

# Recommendations for the Management of Shared Information Systems

Signatures removed from electronic version

## Synopsis

This document supports Railway Group Standard [GE/RT8054](#), and provides recommendations for managing shared information systems that process safety information.

## 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

Uncontrolled When Printed

This page has been left blank intentionally

# Recommendations for the Management of Shared Information Systems

---

 Railway Safety Approved Code of Practice

 GE/RC8554
 

---

 Issue One
 

---

 Date June 2002
 

---

 Page 1 of 17
 

---

## Contents

Section	Description	Page
<b>Part A</b>		
A1	Issue record	2
A2	Implementation of this document	2
A3	Scope of Railway Group Standards	2
A4	Responsibilities	2
A5	Health and safety responsibilities	2
A6	Technical content	2
A7	Supply	2
<b>Part B</b>		
B1	Purpose	3
B2	Application of this document	3
B3	Definitions	5
B4	General requirements	6
B5	Shared <b>information system</b> identification	7
B6	<b>System</b> Safety Implication Statements	8
B7	<b>System</b> Management Group	9
B8	<b>System</b> Safety Case	11
B9	<b>System</b> change arrangements	14
B10	<b>Information system</b> acceptance	14
B11	Security and incident management	15
<b>Appendix A</b>		
	<b>Information</b> systems	16
<b>References</b>		17

# Recommendations for the Management of Shared Information Systems

## Part A

### A1 Issue Record

Issue	Date	Comments
One	June 2002	Original Document

This document supports [GE/RT8054](#), 'Management of Shared Information Systems', and 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 does not supersede any other Railway Safety Approved Code of Practice.

This document quotes, verbatim and boxed, the mandatory sections of [GE/RT8054](#) and, following each portion of quoted text, gives relevant recommendations and guidance in italics.

### 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 Safety Approved Codes of Practice are non-mandatory documents, providing a recommended method of meeting the requirements of a Railway Group Standard, either in whole or in part.

\* 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.

### 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.

# Recommendations for the Management of Shared Information Systems

## Part B

### B1 Purpose

This document supports Railway Group Standard [GE/RT8054](#), and provides recommendations for managing shared **information** systems that process safety **information**.

The purpose of [GE/RT8054](#) is to ensure that **information** systems identified as shared **information** systems that process **information** used for the safe operation and interworking of trains, are managed to standards achieving the appropriate integrity and availability of **information** for the safety use involved.

These **information** systems will invariably be computer based. See Figure 1 in Appendix A of this document.

### B2 Application of this document

#### B2.1 To whom the recommendations apply

This document contains recommendations that 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

The recommendations of this Railway Safety Approved Code of Practice 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.

Railway Group Standard [GE/RT8054](#) deals with the responsibility of Railway Group members, including responsibility for use by their contractors, where the Railway Group member will need to establish arrangements with those who are not Railway Group members but are supplying or using data on their behalf. This will enable the Railway Group member to fulfill their Railway Group obligations.

A shared **system** is one where one Railway Group member depends on another for data; and where the data is not transferred directly, but is mediated by a **system**. It is this complex form of interdependence which the Railway Group Standard is designed to control. It does not apply to any situations where the relationship between the Railway Group members is confined to that of IT supplier and client. It applies to situations where one Railway Group member inputs and another extracts.

#### B2.2 Scope

The form of the IT arrangements within the **system** is not relevant. They may be mainframe-based or distributed. They may be uniform or diverse.

**Information system** boundaries are set (for the purposes of Railway Group Standard [GE/RT8054](#)) by the manual processes of data input and extraction. Two **information** systems separated by manual extraction and re-entry of data do not count as one **information system** for the purposes of [GE/RT8054](#).

Within these outer boundaries of manual processes, it will often be convenient to define more than one **information system** (IS) for the purposes of preparing **System** Safety Implication Statements and **System** Safety Case(s). How this is

## Recommendations for the Management of Shared Information Systems

done is a matter of judgement and agreement between those Railway Group members that are users.

### B2.3 Software

Software, such as a proprietary word processor package, is in scope if it forms part of a shared **information system**, in terms of its role in that IS. The fact that no Railway Group member controls the code of such IT systems does not put it out of scope; Railway Group members need to address issues such as choosing between alternative software options, handling of software upgrades, recognising and controlling software weaknesses.

### B2.4 Communications

Pure communications systems such as NRN, and alarm systems, are excluded, however, the communications links forming part of shared **information systems** are to be taken into account in assessing safety implications and preparing **System Safety Cases**.

### B2.5 Storage-only systems

A shared **system** is one where at least one Railway Group member inputs data and at least one (different) Railway Group member extracts data. Hence a **system** where the only functions of the IT are to receive, store and make available data (ie without processing the data) is within scope only if at least one Railway Group member inputs data and at least one Railway Group member extracts data. Even if no Railway Group member controls the IT **system**, and the IT **system** makes no change to the data, there are still issues to be considered such as input data quality, understanding of definitions by the extractor, IT **system** availability and security.

### B2.6 Distributed systems

Where an **information system** runs by means of IT systems which are distributed, it can still be a shared **information system**.

### B2.7 Interface specifications

The relevance of an interface specification to the definition of an **information system**, for the purposes of Railway Group Standard **GE/RT8054**, is that it provides for electronic data flow between Railway Group members, and hence does not constitute a necessary boundary to the **information system** (although it may be appropriate and convenient to treat it as dividing the **information system** into two **information systems**, for the purposes of preparing **System Safety Implication Statements/System Safety Cases**).

### B2.8 Identifying and defining IS for the purposes of the Standard

An **information system** has its natural boundaries where data is input or extracted manually. An **information system** (for the purposes of **GE/RT8054**) cannot extend over such a boundary.

It will often be convenient to define more than one **information system** within those natural boundaries. For example, RSL, RAVERS, TOPS and the timetabling group of systems intercommunicate electronically, but they are managed separately, and it is convenient for the purposes of Railway Group Standard **GE/RT8054** to treat them as four different shared **information systems**.

The boundaries of IT systems, as defined for IT purposes, have no status for the purposes of Railway Group Standard **GE/RT8054**, except where it is decided for managerial convenience to divide one **information system** into two or more. In such cases it would normally be sensible to place the precise boundary by reference to IT considerations.

It follows from this that an IT **system** can be part of a shared **information system** for the purposes of the **GE/RT8054**, even if it has only one user who is a direct Railway Group member. If it connects electronically to other Railway Group members, it will be shared.

# Recommendations for the Management of Shared Information Systems

## 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.

*Figure 1 in Appendix A of this document identifies in diagrammatic form what is meant by the term 'information system'. Such information systems will usually involve the use of computer systems.*

## Recommendations for the Management of Shared Information Systems

### B4 General requirements

Railway Group members shall:

- a) identify those **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
- 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.

*Some owners of computer systems within an **information system** are not Railway Group members and therefore have no direct role in the Railway Group Standard process. Some **information** systems contain computer systems with several owners. In addition, computer **system** issues do not have an inherent primacy in terms of possible malfunctions of the **information system** or their controls.*

*Railway Group Standard [GE/RT8054](#) does not mandate a process for identifying or appointing a lead Railway Group member for fulfilling the obligations of the Group Standard. In requiring Railway Group members to co-operate, the Standard ensures that users decide if they wish to appoint or agree a lead organisation and how they will take that decision. There are important **information** systems where all of the Railway Group members' users are of similar size and status, and the infrastructure controller is not a user. There are others where the infrastructure controller is a relatively minor user, and there is no single user who might be seen as having primacy in terms of fulfilling the obligations of the Railway Group Standard.*

*Railway Group Standard [GE/RT8054](#), whilst not mandating a process for identifying or appointing a lead Railway Group member, for fulfilling the obligations of the Standard, does expect Railway Group members to co-operate. Each Railway Group member has to determine its process for management and use of **information** systems, how they will co-operate with other Railway Group members, and who will represent their interest.*

*Co-operation in fulfilling the obligations of the Railway Group Standard brings clarity to the process of managing individual **information** systems. Without co-operation, Railway Group members using **information** systems would still need to prepare and gain endorsement or acceptance of **System** Safety Implication Statements and **System** Safety Cases for systems they use.*

*Railway Group members need to be able to demonstrate that they have complied with Railway Group Standard [GE/RT8054](#), and that their use of shared*

# Recommendations for the Management of Shared Information Systems

*information systems is, and remains, appropriate. Documentation to support this demonstration includes:*

- a) descriptions of management processes and procedures controlling application and risk
- b) **System** Management Group records
- c) response to review of a **System** Safety Implication Statement/**System** Safety Case
- d) specifications for the **system**.

*This list is not exhaustive.*

## 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.

*Railway Group members who use safety **information** from a shared **information system** as part of their business processes, remain responsible for the safety integrity of their business process.*

*Whilst this document applies to shared **information** systems, that is not to say that single user systems are not important. It is, however, for Railway Group members to manage the latter within their management responsibilities - as they would for other railway safety case obligations. The overall responsibility for single user systems thus rests with the using organisation. These may be managed in line with the general processes contained in this document, but totally within the using organisation. However, with shared systems, arrangements are more complex and require a wider management, hence the requirements contained in this document.*

*Clearly, both direct and indirect users of a computer **system** should be identified by asking the computer **system** provider. It is important to recognise that the need to identify indirect users relates only to data with a material safety implication.*

*Having identified all of the **information** systems they use, Railway Group members will need to identify what computer systems these contain and whether another Railway Group member uses the latter in any way.*

*As **information** systems are liable to change, there is no list of systems covered by the Railway Group Standard. Each Railway Group member is best placed to identify those **information** systems it uses.*

*Consideration should be given to the fact that **information** from a computer **system** that is not shared may still feed another computer **system**, and the computer **system** to which **information** is being passed may have a safety implication. It may, for example, be a control **system**. It may be a **system** not used directly by a Railway Group member, but one used by a contractor to a Railway Group member.*

*These **information** interfaces, where there is a material safety implication (see section B6) within the scope of GE/RT8054, need to be identified so that the*

## Recommendations for the Management of Shared Information Systems

*overall arrangements can be effectively managed within the requirements of this document.*

### 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
- 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).

*Endorsement of a **System** Safety Implication Statement by the **System** Management Group signifies that the **System** Safety Implication Statement adequately characterises every user organisation's own safety use and the extent of reliance they place on the **system**. Endorsement also signifies that the procedures described for maintaining the **System** Safety Implication Statement will be applied.*

*For Railtrack-owned systems, Railtrack appoint a business **system** owner with the responsibility of supporting users and the user group (acting as the **system**'s **System** Management Group) in producing and maintaining the **System** Safety Implication Statement and **System** Safety Case (where appropriate).*

*For systems not owned by Railtrack, it will be necessary for users to agree how the task of performing the necessary activities to produce and maintain these documents is to be performed. Users who are Railway Group members are each responsible for ensuring that arrangements to achieve this are established.*

# Recommendations for the Management of Shared Information Systems

*In assessing whether a safety implication is material, a view is to be taken on whether there is a real prospect of harm arising (eg from a **system** malfunction) given the checks, competencies and other controls that exist in the business processes that use the **information**.*

An **information system** malfunction includes :

- a) total or partial unavailability of the **system**
- b) mis-recording, loss, or corruption of data
- c) mis-selection, incorrect summation or other incorrect manipulation or calculation of **information**
- d) incorrect or insufficient entry or failure to provide data when required
- e) incorrect or inadequate documentation, description or specification of **information** within the **system**.

*This list is not exhaustive.*

*As it is for a Railway Group member to determine how they fulfil the requirements of this Group Standard there is no predetermined template for a **System** Safety Implication Statement. However the infrastructure controller's SRP deals with systems on this basis – see Section B10.*

## 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.

*Systems owned by Railtrack and falling under the infrastructure controller's Railway Systems Code have a user group, which acts as the **System** Management Group for the purposes of this document.*

*Where a shared **information system** does not have a user group under infrastructure controller's arrangements, it is for users to agree and arrange that a body take the role of a **System** Management Group. This body may be an existing management group, or stakeholder group, provided it has (or is given) an appropriate remit. Users who are Railway Group members are each responsible for ensuring that a **System** Management Group is established.*

*The **System** Management Group arrangements do not change the substantive risk management responsibility which remains with the user organisation.*

### 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.

*The interests of each user need to be represented, but not necessarily in person, on each **System** Management Group. Potential users need to be directed to the **System** Management Group to determine how their interests will be handled. Members of a **System** Management Group are not necessarily safety experts assessing and approving documents and the **system** they describe. This is the job of appropriate specialists in the organisations involved.*

## Recommendations for the Management of Shared Information Systems

### 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 objectives 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.

*The following additional aspects may be considered in determining the remit of **System** Management Groups:*

- a) *determining the formation and membership of the **System** Management Group, to provide a focus for all types of user of the **information** systems that the **System** Management Group represent*
- b) *frequency of meetings*
- c) *identifying future **system** development and/or enhancement*
- d) *determining **system** allowed outage time periods*
- e) *determining the disaster recovery timescale for systems*
- f) *assisting users in awareness, training and competence requirements as an aid to effective and safe use of systems and their output.*

*This list is not exhaustive.*

*As far as membership is concerned, the **System** Management Group should aim to have a mix of expertise. Specialist computer **system** expertise can be provided by the computer **system** supplier, so would not normally be expected of the members of the **System** Management Group. Specialist safety and risk analysis expertise should be provided by application of the process for drafting the **System** Safety Implication Statement/**System** Safety Case and would not, therefore, normally be expected of members of the **System** Management Group. What is important is knowledge of the uses to which the data is put and of the sources from which the data comes. **System** Management Groups are*

# Recommendations for the Management of Shared Information Systems

*defined as multi-purpose groups, so require knowledge of both safety and non-safety applications. It is because no one member can bring the whole range of expertise that a group is necessary.*

## **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.

*Specialist aspects relating to computer technology may be referred to an appropriate professional body, eg The British Computer Society, or Computer Systems and Services Association.*

*Issues affecting safe operation and interworking of trains may also be referred to Railway Safety, for guidance.*

## **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 needs to 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**.

## Recommendations for the Management of Shared Information Systems

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.

*The processes and procedures set out in the **System** Safety Case need to ensure that:*

- a) *the roles and responsibilities of the various parties are clear*
- b) *the processes for the provision, operation, access, data input, data output, development, change and fault correction are suitable and sufficient, given the identified risks from use, so that:*
  - i) *risks arising from the use of the **system** that can be controlled through the management of the **system** are at an acceptable level*
  - ii) *problems that have the potential to prejudice safety are identified and communicated in a timely manner to users who may be affected – including users via other systems. This can only apply to those users that can be identified as using a **system** by a Railway Group member. Where systems are used in the public domain, it would be appropriate to publish at what date the **system** was last updated and the authority for change.*

*It is important that users of **information** systems can be sure that their safety-related uses are not more reliant on the **information system**, than can be justified by a reasonable expectation of the **information system** performance. This can be achieved by:*

- a) *demonstrating an appropriate relationship between the assessed vulnerability of the business process and the applied controls*
- b) *having adequate arrangements to ensure that the integrity of the **system** (including the **information** obtained from it) and users' reasonable expectations of that integrity match.*

*The **System** Safety Case sets out the management arrangements. This does not constitute technical documentation, but addresses how **system** performance and safety reliance can be maintained in an appropriate relationship. The **System** Safety Case also needs to set out the arrangements that assist Railway Group members in:*

- a) *understanding the expected performance of an **information system***
- b) *understanding their obligations with regard to the **information system** in relation to data being wrong or not available, and also of the reliance placed by users on that data for safety use in the event of it being wrong or not available*
- c) *influencing the management of the **information system** and its change, so as to give the necessary reliability and dependability*
- d) *identifying the means by which data and service suppliers have to meet the relevant requirements of the **System** Safety Case (eg by use of a contract specifying obligations, or agreement to parts of the **System** Safety Case).*

*In determining the content of a **System** Safety Case, aspects that need considering are:*

# Recommendations for the Management of Shared Information Systems

- a) the potential risks of a **system** on the safe operation and interworking of trains
- b) how the safety implication of any computer **system** forming part of an **information system** has been assessed (see section B6)
- c) the assessment of the potential risk of use of the output from the **system**, possibly by direct link with other non-shared systems, on the safe operation and interworking of trains, and the safety of those on and adjacent to the railway. Consideration is to include the use of specialist techniques, where appropriate
- d) the functional design specification of the contained computer **system(s)**
- e) the clarity of software definition and documented requirements
- f) the specified management processes and procedures, controlling the complete **information system** arrangements, the contained computer **system(s)**, and the identified risks arising from use of the **information system**
- g) the procedures and controls that have been established to handle and ensure the accuracy and timeliness of **system** input data, and the correct use of output data
- h) the means of achieving and maintaining competence of those, including **system** suppliers, involved with **information** systems
- i) the maintenance and operational arrangements applied to the contained computer **system(s)**
- j) the need to retain records of the decision-making processes and decisions made
- k) the means of regularly reviewing the **system** and its management, taking into account its performance, data issues and changes in use
- l) how a computer **system** forming part of an **information system** is changed.

This list is not exhaustive.

The degree of detail necessary in a **System** Safety Case will vary according to the scope, structure and safety implication of the **information** provided, either by the **system** itself or through other systems using data supplied from that **system**.

It is important that users of shared **information** systems are given an opportunity to comment on drafts of the **System** Safety Case as this is developed, particularly the final draft. It is also important that users recognise the need to give comments/agreement within a reasonable timescale to enable an effective process.

Where an organisation, not a Railway Group member, uses **information** supplied from a shared **information system**, subject to a **System** Safety Case, responsibility for this use is theirs. If that **information** is supplied to a Railway Group member, that member will need to ensure that the requirements of [GE/RT8054](#) are applied to that provision.

For example, with regard to output from shared **information** systems and the responsibility of a Railway Group member to users who are not Railway Group members, it is appropriate that recognition is given to:

- a) health and safety obligations to consult (with output users when preparing a **System** Safety Case) and take account of their input

## Recommendations for the Management of Shared Information Systems

- b) *the need, in relation to health and safety, to make those that are not Railway Group members aware of the provisions of the **System** Safety Case, to enable the latter to take them into account*
- c) *the need for those that are not Railway Group members to satisfy themselves that the **information** they use is fit for those purposes that only they can authoritatively identify*
- d) *the fact that **information** (or a **system**) may be used by a non-Railway Group member at the behest of a Railway Group member.*

*This would involve, for example, the **information system** supplier being closely involved in development of the **System** Safety Case and agreeing with its content.*

*Where a user is not a Railway Group member, it is for Railway Group members to obtain any necessary agreement of that user to the **System** Safety Case.*

*As it is for Railway Group members to determine how they fulfil the requirements of Railway Group Standard **GE/RT8054**, there is no predetermined template for a **System** Safety Case. However, the infrastructure controller's SRP deals with systems on this basis – see Section B10.*

### 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**.

*The Code of Practice for the Management and Development of Railway Code Systems produced by Railtrack, and the corresponding Traction and Rolling Stock Code, are adequate to fulfil the requirements of section B9.*

*Notification to all users is important when common interfaces and data standards are used. It enables preparation for any unexpected problems that may arise when these changes are made, and it also enables changes to be made to associated business management processes and procedures.*

### 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.

# Recommendations for the Management of Shared Information Systems

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.

*Railtrack, as the owner of many shared systems, have for this purpose established an independent body known as the **System Review Panel - Information Systems (SRP-IS)** under its Rolling Stock Acceptance Board.*

## 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 appropriate 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.

*Provision of adequate security is important in ensuring that the controls applied, commensurate with the safety implication, are not undermined. It is also important that incidents, including near misses involving these systems, are recorded, and that the cause and response are analysed to identify how future arrangements might be improved.*

*Planned outages and the control of unplanned outages need to be managed to ensure that the safety implications are properly considered and addressed in the response.*

# Recommendations for the Management of Shared Information Systems

## Appendix A Information systems

The following diagram, Figure 1, illustrates what is meant by an *information system* in the context of this document and the Standard GE/RT8054. It incorporates the:

- computer *system* and programs that hold and process the data
- infrastructure on which the computer *system* runs
- operational, maintenance, change and incident response
- data input and output
- support processes and procedures.

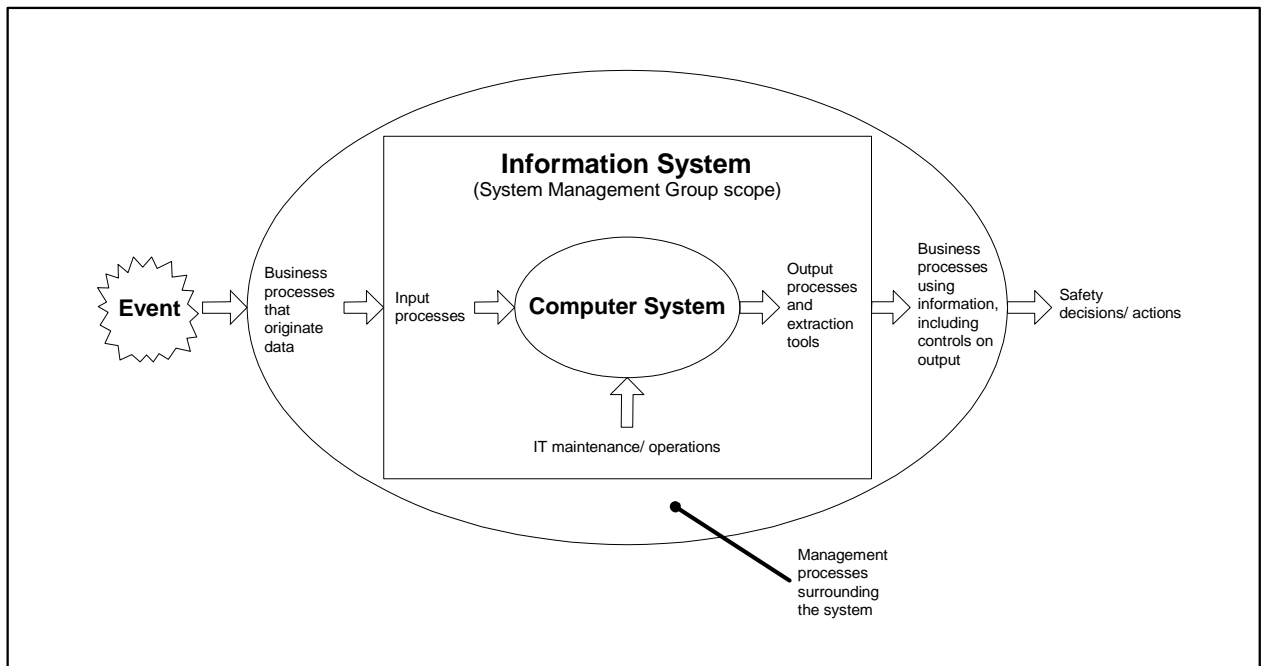


Figure 1

# Recommendations for the Management of Shared Information Systems

Railway Safety Approved Code of Practice

GE/RC8554

Issue One

Date June 2002

Page 17 of 17

## References

- Railway Group Standards**
- GA/RT6001** Railway Group Standards Change Procedures
  - GA/RT6004** Temporary Non-Compliance with Railway Group Standards
  - GA/RT6006** Derogations from Railway Group Standards
  - GE/RT8054** Management of Shared **Information** Systems

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.