Recommendation Status Report: Loss of safety critical signalling data on the Cambrian Coast line

This report is based on information provided to the RAIB by the relevant safety authority or public body.

The status of the recommendation(s), as reported to us, are described by the following categories:

Key to Recommendation Status

Open **(replaces Progressing and Implementation On-going)**	Actions to address the recommendation are ongoing.
Closed **(replaces Implemented, Implemented by alternative means, and Non-implementation)**	ORR consider the recommendation to have been taken into consideration by an end implementer and evidence provided to show action taken or justification for no action taken.
Insufficient response:	The end implementer has not provided sufficient evidence that the recommendation has been taken into consideration, or if it has, the action proposed does not address the recommendation, or there is insufficient evidence to support no action being taken.
Superseded:	The recommendation has been superseded either by a newer recommendation or actions have subsequently been taken by the end implementer that have superseded the recommendation.
Awaiting response:	Awaiting initial report from the relevant safety authority or public body on the status of the recommendation.

RAIB concern over the way that an organisation has responded to a recommendation are indicated by one of the following:

Red – RAIB has concerns that no actions have been taken in response to a recommendation.

Blue – RAIB has concerns that the actions taken, or proposed, are inappropriate or insufficient to address the risk identified during the investigation.

White – RAIB notes substantive actions have been reported, but the RAIB still has concerns.

Recommendation Status Report

Report Title	Loss of safety critical signalling data on the Cambrian Coast line
Report Number	17/2019
Date of Incident	20/10/2017

Rec No.	Status	RAIB Concern	Recommendation	RAIB Summary of current status
17/2019/01	Closed - I	None	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 softwarebased 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: l 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; l selection of suppliers that are competent and capable of delivering a safe system; l specifying the role of independent safety assessment bodies, such as	ORR has reported that Network Rail has reported that it has completed actions taken in response to this recommendation. ORR proposes to take no further action unless they become aware that the information provided becomes inaccurate.

Recommendation Status Report

			ASBOs (assessment bodies); l capturing the need for good engineering safety management, robust configuration management and change control in the contractual requirements; l defining the required safety integrity of the key safety functions, the operational context and external interfaces; l 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; l working with the supplier to properly understand the safety risks and define the system safety requirements and architecture; l monitoring the supplier's verification of its design (hardware and software); l ensuring that the design is suitably validated prior to commissioning; l audit and inspection by the client; l the extent of the client's review of independent assessments, and its own consideration of the safety justifications as part of the approval process; l testing and commissioning of the installed system, and subsequent maintenance; and l recording and retaining data needed for investigation of safety related failures.	

Recommendation Status Report

			This procedure should be shared with the wider rail industry with a view to it being adopted by other potential clients of high integrity softwarebased systems, such as train operators and rolling stock owners. (paragraphs 143d, 143f (I, iii and iv))	
17/2019/02	Closed - I	None	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: l the use of error messages generated by internal equipment functions to alert users to potential failures of the safety critical system; and l 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))	ORR has reported that Network Rail has reported that it has completed actions taken in response to this recommendation. ORR proposes to take no further action unless they become aware that the information provided becomes inaccurate.

Recommendation Status Report

17/2019/03	Closed - I	Blue	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; l completing the documenting and categorising of safety critical ERTMS/ ETCS failures; l identification of and implementing suitable means of collecting relevant information from all disciplines; and l assimilation of relevant information by staff from appropriate disciplines and those specialising in systems engineering. (paragraph 145c)	ORR has reported that Network Rail has reported that it has completed actions taken in response to this recommendation. ORR proposes to take no further action unless they become aware that the information provided becomes inaccurate.
17/2019/04	Closed - I	None	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.	ORR has reported that Network Rail has reported that it has completed actions taken in response to this recommendation. ORR proposes to take no further action unless they become aware that the information provided becomes inaccurate.

Recommendation Status Report

			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).	
17/2019/05	Closed - I	None	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).	ORR has reported that Network Rail has reported that it has completed actions taken in response to this recommendation. ORR proposes to take no further action unless they become aware that the information provided becomes inaccurate.