

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

Signatures removed from electronic version

Synopsis

This document provides guidance on meeting the requirements of Railway Group Standard [GK/RT0206](#).

This Guidance Note has been produced by

Marie Marks
Standards Project Manager

Authorised by

Brian Alston
Controller, Railway Group Standards

This document is the property of Railway Safety. It shall not be reproduced in whole or in part without the written permission of the Controller, Railway Group Standards, Railway Safety.

**Published by:
Railway Safety
Evergreen House
160 Euston Road
London NW1 2DX**

Uncontrolled When Printed

This page has been left blank intentionally

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

Contents

Section	Description	Page
Part A		
A1	Issue Record	2
A2	Implementation of this document	2
A3	Responsibilities	2
A4	Health and safety responsibilities	2
A5	Technical content	2
A6	Supply	2
Part B		
B1	Purpose	3
B2	Application of this document	3
B3	Definitions	3
B4	Requirements	4
References		24

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

Part A

A1 Issue Record

Issue	Date	Comments
One	April 2002	Original Document – supports GK/RT0206

This document will be updated when necessary by distribution of a complete replacement.

A2 Implementation of this document

The publication date of this document is 06 April 2002.

This document supersedes the following Railway Group documents either in whole or in part as indicated:

Railway Group document	Issue No.	Title	Sections superseded by GK/RT0206 and GK/GN0806	Date(s) as of which sections are superseded
GK/RM0501	18	Manual of Signalling Principles Standards	Part B	06 April 2002

The Signalling Principles Standards, as listed in Part A of GK/RM0501, are not superseded.

A3 Responsibilities

Railway Group Guidance Notes are non-mandatory documents providing helpful information relating to the control of hazards and often set out a suggested approach, which may be appropriate for Railway Group* Members to follow.

* The Railway Group comprises Railtrack PLC, Railway Safety, and the train and station operators who hold railway safety cases for operation on or related to infrastructure controlled by Railtrack PLC.

Railtrack PLC is known as Railtrack.

A4 Health and safety responsibilities

In issuing this document, Railway Safety makes no warranties, express or implied, that compliance with all or any document published by Railway Safety is sufficient on its own to ensure safe systems of work or operation. Each user is reminded of its own responsibilities to ensure health and safety at work and its individual duties under health and safety legislation.

A5 Technical Content

The technical content of this document has been approved by:

Jeff Allan, Principal S&T Engineer, Railway Safety

Enquiries should be directed to Railway Safety – Tel: 020 7904 7518

A6 Supply

Controlled and uncontrolled copies of this document may be obtained from the Industry Safety Liaison Dept, Railway Safety, Evergreen House, 160 Euston Road, London NW1 2DX.

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

Part B

B1 Purpose

To provide guidance on meeting the requirements of Railway Group Standard [GK/RT0206](#).

B2 Application of this document

B2.1 To whom the guidance applies

This document contains guidance that is applicable to the duty holders of the infrastructure controller category of Railway Safety Case. However, train and station operators may also wish to consider the applicability of this document to their systems.

Where a **system** is owned by more than one Railway Group member (eg for track-train systems), the development of the safety requirements and issues relating to the life management of those systems may be best dealt with by the creation of a systems authority. [GE/RT8049](#) sets out the process by which a systems authority is created and managed.

B2.2 Documents supported by this Guidance Note

[GK/RT0206](#) - Signalling and Operational Telecommunications Systems: Safety Requirements is supported by this document.

[GK/RT0206](#) defines the general safety requirements for signalling and operational telecommunications systems. It does not address the processes by which requirements are developed, nor issues relating to the ownership and life management of such systems. It is, however, important that the ownership of, and responsibility for, a **system** is clearly defined during the development of the **system** requirements.

B3 Definitions

Functional requirement

A requirement that defines what the **system** must do, and the desired behaviour in terms of an effect produced, or an action or service to be performed.

Interface requirement

A requirement that defines the conditions of interaction between the **system** and other equipment, infrastructure or trains [including interactions with other railways, eg London Underground Ltd (LUL)], and people.

Non-functional requirement

A requirement that defines a property, characteristic or constraint of the **system** (or a part of the **system**), other than a functional or interface requirement.

Signalling and operational telecommunication systems and equipment

Systems and equipment within the scope of this standard and that are used for:

- a) authorising and safeguarding the movement of trains (eg interlockings, train protection systems, train detection equipment, signals, point operating mechanisms, level crossings, cables, cable routes, apparatus cases)
- b) safety-related communications purposes in the direct operation of the railway (eg lineside telephone systems, train radio systems, signalling data communications systems)
- c) providing protection and/or warnings for trackside personnel, where such systems and equipment form part of the whole signalling **system**.

Definitions for terms such as **reliability**, **availability**, maintainability and safety-related are contained in European Standards EN50126 and EN50129. Other definitions are contained in [GK/RT0002](#).

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

B4 Requirements

B4.1 Defining **system** requirements

B4.1.1

System requirements shall be defined and documented for the purposes of design, testing and acceptance.

B4.1.2

The customer requirements for the **system** shall be defined and documented sufficiently for the purposes of developing the safety requirements of the **system**.

Explanation:

- a) In order to develop a **specification** for a **system** (including safety requirements), it is first necessary to define the customer requirements (also known as the operational requirements) for the **system**.
- b) The **system** requirements represent the developer's **specification** for the **system**, in response to the customer requirements. **System** requirements are generally developed iteratively and in increasing detail, until they are sufficient for design purposes.

Guidance:

- c) In defining the customer requirements, account should be taken of:
 - 1) the purpose of the **system**
 - 2) the concept of operation of the **system**
 - 3) the principal functions that the customer requires the **system** to perform, and the needs of other stakeholders
 - 4) how well each function must be performed (see section B4.3)
 - 5) modes of operation (the normal and degraded modes in which the customer wishes to be able to operate the **system**) – see (f) below
 - 6) operational parameters which the **system** is required to meet or support under both normal and abnormal (emergency) conditions (eg frequency of demands on the **system**, traffic levels, response times)
 - 7) the scope of the **system** (both geographically and operationally)
 - 8) other equipment with which the **system** is required to interface or operate
 - 9) the people who will use, operate and maintain the **system**.
- d) The **system** requirements are developed in response to the customer requirements. They include both safety-related and non-safety-related requirements, although these should be listed as two separate sets of requirements wherever possible. **System** requirements should be understood to include:
 - 1) Functional requirements:
 - i) the primary functions that the **system** is required to perform
 - ii) the defined modes of operation and conditions for transition between them (for both normal and degraded modes) - see (f) below

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

iii) **system** behaviour under failure conditions, and recovery from failure.

2) Non-functional requirements:

- i) RAMS requirements (**reliability, availability, maintainability, safety targets and safety integrity levels**)
- ii) requirements relevant to the management of the **system** throughout its life cycle (construction, commissioning, maintenance, modification and decommissioning)
- iii) compatibility requirements relevant to the environment in which the **system** will operate (including both the railway-specific, and the general, environment)
- iv) requirements for the control of general health and safety risks associated with the existence and operation of the **system**.

3) Boundaries and interface requirements:

- i) boundaries of the **system**
- ii) interfaces with other equipment and entities
- iii) interfaces with people (users and maintainers).

These requirements are amplified in sections B4.2 – B4.10.

e) The development of the **system** requirements should also include consideration of:

- 1) the proposed **system** architecture, the principal hardware and software sub-systems that comprise the **system**, and the interfaces between them
- 2) hardware and software tools which are required in order to support the safe design, testing, operation, maintenance and modification of the **system**
- 3) constraints on the choice of technology, whether imposed by the customer requirements or the **availability** of the technology
- 4) risks associated with unproven technology and the use of existing technology in a novel application
- 5) the required service life of the **system**
- 6) foreseeable upgrades and modifications of the **system** during its service life
- 7) mandatory requirements with which the **system** is required to comply (eg legislation and Railway Group Standards).

f) The permitted modes of operation associated with the use of the **system** should be defined as a part of the **system** requirements. The term 'modes of operation' refers to the various modes in which users operate the **system**, and it includes both normal and degraded modes (see section B4.4).

The permitted transitions between the various modes of operation (both normal and degraded) should be defined, together with the conditions that need to be fulfilled before those transitions can be made. The modes and conditions determine in part the procedural requirements for the operation of

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

the **system** (see section B4.10), and may also determine some features of the **system** design.

For **system** design purposes, it may also be appropriate to define **system** modes. However, these will not necessarily correspond to operational modes, and in some cases may not have any real meaning for a user of the **system**.

- g) The requirements should address the concept of 'fitness for purpose'. This term includes not only **reliability** and **availability** (see section B4.3), but also maintainability (see section B4.5) and the concept of the **system** being suitable for use. The design and construction should be such that the **system** is user-friendly and ergonomically appropriate (see section B4.7). By so doing, its full and proper use will be promoted. Conversely, a **system** which is not user-friendly or ergonomically appropriate may result in it being used improperly, which could in turn affect safety.
- h) Requirements should be partitioned between the various sub-systems that comprise the **system** (an activity known as 'requirements allocation'). This is relevant to both normal and degraded modes of operation. For all modes, there should be clarity regarding the contribution made by the **system** to the achievement of safety, and that contributed by the users and the procedures they are required to apply (see sections B4.7 and B4.10).

In some cases, individual **system** requirements cannot be directly allocated to particular sub-systems. Instead, sub-systems requirements have to be derived from the overall **system** requirements, although they are not the same as the **system** requirements. In particular, sub-**system** requirements will include their interactions with each other.

- i) Customer and **system** requirements should be stated so that they:
 - 1) are readily understandable
 - 2) do not contain any errors of fact
 - 3) can be met within the constraints imposed by factors such as legislation, natural physical constraints, and the available technology
 - 4) are expressed in terms of 'what' has to be achieved, not how to do it (although requirements which lead directly to detailed design work may contain 'how to' statements)
 - 5) contain sufficient information to enable the requirement to be met as intended
 - 6) can be interpreted in only one way (ie there is no ambiguity in the meaning)
 - 7) are specified only once (ie there is no repetition of requirements)
 - 8) are self-consistent (ie no conflicts or inconsistencies within any one requirement)
 - 9) are not in conflict with other requirements
 - 10) relate properly to other requirements so that the set as a whole is consistent and integrated
 - 11) are capable of being verified and validated during the design, construction and testing phases

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

- 12) are structured in a manner that facilitates subsequent **system** change and development without introducing inconsistencies or contradictions into the requirements.
- j) Requirements should be traceable to, and demonstrably compliant with, the core safety requirements specified in other higher level standards, including mandated European Standards, Her Majesty's Railway Inspectorate Principles and Guidance, and Railway Group Standards.
- k) There should be clarity and agreement about who is responsible for compliance with the requirements. This is particularly important where ownership of the **system** is shared between Railway Group members.
- l) Assumptions and constraints associated with the **system** requirements should be identified and recorded, as they may have relevance to the subsequent design, operation, maintenance or modification of the **system**.
- m) European Standard EN50126 provides further guidance on the development of **system** requirements, under the life cycle phases of 'Concept', '**system** Definition and Application Conditions', 'Risk Analysis', '**system** Requirements' and 'Apportionment of **system** Requirements'.

B4.2 Safety performance

The totality of risk associated with the operation of the **system** shall be:

- a) tolerable
- b) as low as reasonably practicable (ALARP)
- c) no worse than for comparable existing systems.

Explanation:

- a) This clause addresses the overall requirement that the risk associated with the use of the **system** is properly controlled in accordance with legal requirements and good practice.

Guidance:

- b) The 'totality of risk' should take into account:
 - 1) the extent to which the **system** controls the risks that are within its purpose and scope
 - 2) the risks associated with the application of the procedures and rules relevant to the operation of the **system**
 - 3) the risk of human error in the operation of the **system**
 - 4) the risks associated with any malfunction of the **system**
 - 5) the risks associated with interactions with other systems
 - 6) any transfer of risk (to/from another part of the railway) and any new hazards arising from the introduction of the **system** (see also (h) below).
- c) There should be clarity as to what hazards are controlled by the **system**, and whether the control of each hazard is achieved entirely by the **system**, or is dependent upon other control measures outside the **system**. So far as is possible, the contribution made by the **system** in controlling each hazard should be quantified.

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

- d) Proper application of the ALARP principle may necessitate the use of a monetary value of preventing a fatality (VPF) as a means of informing decisions. VPF figures applicable to the rail industry are published in the annual Railway Group Safety Plan. Separate figures are provided for single and multi-fatality accidents. Railtrack's Railway Safety Case also contains limits for tolerable levels of risk on the railway. In some cases the use of a higher VPF than the published figures may be appropriate.
- e) The existence of industry targets may be relevant when designing a **system**. The Railway Group Safety Plan, published annually by Railway Safety on behalf of the rail industry, sets out targets for safety improvements.
- f) The requirement for risk to be 'no worse than for comparable systems' should be interpreted as meaning that the overall level of risk should be no worse than either that of:
 - 1) the **system** it replaces, or
 - 2) comparable systems in service elsewhere, including any in use in other countries.
- g) In some circumstances it may be necessary to exceed the requirements of the ALARP principle. Where a proposed risk reduction measure does not meet the ALARP criteria, it may still be appropriate to apply that measure if:
 - 1) the measure provides an improvement in safety, and
 - 2) the cost of providing that measure is small compared with the overall cost of the project of which it is a part.
- h) Special attention should be given to the identification and mitigation of hazards arising from the change from an existing **system** to one that is significantly different in terms of its functionality. In particular, the risks associated with 'lost benefits' should be considered. These are safety benefits which were associated with the existing **system** but which are not a feature of the new **system** (although other new benefits may arise which make the new **system** an attractive proposition).

B4.3 Reliability and availability

The **reliability** and **availability** of the **system** to perform its intended functions shall be sufficient to ensure that the required safety performance can be achieved.

Explanation:

- a) The **reliability** and **availability** of the **system** determine, in some measure, the overall safety of the railway (depending upon the specific application under consideration). Risks may arise in three key areas:
 - 1) the direct safety risks posed by a failure of the **system** to perform its safety functions
 - 2) the safety risks associated with the operation of the railway under conditions of total and partial **system** failure (this includes both failures where the **system** enters/remains in a safe state and those where it does not)
 - 3) the safety risks associated with the restoration of the **system** to full functionality after a failure has been diagnosed and corrected.

These are addressed further in section B4.4.

- b) Because of the risks outlined above, emphasis needs to be placed not only on designs that provide protection in the event of failure (see section B4.4), but also on designing to preventing failure occurring, ie designing systems so as to have high **reliability** and **availability**.

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

Guidance:

c) When specifying **reliability** and **availability**, it is important that the definitions of the terms adopted are appropriate and unambiguous. In particular, it will be necessary to clarify:

- 1) whether the **reliability** (and therefore **availability**) relates to the continuous operation of the **system**, or to failure to respond correctly when a valid demand is made on the **system** ('failure on demand')
- 2) whether the **availability** relates to the total time for which the **system** is required to be in service and fully meeting its functional and non-functional requirements, or whether the measure of **availability** includes operation in degraded modes.

d) When specifying requirements, it is important to distinguish between operational and logistical **reliability**.

Operational **reliability** is the **reliability** as perceived by the user, and is a measure of the frequency with which the **system** experiences failures that affect the functionality of the **system**.

Logistical **reliability** is a measure of the frequency with which the **system** experiences component or sub-**system** failures, even though such failures may be invisible to the user because the **system** is designed with a measure of fault tolerance to improve its **availability**.

e) Designing for reliable performance includes consideration of design features such as:

- 1) choice of sub-systems and components with suitable life expectancy and appropriately low failure rates, and operation of those components well within the limits of their performance (to reduce stress)
- 2) use of redundancy within the **system** to ensure adequate operational **reliability** and fault tolerance. Redundant sub-systems may operate concurrently (ie always operational) or in some form of standby mode (automatic or manual), depending upon requirements for continuity of operation
- 3) **reliability** required of supporting sub-systems (eg power supplies) and of other systems, railway infrastructure and trains with which the **system** interfaces or interacts, where failure of these could adversely affect the **reliability** of the **system**.

f) Where some parts of the total **system** are not owned by Railway Group members, as is the case for instance with leased lines, then the **reliability** and **availability** of those elements should be specified in the agreement with the owner or service provider.

g) When considering the **availability** requirements for the **system**, it may be necessary to make trade-offs between **reliability** and maintainability to achieve the desired level of **availability**.

h) The **specification** of **reliability** and **availability** requirements necessitates not only that consideration be given to the design of the **system**, but also to the arrangements for the maintenance of the **system** (see section B4.5 and also [GK/RT0210](#)).

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

B4.4 Failures and degraded modes of operation

B4.4.1

The **system** shall be designed so that no credible failure could occur which could result in an intolerable level of risk.

B4.4.2

So far as is reasonably practicable, in the event of a failure the **system** shall behave in a controlled, predictable and pre-determined manner.

B4.4.3

So far as is reasonably practicable, degraded modes of operation shall be provided in order to minimise the need, under failure conditions, to rely upon human action for safety-critical tasks that are performed by the **system** itself in normal operation.

B4.4.4

The design of the **system** shall facilitate safe recovery from credible failure conditions and degraded modes.

Explanation:

- a) Design defences against unsafe failures require both the avoidance of failures wherever possible, and also controlled degradation of **system** performance to mitigate the effects of failures. This includes, where possible, the provision of degraded modes of operation so as to avoid total failure (in which condition the **system** is not available for use at all).

Guidance:

- b) It should be noted that some of the requirements (B4.4.2 and B4.4.3) in this section are subject to the test of reasonable practicability. If it is reasonably practicable to specify and procure systems and equipment which meet these requirements, then that is what has to be done. Where the costs of developing and procuring bespoke products that meet these requirements significantly outweigh the safety benefits, then the use of alternative commercial off the shelf (COTS) products that do not meet the 'reasonably practicable' requirements is justifiable.
- c) Failures for consideration include (but are not limited to):
- 1) single point failures (susceptibility to which should be avoided where possible)
 - 2) common cause/mode failures (ie failures that are the result of an event that causes coincident faults in two or more parts of a **system**, either one of which would be tolerable but which together give rise to an unacceptable level of risk)
 - 3) hidden failures which, although not presenting a hazard in themselves, when in combination with other subsequent failures, could lead to an unacceptable level of risk
 - 4) failures that are associated with catastrophic levels of risk
 - 5) failures of interfaces between systems or sub-systems
 - 6) failures of other systems, railway infrastructure and trainborne equipment that cause failure or malfunction of the **system**. This also includes systems and sub-systems that are not part of the railway, eg leased lines.

See Annexes B, C, D and E of EN50129 for more information on failure modes.

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

The 'Yellow Book' (Engineering Safety Management), EN50126 and EN50129 contain guidance on processes for identifying and addressing **system** failures and associated hazards.

- d) Both random and systematic failures need to be considered when specifying and designing the **system**. Safety Integrity Levels should be used as a measure of the confidence required of a **system** that it is capable of operating safely without undue propensity for random (hardware) or systematic (design deficiency) failures. EN50129 provides further information on these topics.
- e) Clause B4.4.1 requires that the design of the **system** avoids credible failures that could give rise to intolerable levels of risk. Therefore both probability of failure and its possible consequences need to be considered. However, the frequency with which some very low probability catastrophic events occur may be difficult to estimate. In these circumstances, design effort should be focussed on preventing the failure (or combination of failures) that could lead to the catastrophic outcome (ie reducing the probability of failure to the point where it is not credible).
- f) The 'time at risk' between a failure occurring and action being taken to protect the failure (whether by the **system** or by people) needs to be taken into account when specifying the **system** requirements. This will involve consideration of the speed and dependability with which the failure is detected and protection is applied.
- g) It is legitimate, when assessing whether the level of risk associated with a particular failure is acceptably low, to consider the extent to which the risk is controlled by measures (both technical and procedural) that are outside the **system**. However, so far as is reasonably practicable, one or more of the following strategies should be incorporated into the design of the **system** to cater for the various failures (in descending order of preference):
 - 1) full fault tolerance (the **system** continues to operate without impairment of safety or functionality)
 - 2) limited fault tolerance (the **system** enters a degraded mode whereby some functionality is preserved, possibly with some impairment of safety)
 - 3) self-protection of failures (the **system** enters a known safe state, but with a significant loss of functionality, and with possible exposure to secondary safety risks)
 - 4) self-revelation of failures (the occurrence of the fault is indicated to the operator, but without providing any other protection against safety-related consequences).

In all cases, consideration should be given to the means by which the fault is indicated to users or maintainers.

In some designs, functionality may be retained by automatic reconfiguration of the **system**. The risks associated with this should be considered during the **system** design.

- h) Where protection is to be provided by ensuring that, in the event of a failure, the **system** automatically enters a known safe state, one or more of the following design philosophies should be adopted:
 - 1) the use of components that are of fail-safe design, incorporated into a fail-safe application design (inherent fail safety)
 - 2) the use of duplicated or triplicated sub-systems (composite fail safety using hardware)

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

- 3) the use of two or more diverse sets of software and data within a single channel **system** (composite fail safety using software)
 - 4) self-checking within a single channel **system**, with rapid detection and shutdown in the event of a failure (reactive fail safety).
- i) The degraded modes of operation should be arranged in a hierarchy, so that modes in which safety is ensured principally by the **system** are used in preference to those that depend principally upon human action.

So far as is reasonably practicable, the degradation of the **system** from normal modes through its degraded modes should be designed so as to be 'graceful', retaining essential functionality as much as possible.

The **system** should be designed so that when it moves into a degraded mode the change in mode of operation is recognisable by (or indicated to) users.

- j) The design of the **system** should facilitate easy, error-free recovery from failure conditions back to normal operation. The means of recovery may be automatic (not involving operators or maintainers), or semi-automatic or manual (involving operators or maintainers).

It may be appropriate to incorporate **system** self-checks so as to avoid operator or maintainer errors when undertaking the recovery process, where such errors could lead to impairment of safety.

- k) In addition to the design philosophy adopted to cope with failures, the following safety-related factors should be considered when planning the overall **system** architecture and design:
- 1) the risks associated with the use of complex systems and architectures, and in particular the consequential difficulties of both achieving a safe design solution and demonstrating that it meets requirements relevant to safety
 - 2) segregation of safety-related sub-systems from non safety-related sub-systems, with well defined interfaces between them (see section B4.6)
 - 3) physical design of sub-systems and layout of components in such a way as to minimise the risk of safety-related hardware failure (eg galvanic action, short/open circuits, overheating, cross-talk, components going out of tolerance).

B4.5 Design for whole **system** life cycle

The **system** shall be designed so as to ensure that it can be constructed, installed and tested, and subsequently operated, maintained, modified and decommissioned safely.

Explanation:

- a) This requirement addresses the need for designers to design for continuing safety throughout the **system** life cycle. This involves consideration of safety issues affecting trains, the public and personnel who use or work on the **system**.
- b) Guidance on the requirements for designs to ensure that the **system** can be operated safely by users is given under sections B4.7 and B4.10.

Guidance:

- c) When planning the **system** architecture and selecting hardware and software, maintainability should be considered, including:

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

- 1) the provision of safe access by maintenance personnel to carry out their work for maintenance, fault-finding and repair purposes
 - 2) the ease with which the functionality and general health of the **system** can be tested when it is in service, and adjustments made when required
 - 3) the ease with which the **system** (or individual sub-systems) can be taken out of service for investigation/repair, including both taking equipment off-line and the physical removal of sub-systems/components
 - 4) arrangements for the subsequent safe restoration of the **system** to service, and for status indications to be provided to users and maintainers during the restoration process
 - 5) arrangements for preventing safety-related errors when replacing sub-systems and components (eg by use of pin coding or electronic coding)
 - 6) the ease with which modifications can be safely made to the **system** during its service life.
 - 7) The competencies required for maintenance of the **system**.
- d) The provision of maintenance and fault-finding aids should be considered, including:
- 1) monitoring equipment and status indication sub-systems to aid maintenance and to facilitate early detection of impending failures and failures in fault-tolerant systems (so far as possible, these should be non-invasive)
 - 2) diagnostic tools, data logging equipment and fault indications to facilitate failure investigation.

However, the benefits of including such aids should be weighed against the complexity added to the **system** and any resultant reduction in **system reliability** that may occur.

- e) The long-term supportability of the **system** should be considered when selecting hardware and software, including:
- 1) the likelihood and timescales of obsolescence, and the problems that would consequentially arise
 - 2) the ability and willingness of the supplier(s) to support the **system**, sub-systems and components throughout the service life, in terms of:
 - i) provision of maintenance documentation
 - ii) spares **availability**
 - iii) interchangeability of different suppliers' components
 - iv) specialist expertise to advise on problems
 - v) support and information to facilitate modification or upgrading.
- f) Maintenance arrangements can affect **reliability**, **availability** and safety. Aspects of maintenance that are relevant to this include:

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

- 1) whether or not a preventative maintenance regime is to be adopted, and if so what specific failures it is intended to prevent
- 2) strategies for the midlife renewal/replacement of components
- 3) strategies for responding to failures and effecting repairs.

B4.6 Interfaces with other equipment

The **system** shall be designed so that, where it has an interface with other equipment, the safe operation of the **system** and of the other equipment is not jeopardised by the form or functionality of the interface.

Explanation:

- a) This section addresses the requirements for interfaces between the **system** and other equipment, infrastructure and trains. It does not include unplanned interactions with other equipment, infrastructure and trains (these are addressed in section B4.8).

Guidance:

- b) Interfaces between the **system** and other equipment, infrastructure, trains and trainborne systems need careful consideration, because:
 - 1) the equipment on the other side of the interface may already exist. The interface requirements for the **system** would therefore have to take this into account, both at the functional level (what the interface does) and at the physical level (the form of the interface)
 - 2) the nature of the interface may be such that the safe and reliable transmission of information/data across the interface is difficult to achieve in the railway environment
 - 3) the dependencies between systems may be complex. Dependencies to be considered include both those between systems/equipment which have a formal interface, and those between systems/equipment where there is no formal interface, but nevertheless correct operation of one is dependent upon the behaviour of the other.
- c) It may therefore be necessary to define the interface requirements in detail at an early stage in the development of the **system specification**. This is particularly important when the systems, equipment or infrastructure on either side of the interface are under the control of different Railway Group members. In many cases such interfaces will be the subject of Railway Group Standards.
- d) Interface requirements should adequately control:
 - 1) the transfer of risk in either direction across the interface
 - 2) the risks associated with failure of the interface
 - 3) the creation of risk by an inappropriate interface (ie non-intentional effects of the interface).
- e) Interfaces should be specified and designed so as to ensure safe and reliable operation under all reasonably foreseeable circumstances. This may include the use of adequate margins (eg timings, signal strengths) or the use of techniques (eg error-tolerant data coding techniques).

B4.7 Interfaces with people

Interfaces between the **system** and operators shall be designed so as to minimise the risk of operator error giving rise to an unsafe situation.

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

Explanation:

- a) This requirement addresses the need for a human factors/ergonomics approach to the interfaces between systems and people.
- b) The term 'operators' includes not only those who operate and use the **system** (eg drivers, signallers), but also others who work with the **system** in any capacity, eg maintainers. For some systems, it may also include passengers and the public.

Guidance:

- c) During the development of the **system** requirements, the allocation of functional requirements should include the allocation of functions between the **system** and the personnel who use/operate/maintain the **system**. This allocation should be based on their respective capabilities and limitations, not on the simplistic assignment to people of those tasks that cannot be automated. Factors for consideration when allocating functions between the **system** and people include:
 - 1) legislative or Railway Group Standard requirements for functions to be performed by the **system**
 - 2) the safety criticality of the activity and the potential for catastrophic consequences if it is performed incorrectly
 - 3) the (generally) superior ability of people to make decisions and respond flexibly in circumstances where the information leading to the decision is complex, incomplete, or imprecise
 - 4) the workload on users, under both normal and exceptional circumstances. This includes not only the workload associated with use of the **system** itself, but also the total workload on users (eg where an operator may be controlling several systems)
 - 5) the difficulties that users may have in acting correctly in circumstances that occur only very rarely, including:
 - i) the vigilance required to monitor the actions performed by the **system** in case it malfunctions
 - ii) the risk of non-recognition of a malfunction because of its rarity
 - iii) the likelihood of a user making an error under **system** failure or emergency conditions (when the **system** is not providing the safety protection that it normally does), and the user is having to perform actions in place of the functions normally carried out by the **system**
 - iv) the stress placed on users in these circumstances.
 - 6) personnel issues such as job design and job satisfaction, organisation management, numbers of users/operators required, security issues, trainability and skill levels (particularly where the activities performed by users are significantly different from those with previous systems)
 - 7) the **reliability** and repetitiveness with which the activity needs to be performed (systems are generally better at this than people).
 - 8) the technological feasibility of automating the functions (ie allocating them to the **system**)
 - 9) public perception of the acceptability of activities being automated or performed by people

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

- 10) relative economics of people-based and **system**-based solutions.
- d) Where a function is to be performed by users (usually in conjunction with the **system**), then consideration should be given to:
- 1) security of access, so that only authorised personnel can perform the function
 - 2) how the user will be aware of the need for the function to be performed (what cues are provided by the **system**)
 - 3) the cues and information provided to the user to promote a correct action or response
 - 4) how the **system** will respond in the event of a user error, for instance by:
 - i) prevention of an unsafe action (with or without appropriate feedback to alert the user to the error)
 - ii) warning (but not prevention) of an unsafe action
 - iii) self-correction by the **system** (doing what the user intended, instead of what was actually commanded)
 - iv) provision of context-sensitive help facilities.
 - 5) the ergonomic design of the interface so that its operation by the user is as intuitive as possible, making it 'natural' to perform the correct actions.
- e) Other factors for consideration in the design of user interfaces include:
- 1) consistency of form, if a user might work at several interfaces or locations
 - 2) clarity about **system** boundaries and areas of control.
 - 3) visibility and legibility of interface control devices and indications (choice of text, symbols, colours etc)
 - 4) the environmental conditions under which the interface will be used (lighting conditions, background noise etc)
 - 5) provision of a defined and logical hierarchy for the presentation of audible/visual warnings and alarms, optimised for human responses to such warnings and for the importance/urgency of the actions to be taken
 - 6) time duration for which audible/visual information is presented
 - 7) risks associated with the provision of configurable displays.
- f) Consideration should be given to the information that the **system** needs to provide to users for each of the following:
- 1) **system** start-up/initialisation/commencement of use
 - 2) normal operation
 - 3) responses to abnormal/failure/emergency conditions
 - 4) operation and supervision under degraded modes of operation and total failure conditions

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

- 5) safe restoration to normal operation after a failure or operation in a degraded mode
- 6) **system** shutdown.

Account should be taken not only of what information is required, but also the accuracy and dependability of the information.

- g) Consideration should be given to interfaces with non-railway personnel, taking into account issues such as the lack of training or special skills, the infrequent use of the interface, etc. Such interfaces include:
 - 1) user worked interfaces (eg telephones, level crossings)
 - 2) interfaces used by emergency services
 - 3) information systems for the public and others.

B4.8 Environmental compatibility

B4.8.1

The **system** shall be designed so as to ensure that it is capable of functioning correctly within its operational environment.

B4.8.2

The systems shall be designed so as to ensure that it does not jeopardise the safe operation of neighbouring equipment and systems.

Explanation:

- a) This requirement addresses the need for the **system** to be compatible with its operational environment, involving:
 - 1) protection of the **system** against undesirable safety-related interactions with, and interference from, the rest of the railway, neighbours and the general environment
 - 2) avoiding the export of risk to other non-railway enterprises and activities.

Guidance:

- b) Environmental compatibility of the **system** should be considered in relation to:
 - 1) trains
 - 2) other railway signalling and telecommunications equipment
 - 3) other railway infrastructure equipment
 - 4) railway neighbours
 - 5) the general environment.
- c) Environmental factors to which the **system** could be subjected include:
 - 1) mechanical stress (vibration, shock, strain, explosion)
 - 2) climatic conditions (temperature, humidity, flooding, sunlight)
 - 3) chemical effects (corrosion, dust, sea-spray, fumes)
 - 4) electrical effects (lightning, electromagnetic interference, galvanic action)

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

Both normal conditions and abnormal (reasonably foreseeable extreme) conditions should be considered.

- d) The effects of the **system** on the rest of the railway, the non-railway environment and neighbours should also be considered, including:
 - 1) impairment of the mechanical integrity of other railway infrastructure (eg by the physical location or method of fixing of elements of the **system** at the trackside)
 - 2) inductive and conductive electrical interference with other infrastructure, or with trainborne and non-railway equipment.
- e) Consideration should be given to protection against:
 - 1) inadvertent interference with the correct operation of the **system** by unauthorised persons
 - 2) malicious interference and vandalism.
- f) European standards EN50121, EN50125 (part 3) and EN50129 (Annexes B (4) and D) are relevant to this topic.

B4.9 General health and safety risks

The **system** shall be designed so that the general risks to the health and safety of persons working on the railway, the public and the railway's neighbours are as low as reasonably practicable.

Explanation:

- a) The design of the **system** should take into account not only the safety-related purpose(s) for which it is provided, but also the general health and safety risks that the existence of the **system** may present to railway personnel and to others.

Guidance:

- b) When designing the **system**, potential hazards should be identified, and risks controlled, in respect of:
 - 1) the occupational health and safety of personnel working on the railway
 - 2) the health and safety of railway neighbours
 - 3) the general health and safety of the public and passengers.
- c) The requirements to control occupational safety risks are, in many cases, addressed through particular safety regulations made under the Health and Safety at Work etc Act 1974. These requirements should be identified, and their relevance to the **system** design considered.
- d) Factors for consideration in respect of personnel who work on the railway include:
 - 1) chemical hazards which may be presented by the materials of which the **system** is constructed
 - 2) hazards associated with the electrical elements of the **system**
 - 3) the physical construction of the **system** (height, weight, accessibility, confined spaces, obstruction of walkways and platforms, etc)

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

- 4) fire risks arising from the materials used in, or the form of, elements of the **system** (including flammability, smoke and toxic fume emission)
 - 5) the proximity to the running lines of parts of the **system** to which railway personnel require access
 - 6) noise generated by the **system**.
- e) Consideration should also be given to the risks associated with the eventual disposal of the **system**. The **system** requirements should, so far as is achievable, minimise disposal risks.
- f) Measures that control general health and safety risks should be applied in descending order of preference as follows:
- 1) eliminate the hazard
 - 2) reduce the hazard at source
 - 3) isolate the hazard (eg by enclosure)
 - 4) control exposure to the hazard (eg reduced time exposure)
 - 5) provide personal protective equipment
 - 6) apply procedures and rules.

B4.10 Procedures and rules for **system operation**

B4.10.1

The rules and procedures associated with the safe operation of the **system** shall be developed in conjunction with the **system** requirements and the **system** design.

B4.10.2

Rules and procedures shall be defined, documented and implemented, and relevant supporting information provided for:

- a) each normal and degraded mode of operation
- b) the means of transition from one mode to another
- c) recovery from credible failure conditions.

Explanation:

- a) Most systems require the involvement of users (operators) and, to a greater or lesser extent the overall safety associated with the use of the **system** depends upon correct operation by the user. In order to control risk appropriately, it is therefore necessary to develop procedures and rules for users. This needs to be done in conjunction with the **system** requirements **specification** and design phases, rather than doing so afterwards. Only by so doing (and by consideration of the issues in section B4.7) can safety be optimised.

Guidance:

- b) Human factors analysis should be undertaken to facilitate the development of operational rules and procedures (see also section B4.7). **System** designers, **system** users and human factors experts should all be involved.
- c) The rules and procedures covered by this clause include:
 - 1) rules and procedures that are applicable on a day-to-day basis in the use of the **system**

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

- 2) associated information or data required by users in order to apply the rules. The information may be required for normal modes of operation, and for situations when the **system** is operating in a degraded mode, or has totally failed
- 3) procedures associated with the operational management of the **system**. These are not used on a daily basis, and are likely to be higher level procedures, for instance:
 - i) policies or procedures from which the rules for day-to-day operation are derived
 - ii) procedures associated with planning changes in the manner of use of the **system**.
- d) In many cases rules may already exist (eg in the Rule Book or local publications). The adequacy of these for application with the **system** should be reviewed.
- e) Rules and procedures should be written taking into account the competence of users. At one extreme these may be newly qualified personnel who are operating in a 'knowledge based' manner, where they are heavily dependent upon the rules and apply them exactly as trained to do. At the other extreme they may be experienced people operating in a 'skill based' manner, where they have fully assimilated the rules and make little reference to the documentation except in very unusual circumstances.
- f) The procedures and rules should take into account:
 - 1) any operational constraints that need to be imposed as a consequence of the design of the **system** and that cannot be enforced by any other means
 - 2) any assumptions associated with the design of the **system** that are relevant to the manner of use.
- g) Rules for day-to-day use of the **system** should address:
 - 1) **system** access (arrangements to facilitate access by authorised users)
 - 2) **system** start-up/initialisation/commencement of use
 - 3) Routine operation
 - 4) Actions in the event of failure/emergency conditions, and conditions of abnormal loading/usage of the **system**, including:
 - ii) recognition of the condition
 - iii) application of measures to ensure safety
 - iv) stabilising and controlling the situation/**system**
 - v) operation of the **system**, or the application of alternative arrangements, under conditions of partial or total failure
 - vi) safe recovery to normal operation.
 - 5) **system** shutdown/termination of use/taking out of service (eg for maintenance purposes)
 - 6) specific precautions to ensure the safety of personnel engaged in the operation, use and maintenance of the **system**

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

- h) Rules should be formulated and presented to the user (whether in the form of documents, or by means of signs/labels, or by 'help' utilities within computer systems) in a manner which minimises the risk of misapplication. Rules should be:
- 1) unambiguous and precise
 - 2) user-friendly (written with the user in mind)
 - 3) clear as to the context/conditions in which they are to be applied
 - 4) clear as to the decision criteria to be applied, where the user has to make decisions during the application of the rules.

The normal and abnormal outcomes of the application of each rule should be made clear to the users.

- i) Particular attention should be given to the formulation of rules to be applied under exceptional circumstances, since users may have little opportunity to reinforce their assimilation of such rules, and therefore will be heavily dependent upon the documentation provided.

B4.11 Alterations to existing systems

Where existing systems are being altered, and there is no obligation bring all of the **system** into compliance with the requirements of current mandatory standards, the risks associated with a mix of old and current standards shall be assessed, recorded and controlled.

Explanation:

- a) In many situations the design involves alterations to an existing **system**. Where this is so, and legislation and Railway Group Standards apply only to parts of the **system** that are the subject of the alteration, risks may arise because of the mixing of old and new standards within the one **system**. This clause addresses such risks.
- b) The term 'standards' in this clause and in the supporting guidance includes legislation, Railway Group Standards and any other mandatory standards (eg European standards) applicable to the **system**.

Guidance:

- c) Where alterations are to be made to an existing **system**, three options are available:
- 1) upgrade the whole **system** to current standards
 - 2) tolerate a mix of standards, with the alterations being made in accordance with current standards but leaving the other parts of the **system** unaltered
 - 3) undertake the alterations in conformance with the standards of the original **system**.
- d) Where option (2) of (c) [above] is proposed, an assessment of the risks of mixing standards is required. In carrying out such an assessment, the following should be considered:
- 1) the possibility of a technical malfunction as a result of incompatibility between modified and unmodified parts of the **system**, and the seriousness of the consequences
 - 2) the potential for confusion to be caused to users (operators and maintainers), under normal, degraded and failure conditions
 - 3) the life expectancy of the 'mixed standard' **system**

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

The infrastructure controller is responsible for ensuring that the risk assessment is conducted properly and that a decision to mix standards, where that is the outcome, is justifiable.

- e) Where option (3) of (c) [above] is proposed and non-compliances with current Railway Group Standards are proposed, the situation has to be regularised by the authorisation of each non-compliance. [GA/RT6004](#) and [GA/RT6006](#) set out the arrangements to be applied. Valid circumstances for seeking a non-compliance include those where:
- 1) it is not reasonably practicable on technical grounds to apply current standards to the whole **system**, or
 - 2) application of a standard to part of a **system** would result in confusion, inconsistency or a direct safety risk.

[GA/RT6004](#) and [GA/RT6006](#) require that any application for a non-compliance against a Railway Group Standard is supported by an assessment of the risks and a justification for the proposed course of action (this is also good practice for non-compliances against standards other than Railway Group Standards).

It is important that an application for authorisation of a non-compliance against Railway Group Standards is made as soon as possible when a problem is discovered.

- f) Consideration should be given to the elimination of existing hazards in a **system** that is being modified, even if the modifications do not affect the part of the **system** where the hazard is. Such hazards may include those which have been identified and addressed in current Railway Group Standards, but were not adequately controlled by the standards that prevailed at the time of the original design.

B4.12 Demonstration of safety

Conformance of the **system** design shall be demonstrated by either or both of the following approaches:

- a) safety analysis and risk assessment, in the case of novel designs and novel elements of the design
- b) application of proven designs.

Explanation:

- a) Although [GK/RT0206](#) does not specify processes for demonstrating that systems are acceptably safe, this clause does specify the circumstances under which such a demonstration has to be made.
- b) A proven design is one that has already been accepted for use. This can be a specific product or **system**, manufactured to an approved **specification**. It could also be an approved standard set of circuits or software which is applied in accordance with approved principles and rules.

Guidance:

- c) Where it is proposed to use a proven **system** for an application for which it has already received product acceptance, there is generally no requirement to demonstrate by safety analysis and risk assessment that the application is acceptably safe. This does not, of course, remove the need for verification and validation of the application design.
- d) Similarly, where a **system** is being designed using a proven design arrangement, then there is generally no requirement for safety analysis and risk assessment of the design, provided that the application is valid for the proven design. Again, this does not remove need for design verification and validation.

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

Where the **system** is novel, or its application is novel, or it contains novel design elements or products, then it will be necessary to perform safety analysis and risk assessment to demonstrate that the proposals are acceptably safe. The extent of the analysis and assessment will depend upon the degree of novelty. The term 'novel' in this context applies to:

- 1) a **system** or design which has not been used on the controlled infrastructure before
 - 2) a **system** or design which has been used on the controlled infrastructure before, but where the application is different to its previous application(s).
- f) Particular difficulties may arise in demonstrating safety for certain categories of existing systems because of the lack of a formal, documented safety analysis on which to base the safety argument for the proposed application. These categories of systems include:
- 1) 'heritage' systems to which modifications are proposed
 - 2) systems already in use on other railway administrations and for which cross acceptance is proposed
 - 3) COTS systems.
- g) Various documents (eg Engineering Safety Management [the 'Yellow Book'], EN50126 and 50129) contain details of processes for demonstrating safety. See also [GI/RT7002](#), which sets out the mandatory requirements for product acceptance.

Guidance Note: Signalling and Operational Telecommunications Systems: Safety Requirements

References

Railway Group Standards and other Railway Group Documents

- [GA/RT6004](#) Temporary Non-Compliance with Railway Group Standards
- [GA/RT6006](#) Derogations from Railway Group Standards
- [GE/RT8049](#) The Creation and Management of **System** Authorities
- [GI/RT7002](#) Acceptance of Systems, Equipment and Materials for Use on Railtrack Controlled Infrastructure
- [GK/RT0002](#) Glossary of Signalling Terms
- [GK/RT0206](#) Signalling and Operational Telecommunications Systems: Safety Requirements
- [GK/RT0210](#) Asset Management for the Safety of Signalling and Operational Telecommunication Systems and Equipment

The Catalogue of Railway Group Standards and the Railway Group Standards CD-ROM give the current issue number and status of documents published by Railway Safety.

Other References

- EN50121** Railway applications – Electromagnetic compatibility
- EN50125** Railway applications – Environmental conditions for equipment
- EN50126** Railway applications – The **specification** and demonstration of **Reliability, Availability**, Maintainability and Safety (RAMS)
- EN50129** Railway applications – Safety related electronic systems for signalling

Engineering Safety Management (“Yellow Book” – ISBN: 0 9537595 1 2 and 0 9537595 0 4) - available from Praxis Critical Systems, Bath

HMRI Railway Safety Principles and Guidance (ISBN: 0 7176 0712 7)

Further Reference Material

- BS5760** **Reliability** of systems, equipment and components
- BS EN ISO 13407:1999** Human-centred design processes for interactive systems
- EIA 632** Processes for engineering a **system**
- IEC 61508** Functional safety of electrical/electronic/programmable electronic safety-related systems