

Guidance on Safety Requirements for **Cab Signalling** Systems

Synopsis

This document provides guidance on meeting the requirements of Railway Group Standard [GE/RT8026](#).

Signatures removed from electronic version

This Guidance Note has been produced by

Anne Blakeney
Standards Project Manager

Authorised by

Brian Alston
Controller, Railway Group Standards

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

Published by:
Safety & Standards Directorate
Railtrack PLC
Evergreen House
160 Euston Road
London NW1 2DX

© Copyright 2000 Railtrack PLC



Documents

Document Sharing Hub

This page has been left blank intentionally

Guidance on Safety Requirements for Cab Signalling Systems

Contents

Section	Description	Page
Part A		
	Issue Record	2
	Technical Content	2
	Application	2
	Health and Safety Responsibilities	2
	Supply	2
Part B		
1	Purpose	3
2	Scope	3
3	Definitions	3
4	System Overview	4
5	General Safety Requirements	11
5.1	Life Cycle System Safety	11
6	Modes of Operation	15
6.1	Permitted Modes	15
7	Authorising and Protecting Train Movements	17
7.1	Providing Movement Authorities	17
7.2	Compatibility of Trains with Infrastructure	20
7.3	Route Holding for an Authorised Movement	22
7.4	Protection against Unsafe Events and Conditions	24
8	Controlling the Risks of Overrun and Excessive Speed	26
8.1	Controlling and Mitigating Unauthorised Movements	26
8.2	Controlling and Mitigating Excessive Speed	30
9	Driver's Interface (MMI)	32
9.1	Provision of Movement Authority Information	35
9.3	General Requirements For Information Displayed to Drivers	36
10	Non-Driver Interfaces	42
10.1	Signaller's Interface (MMI)	42
10.2	Protection for Trackworkers and Engineering Work	45
10.3	Level Crossings	46
10.4	Control of unwanted System /non- System Interactions	48
11	System Management	50
11.1	System Maintenance	50
11.2	System Operation	52
11.3	Work Affecting System Operation	55
Appendix A		
	Other Signalling Standards Relevant to RTMCS Requirements	58
References		60

Guidance on Safety Requirements for Cab Signalling Systems

Part A

Issue Record

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

Issue	Date	Comments
One	December 2000	Original Document

Technical Content

Approved by: Francis How, Principal Signal & Telecomms Engineer, Railtrack S&SD
Richard Evans, Principal, Operations, Railtrack S&SD
Keith Rose, Principal Vehicles Engineer, Railtrack S&SD
Enquires to be directed to the Industry Safety Liaison Dept – Tel: 020 7904 7518

Application

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.

Health and Safety Responsibilities

In issuing this document, Railtrack PLC makes no warranties, express or implied, that compliance with all or any document published by the Safety & Standards Directorate 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.

Supply

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

Guidance on Safety Requirements for Cab Signalling Systems

Part B

1 Purpose

The purpose of this document is to provide guidance on, and explanation of, the safety requirements for rail traffic management and control systems which make use of **cab signalling**. These safety requirements are defined in [GE/RT8026](#) (hereafter referred to as the Standard).

2 Scope

The Scope of this document is the same as that of the Standard.

3 Definitions

Cab Signalling

A **system** of **signalling** whereby a set of visual display devices, fitted in the driving **cab** of the train, conveys instructions and information regarding the driver's authority to proceed.

Degraded Modes

Any **mode** of operation which is used to keep trains moving under **System** failure conditions, when normal operational modes are not available.

Dynamic Data

Data which changes without direct human action during the day to day operation of the **System**. It includes data such as train speed, train position etc.

Dual Signalled Lines

Parts of the railway where lineside signals are provided for controlling the movement of conventional trains and the **System** controls the movement of **cab**-signalled trains in the same geographical area.

End of Movement Authority

End of Movement Authority (EoA) is the location to which the train is permitted to proceed and where the target speed of the train is zero.

European Rail Traffic Management System/European Train Control System

European Rail Traffic Management **System**/European Train Control **System** (ERTMS/ETC) is the functional requirements specification and the UNISIG **System** Requirements Specification, reference Subset-026.

Exposed Groups

Groups of persons whose safety may be affected by the **System**. This includes passengers, railway workers, neighbours, users of level crossings, etc.

Fixed Infrastructure Element (of the System)

Those elements of the train control **system** which are located at the trackside and which perform high integrity safety functions. These elements are controlled by, and provide information back to, the interlocking and movement authority sub-systems.

Fixed Operational Data

Data which configures the generic **System** design for a specific application. It does not change during the day to day operation of the **System**. It includes data such as gradients, speed limits (track and train), infrastructure layout data, default braking data etc.

Movement Authority

Movement Authority (MA) is an instruction given to a train or driver (usually by the **System**) which allows a train movement to be carried out, under the conditions of that MA (eg speed, direction, etc).

Guidance on Safety Requirements for Cab Signalling Systems

Man Machine Interface

Man Machine Interface (MMI) is the interface device which indicates information to the operator (user) and which is used by the operator for the purpose of operating the associated **system**(s).

Overlap

A protected length of track ahead of an EoA provided to mitigate the consequences of a train exceeding its EoA.

System

This refers to the rail traffic management and control **system**, which comprises both the train control **system** and the associated control centre systems.

Train Borne Element (of the **System**)

Those elements of the train control **system** which are located on the train and which perform high integrity safety functions. These elements are controlled by, and provide information back to, the interlocking and movement authority sub-systems. These elements include associated sub-systems such as odometry where safety is dependent upon such sub-systems.

Variable Operational Data

Data which can be directly changed by operators and drivers during the day to day operation of the **System**. It includes data such as temporary speed restrictions, temporary prohibitions on the setting of routes, train length, train braking capability, etc.

Note: All technical terms and abbreviations contained in this document, other than those listed above, are defined in [GK/RT0002](#).

4 Introduction

4.1 Overview

[GE/RT8026](#) mandates the core safety requirements for train control systems which utilise **cab signalling**. The train control **system** requirements are based upon ERTMS/ETCS levels 2 and 3 functional requirements, but make few assumptions about the **system** architecture or technology.

These systems are currently in the development stage and this document may be subject to refinement as the systems are developed.

This section of this document provides a descriptive overview of the **System**. Guidance on compliance with the mandatory requirements of [GE/RT8026](#) is set out in sections 5 to 11.

4.2 Structure of this Document

The structure of this document is based upon six key areas associated with rail traffic management and control systems, namely:

- Modes of Operation;
- Movement Authorities;
- Train Speed Control;
- Driver's Man Machine Interface (MMI);
- Non-Driver Interfaces; and
- System** Management.

For each of these key areas, a number of principal safety requirements have been developed, together with a number of more detailed requirements. A diagram of the Safety Requirements Structure and Hierarchy is provided on page 8.

Guidance on Safety Requirements for Cab Signalling Systems

Railway Group Guidance Note
GE/GN8526
Issue One
Date December 2000
Page 5 of 5

The safety requirements are specified in a manner which is intended to facilitate compliance with the EC Directive on Interoperability, 96/48/EC, and all associated derivative specifications.

Guidance on Safety Requirements for Cab Signalling Systems

4.3 Main Functions of the System

The main functions of the System are to:

- a) facilitate the efficient use of the track for the purposes of moving trains;
- b) facilitate achievement of the timetable and recovery from train service perturbations;
- c) ensure safety in the significant accident scenarios (see section 4.4).

4.4 Accident Scenarios Controlled by the System

The significant accident scenarios controlled by the System are:

- a) collisions between trains (rear end, head on, same direction converging);
- b) buffer stop collisions;
- c) derailments and overturning of trains;
- d) accidents at level crossings; and
- e) accidents involving personnel working on the railway.

4.5 Hazards Mitigated by the System

The System has the potential to reduce the level of risk in some key areas compared with conventional signalling systems, notably:

- a) passing the EoA (via Automatic Train Protection [ATP]);
- b) overspeeding (via ATP);
- c) exposure of trackside workers to hazards (less lineside equipment and better warning/access control); and
- d) vandalism (less lineside equipment).

The System also provides the potential for mitigating the effects of other hazards which are not directly within the scope of the System's purpose. This arises largely because of the potential for revoking a MA and stopping a train more promptly than is possible with conventional lineside signalling.

For these purposes, the System will be provided with inputs from other detection mechanisms (which are outside the scope of the System), to which it then responds accordingly.

Guidance on Safety Requirements for Cab Signalling Systems

4.6 Hazards Potentially Introduced by the System

The System has the potential for introducing new hazards or increased levels of risk compared with conventional signalling systems, including:

- a) difficulties of proving train complete where train detection systems are not track-based;
- b) potential errors in, or lack of knowledge about, train position information, particularly following catastrophic System failure where track circuits are not used;
- c) the need for extensive input and modification of safety-critical data as part of the routine operation and use of the System;
- d) greater difficulties in managing train movements in the event of a catastrophic System failure;
- e) lack of broken rail detection where track circuits are not used;
- f) controlling the movements of trains leaving possessions;
- g) loss of trackside telephones; and
- h) cultural changes and other human factors associated with changing from a lineside signalling system.

This document contains safety requirements that address these hazards.

4.7 System Description

A diagram of the outline System architecture is provided on page 9. This diagram, and the description given in sections 4.7.1 to 4.7.6 below, are not definitive or mandatory. The mandatory safety requirements, set out in Sections 5 to 11 of this document, make few assumptions about the System architecture. However, the diagram serves to illustrate the general scope/boundaries of the System and the broad partitioning of the safety functions between the main sub-systems. The System comprises:

4.7.1 Interfaces for the Signaller and Others who Operate the System

These will typically include:

- a) visual display units showing the movements of trains and status of the infrastructure, in pictorial and/or tabular form;
- b) push-button control panels, keyboards and other devices for controlling the infrastructure and the train movements, controlling access for engineering work, etc; and
- c) other interfaces such as Closed Circuit Television (CCTV) monitors for controlled level crossings and hot axle box detection reporting systems.

The signallers and other operators are considered to be a key element in the safe operation of the System, and therefore the likelihood of human error, the development of procedures, ergonomic issues and competency requirements are addressed by the requirements.

Guidance on Safety Requirements for Cab Signalling Systems

4.7.2 Train Routing and Regulation Sub-Systems

It is envisaged that normal train running will be handled automatically by the **System**, with relatively little need for the signaller to intervene. Typically, sub-systems will be provided for:

- a) the automatic setting of routes in accordance with timetable data and decision-making criteria; and
- b) regulating the flow of trains (eg for energy-efficiency purposes or optimisation of throughput).

In addition to facilities for automatic train routing and routing initiated by the signaller, facilities may also be provided for trains to initiate route requests automatically (eg before they reach their EoA, or when waiting to depart from a station).

Where trains are following closely in moving block operation, the EoA for each train can be advanced incrementally, with reference to the rear of the train in front (allowing a suitable margin for safety). The giving of a MA, whether by the signaller or automatically, is based on the assumption that any train ahead is stationary, whether or not it is moving in practice.

4.7.3 Interlocking and Movement Authority Sub-Systems

These sub-systems perform the core safety functions of the fixed infrastructure. They comprise:

- a) interlockings, which set, lock, prove and hold routes for the passage of trains in response to commands from the signaller and train routing and regulation sub-systems;
- b) sub-systems which generate and receive/process data messages transmitted to/from the trackside equipment, the control centre, other interlockings and the trains.

These sub-systems have access to data about the fixed infrastructure and the trains which is necessary in order for correct MA and speed-related information to be given to the trains.

4.7.4 Trackside Equipment

The trackside equipment comprises items such as:

- a) point operating mechanisms;
- b) balises/loops (for train position determination and/or passing supplementary information to trains);
- c) level crossings;
- d) in dual-signalled areas, other conventional equipment such as signals, train detection equipment; Automatic Warning **System** (AWS), Train Protection and Warning **System** (TPWS); and
- e) track-based train detection systems.

These items are controlled by, and/or provide information back to, the interlocking and MA sub-systems.

Guidance on Safety Requirements for Cab Signalling Systems

Railway Group Guidance Note
GE/GN8526
Issue One
Date December 2000
Page 9 of 9

4.7.5 Train-Borne Sub-Systems

The train-borne equipment comprises:

- a) the driver's MMI;
- b) sub-systems which receive/process and generate data messages transmitted from/to the fixed infrastructure;
- c) ATP sub-system; and
- d) train position and train integrity equipment.

As with the interlocking and MA sub-systems, the train-borne sub-systems need to possess, or have access to, data about both the train and the fixed infrastructure. It should be noted that the safety requirements do not make assumptions about where in the **System** this data is held, nor which part of the **System** uses the data for calculating MAs, speed information, etc.

Train drivers are a key element in the safe operation of the **System**, and therefore the likelihood of human error, the development of procedures, ergonomic issues and competency requirements are addressed by the requirements.

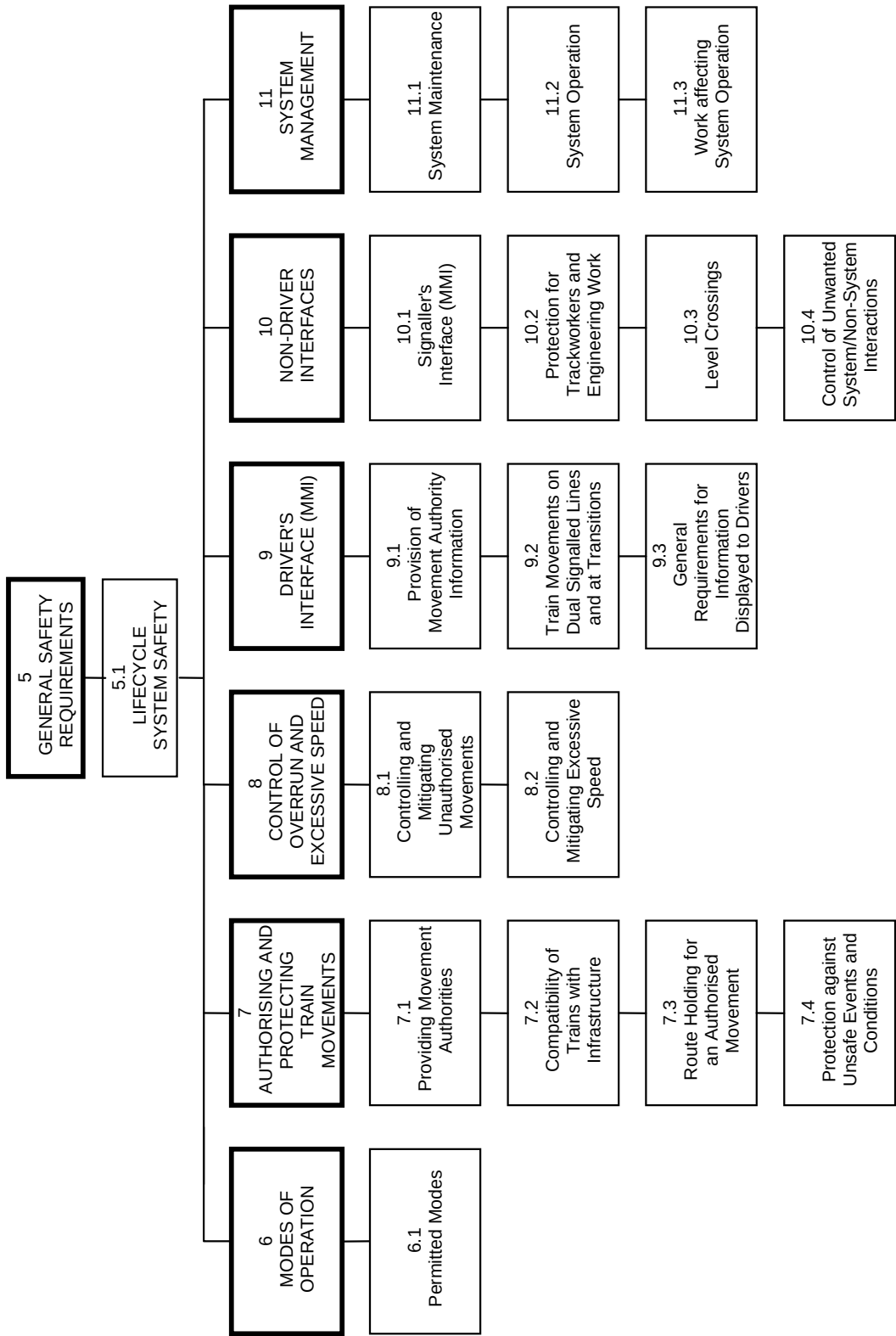
4.7.6 Other Equipment

The requirements also make provision for the **System** to accept inputs from ancillary systems such as hot axle box detectors, dragging equipment detectors, etc. These are not regarded as part of the **System** itself, however.

In addition, the communication links between the various parts of the fixed infrastructure and trains are not necessarily part of the **System**. In many cases these will be open systems and transparent to the data, where the integrity of the **System** is independent of the communication links.

Other related train-borne systems, such as the train braking systems, train health monitoring systems, etc are key to the safe operation of the train, but are not regarded as part of the **System**.

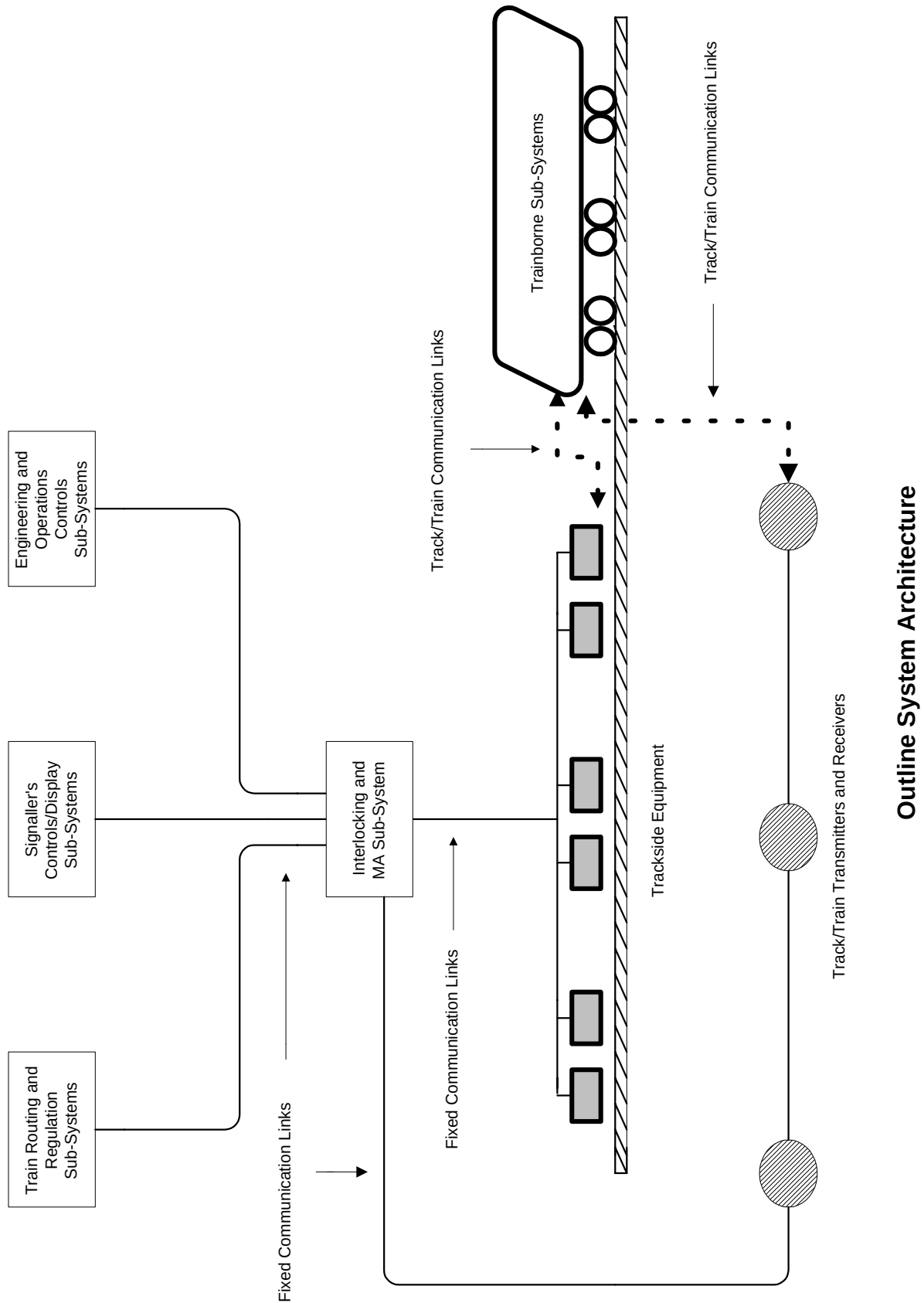
Guidance on Safety Requirements
for Cab Signalling Systems



Safety Requirements Structure and Hierarchy

The numerical references shown refer to the clause identities of the Requirements within this document.

Guidance on Safety Requirements for Cab Signalling Systems



Guidance on Safety Requirements for Cab Signalling Systems

5 General Safety Requirements

5.1 Life Cycle **System** safety

The overall level of safety associated with the use of the **System** shall be established and subsequently sustained throughout its operational life at a level which meets the requirements of legislation and the reasonable expectations of exposed groups.

Explanation: The "level of safety associated with the use of the **System**" should be understood to mean not just the safety provided by the **System** itself, but also includes the contribution from the procedures which are applied in the use of the **System**, and should take account of the manner in which the **system** is used (traffic speeds, traffic densities, regulation and timetabling issues).

The term "exposed groups" includes consideration of the safety of all passengers, railway workers, neighbours, users of level crossings etc. The subject of "reasonable expectations" of exposed groups is further developed in section 5.1.5.

Guidance: European Standard prEN50126 provides a process for establishing and sustaining safety (and non-safety) requirements throughout the life cycle of railway systems.

Related sections: 5.1.5

5.1.1 **System** Life Cycle Management

Railway Group members shall agree their respective responsibilities and implement suitable arrangements for **System** design and for controlling the **System** configuration and safety performance throughout the **System** life cycle.

Explanation: Suitable arrangements should include resources, organisational structures, defined responsibilities, processes and procedures.

Guidance: This requirement addresses the need for a "**System** Authority" or equivalent, supported by other organisations with defined roles, to provide for the safe management of the **System** throughout its life cycle, from concept to decommissioning. Key elements of the **System** Authority role are to ensure that the following activities are discharged:

- Specifying the **System** requirements;
- **System** and sub-**system** acceptance;
- **System** maintenance;
- Safety performance monitoring and corrective action;
- Configuration management;
- Change control.

European Standard prEN50126 addresses some of the life cycle management issues relevant to this requirement.

5.1.2 Definition of Scope and Functionality of the **System**

The scope, functionality, proposed use and expected life of the **System** shall be defined sufficiently for the purposes of developing the detailed safety requirements of the **System**.

Guidance: The identification of the scope and functionality includes consideration of:

- the **System** architecture, including the hardware and software which comprises the **System**;
- the principal functions that the **System** is required to perform. This includes specific safety functions (eg the provision of ATP) and functional requirements (eg the types of train movements which the **System** must be able to support);
- the geographical scope of the **System**;

Guidance on Safety Requirements for Cab Signalling Systems

- the operational parameters which the **System** is required to meet or support (eg train speeds, train lengths, train braking capabilities; traffic types; traffic densities; timetabling and regulation requirements). In some cases (eg train braking capabilities) tolerances or ranges may be placed on these parameters, within which the **System** must continue to operate safely;
- other systems and entities with which the **System** is required to interface, operate or be compatible (ie other systems and equipment which form part of the fixed infrastructure, and trains);
- the human interfaces;
- the physical environment within which the **System** is required to operate;
- hardware and software tools which are required in order to support the safe design, testing, operation, maintenance and modification of the **System**.

In respect of the operational parameters, it should not be assumed that these are "givens" for which the **System** design has to provide appropriate solutions. In some cases it may be necessary to modify elements such as the track layout, traffic patterns, etc in order that a **System** with an acceptably low level of risk can be designed.

European Standard prEN50126 provides further guidance on the development of the scope and functionality requirements, under the life cycle phases of "Concept" and "**System** Definition and Application Conditions".

Related sections: 5.1.3; 10.4, 11.2.1

5.1.3 Development of Detailed Safety Requirements

Detailed **System** requirements, which are relevant to safety, shall be established for the purposes of **System** design, testing and acceptance.

Explanation: The term "**System** requirements" should be understood in this context to include all those requirements which are relevant to the safety performance of the **System**. This includes:

- functional requirements relating to the purposes for which the **System** is provided;
- specific safety requirements (both functional and non-functional);
- Reliability, Availability, Maintainability and Safety (RAMS) targets;
- integrity levels (SILs);

Guidance: The requirements should be traceable to, and demonstrably compliant with, the core safety requirements specified in [GE/RT8026](#).

It will also be necessary to identify requirements in other RGSs which are applicable or relevant to the development of the detailed Safety Requirements (see Appendix A).

Requirements should be partitioned between the various sub-systems that comprise the **System**. This may also include the need to partition safety "responsibility" between the **System** and people who use/operate the **System**.

The requirements should address the wider concept of "fitness for purpose". This term includes reliability, availability and maintainability, and also embraces 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. 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.

European Standard prEN50126 provides further guidance on the development of the **System** requirements, under the life cycle phases of "Risk Analysis", "**System** Requirements" and "Apportionment of **System** Requirements".

The **System** shall comply with relevant UK and EC legislation and HMRI Safety Principles.

Guidance on Safety Requirements for Cab Signalling Systems

"EC legislation" includes:

- EC Directive on Interoperability, 96/48/EC, and all derivative specifications thereof;
- Cenelec Standards (including those with prEN and ENV status), notably 50121, 50126, 50128, 50129 and 50159. Some of these Standards relate to processes for **System** development, design and life-cycle management, and are not confined simply to the **System** requirements;
- ETCS Functional Requirements Specification, reference A 200/FRS.02-935614-04.00-960827, dated 27/08/96.

Related sections: 5.1.2; 11.2.1

5.1.4 Development of Operational Procedures

The associated rules/procedures for the safe operation of the railway shall be developed in conjunction with the **System** requirements.

Guidance: Human factors analysis should be undertaken to facilitate the development of operational rules and procedures.

Related sections: 6.1.3; 11.2.3

5.1.5 Safety Targets

The totality of risk associated with the operation of the **System**, and where appropriate the particular level of risk associated with sub-systems and elements of the **System**, shall be:

- tolerable; and
- As Low As Reasonably Practicable (ALARP); and
- no worse than at present.

Guidance: 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.

The "totality of risk" should take into account not only the hazards relating to the **System** itself (malfunction etc) but also the risks associated with the use of the **System**. Included within this latter category are: track layout; train speeds; traffic densities; movements onto occupied lines; rules and procedures for operation and maintenance etc.

The requirement for risk to be "no worse than at present" should be interpreted as meaning that the overall level of risk should be no worse (and ideally substantially lower) than the level which existed with the conventional **signalling** that the **System** replaces, even though speeds might be increased and the traffic density greater. This requires a "whole railway" approach to risk apportionment and management.

Further guidance on the assessment and management of risk is provided in the Engineering Management **System**, Issue 3 (Yellow Book 3).

Special attention should be given to the identification and mitigation of hazards arising from the change from a conventional **signalling system** to one based on in-cab **signalling**. Two key areas for consideration are those of "lost benefits" and "human factors":

- Lost benefits include factors such as: the loss of track circuiting (rail breaks are consequentially less readily detected and track circuit operating clips are ineffective); the loss of lineside "landmarks" (signals, etc) for on-track personnel

Guidance on Safety Requirements for Cab Signalling Systems

- to use for locating their position; loss of trackside telephones.
- Human factors issues include: the major cultural changes associated with changing from a lineside **signalling system** (affecting operators, maintainers, emergency services, etc); assumptions inherent in ways of working which are no longer valid in for an in-cab **System**; the capability of people to manage the railway under normal, **degraded** and total failure conditions.

The **System** should be designed so that no credible failure **mode** exists which could lead to a hazard resulting in an unacceptable level of risk. Situations where hazards arise may include, but are not necessarily confined to:

- exceeding an EoA by an extent which jeopardises safety (see section 8.1);
- travelling at unsafe speed (see section 8.2);
- issuing/displaying a MA for a movement which it is not safe to make (see section 7.1 and section 7.3);
- issuing a MA to the wrong train (see section 9.1);
- jeopardising an authorised train movement (see section 7.3);
- inability to revoke a MA in an emergency (see section 7.4);
- inadequate protection of pedestrians and vehicular traffic at level crossings (see section 10.3);
- inadequate protection of trains and trackworkers when engineering work is taking place (see section 10.2);
- loss of control resulting in heavy dependency upon **Degraded** Modes of operation (see section 6.1);
- loss of route inhibition facilities (see section 10.1).

The term "failure modes" includes modes whereby hidden failures, in combination with other subsequent failures, could lead to a hazardous situation.

Formal hazard identification and risk assessment will be necessary in order to determine those hazards that present an unacceptable level of risk and therefore require controlling. The measures applied are likely to address both causes and consequences of the hazards, rather than focussing solely on either prevention or mitigation.

Consideration should be given to the choice of data transmission protocols, to ensure that the overall **System** safety performance cannot be jeopardised by faults or errors within the various data transmission sub-systems.

Related sections: 5.1; 6.1; 6.1.1; 7.1; 7.3; 7.4; 8.1; 8.2; 9.1; 10.1; 10.2; 10.3

5.1.6 Compliance with Standards for Conventional **Signalling**

Where the **System** is provided in conjunction with conventional lineside **signalling** systems, the requirements for the lineside **signalling system** are set out in Railway Group Standard **GK/RM0501**.

Explanation: The reference to **GK/RM0501** should be understood to refer to all Standards that apply to lineside **signalling**. These Standards are listed in the introductory sections to **GK/RM0501**.

Guidance: Typical scenarios include transitions between lineside **signalling** and the **System**, and dual-signalled areas.

Lineside signals on dual signalled lines may be, but do not have to be, equipped with ATP. They do, however, have to be equipped with a train protection **system** in accordance with the requirements of the Railway Safety Regulations 1999.

5.1.7 **System** Life Cycle Design

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.

Guidance on Safety Requirements for Cab Signalling Systems

Guidance: 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**.

Amongst the issues to be addressed through this requirement are:

- obsolescence of hardware and software;
- appropriate architecture and design of hardware and software in order to minimise the level of risk associated with modifications;
- provision of diagnostic aids to support maintenance.

6 Modes of Operation

6.1 Permitted Modes

The permitted modes of operation associated with the use of the **System** shall be defined for both normal and credible failure conditions.

Explanation: The term "modes of operation" refers to the different ways in which drivers and signallers use and interact with the **System**. For a driver, these may include the modes listed below. Modes also need to be defined for the signaller, and possibly for other users.

Operational modes for drivers (this list is provided for example purposes only, and is not necessarily exhaustive):

- off;
- undergoing self-test/initialisation;
- on but inactive;
- active and providing full driver supervision for running movements;
- active and providing driver supervision for shunting movements;
- failed (no driver supervision but **cab signalling** operational);
- failed (partial driver supervision but **cab signalling** operational);

Guidance: 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**.

Related sections: 5.1.5

6.1.1 Safety levels for individual modes

For each normal and **degraded mode** of operation, the overall level of safety achieved and the apportionment of safety responsibility between the **System** and the users shall be clearly defined.

Guidance: The overall level of safety shall take into account both the safety provided through operational procedures, and that provided by the **System**. It is important, for each **mode**, that the degree of responsibility for safety placed upon the users (drivers and signallers) is clearly understood.

Related sections: 5.1.5

6.1.2 Transitions Between Modes

The permitted transitions between the various modes of operation (both normal and **degraded**) shall be defined.

Guidance: It is important for safety that there are defined conditions to be met before a change can be made from one **mode** of operation to another. These conditions will determine in part the procedural requirements (see section 6.1.3), and may also determine aspects of the **System** design.

It will not normally be possible to make a **transition** from any one **mode** to all other modes. Only some transitions will be permitted.

Guidance on Safety Requirements for Cab Signalling Systems

Related sections: 6.1.3; 10.1

6.1.3 Procedures and Rules for Modes

Rules and procedures shall be defined 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; and
- c) recovery from credible failure conditions.

Explanation: "Procedures and supporting information" includes: Rule Book, signallers' and drivers' instructions etc, which tell users how they are to perform, and what their responsibilities are.

Guidance: This requirement also points to the need for ancillary information (particularly for ensuring safety when operating in **degraded** modes), such as; lineside position markers, point end identifiers on the track for use by route setting Agents, route setting tables and track layout diagrams for signallers.

Particular attention will need to be paid to the integrity of variable operational data (eg prohibitions) and dynamic data (eg train positions) during the process of restoration from credible failure conditions.

RGS [GO/RT3437](#) specifies the requirements for taking trains out of service in the event of a failure of a train-borne sub-**system**.

Related sections: 5.1.4; 6.1.2; 6.1.6; 10.1.2; 11.2.2; 11.3.4

6.1.4 **System** Availability for Normal Modes

The reliability and availability of the **System** shall be such as to avoid, so far as is reasonably practicable, the need to use **degraded** modes of operation instead of normal modes.

Guidance: High reliability/availability at the operational level may be achieved by high inherent sub-**system** reliability, coupled with additional measures such as redundancy, other suitable standby arrangements and graceful degradation mechanisms.

Related sections: 10.1

6.1.5 Hierarchy of **Degraded** Modes

The **degraded** modes of operation shall 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.

Guidance: The hierarchy of modes, and the conditions for entry to them, should be such as to prevent, so far as is achievable, the **System** failing to an unpredictable or unsafe state.

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".

So far as reasonably practicable, the **System** should continue to provide the following functionality in **degraded** modes of operation:

- conflicting/opposing movements should not be authorised;
- level crossings should be proved to be safe for the passage of trains and the stopping of road traffic;
- points should be proved to be in the correct position and prevented from moving;
- restricted MAs (eg for movements at low speed) should be issued to trains by

Guidance on Safety Requirements for Cab Signalling Systems

the **System**, in preference to the use of verbal instructions;