Oliver Stewart
RAIB Recommendation Handling Manager

25 March 2024

Mr Andy Lewis
Deputy Chief Inspector of Rail Accidents

Dear Andy,

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

I write to provide an update[1] on the action taken in respect of recommendations 3 & 5 addressed to ORR in the above report, published on 19 December 2019.

The annex to this letter provides details of actions taken in response to the recommendations and the status decided by ORR. The status of recommendations 3 & 5 is **'Closed'.**

We do not propose to take any further action in respect of the recommendations, unless we become aware that any of the information provided has become inaccurate, in which case I will write to you again.

We will publish this response on the ORR website.

Yours sincerely,

Oliver Stewart

[1] In accordance with Regulation 12(2)(b) of the Railways (Accident Investigation and Reporting) Regulations 2005

Recommendation 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

ORR decision

1. The recommendation has been taken into consideration by the RSSB Asset Integrity Group (AIG). To improve the dissemination of safety learning from incidents involving complex software-based system failures, a page has been created on the Safety Central website titled 'Improving Railway System Safety' and further supporting material and case studies has been produced by RSSB and uploaded to their website page on 'Accident Investigation and Learning[2]. The library of case studies are mainly incidents outside the rail sector, where safety learning has been identified regarding complex software-based system failure. The case studies are on the RSSB website and access is freely available to those with a valid email address; full RSSB membership is not required.

2. After reviewing the information provided ORR has concluded that, in accordance with the Railways (Accident Investigation and Reporting) Regulations 2005, Network Rail, in consultation with RSSB, have:

- taken the recommendation into consideration; and
- have taken action to close it.

Status: Closed.

Previously reported to RAIB

[2] Learning from Other Sectors (rssb.co.uk)

3. On 18 December 2020 ORR reported the following:

In response to this recommendation, Network Rail is working with the RSSB AIG to develop a library of case studies where a complex software-based system has had a critical role in an incident. Case studies will be drawn from other safety critical industries as well as rail. The causal factors for each case will be aligned to the outputs of the failure mode identification exercise proposed in response to recommendation 1. We support the approach being taken by Network Rail and the AIG.

When passing the recommendation to Network Rail, we asked for the response to include evidence of how the recommendation was being implemented in the East Coast Mainline Digital Railway project. Network Rail have set out how the learning from case studies has informed the development of the DRACAS (Data Reporting, Analysis and Corrective Action system) for the project.

Update

4. On 9 August 2023 Network Rail provided the following closure statement:

[N216-14] Cambrian Rec 3.pdf

Recommendation 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.

ORR decision

5. Hitachi STS has made changes to the system architecture of the GEST tools on the ERTMS signalling system installed on the Cambrian line, to address the risk of the Radio Block Centre (RBC) failing to provide the correct Temporary Speed Restriction (TSR) information when service is restored following a software rollover. The GEST provides a system interface between signallers and the RBC, which sends movement authorities to trains. The addition of non-volatile memory for the storage of the TSR data in the RBC ensures that the recovery of TSRs after an RBC restart achieves SIL4.

6. The system has been in use by Network Rail since May 2022 and has been tested to demonstrate that the failure mode that occurred on the Cambrian line on 20 October 2017 has been eliminated.

7. Network Rail carried out integration and functionality tests for the Cambrian RBC and associated control system. This testing did not form a significant part of the claim for system integrity as it is not possible to provide a 100% guarantee of software functionality by testing in the conventional manner. The claim for software integrity is based on compliance with established standards for software development, such as Ens50126,8,9. Compliance with those standards was assessed by NCB, with a final review by F-CCS SRP/NRAP. RIS 0745 was produced by RSSB as a result of recommendation 1 from the Cambrian RAIB report and is broadly a railway application guide to the relevant ENs, such as Ens50126,8,9.

8. After reviewing the information provided ORR has concluded that, in accordance with the Railways (Accident Investigation and Reporting) Regulations 2005, Hitachi STS and Network Rail have:

- taken the recommendation into consideration; and
- have taken action to close it.

Status: Closed.

Previously reported to RAIB

9. On 18 December 2020 ORR reported the following:

Hitachi STS is developing an upgraded GEST for the Cambrian RBC that stores TSR information in non-volatile memory, ensuring it is available after a rollover. The prototype of the upgraded GEST had been validated in factory and is awaiting Network Rail approval.

Update

10. On 11 October 2023 Network Rail provided the following closure statement:

RAIB Report
17_2019 Recommen

Previously reported to RAIB

Recommendation 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:

- l 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

.

ORR decision

1. In response to this recommendation, Network Rail is working with the RSSB AIG to develop a library of case studies where a complex software-based system has had a critical role in an incident. Case studies will be drawn from other safety critical industries as well as rail. The causal factors for each case will be aligned to the outputs of the failure mode identification exercise proposed in response to recommendation 1. We support the approach being taken by Network Rail and the AIG.

2. When passing the recommendation to Network Rail, we asked for the response to include evidence of how the recommendation was being implemented in the East Coast Mainline Digital Railway project. Network Rail have set out how the learning from case studies has informed the development of the DRACAS (Data Reporting, Analysis and Corrective Action system) for the project.

3. After reviewing the information provided ORR has concluded that, in accordance with the Railways (Accident Investigation and Reporting) Regulations 2005, Network Rail has:

- taken the recommendation into consideration; and
- is taking action to implement it by 31 July 2021

Status: Implementation on-going. **ORR will advise RAIB when further information is available regarding actions being taken to address this recommendation.**

Information in support of ORR decision

4. On 10 August 2020 Network Rail provided the following initial response:

In response to this recommendation, Network Rail has recognised (like RAIB Cambrian Recommendation 1) that an industry response needs to be taken to address this recommendation as complex software-based systems can be infrastructure and/or train based e.g. trackside and on-board signalling systems.

Network Rail has therefore engaged with the new industry-wide Asset Integrity Group (AIG) established by RSSB to look at how the industry could best respond to this recommendation.

AIG has agreed that a workstream will be undertaken to identify some relevant case studies to illustrate where a complex software-based system has played a part in an incident. An initial list of case studies has been proposed and these are recorded in the minutes of the 29 July 2020 meeting. These include case studies from other safety critical industries. The next steps will be to use technical authoring to bring case studies that have key transferrable learning points for the railway system to life, making sure they are easy to understand and to disseminate them widely for maximum impact. In parallel we will ask industry for further case studies to build the case study library, as part of the wider AIG programme. Review of case studies will be a regular part of AIG activities, and once a few case studies have been produced and reviewed they will be used to identify and illustrate common themes. The causal factors will be aligned to the outputs of the failure mode identification exercise proposed in response to RAIB Cambrian Recommendation 1 to make sure it is complete.

In parallel with this, through AIG and under RSSB's lead, we are investigating how the principles and process of the DRACAS currently being developed for Digital Railway by the East Coast Train Control Partnership project can be expanded to cover other complex software-based systems to ensure communication of defects and corrective actions throughout the industry supply chain. As part of this review, we will consider ways to improve implementation of the existing RIS-0707-CCS (Management of Safety Related Control, Command and Signalling System). This workstream will address the second, third and fourth bullet of this recommendation.

As this recommendation is closely related to RAIB Cambrian Recommendation 1 we will provide on the planned schedule of activities by end-November 2020.

The first bullet of this recommendation primarily relates to the specification of the systems themselves regarding event data capture/recording. This will be addressed through AIG's response to RAIB Cambrian Recommendation 1.

Evidence required to support closure of recommendation

A library of case studies that are easy to understand and widely available, illustrating where a complex software-based system has played a part in an incident.

Output of the review of the principles and process of the DRACAS and its future application (including any related standards), including improvement actions relating

to event reporting, data recording, investigation, recommendation and communication processes.

5. On 1 December 2020, Network Rail provided the following additional information:

Activities undertaken (up to 30 November 2020)

- *Initial case study produced using the RAIB Cambrian incident itself, which included mapping the causal factors back to the project lifecycle (V-cycle).*
- *Further case studies prepared in this format to test the approach – some actual events and other theoretical events that are reasonably foreseeable.*
- *Recommendations obtained for further suitable case studies involving complex software-based systems from both rail and other industries n.b. reasonably foreseeable scenarios which contain potential security vulnerabilities will be first reviewed and screened through separate committee (proposal to be presented to NCSC Railway Information Exchange on the 8 December 2020).*
- *Presentation to industry AIG on 18 November 2020 to obtain continued industry support for the approach.*
- *Further review of proposed case studies at the AIG meeting on 18 November 2020 including a presentation on an example case study from the aviation sector.*
- *Broader activities on improving alerting, reporting and understanding of incidents (e.g. potential changes to NIR Online, increasing use of SMIS by maintainers) are ongoing. Once realised these may interface assist with longer-term implementation of Rec 3.*

Milestones for the remaining action plan

Milestone	***Date***
Select a sub-set of the proposed case studies for developing into documents that can be published to an external audience.	*18 December 2020*
Produce, review and publish initial series of case studies via Safety Central	*26 February 2021*
Seek feedback from industry and select-further case studies for production.	*26 March 2021*
Produce, review and publish second series of case studies.	*28 May 2021*
Based on the experience and feedback gained, produce and agree procedure for ongoing collation of future case studies to further populate the library going forwards.	*30 July 2021*
Complete review into how the principles and process of the DRACAS currently being developed for Digital Railway could be expanded to cover other complex software-based systems and make recommendations for improvement.	*30 July 2021*
Produce action plan in response to recommendations from the DRACAS review and implement.	*Timescales dependent on nature of recommendations.*

6. On 29 May 2020 HS1 provided the following initial response to recommendations 1 & 3:

The HS1 Signalling Environment and Similarities with Cambrian
Apart from the St Pancras area, HS1 operates the widely used TVM430 in-cab signalling system, as used throughout France, Belgium and South Korea on their high-speed lines. The system used on HS1 uses an Ansaldo supplied train controls system, known as the Route Control Centre System (RCCS) and TVM430 SEI interlockings,know in the UK as ITCS (Integrated Train Control System).

At St Pancras, HS1 uses ITCS interlockings but conveys movement authorities via Multi-Aspect Colour Light (MACL) signals with supervision/ATP provided by KVB (Kontrole de Vitesse par Balise) located in the '4 foot' and read by trains as they pass over them.

The HSl system shares some basic similarities with the ETCS level 2 system deployed on Cambrian. Both systems incorporate permanent Automatic Train Protection and supervision with in-cab signalling. Both systems were designed and supplied by Ansaldo STS and the interlocking technology deployed on both lines is very similar.

The Cambrian train control system does not have the same level of functionality as HS1's RCCS despite having visual similarities. For example, it does not incorporate ARS (Automatic Route Setting). Also, the Cambrian interlocking does not form part of the overall TSR process.

Despite similarities, there are major differences which are key in understanding the cause of the failure on Cambrian and its inapplicability, in the same manner, as to HS1.

The method of applying a TSR on Cambrian involves the GEST control terminal and server which links directly to the RBC which issues the movement authority, including the TSR, to the trains; HS1 has neither a GEST terminal nor an RBC. For HS1, TSR's are normally commanded via the RCCS and implemented in the ITCS interlocking, which can be remotely and locally applied. The Cambrian TSR function is managed by the additional GEST system.

Having described the key architectural differences, the question arises as the whether the same failure could present on HS1 given a similar scenario.

There are two issues to address in the case experienced on Cambrian Line ERTMS line for HS1:

1. *Are TSR's retained within the HS1 signalling if the system used to apply them (RCCS) is rebooted or powered down and back up again?*
2. *Can the indications for TSR's shown on the HS1 RCCS be incorrect after a reboot of the TMS?*

The HS1 RCCS is directly connected to the interlockings which are distributed locally along the length of HS1.

The interlockings convey the movement authority to the train through the rails so, unlike ETCS, no Radio Block Centre (RBC) is needed.

The HS1 signalling system also employs local TSR switch panels in each signalling room, which are spaced approximately every 14km along the line. This allows pre-set TSR's, typically 160km/h and 80km/h, to be physically switched at a panel and padlocked for the duration of the restriction. This directly feeds the interlocking and is not affected should the interlocking be powered down and then back up.

TSR's on HS1, therefore can be applied remotely at the RCCS over a wide area, locally via the switch panel or at St Pancras using the KVB system.

The table below shows the impact of a TSR applied in one of three scenarios on HS1 and provides details regarding their status at the interlocking level and at the control level, i.e. the signaller's display.

The system in use on HS1 for the application, retention and removal of a TSR incorporates three levels:

TSR Type	Detail	Affected by a TMS reboot	TSR indication on signaller's screen
KVB TSR. These TSR's are applied for speeds less than 80 km/h and are combined with a TSR applied on local switching panel in the signalling technical room.	Local TSR applied using KVB a beacon placed in the '4 foot' at the appropriate distance.	Not affected, the TSR beacons remain in place and the local switch is still activated.	Not affected, the TSR are local switches which are directly wired to the interlocking
TSR applied on local panel in signalling room.	TSRs have been applied by maintainers using an Ops instruction at local TSR panels.	Not affected, the TSR are local switches which are directly 'hard-wired' to the interlocking.	Not affected, the TSR are local switches which are directly wired to the interlocking
TSR applied remotely.	Remote TSR applied by the signaller using the RCCS.	Not affected as the TSR's are set within the ITCS interlocking. A reboot of the RCCS will not affect the existing TSR's.	Not affected as the TSR's are set in the interlocking. A reboot of the RCCS will not affect the existing TSR's

Conclusion:

There are no issues with TSRs on H1l if the RCCS or ITCS is rebooted, as the TSR's are set directly and retained within the ITCS interlocking; this differs significantly from Cambrian which applies TSR's using the GEST terminal and the RBC, neither of which are used on HS1.

When the HS1l RCCS system is rebooted, it is initialised with the complete status of all the signalling field equipment from the ITCS interlocking. This includes any protection and TSRs previously set and memorised in the interlocking. This avoids any discrepancy between the status of the track system and the indication on the

signaller's display.

If an interlocking is rebooted, all the remote protections are applied automatically by the interlocking within the area controlled.

7. On 1 July 2020 HS2 provided the following initial response:

HS2 has been working with NR, RSSB and the wider supply chain to understand these issues. Reports on software and signalling issues come through a variety of forums, including:

- *RSSB HISG.*
- *RSSB Standards Committees, especially CCS SC in this scope.*
- *EIM newsletters and EIM industry groups.*
- *RAIB reports.*
- *Wider engagement at conferences, meetings and elsewhere.*
- *Various other groups on GSM-R, FGG and other technologies at RSSB.*

HS2 has not yet procured any CCS systems and is in the process of developing its requirement specification. We include high-level requirements about fault recording, electronic security incidents and related faults and plan to work with the appointed contractors during detailed design to ensure the system has a robust process in place to log, manage and integrate these.

HS2 is working with NR and manufacturers through these forums to identify and manage the appropriate means to disseminate this material.

HS2 has also commissions regular analysis of high speed rail accidents and incidents to be produced as internal reports. Whilst these accidents result from many causes, relevant signalling issues are included.

8. On 27 May 2020 Transport for London provided the following initial response:

Recommendation 3 in the report focused on the importance of improving the capture and dissemination of safety learning available through the reporting and systematic investigation of complex software-based system failures.

All incidents that occur within the software based signalling systems on TfL are investigated thoroughly in line with standard TfL practices and are recorded and resolved accordingly. The investigation will also include in-depth analysis of the data generated and stored by the system and also include the use of independent software analysis tools and operational simulators to fully understand the scenario

and conditions that led to the incident. Where necessary the system supplier is engaged to investigate further, and the outcomes recorded. These outcomes are then disseminated

to all relevant parties through various mediums from technical notes, updates to user manuals, reports, Design Office instructions, project communications etc. Where required TfL also ensures that the supplier also raises the outcomes on their own quality and assurance systems to ensure full coverage and to prevent a repeat in the future.

TfL uses a number of mechanisms to ensure that learning from safety incidents from other railways is also applied. These can range from simple toolbox talks and cascade briefings to role play. As an example, the Four Lines Modernisation (4LM) project undertook role play which took in the findings from the Waterloo incident and refreshed the learning from Clapham.

Recommendation 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

ORR decision

9. Hitachi STS is developing an upgraded GEST for the Cambrian RBC that stores TSR information in non-volatile memory, ensuring it is available after a rollover. The prototype of the upgraded GEST had been validated in factory and is awaiting Network Rail approval.

10. After reviewing the information provided ORR has concluded that, in accordance with the Railways (Accident Investigation and Reporting) Regulations 2005, Network Rail and Hitachi STS have:

- taken the recommendation into consideration; and
- is taking action to implement it by 30 June 2021.

Status: Implementation ongoing. **ORR will advise RAIB when actions to address this recommendation have been completed.**

Information in support of ORR decision

11. On 23 April 2020 Hitachi STS provided the following initial response:

The technological fix is the upgrade of the RBC to implement Non Volatile Memory to store the TSR information in the RBC. So in case of a rollover the TSR information will stay inside the RBC and there will be no need for the GEST to send to the RBC the TSR information when the RBC is restored to service.

The proposed timescale for this implementation is December 2020.

The current Cambrian GEST v1.9 addresses two main functions:

- *Temporary Speed Restriction (TSR)*
- *Train Information Display (TID) including TRIP alarm*

The solution consists in re-using LGVEE GEST v3.1.7 application to manage the TSR function and to maintain Cambrian GEST v1.9 application for the TID function. Both functions will be managed physically in separate servers and workstations.

A new RBC generic application will provide the NVM feature and the new RBC GEST interface compatible with LGVEE GEST v3.1.7. The RBC / GEST interface is provided by two serial links (LS1 and LS2). The train information data uses the LS1 downlink. The TSR information data uses the LS1 uplink and LS2 downlink. Interface is changed for TSR information to support GEST LGVEE.

12. On 11 November 2020, Hitachi STS confirmed a revised timescale of 30 June 2021 and confirmed the prototype of the upgraded GEST had been validated in factory and is awaiting Network Rail approval.