Oliver Stewart
RAIB Recommendation Handling Manager
T: 020 7282 3864
M: 07710069402
E-mail oliver.stewart@orr.gov.uk

18 December 2020

Mr Andrew Hall
Deputy Chief Inspector of Rail Accidents
Cullen House
Berkshire Copse Rd
Aldershot
Hampshire GU11 2HP

Dear Andrew,

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

I write to report[1] on the consideration given and action taken in respect of the recommendations 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 1, 3, 4 and 5 is **'Implementation on-going'**. The status of recommendation 2 is **'Implemented'**.

ORR will advise RAIB when further information is available regarding actions being taken to address these recommendations.

We will publish this response on the ORR website on 21 December 2020.

Yours sincerely,

Oliver Stewart

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

Initial consideration by ORR

1. All 5 recommendations were addressed to ORR when the report was published on 19 December 2019.

2. After considering the recommendations ORR passed recommendations 1 & 3 to Network Rail, recommendations 2 & 5 to Hitachi STS, and recommendation 4 to Network Rail and Hitachi STS asking them to consider and where appropriate act upon them and advise ORR of its conclusions. The consideration given to each recommendation is included below. We also asked HS1, HS2 and Transport for London to respond to recommendations 1 and 3 in order to share learning from their own experience with high integrity software systems more widely. We have not provided a status for these organisations.

3. This annex identifies the correspondence with end implementers on which ORR's decision has been based.

Recommendation 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;
- 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.

ORR decision

4. Network Rail have set in motion the actions the recommendation envisages and is working with the RSSB Asset Integrity Group (AIG) to develop an industry wide action plan. AIG is incorporating the existing activities of the former High Integrity Software Group (HISG) as it had already been considering some of the subject areas associated with this recommendation.

5. AIG is planning to produce guidance to outline the key requirements for companies involved in designing and installing new or modified high integrity software-based systems. The guidance will aim to address the bullet points listed in the recommendation and reference, or consolidate, the existing guidance note GEGN8650 (Guidance on High-Integrity Software-Based Systems for Railway Applications). The guidance is expected to be issued by 3 September 2022.

6. We considered the recommendation an opportunity to share lessons learned and best practice with other railway infrastructure managers (HS1, HS2, London Underground) and asked those organisations to provide a response.

7. 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 3 September 2022

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

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

In response to this recommendation, Network Rail has recognised that an industry response needs to be taken to address this recommendation as high integrity 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.

The AIG has agreed to lead on scoping the action plan to address the recommendation. An initial scoping paper (attached) was submitted to the meeting on the 29 July 2020, which received agreement. The paper proposed that a Rail Industry Standard (RIS) be produced to outline the key requirements and guidance for clients involved in designing and installing new or modified high integrity software-based systems. It will seek to address the bullet points listed in the recommendation and reference, or consolidate, the existing guidance note GEGN8650 (Guidance on High-Integrity Software-Based Systems for Railway Applications). Compliance with RISs are a licence condition of Network Rail, train operators and station operators. The requirement to comply with the RIS can also form part of the contractual requirements for infrastructure and train system suppliers.

RSSB is currently leading the drafting of the 'case for change' proposal (including the business case) to develop the RIS, which will require a sponsoring standards committee. Due to the scope, multiple standards committees will need to be involved, increasing the importance of an efficient and effective project strategy. AIG will be briefed on the progress at the next meeting which is scheduled on 18 September 2020.

As part of the wider industry activities, AIG is also in the process of incorporating the existing activities of the former High Integrity Software Group (HISG) as this is the ideal forum to progress this recommendation.

When RSSB has received confirmation of the approval of the business case and the multi-functional drafting review group has been established, we will be able to provide an update on the planned schedule. This update will be provided by end-November 2020.

As part of this workplan, it is proposed that a desktop review will be undertaken to identify potential failure modes associated with both the procurement process as well as the technical elements of the system themselves. A failure mode could be lack of specification of the parties' responsibilities (e.g. not appointed an independent assessor, incorrect remit, omissions in remit), as well as technical failure modes relating to software and hardware functionality (e.g. memory buffer, requirements for data backup).

As part of wider industry engagement, a CP6 workplan for AIG is under development, including broader engagement throughout the supply chain, including both train and infrastructure elements.

Whilst it may take some time to develop, agree and publish the RIS in response to RAIB Cambrian Recommendation 1, the actions being taken in response to RAIB Cambrian Recommendation 3 will seek to promote greater industry awareness of the potential failure modes through referencing case studies involving high

integrity software-based systems. These will include case studies from other safety critical industries.

Evidence required to support closure of recommendation

Publication of the Rail Industry Standard.

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

Activities undertaken (up to 30 November 2020)

- *Initial hazard identification sessions held to identify the procurement and technical hazards attended by experienced safety, cyber security and information technology experts.*
- *Presentation to industry AIG on 18 November 2020 to obtain continued industry support for the approach.*
- *Project Manager identified for production of the business case for change for a RIS, and indicative timelines identified for different routes to publication. The case-for-change for a RIS may, depending on Standards Committee feedback, need to be modified to include additional or interim routes to publication.*
- *Two meetings held with Network Rail and RSSB attendees to discuss and outline the proposals for the content to form part of the business case for change n.b. further meetings are planned that include evaluating the optimum approach for alignment for new document with GEGN8650. Alignment of the RIS with ECM regulations and ROGS will be noted, particularly where the OEM is also an ECM.*

Milestones for the remaining action plan

Milestone	***Date***
Produce first draft of more detailed content for proposed RIS identifying key linkages with the existing guidance note	*26 February 2021*
Detailed content for proposed RIS produced in required format following working group review	*30 July 2021*
RIS content finalised by working group	*1 Sep 2021*
Standards Committees review and approve for consultation	*5 Nov 2021*
Consultation completed	*15 Dec 2021*
Produce updated draft, including review of outcome of consultation with working group, and finalise document for approval	*15 Feb 2022*
Standards Committees approve for publication	*15 May 2022*
Publish RIS	*3 Sept 2022 (n.b. an earlier date may be achieved if Standards Committees approve alternative route to publication changes)*

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

The HSl 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 HSl 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 HS1 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 HS1 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.

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

The HS2 Safety Strategy and associated Rail Systems Safety Plan defines the system safety activities required to support the creation of the High Speed 2 (HS2) system solution. With respect to the Railway Communication, Signalling and Processing Systems is concerned, HS2, the approach defined therein:

- *complies with the requirements of RSSB Guidance Note GEGN8650 that refers out to BS EN 50128:201, BS EN 50159:2010 and BS EN 50126:1999.*
- *complies with the risk management activities of CSM RA Regulation 402/2013 as amended by Regulation 2015/1136;*
- *The CSM-RA Regulations* ***Error! Reference source not found.*** *and CENELEC standards EN 50129:2018, EN 50126-1 (2017), EN 50126-2 (2017) and BS EN 50128:2011 to develop the HS2 Railway System Safety Case.*
- *supports the production of a suite of generic and specific application safety cases and the associated Safety-Related Application Conditions (SRACs), as defined by BSEN50129, that is developed in accordance with the life cycle mapped out in the Railway Systems Safety Plan;*
- *supports the production of a Safety Justification reports; these are required to be delivered at different stages in the system lifecycle to the HS2 System Review Panel (SRP) for approval prior to proceeding to the next design stage.*
- *ensures that a consistent approach to system safety is adopted for all Railway system and sub-system development activities (where system includes people, product and processes);*
- *The HS2 Head of System Safety, Security and Interoperability sits on the RSSB High Integrity System Group (HISG) and has done since its inception in 2013. As part of this they have been part of the development of GEGN 8650.*

Approach to Safety

Specifically, our approach provides

- *an overview of the systems that comprise HS2, as defined in the suite of System Definitions;*
- *the structure of the Systems Safety management organisation and the related responsibilities will be clearly defined and communicated to all.*
- *the process for thorough and systematic hazard identification, evaluation and risk assessment that will ensure a common approach to the identification of hazards and their elimination or reduction to acceptable levels of risk;*
- *a baseline suite of the safety deliverables required to support the overall HS2 Safety Case, as defined by BS EN 50129 and BS EN 50128, The deliverables being developed in accordance with the life cycle mapped out in Rail Safety Plan; and include Generic Product Safety Case (GPSC), Generic Application Safety Case (GASC) and a Specific Application Safety Case (SASC).*
- *an aligned delivery programme between the respective systems' safety programmes.*
- *A robust Safety Requirements derivation and control process that apportions all HS2 requirements to each sub-system. This will include Tolerable Hazard Rates and where appropriate SIL levels for each function.*

- *Robust requirements traceability using the HS2 requirements management database (DOORS). This ensures:*
  - *the inclusion of all Safety Measures and requirements within the ITT, serving as the basis for verification of the respective system designs with respect to safety (during Tender Review and subsequent delivery).*
  - *formalised links are established between each Safety Measure / Requirement and the associated Hazard Record.*
  - *traceability to the source of the Safety Measures and requirements.*
- *the System Safety management controls to ensure that*
  - *hazards and requirements are managed adequately and transferred appropriately from one system owner to another throughout the system life cycle.*
  - *a close interaction between the systems (which includes engineering, operations, maintenance and business change) and System Safety functions is established to ensure that System Safety deliverables are of the required specification and fully integrated into the design.*
  - *the correct supplier is selected to deliver the sub-systems based upon a rigorous review of the response to the ITT*
- *The System Safety approval process that will be supported by provision of evidence to independent Safety Authorities – e.g. evidence of safety requirement validation, verification of Safety-Related Application Conditions and other safety case constraints. This process is addressed in the HS2 Authorisation Plan*
- *Independent Internal and External (e.g. ISA, AsBo, DeBo, and NoBo) Assurance Bodies have be engaged to provide a HS2 Independent Assurance function and provide regular reports to the HS2 SRP.*

Safety Controls

Change Management / Configuration Management

Configuration Management is essential on any safety-critical programme in order to track changes on those items used to achieve or demonstrate safety and the relationships between them. Further details of the arrangements in relation to this will be provided in the HS2 Configuration Management Plan.

Each sub-contractor shall be responsible for implementing their own change management process, with all software and data related changes managed in accordance with BS EN 50128.

It is the responsibility of HS2 to provide appropriate surveillance of the supplier's system safety programmes so that timely management action can be taken as the need arises and programme progress ascertained. This surveillance will involve reviewing System Safety Plans, Safety Analysis and Justifications, and performing Safety Audits.

Supplier Control and Management

Adherence to the requirements specification throughout the life of the project will be controlled through the integration and close co-operation of the HS2 and Supplier Project Teams via the following activities:

- *HS2 supplying the specification to the supply chain with detailed requirements and ensuring that the requirements are understood;*
- *Agreeing the methods and solutions to be used by the specification and generic design teams in order to meet the System Safety requirements;*
- *Agreeing the type, format and schedule of data to be prepared by the specification and generic design teams in support of System Safety activities;*
- *Monitoring of performance of the specification and design through informal day-to-day contact, design reviews and reports; and*
- *Achieving solutions to existing or potential problems and ensuring that the solutions are implemented.*

Safety Auditing

In addition to the System Safety analysis activities, the Systems Safety and Assurance team will undertake a series of safety audits to ensure that, where hazard management is reliant on evidence from other engineering disciplines and System delivery teams, that evidence will be sufficient.

A Safety Audit Plan will be produced and subsequent reviewed and updated regularly in parallel with the System Safety Plan reviews.

The audits conducted by HS2 to correspond to the LoD 1 assurance described in the HS2 Authorisation Plan.

Safety Audits are focused on the high-risk areas of the programme upon which hazard control relies; these will include, as a minimum:

- *Engineering Log records (including Designers' Risk Assessments)*
- *Requirements traceability*
- *Configuration Management (including impact assessment and regression testing, where applicable)*
- *Human Factors*
- *Hazard Management Process*

Risks, Assumptions, Issues and Dependencies (RAID)

The HS2 programme deals with risks, assumptions, issues and dependencies by the use of a RAID Log. This will allow for early identification and communication with the relevant stakeholders for clarification and resolution.

Where any risks, assumptions, issues and dependencies have an impact on system safety, whether it is programme or argument related, then the responsibility for resolving these items will fall to the Safety and Assurance Manager.

Verification and Validation (V&V)

The HS2 Systems Acceptance Plan defines the verification and validation process, roles and responsibilities to be applied across the HS2 Programme with the objective of ensuring that the HS2 Railway, as specified, designed and deployed, will meet the specified requirements.

The output from the V&V activities is a Verification and Validation Matrix (VVM) which is used to plan and track the status of V&V activities against the requirements throughout the programme and programme life cycles. This will include analysis, SAT, FAT, Testing and Commissioning.

This matrix will include the evidence required to verify the system safety requirements.

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

Recommendation 1 in the report focused on the importance of a mandatory safety assurance procedure (and associated guidance) for its client role on projects involving installation and modification of high integrity software-based systems.

TfL has robust processes for assurance of the introduction on new software-based systems. These process are based on British Standards, such as BS EN 50126 :2017 (Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)), BS EN 50128:2011 (Railway Applications-Communications, signalling and processing systems-Software for railway control and protection systems) and BS EN 50129:2003 (Railway applications - communication, signalling and processing systems - safety related electronic systems for signalling Railway applications - communication, signalling and processing systems - safety related electronic systems for signalling).

These standards are adopted into TfL's engineering standards, including:

S1538: Assurance

S1201: Signalling & Signalling Control – Approvals

S1198: Signalling & Signalling Control – Installation, test, commissioning and handover

S1199: Signalling & Signalling Control – Operation and Maintenance

S1209: The System Engineering process applied to projects

S1210: Safety Related Software Engineering

These standards, which are supported by more detailed processes, set out TfL and LU's approach to assurance for projects involving installation and modification of high integrity software-based systems. The standards, which are mandatory for LU and our suppliers, also set out the accountabilities and competence requirements involved in this process.

We are currently applying these processes in the introduction of the new signalling system on the District, Hammersmith & City, Metropolitan and Circle lines. This involves detailed assurance at the most senior level in LU and in Thales (the supplier of our new signalling system) to confirm that we receive the appropriate assurances on safety at the relevant decision points.

We have noted the points highlighted in Recommendation 1 of the report and we will review our processes in light of this report to ensure that TfL learns the appropriate lessons from the RAIB report.

Recommendation 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.

ORR decision

13. Hitachi STS has reviewed its safety management processes for the design, design verification, design validation, and retention of records for high integrity software-based systems, based on the finding of the Cambrian Coastline RAIB report. Following Hitachi's initial response, we had identified a number of areas we wanted the review to cover which have now been addressed.

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

- taken the recommendation into consideration; and
- has taken action to implement it

Status: Implemented.

Information in support of ORR decision

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

The development of the GEST has been carried out approximatively in 2009, based on a development made for SNCF project. Hitachi Rail STS (HRSTS) is continuously reviewing and improving its internal processes taking lessons learnt of various projects. Internal processes have been challenged with the feedback of different national and international projects. HRSTS is a worldwide company working with different customers, different ISA leading to have a lot of feedbacks on HRSTS processes and ways of working. All of these information are collected all along the projects life cycles and during dedicated interviews made through a questioner.

Feedbacks are also internal feedbacks according to the scope of each project (suppliers of products, or suppliers of system including wayside, on board, …).

Feedbacks since the Cambrian Lines commissioning are notably coming from the following projects:

- *LGVEE (New High Speed Line in France – East of France) : Interlocking, ATP, ERTMS L2 : first commissioning in 2013, the 20th of December; second commissioning in 2016, the 11th of December (expansion of the line)*

- *BPL (New High speed line in France – Le Mans to Rennes) : Interlocking, ATP, ERTMS L2, ERTMS L1 : put in revenue service in 2017 the 2nd of July*

- *SEA (New High speed Line in France – Tours to Bordeaux) : Interlocking, ATP, ERTMS L2 : put in revenue service in 2017 the 2nd of July*

- *Morocco Project (New High Speed Line in Morocco): Interlocking, ERTMS L2, ERTMS L1, CTC : put in revenue service in 2018 the 26th of November*

- *Deployment of interlocking in France for several stations*

According to this process of feedbacks in place:

- *More relevant safety analyses are done regarding development processes and validation processes leading to improve all HRSTS processes*

- *Safety analyses are realised on degraded mode including multiple failures analyses*

- *Process of cross acceptance has been reinforced*

- *Common Safety Methods are applied and especially, system impact analysis and safety system impact analysis*

- *Audit activities in place: The application of the 2011 50128 standard on various projects has enabled development projects using the 2001 version to carry out additional activities not requested by the 2001 standard*

- *Certification IRIS achieved 18/12/2015. This IRIS certification has led to define local process owner, KPI, internal review of the processes to verify if the processes are still applicable or if HRSTS has to update the processes.*

Last certificate IRIS Certification rules: 2017 and based on ISO/TS 22163:2017 has been obtained in September 2019.

HRSTS considers that safety assurance process has progressed in a positive way and all necessary and sufficient measures have been put in place. All projects under Hitachi's responsibility have been independently assessed by different ISA. All processes in place have been audited and compliance with European standards have been demonstrated.

Regarding the overall actions in place on the safety assurance process and on the safety analyses since the development of the GEST, Hitachi estimates that the progress made secures the same outcome and the risks are reasonably mitigated.

16. On 5 November 2020 Hitachi STS provided the following update in response to questions we raised following review of its initial response:

1) What safety analysis is being done during the development and analysis processes?
[HR] : Our safety process in Hitachi is described in our IMS (Integrated Management System). The RAMS processes to be applied are described in different procedures and instructions. These procedures cover how HR plans, executes, monitors and controls the project RAMS activities pertaining to safety-related-systems, sub-systems, parts or components, consistent with the required standards (CENELEC standards).

2) How is the safety analysis in degraded mode recorded and used to prevent future errors?
[HR] : See previous response.

3) In what way has the process of cross acceptance been reinforced?
[HR] : For the cross acceptance process, HR is now using as input the following standard "50506-1 : Railway applications – Communication, signaling and processing systems – Application Guide for 50129 – Part 1 : Cross acceptance. The process of cross acceptance has been used on different HSL project. The last railways projects using the "cross acceptance" process are : Bretagne Pays de Loire in France (BPL) and Morocco Project. These projects implement the following technologies : Interlocking, ERTMS level 2, ERTMS Level1. These projects are in revenue service.

4) Please expand on how the Common Safety Methods are applied.
[HR] : The CSM are taken into account in the safety plan made on each project, according to the scope of the project. The safety plan describes the management of the safety, the safety methods used to demonstrate the achievement of the safety objectives. Risks are analyzed at the beginning of the project and mitigated. Risks are managed in an Hazard log, including the mitigation. Hazard log also includes the management of the safety requirements. Safety Related Applications Conditions (SRAC) – Safety requirements applicable to external stakeholder - are also part of the Hazard Log and reminded in the Safety Case. An Independent Safety Assessment (ISA) is undertaken on all safety activities made by Hitachi Rail STS.

5) What additional activities are being carried out which were not previously requested by the 2001 50128 standard?
[HR] : Tools Conformity analysis are now carried out according to the classification of the tools (T1, T2 and T3) in the version 2011 of the EN50128 standard.

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

17. 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.

18. 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.

19. 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

20. 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.

21. 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.*

22. 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.

23. 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.

24. 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 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

ORR decision

25. Network Rail Wales route has implemented a procedure to download and retain data held in the ETCS. Hitachi STS are developing a suitable data logging system as part of the Baseline 2.3.0.d development and implementation work required for the operation of the CAF train fleet. The work was expected to be completed by September 2020, but has been delayed by the COVID-19 pandemic. Commissioning is not expected until March 2021.

26. 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 March 2021.

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

Information in support of ORR decision

27. On 27 March 2020 Network Rail provided the following initial response:

NR has procedures in place to retain incident evidence at the time of an incident prior to any destructive testing or intentional system reboot.

Network Rail Wales route has implemented a procedure to download and retain data held in the ETCS. Data is extracted in hexadecimal form and converted to a

useable form by the technicians as part of a daily scheduled routine and would be undertaken prior to any destructive testing or intentional system reboot.

A process was developed for the recovery of service to ensure insertion of TSRs into the GEST following the incident in October 2017. This was used satisfactorily by the technicians following subsequent rollovers of the RBC. It should be noted that a rollover is not a fault. The RBC software will trigger a rollover as a safe response when authority movement conflicts, or other exceptional events, are detected.

An update was made to the RBC in approximately March 2019 since which no rollover has occurred and the recovery process has not been required.

Hitachi STS has agreed to replace the GEST with a version similar to that used on the TGV system which includes non-volatile memory to retain TSRs. This system is planned to be installed in summer 2020. (Recommendation 5). This will remove reliance on the recovery of service process which has not been invoked since the RBC update.

A data logger does not currently exist to extract and retain data. Discussions with Hitachi STS indicate this would not be a simple task and would take more than installation of typical data loggers. It would most likely involve significant data changes to the SICAM/SILAM equipment systems and the data collection ability of the track side equipment at Machynlleth. This would be a lengthy and costly exercise if undertaken as a standalone project.

Hitachi STS are being instructed to investigate the development of a suitable data logging system as part of the Baseline 2.3.0.d development and implementation work required for the operation of the CAF train fleet.

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

The system delivered on Cambrian has a Juridical recorder with the EVC on-board and a RBC maintenance equipment which automatically stores RBC internal status and data exchanged with other sub-systems.

A note will be produced containing a table which will list every log in all the Trackside (and Onboard) systems that should be downloaded in case of a suspected wrong-side failure. We will just list the titles of the logs and provide a cross-reference to the relevant O&M manual that documents the details. This note will also advise about the periodic download and the process to follow in case a failure before or after the recovery of the system.

The proposed timescale for this implementation is September 2020.

29. On 11 November 2020, Hitachi STS confirmed a revised timescale of 18 December 2020.

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

30. 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.

31. 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

32. 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.

33. 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.