Rail Industry Standard
RIS-0707-CCS
Issue One
Date September 2016

Management of Safety Related Control, Command and Signalling System Failures

Synopsis

This standard sets out requirements for sharing information about safety related failures of the control, command and signalling (CCS) system.

Published by:

RSSB

Issue record

Issue	Date	Comments
One	September 2016	Original document

Superseded or replaced documents

The following Railway Group Standard is superseded or replaced, either in whole or in part as indicated:

Superseded documents	Sections superseded	Date when sections are superseded
GERT8106 issue two Management of Safety Related Control, Command and Signalling (CCS) System Failures	All	03 September 2016

GERT8106 issue two Management of Safety Related Control, Command and Signalling (CCS) System Failures, ceases to be in force and is withdrawn as of 03 September 2016.

Supply

The authoritative version of this document is available at www.rssb.co.uk/railway-group-standards. Enquiries on this document can be forwarded to enquirydesk@rssb.co.uk.

Contents

Management of Safety Related Control, Command and Signalling System Failures

Part 1 Introduction

1.1 Purpose of this document

1.1.1 This document is a standard on the Management of Safety Related Control, Command and Signalling (CCS) System Failures, for members of RSSB to use if they so choose.

1.2 Background

1.2.1 The requirements in GERT8106 issue two set out requirements for infrastructure managers and railway undertakings to share information about safety related failures of CCS systems. The requirements are also relevant to the development of a cross-industry Defect Recording Analysis and Corrective Action System (DRACAS).

1.2.2 GERT8106 issue two was notified as a National Safety Rule (NSR). However, the requirements had been identified as not being valid as NSRs in accordance with the rule management tool included in Annex 3 of the final report of the European Rail Agency's Task Force on National Safety Rules. GERT8106 issue two was therefore formally 'redundant' as an NSR, and therefore also as a Railway Group Standard. As a consequence, it has been withdrawn.

1.2.3 GERT8106 issue two has therefore been replaced by this Rail Industry Standard (RIS-0707-CCS Rail Industry Standard for the Management of Safety Related Control, Command and Signalling System Failures), which reproduces the relevant text of GERT8106 issue two in its entirety as Annex A.

1.3 Application of this document

1.3.1 A member of RSSB may choose to adopt all or part of this document through internal procedures or contract conditions. Where this is the case the member of RSSB will specify the nature and extent of application.

1.3.2 Therefore compliance requirements and dates have not been specified since these will be the subject of internal procedures or contract conditions.

1.3.3 The Standards Manual does not currently provide a formal process for deviating from RISs. However, a member of RSSB, having adopted a RIS and wishing to deviate from its requirements, may request a Standards Committee to provide observations and comments on their proposed alternative to the requirement in the RIS. Requests for opinions and comments should be submitted to RSSB by e-mail to proposals.deviation@rssb.co.uk. When formulating a request, consideration should be given to the advice set out in the 'Guidance to applicants and members of Standards Committee on deviation applications', available from RSSB's website.

1.4 Health and safety responsibilities

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

1.5 The structure of this document

1.5.1 The requirements of this RIS are the requirements set out in Annex A

1.6 Approval and authorisation of this document

1.6.1 The content of this document was approved by Control Command and Signalling Standards Committee on 14 April 2016.

1.6.2 This document was authorised by RSSB on 26 July 2016.

Annex A. Text of GERT8106 Management of Safety Related Control, Command and Signalling System Failures, issue two

Management of Safety Related Control, Command and Signalling System Failures

Part 1 Purpose and Introduction

1.1 Purpose

1.1.1 This standard mandates the requirements for sharing information relating to reported safety related failures of control, command and signalling (CCS) systems between infrastructure managers and railway undertakings when the complete system includes both a trainborne CCS equipment sub-system and an infrastructure equipment CCS sub-system. This is to ensure that sufficient, timely and relevant information about failures is available to support a failure management process, with the aim of establishing the cause of each failure so that the necessary corrective action is taken.

1.1.2 The purpose of this standard is to ensure that:

a) Necessary information about safety related failures of these CCS systems is shared by railway undertakings and infrastructure managers

b) Shared information is correctly communicated so that it can be used by railway undertakings and infrastructure managers when decisions are taken to return assets to operational use following completion of failure investigations

c) Implementation of new CCS systems and each duty holder's responsibility for the equipment in their control is supported by a defect reporting analysis and corrective action system (DRACAS).

1.2 Introduction

1.2.1 Background

1.2.1.1 GE/RT8000, the Rule Book, sets out the requirements for managing safe railway operations when failure symptoms are detected in CCS systems. Compliance with the Rule Book requires that:

a) Detected failure symptoms are correctly reported to the signaller by the infrastructure manager and railway undertaking personnel

b) The appropriate action is taken to protect the operational railway during times of failure, for example disconnection or application of a restriction to defective equipment

c) CCS systems are only returned to normal operational use when it is safe to do so.

1.2.1.2 Safety related failures of CCS systems, where complete systems are made up of equipment that is wholly operated by a single infrastructure manager or railway undertaking, are managed by the system operator.

1.2.1.3 Where CCS systems include an infrastructure manager CCS sub-system and a railway undertaking CCS sub-system, a failure symptom detected in either of the sub-systems can result from an equipment malfunction anywhere within the complete system. A full list of these systems is given in Appendix A. Safety related failures of these CCS systems are managed by the operators of both sub-systems.

1.2.1.4 The information that is shared by infrastructure managers and railway undertakings is specified in this standard.

1.2.1.5 The requirements of this standard are in addition to those contained in GE/RT8047 Reporting of Safety Related Information. GE/RT8047 relates to information reported to the Safety Management Information System (SMIS).

1.2.1.6 The requirements of this standard are in addition to those contained in GE/RT8250 Reporting High Risk Defects, to notify other infrastructure managers and railway undertakings when notification of a safety related failure is required.

1.2.1.7 The requirements of this standard are in addition to those contained in GO/RT3437 Defective On-Train Equipment.

1.2.1.8 The requirements of this standard are in addition to those contained in GO/RT3119 Accident and Incident Investigation.

1.2.2 Principles

1.2.2.1 A set of processes is required by railway undertakings and infrastructure managers for establishing the primary and root causes of reported safety related failures of the CCS system to enable the necessary corrective action to be taken. This is so that the system is fit for service when it is returned to normal operational use.

1.2.2.2 Railway undertakings are responsible, as part of their safety management system, for managing failures that could have been caused by defective trainborne equipment.

1.2.2.3 Infrastructure managers are responsible, as part of their safety management system, for managing failures that could have been caused by defective infrastructure equipment.

1.2.2.4 The information to be shared about failures is to be managed consistently by railway undertakings and infrastructure managers. Appendices B1 and B2 present a typical example of the information sharing involved in the failure management process set out in Part 2.

1.2.2.5 The information shared by infrastructure managers and railway undertakings is to be accurate, traceable, relevant, complete and comprehensible. This is so that infrastructure managers and railway undertakings have the necessary information to take safety related decisions about whether or not to return CCS equipment to normal operational use.

1.2.2.6 The final decision to return CCS equipment to normal operational use (such that all or part of the CCS system is returned to normal operational use) is the sole responsibility of the infrastructure manager or railway undertaking that operates the equipment, having established that it is safe to do so.

1.2.2.7 The figure in non-mandatory Appendix C shows typical infrastructure manager and railway undertaking organisational structures and the communication links that would support the requirement to share information about CCS system failures.

1.2.2.8 The infrastructure manager and railway undertaking processes should include the main interactions between and within organisations, so that sufficient information about failure investigations is made available to establish the causes of CCS system failures.

1.2.3 Related requirements in other documents

1.2.3.1 The following Railway Group Standard contains requirements that are relevant to the scope of this document, to ensure the reporting of failures:

GE/RT8000	Rule Book

Part 2 Requirements for managing information about control, command and signalling (CCS) system failures

2.1 Classification of CCS system failures

2.1.1 Classifying reported failures

2.1.1.1 Safety related failures of CCS systems that include an infrastructure manager CCS sub-system and a railway undertaking CCS sub-system, shall be classified by the infrastructure manager and the railway undertaking using the classifications specified in Appendix A, unless:

a) The failure symptom was detected by the infrastructure manager and it is confirmed that it is an infrastructure equipment failure and no trainborne CCS equipment is involved, or

b) The failure symptom was detected by the railway undertaking and it is confirmed that it is a trainborne equipment failure and no infrastructure CCS equipment is involved.

2.1.1.2 Failures shall be initially classified before commencement of failure investigation so that an appropriate failure response plan is implemented.

2.1.1.3 If it is not possible to confirm the appropriate failure classification from the reported failure symptom, the highest of the considered classifications shall be used until further evidence justifies a different classification.

2.1.1.4 If a reported failure symptom is not included in Appendix A, the failure shall be classified as safety related (high risk) unless a lower initial classification can be justified from the failure symptoms. In this case the railway undertaking or infrastructure manager shall submit a proposal defining the classification.

2.1.1.5 The process for submitting a proposal for a change to Railway Group Standards is set out in RGSC 01 Railway Group Standards Code.

2.1.2 Updating failure classifications as a result of failure investigation

2.1.2.1 When failure investigation by either party finds evidence that justifies a different failure classification to the classification originally used, that party shall share information about the evidence with the other party before the failure classification is updated.

2.1.2.2 When failure investigation by either party concludes that a CCS system failure has not occurred (for example, due to operator error or an erroneous report), and information has been received from the other party that a failure has not occurred, the failure shall be reclassified as ‘not a failure’, subject to the following criteria being met:

a) The evidence arising from failure investigation shows that the failure symptom was not the result of a CCS infrastructure equipment failure or a CCS trainborne equipment failure, and

b) The failure symptom was not the result of a systematic failure, for example, due to a design error.

2.2 Communication of information about CCS system failures

2.2.1 Requirements for communication systems

2.2.1.1 Infrastructure managers and railway undertakings shall implement one or more dedicated failure reporting facilities that are contactable 24 hours a day, for the purpose of communicating information about safety related failures.

2.2.1.2 Infrastructure managers and railway undertakings shall provide details to each other of:

a) The failure reporting facility to be used when information about safety related failures is to be communicated between organisations, and

b) The methods of communication to be used for transfer of information between organisations.

2.2.1.3 Infrastructure managers and railway undertakings shall implement communication systems that are capable of sending and receiving information about CCS system and equipment failures between the failure reporting facilities in normal, degraded and emergency operational situations.

2.2.1.4 The communication systems shall be capable of transmitting all of the information required to manage safety related failures of CCS systems and equipment in the required formats and media, including written, verbal and electronic information.

2.2.1.5 Infrastructure managers and railway undertakings shall put arrangements in place to ensure that:

a) A specified sequence of activities is consistently implemented to support investigation, resolution and closure of safety related failures

b) The requirement for information to be shared with other infrastructure managers and railway undertakings is correctly followed

c) Information about safety related failures is correctly transmitted to other infrastructure managers and railway undertakings using the agreed methods of communication and at the earliest opportunity.

2.2.1.6 Where information is to be shared automatically between electronic databases:

a) Railway undertaking databases shall be capable of pushing data that meets the requirements of 2.2.3.5

b) Infrastructure manager databases shall be capable of pushing data that meets the requirements of 2.2.3.6

c) Railway undertaking and infrastructure manager database management activities shall include provision of an error log to record whenever electronic data transfer is unsuccessful.

2.2.1.7 Infrastructure managers and railway undertakings shall check that information received is correct, accurate, complete and comprehensible.

2.2.1.8 Whenever transmission of the information is unsuccessful, or the received information is incomprehensible, corrupted or is suspected to be incorrect or incomplete, the infrastructure managers and railway undertakings concerned shall repeat the transfer of information to ensure that the transfer of information is correctly completed.

2.2.2 Identification of safety related failures

2.2.2.1 In order to ensure that information about safety related failures is traceable to the corresponding failure record, infrastructure managers and railway undertakings shall identify each reported failure using a failure specific alphanumeric failure identifier.

2.2.2.2 Infrastructure managers and railway undertakings shall share details about how the failure identifiers are structured. The failure identifier(s) shall support traceability of each failure record to:

a) The infrastructure manager or railway undertaking owning the failure record

b) The date of the failure

c) The failure reference.

2.2.2.3 The failure identifier(s) shall be applied by the infrastructure manager and railway undertaking whenever a safety related failure is reported, including reported allegations of safety related failures, and safety related failures found during in-service maintenance and testing.

2.2.2.4 The failure identifier(s) shall be incorporated into all information about safety related CCS failures that is shared between infrastructure managers and railway undertakings.

2.2.2.5 Infrastructure managers and railway undertakings shall use the failure identifier(s) to ensure that information that is sent and received is assigned to the correct failure record.

2.2.3 Communicating information about safety related failures

2.2.3.1 Infrastructure managers and railway undertakings shall ensure that, when reported safety related failures of the CCS system is suspected to involve any railway equipment under the control of the other party, details are brought to the attention of that party at the earliest opportunity.

2.2.3.2 Information about the action being taken and the expected duration of the initial failure investigation shall be shared by the infrastructure manager and railway undertaking at the earliest opportunity after the failure has been reported.

2.2.3.3 Infrastructure managers and railway undertakings shall share information as soon as it is available:

a) About the conclusions of the initial failure investigation, and

b) When the result of any follow-up investigation has implications at the technical interface that can impact on another infrastructure manager or railway undertaking.

2.2.3.4 An example of a typical failure investigation, showing when information is shared, is set out in Appendices B1 and B2. An example failure data collection form is set out in Form RT8106 which is available on www.rssb.co.uk.

2.2.3.5 Railway undertakings shall share the following information with the infrastructure manager:

a) The failure identifier assigned by the railway undertaking

b) The failure classification applied by the railway undertaking

c) The system description, for example TPWS

d) The reported failure symptom

e) The time and date of the failure

f) The train head-code, when the train is in service at the time of failure

g) The rolling stock and vehicle type

h) The rolling stock set identification, vehicle identification and cab identification

i) The equipment serial number (to support component traceability)

j) The location, in terms of railway geography, where the failure symptom was detected

k) The results of the initial failure investigation by the railway undertaking, including any reports of ‘no fault found’

l) The results of any follow-up investigation with implications that affect the technical interface with the infrastructure manager

m) The actions taken by the railway undertaking to rectify the failure

n) The conclusion arising from completion of the failure investigation in terms of whether the reported failure was caused by railway equipment operated by the railway undertaking.

2.2.3.6 Infrastructure managers shall share the following information with the railway undertaking or other infrastructure manager:

a) The failure identifier assigned by the infrastructure manager

b) The failure classification applied by the infrastructure manager

c) The system description, for example TPWS

d) The reported failure symptom

e) The time and date of the failure

f) The identification of the infrastructure asset

g) The location, in terms of railway geography, of the asset

h) The train head-code whenever a train is a possible cause of system failure

i) The results of the initial failure investigation by the infrastructure manager, including any reports of ‘no fault found’

j) The results of any follow-up investigation with implications that affect the technical interface with the railway undertaking

k) The actions taken to rectify the failure

l) The conclusion arising from completion of the failure investigation in terms of whether the reported failure was caused by railway equipment operated by the infrastructure manager.

2.2.3.7 Where information that has been shared is subsequently updated by an infrastructure manager or railway undertaking, the updated information shall be shared at the earliest opportunity.

2.2.4 Management of CCS system failures where the failure investigations conducted by the railway undertaking(s) and infrastructure manager have not identified a fault with either the infrastructure or trainborne sub-systems

2.2.4.1 The infrastructure manager and railway undertaking(s) shall jointly decide the appropriate course of action necessary to identify and address CCS system faults when all of the following apply:

a) Failure investigation concludes that both the trainborne sub-system and the infrastructure sub-system are operating within the parameters specified in the relevant functional and operational specifications

b) Nothing has been found to confirm that the CCS system failure was caused by other railway equipment

c) There are at least two occurrences of no fault found reports for this failure mode.

2.3 Failure management requirements for new CCS systems

2.3.1 Requirements for DRACAS

2.3.1.1 Infrastructure managers and railway undertakings shall incorporate a defect reporting analysis and corrective action system (DRACAS) as part of all projects that implement new CCS systems.

2.3.1.2 The infrastructure manager and railway undertakings shall use DRACAS to:

a) Implement the requirements for communicating information about CCS system failures set out in section 2.2.

b) Compare the predicted system reliability with actual reliability across all applications of the systems

c) Compare the predicted system failure symptoms with failure symptoms experienced during system operation

d) Analyse system failure and performance data to identify the root causes of system failures

e) Identify whether the root cause is technical or operational in nature

f) Identify whether a technical root cause is associated with trainborne equipment or infrastructure equipment

g) Support decisions about the corrective actions necessary to improve system performance.

Appendix A. Classification of failures of control, command and signalling (CCS) systems that include a trainborne sub-system

The content of this appendix is mandatory

A.1 A.1 Classification scheme

A.1.1 Safety related failures of CCS systems, including reported failure allegations and failures found during in-service maintenance and testing, shall be classified into one of three categories:

1) Safety related failures (high risk)

2) Safety related failures (low risk)

3) Other failures (negligible risk).

A.1.2 Tables A.1 to A.13 on the following pages set out the failure classification that shall be applied to the failure symptoms exhibited by trainborne control, command and signalling equipment:

Table A.1 Automatic Warning System (AWS) failures

Table A.2 Train Protection and Warning System (TPWS) failures

Table A.3 Great Western and Chiltern Automatic Train Protection System (ATP) failures

Table A.4 TVM430 Cab Signalling System failures

Table A.5 European Train Control System (ETCS) failures. (Note: ETCS failure classifications will be addressed when the information becomes available)

Table A.6 Mechanical train stop failures

Table A.7 Train detection system failures (including track circuit, axle counter, treadle, depression bar)

Table A.8 Cab Secure Radio (CSR) failures

Table A.9 National Radio Network (NRN) failures

Table A.10 Radio Electronic Token Block (RETB) failures

Table A.11 Interim Vehicle Radio System (IVRS) failures

Table A.12 Global System Mobile – Railway (GSM-R) failures

Table A.13 Tilt Authorisation and Supervision System (TASS) failures

Failure symptom	**Failure classification**		
	Safety related (High Risk)	Safety related (Low Risk)	Negligible Risk
Horn and bell when clear indication expected (Code 1)			●
Horn instead of bell when clear indication expected (Code 2)			●
No horn or bell when clear indication expected (Code 3)	● If experienced at two consecutive clear signals by the train or by two successive trains at the same signal. Otherwise it shall be allocated a Negligible Risk classification		
Horn and bell when warning indication expected (Code 4)		●	
Bell instead of horn when warning indication expected (Code 5)	●		
Brake without horn when warning indication expected (Code 6)		●	
No indication or brake when warning indication expected (Code 7)	●		
Audible warning received but indicator did not change to yellow and black (Code 7a)		●	
Horn when no indication expected (Code 8)			●
Bell when no indication expected (Code 9)			●
Unable to cancel (Code 10)			●
Indicator not changing to black (Code 11)			●
AWS fails to arm (Code 12)	● If equipment failure is not indicated to the driver. Otherwise it shall be allocated a Low Risk classification		
AWS fails to disarm (Code 13)			●
Other failure	● Unless evidence can justify a lower initial classification		

Table A.1 **Automatic Warning System (AWS) failures**

Failure symptom	**Failure classification**		
	Safety related (High Risk)	Safety related (Low Risk)	Negligible Risk
TPWS fails to activate when required (Code 16)	● Unless the failure is indicated or advised to the signaller prior to the approach of a train in which case the Low Risk classification shall be allocated		
TPWS operates when not required (Code 17)			●
Unable to override train stop using override facilities			●
TPWS trainborne equipment indicated as having failed		●	
Spurious intervention or indication			●
Other failure	● Unless evidence can justify a lower initial classification		

Table A.2 **Train Protection and Warning System (TPWS) failures**

Failure symptom	**Failure classification**		
	Safety related (High Risk)	Safety related (Low Risk)	Negligible Risk
No target speed in main display under restrictive circumstances		●	
No permitted speed indicated		●	
Permitted speed indication higher than it should be	●		
ATP fails to prevent point of danger being passed	●		
ATP fails to initiate adequate brake application	●		
Spurious intervention or indication			●
ATP trainborne equipment indicated as having failed		●	
Unable to initialise the system			●
Unable to isolate the system			●
Cannot enter data			●
Cannot correct data			●
Train will not change level / mode		●	
ATP fails to arm at transition (Code 14)		●	
ATP fails to disarm at transition (Code 15)			●
No speed indication		●	
Frozen display		●	
Unable to reach end of authority			●
Unable to move (no movement authority)			●
ATP trackside equipment indicated as having failed		●	
ATP failure codes displayed, which indicate a fault in the ATP ground equipment			●
Train maximum safe speed greater than permissible	●		
Other failure	● Unless evidence can justify a lower initial classification		

Table A.3 **Great Western and Chiltern Automatic Train Protection System (ATP) failures**

Failure symptom	**Failure classification**		
	Safety related (High Risk)	Safety related (Low Risk)	Negligible Risk
No target speed indicated		●	
No permitted speed indicated		●	
Target speed indication higher than it should be	●		
Permitted speed indication higher than it should be	●		
Target speed indication lower than it should be			●
Permitted speed indication lower than it should be			●
TVM ATP fails to prevent point of danger being passed	●		
TVM ATP fails to initiate brake application	●		
Spurious TVM ATP intervention or indication			●
TVM trainborne equipment indicated as having failed		●	
Unable to initialise the TVM system			●
Unable to isolate the TVM system			●
TVM fails to arm at transition (Code 14)		●	
TVM fails to disarm at transition (Code 15)			●
Unable to move (when proceed on sight should be available)			●
Unable to exceed proceed on sight speed (when permitted speed should be available)			●
Other failure	● Unless evidence can justify a lower initial classification		

Table A.4 **TVM430 Cab Signalling System failures**

Failure symptom	**Failure classification**		
	Safety related (High Risk)	Safety related (Low Risk)	Negligible Risk

Table A.5 **European Train Control System (ETCS) failures**

The table of ETCS failures will be published when information about failure symptoms and failure classifications is available.

Failure symptom	**Failure classification**		
	Safety related (High Risk)	Safety related (Low Risk)	Negligible Risk
Train stop function not activated when fitted signal at danger or where provided as a speed trap function	● Unless the failure is indicated or advised to the signaller prior to the approach of a train in which case the Low Risk classification shall be allocated		
Unable to override / reset train stop using override / reset facilities			●
Spurious intervention			●
Train stop function activated when fitted signal at clear			●
Trainborne train stop equipment indicated as having failed		●	
Trip-cock tester fails to indicate correct trip-cock position			●
Trip-cock tester falsely indicates trip-cock correctly positioned when trip-cock not in correct position	●		
Other failure	● Unless evidence can justify a lower initial classification		

Table A.6 **Mechanical train stop failures**

Failure symptom	**Failure classification**		
	Safety related (High Risk)	Safety related (Low Risk)	Negligible Risk
Train detection system detects track section clear when occupied (SCWO)	●		
Train detection system detects track section occupied when clear (SOWC)		● Unless occupancy of the track section does not initiate a time-critical function in which case a Negligible Risk classification shall be allocated	
Train detection system correctly detects vehicle but indication shows track section clear when occupied		●	
Track section indication shows track section occupied when clear			●
TCA equipment fails in service (indicated to driver)		●	
TCA equipment fails in service (not indicated to driver)	●		
Other failure	● Unless evidence can justify a lower initial classification		

Table A.7 **Train detection system failures (including track circuit, axle counter, treadle, depression bar)**

Failure symptom	**Failure classification**		
	Safety related (High Risk)	Safety related (Low Risk)	Negligible Risk
Driver unable to establish contact with signal box		●	
Driver unable to establish contact (emergency call)	●		
Train initiates false call			●
Call interrupted, but able to re-establish immediately			●
Driver receives call from someone other than the correct controlling signaller	●		
Driver able to answer or receive call intended for another train	●		
Signaller receives call from one train, but indicated as from another	●		
Signaller unable to establish contact with driver		●	
Signaller unable to establish contact with driver (emergency call)	●		
Signaller unable to establish call with PA system		● Where this is a Driver Only Operation (DOO) functional requirement. Otherwise a Negligible Risk classification shall be allocated	
Vigilance alarm not indicated to signaller		● Where this is a Driver Only Operation (DOO) functional requirement. Otherwise a Negligible Risk classification shall be allocated	
Radio fails to switch off when driver’s key removed			●
Loss of designed coverage		●	
Other failure	● Unless evidence can justify a lower initial classification		

Table A.8 **Cab Secure Radio (CSR) failures**

Failure symptom	Failure classification		
	Safety related (High Risk)	Safety related (Low Risk)	Negligible Risk
Driver unable to make or receive calls		●	
Driver unable to set up emergency call	●		
Loss of designed coverage		●	
Other failure	● Unless evidence can justify a lower initial classification		

Table A.9 **National Radio Network (NRN) failures**

Failure symptom	**Failure classification**		
	Safety related (High Risk)	Safety related (Low Risk)	Negligible Risk
Driver unable to accept token			●
Driver unable to give up token			●
Driver receives token already issued to another train	●		
Driver and signaller unable to establish voice contact		●	
Unable to complete set-up procedure			●
Display corrupted	● Unless the corruption is obvious and observed in which case a Low Risk classification shall be allocated		
Other failure	● Unless evidence can justify a lower initial classification		

Table A.10 **Radio Electronic Token Block (RETB) failures**

Failure symptom	**Failure classification**		
	Safety related (High Risk)	Safety related (Low Risk)	Negligible Risk
Driver unable to establish contact with signalling control centre		●	
Driver unable to establish contact (emergency call)	●		
Train initiates false call			●
Call interrupted, but able to re-establish immediately			●
Driver able to answer or receive call intended for another train	●		
Signaller receives call from one train, but indicated as from another	●		
Signaller unable to establish contact with driver		●	
Signaller unable to establish contact with driver (emergency call)	●		
Loss of designed coverage		●	
Other failure	● Unless evidence can justify a lower initial classification		

Table A.11 **Interim Vehicle Radio System (IVRS) failures**

Failure symptom	Failure classification		
	Safety related (High Risk)	Safety related (Low Risk)	Negligible Risk
Driver unable to establish contact with signal box		●	
Driver unable to establish Railway Emergency Call	●		
Driver receives Point-to-Point Voice Call from an unauthorised person	●		
Driver able to answer or receive call intended for another train (Not Broadcast or Group Calls)	●		
Radio display fails to switch off when driver's key removed			●
Driver unable to register before commencing journey (one train affected at location)		●	
Driver unable to register before commencing journey (more than one train affected at location)	●		
Cab radio shows warning message			●
Cab radio shows radio failure message		●	
An unintended Point-to-Point Voice Call is initiated from the train			●
An unintended Railway Emergency Call is initiated from the train		●	
Signaller or driver unable to establish an urgent Point-to-Point Voice Call		●	
Call prematurely terminated, but able to re-establish immediately			●
An unintended DSD alarm is initiated from the train		●	
Signaller or controller unable to establish Railway Emergency Call	●		
Railway Emergency Call does not include all signallers, controllers and trains for area	●		

Table A.12 Global System for Mobile Communications – Railway (GSM-R) failures [cont'd over]

Failure symptom	**Failure classification**		
	Safety related (High Risk)	Safety related (Low Risk)	Negligible Risk
Signaller receives a call which should have been routed to a different signaller		●	
Signaller receives call from one train, but indicated as another	●		
Signaller unable to establish contact with driver		●	
Signaller unable to establish call with PA system on a DOO-P service		●	
Signaller unable to establish call with PA system on a non-DOO-P service			●
DSD alarm not indicated to signaller from a DOO-P service		●	
DSD alarm not indicated to signaller from a non-DOO-P service			●
Loss of designed coverage		●	
Failure of display or buttons on signaller’s or driver’s MMI		●	
Noisy, faint or one-way communications		●	
Wrong stock number displayed			●
Incorrect indication of lead signaller		●	
Incorrect or missing train identity and/or location information shown on incoming call		●	
Incorrect or missing train identity and/or location information shown on train list			●
Network or signaller initiates a false call (of any type)			●
‘Contact Signaller’ message not delivered to correct driver, or signaller unable to send			●
‘Waiting at Signal Message’ not delivered to correct signaller, or driver unable to send		●	
‘Wait’ message not delivered to correct driver, or signaller unable to send			●
Other failures	● Unless evidence can justify a lower initial classification		

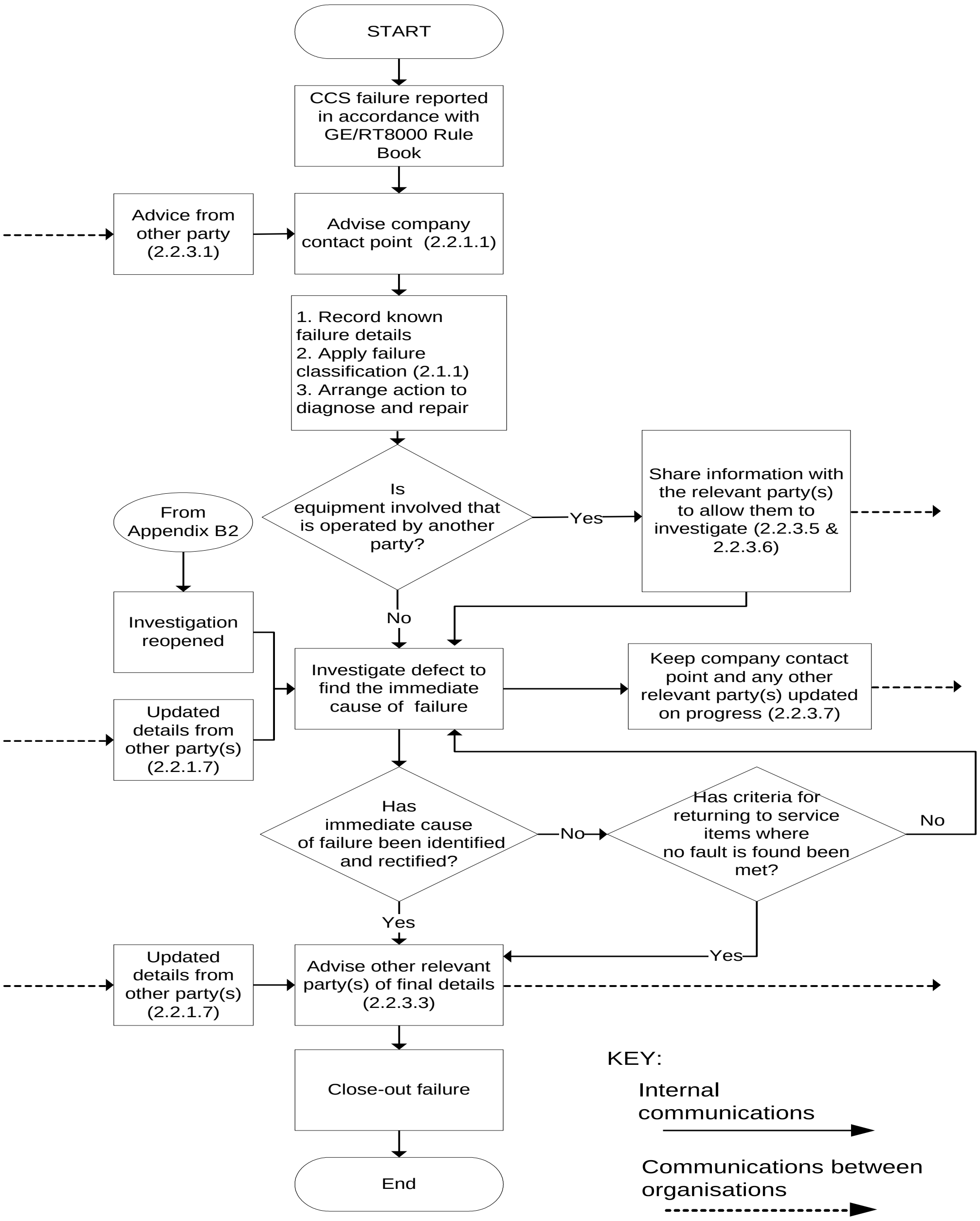
Table A.12 **Global System for Mobile Communications – Railway (GSM-R) failures**

Failure symptom	Failure classification		
	Safety related (High Risk)	Safety related (Low Risk)	Negligible Risk
TASS authorisation not available where it should be			●
TASS system fault resulting in brake application			●
Spurious speed supervision intervention			●
Erroneous speed supervision indication in area where TASS should not be supervising speed		●	
Erroneous tilt authorisation – route not gauge cleared for tilt operation	●		
Erroneous tilt authorisation – route gauge cleared for tilt operation		●	
TPWS not suppressed where required			●
TPWS suppressed where required to be available	●		
Other failure	● Unless evidence can justify a lower initial classification		

Table A.13 **Tilt Authorisation and Supervision System (TASS) failures**

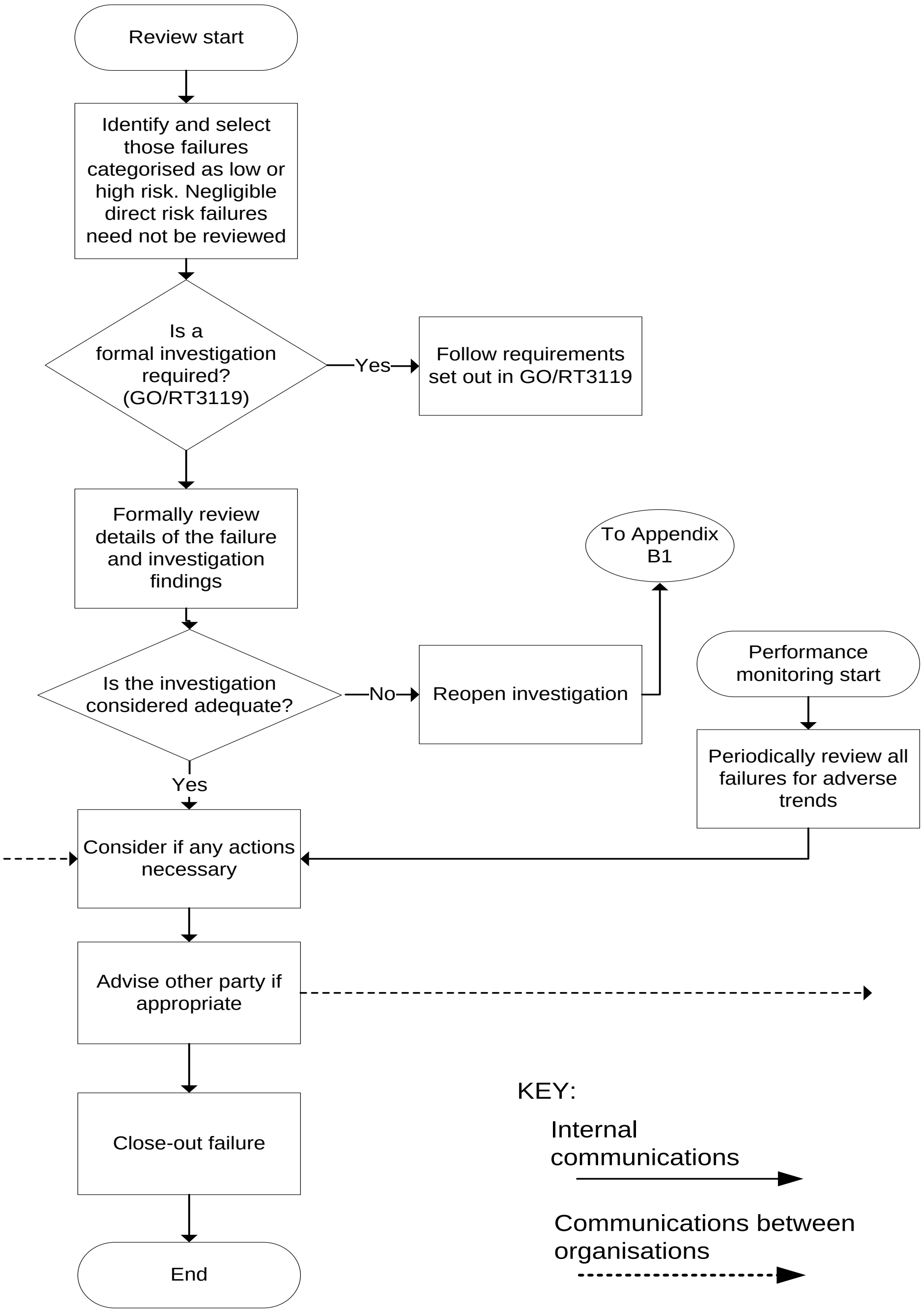
Appendix B1 Flowchart for a typical CCS failure investigation

The content of this appendix is not mandatory and is provided for guidance only


START
CCS failure reported in accordance with GE/RT8000 Rule Book
Advice from other party (2.2.3.1)
Advise company contact point (2.2.1.1)
1. Record known failure details
2. Apply failure classification (2.1.1)
3. Arrange action to diagnose and repair
Is equipment involved that is operated by another party?
Yes
Share information with the relevant party(s) to allow them to investigate (2.2.3.5 & 2.2.3.6)
From Appendix B2
Investigation reopened
No
Investigate defect to find the immediate cause of failure
Keep company contact point and any other relevant party(s) updated on progress (2.2.3.7)
Updated details from other party(s) (2.2.1.7)
Has immediate cause of failure been identified and rectified?
No
Has criteria for returning to service items where no fault is found been met?
No
Yes
Yes
Updated details from other party(s) (2.2.1.7)
Advise other relevant party(s) of final details (2.2.3.3)
Close-out failure
End
KEY:
Internal communications
Communications between organisations

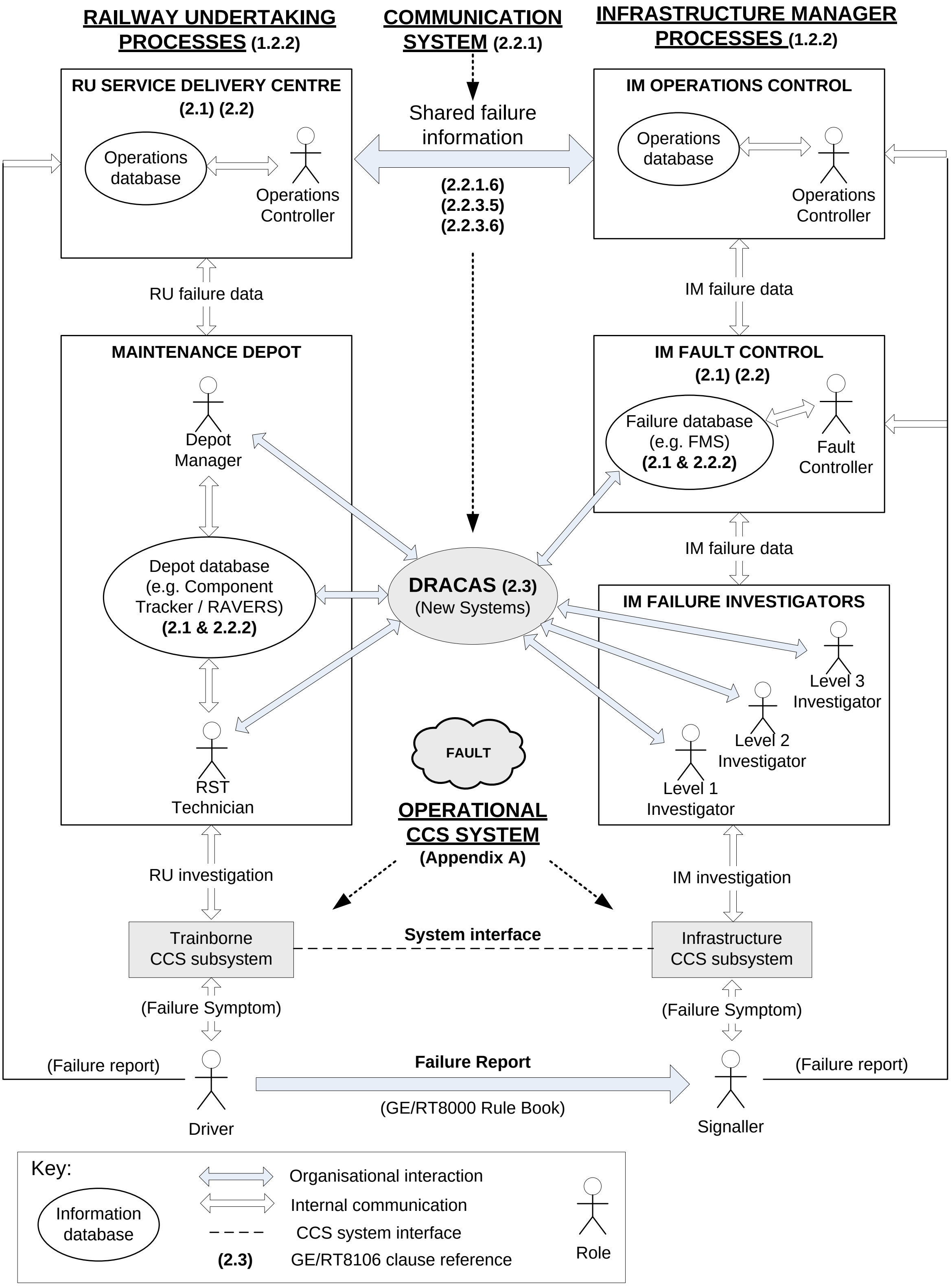
Appendix B2 Flowchart for a typical CCS failure review

The content of this appendix is not mandatory and is provided for guidance only


Review start
Identify and select those failures categorised as low or high risk. Negligible direct risk failures need not be reviewed
Is a formal investigation required? (GO/RT3119)
Yes
Follow requirements set out in GO/RT3119
Formally review details of the failure and investigation findings
To Appendix B1
Is the investigation considered adequate?
No
Reopen investigation
Performance monitoring start
Periodically review all failures for adverse trends
Yes
Consider if any actions necessary
Advise other party if appropriate
Close-out failure
End
KEY:
Internal communications
Communications between organisations

Appendix C. Typical interactions and communication links

The content of this appendix is not mandatory and is provided for guidance only



Definitions

Cab identification

The unique identification code that identifies each cab, where a vehicle or train set has more than one driving cab, for example cab A, or cab B.

CCS equipment

The component parts that, when correctly connected together and operated within designed parameters, make up a control, command and signalling (CCS) system.

CCS system

Systems used for authorising and safeguarding the safe operation of trains, and communication systems provided for safety purposes in the direct operation of the railway.

DRACAS

Defect reporting analysis and corrective action system: a formal closed loop corrective action process that is used to continually monitor a system, in order to continually improve quality of service and system reliability.

Failure

Deviation from the normal and intended operation of a control, command and signalling (CCS) system, including trainborne equipment.

Failure classification

The method of ranking system failures relative to the level of uncontrolled safety risk introduced into the operational railway by the failure.

Failure identifier

A unique identification code allocated by infrastructure managers and railway undertakings to each reported failure in accordance with their safety management systems.

Failure symptom

The way in which a control, command and signalling (CCS) system fails to operate or operates incorrectly.

Indication

A function of a protection system or a warning system that displays system status.

Infrastructure sub-system

The infrastructure part of a control, command and signalling (CCS) system that also includes a corresponding trainborne sub-system.

Intervention

The call for the application of the train’s brakes from either the warning function or the protection function.

Negligible risk failure

Failure of the control, command and signalling (CCS) system that does not directly increase the risk to persons or the operational railway.

New CCS system

A CCS system that either:

a) Implements a new technology within the railway system, or

b) Applies an existing technology to a new operational railway context.

Party, other party

Where the party concerned is the infrastructure manager, the other party is the railway undertaking and where the party concerned is the railway undertaking, the other party is the infrastructure manager.

Pushing data

The process of automatically uploading data from one computer server to another.

Railway equipment

Any equipment within the railway system operated by an infrastructure manager or railway undertaking.

Reported safety related failures of CCS systems

Failures of control, command and signalling (CCS) systems that have been reported in accordance with GE/RT8000, the Rule Book, including reported failure allegations and failures found during in-service maintenance and testing.

Safety related failure

A failure of a control, command and signalling (CCS) system or item of equipment, which may result in increased risk, for example due to the absence, or deterioration, of control measures necessary to prevent an accident.

Safety related failure (low risk)

A failure of control, command and signalling (CCS) equipment where an acceptable level of protection is maintained (by the CCS system or by procedures) even though safety is degraded by the failure.

Safety related failure (high risk)

A failure of control, command and signalling (CCS) equipment where no other part of the control, command and signalling (CCS) system provides acceptable protection.

Train head-code

The train reporting number shown in the working timetable.

Trainborne sub-system

The trainborne part of a control, command and signalling (CCS) system that also includes a corresponding infrastructure sub-system.

Vehicle identification

The unique code that identifies each railway vehicle.

References

The Catalogue of Railway Group Standards gives the current issue number and status of documents published by RSSB. This information is also available from www.rssb.co.uk/railway-group-standards

Documents referenced in the text

RGSC 01	Railway Group Standards Code
RGSC 02	Standards Manual

Railway Group Standards

GE/RT8000	Rule Book
GE/RT8047	Reporting of Safety Related Information
GE/RT8250	Reporting High Risk Defects
GO/RT3437	Defective On-Train Equipment
GO/RT3119	Accident and Incident Investigation

RSSB documents

Form RT8106	Example failure data collection form