Management of Shared Information Systems

Synopsis
This document defines the requirements for managing shared information systems that process information used for the safe operation and interworking of trains.

Submitted by
Paul Woolford
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

© Copyright 2002 Railway Safety
This page has been left blank intentionally
# Management of Shared Information Systems

## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Part A</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A1</td>
<td>Issue record</td>
<td>2</td>
</tr>
<tr>
<td>A2</td>
<td>Implementation of this document</td>
<td>2</td>
</tr>
<tr>
<td>A3</td>
<td>Scope of Railway Group Standards</td>
<td>2</td>
</tr>
<tr>
<td>A4</td>
<td>Responsibilities</td>
<td>2</td>
</tr>
<tr>
<td>A5</td>
<td>Health and safety responsibilities</td>
<td>3</td>
</tr>
<tr>
<td>A6</td>
<td>Technical content</td>
<td>3</td>
</tr>
<tr>
<td>A7</td>
<td>Supply</td>
<td>3</td>
</tr>
<tr>
<td><strong>Part B</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B1</td>
<td>Purpose</td>
<td>5</td>
</tr>
<tr>
<td>B2</td>
<td>Application of this document</td>
<td>5</td>
</tr>
<tr>
<td>B3</td>
<td>Definitions</td>
<td>6</td>
</tr>
<tr>
<td>B4</td>
<td>General requirements</td>
<td>6</td>
</tr>
<tr>
<td>B5</td>
<td>Shared information system identification</td>
<td>7</td>
</tr>
<tr>
<td>B6</td>
<td>System Safety Implication Statements</td>
<td>7</td>
</tr>
<tr>
<td>B7</td>
<td>System Management Group</td>
<td>8</td>
</tr>
<tr>
<td>B8</td>
<td>System Safety Case</td>
<td>9</td>
</tr>
<tr>
<td>B9</td>
<td>System change arrangements</td>
<td>10</td>
</tr>
<tr>
<td>B10</td>
<td>Information system acceptance</td>
<td>10</td>
</tr>
<tr>
<td>B11</td>
<td>Security and incident management</td>
<td>10</td>
</tr>
</tbody>
</table>

## References

11
Management of Shared Information Systems

Part A

A1 Issue record

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>One</td>
<td>June 2002</td>
<td>Original document.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supersedes GO/RT3435</td>
</tr>
</tbody>
</table>

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 June 2002.

This document comes into force on 3 August 2002.

The dates by which compliance with the requirements of this document is to be achieved are set out in Part B2. Where those dates are later than the date on which this document comes into force, this is to give Railway Group members additional time to plan and commence implementation so as to achieve full compliance by the dates set out in Part B2.

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

<table>
<thead>
<tr>
<th>Railway Group Standard</th>
<th>Issue No.</th>
<th>Title</th>
<th>RGS sections superseded by this document</th>
<th>Date(s) as of which sections are superseded</th>
</tr>
</thead>
<tbody>
<tr>
<td>GO/RT3435</td>
<td>One</td>
<td>Management and Development of Railway Group Safety-Related Computer Information Systems</td>
<td>All</td>
<td>7 June 2003</td>
</tr>
</tbody>
</table>

The superseded document GO/RT3435 Issue One, listed above, is withdrawn from 7 June 2003.

A3 Scope of Railway Group Standards

The overall scope of Railway Group Standards is set out in Appendix A of GA/RT6001. The specific scope of this document is set out in Part B2.

A4 Responsibilities

Railway Group Standards are mandatory on all Railway Group members * and apply to all relevant activities that fall into the scope of each individual’s Railway Safety Case. If any of those activities are performed by a contractor, the contractor’s obligation in respect of Railway Group Standards is determined by the terms of the contract between the respective parties. Where a contractor is a duty holder of a Railway Safety Case then Railway Group Standards apply directly to the activities described in the Safety Case.

* 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.
Management of Shared Information Systems

A5 Health and safety responsibilities

In issuing this document, Railway Safety makes no warranties, express or implied, that compliance with all or any documents 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.

A6 Technical content

The technical content of this document has been approved by:

Richard Evans, Technical Principal, Operations, Railway Safety

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

A7 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.
This page has been left blank intentionally
Management of Shared Information Systems

Part B

B1 Purpose

This document defines the requirements for managing shared information systems that process information used for the safe operation and interworking of trains.

B2 Application of this document

B2.1 To whom the requirements apply

This document contains requirements which are applicable to Railway Safety and the duty holders of the following categories of Railway Safety Case:

a) infrastructure controller
b) station operator
c) train operator

Under the Railways (Safety Case) Regulations 2000, the duty holder at a station (as defined in those Regulations) is responsible for ensuring that the requirements of Railway Group Standards are complied with. At a station, contractual arrangements (including a lease) do not of themselves relieve the duty holder of his obligations under those Regulations.

B2.2 Compliance requirements

This document specifically applies to shared information systems where the information they process or hold is used by more than one Railway Group member. These information systems will usually be computer based. See section B2.3 for exclusions.

All shared information systems that are commissioned after 3 August 2002 shall comply with all the requirements of this document from the date they are commissioned.

All shared information systems commissioned on or before 3 August 2002 shall comply with the requirements of this document by 7 June 2003, except that all shared RTIS catalogue systems commissioned on or before 3 August 2002 shall comply with all requirements of this document by 3 August 2002.

The identification of all shared information systems, as required by section B5 of this document, shall be completed by 3 August 2002.

Until the compliance dates above, or the date by which compliance is achieved (if earlier), the applicable requirements of GO/RT3435 Issue 1 shall continue to be met.

After the compliance dates, or after the date by which compliance is achieved (if earlier), Railway Group members shall not deviate from the requirements set out in this document.

Where it is considered not practicable, or not reasonably practicable, to comply with the requirements set out in this document, authorisation not to comply shall be sought in accordance with GA/RT6001, GA/RT6004 or GA/RT6006.

B2.3 Exclusions from the application of this document

The requirements of this document do not apply to:

a) real time control systems, where the effect of the system on the railway is immediate, that is, without the intervention of people
b) computer systems used by one Railway Group member only.
**B3 Definitions**

**Computer system**
A set of application code, together with the supporting hardware and operating arrangements used to perform a particular set of tasks.

**Integrity**
Conformity of data with its definition.

**Information system**
A system containing one or more computer systems, that accepts and provides data where all data change is automatic and non-manual, together with its supporting business processes and procedures for operational change, maintenance, input and output.

**Input data**
Alphabetic or numeric information that a computer needs to undertake its function and hence provide output data.

**RTIS Catalogue System**
A system covered by the Systems Code and listed in the Systems Catalogue.

**Safety implication**
The safety effect on the operation and inter-working of trains, of the use of an item of data or process contained in an information system.

**Safety Implication Statement**
Documented evidence stating for each Railway Group member or their agents using an information system, whether any use of the system has a material safety implication, and if so how the Safety Implication Statement is kept up-to-date.

**Shared information system**
Any information system where more than one Railway Group member uses the system, and at least one Railway Group member inputs data to the system, and at least one Railway Group member extracts data from the system.

**System Management Group**
A formally constituted group of people who represent the users of an information system to assist their proper management of change, support and access to that information system.

**System Safety Case**
Documented evidence of risk assessment, the existence of a safety management system, and the maintenance and operational arrangements, for an information system which has an identified material safety implication, compliance with which is required of any users of that information system.

**User**
An organisation, or its agent, which inputs data to, or extracts data from, an information system whether directly, or by automatic or non-manual means through another information system.

**B4 General requirements**

Railway Group members shall:

a) identify those shared information systems which they use

b) co-operate in creating and maintaining a System Safety Implication Statement for each shared information system that they use. They shall also ensure that records are retained to demonstrate that the requirements of the System Safety Implication Statement are being met
Management of Shared Information Systems

c) co-operate in the arrangements of a System Management Group for each shared information system that they use

d) for each shared information system they use, and which has a material safety implication, co-operate in creating and/or maintaining a suitable and sufficient System Safety Case for that system. They shall also ensure that records are retained to demonstrate that the requirements of the System Safety Case are being met

e) ensure that the System Safety Implication Statement and (where appropriate) the System Safety Case are accepted by a formally constituted acceptance body

f) ensure that where the shared information system has a material safety implication, the system management arrangements described in the System Safety Case are applied

g) co-operate in applying the requirements of this document to the development of new information systems.

B5 Shared information system identification

Railway Group members shall identify and document the shared information systems that they use, including information systems that:

a) they use directly, and which other Railway Group members also use directly

b) they use directly, and which supply data to other information systems where it is then used by other Railway Group members

c) they use indirectly through another system and which are used either directly or indirectly by other Railway Group members.

B6 System Safety Implication Statements

Shared information systems shall be assessed by each user to determine whether any of that organisation’s use of the system has a safety implication and, if so, whether this is a material safety implication.

This assessment shall encompass both direct uses of the system and uses through other systems fed by that system. If any one Railway Group member assesses their use of a system as having a material safety implication, the complete system shall be regarded as having a material safety implication.

The results of the assessment shall be documented in a System Safety Implication Statement. The System Safety Implication Statement shall be produced whether or not a system is found to have a material safety implication. The System Safety Implication Statement shall be agreed by all Railway Group members using the system and endorsed by the applicable System Management Group (see section B7).

The System Safety Implication Statement shall identify:

a) all uses and users, including users of other systems that are not shared but use data supplied by the system

b) those uses which are relevant to safety but do not have a material safety implication

c) those uses which have a material safety implication
Management of Shared Information Systems

d) how the System Safety Implication Statement is reviewed (frequency shall be not less than annually) and is kept up-to-date in respect of changes in organisation and business processes which have the potential to affect the materiality of the safety implication.

Users shall ensure that there are suitable arrangements in place to review and update the System Safety Implication Statement, as necessary, to reflect changes in the system or its use.

Where the System Safety Implication Statement identifies a material safety implication by any Railway Group member using that system, whether as a direct use of the system or through other systems fed by that system, a System Safety Case shall be developed. In these circumstances the System Safety Implication Statement shall be maintained under the System Safety Case arrangements (see section B8).

B7 System Management Group

B7.1 Formation
System users shall establish a System Management Group for each shared information system. Shared information systems may be grouped together within a single System Management Group for this purpose, but each system within any such grouping shall not be considered by more than one System Management Group.

B7.2 Membership
Membership of a System Management Group shall be representative of the users of the shared information system, to ensure the requirements to change, support, and manage access to information are correctly managed.

B7.3 Remit
The System Management Group shall:

a) assist the safe usage, maintenance and development of the shared information system

b) co-operate in establishing appropriate arrangements for the production and maintenance of System Safety Implication Statements and System Safety Cases

c) review and endorse System Safety Implication Statements (see section B6)

d) review and endorse System Safety Cases (see section B8)

e) endorse change to System Safety Implication Statements or System Safety Cases

f) assist users to identify and manage problems with the system and its data

g) liaise with other System Management Groups, and the users of other systems using information from a shared system, as necessary, to ensure associated systems work effectively together

h) assist in identifying system controls required to improve the system’s fitness for the purposes, including safety, to which its users put it.

The System Management Group shall establish clear procedures that enable activities a) to h) in this section to be completed.

The System Management Group shall have no authority over the business processes generating or using information. The safety responsibility shall remain with the user organisation.
Management of Shared Information Systems

B7.4 Independent advice
Where agreement cannot be reached within a System Management Group or between System Management Groups, on issues of substance, independent advice or arbitration shall be sought.

B8 System Safety Case
For those shared information systems with a System Safety Implication Statement that identifies a material safety implication, the following shall be documented in a System Safety Case:

a) the risks to be managed with regard to the shared information system

b) the system management arrangements, identifying the roles and responsibilities of the various parties involved, ie owner, supplier and/or maintainer, and users

c) the roles, responsibilities and rights for operation and use of a shared information system

d) the controls, supporting processes and procedures important to managing the risks

e) the arrangements to ensure that those with responsibilities for the operation of processes and procedures, important to the safe usage and development of the system, perform as required

f) the arrangements that ensure that users are aware of the degree of integrity with which the system and its data can be expected to perform

g) the processes for review and improvement of the information system

h) the processes for review and improvement of the system management arrangements

i) the processes for review of the System Safety Case.

The System Safety Case shall demonstrate that the processes and procedures the system contains are suitable and sufficient for the safety reliance placed upon the system, and that there are adequate arrangements in place to ensure that the integrity of the system will continue to match the reasonable expectations of users.

The System Safety Case shall be agreed by users who are Railway Group members, whose agreement shall not be unreasonably withheld. Agreement shall constitute acceptance that the processes and procedures are suitable and sufficient for the safety purpose to which that user puts the system, and that they will comply with the processes and procedures specified.

Railway Group members shall also ensure that others who are not Railway Group members, but who they commission or involve in using a system covered by a System Safety Case, understand and accept the requirements of this document for that system.

The System Safety Case shall then be endorsed by the System Management Group. Such endorsement shall be recorded.

Endorsement of a System Safety Case by the System Management Group signifies that the System Safety Case records a correct representation of the management arrangements for the system, and that an adequate process to achieve agreement by users has been executed.
Management of Shared Information Systems

B9 System change arrangements

Changes to shared information systems with material safety implications shall not be made unless:

a) change is supported by an assessment of the safety implication
b) the System Management Group agree that the proposed change is acceptable from a safety point of view
c) the System Safety Implication Statement and the System Safety Case (if any) are amended, if necessary
d) arrangements for change set out in the System Safety Case (if any) are followed
e) where there is a possibility that the change may affect a safety use, whether directly or indirectly, any potentially affected users are notified.

Where a change is made to a shared information system that does not have a material safety implication, but the change means that the system, as altered, will have a material safety implication, then a System Safety Case shall be produced for that system.

B10 Information system acceptance

After endorsement by the System Management Group, all System Safety Implication Statements and System Safety Cases shall be submitted for approval to a formally constituted acceptance body.

The function of the acceptance body shall be to grant approval on the basis of the shared information system’s management arrangements being suitable and sufficient to ensure the system’s fitness for the safety purposes to which users put it.

B11 Security and incident management

Each shared information system with a material safety implication, and its contained computer systems and associated equipment, shall have applied to it arrangements for:

a) computer system security
b) controlling access to the system
c) recording safety-related incidents, together with recovery action taken
d) controlling and responding to planned and unplanned non-availability outages.
Management of Shared Information Systems

References

Railway Group Standards and other Railway Group Documents

GA/RT6001 Railway Group Standards Change Procedures
GA/RT6004 Temporary Non-Compliance with Railway Group Standards
GA/RT6006 Derogations from Railway Group Standards
GE/RC8554 Recommendations for the Management of Shared Information Systems