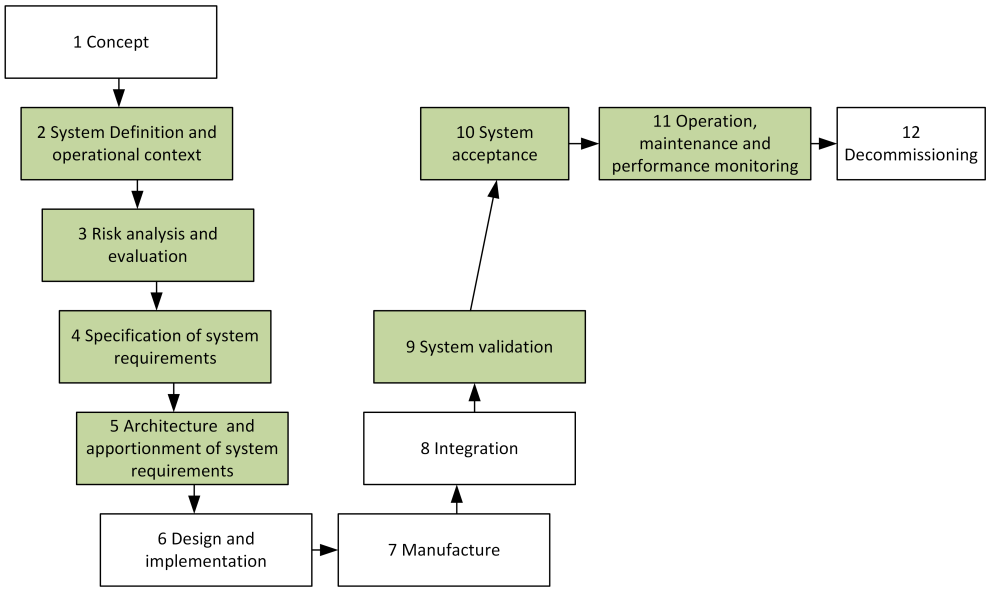

Figure 1: BS EN 50126-1:2017 system lifecycle phases

2.5 Relationship with other disciplines

Guidance

G 2.5.1 Some of the possible causes of system hazards are controlled by other specialist disciplines in their own right, as indicated in Table 1 below.

Generic hazard cause	Controlling discipline
Electromagnetic interference	Electromagnetic compatibility
Confusion, misunderstanding or delayed action on the part of users related to the design of interfaces between the system and its users	Ergonomics or human factors
Unauthorised access	Security (for software-based systems, particularly cyber-security) Note: one area of cyber-security is the prevention of unauthorised people accessing confidential data on it or causing it to stop working or causing it to do something unwanted.

Generic hazard cause	Controlling discipline
Hardware failure	Reliability, Availability and Maintainability (RAM) Note that programmable hardware (such as field programmable gate arrays and application specific integrated circuits) share many of the properties of software-based systems and need similar assurance processes.
Telecommunications failure	Telecommunications

Table 1: Generic hazard causes and their controlling disciplines

G 2.5.2 Typically, the disciplines named above are concerned with delivering operational usability and performance as well as safety, but the assurance of safety does depend upon the work done by these disciplines. Each of these disciplines has its own standards setting out methods and approaches.

G 2.5.3 This standard does not attempt to define specific requirements or guidance relating to these specialist discipline areas, but does address identification of controlling standards in *3.1.1* of this document. The compliance with those standards is included in contract terms as set out in *3.3.1* of this document and assured by audit, the requirements of which are set out in *3.6* of this document.

2.6 Summary of software assurance process

Guidance

G 2.6.1 Figure *2* provides a summary depiction of how the actions required by this standard link together into an overall process for assuring the safety of a high integrity software-based system. It is approximate because it does not show the iteration that is necessary in any real project.

G 2.6.2 Within the diagram, the rectangles depict activities that are addressed by this standard. Each rectangle includes the relevant number of the section within this standard. Shaded rectangles show those activities that are carried out by the client and clear rectangles show those where the client can delegate responsibility.

G 2.6.3 Lifecycle phases proceed sequentially; general activities take place throughout the lifecycle. All activities within a phase, and all general activities, are carried out in parallel unless specific dependencies are shown by arrows.

G 2.6.4 The process depicted in Figure *2* is designed to, if followed, assure the client and, if applicable, its regulators that safety risk associated with the system has been effectively controlled. That assurance is based upon evidence provided by the client, the supplier and possibly by other organisations, such as those providing independent assurance of safety or compliance with standards.

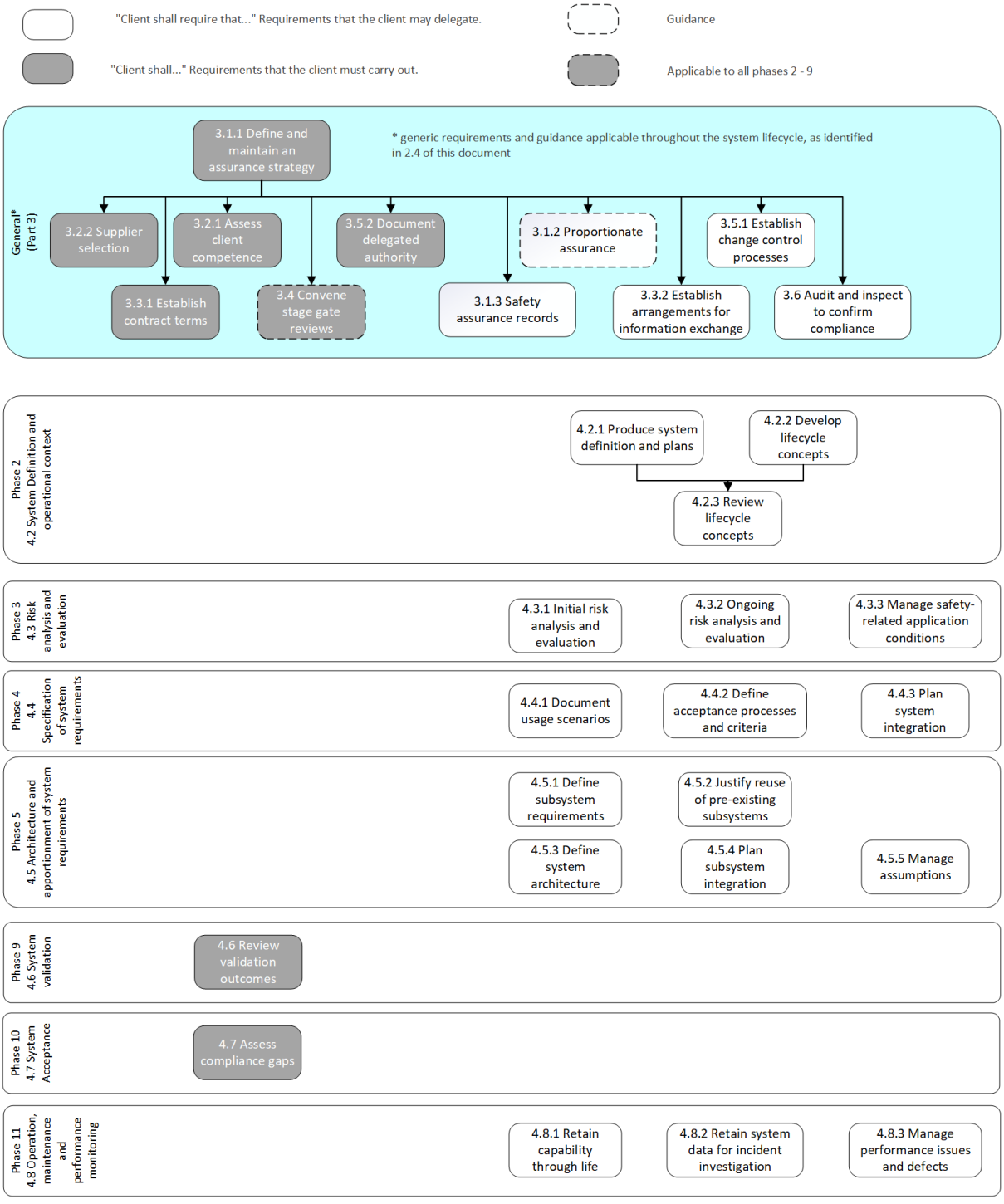

Figure 2: Summary of software assurance process in this standard

Part 3 General requirements

3.1 Approach to safety assurance

3.1.1 Safety assurance strategy

3.1.1.1 The client shall set out at the start of the project, and maintain through the lifecycle of the system, a safety assurance strategy that defines and justifies how the requirements of this standard are being applied on the project including:

a) a description of the system in terms of its functions, users, and interfaced external systems;
b) a definition of targets and top-level requirements for safety;
c) all organisations involved in the system development and safety assurance (including any acceptance panels and independent assessors), their roles, scope of supply, safety assurance responsibilities, and interdependencies;
d) anticipated changes to these organisations, roles and responsibilities through the lifecycle of the system and a description of how safety assurance responsibilities will be handed over;
e) other related railway change programmes that impact on the system under consideration;
f) the lifecycle stage for each of the major subsystems and the relationship between safety assurance activities at different levels of the system;
g) stating how requirements of the safety assurance strategy are applied. Where the delivery of safety assurance activities are delegated, they are explicitly justified and recorded;
h) the activities that have been and will be undertaken in order to comply with the requirements of this standard, and who is responsible for carrying out those activities;
i) the documents and other artefacts that have been and will be produced in order to comply with the requirements of this standard, and who is responsible for producing the artefact; and
j) the processes and standards (including specialist discipline areas and generic hazard causes identified in *2.5* of this document) that contribute to the safety of the system.

Rationale

G 3.1.1.2 Projects involving high integrity software-based systems could be established by many different organisations, for many different purposes, and under many different management arrangements. The safety assurance strategy is used to confirm that this context is considered when choosing how to apply the requirements of this standard. It is also used to demonstrate compliance, and to communicate the chosen approach to safety assurance to those who are involved in implementing it.

G 3.1.1.3 The safety assurance strategy is maintained throughout the life of the system. It contains information about what was done as well as what is planned to be done, and will evolve over time into a historical report. At any stage it can be used to demonstrate compliance with the requirements of this standard.

Guidance

G 3.1.1.4 A target or top-level requirement for safety can be defined in various ways:

a) a maximum tolerable rate for hazard occurrence;
b) the reduction of risk to as low as reasonably practicable;
c) the provision of certain functionality;
d) prevention of a hazard caused by a single failure; or
e) a new system is at least as safe as an existing system.

G 3.1.1.5 Regardless of the identified safety target, the concept of managing risk as low as reasonably practicable always applies to comply with the law.

G 3.1.1.6 The safety assurance strategy does not have to be a separate document; it could be embedded within a document with broader scope, such as a more general assurance strategy.

G 3.1.1.7 In the early stages of the project, it might not be possible to provide some of the content because information is not yet available or decisions have not yet been taken. In that case, the safety assurance strategy might describe the activities which will lead to obtaining the information or taking the decision, with the outcome being incorporated at a later point as the strategy is maintained through the life of the system.

G 3.1.1.8 Information about the factors that might contribute to safety risk is set out in *3.1.2* of this document.

G 3.1.1.9 The organisations involved include suppliers, Independent Safety Assessors (ISAs), other independent assessors, and third-party consultants or subject matter experts.

G 3.1.1.10 Changes to the organisations involved, or the roles and responsibilities of those organisations, might occur as a result of the transition between lifecycle stages, for example from development to operational use. The client organisation itself might change through the lifecycle, for example from the development project client to the end asset owner. Updating the safety assurance strategy ensures that the wider impact of these changes is considered.

G 3.1.1.11 Using named roles, instead of named individuals, in the safety assurance strategy reduces the need to update the document to reflect routine changes in personnel. Any organisational changes resulting in the alteration of related roles can give rise to competency gaps. Under these circumstances, a competency assessment as set out in *3.2* of this document applies.

G 3.1.1.12 The activities documented in the safety assurance strategy include those set out in *3.6* of this document to meet the requirement for audit and assessment. These activities are essential to assure that the project is complying with the safety assurance strategy.

G 3.1.1.13 The processes and standards contributing to system safety include those that control the work of specialist disciplines (*2.5*) on which safety assurance also relies.

3.1.2 Proportionate assurance

Guidance

G 3.1.2.1 Proportionate assurance is an approach to risk management that seeks to target efforts and resources to reduce hazards where the risk is greatest and not expend unwarranted levels of effort where risks are low.

G 3.1.2.2 Proportionate assurance is a well-established principle and following it can contribute to managing the safety risk by deploying resources in a way that will efficiently yield the greatest safety benefit.

G 3.1.2.3 The determination of a SIL will partly implement this approach because higher SILs could result in more resources being committed to assurance as well as development.

G 3.1.2.4 SILs are determined for system functions and then used to determine a SIL for a system and, possibly for its subsystems which will be a mixture of hardware and software.

G 3.1.2.5 A system might have subsystems with different SILs and this is sometimes the result of deliberate design decisions taken to concentrate the key safety functions in one area. The suite of railway software standards contains further explanation of how SILs are determined and used.

G 3.1.2.6 The SIL for a system reflects factors outside the system that contribute to safety risk. There are also other factors within the system or the project that contribute to safety risk, including:

a) tight timescales
b) large and complex projects (for example, lots of suppliers)
c) large and complex systems
d) high novelty (such as new technologies, existing technology used in new ways, or technology that is new to a supplier).

G 3.1.2.7 Although these can affect the whole system, novelty and complexity affect some parts of the system more than others.

G 3.1.2.8 There are other factors that might not change the assessment of SIL for the system, but might increase the level of assurance scrutiny needed. These factors include:

a) using components which are nearing obsolescence;
b) re-use or adaptation of items from previous applications;
c) complex or numerous external interfaces;
d) complex user interfaces; and
e) constraints on the types of testing that can be carried out.

G 3.1.2.9 The factors that might increase risk are identified and taken into account when defining the safety assurance arrangements. The rigour of these arrangements might be increased by measures such as:

a) calling for additional deliverables from the supplier as input to assurance;
b) increasing the number of reviewers or depth of review for assurance products;
c) increasing the number of audits; and
d) engaging independent assurers to carry out assurance of the project.

G 3.1.2.10 The decisions taken are reflected in the safety assurance strategy as set out in *3.1* of this document.

G 3.1.2.11 The client will generally also seek assurance of aspects of the system that are not directly related to safety, such as performance and reliability, as well as safety. Many assurance products will contribute to the assurance of multiple aspects. As a result, it can be beneficial to coordinate assurance activities across different aspects of the system.

G 3.1.2.12 CSM RA defines the assessment of the complexity and novelty of certain changes to the railway, some of which will involve the procurement of high integrity software-based systems. If the CSM RA applies to a project, then it might be efficient to align the safety assurance activities set out in the safety assurance strategy with those for the CSM RA.

3.1.3 Safety assurance records

3.1.3.1 The client shall require that the following records are established at the outset of the project and maintained throughout the lifecycle of the system:

a) the identified safety functions of the system;
b) the SIL determination for each safety function;
c) the system requirements delivering each safety function;
d) the allocation of system safety requirements within the system architecture;
e) the responsibility for assurance of each safety function; and
f) the assurance evidence supporting the delivery of each safety function.

3.1.3.2 The client shall require that traceability between the records is established.

Rationale

G 3.1.3.3 Having clear and traceable records of assurance coverage allows gaps and overlaps in assurance activity to be identified more easily. Provision of traceability supports the demonstration of the delivery of safety functions.

Guidance

G 3.1.3.4 The records to meet this requirement will be built up over the course of the system lifecycle, as only preliminary details are available at the outset of the project.

3.2 Competency

3.2.1 Client competency

3.2.1.1 At the outset of the project, and at the starts of the system lifecycle phases 3, 4, 5 and 11, the client shall:

a) identify the competencies that it needs to possess to carry out its responsibilities specified in the safety assurance strategy; and
b) assess whether or not the client organisation has these competencies; and
c) plan and execute activities to close any gaps.

Rationale

G 3.2.1.2 The client can effectively apply the safety assurance strategy only if it has the necessary competencies.

Guidance

G 3.2.1.3 This requirement does not expect every member of the client organisation to have all the competencies needed to discharge all the responsibilities of the client. The competencies can be spread within the project team of the client organisation.

G 3.2.1.4 Client organisation competence would include:

a) a high-level understanding of the suite of railway software standards and of the concepts defined in them;
b) a high-level understanding of the technologies being used in the system under development; and
c) familiarity with the operational environment in which the system will run, including user roles and interfaced external systems.

G 3.2.1.5 Key competencies for roles in the system development process are defined in Annex G of BS EN 50126-2:2017, Annex B of BS EN 50128:2011 and Annex B of BS EN 50657:2017 which might be relevant if the client organisation is carrying out tasks associated with these roles.

G 3.2.1.6 Gaps could be closed by adding members to the team or providing training and/or mentoring to existing members of the team.

3.2.2 Supplier selection

3.2.2.1 As part of the procurement process the client shall:

a) identify which prospective suppliers will be engaged in safety-related activities;
b) identify the competencies that these prospective suppliers need in order to perform these activities;
c) require these prospective suppliers to provide evidence that they have these competencies; and
d) assess whether or not these prospective suppliers have these competencies.

Rationale

G 3.2.2.2 This provides the information to allow the client to confirm that all organisations involved in the system development and safety assurance are competent to carry out their responsibilities.

Guidance

G 3.2.2.3 The supplier's responsibilities are described in the safety assurance strategy (*3.1* of this document).

G 3.2.2.4 If the project includes an Independent Safety Assessors (ISA) then the suite of railway software standards places a specific responsibility on them for the evaluation of the competency of the project staff and organisation.

G 3.2.2.5 ISO 9001:2015 sets out processes for organisations to determine staff competency requirements and resolve gaps, as well as evaluating suppliers based on their ability to provide products and services. BS EN 50126-1:2017 sets out processes for the organisation and management of personnel and responsibilities that are equivalent to those in ISO 9001:2015.

G 3.2.2.6 Key competencies for roles in the system development process are defined in Annex G of BS EN 50126-2:2017, Annex B of BS EN 50128:2011 and Annex B of BS EN 50657:2017.

G 3.2.2.7 Requirements and guidance on supplier assurance that assist the control of risks associated with procurement and the supply chain are set out in RIS-2750-RST.

G 3.2.2.8 Supplier organisations managing competency throughout their involvement in the project is covered by competency management requirements of existing standards, specifically the suite of railway software standards and ISO 9001:2015. These standards are included as part of the contract terms (*3.3.1* of this document) in support of safety assurance.

G 3.2.2.9 There is a checklist in *A.2* of this document which contains points that are considered when seeking evidence of supplier competence.

3.3 Contract terms and information sharing

3.3.1 Contract terms

3.3.1.1 The client shall place contract terms on suppliers engaged in safety-related activities that oblige the suppliers to:

a) carry out the activities assigned to them and produce the artefacts assigned to them in the safety assurance strategy;
b) comply with the processes and standards identified in the safety assurance strategy;
c) comply with ISO 9001:2015;
d) comply with BS EN 50126-1:2017, BS EN 50126-2:2017, and BS EN 50128:2011 or BS EN 50657:2017;
e) engage in stage gate reviews;
f) inform the client of safety-related changes, updates, and incidents related to their scope of supply for the system's service life; and
g) cascade equivalent terms to their suppliers where appropriate.

Rationale

G 3.3.1.2 The client can effectively apply the safety assurance strategy only if it has contractual arrangements in place to do so. The contract terms placed on suppliers (and from those suppliers to the extended supply chain) supports the control of safety risk and the provision of evidence that supports the safety assurance strategy and other standards identified in the strategy.

G 3.3.1.3 Supply chain compliance with ISO 9001:2015 and the suite of railway software standards supports quality management of software and compliance to other requirements in this standard.

G 3.3.1.4 A commitment to providing information about safety-related changes to the system for the system's service life supports the client's safety assurance activities throughout its lifetime.

Guidance

G 3.3.1.5 The activities assigned to suppliers in the safety assurance strategy might include supporting the activities of external auditors, assessment bodies, and other third parties.

G 3.3.1.6 Certification is a way for an organisation to demonstrate compliance with ISO 9001:2015.

3.3.2 Information exchange

3.3.2.1 The client shall require that arrangements are put in place and communicated to project staff, to allow information needed for safety assurance to be exchanged between organisations involved in the system development and safety assurance.

Rationale

G 3.3.2.2 In order to perform safety assurance, the organisations delivering the assurance need access to information owned by those doing the development.

G 3.3.2.3 All project staff need to be aware of the arrangements for information exchange to ensure that uncertainties about what can be shared and how, do not arise and make communication ineffective.

Guidance

G 3.3.2.4 Non-disclosure agreements (NDAs) are a typical way of allowing information to be exchanged while maintaining confidentiality.

3.4 Stage gate reviews

3.4.1 At the end of each phase for the system lifecycle phases 2 through 9, the client shall convene and undertake gate reviews.

3.4.2 The client shall permit the project to proceed to the next phase only when satisfied that the risk to safety arising from deficiencies in the outputs from the current phase is controlled, and that activities are scheduled to remedy them.

Rationale

G 3.4.3 Gate reviews enable the client to exercise appropriate due diligence as part of safety management. They create a shared understanding of the status of the system design, and allow stakeholders to understand their role in the wider project.

Guidance

G 3.4.4 Whilst detailed criteria are provided within the suite of railway software standards the client is also responsible for ensuring that the review of phase outputs considers:

a) the whole system lifecycle (and particularly as set out in the lifecycle concepts and scenarios described in *4.2* and *4.4* of this document); and
b) the reasonably foreseeable range of use cases for all system users.

G 3.4.5 In addition to this general requirement for the review of phase outputs, the requirements in Part 4 of this document provide more specific obligations for client activity within individual lifecycle phases.

G 3.4.6 To assist a stage gate review to proceed in a controlled and structured manner, exit criteria (conditions for allowing the project to proceed to the next phase) could be defined and communicated to all involved. This ensures that stage gates consider both the work done by the project in the phase being completed and also the project's readiness to undertake the work in the next phase.

G 3.4.7 It could also help to avoid wasted time if entry criteria conditions for allowing the stage review to start are defined and communicated to all involved.

G 3.4.8 Depending on the development model selected for the project, different parts of the system might proceed through the lifecycle phases at different times. In these cases there are interim points where the activities of a phase are complete for some parts of the system, but not for the whole of it. This might allow some parts to proceed to the next phase before others. The requirement for gate reviews does not apply to these interim points, although it might be desirable to hold additional interim gate reviews in order to control the risk of starting work early.

3.5 Change control

3.5.1 Change control processes

3.5.1.1 The client shall require that processes are established for configuration management of the system, its applications, its components and associated documentation and data, including arrangement for controlling change.

Rationale

G 3.5.1.2 If the precise configuration of the system is not known, or if there are uncontrolled changes to it, then it is not possible to be sure that the arguments compiled for its safety are valid. Without change control, safety activities might not be carried out on a consistent version of the design, which would make it difficult to determine whether identified defects have been fixed.

Guidance

G 3.5.1.3 Configuration comprises the system, its components, its specification, and other items that are kept aligned with the system, including manuals and test material. The configuration does not encompass everything that the project produces – only the key items. Anything included within the configuration is referred to as a configuration item.

G 3.5.1.4 The configuration items typically include:

a) Requirements (at all levels of the system)
b) Outputs of design activities (for example lifecycle concepts, usage scenarios, architecture)
c) Outputs of verification and validation activities (for example plans, procedures, test results)
d) Delivered assets (for example executable software, including support tools, user manuals)
e) Configuration data.

G 3.5.1.5 Configuration management is intended to ensure that, as things change, changes are properly considered and thoroughly applied so that the configuration items remain consistent.

G 3.5.1.6 Configuration management is made up of six basic functions:

a) Configuration item identification

Ensuring that every configuration item has a unique identifier and that, if it changes, every significant version has a version identifier;

b) Configuration baselines

Establishing and documenting self-consistent sets of configuration items at key points in the project (for instance at stage gate reviews) which then form a starting point for change control;

c) Configuration status accounting

Maintaining records about the configuration items and about proposed and actual changes which are sufficient to answer questions such as:

i) What configuration items would be affected by this proposed change?
ii) What changes have been applied to this version of this configuration item and what potential changes are under consideration?
iii) What version of this configuration item has been installed at this location?

d) Configuration audits

A configuration audit is a check that:

i) all configuration items have been produced;
ii) all configuration items produced comply with specified requirements;
iii) technical documentation is complete and accurately describes the configuration items; and
iv) all approved change requests have been resolved

e) Change control

Once a configuration item has been included within a baseline, any proposed change to it is fully assessed and approved before the change is made and tracked to completion. The assessment of the change includes safety analysis of the impact of the change. Changes might be made in order to correct faults and therefore the arrangements for controlling change need to cover the diagnosis of

problems with configuration items, the corrections made to resolve these problems, and a 'regression testing' to confirm that the change has been correctly implemented, and also that other system functions remain unaffected.

f) Configuration management planning

Planning of the activities in a) to e) above.

G 3.5.1.7 In a project with a complex supply chain, linked arrangements could be set up by multiple organisations. In such circumstances, the client will normally establish configuration management arrangements for items under the clients control and ensure that other items are under adequate configuration management.

G 3.5.1.8 A generic system might have multiple applications in different parts of the railway. Different organisations could perform configuration management for the generic systems and for the specific applications. For example, the supplier could manage the generic software and would have the configuration processes in place for this (for example records to establish exactly what modules were in a specific software release and what faults were corrected in that release) while the duty holder might be responsible for keeping records of what release of software were loaded onto different applications (for example individual units installed at specific locations).

G 3.5.1.9 As a system changes, and particularly where a system is made up of multiple parts with their own lifecycles, it might be necessary to maintain records of compatibility between parts from different configuration baselines.

G 3.5.1.10 Further guidance is set out in Network Rail System Engineering handbook (NR/SE/001).

G 3.5.1.11 Good practice in configuration management is documented in an international standard, BS ISO 10007:2017.

3.5.2 Delegation

3.5.2.1 The client shall document any delegation of change control authority to suppliers, including escalation paths to be used where changes exceed the limits of this delegation.

Rationale

G 3.5.2.2 Documented delegation allows change to be managed at an appropriate level within the supply chain and all parties to be clearly informed of their responsibility, and the limits of their authority.

Guidance

G 3.5.2.3 Typically, limits of delegated authority, for which the defined escalation paths are used, include situations in which the change:

a) affects systems outside the supplier's scope (including the operational railway and users);
b) modifies aspects of supplier work that have already been subject to client approval; or

c) impacts client costs or timescales.

3.6 Audit and assessment

3.6.1 The client shall require that audits and assessments are planned and carried out in order to confirm compliance with the safety assurance strategy.

Rationale

G 3.6.2 The safety integrity of software-based systems rests, in part, on the rigour of the development processes employed in the software design. Audit and assessment are used in delivering assurance of compliance with agreed processes, and show that the system is fit for its intended purpose.

Guidance

G 3.6.3 The safety assurance strategy is described in *3.1.1* of this document.

G 3.6.4 The audits and assessments expected by the client are set out in the safety assurance strategy and focus on areas of greatest risk as described in *3.1.2* of this document.

G 3.6.5 Processes and standards that contribute to the safety of the system are identified within the safety assurance strategy set out in *3.1.1* of this document.

G 3.6.6 Some form of independent assessment might be applicable to comply with the law or policy. This is carried out by someone independent of the delivery organisation. Independence from the delivery organisation is often achieved by engaging an outside supplier to fulfil this role. The suite of railway software standards also provides guidance on how this is carried out. Under certain circumstances, there are legal requirements for procuring independent assessment, such as review by Independent Competent Persons, Assessment Bodies, Designated Bodies, Approved Bodies and ISAs. These assessments have different scopes but might overlap and could be performed by the same organisation. The relationship between assessors, their scope of work, roles and responsibilities, and interdependencies, is set out in the safety assurance strategy (*3.1.1* of this document).

G 3.6.7 The suite of railway software standards defines audit in terms of the objective use of information to determine the extent to which specified requirements are fulfilled. This is typically applied to management systems. The need for objectivity in audit contrasts with the definition of independent safety assessment that explicitly includes the need for judgement.

G 3.6.8 Both direct and indirect evidence can be used to support the audit process, for example by:

a) using review and test outcomes, and configuration management evidence to confirm that faults are being found, assessed and fixed;
b) using meeting minutes to confirm that gate reviews were conducted with sufficient time allowed for adequate deliberation; or
c) confirming that project team members understand the processes and tools used and the reason for them.

G 3.6.9 The client could also carry out audits and assessments or require suppliers to have audits and assessments carried out by their quality assurance functions, or both.

G 3.6.10 There is a checklist in *A.3* of this document which contains points that are considered when checking a programme of audit and assessment.

Part 4 Requirements for lifecycle phases

4.1 Introduction

Guidance

G 4.1.1 Requirements in this section of the standard apply within the specific system lifecycle phase indicated. The phases are based on those described in BS EN 50126-1:2017 - further information about the relationship between this standard and the system lifecycle is described in *2.4* of this document.

G 4.1.2 The specific requirements placed on the client take account of the fact that, while the supplier will generally be the expert in the system and how it works, it is the client that has (or has access to) expertise in how the system will be used and how it will fit into the rest of the railway.

G 4.1.3 Not all system lifecycle phases have specific requirements defined in this standard.

G 4.1.4 The following table provides a summary of the client's part in achieving the purpose of each section and the related clauses in BS EN 50126-1:2017:

RIS-0745-CCS			Related clauses in BS EN 50126 -1:2017
Section	**Purpose**	**Relevant client's activities**	
4.2 Phase 2 - System Definition and Operational context	System definition is developed with consideration given to the lifecycle of the system under consideration, and that it is reviewed by an appropriate set of stakeholders.	• Directly engages with all activities in the phase, because this phase could occur before a supplier is appointed to deliver the system; • Prepare and review documents relating to how the system will be used, because the client will generally have access to people who know how and the supplier will generally not have this knowledge.	7.3.3. Deliverables

RIS-0745-CCS			Related clauses in BS EN 50126 -1:2017
Section	**Purpose**	**Relevant client's activities**	
4.3 Phase 3 - Risk Analysis and Evaluation	Ongoing process of hazard identification and risk assessment is carried out considering the full scope of the system under consideration, and areas of risk for software-based systems are identified.	• Engage with hazard identification and risk assessment because it will need involvement from people with knowledge about how the system will be used and how it will fit into the rest of the railway; • Confirm that 'Safety-related Application Conditions' (SRAC) identified by the hazard identification and risk assessment processes are accepted and understood by the people who will have to respect them.	7.4.1 Objectives 7.4.3 Deliverables
4.4 Phase 4 - Specification of System Requirements	A complete set of system requirements and design constraints is identified by considering the full range of lifecycle concepts defined in Phase 2; and these are supported by a defined acceptance and integration plan.	• Compile information about how the system will be used, in the form of usage scenarios, because the supplier will not generally have access to this information; • Define acceptance criteria, because the client will accept the system later; and • Define how the system will be integrated with the rest of the railway, because the supplier will generally be unable to do this on its own.	7.5.1 Objectives

RIS-0745-CCS			Related clauses in BS EN 50126 -1:2017
Section	**Purpose**	**Relevant client's activities**	
4.5 Phase 5 - Architecture and Apportionment	The apportionment of system requirements is carried out and that: a) re-use of existing elements is justified; b) requirements are set for supporting tools; and c) assumptions that involve multiple stakeholders are managed.	• Engage with the decisions taken during this phase that could have a significant effect on safety and other outcomes of the project.	7.6.1 Objectives
4.6 Phase 9 - System Validation	The validation outcomes are reviewed.	• Review and decide whether to accept the compliance of the system based on validation evidence.	7.10.1 Objectives
4.7 Phase 10 - System Acceptance	Information regarding risks associated with all compliance gaps are used as input to the acceptance decision.	• Assess and only accept the system for entry into service if the risk associated with any non-compliance or gap in compliance evidence has been shown to be controlled.	7.11.1 Objectives
4.8 Phase 11 - Operation, Maintenance, and Performance Monitoring	Appropriate processes are established to support the system such that compliance with the safety requirements is maintained.	• Liaise with stakeholders inside and outside the client's organisation to set up the necessary arrangements that retain the system capability through life.	7.12.1 Objectives

Table 2: Client activities in specific phases and related BS EN clauses

4.2 Phase 2 - System definition and operational context

4.2.1 Definition and plan

4.2.1.1 The client shall require that the activities of phase 2 in the lifecycle defined in section 7.3 of BS EN 50126-1:2017 are carried out and the deliverables of Phase 2 are produced.

Rationale

G 4.2.1.2 This requirement supports the understanding of the system function, interfaces, and the lifecycle management of safety and RAM. This requirement covers all of the phase activities set out in section 7.3 of BS EN 50126-1:2017 because the client will generally have access to people who have the required competence and the supplier will generally not have this knowledge.

Guidance

G 4.2.1.3 The deliverables identified in section 7.3.3 of BS EN 50126-1:2017 are a system definition, a safety plan, and a RAM plan. Guidance on these deliverables and the activities needed to produce them is provided in the suite of railway software standards.

G 4.2.1.4 The activities in this system lifecycle Phase 2 could be performed by the client before a supplier for the system is contracted and there is not necessarily anyone for the client to delegate these activities to.

G 4.2.1.5 CSM RA is applicable to certain changes to the railway, and there might be overlap between material produced, for example, the production of a system definition, to meet the requirements of this standard and that needed by CSM RA.

G 4.2.1.6 Although the safety plan referred to in BS EN 50126-1:2017 and the safety assurance plan have different emphases, their scopes do overlap, one can refer to the other or the two can be combined.

4.2.2 Lifecycle concept development

4.2.2.1 The client shall require that lifecycle concepts for the system under consideration are produced which:

a) cover phases 8, 9, 11 and 12 of the system lifecycle;
b) determine implications for the user roles involved;
c) identify external interfaces to other systems; and
d) identify the functions provided to those users and systems.

Rationale

G 4.2.2.2 The lifecycle concepts can act as a basis for the definition of system requirements and operational scenarios in later phases. Without lifecycle concepts, some system functions, interfaces, and users might be missed. This could result in a system that cannot be integrated into its operational environment, or a late change in the system design.

Guidance

G 4.2.2.3 A lifecycle concept is a high-level description of how a system will be operated, maintained, installed, integrated with other systems and placed into service. The production of lifecycle concepts enables the production of a system requirements specification, but the two are distinct. While the system requirements focus on the system and define what it will do, lifecycle concepts focus on the users of the system (including people and other systems) and describe how they will use the system. Creating lifecycle concepts before finalising the system requirements makes it possible to confirm that the functionality offered by the system will let users do what they need to do with it and to do it safely.

G 4.2.2.4 Development of the lifecycle concepts is often an iterative process involving both client and supplier organisations.

G 4.2.2.5 The content of the system definition is defined in the description of lifecycle Phase 2 in BS EN 50126-1:2017. Annex D of BS EN 50126-1:2017 provides guidance on system definition.

G 4.2.2.6 The concept for operation is often abbreviated as 'ConOps'. Similar lifecycle concepts can be produced for other system lifecycle stages, for example concept for maintenance, concept for system integration, etc.

G 4.2.2.7 The phases of the system lifecycle identified in the requirement cover system integration, system validation, operation, maintenance, performance monitoring, and decommissioning. Guidance for each of these lifecycle concepts is included in Table 3.

Lifecycle stage for concept	Content of Lifecycle Concept
System integration	Describes how the system will be integrated into its intended operational environment. It describes how the system will be installed, configured, and commissioned for operational use. Depending on the nature of the configuration data for the system the processes involved in designing the configuration data for a specific application installation can be highly complex. Further information on integration planning is provided in *4.4.3* of this document.
System validation	Describes the approach to validating the system to demonstrate compliance with requirements, including the identification of tools and test environments.

Lifecycle stage for concept	Content of Lifecycle Concept
Operation	Describes what the system will do from the viewpoint of operational users. The concept for operation considers aspects relating to the transition from development to operational use, including confirming operational and maintenance readiness. This could cover: • Staging • Training of operational users and maintainers • Availability of manuals and other documentation • Changes to operational processes • Temporary arrangements for the period immediately after entry into service • Availability of tools and spares • Synchronisation with changes to other systems
Maintenance	Describes the maintenance environment for the system, and the associated activities and constraints. This includes areas such as: • The operational status of the system during maintenance activities: can the system operation continue during maintenance? • Support tooling and logistics arrangements: are maintenance terminals expected to interface to the system? How are these units made available to maintenance users? • Testing: what level of testing is expected before the maintained system can be returned to operational use? Does this testing involve specific functionality or equipment? • The policy for applying software updates (for example to operating systems).
Performance monitoring	Describes the approach to monitoring the performance of the system under consideration throughout its operational life. This includes areas such as support tooling and interfaces to external monitoring systems.
Decommissioning	Describes the approach to removing the system under consideration from operational use at the end of its life.

Table 3: Lifecycle concept guidance

G 4.2.2.8 In addition to the usual operators and maintainers, software-based systems can also have specialist user roles involved in activities such as:

- system administration - using privileged access to the system to carry out system updates;
- account management - updating user access; and
- system configuration - developing system configuration data (for example for extending system deployment or adapting to changes in operation).

4.2.3 Lifecycle concept review

4.2.3.1 The client shall require that the system definition and lifecycle concepts are reviewed by representatives of all user roles and interfaced external systems.

Rationale

G 4.2.3.2 An appropriate set of stakeholders involved in the review of the system definition and lifecycle concepts supports the completeness of the deliverables.

Guidance

G 4.2.3.3 In order to represent a user role or an interfaced external system, a representative will be knowledgeable about the role or system whether or not they are currently performing the roles or working on the system. This knowledge is covered in client competency in *3.2.1* of this document.

G 4.2.3.4 The user roles and interfaced external systems are identified in the safety assurance strategy.

4.3 Phase 3 - Risk analysis and evaluation

4.3.1 Introduction

Guidance

G 4.3.1.1 Compliance with CSM RA is required in GB for duty holders through the safety management system under ROGS. Further guidance on CSM RA is provided in GEGN8646.

G 4.3.1.2 There might be overlap between activities undertaken to meet the requirements of this standard and those needed by CSM RA. it is efficient to align the safety assurance activities set out in the safety assurance strategy with those for the CSM RA.

4.3.2 Initial risk analysis and evaluation

4.3.2.1 The client shall require that a process of identifying system hazards and assessing risk is carried out and documented, considering the full scope of system functions, interfaces, user roles, lifecycle concepts, and usage scenarios.

Rationale

G 4.3.2.2 Safety is delivered by eliminating hazards and reducing to an acceptable level the risk associated with those hazards that cannot be eliminated. Understanding what the

hazards are and what is the risk associated with the hazards is a necessary pre-requisite to delivering safety.

G 4.3.2.3 If a hazard is not identified, it is not possible to work deliberately to control it. It is therefore not sufficient just to identify the obvious hazards. It is important to consider the full scope of system functions, interfaces, user roles, lifecycle concepts, and usage scenarios to identify reasonably foreseeable hazards.

G 4.3.2.4 The process would need to start before the system is specified if safety is to be built into the system.

Guidance

G 4.3.2.5 A hazard of a system is a possible state of that system which could contribute to an accident.

G 4.3.2.6 The risk associated with a hazard is a combination of the severity of the possible consequences of that hazard and the likelihood of those consequences occurring. The risk associated with a system is the total risk associated with all its hazards.

G 4.3.2.7 If the risk associated with hazards is not identified, it is difficult to allocate effort between controlling different hazards and very difficult or impossible to know when the risk is acceptable.

G 4.3.2.8 The process of assessing the risk associated with a hazard normally involves an understanding of the possible causes of the hazard as well as its possible consequences.

G 4.3.2.9 There are various techniques for identifying hazards and analysing their causes and consequences. For simple systems this can be done effectively by informal methods informed by experience and written up in prose or in tables. Software-intensive systems are usually more complex and might merit application of more systematic techniques such as Hazard and Operability Studies (HAZOPS), Failure Mode, Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA) or Event Trees. Some of these are supported by computer tools.

G 4.3.2.10 Risk assessment can be performed using qualitative categories for the assessed frequency and consequence or by making numerical estimates of the frequency and consequence.

G 4.3.2.11 Experienced safety professionals will be able to advise on the selection of techniques.

G 4.3.2.12 For hazard identification and consequence analysis, to be confident that no hazards or consequences have been missed, the process involves participants with broad knowledge of the system and how it will be installed, operated and maintained. The client might need to arrange access to these people and that will generally entail the production of a clear programme of risk analysis and evaluation activities.

G 4.3.2.13 Software-based systems are often highly configurable and include a significant amount of configuration data that defines the environment in which the system will run and its desired behaviour. Defects in this configuration data might cause system hazards. The system configuration data, together with the tools and processes used to derive this data are included within the system definition and the system architecture and hence are within the scope of hazard identification and risk

assessment. The effort involved in undertaking this activity, and the benefit of undertaking the analysis early in the system lifecycle, is sometimes underestimated.

G 4.3.2.14 It could be the case that it is not possible to assess risk precisely, particularly when the project is doing something that has not been done before, and it is only possible to claim that it lies within a broad range. In that case, it is good practice to apply the precautionary principle, which is to proceed on the assumption that the risk is towards the higher end of the range.

G 4.3.2.15 If the system is used by people then it is possible that the way in which the human-machine interface is designed can either contribute to hazardous mistakes by the user or mitigate them. This can be taken into account when identifying hazards and deciding how to control them.

4.3.3 Ongoing risk analysis and evaluation

4.3.3.1 The client shall require that a hazard record is produced to record the results of system hazard identification and risk assessment and is kept up-to-date as relevant new information becomes available and changes occur.

Rationale

G 4.3.3.2 When the initial risk analysis and evaluation is undertaken all of the information needed to produce a definitive analysis will not yet be available. In addition, it might be invalidated by change. The ongoing process of risk analysis and evaluation is essential for the risk analysis and evaluation to be effective.

Guidance

G 4.3.3.3 A hazard record (also referred to in the suite of railway software standards as a hazard log) contains a summary of what is known about hazards, including their causes, their consequences, measures in place to control them, the risk assessed for them and actions underway to understand them or control them better.

G 4.3.3.4 The production of a hazard record is applicable for certain changes to the railway as set out in the CSM RA.

G 4.3.3.5 While the reports arising from risk analysis and evaluation activities could concern only one aspect of the system and are generally valid for a point in time, the hazard record provides a consolidated repository of information which is maintained up to date.

G 4.3.3.6 The hazard record is used to inform decisions about whether to put additional measures in place to control hazards. Additional measures can include the application conditions set out in *4.3.4* of this document or additional technical features (expressed as requirements) for the system under consideration.

G 4.3.3.7 Hazard records can be maintained using a spreadsheet tool or a general-purpose database tool although special-purpose tools exist.

G 4.3.3.8 If the hazard record is to be maintained, then the risk analysis and evaluation activities, particularly the causal analysis, are extended as design information becomes available.

G 4.3.3.9 The hazard record can also support partially repeating the risk analysis and evaluation activities to take account of:

- any changes to the system; and
- changes to the environment, the way in which the system will be installed, used or maintained, if they affect the risk analysis and evaluation activities.

To be confident that no hazards or consequences have been missed some of the continuing risk analysis and evaluation activities will involve participants with broad knowledge of the system and how it will be installed, operated and maintained. The client might need to arrange access to these people.

4.3.4 Safety-related Application Conditions

4.3.4.1 The client shall require that a register of safety-related conditions on the application of the system is prepared.

4.3.4.2 The client shall require that the conditions in the register of Safety-related Application Conditions are respected.

4.3.4.3 The client shall require that each condition of the register of Safety-related Application Conditions is:

a) traceable to the hazards that it relates to;
b) communicated to whoever is responsible for ensuring that it is respected; and
c) agreed with representatives of the relevant user roles.

4.3.4.4 The client shall require that the register of Safety-related Application Conditions is kept up to date.

Rationale

G 4.3.4.5 If the requirement is not complied with, the system might be used in a manner which undermines the work done to make it safe. Conditions being agreed to by a user representative reduces the chance of the conditions being found to be unacceptable or impracticable at a later stage of system design.

G 4.3.4.6 Conditions on the application of the system that have to be respected in order to control risk might be identified throughout the development of the system.

Guidance

G 4.3.4.7 The suite of railway software standards refers to conditions on the application of the system that have to be respected in order to control risk as Safety-related Application Conditions (SRACs).

G 4.3.4.8 If the system requirements are maintained in a database then it could make it easier to maintain the register of SRACs if kept in the same database.

G 4.3.4.9 It is important for the representative of the relevant user roles to be knowledgeable about the role. It does not matter whether they are currently performing that role or not .

G 4.3.4.10 SRACs might concern, among other things:

a) how the system is installed, operated, maintained, or configured;
b) the competences of users and maintainers;
c) the environment within which the system is installed; and
d) aspects of other systems to which it is connected.

G 4.3.4.11 SRACs could be communicated by inclusion in user documentation, training material, or operating rules.

4.4 Phase 4 - Specification of system requirements

4.4.1 Usage scenarios

4.4.1.1 The client shall require that usage scenarios for the system under consideration, covering all modes of use are documented and employed to define and check system requirements, including requirements for safety-related functions.

Rationale

G 4.4.1.2 Without understanding how the system will be used it is not generally possible to control a hazard effectively and to show that it has been controlled, or to deliver operability, maintainability, reliability, security and performance. Usage scenarios covering all modes of use supports the identification of gaps in requirements specifications.

Guidance

G 4.4.1.3 Modes of use might include installation, configuration, testing, commissioning, user training, trial operation, normal operation, maintenance, renewal, replacement, disposal, operation with failures or degraded performance, abnormal operation, misuse and incident investigation.

G 4.4.1.4 Abnormal operation in this context refers to the system's response to scenarios that are unusual but allowed by operational rules and procedures.

G 4.4.1.5 Failure or degraded performance might arise either inside or outside the boundary of the system under consideration.

G 4.4.1.6 Incident investigation covers the provision of facilities to retain system data to support the identification of root cause of adverse events.

G 4.4.1.7 Scenarios can be written up as narrative prose but there are also more precise diagrammatic notations, such as the Unified Modelling Language (UML), which could be used.

G 4.4.1.8 The suite of railway software standards states that a validation report be produced at the end of Phase 4 which includes confirmation that all system requirements are adequately analysed and specified in order to allow the system under consideration to serve the intended use. Requirements modelling can help to provide this confirmation and many approaches are available including formal modelling, prototyping, and usage scenario walkthroughs.

G 4.4.1.9 To be confident that the scenarios are accurate and comprehensive, the process of defining them involves participants with a broad knowledge of the system and how it

will be installed, operated and maintained. The client might need to arrange access to these people. It is likely that the process will involve multiple iterations, and an interactive approach (for example scenario walkthrough or using simulators).

G 4.4.1.10 The process of checking system requirements against the usage scenarios will allow the identification of those key safety functions, whose correct behaviour is relied upon to avoid hazards. The system designers can use this information to design in the necessary controls.

G 4.4.1.11 A requirement that the system complies with a standard is a system requirement. It could make later stages of the development process easier if the requirement to comply with the standard is expanded to include the relevant provisions within the standard as individual system requirements and accompanied by a rationale for why compliance with the specified standard is expected.

G 4.4.1.12 Guidance on the preparation of high integrity software specification is given in Appendix C of this document.

G 4.4.1.13 There is a checklist in *A.4* of this document which contains points that are considered as well as the lifecycle concepts when looking for missing system requirements.

4.4.2 Acceptance processes and criteria

4.4.2.1 The client shall require that criteria are set for the acceptance of each requirement.

4.4.2.2 The client shall require that plans are produced for the processes to deliver evidence that the acceptance criteria for requirements have been met.

4.4.2.3 The client shall require that processes are in place for the acceptance of all Safety-Related Application Conditions.

Rationale

G 4.4.2.4 If criteria are not set for the acceptance of a requirement, it is possible to proceed with a requirement that is not demonstrable and will be difficult to validate. If the processes for demonstrating that the acceptance criteria have been met are not planned, it is possible to miss the fact that additional functions or equipment might be needed to demonstrate these criteria, which might result in expensive rework later in the project.

G 4.4.2.5 The SRACs represent conditions about the application of the system that have to be respected in order to control risk. If processes are not in place to confirm that these conditions are acceptable then a functionally compliant system might be unusable in its operational environment.

Guidance

G 4.4.2.6 The suite of railway software standards states that acceptance criteria and processes are defined during Phase 4.

G 4.4.2.7 Acceptance of a system might be defined for commercial or performance reasons as well as for safety reasons and the plans for all of these aspects can be combined in a single acceptance plan.

G 4.4.2.8 It is usually convenient to record the acceptance criteria for a requirement together with that requirement. If the system requirements are maintained in a database, then it could be convenient to maintain the acceptance criteria in the same database.

G 4.4.2.9 Software-based systems are often highly configurable and include a significant amount of configuration data which define the environment the system is intended to operate in as well as its desired behaviour. It is rarely possible to demonstrate that a system will work for every combination of configuration data values. However, it is important that the software-based system remains safe with data values that are outside 'normal bounds' and mitigations are in place for safety risks associated with data defects.

G 4.4.2.10 The acceptance plan considers the range of configuration data and the processes used to generate the configuration data and commission systems into operational use.

G 4.4.2.11 The risk of defining unacceptable SRACs is mitigated by the requirement to agree on these with representatives of the relevant user roles as they are identified (*4.3.4* of this document).

4.4.3 System integration planning

4.4.3.1 The client shall require that plans are produced that describe how the system will be integrated within its intended operational environment including:

a) the sequence of integration steps;
b) entry criteria to be fulfilled before system integration can commence;
c) integration test activities to be undertaken during each step;
d) the integration environment at each step; and
e) how other operational systems will be protected from failure of the system under consideration during integration.

Rationale

G 4.4.3.2 If integration is not carried out in a planned and systematic way within a realistic and representative environment, hazardous faults could be missed and hazardous interactions with other systems might be caused. In addition, if integration is not carried out in a planned and systematic way, it could take longer and cost more than is necessary.

G 4.4.3.3 If integration is not planned, it is possible to miss the fact that additional functions or equipment will be needed to perform integration, which might result in expensive rework later in the project.

Guidance

G 4.4.3.4 BS EN 50126-1:2017 uses the term 'integration' to cover both:

a) the integration of subsystems and components to form the whole system in order to demonstrate that the system fulfils its requirements; and
b) the integration of the system into its operational environment.

G 4.4.3.5 Within this standard, the term 'system integration' is taken to mean integration of the system into the operational environment.

G 4.4.3.6 Integration of subsystems to form the whole system is referred to as 'subsystem integration'. Planning for that activity is set out in *4.5.4* of this document.

G 4.4.3.7 Integration considers problems at interfaces between systems. If a system has interfaces with many external systems and everything is put together at the same time, problems can be very difficult to find. It could result in an excessive risk of causing problems with the external systems. It could be safer and more efficient to start by integrating the system under development with simulators of external systems and replacing the simulators with the real systems when the simulators find no more faults. A simulator can only be considered effective and valid if it is representative of the real external system.

G 4.4.3.8 The use of simulators is part of defining the environment for each integration step, and they fall under the scope of tools to be considered for justification within the suite of railway software standards. Where an interface simulator is not produced independently of the system under consideration, there is a risk that misinterpretation of the interface definition is repeated in both the system and the simulator, which can result in a system that operates correctly when tested against the simulator, but fails to integrate into the real environment.

G 4.4.3.9 RSSB research report T1047 (2014) has provided guidance on the use of software-based systems for railway applications, which includes guidance on system integration.

4.5 Phase 5 - Architecture and apportionment

4.5.1 Subsystem, interface and software requirements

4.5.1.1 The client shall require that:

a) requirements are defined for all subsystems, interfaces and software elements within the system under consideration; and
b) it is verified that these subsystems, interfaces and software requirements, in combination with the application conditions, are sufficient to ensure that the system requirements are met.

Rationale

G 4.5.1.2 If this requirement is not complied with it might later be discovered that the subsystems, interfaces and software requirements are not sufficient to ensure that a safety-related system requirement is met. If this happens later in the project, the rework could be expensive. A hazard might be caused if this happens after the system has entered service.

Guidance

G 4.5.1.3 Some software-intensive systems might not have significant subsystems, in which case there is no apportionment of system requirements to subsystems although software requirements for such systems are produced.

G 4.5.1.4 Where an interface exists between two systems or subsystems, the requirements can only be met by both. The requirements for an interface are often contained in a document with the title Interface Control Document (ICD).

G 4.5.1.5 If a subsystem, interface or software element is to be developed, then the requirements for the element will be the starting point for the development. If a subsystem, interface or software element already exists and is to be reused then the requirements that already exist for it will constitute a description of how it functions. In both cases, new development and reuse, the requirements will be input into the verification process to show that the combination is sufficient to meet the system requirements.

G 4.5.1.6 The usage scenarios that were developed during Phase 4 can be refined to include interactions between subsystems (that is over internal interfaces) and used to support the verification. The verification that the subsystem, interface and software requirements are sufficient to ensure that the system requirements are met might be carried out by associating each system requirement with a satisfaction argument that links to supporting subsystem, interface and software requirements and explains how these are combined to deliver the system requirement. The satisfaction argument might also refer to one or more SRACs (*4.3.4* of this document).

G 4.5.1.7 The process of apportionment could result in changes to the system requirements, interfaces, or application conditions. These changes might arise as a result of various design activities including trade-offs (for example between performance and cost) or ongoing risk analysis and evaluation (*4.3.3* of this document). These will be made under change control as set out in *3.5* of this document and the client might need to liaise with stakeholders to agree them.

G 4.5.1.8 Supporting tools used for installation, configuration, commissioning, and maintenance of the system under consideration will be included in the system architecture (*4.5.3* of this document) and requirements for these tools will be developed in order to demonstrate that the system requirements are met. These tools might themselves be sources of hazard and are subjected to safety assurance as part of the system.

4.5.2 Pre-existing subsystems or software elements

4.5.2.1 When a pre-existing subsystem or software element is proposed for use within the system, and when the failure of this subsystem or software element could cause a hazard, the client shall require that a safety justification is produced.

4.5.2.2 The safety justification shall demonstrate that the subsystem or software element under consideration does not introduce unacceptable safety risk and shall cover:

a) the extent of prior use of the subsystem, including similarities and differences in the intended use in the system;
b) design changes to the subsystem since any previous approval;
c) the nature of prior approvals and certification, the scope of evidence available, and how these integrate with the safety case for the system;
d) the consequences of failure of the subsystem, as well as design mitigations to control these, and that the mitigations have been included in the system; and

e) any additional verification and validation activities to be undertaken to provide evidence to support the use of the subsystem in the system.

Rationale

G 4.5.2.3 If this analysis was not carried out it might be discovered later that the subsystem or software requirements could cause a hazard. If this happens later in the project, the rework could be expensive. If this happens after the system has entered service, a hazard might be caused.

Guidance

G 4.5.2.4 The suite of railway software standards contains guidance relating to re-use.

G 4.5.2.5 The intended use of the subsystem includes both functional and non-functional requirements placed on the subsystem. As such, these are included when considering the similarities and differences in intended use.

G 4.5.2.6 The use of pre-existing systems might give rise to obsolescence issues. A complete set of system requirements includes service life, and this allows those obsolescence issues to be identified when considering the intended use of the subsystem.

G 4.5.2.7 The term commercial off-the-shelf (COTS) is used to describe components or software elements that are made available to the market as commercial products. Requirements and guidance in this section are applicable to COTS components or software elements if they are customised to perform safety-related functions.

G 4.5.2.8 There is a checklist in *A.5* of this document which contains points to consider when confirming that a pre-existing element is suitable for application in the system under consideration.

4.5.3 System architecture

4.5.3.1 The client shall require that an architecture description is produced which describes:

a) the components of the system (including software components and tools for configuration, installation and maintenance of the system);
b) the interfaces between components;
c) the external interfaces with people and other railway systems; and
d) how the components work together with people and other railway systems in order to deliver the requirements.

Rationale

G 4.5.3.2 Without a system architecture, it might be difficult or impossible to demonstrate that the subsystems, interface and software requirements are sufficient to ensure that the system requirements are met.

G 4.5.3.3 Including tools for configuration, installation and maintenance within the system architecture aims to ensure that they are considered as part of the apportioning of system requirements as set out in *4.5.1*, and within the ongoing process of risk analysis and evaluation as set out in *4.3.3*.

G 4.5.3.4 For software-based systems, the system architecture has a major role in delivering the non-functional requirements of the system, for example, requirements relating to performance, reliability, etc. This is because these aspects of the system depend not just on the performance and reliability of the subsystems but also on how the subsystems combine to deliver the system requirements. It could, for example, be possible to increase reliability by introducing redundancy into the architecture.

Guidance

G 4.5.3.5 There is a substantial amount of good practice in systems architecture development available, particularly from the International Council on Systems Engineering (INCOSE) such as INCOSE zGuide Z8. This includes notations such as the Unified Modelling Language (UML).

G 4.5.3.6 The client might need to facilitate the agreement of the description of the external interfaces to other railway systems with the party on the other side of the interface.

G 4.5.3.7 Software-based railway systems are often dependent on configuration data to define aspects of behaviour in a specific application. The tools used to prepare this configuration data might themselves be sources of hazard. Similarly, tools used to install software for operational use can also be a source of hazard if they function incorrectly.

G 4.5.3.8 Where a system delivers functions that have been determined to have different SILs the architecture is sometimes designed to separate the highest SIL functions from the remainder of the system functionality in order to limit the scope that is subjected to the more rigorous development processes. Particular attention is given in such cases to ensure that the risk of interference has been adequately managed. The consequence of failures in interfacing systems is considered when undertaking risk analysis as set out in *4.3.2* and *4.3.3* of this document.

4.5.4 Subsystem integration

4.5.4.1 The client shall require that plans are produced that describe how the subsystems will be integrated to form a complete system.

Rationale

G 4.5.4.2 If integration is not carried out in a planned and systematic way within a realistic and representative environment, hazardous faults might be missed and hazardous interactions with other systems could be caused. In addition, if integration is not carried out in a planned and systematic way, it could take longer and cost more than is necessary.

G 4.5.4.3 If integration is not planned, it is possible to miss the fact that additional functions or equipment will be needed to perform integration, which could result in expensive rework later in the project.

Guidance

G 4.5.4.4 The guidance on planning system integration outlined in *4.4.3* of this document is also applicable to subsystem integration.

G 4.5.4.5 System integration as set out in *4.4.3* of this document and subsystem integration into the system can be planned together.

G 4.5.4.6 Typically, the integration of the system under consideration with existing external systems is planned with the owners of those systems. The client might need to liaise with those owners in order to make this happen.

4.5.5 Managing assumptions

4.5.5.1 The client shall require that assumptions relevant to safety which are made by one stakeholder of the project and need to be confirmed by another stakeholder, are documented, managed, and traced to their use.

Rationale

G 4.5.5.2 Project designers sometimes have to proceed with incomplete information, in which case they have to proceed on the basis of assumptions. It is essential to establish whether the assumptions relevant to safety are true or false and to initiate rework if false assumptions are identified. Suppliers and other project stakeholders can manage assumptions that they can check themselves without involvement by the client but the client will need to be involved when multiple stakeholders are involved.

G 4.5.5.3 Tracing assumptions to where they are used allows the impact to be assessed if or when those assumptions are established to be false.

Guidance

G 4.5.5.4 It is common to establish a register of assumptions so that suppliers and other project stakeholders can enter assumptions into this register. There can be benefit in a centralised register since it helps to ensure that the project has a common set of assumptions.

G 4.5.5.5 Although this requirement relates only to assumptions relevant to safety, the register could be used for other assumptions as well.

G 4.5.5.6 The register could also be used for other project 'loose ends' such as caveats, dependencies and issues.

G 4.5.5.7 A typical lifecycle for an entry in an assumptions register is as shown in Figure *3*.

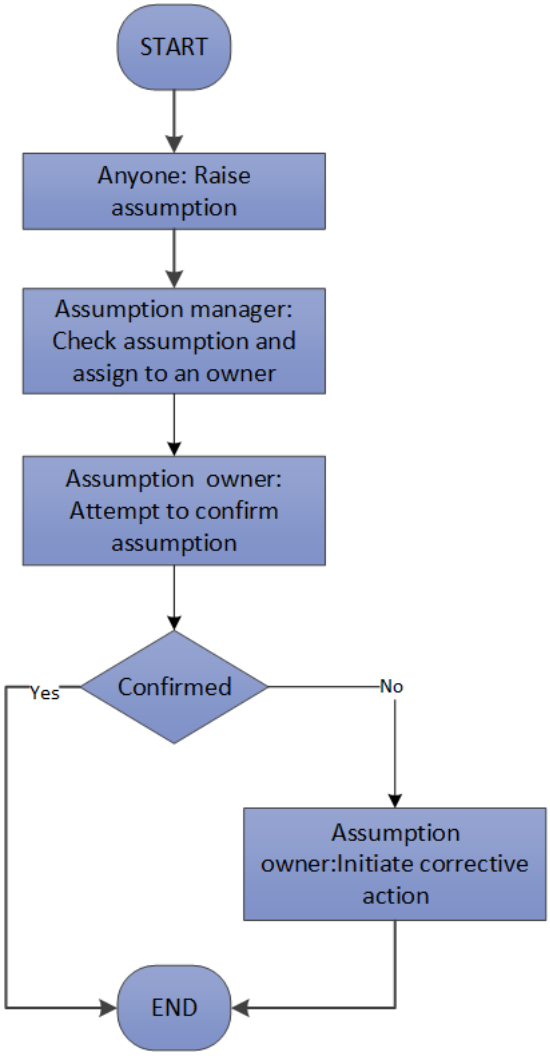

Figure 3: Typical issues resolution process

4.6 Phase 9 - System validation

4.6.1 The client shall review validation outcomes and confirm that compliance with system requirements is demonstrated across a representative breadth of usage scenarios, and system configuration values, and in a test environment that is representative of operational use.

Rationale

G 4.6.2 If validation is not carried out across a representative range of usage scenarios and system configuration values, then the system might not fulfil the intended user need during operation. If validation is not carried out in a representative test environment, then the evidence gathered might not support a claim that the system will function correctly in service.

Guidance

G 4.6.3 The definition of the term validation in BS EN 50126-1:2017 is 'confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.'

G 4.6.4 This definition is accompanied by a number of notes, including note 3 which reads 'in design and development, validation concerns the process of examining an item to determine conformity with user needs.'

G 4.6.5 The objectives of system validation are:

a) to confirm that the system behaves as expected (that is, in accordance with its requirements) in its operational environment; and
b) to determine whether the operation of the system results in any unwanted side-effects.

G 4.6.6 The use of a representative test environment for system validation includes operation by representative users. Ideally, this would be by the actual user community.

G 4.6.7 The importance of care in planning the acceptance of systems that contain configuration data is set out in *4.4.2* of this document.

G 4.6.8 An operational trial is a typical method used to ensure that validation takes place in a representative environment.

G 4.6.9 If the validation exercise is to support acceptance of a system before entry into service then it is vital that the configuration, that is subject to validation, is known, and any changes between the completion of validation and entry into service are controlled. Further guidance on the control of change is set out in *3.5* of this document.

G 4.6.10 Defects identified during system validation are often expensive to rectify. The client might choose to put in place restrictions on the use of the system to mitigate these defects and allow the system to continue into operation. These restrictions might be permanent, or temporary until the fault is fixed and the validation activity repeated. Operational mitigations are used as a last resort and are only considered when the source of the defect has been identified, as putting system into use might restrict the access to investigate and rectify the underlying problem thus further extending the defect period and potentially the cost impact.

G 4.6.11 Audit and inspection to ensure compliance with approved plans is set out in *3.6* of this document.

G 4.6.12 There is a checklist *A.6* of this document which contains points for consideration when confirming, prior to validation, that the arrangements are comprehensive.

4.7 Phase 10 - System acceptance

4.7.1 The client shall only accept the system when the risk associated with any non-compliance or gap in compliance evidence has been shown to be adequately controlled. Any decision to accept the system shall confirm:

a) the actions are in place to achieve compliance and the timescales for those actions;
b) any measures are in place to control risk while the gap is rectified.

Rationale

G 4.7.2 With the information required, the client can assess the total risk associated with all compliance gaps and use this as input to the acceptance decision.

Guidance

G 4.7.3 Gaps in compliance might be areas where a system is not yet compliant with a requirement or where compliance has not yet been demonstrated.

G 4.7.4 Measures to control risk might include restrictions on the operation of the system.

4.8 Phase 11 - Operation, maintenance, and performance monitoring

4.8.1 Retain system capability through life

4.8.1.1 The client shall require that activities are planned and carried out to retain system capability through life.

Rationale

G 4.8.1.2 System capability can be reduced by changes inside the system, such as obsolescence, as well as changes outside the system, such as lack of familiarity with the operation of system functions. A rapid response can be made if the reduced system capability that could impact safe operation is identified quickly.

Guidance

G 4.8.1.3 Although the supplier might provide a warranty for the system and be responsible for supporting it for a period after entry into service, the client's organisation will generally be involved in the operations, maintenance and support of the system.

G 4.8.1.4 Examples of functions that are rarely used, and could increase risk owing to lack of familiarity, include those that support restoring system function from backups or the retrieval of information for incident investigation.

G 4.8.1.5 Even when a system continues to perform as intended, it might cease to meet operational needs as a result of those needs changing. These changes in operational needs might be obvious, such as the lack of a desired system function, but might be more subtle, such as a need to deliver the same system functions for a longer lifetime than originally intended.

G 4.8.1.6 Activities planned and carried out under this requirement will include those identified in the maintenance lifecycle concept (*4.2.2* of this document) and related usage scenarios (*4.4.1* of this document). Activities to satisfy SRACs will remain in place. These activities will often be an integral part of the business-as-usual processes for the system's operator and maintainer.

4.8.2 Retain system data for incident investigation

4.8.2.1 The client shall require that facilities are in place to retain system data to support incident investigation.

4.8.2.2 The client shall require that operating processes and user training include instructions for the retaining of system data to support incident investigation.

Rationale

G 4.8.2.3 Without retention of such data, it could be difficult to find the cause of incidents and therefore to act to prevent their recurrence. The client organisation might have legal and regulatory requirements to retain such data.

Guidance

G 4.8.2.4 In order to comply with this requirement, it is vital that the design of the system under consideration includes the functions to support incident investigation. Guidance is provided in *4.4.1* of this document that explicitly identifies incident investigation as a usage scenario for the system.

G 4.8.2.5 Processes to retain data in the event of an accident are an integral part of the business-as-usual processes for the system's operator and maintainer.

G 4.8.2.6 There is a checklist in *A.7* of this document which contains points to be considered when confirming that arrangements for retaining data for incident investigation are thoroughly defined and fit for purpose.

4.8.3 Report, analyse, and correct system performance issues and defects

4.8.3.1 The client shall require that:

a) system performance is monitored;
b) defects and deviations from expected performance are reported, analysed to identify the root cause;
c) defects in the systems arising from the identified root cause are corrected;
d) other root causes, such as misuse of the system, are mitigated.

Rationale

G 4.8.3.2 The system might not exhibit, when it is put into service, the performance which was expected. In addition, performance can degrade over time for reasons such as degradation in hardware, changes to other systems, processes, or technology obsolescence.

G 4.8.3.3 If hazardous defects, failures, and performance deviations are not promptly identified and corrected, they could recur and cause an accident.

G 4.8.3.4 This requirement ensures that the scope of a Defect Recording Analysis and Corrective Action System (DRACAS) includes deviation from expected performance even when this has not resulted in a failure.

Guidance

G 4.8.3.5 Performance information is often collected using a DRACAS. Performance metrics such as the mean time between failure can be calculated from the underlying information in order establish not just current performance but performance over time. Setting targets for these metrics is particularly important for metrics which are correlated with safety risk.

G 4.8.3.6 While some defects might be clearly hazardous, performance that deviates from expectations could indicate an underlying defect that needs investigation. Defects could exist even if operational performance is not adversely affected.

G 4.8.3.7 It can take time to identify, analyse, and correct a fault. The longer this process takes, the greater the opportunity for a corresponding hazard to occur and cause an accident. Examples of immediate operational response include restricting the use of the system, adding additional checks, or even taking the system out of service.

G 4.8.3.8 System performance for software-based systems includes aspects such as:

a) resource usage (memory, processor, non-volatile storage);
b) logged incidents (for example detected error conditions) and the rate of those incidents; and
c) occurrences of intended responses to exceptional events to ensure they do not indicate an underlying defect (for example system restarts due to error conditions - if these responses are more frequent than expected during design, then the underlying cause is investigated).

G 4.8.3.9 Engagement from system suppliers, particularly in the early stages of system operation, is often needed to support the analysis of system performance. It is important to include the support as part of the supplier activities identified and assigned in the safety assurance strategy.

G 4.8.3.10 Changes to the system to correct identified defects are subject to change controls as set out in *3.5.1* of this document.

G 4.8.3.11 These activities will often be an integral part of the business-as-usual processes for the system's operator and maintainer.

Appendices

Appendix A Checklists

Note: The content of this appendix is provided for guidance only.

A.1 Introduction

Guidance

G A.1.1 Checklists are used in this standard to include points that users might wish to consider, to help achieve compliance of the related requirements.

G A.1.2 Cross reference to the related requirement is provided for each checklist.

A.2 Supplier selection

Guidance

G A.2.1 Referenced from *3.2.2* of this document.

G A.2.2 The following points can be considered when seeking evidence of supplier competence:

a) Evidence of demonstration of competencies on comparable projects
b) Description of general management systems
c) Evidence of proven processes for
    i) requirements management
    ii) design and manufacture
    iii) installation
    iv) verification
    v) validation
    vi) testing
    vii) commissioning
    viii) maintenance
    ix) configuration management
    x) interface management
    xi) safety analysis and management
    xii) assurance
d) Evidence of competence management systems
e) CVs of key project staff members.

A.3 Audit and assessment

Guidance

G A.3.1 Referenced from *3.6* of this document.

G A.3.2 The following points are considerations when checking a programme of audit and inspection:

a) Are there any third parties involved?
b) Have minimum frequencies of audit and inspection been defined?
c) Is there a need to define arrangements for inspection of sealed components?
d) Is there a need to define arrangements for inspection of supporting documentation (for example software development cycle outputs, material and data sheets)?
e) Is there a need to define arrangements for inspection of testing records?
f) Have thresholds been defined for escalation of issues that are found?
g) Is the relationship between audit and inspection activities and stage gate reviews clear?
h) Has the approach to tracking and resolution of actions identified as well as confirming their resolution at stage gates been defined?
i) Does there need to be 'spot checks' (unannounced and announced) on the supplier and supply chain?

A.4 Usage scenarios

Guidance

G A.4.1 Referenced from *4.4.1* of this document.

G A.4.2 The following points could be considered when looking for missing system requirements:

a) Have all abnormal, degraded and failure scenarios been identified?
b) Have criteria been defined for tolerable obsolescence?
c) Have criteria been defined for ease of maintenance?
d) Have criteria been defined for ease of renewal?
e) Have requirements been defined for software version control and storage, including retaining supporting design and maintenance documents?
f) Have requirements been defined for access to data records during live operation of the system?
g) Is there a need to define limitations on the use of volatile memory, or temporary storage media?
h) Is there a need to define the types of backup storage media and supporting systems (for example power) to be used?
i) Have requirements been defined to support reversion to earlier versions of software and data, including the ability to recreate software versions?
j) Have requirements been defined to deal with defect data or data values that are outside boundaries?

A.5 Pre-existing subsystems or software elements

Guidance

G A.5.1 Referenced from *4.5.2* of this document.

G A.5.2 The following points are considerations when confirming that a pre-existing element is suitable for the system under consideration:

a) Is there a mapping between the specification of the pre-existing element and the requirements to be met by the system?
b) How much change is needed to make the pre-existing element suitable?
c) What is the risk associated with carrying out this change?
d) What evidence is there for reliable performance of the pre-existing element in its current applications?
e) What mitigation actions are available to control the risk in the previous points?
f) Are there clear limitations on the use of the pre-existing element?
g) Is it intended to use the pre-existing element outside the limitations in the previous points?

A.6 System validation

Guidance

G A.6.1 Referenced from *4.6* of this document.

G A.6.2 The following points are considerations when confirming, prior to validation, that the arrangements are comprehensive:

a) Is there an appropriate division of tests between factory tests and site tests?
b) For site tests, have safety arrangements been confirmed? Is the system under test being relied on for safety? What mitigations are in place in case of failure?
c) How are test results recorded and delivered?
d) How are test results stored?
e) Is the test environment defined?
f) Do the tests cover a representative range of usage scenarios?
g) Are the criteria for suspending and restarting tests defined?
h) Are there agreements in place to support the necessary access to test data?
i) Are there agreements in place for ensuring that test data, results, software and equipment are not disposed of until they are no longer needed (bearing in mind the potential need for them to support future incident investigation)?

A.7 Retain system data for incident investigation

Guidance

G A.7.1 Referenced from *4.8.2* of this document.

G A.7.2 The following points are considerations when confirming that arrangements for retaining data for incident investigation are fit for purpose:

a) How frequently does the data need to be collected or looked at?
b) What steps need to be taken to secure data when carrying out software upgrades?
c) What systems and software are involved to record, store, access, view and analyse system data, including interfaces with third party tools?

d) Have the recording and retention elements of the system been integrated with the rest of the design?
e) Is there an agreement in place between the suppliers and client about who will perform regular tests and analysis of the recording and retention systems?
f) Are there agreements in place for the sharing of data between client and suppliers?
g) Are there processes in place for using the data to support root cause analysis of incidents leading to lessons learned and corrective actions?
h) Does the scope of defects to be recorded include all which could create the potential for an incident?
i) Are there agreements in place that will allow the suppliers to participate in the investigation of safety-related failures?

Appendix B Case studies

Note: The content of this appendix is provided for guidance only.

B.1 Introduction

Guidance

G B.1.1 This appendix contains a set of case-studies relating to incidents caused by software failure both inside and outside the rail industry. A summary of the incident is provided for each case study. This is followed by a table of key safety assurance concepts and related requirements in this standard that could be applicable to an incident with similar cause.

G B.1.2 Additionally, in response to the RAIB Cambrian recommendations, Network Rail has set up a website to 'support the wider rail industry with improved capture and dissemination of safety learning through the reporting and systematic investigation of complex software-based system failures'. This is available from www.safety.networkrail.co.uk.

G B.1.3 A series of podcasts on software incidents can be found on RSSB's website www.rssb.co.uk. Members of RSSB can access case studies from other sectors on the RSSB website.

B.2 Cambrian Coast line incident

Guidance

G B.2.1 This case study has been derived from material presented in the RAIB report (2017). It highlights the need for the clear communication of assurance responsibilities, and the importance of challenging non-standard safety justifications for re-used system components. Additionally, the difficulties experienced by the investigation team as a result of the lack of system log data reinforces the importance of this aspect of system design.

G B.2.2 On the morning of 20 October 2017, four trains travelled over the Cambrian Coast line, Gwynedd, while temporary speed restriction data was not being sent to the trains by the signalling system. No accident resulted but a train approached a level crossing at 80 km/h (50 mph), significantly exceeding the temporary speed restriction (TSR) of 30 km/h (19 mph) needed to give adequate warning time for level crossing users.

G B.2.3 The Cambrian Coast line is operated using an installation of the European Rail Traffic Management System (ERTMS) which replaces traditional lineside signals and signs by transmitting data direct to the train for display to the train driver and for automatic supervision of train speed. The data transmitted to the train includes TSRs.

G B.2.4 The ERTMS system operating on the Cambrian Coast line consists of a number of subsystems. For simplicity only three are considered here:

a) Radio Block Centre (RBC) - part of the communication chain between the interlocking and the train. Generates messages to, and interprets messages from,

the train including movement authorities, and speed restrictions (both temporary and permanent);

b) Poste de Gestation des Signalisations Temporaires (GEST) server - manages the implementation and removal of TSRs, communicating these to the RBC; and

c) GEST terminal - the signaller interface to the GEST server.

G B.2.5 On investigation it was found that the ERTMS had stopped transmitting TSR data to trains after a shutdown and restart of the RBC the previous evening. There was no indication to the signallers of an abnormal condition, and the GEST terminal display at the signalling control centre wrongly showed the TSRs as being applied correctly. During the investigation it was found that RBC restarts were being used more frequently than would be expected, although this was not directly related to the cause of the incident.

G B.2.6 The TSR data on the RBC was held in volatile memory, meaning that it was lost during an RBC restart and was reloaded from the GEST server.

G B.2.7 A lack of system logging data meant that the investigation could not conclusively determine the cause of the software failure. However, the most likely cause was identified as a corrupt database within the GEST server resulting in a software module ceasing to operate. This software module was responsible for communicating TSR data between the GEST terminal and the RBC. The failure was not indicated to the signallers, and other software modules on the GEST server continued to operate causing:

a) the appearance of correct behaviour to the signallers on the GEST terminal, resulting in their manual check of the active TSRs being carried out based on false information; and

b) the communication of an incorrect empty set of TSRs from the GEST server to the RBC when the RBC restarted.

G B.2.8 The GEST server and terminal were designed to achieve SIL 2. However, the ERTMS functions relating to TSRs were required to achieve SIL 4. Recognising this, an independent manual integrity check was provided to support the use of SIL 2 GEST system. However, the software module failure that resulted in the Cambrian incident affected both the provision of TSR data to the RBC and the display of that data to the signallers: it was a failure common to both functions, demonstrating that the functions were not independent, and that the system design did not meet the required SIL.

G B.2.9 The GEST server and terminal were pre-existing subsystems within the ERTMS architecture and were accepted into service without the production of a generic product safety case but instead relied on other documentation including a safety report considering the differences between the Cambrian version of GEST and the version produced for a project in France, and also an SNCF review of the ERTMS system produced for the same project in France. The RAIB investigation concluded that these documents 'were not an adequate substitute for a generic product safety case' (paragraph 109). Additionally, the ERTMS system supplier had modified the design of the system for the project in France from that which was considered in the safety report and SNCF review that were submitted in support of the Cambrian implementation. The modified design stored TSR data in non-volatile memory in the

RBC. This change was not considered necessary for the Cambrian line implementation, but had the change been implemented then there would have been no need for the RBC to retrieve TSR data from the GEST when the RBC restarted.

Key safety assurance concept	Related requirements in this standard
Responsibilities for safety assurance are clearly identified.	*3.1.1* Safety assurance strategy
The use of pre-existing software elements is justified and includes consideration of how the associated safety risk is managed.	*4.5.2* Pre-existing subsystems or software elements
Suppliers are required to inform the client of safety-related changes to systems.	*3.3.1* Contract terms
System logs are retained and available for incident investigation.	*4.8.1* Retain system capability through life *4.8.2* Retain system data for incident investigation
System validation demonstrates compliance across a representative breadth of scenarios and system configuration, including failures, degraded operation, abnormal operation, and misuse.	*4.6* Phase 9 - System validation
Traceable records exist from safety functions to design and assurance evidence.	*3.1.3* Safety assurance records
System performance is monitored and analysed to determine the cause of deviations from expected performance.	*4.8.3* Report, analyse, and correct system performance issues and defects

Table 4: Key safety assurance concepts (Cambrian Coast line incident)

B.3 Irregular signal sequence at Milton Keynes

Guidance

G B.3.1 This case study has been derived from material presented in the RAIB special investigation report (2014). It highlights the possible consequences of defects in configuration data, and invites the reader to consider that configuration data can be sufficiently complex that it represents a form of software in its own right (in this case the configuration data effectively 'programs' the interlocking).

G B.3.2 On 29 December 2008 an irregular signal sequence was reported by the driver of a train at Milton Keynes central station. A signal was seen to change from a red aspect

to a green aspect even though the track beyond the signal was occupied by another train that was visible to the driver.

G B.3.3 New signalling had been commissioned in the Milton Keynes area on the day before the incident as part of the West Coast Route Modernisation (WCRM) project. Investigation undertaken by WCRM project staff discovered errors in the configuration data for the solid state interlockings (SSI) covering the Milton Keynes station area. The affected route was removed from use for approximately a week while the issue was rectified and tested.

G B.3.4 A formal investigation led by Network Rail found that the occupation status of some axle counter sections were not included in the SSI configuration data for the affected signal. The investigation report identified a number of failures in the processes for developing and testing the SSI configuration data, and for commissioning the updated signalling.

G B.3.5 The RAIB also undertook a review of the formal investigation and identified further findings relating to shortcomings in the Network Rail investigation. The RAIB findings of particular relevance to this standard cover areas such as regression testing following system changes, the definition of interfaces between SSIs, the role of configuration data design tools in both reducing the risk of errors by the designer and verifying the configuration data against signalling principles, and the depth and quality of the evaluation undertaken by the safety review panel for the signalling change.

Key safety assurance concept	Related requirements in this standard
System hazard identification and risk assessment carried out giving consideration to the full scope of system functions and scenarios.	*4.3.2* Initial risk analysis and evaluation
The system architecture and requirements include any supporting tools used for installation, configuration, commissioning and maintenance of the system.	*4.5.1* Subsystem, interface and software requirements *4.5.3* system architecture
The system architecture includes descriptions of the interfaces between system components, and between the system and other railway systems.	*4.5.3* System architecture
System validation demonstrates compliance across a representative breadth of scenarios and system configuration, including failures, degraded operation, abnormal operation, and misuse.	*4.6* Phase 9 - System validation

Key safety assurance concept	Related requirements in this standard
Configuration management processes include the assessment of the impact of changes to configuration items, including configuration data.	*3.5.1* Change Control Processes
Acceptance planning includes the processes used to generate the configuration data and commission systems into operational use.	*4.4.2* Acceptance processes and criteria

Table 5: Key safety assurance concepts (Irregular signal sequence at Milton Keynes)

B.4 NATS air traffic control system failure

Guidance

G B.4.1 This case study has been derived from material presented in the CAA report (2015). Although it is not clear that additional reasonable measures could have prevented this incident, the example does point out the need for validation to be conducted in a way that is representative of operational use, and the potential for changes in operational use to expose latent faults.

G B.4.2 On the afternoon of 12 December 2014 the failure of a computer system used to provide information to Air Traffic Controllers resulted in disruption to flights in UK airspace. Traffic restrictions were in place for over five hours, and estimates of the impact of these restrictions determined that a maximum of 1900 flights and 230,000 passengers were directly or indirectly affected. An independent enquiry was established to investigate the cause of the failure, the recovery, and other relevant factors.

G B.4.3 The enquiry determined that the immediate cause of the incident was a latent fault within the system software that implemented an incorrect limit on the number of Atomic Functions in the system. In broad terms, the number of Atomic Functions relates to the number of recipients of air traffic data from the central System Flight Server (SFS). The fault had been present in the software since at least 1998, and was triggered because changes in the operational use of the system caused the number of Atomic Functions to exceed the incorrectly implemented limit. These operational changes were put in place on 11 December 2014 - the day before the incident.

G B.4.4 Failure of the SFS can have safety consequences since it may result in differences between the information presented to controllers and the underlying air traffic data. The system design includes a redundant pair of SFSs - failure of the primary SFS results in the transfer of operation to the secondary SFS. Air traffic control continues with a single SFS until the primary can be restored.

G B.4.5 When the number of Atomic Functions exceeded the incorrect limit the software on the primary SFS raised an internal error. This error resulted in the primary SFS being shut down and control passed to the secondary SFS. This response would be appropriate if the primary SFS failure was caused by a hardware fault. However, the

software on the secondary SFS implemented the same incorrect check on the number of Atomic Functions and, as a result, the same internal error was raised causing the secondary SFS to also shut down.

G B.4.6 The fault that caused the incident was identified rapidly despite the size of the system (approximately 2 million lines of source code). The enquiry identified that this was a result of the level of detail in system logs, and the accessibility of those logs to the system experts involved in the investigation.

G B.4.7 The enquiry identified opportunities for the fault to have been identified during development, but the tests and reviews that were undertaken at the time of system development and also as part of the software release in support of the operational changes introduced on 11 December 2014, were considered to be reasonable. The fault could also have been found during acceptance tests but the system used for these tests consisted of a reduced set of workstations and could only have breached the incorrectly implemented limit using an artificial configuration that would not be representative of operational use.

Key safety assurance concept	Related requirements in this standard
System validation demonstrates compliance across a representative breadth of scenarios and system configuration in a test environment that is representative of operational use.	*4.6* Phase 9 - System validation
System performance is monitored and the root cause of deviations from expected performance is analysed, even where operational performance is not yet adversely affected.	*4.8.3* Report, analyse, and correct system performance issues and defects
System logs are retained and available for incident investigation.	*4.8.1* Retain system capability through life *4.8.2* Retain system data for incident investigation

Table 6: Key safety assurance concepts (NATS air traffic control system failure)

B.5 A400M Disaster

Guidance

G B.5.1 This case study has been derived from an incident summary report (RSSB, 2021). It demonstrates the need to consider all lifecycle stages and support tools as part of the system for the purposes of hazard identification.

G B.5.2 On 9 May 2015 a military Airbus A400M aircraft crashed near Seville killing four of the six crew members. The crew had reported a technical fault and the plane struck an electricity pylon while attempting an emergency landing.

G B.5.3 The incident investigation determined that three of the plane's four engines did not respond to the crew's attempts to control power as a result of calibration parameter data being wiped during engine software installation. The incident took place on the first flight after assembly. The incorrect configuration resulted in engine power being "all or nothing" - the affected engines were initially stuck at high power and, on being reduced, were then stuck at idle. The resulting loss of power from three engines caused the aircraft to crash.

Key safety assurance concept	Related requirements in this standard
Concepts and scenarios for system installation, configuration, and commissioning are developed.	*4.2.2* Lifecycle concept development *4.4.1* Usage scenarios
System hazard identification and risk assessment carried out giving consideration to the full scope of system functions and scenarios.	*4.3.2* Initial risk analysis and evaluation *4.3.3* Ongoing risk analysis and evaluation
The system architecture and requirements include any supporting tools used for installation, configuration, commissioning and maintenance of the system.	*4.5.1* Subsystem, interface and software requirements *4.5.3* System architecture
System validation demonstrates compliance across a representative breadth of scenarios and system configuration, including failures, degraded operation, abnormal operation, and misuse.	*4.6* Phase 9 - System validation

Table 7: Key safety assurance concepts (A400M disaster)

Appendix C Guidance on the preparation of high integrity software specification

Note: The content of this appendix is provided for guidance only.

C.1 Adequate requirement specification

Guidance

G C.1.1 Adequate requirements are complete, correct, and consistent and include the identification of safety functions. Any requirement that is incorrect, unclear, ambiguous or omitted is a systematic fault.

G C.1.2 Complete requirements are typically supported by documentation that describes the source and reason for the requirement and its development history.

G C.1.3 The need to define usage scenarios that cover all modes of use to identify any gaps in requirements specification are set out in *4.4.1* of this document.

C.2 Principles for complete requirements

C.2.1 Requirement categorisation

Guidance

G C.2.1.1 It is unlikely that all requirements can be derived without an iterative process. The criteria for requirements and the related documentation are set out in clause 7.2 of BS EN 50128:2011.

G C.2.1.2 In order to check the completeness of the requirements, it is useful to consider different categories of requirements. Examples include:

a) Functional
b) Safety
c) Security, for example protection from cyber-attacks and the access rights
d) Operational, for example interaction with other systems and user interface
e) Software performance, for example speed of processing and compatibility with other system processes
f) Input and output data
g) Reliability
h) Maintainability
i) Compatibility with other software applications and communication protocols
j) Data access connectivity (database connection compatibility).

G C.2.1.3 Identifying all stakeholders in a project and understanding how they are related to different categories of requirements helps to prevent important details being omitted.

G C.2.1.4 In the case of a new software development, or in the case of integration of different pieces of software, the involvement of software engineers in the process of specifying the requirements can assist with the supplier's understanding of the requirements.

C.3 Principles for correct requirements

C.3.1 Documenting the system's operating environment

Guidance

G C.3.1.1 Typically, the operating environment of a software-based system contains:

a) Operators, users, or both
b) External interfaces (interfaces with equipment or interfaces with people)
c) Externally connected equipment or system

G C.3.1.2 Inconsistent or incomplete specifications of any of the interfaces could lead to failures.

G C.3.1.3 A 'data dictionary' can be created and maintained as part of the system specification to facilitate understanding of the data items used in the software. The data dictionary describes the meanings and the formats (dimensions, units and representations) of static and dynamic data items that the software-based system either receives from, or transmits to, its intended operating environment.

G C.3.1.4 A data dictionary reduces the potential for different assumptions being made about the meanings and formats of data items. It provides an objective and agreed point of reference for checking the dimensional correctness of the calculations specified to be performed within the software-based system.

G C.3.1.5 The data dictionary supports the implementation of defensive programming, as set out in Annex D.14 of BS EN 50128:2011, which is a useful technique to prevent failure due to unexpected inputs.

C.3.2 Documenting the limits of operations of the software

Guidance

G C.3.2.1 It is possible for software to create hazards in the system's operating environment if it does not perform as intended. It is therefore important for the customer to identify the limits of operation of the software and specify this to the supplier.

G C.3.2.2 Identifying the limits of the inputs, for example, minimum and maximum values, allows invalid inputs to be identified and fault messages created.

G C.3.2.3 A systems engineering approach can be used to aid this process, particularly for safety functions. Example steps are:

a) Define what is the objective or safety target for the function;
b) Identify and list input variables and expected outputs; and
c) Define and document test-cases or scenarios that will demonstrate expected results:
    i) Expected inputs result in expected outputs
    ii) Unexpected inputs do not result in undesired outputs.

G C.3.2.4 An example of guidance that defines the limits of operation is 'When button 'x' is pressed, the speed of the train is displayed in miles per hour'.

C.4 Principles for consistent requirements

C.4.1 Managing changes in software requirements

Guidance

G C.4.1.1 Keeping track of changes to software requirements during the specification development can be challenging.

G C.4.1.2 Principles, to keep requirements consistent include:

a) Documenting the requirements and the rationale for choosing each specific requirement;
b) Keeping requirements under strict version control;
c) Using an automatic tool to document changes in requirements; and
d) Modelling the requirements at the appropriate level of abstraction, if possible.

C.4.2 Verification of requirements

Guidance

G C.4.2.1 Verifying software requirements provides confidence that the correct requirements have been elicited from the software requirements specification. Useful methods of verification include:

a) Prototyping (useful for systems with user interfaces)
b) Simulating the requirements and assessing them for consistency against the core requirements
c) Scenario based walk-throughs
d) State machines
e) Animation and model simulation
f) Model-based design tools.

Definitions

Approved Body (ApBo)	These are bodies approved by the Secretary of State who are responsible for assessing the conformity or suitability for use of the interoperability constituents or for appraising the UK procedure for verification of subsystems.
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. Source: *CSM RA*
assurance	A positive declaration intended to give confidence.
basic integrity	Integrity attribute for safety related function with a Tolerable Functional Failure Rate higher than (less demanding) 10^{-5} [h^{-1}] or non-safety related function. Source: *BS EN 50126-1:2017*
change control	The process of assessing, approving, tracking and managing potential changes against a configuration baseline to ensure no unnecessary changes are introduced.
commercial off-the-shelf (COTS)	Used to describe components or software elements that are pre-existing and of broad application that are made available to the general market as commercial products.
Common Safety Method for Risk Evaluation and Assessment (CSM RA)	Commission Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment.
configuration baseline	A self-consistent set of configuration items at key points in the project (for instance at stage gate reviews) which then form a starting point for change control.
configuration data	Data which is inputted into a system in order to adapt it to its environment or to adjust its functionality.
configuration item	An item under configuration management.
configuration management	The process of identifying and documenting the characteristics of a system and its components (including computer systems and software), and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the system documentation.
configuration status accounting	Maintaining records about the configuration items and about proposed and actual changes.
configuration	A means of describing the system, its components, its specification and other items, including manuals and test material that must be maintained to claim the system composition remains valid.

Data Recording and Corrective Action System or Defect Reporting Analysis and Corrective Action System (DRACAS)	A formal closed loop corrective action process that is used to continually monitor a system, in order to continually improve quality of service and system reliability.
Designated Body (DeBo)	Independent third parties appointed by the Secretary of State to assess and verify conformity of projects with National Technical Rules (NTRs) in the United Kingdom. They operate in tandem with Approved Bodies which assess and verify conformity with National Technical Specification Notices (NTSNs).
entity in charge of maintenance of a vehicle (ECM)	An ECM is registered as an ECM for a vehicle in the national vehicle register, and can include people or organisations such as railway undertakings, infrastructure managers, keepers or maintenance organisations. Source: *ROGS*
entry criteria	Criteria for allowing a stage gate review to start.
European Rail Traffic Management System (ERTMS)	Signalling and operation management system encompassing ETCS for control command, and GSM-R for voice and data. It is a system for providing real-time control and supervision of trains, consisting of trainborne, track and lineside equipment. The objective is to enable the operation on compatible signalling systems across European borders.
exit criteria	Criteria, applied at a stage gate review, for allowing the project to proceed to the next phase.
Failure Mode, Effects and Criticality Analysis (FMECA)	A bottom-up inductive analytical method used to analyse failure modes of processes, products and systems to eliminate them.
GEST	A proprietary terminal which provides an interface between signallers and radio block centre on Ansaldo-STS ERTMS equipment.
hazard	A condition that could lead to an accident. Source: *CSM RA*
hazard log	An alternative name for 'hazard record'.
hazard record	The document in which identified hazards, their related measures, their origin and the reference to the actors that are required to manage them are recorded and referenced. Source: *CSM RA*
high-integrity	Integrity Level greater than basic integrity, and that has been developed using rigorous processes that provide assurance of the system's safety integrity.
independent safety assessment	A process to determine whether the system/product meets the specified safety requirements and to form a judgement as to whether the system/product is fit for its intended purpose in relation to safety.
Independent Safety Assessor (ISA)	A person or organisation that carries out an Independent Safety Assessment.

infrastructure manager (IM)	Has the meaning given to it in the Railways and Other Guided Transport Systems (Safety) Regulations 2006 (as amended), but is limited to those infrastructure managers who hold a safety authorisation issued in respect of the mainline railway. Source: *ROGS*
interface control document	A document which defines an interface between two or more systems.
International Council on Systems Engineering (INCOSE)	A not-for-profit membership organisation founded to develop and disseminate principles and practices that enable the realization of successful systems.
key safety function	A function whose correct behaviour is relied upon to avoid one or more hazards.
lifecycle concept	A high-level description of how a system will be operated, maintained, installed, integrated with other systems including its initial placing into service and subsequent disposal.
National Technical Specification Notice (NTSN)	Document published by the Secretary of State pursuant to regulation 3B of the Railways (Interoperability) Regulations 2011 (as amended) which sets out the standards, technical specifications and technical rules in use in the United Kingdom as amended or varied from time to time. These may be standards to be complied with in relation to the design, construction, placing in service, upgrading, renewal, operation and maintenance of the parts of the rail system. For the purposes of these Regulations, the essential requirements for a project subsystem conforms with applicable National Technical Specification Notices and National Technical Rules. Source: *RIR*
performance level (PL)	No definition.
Poste de Gestation des Signalisations Temporaires (GEST)	A proprietary terminal which provides an interface between signallers and radio block centre on Ansaldo-STS ERTMS equipment.
proposer	One of the following: a) a railway undertaking or an infrastructure manager b) an entity in charge of maintenance c) a contracting entity or a manufacturer which invites: i) an approved body or a designated body to apply the UK verification assessment procedure in accordance with regulation 17 of and Schedule 4 to the Railways (Interoperability) Regulations 2011; or ii) an EU notified body to apply the EC verification procedure in accordance with

	Directive 2008/57/EC or a designated body according to Article 17(3) of that directive. Source: *CSM RA*
Radio Block Centre (RBC)	A centralised computer unit working with an interlocking(s) to establish and control safe train separation. Receives location information via radio from trains and sends movement authorities via radio to trains.
Rail Accident Investigation Branch (RAIB)	No definition.
Rail Safety and Standards Board (RSSB)	No definition.
railway undertaking (RU)	Has the meaning given to the term 'transport undertaking' in the Railways and Other Guided Transport Systems (Safety) Regulations 2006 as amended, but is limited to any private or public undertaking the principal business of which is to provide rail transport services for goods and/or passengers, with a requirement that the undertaking must ensure traction. Source*: ROGS*
Reliability, Availability and Maintainability(RAM)	No definition.
Reliability, Availability, Maintainability, Safety (RAMS)	No definition.
risk	The combination of the likelihood of occurrence of harm and the severity of that harm (specifically defined in CSM RA regulation as: the frequency of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm).
safe function	Function whose sole purpose is to ensure safety. Source: *BS EN 50126-1:2017*
safety assurance strategy	A document defining the approach to assuring the safety of a safety-related, software-intensive system and explaining how that approach meets the requirements of this standard.
safety integrity	The ability of a system to achieve its required safety function under all the stated conditions within a stated operational environment and within a stated period of time. Source: *BS EN 50129:2003*
Safety Integrity Level (SIL)	A number which indicates the required degree of confidence that a system will meet its specified safety function. *Source: BS EN 50129:2003*
safety risk	Risk related to human health or to the environment.

Safety-related Application Condition (SRAC)	A condition which needs to be met in order for a system to be safely operated.
safety-related	Carries responsibility for safety. Note: A function, component, product, system or procedure is called safety-related if at least one of its properties is used in the safety argument for the system in which it is applied. These properties can be of functional or non-functional nature. The requirements attributed to the function can be systematic or random integrity requirements. Source: *BS EN 50126-1:2017*
solid state interlockings (SSI)	No definition.
subsystem integration	Getting the subsystems of a system to work with each other and/or with simulators of subsystems.
System Flight Server (SFS)	No definition.
system integration	Getting a system to work with external systems and/or simulators of these systems.
temporary speed restriction (TSR)	A speed, less than the permissible speed, applied for a pre-planned period not normally exceeding six months.
Unified Modelling Language (UML)	No definition.
validation	Confirmation, through the provision of objective evidence, whether an item (for example, process, documentation, software or application) fits the user needs. In design and development, validation concerns the process of examining an item to determine conformity with user needs. Validation is normally performed during the final stage of development, under defined operating conditions, although it can also be performed in earlier stages.
verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled. Verification is conducted at various life cycle phases of development, examining the system and its constituents to determine conformity to the requirements specified at the beginning of that life cycle phase.
West Coast Route Modernisation (WCRM)	No definition.

References

The Standards catalogue gives the current issue number and status of documents published by RSSB: http://www.rssb.co.uk/standards-catalogue.

RGSC 01	Railway Group Standards Code
RGSC 02	Standards Manual

Documents referenced in the text

RSSB documents

GEGN8646	Guidance on the Common Safety Method for Risk Evaluation and Assessment
RIS-1530-PLT	Rail Industry Standard for Technical Requirements for On-Track Plant and Their Associated Equipment and Trolleys
RIS-1702-PLT	Rail Industry Standard for the Design of On-Track Machines in Travelling and Working Modes
RIS-2750-RST	Supplier Assurance
RSSB, 2021	A400M disaster 2015, RSSB, 2021 [Online]. Available from www.rssb.co.uk [Accessed 7 Jan 2022]
T1047 RSSB (2014)	Industry guidance on the use of software-based systems for railway applications

Other references

BS EN 50126-1:2017	Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), Part 1: Generic RAMS Process
BS EN 50126-2:2017	Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), Part 2: Systems Approach to Safety
BS EN 50128:2011	Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems
BS EN 50129:2018	Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling
BS EN 50155:2021	Railway applications - rolling stock - electronic equipment
BS EN 50159:2010	Railway applications, communication, signalling and processing systems - safety-related communication in transmission systems
BS EN 50657:2017	Railway applications - rolling stock applications - software on board rolling stock
BS EN 61508-1:2010	Functional safety of electrical/ electronic/programmable electronic safety-related systems - Part 1: General requirements

BS EN ISO 13849-1:2015	Safety of machinery. Safety-related parts of control systems - General principles for design
BS EN ISO 13849-2:2012	Safety of machinery. Safety-related parts of control systems - Validation
BS EN ISO 9001:2015	Quality Management Systems. Requirements
BS ISO 10007:2017	Quality management - Guidelines for configuration management
CAA report (2015)	NATS System Failure 12 December 2014 - Final report, CAA, 13 May 2015
INCOSE zGuide Z8	System Architecture
NR/SE/001	Network Rail Systems Engineering Handbook, 30 September 2020
ORR report (2020)	Report following railway power disruption on 9th August 2019, Office of Rail and Road, 3 January 2020
prEN 50716:2021	Railway applications - Cross-functional Software Standard for Railways
RAIB report (2014)	RAIB review of the railway industry's investigation of an irregular signal sequence at Milton Keynes, 10 December 2014
RAIB report (2017)	Loss of safety critical signalling data on the Cambrian Coast line. RAIB, 20 October 2017
Regulation (EU) 2015/1136	Commission Implementing Regulation (EU) 2015/1136 of 13 July 2015 amending Implementing Regulation (EU) no 402/2013 on the common safety method for risk evaluation and assessment (CSM RA)
SI 1999/3242	Management of Health and Safety at Work Regulations 1999
SI 2006/1057	Railways and Other Guided Transport Systems (Safety) Regulations 2006
SI 2008/1597	The Supply of Machinery (Safety) Regulations 2008
SI 2011/3066	The Railways (Interoperability) Regulations 2011 (as amended by the Railways (Interoperability) (Amendment) (EU Exit) 2019 Exit Regulations)
SI 2019/345	Railways (Interoperability) (Amendment) (EU Exit) 2019 Exit Regulations
SI 2019/696	Product Safety and Metrology etc. (Amendment etc.) (EU Exit) Regulations 2019