RAIB

Rail Accident Investigation Branch

Rail Accident Report

Loss of safety critical signalling data on the Cambrian Coast line
20 October 2017

Report 17/2019
December 2019

This investigation was carried out in accordance with:

- the Railway Safety Directive 2004/49/EC;
- the Railways and Transport Safety Act 2003; and
- the Railways (Accident Investigation and Reporting) Regulations 2005.

© Crown copyright 2019

You may reuse this document/publication (not including departmental or agency logos) free of charge in any format or medium. You must reuse it accurately and not in a misleading context. The material must be acknowledged as Crown copyright and you must give the title of the source publication. Where we have identified any third party copyright material you will need to obtain permission from the copyright holders concerned. This document/publication is also available at www.gov.uk/raib.

Any enquiries about this publication should be sent to:

RAIB
The Wharf
Stores Road
Derby UK
DE21 4BA

Email: enquiries@raib.gov.uk
Telephone: 01332 253300
Website: www.gov.uk/raib

This report is published by the Rail Accident Investigation Branch, Department for Transport.

Preface

The purpose of a Rail Accident Investigation Branch (RAIB) investigation is to improve railway safety by preventing future railway accidents or by mitigating their consequences. It is not the purpose of such an investigation to establish blame or liability. Accordingly, it is inappropriate that RAIB reports should be used to assign fault or blame, or determine liability, since neither the investigation nor the reporting process has been undertaken for that purpose.

The RAIB's findings are based on its own evaluation of the evidence that was available at the time of the investigation and are intended to explain what happened, and why, in a fair and unbiased manner.

Where the RAIB has described a factor as being linked to cause and the term is unqualified, this means that the RAIB has satisfied itself that the evidence supports both the presence of the factor and its direct relevance to the causation of the accident or incident that is being investigated. However, where the RAIB is less confident about the existence of a factor, or its role in the causation of the accident or incident, the RAIB will qualify its findings by use of words such as 'probable' or 'possible', as appropriate. Where there is more than one potential explanation the RAIB may describe one factor as being 'more' or 'less' likely than the other.

In some cases factors are described as 'underlying'. Such factors are also relevant to the causation of the accident or incident but are associated with the underlying management arrangements or organisational issues (such as working culture). Where necessary, words such as 'probable' or 'possible' can also be used to qualify 'underlying factor'.

Use of the word 'probable' means that, although it is considered highly likely that the factor applied, some small element of uncertainty remains. Use of the word 'possible' means that, although there is some evidence that supports this factor, there remains a more significant degree of uncertainty.

An 'observation' is a safety issue discovered as part of the investigation that is not considered to be causal or underlying to the accident or incident being investigated, but does deserve scrutiny because of a perceived potential for safety learning.

The above terms are intended to assist readers' interpretation of the report, and to provide suitable explanations where uncertainty remains. The report should therefore be interpreted as the view of the RAIB, expressed with the sole purpose of improving railway safety.

Any information about casualties is based on figures provided to the RAIB from various sources. Considerations of personal privacy may mean that not all of the actual effects of the event are recorded in the report. The RAIB recognises that sudden unexpected events can have both short- and long-term consequences for the physical and/or mental health of people who were involved, both directly and indirectly, in what happened.

The RAIB's investigation (including its scope, methods, conclusions and recommendations) is independent of any inquest or fatal accident inquiry, and all other investigations, including those carried out by the safety authority, police or railway industry.

This page is intentionally left blank

Loss of safety critical signalling data on the Cambrian Coast line, 20 October 2017

Contents

This page is intentionally left blank

Summary

On the morning of 20 October 2017, four trains travelled over the Cambrian Coast line, Gwynedd, while temporary speed restriction data was not being sent to the trains by the signalling system. No accident resulted but a train approached a level crossing at 80 km/h (50 mph), significantly exceeding the temporary speed restriction of 30 km/h (19 mph) needed to give adequate warning time for level crossing users.

The line has been operated since 2011 using a pilot installation of the European Rail Traffic Management System (ERTMS) which replaces traditional lineside signals and signs with movement authorities transmitted to trains. These movement authorities include maximum permitted speeds which are displayed to the train driver and used for automatic supervision of train speed.

The temporary speed restriction data was not uploaded during an automated signalling computer restart the previous evening, but a display screen incorrectly showed the restrictions as being loaded for transmission to trains. An independent check of the upload was needed to achieve safety levels given in European standards and the system designer, Ansaldo STS (now part of Hitachi STS), intended that this would be provided by signallers checking the display. A suitable method of assuring that the correct data was provided to the display had not been clearly defined in the software design documentation prepared by Ansaldo STS and the resulting software product included a single point of failure which affected both the data upload and signallers' display functions. The system safety justification was presented in a non-standard format based on documentation from another project still in development at the time of the Cambrian ERTMS commissioning and which, before completion, made changes that unintentionally mitigated the single point of failure later exhibited on the Cambrian system. Network Rail and the Independent Safety Assessor (Lloyd's Register Rail, now Ricardo Rail/Ricardo Certification) were required to review the design documentation but did not identify the lack of clear definition in design documents and were not aware of the changes made during the development of the other project.

The investigation makes five recommendations. Network Rail, aided by the wider rail industry, should improve its safety assurance process for high integrity software-based systems and improve safety learning from failures of such systems, and develop a process to capture the data needed to understand these failures. Hitachi STS (formerly Ansaldo STS) should review its safety assurance processes in the light of the learning from this investigation, and should provide a technical solution for the Cambrian lines that avoids the need for signallers to verify automatically uploaded speed restrictions.

Learning points cover train drivers reporting inconsistencies in information provided to them; the need for Independent Safety Assessors to understand the scope of checks undertaken by other bodies and to apply extra vigilance if documents form part of a non-standard process; the importance of clients undertaking their client role when procuring high integrity software; and achieving the specified level of safety when implementing temporary speed restrictions in ERTMS.

Introduction

Definitions

1 Metric units are used throughout this report, in accordance with operating practices on the lines involved. Where appropriate the equivalent imperial value is also given.

Acknowledgments

2 The investigation required Hitachi STS (formally Ansaldo STS) to construct a replica system similar to that installed at the Machynlleth control centre. This laboratory-based system, located in France, allowed Hitachi STS to run different test scenarios to emulate the failure which occurred on the Cambrian lines. The RAIB acknowledges the assistance provided by Hitachi STS in preparing this laboratory system and the extensive testing required to determine causation.

3 The RAIB also acknowledges the invaluable assistance provided by RSSB[1] and the rail division of the Accident Investigation Board of Norway (AIBN).

[1] A not-for-profit body whose members are the companies making up the railway industry. The company is registered as Rail Safety and Standards Board Ltd, but trades as RSSB.

The incident

Summary of the incident

4 During the morning of Friday 20 October 2017, a train driver travelling on the Cambrian Coast line in North Wales reported a fault with the information provided on his in-cab display. As signalling staff at the control centre in Machynlleth investigated this report, they became aware that temporary speed restrictions were not being transmitted to several trains under their control. The temporary speed restrictions were required on the approach to seven level crossings to provide level crossing users with sufficient warning of approaching trains so that they could cross safely.

5 The Cambrian lines were equipped with a pilot installation of the European Rail Traffic Management System (ERTMS), a form of railway signalling, in 2011. The ERTMS system provided on the Cambrian lines removed the need for signals along the track by transmitting signalling and control data directly to the train. This transmitted data is used to enforce the permitted speed and display both movement authority[2] and other information, including temporary and permanent speed restrictions, on a screen in front of the driver.

6 Subsequent investigation, by the local maintenance staff, found that the signalling system stopped transmitting temporary speed restriction data after it had experienced a shutdown and restart at around 23:10 hrs the previous evening. The signallers had no indication of an abnormal condition and the display at the signalling control centre wrongly showed these restrictions as being applied correctly.

Context

Location

7 The Cambrian lines run from Shrewsbury to Machynlleth and Dovey Junction, and then from Dovey Junction to Aberystwyth (the Cambrian Main Line), and from Dovey Junction to Pwllheli (the Cambrian Coast Line) (figure 1).

8 The area is controlled from Machynlleth signalling control centre, using signalling designed to comply with the ERTMS train control standard.

Organisations involved

9 Network Rail owns and maintains the Cambrian lines infrastructure, and employs the Machynlleth signalling control centre staff, including signallers and signalling technicians responsible for operation and maintenance of the Cambrian ERTMS system.

10 Arriva Trains Wales Ltd operated the trains and employed the drivers affected by the loss of speed restrictions. Transport for Wales took over operation of these trains in October 2018.

[2] Permission to travel along a specified part of the railway.

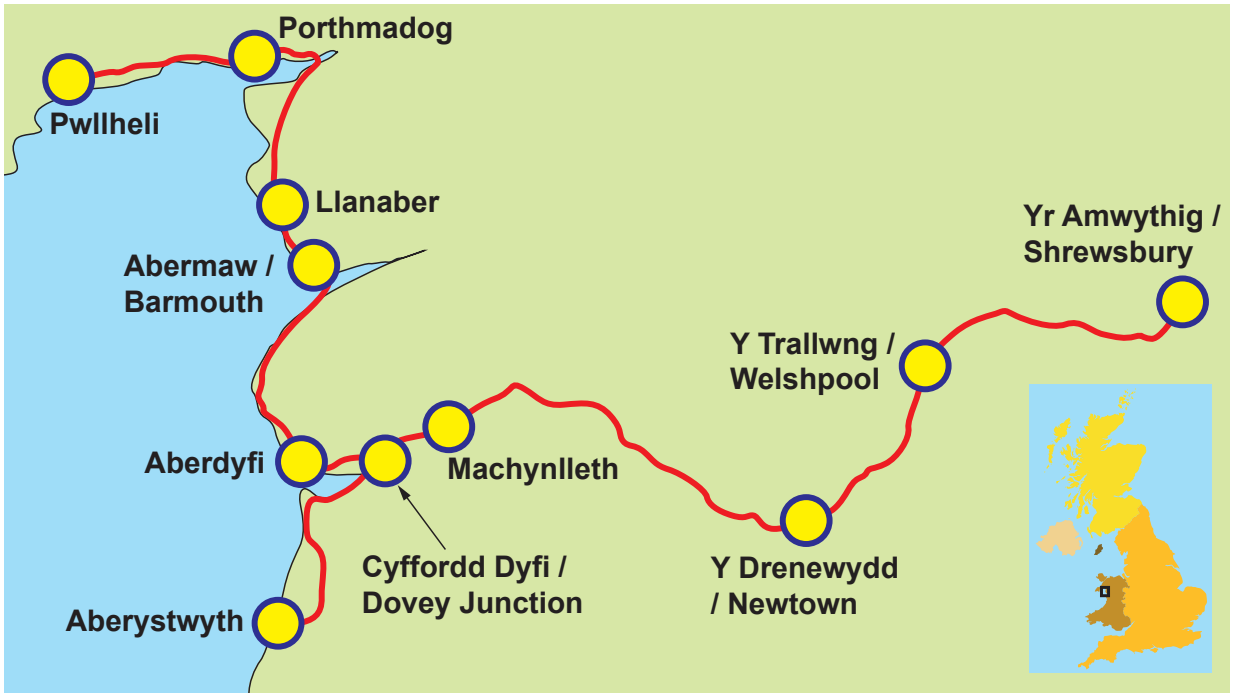


Figure 1: Geographical area controlled by Machynlleth signalling centre

11 Ansaldo STS (now part of Hitachi STS) supplied the equipment for the Cambrian ERTMS installation and provides maintenance assistance to the local Network Rail signalling maintenance staff when requested. It employed the support engineer involved in restoring the train services after the incident.

12 The Cambrian ERTMS project team designed, installed, commissioned and brought the Cambrian ERTMS system into operational use. It included representatives from both Network Rail and Ansaldo STS.

13 Lloyd's Register Rail, now Ricardo Rail/Ricardo Certification, acted as the Independent Safety Assessor (ISA) of safety case documents issued by the Cambrian ERTMS project team.

14 Network Rail chaired and employed the discipline experts which formed the System Review Panel (SRP). The SRP determined the acceptability of the safety case documents submitted to it by the Cambrian ERTMS project team, taking account of the issues that had been identified by the ISA.

15 All organisations freely co-operated with the investigation.

Equipment involved

16 The Cambrian lines ERTMS signalling provided by Ansaldo STS was installed as a pilot scheme for the Great Britain mainline rail network, and was fully commissioned in March 2011. The system was designed to operate with level 2 of the European Train Control System (ETCS), which is defined in the Control-Command and Signalling Technical Specification for Interoperability (CCS-TSI). ETCS uses Global System for Mobile Communications - Railway (GSM-R) for communication between the trackside infrastructure and the trains. ETCS level 2 does not require lineside signals, although some trackside signs are needed.

17 Instead of trackside signals, drivers receive permission to proceed and maximum permitted speed information on a display screen installed in the driving cab. This display is known as a Driver Machine Interface (DMI) (figure 2). Information displayed on the DMI is taken from movement authorities sent to the train as radio messages from the control centre. Movement authorities are derived from geographical 'knowledge' held by the ERTMS system, such as the track layout, gradients, and permanent and temporary speed restrictions, together with location and train status information.

Figure 2: Typical driving cab layout and driver machine interface (DMI) screen

18 The DMI provides the driver with the current train speed and the maximum permissible speed, including any temporary speed restrictions, in kilometres per hour on a simulated analogue speedometer (figure 3). The DMI speedometer switches to miles per hour for use on infrastructure not equipped with ERTMS. A standard analogue speedometer is also provided for degraded operation, specifically where the ERTMS system is isolated so the DMI is switched off.

19 The ERTMS signalling implemented on the Cambrian lines, although new to Network Rail infrastructure, was based on equipment already in operation elsewhere in Europe. Implementation in the United Kingdom (UK) was partly reliant on product validations already achieved in Europe, with the differences required for the Cambrian lines being subject to a full approval process in accordance with UK procedures.

20 The ERTMS equipment and signallers, together with the signalling technicians who maintain the equipment, are all located at Machynlleth. The equipment includes the Radio Block Centre (RBC) which sends movement authorities to trains and the 'poste de GEstion des Signalisations Temporaires' (GEST) system which provides an interface between the signallers and the RBC.

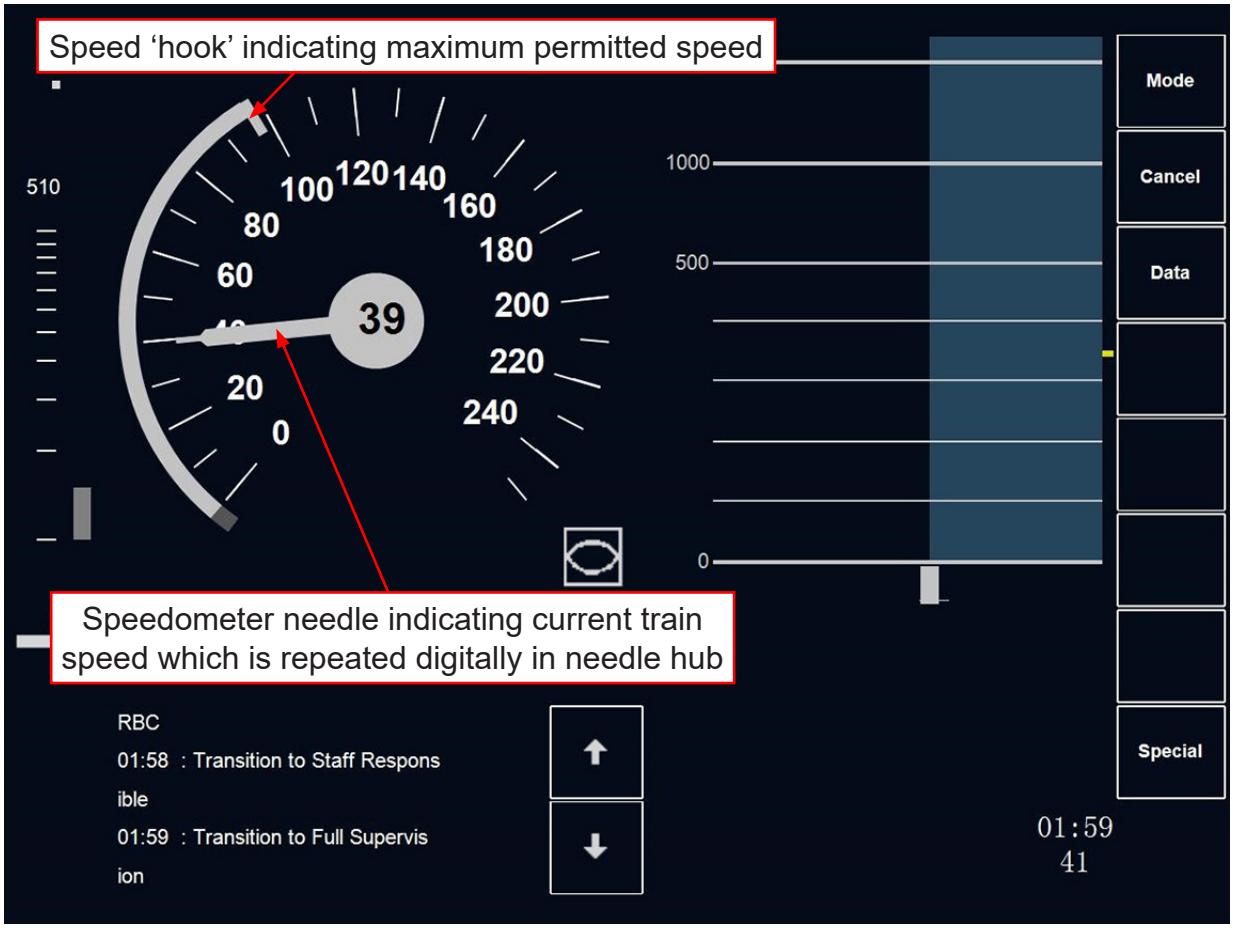


Figure 3: DMI screen showing speedometer with maximum speed supervision and actual speed

21 Two signallers control the movement of trains on the Cambrian lines using two individual workstations, East and West, located on the operating floor of the control centre. The GEST terminal controlling the entire area is located between the workstations and shared by both signallers (figure 4). The GEST terminal includes a computer screen which displays the position of trains on a schematic representation of the line(s) under control. The infrastructure shown on this diagram includes the track layout, stations and level crossings. The extent of any temporary speed restrictions is shown by 'flags' (figure 5). The GEST terminal is used by staff to input and remove temporary speed restrictions, and for other tasks including returning the signalling control system to service after it has been reset.

Temporary speed restrictions

22 A temporary speed restriction is applied when a short-term reduction is required to the maximum permitted line speed at a specified location. Temporary speed restrictions are marked by trackside signs in areas with traditional trackside signalling. For in-cab signalling areas, such as the Cambrian lines, trackside signs are not provided because the temporary speed restrictions should be included in the permitted speed provided to the driver by the DMI. In both types of area, the railway Rule Book[3] requires train drivers to make themselves aware of temporary speed restrictions in the weekly operating notices issued to them.

[3] RSSB document GE/RT8000.

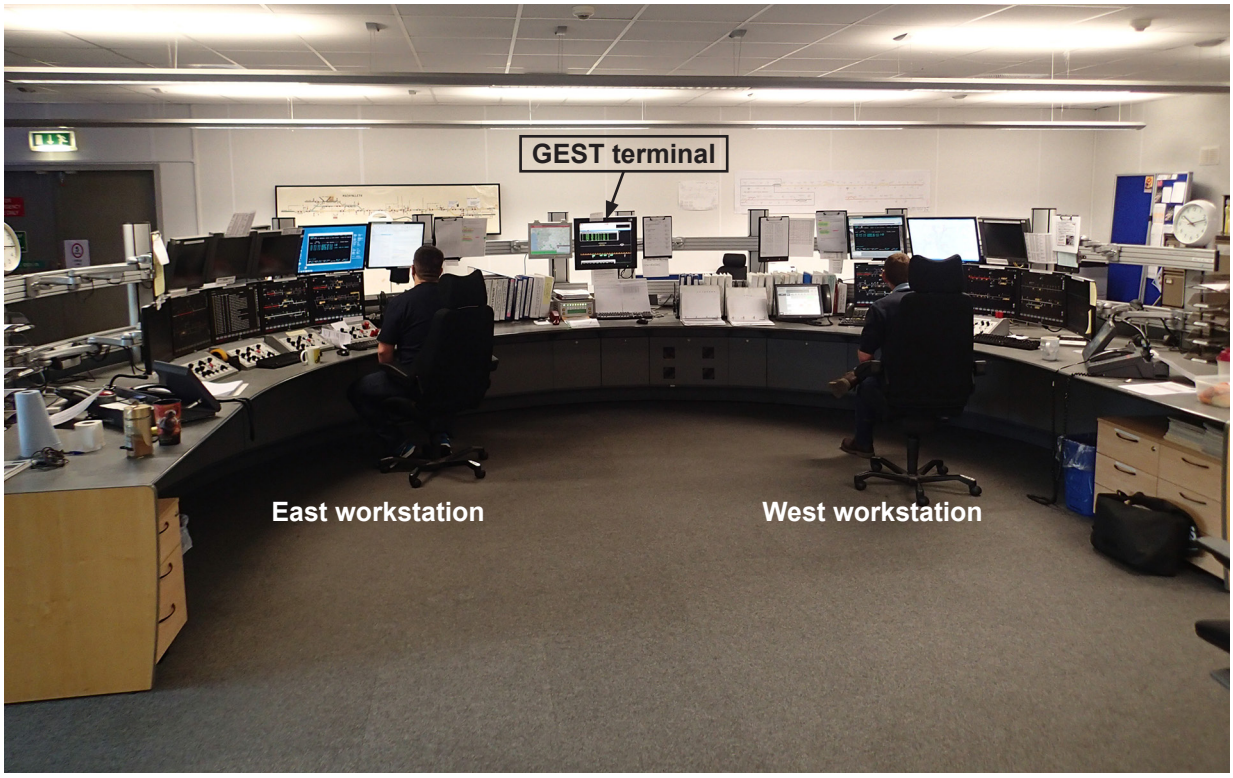


Figure 4: Operating floor at Machynlleth signalling control centre

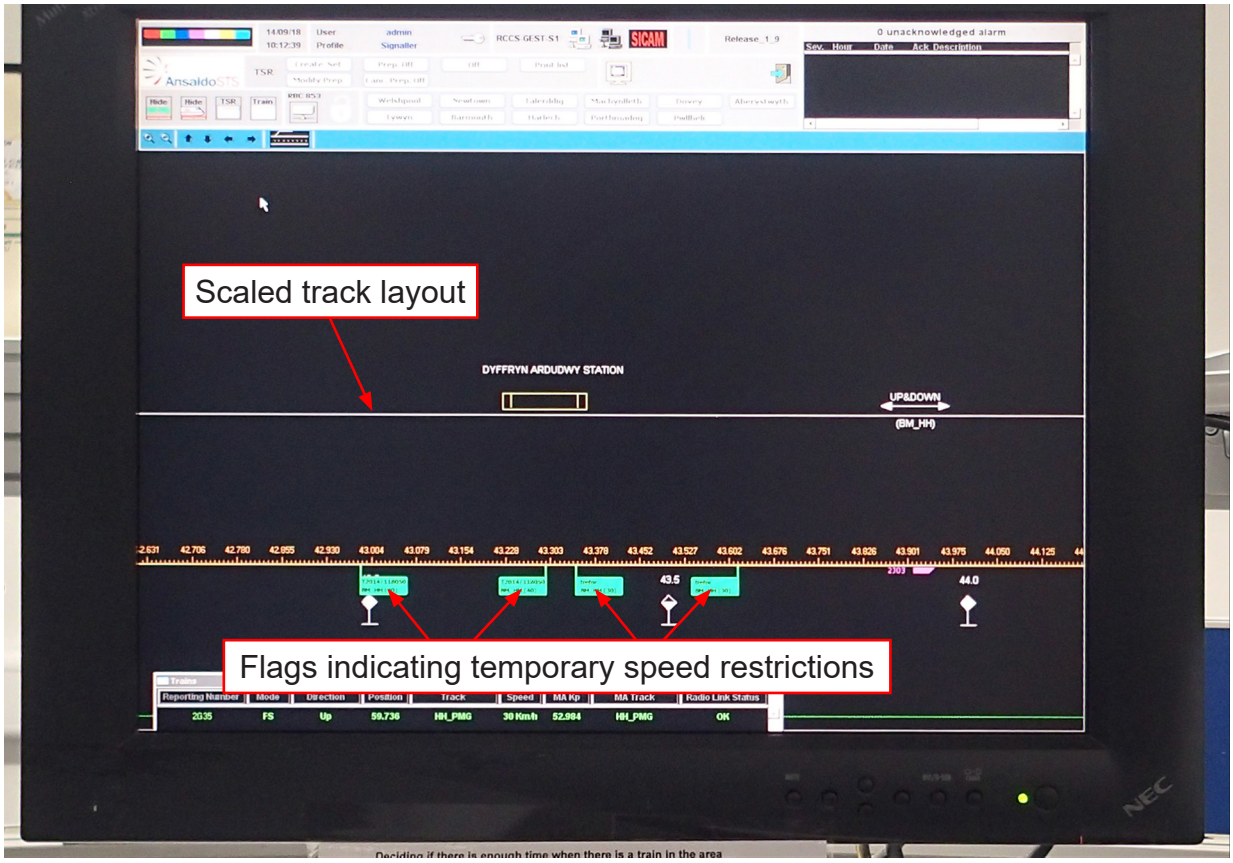


Figure 5: GEST terminal interface screen, here showing a single track with a station and flags at the beginning and the ends of two temporary speed restrictions

23 Temporary speed restrictions on the Cambrian lines are implemented by signallers inputting information into the GEST sub-system. Temporary speed restriction data is then sent by the GEST sub-system to the RBC which includes this in the movement authority data transmitted to the trains (figure 6). At the time of the incident, seven temporary speed restrictions had been implemented on the Cambrian lines. All were located on the Cambrian Coast Line and all related to level crossing sighting times (ie providing level crossing users with sufficient time to see an approaching train). There were no temporary speed restrictions on the Cambrian lines for engineering reasons such as track defects.

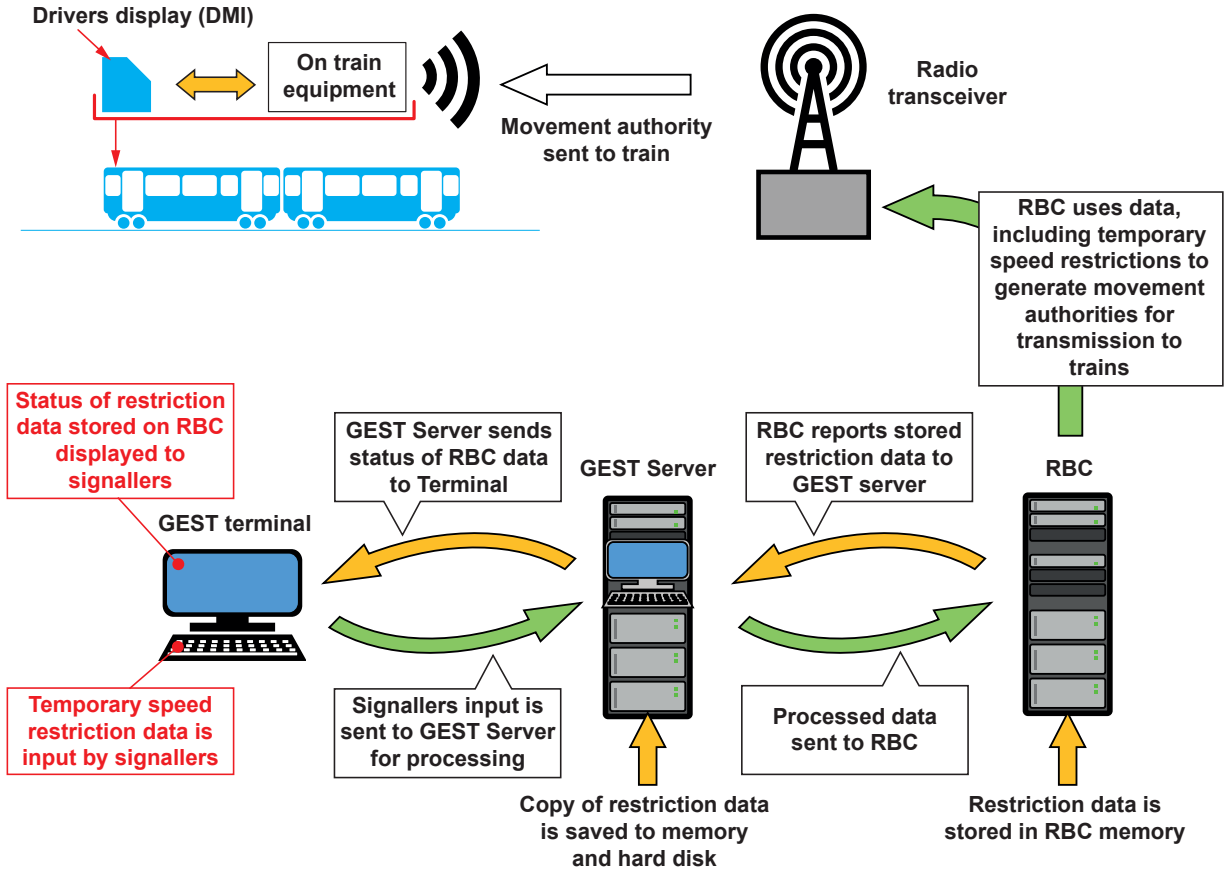


Figure 6: Simplified arrangement of GEST and signalling control system interface

The sequence of events

Events preceding the incident

24 Just after 23:00 hrs on 19 October 2017, and near the end of passenger service, an automated software reset occurred in the RBC. This automatic reset, known as a 'rollover', was triggered when equipment on board a train at Machynlleth station requested part of a movement authority it had previously released for use by another train[4]. The RBC software was written to trigger a rollover as a safe response when movement authority conflicts, and other exceptional events, are detected.

25 At that time, internally triggered software rollovers were occurring between 10 and 12 times each year, and the signalling staff at the control centre followed their established processes for returning to normal service. This process meant that movement authorities were not given to the three trains within the area controlled by the signalling system during the rollover. The signalling staff authorised normal working to resume at about 23:19 hrs and the three trains continued to their respective destinations after a short delay. These were the last trains of the day.

26 During a rollover, the RBC receives information from the GEST sub-system (paragraph 23). This should include information about temporary speed restrictions. However, during the rollover on the 19 October 2017, the data relating to temporary speed restrictions between Dovey Junction and Pwllheli was not uploaded from the GEST sub-system to the RBC. Staff working in the signalling control centre were unaware of this when they subsequently permitted trains to begin operating again because their display indicated the speed restrictions had been correctly implemented.

Events during the incident

27 On 20 October, the morning after the rollover, passenger train services started at 07:17 hrs and, when the first three trains passed over the line with the missing temporary speed restrictions, none of the drivers reported problems with the speed indication displayed on their DMIs.

28 The fourth train over the affected line was the 08:52 hrs Machynlleth to Pwllheli service with the reporting number 2J03[5]. At around 10:02 hrs, train 2J03 passed through a 30 km/h (19 mph) temporary speed restriction at approximately 80 km/h (50 mph) while travelling between Barmouth and Llanaber. The temporary speed restriction had been applied at this location since 2014 to provide level crossing users with sufficient warning of approaching trains so they could cross safely.

29 After passing through this restriction, the driver of train 2J03 reported a fault with the information provided to him by his DMI. While investigating this report, a signalling technician at the Machynlleth control centre discovered that temporary speed restriction information was not being transmitted to any of the trains on the Cambrian lines.

---

[4] Trains release parts of the movement authority as they progress through their route. On this occasion, the train attempted to reallocate to itself a part of the movement authority which had been released and then correctly allocated to another train.

[5] An alphanumeric code, known as the 'train reporting number', is allocated to every train operating on Network Rail's infrastructure.

Events following the incident

30 The signalling technician initiated an RBC reset (software restart) at around 10:11 hrs, intending that this would cause an automatic reloading of the temporary speed restrictions from the GEST sub-system into the RBC. This did not resolve the problem, so the signalling technician reset the GEST server and initiated another RBC reset. At around 11:51 hrs, and after several further unsuccessful attempts to cause an automatic reload of the temporary speed restrictions, the signalling technician contacted the Ansaldo STS support engineer to request assistance. By this time, signallers and train drivers had reverted to using a procedure based system of verbal and written instructions to continue the train service.

31 While restoring normal working after trying other options, the support engineer advised the signalling technician to delete information contained within a database from the GEST sub-system. This instruction required all temporary speed restriction information to be manually re-entered into the GEST terminal and then transferred to the RBC by the GEST software. The manually entered restrictions displayed correctly on the GEST terminal, and upload to the RBC was verified by a test train which passed through the area at reduced speed while the driver confirmed that the restrictions were displayed on the DMI. During this activity to return the system to normal service, event and data logs containing information relating to the system were not saved and were subsequently overwritten. Normal operation was resumed at 15:50 hrs.

Analysis

Background information

Architecture of the train control command and communications system

32 The ERTMS system provided at the Machynlleth control centre consists of several sub-systems working together. The sub-systems relevant to this investigation are shown in figure 7 and their functions are:

- ***Rail Control Centre (RCC)*** - a visual display based sub-system providing an interface between the signalling control system and the signaller setting train routes.
- ***Interlocking (known as SEI)*** – a computer based sub-system which determines the availability of a route request from the RBC by assessing its compatibility with infrastructure and conflicts with other routes.
- ***Poste de GEstion des Signalisations Temporaires (GEST)*** - a server based sub-system with a computer screen interface for managing the implementation and removal of temporary speed restrictions, signaller control of the RBC and display of train location information. This comprises a desktop computer called the GEST terminal and a server computer plus associated ancillary equipment. A second server computer is also provided as a standby in case of failure.
- ***Maintenance sub-system (known as SILAM / SICAM)*** - a simple computer system with connections to the internal data transmission lines. The SILAM / SICAM system creates a log of system activity and internal commands which can be used for maintenance and fault finding.
- ***Radio Block Centre (RBC)*** - generates the messages sent to, and interprets messages received from, trains. Transmitted messages include movement authorities, permanent speed restrictions and track gradients as well as restrictive events such as emergency stop commands and temporary speed restrictions.

33 Only part of an ERTMS installation was required to conform to the CCS-TSI; this is referred to as the ‘ETCS reference architecture’. For the Cambrian project, the trackside elements of the reference architecture consisted of the RBC and the track to train communication radio frequency beacons (known as Eurobalise) used on the project.

34 Peripheral equipment such as GEST was not part of the reference architecture and was accepted as part of the Cambrian scheme by Network Rail on the basis of safety case submissions made to its system review panel (SRP) in accordance with Network Rail standard NR/L2/AMG/013, ‘System Review Panels’. This standard required the review of safety case documents by an Independent Safety Assessor (ISA) before submission to the SRP.

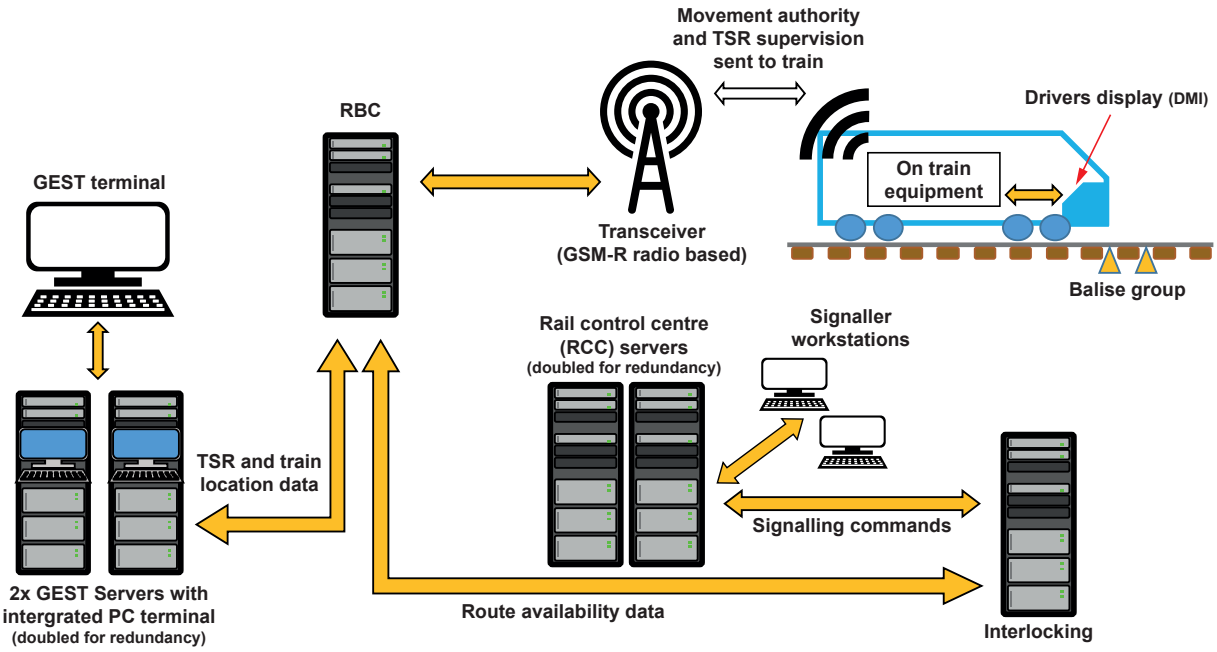


Figure 7: Simplified diagram of Cambrian ERTMS showing sub-systems relevant to the investigation. Note, SILAM / SICAM sub-system not shown.

Investigation methodology

35 The GEST sub-system was developed in Spain using learning gained from the Madrid to Lerida high speed line project. Temporary speed restriction data was managed with a similar RBC interface to that proposed for the LGVEE[6] and Cambrian projects. Only limited amounts of information could be found from the original design work so the investigation needed Hitachi STS (as the successor to Ansaldo STS, paragraph 11) to undertake the time consuming task of reverse engineering the GEST sub-system software to understand how the system operates.

36 Laboratory testing of the GEST sub-system was undertaken at the Hitachi STS offices in France using a system equivalent to that installed at the Machynlleth control centre. Hitachi STS engineers initially advised the RAIB of their intended testing methodology and reported their conclusions on completion of this testing. The RAIB then requested further testing to improve understanding of the ERTMS system and to assist understanding of the failure mechanism.

Safety assurance of high integrity computer-based railway systems

37 High integrity software systems relied upon for safety in railway signalling in Europe are required to comply with a suite of European standards. Those relating to safety assurance, applicable when the Cambrian lines ERTMS project was being designed, and relevant to this investigation were:

- EN 50126-1:1999, 'Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)' – Part 1 (superseded by EN 50126-1:2017).

[6] The Ligne à Grande Vitesse Est Européenne (LGVEE) is a high speed railway line which connects Vaires-sur-Marne, near Paris and Vendenheim, near Strasbourg.

- EN 50128:2001 - ‘Railway applications – Communications, signalling and processing systems – Software for railway control and protection systems’ (superseded by EN 50128:2011).
- EN 50129:2003, ‘Railway applications – Safety related electronic systems for signalling’ (superseded by EN 50129:2018).

38 These standards provided the framework for the development of the software used for the Cambrian ERTMS system. This report refers to the versions of the standards applicable during this development as EN 50126-1, EN 50128 and EN 50129.

39 EN 50126-1 sets out the requirements for safety management and safety integrity levels, and how these can be demonstrated. EN 50128 includes detailed requirements for the development of software to be used for railway signalling and control systems. EN 50129 sets out the approval process for individual systems which can exist within the overall railway control and protection system.

40 It is not practicable to test every combination of variables to identify possible errors in complex software used for safety critical control systems. EN 50128 therefore sets out a software development lifecycle for the evolution of system requirements into program code using formal methods of verification and validation. Following this methodology gives the required level of confidence in the final product.

41 The development lifecycle comprises a verification leg, during which program code intended to meet client requirements is produced, followed by a validation leg intended to ensure that the code does meet those requirements. Key components of the verification leg include the system development phase in which client needs, understood from the concept development and feasibility process, are used to formulate a system requirements specification and a system safety requirements specification. This is followed by a phase in which these specifications are used to produce a software requirements specification which forms the basis for software engineers to undertake three further phases of work with the last, program code implementation, generating computer code. Each phase of the verification leg includes checks that the product meets the requirements of the previous phase; these checks reduce the likelihood of (and ideally prevent) faults in the code, before the validation leg is undertaken.

42 The validation leg involves a ‘look back’ comparison, in which the code is tested against increasingly higher phases of the verification leg to provide assurance that the intended functional requirements and integrity are met (figure 8). This is intended to identify faults in the code which have arisen as a result of mistakes in the verification leg.

43 When procuring a new safety critical product, EN50128 requires a client, such as Network Rail, to play a significant role in developing the system requirements specification and the system safety requirements specification. Those parts of the development model for which the client is primarily responsible are shown in orange in figure 8. This enables the client to confirm that the system meets their requirements, and to understand how they should operate and maintain it.

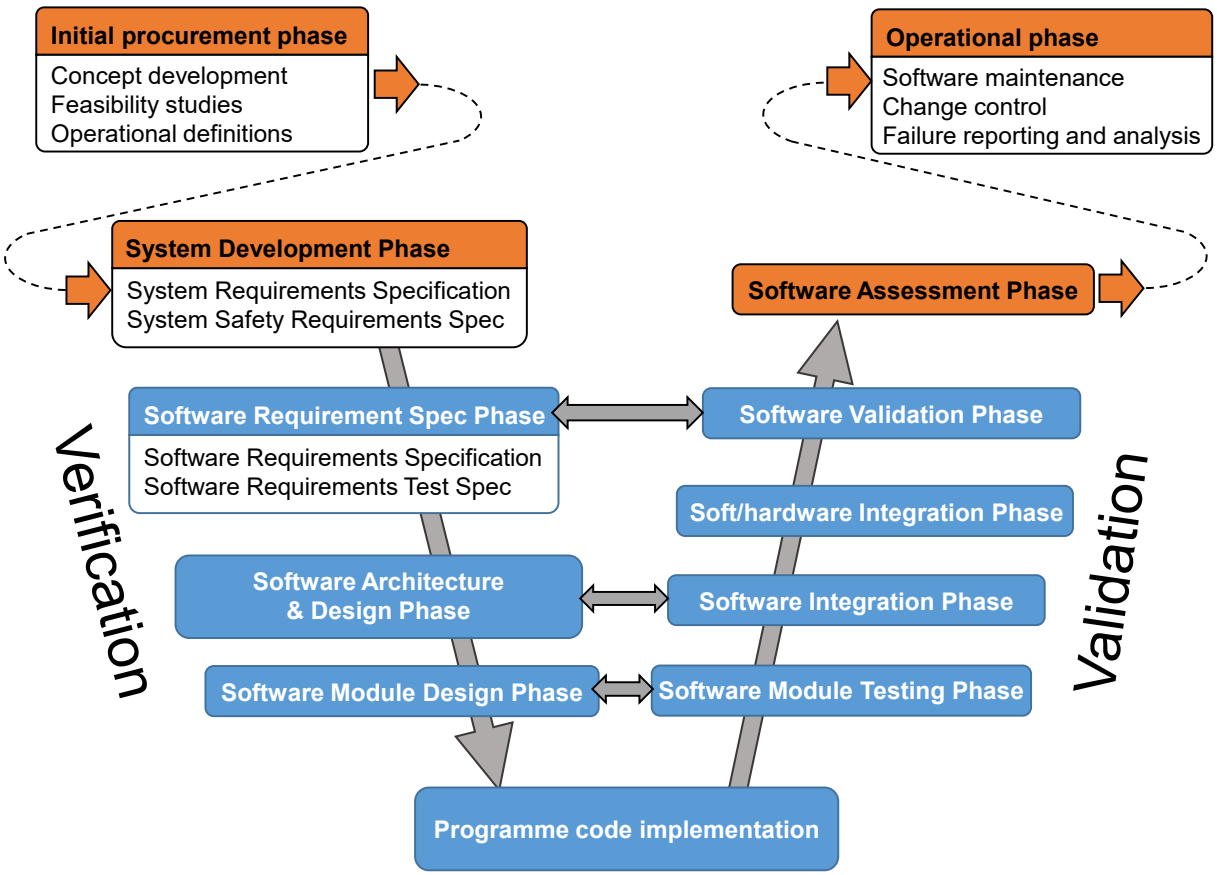


Figure 8: Simplified development lifecycle used for the development of high integrity software from procurement to operation. Only activities and documents referenced in this report have been shown.

Identification of the immediate cause

44 **The ERTMS signalling system was returned to service following an RBC software rollover without temporary speed restriction information for transmission to trains.**

Identification of causal factors

45 The incident occurred due to a combination of the following causal factors:

a. temporary speed restriction data was not uploaded to the RBC after a software rollover because the GEST sub-system had entered a fault condition probably due to a corrupted database (paragraph 46);

b. no indication that the system had failed was provided to signallers (paragraph 51);

c. the memory used for storing temporary speed restrictions in the RBC was volatile, allowing temporary speed restriction data to be lost during a rollover (paragraph 62);

d. the required level of safety integrity for validation of temporary speed restriction data uploaded to the RBC following a rollover was not achieved by the design (paragraph 67);

e. GEST server software was unable to detect and manage the corruption of its database (paragraph 75); and

f. the vulnerability of the system to a single point of failure had neither been detected nor corrected during the design, approval and testing phases of the Cambrian ERTMS project (paragraph 79).

Each of these factors is now considered in turn.

Temporary speed restriction upload

46 **Temporary speed restriction data was not uploaded to the RBC after a software rollover because the GEST sub-system had entered a fault condition, probably due to a corrupted database.**

47 The GEST sub-system includes features intended to receive temporary speed restriction data from signallers, transmit this data to the RBC, store this data and, if required, resend this data to the RBC following a rollover. Laboratory testing has shown that it is likely that the GEST sub-system entered a failure mode when the GEST server attempted to retrieve corrupted data from its own temporary speed restriction storage database. When the GEST sub-system is in this failed mode, described in this report as 'issue mode', the RBC would not be provided with temporary speed restriction data after a rollover. The details of how the GEST server software functions and the consequences of issue mode are provided in Appendix C, paragraphs C1 to C14.

48 The GEST server program is constructed from several smaller pieces of program known as threads. Each thread is written to perform a specific function, or group of functions, within the overall GEST server functionality. The thread responsible for providing temporary speed restriction data to the RBC, known as the 'Operation thread', failed and so caused 'issue mode'.

49 It is certain that database corruption would cause the absence of temporary speed restriction data following a rollover such as that on 19 October 2017. However, due to the overwriting of event log data and deletion of database information when service was restored on 20 October 2017 (paragraph 121), database corruption cannot be confirmed as the actual cause. It is possible that there was a different and unidentified problem within the GEST software programming, or an external factor such as electromagnetic interference, a power supply anomaly or an internal system timing issue which might also have triggered the failure of the Operation thread. However, no alternative explanation has been identified despite extensive investigations. A detailed explanation of how corruption of the database can cause a failure of the Operation thread, the supporting evidence and reasons for uncertainty are given in Appendix C, paragraphs C15 to C31.

50 The Cambrian ERTMS system was vulnerable to failure because the causal factors identified in this report were present in the software development process. As such, the safety learning relating to the design of high integrity systems is valid even in the unlikely event that database corruption was not the initiating event in this incident.

Signallers' display

51 No indication that the system had failed was provided to signallers.

52 After an RBC rollover, and before allowing movement authorities to be issued by the signalling system, signallers are required to check temporary speed restrictions have been loaded correctly on to the RBC[7] by checking they are shown correctly on the GEST terminal screen. Signallers can either scroll across the scaled schematic representation of the Cambrian lines checking each restriction status, or open a tabulated view of all restrictions in a dialogue box on the GEST terminal screen.

53 Signallers ensure the temporary speed restrictions have correctly loaded on the RBC by comparing the displayed restrictions to a printed copy of the imposed restrictions kept alongside the GEST terminal. If the displayed restrictions match those restrictions shown on the printed copy, the signallers are permitted to click an icon on the GEST terminal screen to unlock the RBC to resume the train service. The Ansaldo STS system developers had identified that this signaller check was necessary for the system to achieve the required safety integrity level (paragraph 73).

54 The temporary speed restriction data displayed by the GEST terminal is based on information provided by the RBC. This data is processed by the Operation thread of the GEST server to determine whether it is consistent with the corresponding data input by the signallers (Appendix C, paragraph C10). If consistent, the GEST terminal display shows temporary speed restrictions with green flags, as on figure 5. If there are inconsistencies these flags are coloured red.

55 As a consequence of the GEST server entering issue mode during the rollover on 19 October 2017, the GEST terminal was not provided with up-to-date information about the temporary speed restriction data held by the RBC after the rollover. The terminal continued to hold data from before the rollover when the temporary restrictions were being correctly applied by the RBC, and so the GEST terminal listed these as being applied and showed them with green flags (Appendix C, paragraph C24b).

56 The GEST server software has an internal check function, which activates the control button used by signallers to unlock the RBC after confirming the temporary speed restriction information held by the RBC is consistent with that previously input by the signallers. Any inconsistencies should have prevented this unlock button from being activated. However, on 19 October 2017, the GEST server issue mode meant that the unlock button was incorrectly activated.

57 The fact that all temporary speed restrictions were shown as applied, and the unlock key was activated, meant all information shown to the signallers using the GEST terminal following the 19 October 2017 RBC rollover gave a positive, but incorrect, indication that the temporary speed restrictions were in place and it was safe to resume the train service.

[7] Section 2.3.5 of the 'RCCS GEST User Manual' document reference CL-OM-00627.

58 When entering issue mode, testing showed the GEST server would generate an 'unknown exception' error message on a terminal screen located within the GEST server equipment enclosure and that some data normally recorded on an event log within the GEST server software would be absent. This event log is only saved for future use when commanded by the user and was provided for diagnostic purposes during the GEST sub-system development. The contents were not communicated to any other parts of the system. This event log was not captured during the service recovery process on 20 October 2017, so this data was not available to assist the investigation (paragraph 121). The unknown exception error message would have been indicated for a short time on the GEST server support terminal located in the signalling centre equipment room, and would have been visible to anyone using this terminal at the time. However, no staff are normally located in this room, signallers are not required to use this support terminal, and neither this terminal nor the GEST server data log are routinely used by the signalling technicians.

59 Had the signallers or the signalling technicians been aware of the unknown exception error message, it is unlikely that they would have understood its significance. Neither their training nor the user manual provided by Ansaldo STS referred to unknown exception occurrences.

60 Issue mode results in an unusual sequence of flag colours on the GEST terminal display during a rollover. In normal operation, the flags turn red as the GEST sub-system loses communication with the RBC and then disappear when RBC communication is restored prior to the restriction data being reloaded. Green flags then appear one by one as the temporary speed restrictions are reloaded and verified by the GEST server software. In issue mode, all the flags reappear simultaneously and coloured green. However, signallers were not required to observe this process happening and there is no evidence that they were aware of anything unusual immediately after the rollover.

61 Had the signallers attempted to apply a temporary speed restriction manually following the 19 October 2017 rollover, they would have been alerted to a problem with the GEST sub-system. However, this interaction was not normally necessary during the automated reloading process.

Volatile Memory

62 **The memory used for storing temporary speed restrictions in the RBC was volatile, allowing temporary speed restriction data to be lost during a rollover.**

63 The RBC was developed using two types of memory for the storage of data. Information relating to the infrastructure, including the permanent speed profile and geography of the railway, is stored in non-volatile memory which retains data during a power failure or software reset event. Temporary data, including temporary speed restrictions, is stored in volatile memory which does not retain data during a reset or power failure. This means that it is necessary to reload temporary speed restriction data from the GEST sub-system to the RBC after a rollover, such as occurred on 19 October 2017.

64 Software code, which had been part of another product used in Spain on the Madrid to Lerida high speed line, was adapted to create the GEST sub-system for use on both the French LGVEE high speed railway and the Cambrian lines project. At the time the Cambrian ERTMS was approved, the GEST sub-system was operationally similar to that proposed for the LGVEE project. The LGVEE RBC also used volatile memory to store temporary speed restriction data. For this reason, much of the safety case documentation assessed as part of the introduction of the GEST sub-system on the Cambrian line was based on that prepared for the LGVEE project.

65 Unlike on the Cambrian lines, track maintenance staff rather than signallers apply and remove temporary speed restrictions on the LGVEE. The track maintenance staff also use a GEST terminal, but this is in a location geographically separate to the signallers' control centre. As the LGVEE signallers are not required to apply and remove temporary speed restrictions, they do not have their own GEST terminal. Had the LGVEE RBC used volatile memory, it would have been necessary for the track maintenance staff to verify the temporary speed restrictions and unlock the RBC at the request of the signallers following a rollover. To avoid this undesirable situation, the LGVEE RBC was reconfigured to store temporary speed restrictions in non-volatile RBC memory. This prevented the loss of temporary speed restriction data from the RBC and removed the need for human verification after a rollover.

66 Had the Cambrian RBC been reconfigured to use non-volatile memory, as the LGVEE RBC was, the temporary speed restrictions would not have been lost on the Cambrian lines as they were on 19 October 2017. It would have been possible to retrospectively reconfigure the Cambrian RBC to use non-volatile memory even though it was in service. However, Ansaldo STS stated this was not considered necessary because the visual check done by the Cambrian signallers provided the necessary post-rollover cross checking of temporary speed restrictions (paragraph 73).

Safety integrity

67 **The required level of safety integrity for validation of temporary speed restriction data uploaded to the RBC following a rollover was not achieved by the design.**

68 Signalling systems are defined as reaching one of four discrete safety performance targets or safety integrity levels. The concept of safety integrity level (SIL) is taken from IEC 61508 'Functional safety of electrical/electronic/programmable electronic safety-related systems' (E/E/PE) published by the International Electrotechnical Commission (IEC).

69 The 1998 edition of IEC 61508 was applicable to the ERTMS design process and defined SIL as a *'discrete level for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where SIL 4 has the highest level of safety integrity and SIL 1 has the lowest'*.

70 The Cambrian ERTMS scheme was designed to comply with the requirements of the 2006 version of the CCS-TSI (paragraph 16). This outlined the safety requirement for the RBC as SIL 4 by stating:

> '*for the safety related part of one on-board assembly as well as for one track-side assembly … [was a] tolerable hazard rate (THR) of 10^{-9}/hour (for random failures) corresponding to Safety Integrity Level 4... Less restrictive safety requirements on THR values for track-side equipment may be adopted, provided that the safety objective for the service is met.'*

71 The CCS-TSI refers to technical documents prepared by a European rail industry working group (UNISIG) which contain detailed technical requirements for ERTMS systems. The safety requirements for ETCS level 2, as applied on the Cambrian scheme, were set out in UNISIG SUBSET-091 version 2.2.11, dated 10 August 2005, and included:

4.2.1.6 '*The role of ETCS … [is] to provide the Driver with information to allow him to drive the train safely and to enforce respect of this information.*'

4.2.1.8 '*The Core Hazard for the reference architecture is defined as exceedance of the safe speed / distance as advised to ETCS.*'

4.2.1.9 '*The maximum allowed rate of occurrence for the core hazard … [is] $2.0*10^{-9}$ / hour / train. This is the maximum Tolerable Hazard Rate (THR) for ETCS, denoted as THR_{ETCS}.*'

8.1.1.1 '*The safety integrity level will be derived from the different tolerable hazard rates. For Hazard Rates of < 10^{-9} dangerous failures per hour, a SIL 4 process will be applicable.*'

8.1.1.3 '*The dangerous failure for the ETCS trackside equipment is defined as failure to provide information to the ETCS onboard supervision in accordance with the data advised to the ETCS trackside from external entities.*'

9.2 '*The collection, interpretation, accuracy and allocation of data relating to the railway network shall be undertaken to a quality level commensurate with the SIL 4 allocation to the ETCS equipment.*'

Taken together, these requirements mean that the ETCS should prevent a train from travelling at more than the permitted speed with a safety integrity level of SIL 4. UNISIG SUBSET-091 does not include an exemption for temporary speed restrictions.

72 The integrity of speed management data could only be assured when temporary and permanent speed restriction data had been loaded and verified as correct on the RBC, and then only for as long as that data was retained within the RBC memory. The permanent speed profile for the Cambrian lines had been prepared as part of the design process and loaded into the RBC memory during the system installation. The profile was then validated during the commissioning process and permanently stored within non-volatile memory so it was not lost during a rollover. The RBC was designed to achieve SIL 4, so retaining this profile data within the RBC met the required integrity level.

73 Temporary speed restriction data was not retained in the RBC during a rollover because it was held in volatile memory. To avoid the need for this data to be manually reloaded, the GEST sub-system was programmed to detect an RBC rollover and automatically send the RBC a copy of the temporary speed restriction data stored in the GEST memory. However, because the GEST sub-system was designed to meet a SIL 2 safety integrity level, the Ansaldo STS designers incorporated an additional check intended to meet the specified requirements. This additional integrity check was performed with a human visual cross check undertaken by the GEST operator. This method of validating the integrity of transmitted data was reliant on the process which gives feedback to the operator, in this instance the display of temporary speed restriction data on the GEST terminal, being independent from the upload process.

74 The GEST server entering issue mode due to failure of the Operations thread on 19 October 2017 resulted in both the failure to upload the temporary speed restriction data to the RBC (paragraph 46), and the failure to provide the signallers with the correct information needed for them to undertake the human validation (paragraph 51). This demonstrated that the two functions were not independent and so the supplied system did not achieve the intended integrity level.

Programming

75 **GEST server software was unable to detect and manage the corruption of its database.**

76 It was necessary to supplement the GEST server volatile memory with its own database to store temporary speed restriction data for use when needed during a GEST reset. For this purpose, Ansaldo STS used a commercially available Structured Query Language (SQL) database management system. As each temporary speed restriction is applied, modified or removed by the signallers, copies of the updated restriction data are saved to the SQL database.

77 Information stored on an SQL database can become corrupted and so unreadable by the associated software. This was the most likely cause of the GEST server entering issue mode (paragraph 46 and Appendix C). The GEST server Operation thread software did not have effective defensive programming against such corruption.

78 Defensive programming is intended to implement appropriate precautions if data is invalid or has been corrupted. In this instance, the GEST software could have been designed to alert the signallers to such problems, and the need for these to be corrected. Examples of such programming include corruption testing of information obtained from a database, before any attempt to process, and/or incorporating software routines to manage errors generated by unexpected events such as the unknown exception (paragraph 58).

Safety assurance processes

79 **The vulnerability of the system to a single point of failure had neither been detected nor corrected during the design, approval and testing phases of the Cambrian ERTMS project.**

80 Taken together, the factors described in paragraphs 46 to 78 resulted in a system which was intended to have a high level of safety integrity, but did not achieve this following the rollover of the RBC. These shortcomings had neither been detected nor corrected during the design, approval and testing phases of the Cambrian ERTMS project due to a combination of the following:

a. the safety related software requirements for the GEST software were insufficiently defined (paragraph 81);

b. the hazard analysis process did not identify, and so failed to mitigate against, the GEST software thread failure mode (paragraph 88);

c. the validation process did not ensure that the safety requirement for the correct display of temporary speed restrictions was met (paragraph 94); and

d. GEST was accepted into service without the production of a generic product safety case (or equivalent); had such a process been followed rigorously, it would probably have exposed the shortcomings in the software design (paragraph 99).

Each of these sub-factors is now considered in turn.

Software requirements

81 **The safety related software requirements for the GEST software were insufficiently defined.**

82 To achieve the required safety integrity, the temporary speed restriction data held by the RBC had to be validated by the signallers' visual check of the GEST terminal display (paragraph 73). This validation applied to data entered manually and to data uploaded automatically after an RBC rollover. To provide the necessary assurance, the GEST terminal display always needed to correctly indicate the status of restrictions as stored in the RBC memory.

83 The Cambrian GEST sub-system was developed from requirements defined in the system requirements specification[8]. This document had three requirements relevant to the correct indication of temporary speed restrictions to signallers. These were included as English translations of requirements originally written in French. Where the system requirements refer to 'On restrictions' or 'restrictions ON', they relate to temporary speed restrictions loaded and stored in the RBC memory. The relevant system requirements were:

- **CAM_SRS_RCCS_GEST_0100_A:**

  The On restrictions are refreshed at the rate of sending messages from different RBC to constantly present to the operators the actual status of restrictions effective on the field.

[8] Project document title 'Route Control Centre (RCC) System Requirements Specification (SRS) ERTMS GEST', document reference 604321T709467301

- **CAM_SRS_RCCS_GEST_0224_A:**

  The cyclical transmission by each RBC of restrictions ON ensures a permanent consistency between the field data and the display of the GEST operators. Special provisions are made to manage any cases where a re-synchronisation is necessary.

- **CAM_SRS_RCCS_GEST_0245_A:**

  The RBC sends all the restrictions in place in cycles, the Human Machine Interface would be updated permanently from this information.

84 The system requirements were used to prepare software requirement specifications. This was done by Ansaldo STS engineers in France so that subsequent GEST design could be carried out by software engineers in the Ansaldo STS offices in Spain. This geographical split was a consequence of the decision to evolve the Cambrian GEST from a version previously developed by staff at the Spanish office of Ansaldo STS (paragraph 35).

85 The software requirements specification[9] for the GEST sub-system included the following:

- ***CAM_SWRS_RCCS_GEST_0118_A***

  GEST Client [the GEST terminal] shall display in real time and refresh cyclically the states of each TSR [temporary speed restriction] present in the system.

  [derived from CAM_SRS_RCCS_GEST_0100_A]

- ***CAM_SWRS_RCCS_GEST_0253_A***

  GEST Client shall show continuously the system's date and time.

  GEST server and client shall constantly display the current field status as sent by the RBC, refreshing periodically as new RBC messages are received and processed.

  [derived from CAM_SRS_RCCS_GEST_0100_A]

- ***CAM_SWRS_RCCS_GEST_0021_A***

  The cyclical transmission by each RBC of restrictions ON ensures a permanent consistency between the field data and the display of the GEST operators. Special provisions are made to manage any cases where a re-synchronisation is necessary.

  [a direct quote from CAM_SRS_RCCS_GEST_0224_A]

86 The software requirements specification did not include an item corresponding to system requirement CAM_SRS_RCCS_GEST_0245_A (paragraph 83).

[9] Project document title 'Route Control Centre (RCC) Software Requirements Specification (SWRS) ERTMS GEST' document reference 604321T709747901

87 Neither the system requirements nor the software requirements specification explicitly describe the need for restriction display data to be sent from the RBC to the GEST signallers' terminal display using a data path different from that used to apply the restrictions on the RBC. This independence was essential for the signallers' validation to achieve the necessary level of safety (paragraph 73). Without a written requirement, it is probable that the Ansaldo STS development and validation team in Spain were not aware of the need for diverse data paths, and so the GEST server software was developed incorporating a single point of failure by relying on the Operation thread to provide data to both the RBC and GEST terminal (paragraph 74).

Hazard analysis

88 **The hazard analysis process did not identify, and so did not mitigate against, the GEST software thread failure mode.**

89 A crucial part of electronic system development is the need to identify and mitigate hazards caused by system failures. European standard EN 50126-1 requires that a risk assessment is undertaken and a hazard log maintained for the safety lifecycle of the product. The standard requires the hazard analysis and risk assessment process to identify those specific requirements, known as safety requirements, which are necessary to achieve the system safety integrity. The implementation and validation of these critical safety requirements are required to be tracked throughout the safety life-cycle.

90 The analysis hazard log[10] for the GEST sub-system showed that a failure of the GEST sub-system to implement or display correct temporary speed restrictions had been considered during the hazard identification process. Two key safety requirements were identified which are relevant to the loss of temporary speed restrictions on 19 October 2017. These are:

- ***APR_A_MRR_CSEE_105:***

  The HMI [human machine interface] of the GEST workstation shall be validated.

- ***APR_C_MRR_CSEE_172:***

  The data displayed on GEST workstation shall always be consistent with the ones recorded in GEST servers and with the ones received from RBC, in order to guaranty [sic] the relevancy of these data.

91 These safety requirements demonstrate that achieving the required system safety level was intended to rely on a check, undertaken by signallers, to confirm that restrictions were correctly shown on the GEST terminal display. This implicitly relied on the system ensuring that the restrictions displayed were consistent with those stored on the RBC, and not vulnerable to a single point of failure which might compromise the integrity of that information.

92 The RAIB has not been able to establish why the hazard analysis process did not identify that two key functions of the GEST server relied on the single Operation thread, the failure of which could lead to the RBC holding incorrect data and the GEST terminal displaying out of date information to the signallers (paragraphs 46 and 51).

[10] Project document title 'GEST regression safety analysis (RSA)' document reference CL-SAF-00437

93 European standard EN 50129 requires designers to identify potential single point or common-mode failures within their products and provide suitable mitigations. Had the potential for the single failure of the Operation thread to undermine the system safety integrity been understood, it would have been possible to specify a mitigation such as:

- diverse paths for uploading restrictions to the RBC and sending RBC feedback to the GEST terminal; or
- monitoring of the GEST server's Operation thread for correct function.

Including either of these mitigations within the GEST server software would have prevented the loss of temporary speed restrictions on 19 October 2017.

Validation process

94 **The validation process did not ensure that the safety requirement for the correct display of temporary speed restrictions was met.**

95 EN 50128 requires tests to be devised and conducted on electronic products as part of the validation process. This process is intended to ensure that all requirements, including safety requirements, are met by the product, in this instance the GEST sub-system.

96 The RAIB reviewed the testing documentation with respect to the validation for safety requirement APR_C_MRR_CSEE_172 (paragraph 90). This safety requirement was intended to assure the consistent display of temporary speed restrictions on the GEST terminal display and was documented through to validation testing[11]. The relevant test was *'test 27, GEST HMI Interface'* recorded in the validation tests report[12].

97 The contents of test 27 did not define any testing which would provide assurance that the intent of safety requirement APR_C_MRR_CSEE_172 would be met. Test 27 also lacked any content to ensure that an alert would be provided to the signallers in the event of a software failure such as that described in Appendix C.

98 Due to the limitations of testing within a software environment which can include a very large number of variables, it is normally necessary to include theoretical analysis of failure modes as part of the validation of safety requirements. Ansaldo STS was not able to provide any documented evidence of theoretical analysis that safety requirement APR_C_MRR_CSEE_172 had been identified as vulnerable to a single software thread failure.

Assessment and approval process

99 **GEST was accepted into service without the production of a generic product safety case (or equivalent); had such a process been followed rigorously, it would probably have exposed the shortcomings in the software design.**

100 EN 50129 prescribes the use of the following categories of safety case:

- a generic product safety case, which aims to prove that a re-usable product, such as GEST which might be used in many different train control systems, meets a specified safety target;

[11] Project document title 'GEST regression safety analysis (RSA)' document reference CL-SAF-00437

[12] Project document title 'RCCS ERTMS / GEST Validation tests report' document reference 604321T709748801

- a generic application safety case, which aims to prove that a collection of products (such as the system comprising GEST, the RBC and the interlocking) meets a specified safety target for a particular type of application; and
- a specific application safety case, divided into two parts, one for the design and one for the physical implementation, which aim to prove the connected system will perform in only one particular installation, such as the Cambrian lines.

101 The guidance document supporting the application of EN 50126-1[13] states that a generic product safety case should define the conditions under which the specified safety target is achieved, and specify any interface to other products.

102 The Cambrian GEST sub-system safety justification relied on work being undertaken for the LGVEE project in France and an assessment of changes needed for the Cambrian project (paragraph 64).

103 The Cambrian GEST sub-system was included within the Cambrian RCC system generic application safety case[14]. This safety case was independently reviewed by Lloyd's Register Rail in its role as the ISA, before submission to Network Rail's SRP for approval (paragraph 34). The RCC generic application safety case included the 'GEST Safety Report'[15] which in turn referred to the 'GEST Regression Safety Analysis'[16]. This report considered the differences between the application of the proposed GEST sub-system as part of the LGVEE ERTMS system and as part of the Cambrian ERTMS system.

104 The GEST safety report, which was prepared by Ansaldo STS and countersigned by Network Rail, included as paragraph 4.1:

'The Cambrian version of GEST is based on the product produced for the LGVEE project. The LGVEE product meets safety requirements and achieves the required SIL 2 integrity level. This Safety Report demonstrates that the modifications to the LGVEE product maintain the safety integrity level of the products, and that the appropriate safety analyses have identified the safety requirements on the operating environment necessary to maintain the safety of the GEST in generic Network Rail applications to an acceptable level. The Trackside ERTMS and Signalling System Safety Case demonstrates that the overall specific application design and configuration for Cambrian is safe, that the defined data preparation processes have been followed, that adequate testing has been carried out, and that the safety requirements have been met.'

105 This text included a positive statement that the LGVEE GEST sub-system had met the intended safety requirements for that project, and the Cambrian version met Network Rail's requirements. The text does not mention that the LGVEE system design was not complete, or the potential for the design of GEST to require amendment. Recognition that the LGVEE system design was still subject to change, might have led the ISA or Network Rail's SRP to undertake a further review of any subsequent change made to the GEST product.

---

[13] Standard guidance document titled 'Guide to the application of EN 50126-1 for safety', CLC/TR 50126-2:2007

[14] Project document title 'RCC generic application safety case' document reference CL-SAF-00428.

[15] Project document reference CL-SAF-00752.

[16] Project document reference CL-SAF-00437.

106 When documenting the results of its assessment, Lloyd's Register Rail categorised its findings on a rising scale, a category 1 comment representing a finding of the most serious safety related nature. Lloyd's Register Rail raised a category 1 observation that it had not seen an ISA report showing that a full independent safety assessment had been carried out of 'the correct GEST LGVEE baseline', and requested that Ansaldo STS should provide a copy of such a report. This would normally have been based on an ISA review of a generic product safety case. Ansaldo STS responded that there was no product safety case for GEST as the LGVEE project client, SNCF, had not required one. Hitachi STS (formerly Ansaldo STS) has subsequently advised the RAIB that it would not have been possible to prepare a product safety case for GEST, as the sub-system is based on a commercially available hardware and software platform. The safety analysis was therefore included within the RCC generic application safety case.

107 In response to Lloyd's Register Rail's request, Ansaldo STS provided a copy of SNCF's review[17] of an Ansaldo STS document covering the entire LGVEE ERTMS system, which incorporated the GEST sub-system[18]. SNCF's review identified five issues relevant to GEST, all of which were closed within LGVEE project documentation following responses made by Ansaldo STS.

108 The documentation provided to Lloyd's Register Rail related to SNCF's review which had been carried out before the LGVEE ERTMS system was commissioned. In the time between this version of the SNCF review document and the commissioning of the LGVEE ERTMS system, the LGVEE RBC was modified to store temporary speed restrictions in non-volatile memory and to manage them to SIL 4 (paragraph 65).

109 The RAIB has reviewed the Ansaldo STS safety case documents covering the GEST sub-system and concluded they were not an adequate substitute for a generic product safety case (paragraph 100), because they did not identify the safety integrity required for storage and automatic replication of temporary speed restriction data by GEST following an RBC rollover.

110 Following receipt of the SNCF assessment report, it would have been possible for Lloyd's Register Rail to either request further justification from Ansaldo STS (such as the validation phase safety analysis), report its findings to SRP for further review, or close its observation (paragraph 106). Lloyd's Register Rail closed the observation, concluding that the SNCF review demonstrated the baseline GEST had been independently assessed with no significant issues outstanding. This observation was closed prior to the commissioning of the baseline GEST sub-system on LGVEE, and so subsequent changes to the equipment would not be accounted for.

111 Had Lloyd's Register Rail sought further justification from Ansaldo STS about how the GEST sub-system was capable of meeting the stated safety requirements, or left the observation open, Network Rail's SRP would have been given greater visibility of the deviation from the generic product safety case process. It is then possible that SRP would have required further assurance regarding the design of the GEST sub-system and underlying assumptions.

---

[17] 'Compte rendu de remarques SNCF sur le document: Document d'Analyse de la Sécurité en Phase de Validation du système ERTMS' [RAIB translation: 'Record of SNCF comments on the document: ERTMS System Validation Phase Safety Analysis'] reference IG.SF1/ERTMS/PEEE/DASV/C/0c.

[18] Project document reference 607100 T 7046522-00.

112 GEST was neither part of the ERTMS reference architecture to which technical standards for interoperability apply (paragraph 33), nor did it directly perform any function related to interoperability. Therefore the Notified Body (NoBo) which assessed the Cambrian ERTMS system against the CCS-TSI was not required to assess in any detail how the GEST sub-system worked.

Identification of underlying factors

Understanding of the system

113 **Ansaldo STS did not appreciate the latent single point of failure within the GEST sub-system software.**

114 The GEST server software was developed with a latent single point of failure which could result in temporary speed restriction data stored on the RBC being incorrectly displayed to the signallers (paragraphs 46 and 51). The decisions made during development and after commissioning of the Cambrian ERTMS system indicate a lack of understanding within Ansaldo STS of the GEST sub-system's vulnerabilities. Evidence for this lack of understanding is:

- the system hazard analysis process did not identify, and so did not mitigate against, the GEST server software thread failure (paragraphs 89 to 92);
- the testing intended to validate the correct display of restrictions did not test the product against the possibility of a single thread failure (paragraphs 95 to 97); and
- the decision to not consider the retrospective fitment of non-volatile memory, as used on the LGVEE RBC, was based on the understanding that the signallers' GEST terminal display provided a reliable indication of the restrictions stored on the RBC at all times (paragraph 66).

115 The RAIB has not attempted to establish the exact circumstances which led to Ansaldo STS overlooking the GEST sub-system vulnerabilities. Establishing these historical circumstances would be unlikely to identify further safety learning, as the processes used by all organisations involved with the project have evolved considerably since this vulnerability was overlooked.

116 **Network Rail input did not include effective client role checks to identify the design process shortcomings.**

117 The processes defined in the European standards for the procurement of high integrity systems such as the Cambrian ERTMS system, require the client to be involved in the development of the system (paragraph 37). Network Rail's role therefore included the review and acceptance of the GEST safety case, including the associated system requirements specification and software requirements specification, prepared by Ansaldo STS. This review was carried out but did not identify the following shortcomings in the documents:

- reliance on documents which omitted critical assumptions about operation of GEST and related to a version of GEST liable to change (and which did change) as the design of the LGVEE progressed (paragraphs 104 and 105);
- omission of the non-standard process being used in place of a generic product safety case for the GEST sub-system (paragraph 99); and

- absence of a diverse path requirement for data passing through the GEST server in the system requirements specification and the software requirements specification (paragraph 87).

118 The RAIB's view is that these shortcomings should have been recognised within the client role required by the EN 501xx series of European standards current during the Cambrian ERTMS development (paragraph 37). This is supported by RSSB guidance note GEGN8650, which provides assistance for clients procuring high integrity software. Although published in March 2017, the interpretation of client responsibilities is based on parts of the EN 501xx series which were unaltered from the version applicable during the Cambrian ERTMS development.

119 GEGN8650 stresses the importance of the client playing an active part in the production and review of requirements in the early stages of the software development. GEGN8650 identifies common issues which, if left unresolved, can lead to faults in the final software product. These include omissions in the requirements, incorrect specification of the software architecture and a lack of design in the code to deal with erroneous or unexpected parameters.

120 The Cambrian ERTMS system was procured by Network Rail as an early deployment of ERTMS technology in the UK, and as such Network Rail had limited experience of this technology. To obtain the necessary skills and experience, Network Rail employed a number of contract staff already experienced in the deployment of ERTMS signalling projects elsewhere, and established several review groups including experts from outside Network Rail, specifically tasked with ensuring that the ERTMS deployment met operating requirements. In addition, the duties assigned by Network Rail to the ISA included assessing safety justification documentation in the early development stages of the project. Remit documentation provided by Network Rail indicates that the review groups and the ISA were not remitted to critically assess the GEST sub-system or software requirements specifications. The RAIB considers that, at the time, Network Rail probably lacked the necessary experience and support to critically review the detailed GEST requirements documentation with the necessary level of rigour.

Observations

121 **Preserving data deleted during the attempts to recover the train service would have assisted the safety investigation.**

122 During the attempts to recover the train service after the reported loss of temporary speed restrictions, database information was deleted and system event logs overwritten. This information and the logs would have assisted the investigation and provided positive confirmation of the initial failure mode. It was necessary to cleanse data from the system, but neither Network Rail nor Ansaldo STS had provided guidance concerning the data which should be saved before cleansing to assist later analysis.

123 Without clear guidance, it was necessary for the Network Rail signalling technician and Ansaldo STS maintenance support engineer to improvise a plan based on their shared experience of download times and how useful such data had been in the past. Although data contained in the SILAM log was saved, data contained in the GEST server event log and SQL database was not saved. This information would have removed uncertainty regarding whether the GEST server had entered issue mode (paragraph 58), and would have shown whether the SQL database was corrupted (paragraph 49). This data was not saved during the recovery process because it had not previously been of use.

124 **Defensive rollovers of the RBC were occurring 10-12 times a year, so not meeting the expected performance of a high integrity system and placing an undesirable reliance on the signallers to provide the necessary safety integrity.**

125 The sequence of events leading to the loss of temporary speed restrictions included an automated defensive rollover triggered when the RBC attempted to resolve an operating situation unforeseen by the RBC software programmers. In such circumstances, it is safer to reboot the RBC in a controlled manner (a rollover) rather than allowing an uncontrolled, and potentially unsafe, response. The number of RBC rollovers has been decreasing since the initial project commissioning, but data supplied by Network Rail indicates that the mean time between RBC software failures which affect the train service is less than a third of the reliability-driven target. Network Rail reports that most of the failures relate to the RBC not sending a movement authority, and this type of failure does not result in an unsafe situation. Network Rail and Hitachi STS are working to reduce the number of defensive rollovers (paragraph 147).

126 **Network Rail is not acquiring the corporate knowledge of failure analysis required for future high integrity software system development.**

127 Network Rail's signalling management role requires it to use learning from previous events to influence the design, installation, testing, maintenance and use of equipment throughout its network. This is the final phase of the development lifecycle (figure 8) and requires both collection and analysis of system operation data. In many instances relating to high integrity software, this is a 'client' role, as implementation of technical solutions and changes must be carried out by an appropriate signalling supplier.

128 To facilitate this activity, RSSB introduced Railway Group Standard GE/RT8106 'Management of Safety Related Control, Command and Signalling (CCS) System Failures' in October 2008. This document was intended to provide a standard reporting platform for the recording of signalling failures. Using a standard template allows failures to be placed into classifications by failure type, facilitating thematic and other statistical analysis.

129 GE/RT8106 contained a blank template for ERTMS/ETCS failure reporting, but the failure mode categories were not populated due to a lack of experience with the emerging technology. GE/RT8106 was updated in December 2011 and replaced in September 2016 with RIS-0707-CCS[19]. RIS-0707-CCS reproduced the relevant text from GE/RT8106 issue two in its entirety. This included the blank reporting template for ERTMS/ETCS failures.

[19] Rail Industry Standards (RIS) are standards published by RSSB and compliance is a requirement of the infrastructure management licence conditions for companies such as Network Rail.

130 New control and command projects, such as the Cambrian ERTMS, adopt a 'defect reporting analysis and corrective action system' known as DRACAS which remains in place until the new system has reached a level of maturity considered acceptable for handover to the regular maintenance teams. Defect monitoring is then transferred to the RIS-0707-CCS reporting system.

131 DRACAS defects are logged in a database which is regularly reviewed and closed only when the solution has been implemented to the satisfaction of the stakeholders. In the case of the Cambrian lines, solutions are reviewed before closure by representatives from Hitachi STS (formerly Ansaldo STS), the train operator and Network Rail's maintenance and operations management staff.

132 Network Rail has stated that defects found with the Cambrian ERTMS system are being managed locally using a more detailed process than that required by RIS-0707-CCS, and with an intent to migrate directly to a replacement and more comprehensive defect reporting system using learning from the Cambrian project.

133 There is considerable overlap in safety considerations applicable to high integrity software systems in different disciplines. For example, development of high integrity signalling software could benefit from lessons learnt in the development and use of the complex software used for the supervision and remote control of electrical switching equipment (SCADA), and vice versa. Reporting systems such as RIS-0707-CCS are discipline specific, and although Network Rail and RSSB[20] have undertaken research into a comprehensive reporting system, the rail industry does not have a formal process for transferring such information between disciplines.

134 The RAIB found no evidence that Network Rail has a formal process for gaining knowledge by analysis of data obtained using the RIS-0707-CCS reporting process, no formal process for gathering and transferring such knowledge between disciplines and no formal process to make this knowledge available during future procurement activities. This analysis and dissemination of the resulting knowledge is an essential part of fulfilling the client role in the development of high integrity software.

135 **All of the temporary speed restrictions lost from the signalling system on the Cambrian lines had been retained beyond the time normally permitted by rail industry standards.**

136 Seven temporary speed restrictions had been introduced on the Cambrian Coast line between 2014 and 2016 to provide level crossing users with sufficient warning of approaching trains. At the time of the incident they were still in place.

137 The applicable rail industry standard[21] describes a temporary speed restriction as not normally in place for more than six months. A temporary speed restriction can be removed if the restriction is no longer needed or by incorporating it into the permanent line speed profile.

138 Network Rail has stated that the Cambrian Coast temporary speed restrictions had not been made permanent because it was in the process of implementing a plan to close or upgrade the level crossings, where practicable, in preference to a permanent reduction in speed.

[20] Research project T960 - Specification of a defect recording and corrective actions system architecture and process framework.

[21] RIS-0735-CCS Signing of temporary and emergency speed restrictions, issue 1, December 2018

139 On non-ERTMS equipped Network Rail infrastructure, achieving the required level of safety assurance for temporary speed restriction information depends on drivers recalling temporary speed restrictions in combination with lineside warning signs and magnets fitted between the rails triggering the automatic warning system to sound in the train cab. Drivers should make themselves aware of temporary speed restrictions by reading their weekly operating notices (paragraph 22) and are required, by the railway Rule Book, to report to the signaller where signage is found to be missing or out of place.

140 The Cambrian ERTMS does not rely on drivers' recollection of this information, as the combination of the permitted speed displayed on the DMI and automatic supervision of the speed of the train by the ERTMS equipment provides the necessary assurance. However, drivers are still required to familiarise themselves with temporary speed restrictions on the Cambrian lines and report if they are not shown on the DMI.

141 The long-term retention of temporary speed restrictions, and the three drivers not reporting the missing temporary speed restrictions on the day of the incident, are undesirable in ERTMS equipped areas and not in accordance with the intent of the rail industry standards. However, these issues should have had no impact on the safety of the Cambrian lines because ERTMS is intended to manage temporary speed restrictions to SIL 4. For this reason, this report does not contain recommendations relating to the long-term retention of temporary speed restrictions, or drivers' use of weekly operating notices. However, since railway staff place a high level of reliance on the speed information provided by ERTMS, which may override their recollection of information in the weekly operating notices, it is important that SIL 4 is delivered by the system.

Summary of conclusions

Immediate cause

142 The ERTMS signalling system was returned to service following an RBC software rollover without temporary speed restriction information for transmission to trains (paragraph 44).

Causal factors

143 The causal factors were:

a. temporary speed restriction data was not uploaded to the RBC after a software rollover because the GEST sub-system had entered a fault condition, probably due to a corrupted database (paragraph 46, **Recommendation 5**);

b. no indication that the system had failed was provided to signallers (paragraph 51, **Recommendation 2**);

c. the memory used for storing temporary speed restrictions in the RBC was volatile, allowing temporary speed restriction data to be lost during a rollover (paragraph 62, no recommendation);

d. the required level of safety integrity for validation of temporary speed restriction data uploaded to the RBC following a rollover was not achieved by the design (paragraph 67, **Recommendations 1 and 2**);

e. GEST server software was unable to detect and manage the corruption of its database (paragraph 75, **Recommendation 2**); and

f. the vulnerability of the system to a single point of failure had neither been detected nor corrected during the design, approval and testing phases of the Cambrian ERTMS project due to a combination of the following:

   i. the safety related software requirements for the GEST software were insufficiently defined (paragraph 81, **Recommendations 1 and 2**);

   ii. the hazard analysis process did not identify, and so did not mitigate against, the GEST software thread failure mode. (paragraph 88, **Recommendation 2**);

   iii. the validation process did not ensure that the safety requirement for the correct display of temporary speed restrictions was met (paragraph 94, **Recommendations 1 and 2**); and

   iv. GEST was accepted into service without the production of a generic product safety case (or equivalent); had such a process been followed rigorously, it would probably have exposed the shortcomings in the software design (paragraph 99, actions taken paragraph 149, **Recommendations 1 and 2**, **Learning points 2 and 3**).

Underlying factors

144 The underlying factors were:

a. Ansaldo STS did not appreciate the latent single point of failure within the GEST sub-system software (paragraph 113, **Recommendation 2**); and

b. Network Rail input did not include effective client role checks to identify the design process shortcomings (paragraph 116, **Recommendation 1**, **Learning point 4**).

Observations

145 Although not linked to the incident on 19 October 2017, the RAIB observes that:

a. preserving data deleted during the attempts to recover the train service would have assisted the safety investigation (paragraph 121, **Recommendation 4**);

b. defensive rollovers of the RBC were occurring 10-12 times a year, so not meeting the expected performance of a high integrity system and placing an undesirable reliance on the signallers to provide the necessary safety integrity (paragraph 124 and actions taken paragraph 147);

c. Network Rail is not acquiring the corporate knowledge required to minimise the likelihood of future failures in high integrity software systems (paragraph 126, **Recommendation 3**); and

d. all of the temporary speed restrictions lost from the signalling system on the Cambrian lines had been retained beyond the time normally permitted by rail industry standards (paragraph 135, no recommendation for ERTMS equipped lines, **Learning point 1**).

Actions reported as already taken or in progress relevant to this report

146 Shortly after the incident, a new control centre instruction was issued at Machynlleth. This required all temporary speed restrictions to be entered manually, and verified by a test train, before normal operations were resumed after a rollover. It has since been revised to require a rollover to be followed by a second, manually triggered reset, during which the correct uploading of temporary speed restrictions is checked and then independently verified by signalling centre staff using the SILAM data logger. In addition, local maintenance staff carry out a daily verification that temporary restrictions are being transmitted to trains.

Actions reported that address factors which otherwise would have resulted in a RAIB recommendation

147 Hitachi STS (formally Ansaldo STS), working with Network Rail, is continuing an initiative to reduce the number of defensive RBC rollovers on the Cambrian lines. Historical data is used to grade rollovers by frequency of occurrence. Hitachi STS has used this data to prioritise the development of software improvements to fix recurring issues. Hitachi STS has reported that the cause of type 5c rollovers, one of the more frequent rollovers and the type experienced on 19 October 2017, has been removed in an update of the Cambrian lines software commissioned in March 2019.

148 Hitachi STS has stated that it has been developing its internal processes over several projects since the design of the Cambrian ERTMS commissioning. Improvements have been made in the safety analysis and validation processes, in particular where common safety methods are employed such as system impact and safety system impact analysis. Hitachi STS also states that improvements have come from the application of EN 50128:2011 in place of EN 50128:2001 and through obtaining IRIS Certification based on ISO/TS 22163:2017 and Certification rules:2017.

149 Ricardo Rail/Ricardo Certification has stated that it has revised its assessment processes as part of the work necessary to become a UKAS accredited independent safety assessment service. The revised processes also incorporate the changes required by the Common Safety Method for Risk Evaluation and Assessment (Commission Regulation (EU) 402/2013) in April 2013. Modifications to these assessment processes mean they are more systematic in confirming that there is evidence that safety requirements have been met by ensuring:

a. all reasonably foreseeable hazards are identified;

b. assumptions that underpin the safety behaviours of systems are identified and defined/written down (in system definitions); and

c. evidence is sought for the implementation of all safety requirements associated with hazards.

Recommendations and learning points

Recommendations

150 The following recommendations are made[22]:

1 *The intent of this recommendation is to ensure clear and effective instruction is given to staff discharging the client role responsibilities essential for the safe introduction of new and modified high integrity software-based systems. Implementation is expected to take account of RSSB Guidance Note GEGN8650, 'Guidance on high integrity software-based systems for railway applications'.*

Network Rail, in consultation with RSSB and the wider rail industry and drawing on existing processes where appropriate, should develop and implement a mandatory safety assurance procedure (and associated guidance) for its client role on projects involving installation and modification of high integrity software-based systems. The process should incorporate relevant best practice from other safety critical industries. It should clearly define the role of the client in each of the following areas:

- clearly documenting its expectation of each supplier as part of the project's overall safety assurance process, including the required safety justifications, documentation and the traceability of safety evidence throughout the project's life cycle;
- selection of suppliers that are competent and capable of delivering a safe system;
- specifying the role of independent safety assessment bodies, such as ASBOs (assessment bodies);
- capturing the need for good engineering safety management, robust configuration management and change control in the contractual requirements;
- defining the required safety integrity of the key safety functions, the operational context and external interfaces;

[22] Those identified in the recommendations have a general and ongoing obligation to comply with health and safety legislation, and need to take these recommendations into account in ensuring the safety of their employees and others.

Additionally, for the purposes of regulation 12(1) of the Railways (Accident Investigation and Reporting) Regulations 2005, these recommendations are addressed to the Office of Rail and Road to enable it to carry out its duties under regulation 12(2) to:

(a) ensure that recommendations are duly considered and where appropriate acted upon; and

(b) report back to RAIB details of any implementation measures, or the reasons why no implementation measures are being taken.

Copies of both the regulations and the accompanying guidance notes (paragraphs 200 to 203) can be found on RAIB's website www.gov.uk/raib.

- the process to be applied when placing reliance on the re-use or adaptation of a system with previous acceptance, or commercial off-the-shelf products;
- working with the supplier to properly understand the safety risks and define the system safety requirements and architecture;
- monitoring the supplier's verification of its design (hardware and software);
- ensuring that the design is suitably validated prior to commissioning;
- audit and inspection by the client;
- the extent of the client's review of independent assessments, and its own consideration of the safety justifications as part of the approval process;
- testing and commissioning of the installed system, and subsequent maintenance; and
- recording and retaining data needed for investigation of safety related failures.

This procedure should be shared with the wider rail industry with a view to it being adopted by other potential clients of high integrity software-based systems, such as train operators and rolling stock owners.

(paragraphs 143d, 143f (i, iii and iv))

2 *The intent of this recommendation is to reduce the likelihood of a safety critical failure of a high integrity software-based system caused by a deficient safety assurance process and taking account of the changes made since the design of the Cambrian ERTMS system (paragraph 148).*

Hitachi STS should take account of the findings of this report in a review, and where necessary improvement, of its current safety management processes for the design, design verification, design validation, and retention of records for high integrity software-based systems. This review should ensure that processes ensure the correct identification, and subsequent achievement, of software safety requirements based on a correct understanding of the system architecture and any differences between the intended application and the generic product. The process shall also ensure that sufficient analysis is undertaken to identify areas of potential weakness, such as the absence of diverse data paths, and to enable the implementation of suitable protection measures such as:

- the use of error messages generated by internal equipment functions to alert users to potential failures of the safety critical system; and
- the inclusion and subsequent validation of defensive programming within the software development phase when using storage (such as an SQL database) to protect software from entering an unpredictable or unsafe state.

(paragraphs 143b, 143d, 143e, 143f (i, ii, iii and iv))

3 *The intent of this recommendation is to complete and extend the current processes for capturing control, command and signalling system failures adopted by Network Rail so development and maintenance of high integrity (safety critical) software takes account of relevant learning from all disciplines.*

Network Rail, in consultation with RSSB and the wider railway industry, should review and, where necessary, improve the capture and dissemination of safety learning available through the reporting and systematic investigation of complex software-based system failures. This should include:

- appropriate measures to ensure capture and retention of data which could prove useful for investigating any future safety related failure;
- completing the documenting and categorising of safety critical ERTMS/ETCS failures;
- identification of and implementing suitable means of collecting relevant information from all disciplines; and
- assimilation of relevant information by staff from appropriate disciplines and those specialising in systems engineering.

(paragraph 145c)

4 *The intent of this recommendation is to ensure that data crucial to an investigation, which might otherwise be lost while attempting to recover the train service, is retained after any future control system failure on the Cambrian lines. The recommendation addresses the need for location specific instructions when it is impractical to include necessary detail in documents applying across the rail network.*

Network Rail, in conjunction with Hitachi STS, should implement a procedure to ensure the capture and retention of data which could prove useful for investigating any future safety related failure of the European Rail Traffic Management system (ERTMS) on the Cambrian lines. Implementation should, if appropriate, include installation of additional or modified equipment. Consideration should be given to the periodical download of data as well as specifying a process to be followed during a recovery of service (paragraph 145a).

5 *The intent of this recommendation is to provide a technological fix for the failure mode experienced on the Cambrian lines. This should remove the current reliance on procedures to ensure temporary speed restrictions are applied correctly following an RBC rollover.*

Hitachi STS should provide a technical solution meeting the intended safety integrity level (SIL) 4 to ensure that the radio block centre (RBC) on the Cambrian lines contains correct temporary speed restriction information when restored to service after a rollover (paragraph 143a).

Learning points

151 The RAIB has identified the following learning points[23]:

1 This investigation shows how drivers can avoid accidents and incidents by promptly reporting inconsistencies between information they are required to read in weekly operating notices and other information presented to them (paragraph 145d).

2 Independent safety assessment bodies (including ASBOs) are reminded to apply extra vigilance when a safety justification is based on previous use on a project that did not follow the specified requirements of European standard EN 50126-1; and to ensure that a product's previous application was comparable to that now planned (paragraph 143f iv).

3 Independent safety assessment bodies (including ASBOs) are reminded of the need to understand the scope and thoroughness of any review undertaken by others before accepting their conclusions. The other assessment body might be undertaking product assessments to a different project development stage or requirement (paragraph 143f iv).

4 The importance of clients understanding and undertaking their role in procuring safety critical high integrity software is demonstrated by this investigation. Relevant guidance is given in RSSB Guidance Note GEGN8650, 'Guidance on high integrity software-based systems for railway applications' (paragraph 144b).

5 Organisations procuring and implementing ERTMS projects should note that the specification for this system requires management of temporary speed restrictions to achieve safety integrity level 4 (SIL4) (paragraph 145d).

[23] 'Learning points' are intended to disseminate safety learning that is not covered by a recommendation. They are included in a report when the RAIB wishes to reinforce the importance of compliance with existing safety arrangements (where the RAIB has not identified management issues that justify a recommendation) and the consequences of failing to do so. They also record good practice and actions already taken by industry bodies that may have a wider application.

Appendices

Appendix A - Glossary of abbreviations and acronyms

AIBN	Accident Investigation Board of Norway
ASBO	An assessment body as referred to in Article 6 of European Regulation 402/2013 (the regulation on a common safety method for risk evaluation and assessment).
CCS-TSI	Control-Command and Signalling Technical Specification for Interoperability
CENELEC	Comité Européen de Normalisation Électrotechnique
DMI	Driver Machine Interface
E/E/PE	Electrical/Electronic/Programmable Electronic
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
GEST	poste de GEstion des Signalisations Temporaires
GSM-R	Global System for Mobile Communications - Railway
HMI	Human Machine Interface
IEC	International Electrotechnical Committee
ISA	Independent Safety Assessor
JRU	Juridical Recording Unit
LGVEE	Lignes à Grande Vitesse Est Européenne
NoBo	Notified Body
RAIB	Rail Accident Investigation Branch
RAMS	Reliability, Availability, Maintainability and Safety
RBC	Radio Block Centre
RCC	Rail Control Centre
RIS	Rail Industry Standard
RSSB	Organisation formally known as the Rail Safety and Standards Board
SCADA	Supervisory Control And Data Acquisition
SIL	Safety Integrity Level

Appendix A - Glossary of abbreviations and acronyms

SILAM / SICAM	Système Local d'Aide à la Maintenance / Système Central d'Aide à la Maintenance
SNCF	The French national state owned railway company
SQL	Structured Query Language
SRP	System Review Panel
THR	Tolerable Hazard Rate
TSI	Technical Standard for Interoperability
UK	United Kingdom
UKAS	United Kingdom Accreditation Service
UNISIG	Industrial consortium created to develop the ERTMS/ETCS technical specifications

Appendix B - Investigation details

The RAIB used the following sources of evidence in this investigation:

- information provided by witnesses;
- information taken from the on-train data recorders, known as Juridical Recording Units (JRU);
- testing undertaken at Hitachi STS systems laboratory;
- data recovered from Machynlleth signalling centre;
- Cambrian ERTMS and LGVEE project design and approval documentation;
- Network Rail standards and procedures;
- Cenelec EN 501xx standards; and
- European technical standards for interoperability.

Appendix C - Detailed description of GEST software failure

C1 The loss of temporary speed restrictions on the Cambrian lines was caused by a latent single point of failure within the train control and command system which did not detect or protect against an internal GEST server software failure (paragraph 79).

C2 A latent software design error within the GEST server meant it was possible for the GEST sub-system to enter a degraded mode of operation, referred to in this report as 'issue mode'. In this condition, the GEST server would appear to operate normally, but:

- would not provide temporary speed restriction data to the RBC in the event of a rollover; and
- the GEST terminal could display temporary speed restriction data differing from that in the RBC.

GEST server operation

C3 The Cambrian lines GEST server acts as the interface between, and has direct communication links to, the GEST terminal and the RBC to allow, in addition to other functions, management of temporary speed restriction data. The GEST server is duplicated for redundancy with a master and slave relationship allowing a hot changeover when necessary. Only one GEST server, the master, is communicating to the RBC and GEST terminal at any time.

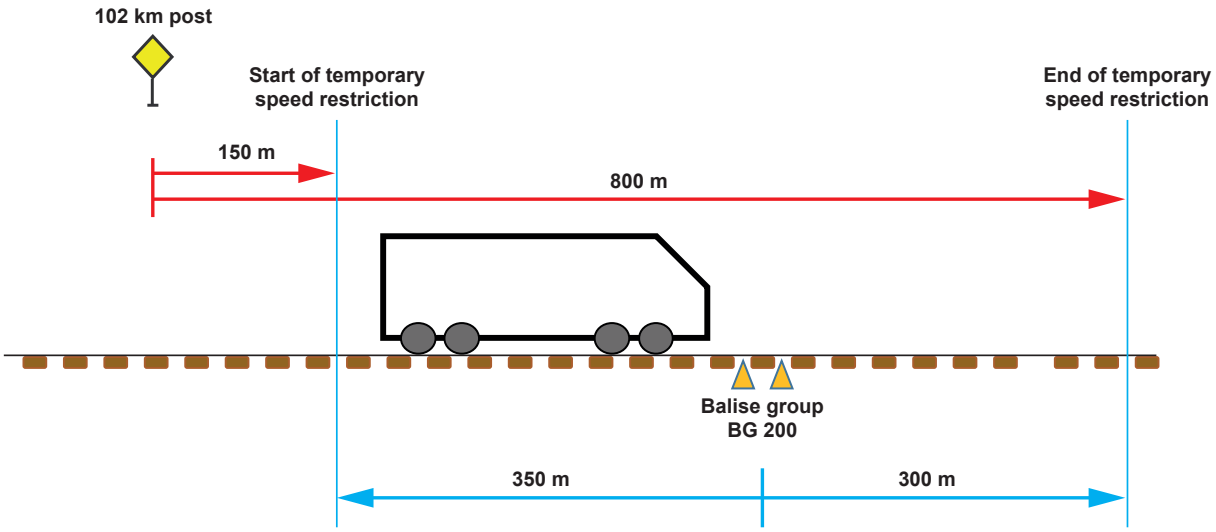
C4 Signallers apply, edit and remove temporary speed restrictions using the GEST terminal. Each temporary speed restriction requires a unique identity, the speed and location of the restriction. Together, this information is called a data set.

C5 Data sets exchanged between the GEST terminal and GEST server refer to the location of a temporary speed restriction in kilometres. Data sets exchanged between the GEST server and the RBC contain similar information, but the location is expressed as a distance to the nearest balise[24] group (figure C1). The GEST software converts restriction data between balise and kilometre formats as necessary with both sets of data using the same identity for corresponding restrictions.

C6 While operating, GEST uses restriction data stored in volatile memory within the GEST server. As the content of this volatile memory is lost during a server reset, data is also stored by the master GEST server software in an SQL database. The SQL database stores the temporary speed restriction data on a hard drive in both balise and kilometre formats. The master and slave server SQL databases are linked and the slave database is updated with data from the master SQL database every 5 seconds, or when a change is made, to ensure it contains current temporary speed restriction data (figure C2).

C7 In the event of the master GEST server being reset, the slave server will automatically become the master and retrieve temporary speed restriction data from its SQL database. The server will then send the kilometre data to the GEST terminal, connect to the RBC and receive the balise group data stored on the RBC.

[24] A balise is a transponder device located between the running rails which acts as a datum for passing trains to determine their exact location without reliance on an odometer which might contain an error.



Data Format	Kilometre based data set as used by GEST terminal	Balise Group based data set as used by RBC
Restriction Identity	TSR01	TSR01
Restriction Speed	20 km/h	20 km/h
Restriction Start	102 km 150 m	BG 200 – 350 m
Restriction End	102 km 800 m	BG 200 + 300 m

Figure C1: Diagram showing how the same temporary speed restriction location is expressed in kilometres or distance to balise group data sets

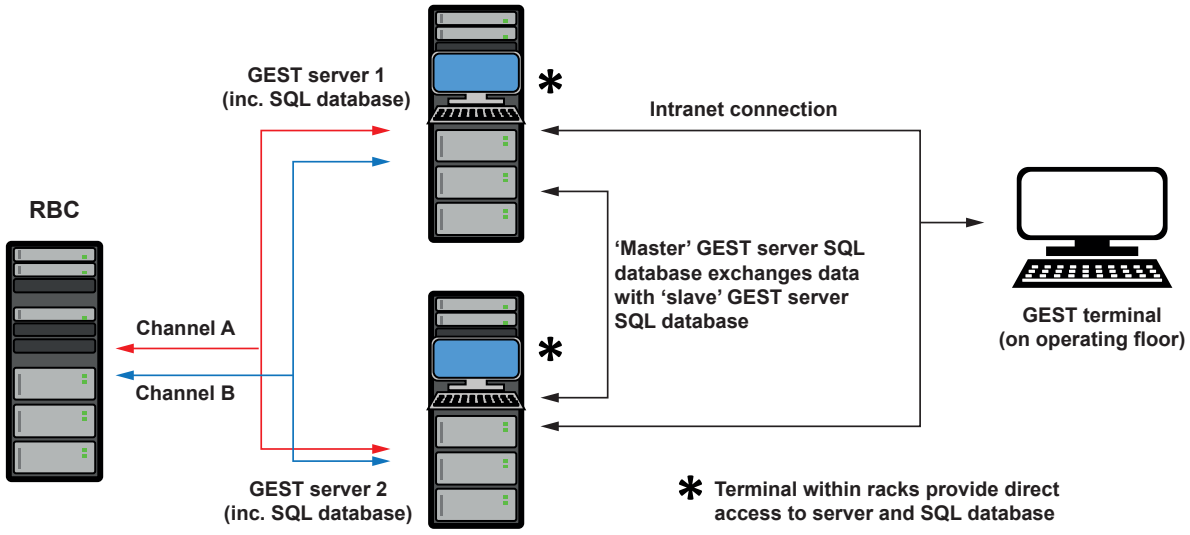


Figure C2: Relationship of duplicated GEST servers, RBC and GEST terminal

Software construct

C8 The GEST server software is intended to take restriction data input by signallers at the GEST terminal keyboard, store this in both memory and the SQL database as necessary, and upload it to the RBC. So that signallers know which restrictions are being applied by the RBC, the GEST terminal is intended to display the restriction data as provided by the RBC.

C9 The GEST server compares the balise group data sent by the RBC with the kilometre based data input by the signallers. The result of this comparison indicates whether the RBC is using the intended data or not, and is sent with the restriction data to the GEST terminal for display to the signallers. This comparison relies on the corresponding restrictions having the same identity in both data sets.

C10 The program running on the GEST server is constructed from several smaller pieces of program known as threads. The GEST server software thread functions relevant to the investigation are listed below. Data is exchanged between the three threads using shared memory (figure C3).

- ***Supervision thread***

  Facilitates the server to terminal communications, sending messages over the external data link at half second intervals to confirm that this link is intact. Exchanges data with the Operation thread by retrieving and depositing data in shared memory. Temporary speed restriction data is sent to the terminal if/when prompted by the Operation thread that there is a change in the data previously sent.

- ***Operation thread***

  - Provides the link between the supervision and the RBC Comm DATA threads to obtain and supply information from/to the GEST terminal and from/to the RBC.
  - Retrieves the current restriction data stored by the RBC from memory shared with the RBC Comm DATA thread and compares this with current restriction data as entered by signallers to create the restriction status indications. Deposits this data in shared memory for onward transmission to the GEST terminal by the Supervision thread.
  - During a switch from slave to master, retrieves the kilometre data set held in the SQL database, deposits this into shared memory for transmission to the GEST terminal. Then compares balise data sets received from the RBC with those held in the SQL database and, if consistent, uploads them for use within GEST.

- ***RBC Comm DATA thread***

  Exchanges data with the Operation thread by retrieving and depositing data in shared memory. This data is sent over the external data link to the RBC at half second intervals to confirm that this link is intact. The RBC Comm DATA thread continuously exchanges data, including temporary speed restriction information, between the RBC and the memory shared with the Operation thread.

C11 The half second communication checks undertaken by the Supervision and RBC Comm DATA threads raise a ‘watchdog’ alarm if the associated datalink fails. There is no internal watchdog function supervising the Operation thread and it does not incorporate any means of reporting its continued operation or a means to alert users to an unexpected stoppage.

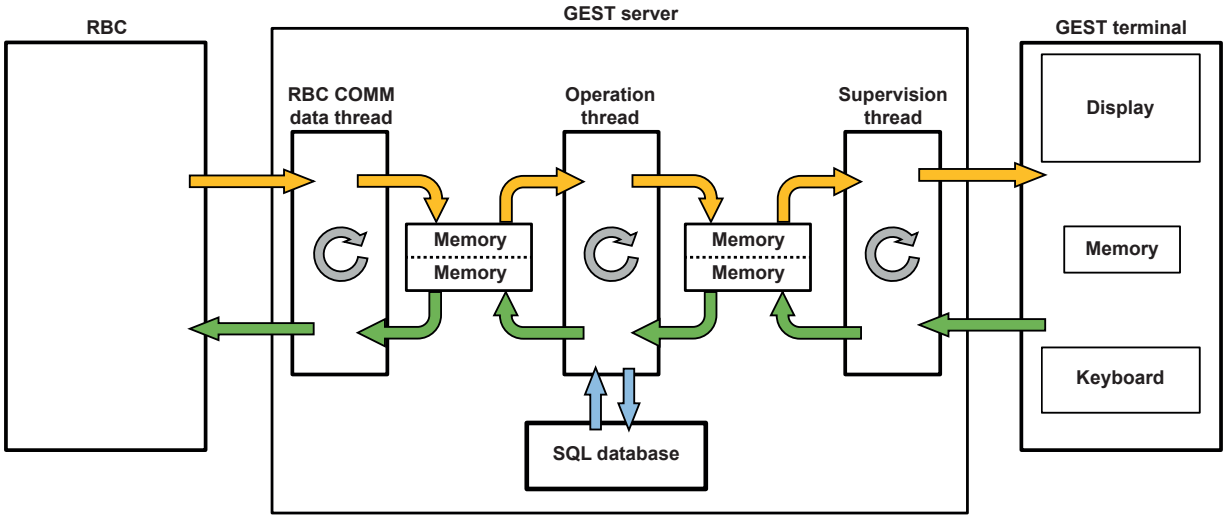


Figure C3: Information flows

C12 The GEST terminal displays temporary speed restriction data based on information provided by the RBC and then processed by the Operation thread. The Operation thread was designed to send temporary speed restriction data to the terminal only if a change is required to the data previously sent to, and stored by, the terminal.

Operation thread failure and database corruption

C13 Following the loss of temporary speed restrictions on the Cambrian lines, Ansaldo STS constructed a replica system similar to that installed at the Machynlleth control centre. Using this laboratory based system, it undertook testing to understand how the GEST sub-system might have failed.

C14 The testing revealed that stopping the Operation thread could produce a failure mode which mimicked that found following the rollover on the 19 October 2017. Using fault diagnostic software, the Ansaldo STS engineers were able to stop the Operation thread without disrupting the RBC Comm DATA or Supervision threads. These threads continued to use data in their respective memories although there was no longer any linkage between them. The datalinks between the RBC and the server and between the server and GEST terminal remained operational so the associated watchdog functions did not raise an alarm (paragraph C11). In this condition the GEST server appeared to be operating normally (figure C4).

C15 Further testing found that no other failure mode matches the conditions found following the 19 October 2017 rollover. Other scenarios would provide an alert or datalog entry which was absent in the events logged following the incident.

C16 Testing was then carried out to determine plausible causes for failure of the Operation thread. This testing found that it was possible to cause the Operation thread to stop when retrieving data from the SQL database if a temporary speed restriction identity had become corrupt within that database.

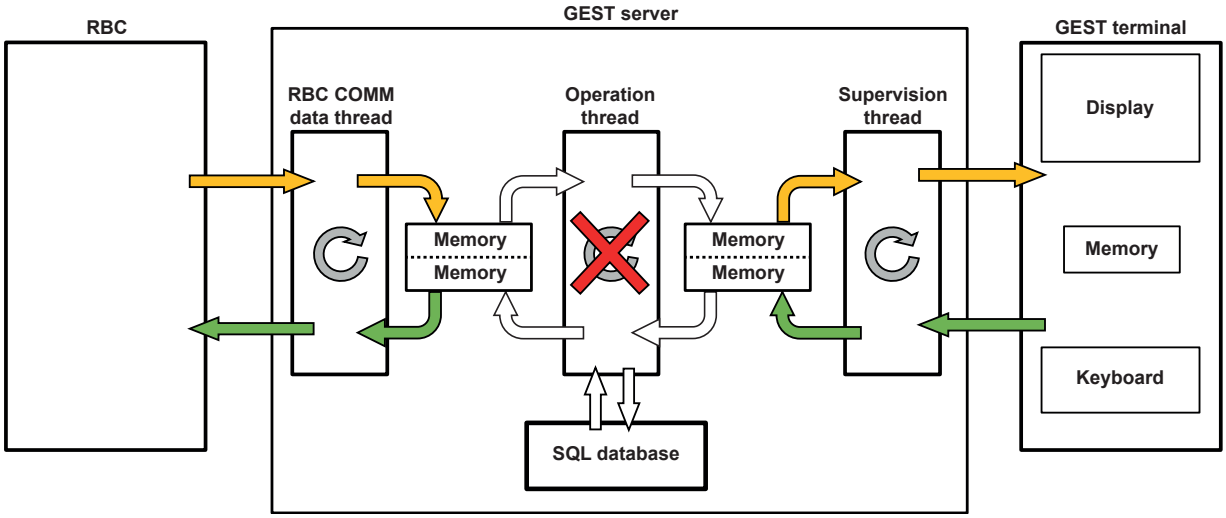


Figure C4: Information flow between RBC and GEST terminal broken due to stopped Operation thread

C17 When the Operation thread extracts data from the SQL database during a GEST server reset, it validates the kilometre and balise group based data sets against each other (paragraph C7). If the Operation thread cannot find a matching pair of data set identities to compare, the Operation thread was found to stop with an 'unknown exception' message.

C18 It is possible to corrupt data within the SQL database by creating differing identities for the kilometre data and corresponding balise data relating to the same restriction in three ways (figure C6, stage 1):

- **User intervention:** Signalling maintenance staff are required to access the SQL database to delete all data during some fault conditions. Although these circumstances are rare, instructions are provided within the maintenance manuals provided to Network Rail by Ansaldo STS. This would provide an opportunity to accidentally change one or more characters in a data set identity.
- **Electronic corruption:** An error in the read/write process undertaken by the normal operation of the GEST server software could create an incorrect identity in the SQL data.
- **Hardware/Firmware failure:** Although unlikely, it is possible that corruption could be caused by a fault in the storage medium of the SQL database. This could be degradation of the medium over time or external effects such as cosmic radiation.

C19 The RAIB was not able to establish which of these three possible forms of SQL database corruption might have occurred, due to a lack of available evidence. However, there is evidence that the correct data was held in all parts of the system after the previous rollover on 27 September 2017. SILAM data log records indicate that all temporary speed restrictions were correctly transmitted from the master GEST server and stored on the RBC on this date. Any incorrect data held on the slave GEST server would have been almost immediately overwritten by routine updating from the master server (paragraph C6).

C20 This means that any SQL database corruption must have occurred between the rollovers on 27 September and 19 October 2017. There is no record of staff requiring access to either master or slave SQL databases in the journal used by local maintenance staff to record significant maintenance activities including accessing the SQL database.

Sequence of events

C21 For corruption of the SQL database to lead to the loss of temporary speed restrictions transmitted by the RBC, it would have been necessary for this to be part of a particular sequence of events. Stopping the Operation thread required the SQL database to contain corrupt data and the master server to reset. This causes the slave GEST server to access its SQL database for information. So, while accessing corrupt SQL data and comparing the kilometre and balise data sets, the GEST server Operation thread would encounter corrupt data and stop. In this condition, the affected GEST server would be in issue mode.

C22 Stopping in issue mode would generate an 'unknown exception' error message indicated for a short time on a GEST server support terminal. At the Machynlleth control centre, this support terminal is located in the GEST server equipment enclosure within the signalling centre equipment room (figure C5). The unknown exception error message would have been visible to anyone using the terminal at the time, but this terminal is not routinely used by signalling staff.

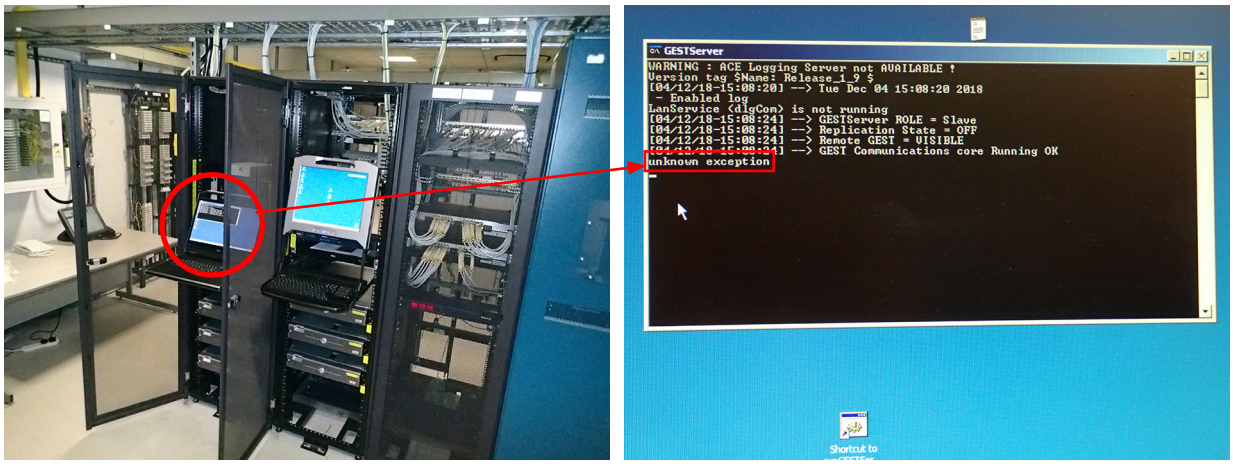


Figure C5: Computer terminal located within the GEST server equipment enclosure at Machynlleth control centre (left image) and unknown exception message seen on laboratory system (right image)

C23 The signalling system would still appear to operate normally unless signalling staff attempted to make changes such as installing, removing or modifying any temporary speed restrictions. They would then be interacting with the GEST server in issue mode and attempting to edit restrictions would result in an error message on the GEST terminal stating 'unable to communicate' (figure C6, stage 2). In this condition, the correct temporary speed restriction data would be stored on the RBC volatile memory and be transmitted to trains.

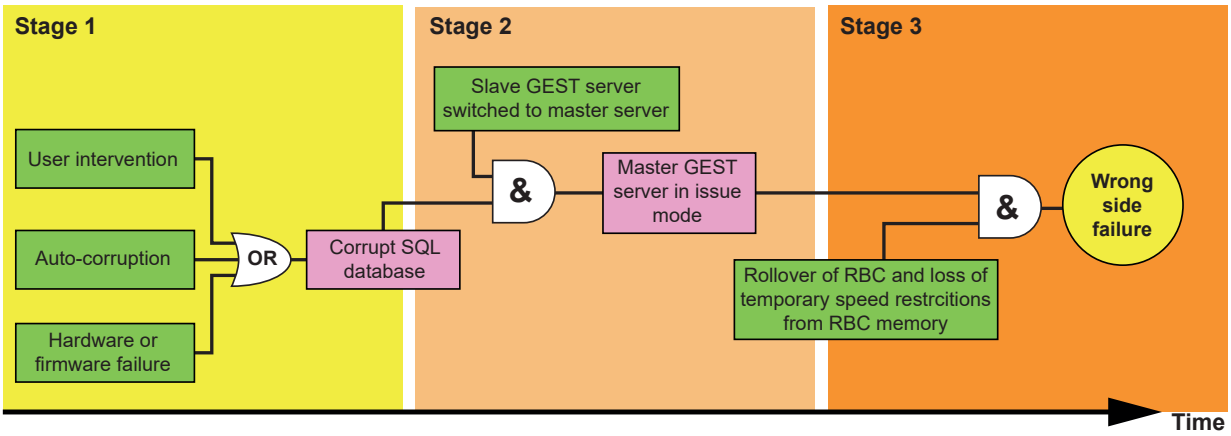


Figure C6: Sequence of events from SQL database corruption to loss of temporary speed restrictions

C24 There is no specific time limit for how long the signalling system would appear to operate normally with the master GEST server in issue mode due to a stopped Operation thread. However, during and after RBC rollover (figure C6, stage 3), such as occurred on 19 October 2017, the stopped Operation thread would mean:

- no temporary speed restriction data would be passed to the RBC, so the RBC would operate on the basis that there were no temporary speed restrictions to be transmitted to trains (figure C6, stage 3); and
- no information concerning changes to previous temporary speed restriction data would be passed to the GEST terminal, so this would operate on the basis of data held before the rollover.

C25 In these circumstances, both the RBC and GEST terminal would be communicating with the GEST server through, respectively, the RBC COMM data thread and the Supervision thread. The RBC and GEST terminals would not recognise that the intermediate Operation thread had stopped, and so would continue operating unaware that the server was in issue mode.

Evidence from restoration of service on 20 October 2017

C26 While attempting to identify the reasons for the loss of temporary speed restrictions from the RBC on 20 October 2017, a sequence of testing was improvised by the Network Rail signalling technician and Ansaldo STS maintenance support engineer, as maintenance documentation gave no guidance on this topic. Their testing sequence was intended to identify the location of the fault causing the loss of temporary speed restrictions. The sequence followed is shown in table C1.

C27 At the time of the rollover, and until the beginning of this testing sequence, GEST server 1 was the master server. The first three actions, isolating GEST server 1 (so making GEST server 2 master), deleting the server 2 SQL database and resetting server 2 had the effect of downloading the contents of the RBC memory to server 2. No temporary speed restriction data was downloaded, confirming that this data was not in the RBC memory.

C28 The next test sequence isolated GEST server 2 and switched server 1 back online to become master. At that time, if GEST server 1 was in issue mode, the server 1 SQL database would contain any corrupted data present prior to the 19 October 2017 rollover. The RBC was reset to simulate an automated rollover which would normally trigger a download of temporary speed restriction data from the GEST server 1 to the RBC. A test train found that no temporary speed restrictions were being transmitted and the GEST terminal was seen to incorrectly show that all restrictions had been loaded on the RBC.

C29 The GEST server 2 was then switched back online as the slave server, an action which should have resulted in the server 2 SQL database being loaded with data from the server 1 SQL database due to the normal slave server updating process (paragraph C6). GEST server 2 was then reset while remaining in slave mode, and an unknown exception message was observed by the signalling maintenance technician on the server terminal. This same message was later seen in laboratory testing when a slave server was restarted with a corrupt SQL database.

C30 The final three parts of the testing on 20 October 2017 showed that clearing the server 1 SQL database (an action which would remove corrupt data) allowed a successful restart of this server.

C31 Comparison of information from the testing undertaken on 20 October 2017 and the laboratory testing described in paragraphs C21 to C23 provides strong evidence that corruption of data in an SQL database in a GEST server explains the loss of temporary speed restrictions on 19 October 2017. Unfortunately, this cannot be demonstrated with complete certainty because some data was deleted during recovery from the incident (paragraph 121).

	Action	Rationale
Paragraph C27	**GEST Server 1 switched offline** Note: GEST Server 1 was online and master when the temporary speed restriction data failed to upload to the RBC	*To prevent SQL download to server 2 from server 1 and make server 2 master*
	GEST Server 2 SQL database cleared	*To provide a sterile memory for RBC download*
	GEST Server 2 reset	*To cause server 2 to download contents of RBC memory*
	No restriction data downloaded from RBC indicating RBC memory was blank	
Paragraph C28	**GEST Server 2 switched offline**	*To prevent SQL download to server 2*
	GEST Server 1 switched online	*To make server 1 master*
	RBC Reset	*To empty RBC memory and cause automatic reload of restriction data from Server 1*
	Test train run over affected lines	*To determine whether temporary speed restriction data is transmitted by RBC*
	Flags green on GEST terminal, no data sent to test train. Issue present	
Paragraph C29	**GEST Server 2 switched online as slave**	*To cause an SQL download from Server 1 to sterile Server 2 database*
	GEST Server 2 reset	*To cause Server 2 to upload restriction data from SQL data duplicated from Server 1*
	Server 2 shows 'unknown exception' message when using SQL data	
Paragraph C30	**GEST Server 2 switched offline**	*To ensure no SQL connection to Server 2 and make Server 1 master*
	GEST Server 1 SQL database cleared	*To sterilize Server 1 SQL database*
	GEST Server 1 reset	*To test if Server reset with blank SQL database clears issue mode on Server 1*
	Server 1 restarts successfully when SQL database is cleared	

Table C1: Sequence of testing undertaken to isolate system failure on 20 October 2017

This report is published by the Rail Accident Investigation Branch,
Department for Transport.

© Crown copyright 2019

Any enquiries about this publication should be sent to:

RAIB
The Wharf
Stores Road
Derby UK
DE21 4BA

Email: enquiries@raib.gov.uk
Telephone: 01332 253300
Website: www.gov.uk/raib