

Where next for “complex software-based systems”?



Dr Emma Taylor discusses the Cambrian railway incident and the roadmap for overcoming the challenges of implementing some of the Rail Accident Investigation Branch (RAIB) report's recommendations. Emma reflects on where and how the next insight-generating Cambrian-type analysis might come from, and considers whether the context provided by “cybersecurity” might add a complementary framework to create more clarity.

As an experienced safety engineer, used to imagining and asking, “what if (this happens)?” – in a rigorous and structured fashion of course – it can sometimes feel as if I inhabit a different world to many of my differently disciplined colleagues. For them, designing to requirements, standards and environmental and operational constraints to meet client and legislative requirements provides a focussed target. In contrast, safety can seem a bit open ended, for them we never seem to be in a position where we can stop worrying.

Whatever sector we work in, working in safety means that we rightly ‘lean in’ to the challenge of exploring and communicating the many combinations of potential paths to system malfunction (both potential and realised). Pointing to previous incidents and near misses remains an effective way of raising awareness and action, and as trends emerge through reporting and analysis, the evidence for a sustained and focussed campaign of action is strengthened. In some sectors such as rail, the requirement to report, understand and share through common systems is codified in legislation. For an overview of complex software-based systems and failures, many of the Safety Critical Systems Club events and publications contain useful guidance and analysis e.g. [1, 2].

This sharing of expertise is a complementary driver for change which sits alongside industry and system-wide changes following major accidents. The latter, perhaps unfortunately, remains an established route for effecting a change in the management of risk. High profile multi-fatality accidents, recently noted for complex software-based systems, such as the Boeing 737 MAX, increase both attention and action. Despite this, identification and understanding of the causal factors, and implementation and supervision of measures to manage the risk remain complex in nature – particularly when anticipating what has not yet happened.

Fortunately, a structured framework for analysis provided by standards and guidance is a recognised route for action, working through identification and implementation of risk mitigation measures ('controls') and spanning across the recognised triad of technology, people and processes. While there are challenges associated with the application of such standards, this is a recognised approach for safety-critical systems, and often also part of a required regulatory and commercial baseline. Third party and independent assessments also play an integral part in the verification and validation over a project lifecycle.

But what changes when you are operating outside the tight constraints of such a framework, or when the framework is not fully implemented? What happens when you are looking at trying to prevent types of failures that are not yet realised or recognised? Is it then still suitable to maintain a focus on learning from lessons identified? What about systems with different SIL levels that are connected? What limitations might occur? And how can the individuals and organisations adapt to the changes being caused through complex software-based systems?

This article provides a brief and personal commentary framed by these questions as seen through the perspective of being part of an industry team addressing recommendations published by Rail Accident Investigation Branch (RAIB) for an incident on a digital signalling system known as ERTMS (The European Railway Traffic Management System).

The full report is available publicly and includes an overview of the ERTMS signalling system, the incident and investigation, and subsequent recommendations placed on industry [3]. A briefing on the UK rail regulator's approach (Office of Rail and Road, ORR) to tracking the recommendations is available [4] and the ORR's publicly available report to RAIB on industry progress at the end of 2020 has been published [5]. A glossary of terms used may be of use for readers who are not familiar with the rail sector, particularly when specific terms are used by RAIB noting specific actions [6]. Industry continues to progress, with timelines set for formal resolution of the recommendations. But some of the questions raised by implementation of the actions themselves have been difficult to answer, and it is the path that's been taken and hurdles identified that are explored in this article.

Loss of safety critical signalling data on the Cambrian Coast line

The ERTMS system is based on the principle that a train driver receives signalling information (including line speed and temporary speed restrictions) from a digital display in the driver's cab. Digital information is transmitted two-way using train communication systems, and wayside computer-based systems are used to manage and update the information used on board by the driver. This necessitates software, databases stored on servers and manual entry of information by technical staff. This may occur when changes to the speed profile are required, such as a temporary speed restriction to reflect operational needs e.g. change in track condition or other temporary condition requiring a slower speed.

Over the past few years, ERTMS has been trialled on an operational line (the Cambrian Coast line) as part of the development towards broader deployment on the GB mainline rail network. On the 20th October 2017, a train driver noticed that a temporary speed restriction that they were expecting to see on their in-cab display was no longer there. It was only when they 'called it in' to the signallers asking what had happened that it was identified that the temporary speed restriction element of the ERTMS system had not functioned as expected. (Note that the temporary speed restriction in question was in place to prevent trains passing a level crossing too quickly so the consequences of a potential collision could have been quite severe). RAIB launched an investigation to work out what had happened and why.

To understand the context, it is key to map out the equipment, software and operational steps involved in providing the driver with signalling information (provided as part of a 'movement authority'). An operational train line is divided into segments and passage of a train in and out of that segment is controlled via signals (there should be normally no more than one train per segment). Speed information and ensuring trains travelling at a set speed is an important part of controlling the flow from one segment to another, and operational reasons may mean that the speed per segment may need to be changed (a temporary speed restriction). This is inputted by the signaller (at the terminal for the GEST System, or 'poste de Gestion des Signalisations Temporaires') and the information is then encoded into the broader packet of information sent to the train. The Radio Block Centre (RBC) sends movement authorities to trains and the (GEST) system. An overview of the systems involved is given in the figure below, taken from the RAIB report. Further information on the design, including the SIL rating of the different systems is reported [3].

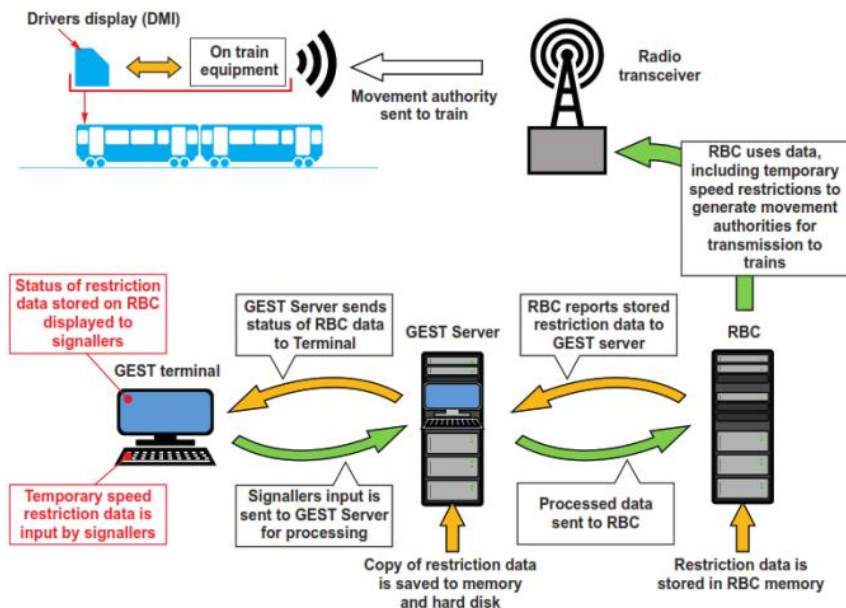


Fig 1 An overview of the Cambrian ERTMS incident [3]

Analysing a complex software-based system incident can be a complex task. The RAIB report was published on 19th December 2019, more than two years after the initial incident [3]. Comparing the date of the incident and the date of the report's publication (more than two years) hints at both the thoroughness of the investigation and the potential challenges associated with turning back time to understand where and how the root causes occur.

The process of incident investigation involved reconstructing the software development lifecycle, tracing back to when and where designs for this installation deviated from other applications of the ERTMS system, and also understanding why some local operational issues hadn't been identified and highlighted earlier. The causal factors pointed to a broad range of often foreseen problems, including problems with definition of safety-related requirements, hazard analysis process, validation of safety requirements, and design limitations around error handling/reporting, integrity checking and management of product upgrades. In the next section I'll discuss what the investigation found in the context of how industry responded to the RAIB recommendations.

An approach to implementation of some RAIB recommendations

Some RAIB recommendations (typically called 'Recs') were placed specifically on individual organisations such as the developer of the ERTMS system and Network Rail (Rec 2, Rec 4 and Rec 5) but two included the phrase "Network Rail, in consultation with RSSB and the wider industry..." (Rec 1 and Rec 3). The text of the recommendations in full are available [3]. Network Rail operated the line where the ERTMS system was installed, and RSSB is the Rail Safety and Standards Board which has a cross-industry role in a number of key areas, including railway safety.

Working in co-ordination, and with a mandate to engage the wider industry, meant that the technical challenges potentially became overshadowed by the wider engagement and communications challenge. The question of how to hit both marks became the subject of some discussion, and iterative planning by myself and others.

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 need for engagement with the 'wider industry' not only reflects the prevalence of complex software-based systems across the network, but also the challenge involved in the capture and dissemination of the learning so as to create the foundation for action. It is not just information distribution for information's sake, but a necessary requirement as a route to creating greater understanding and proactive engagement with software-based systems development and operation. A separate challenge was making sure that even if content was broadcast widely, would it be received and understood; i.e. was the package 'sticky' enough to gain people's attention? Where 'sticky' means not forgotten, laying the foundation for longer-term change. A separate programme of work continues on the other 'wider industry' recommendation addressing procurement of software from a client-based perspective [4].

It was a reasonable assumption that not all incidents that could happen would have happened yet, so learning from experience ('improve capture and dissemination of safety learning') would not give a complete picture. Also, could it be assumed that there was incomplete reporting and analysis of incidents and near misses that had already happened? My view is that physical failures of railway infrastructure are usually easier to spot than those within

the digital context, unless they provoke a visible and sustained block on operations such as the National Grid power supply issue, which led to a number of trains shutting down and requiring technician restart [7]. Separate to these limitations was my opinion (shared by others) that as most people didn't have a technical basis in software-based systems, it meant that some might feel uncomfortable reading overly technical details. Reflecting, it seemed as if a formula was needed to help cut through to reach a wide audience and so 'disseminate' the safety learning.

Network Rail developed a public domain website to support their response to the RAIB Cambrian 'Rec 3' including a case study format which covered only four slides [8]:

- Description of the incident (a few bullets)
- Immediate cause (one bullet, and a picture, [fig 1])
- A summary of causal factors [fig 2]
- Mapping to the V-cycle (verification and validation) [fig 3]

The causal factors (i.e. what happened and why) were extracted from the RAIB report and then condensed down, with common themes highlighted in green, using only the RAIB form of words. Looking at this one slide allowed a non-expert to gain an overview [fig 2].

Causal Factors

- Temporary speed restriction data was not uploaded to the RBC after a software rollover because the GEST sub-system had entered a fault condition, probably due to a corrupted database.
- No indication that the system had failed was provided to signallers.
- The memory used for storing temporary speed restrictions in the RBC was volatile, allowing temporary speed restriction data to be lost during a rollover.
- The required level of safety integrity for validation of temporary speed restriction data uploaded to the RBC following a rollover was not achieved by the design.
- GEST server software was unable to detect and manage the corruption of its database.
- The vulnerability of the system to a single point of failure had neither been detected nor corrected during the design, approval and testing phases of the Cambrian ERTMS project.
- The safety-related software requirements for the GEST software were insufficiently defined.
- The hazard analysis process did not identify, and so did not mitigate against, the GEST software thread failure mode.
- The validation process did not ensure that the safety requirement for the correct display of temporary speed restrictions was met.
- GEST was accepted into service without the production of a generic product safety case (or equivalent); had such a process been followed rigorously, it would probably have exposed the shortcomings in the software design.

Fig 2 Summarised causal factors for the Cambrian ERTMS incident [8]

To create further clarity, the causal factors were then mapped to the V-cycle as shown in fig 3. This approach usefully mirrors the guidance provided by RAIB in 2019 [9].

"Demonstrating digital system safety can be difficult, but that doesn't mean that we shouldn't try to master the problem. Existing industry guidance helps us by breaking the problem down into distinct steps: specification; definition of requirements; design, checking and testing; and validation against the originally specified requirements."

Design Issues

- Key operational data not uploaded to the main system after a software rollover due to a sub-system fault condition.
- No indication provided that the system had failed to the operators.
- Loss of key operational data during system rollover due to use of volatile memory.
- Sub-system software unable to detect and manage the corruption of its own database.

Process Issues

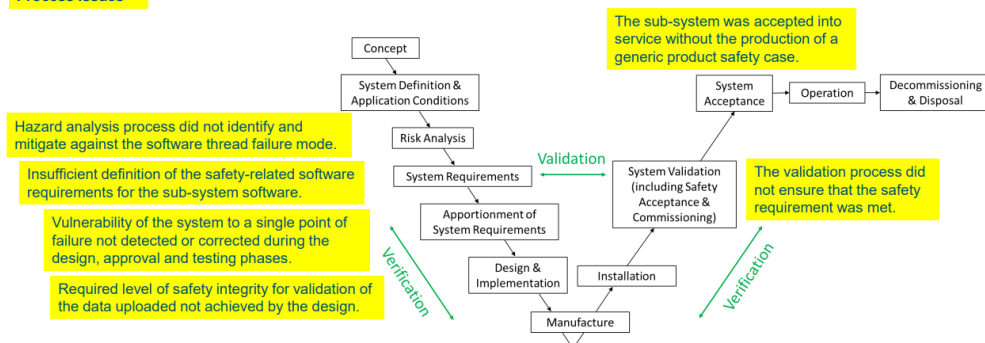


Fig 3 Mapping of Cambrian ERTMS causal factors to the V-cycle [8]

Working with the support of industry stakeholders, this formula was then used to develop ‘reasonably foreseeable scenarios’, further taking the causal factors and dividing them into people, technology and processes, mapping them into the categories typically used within the energy and other sectors.

The approach got people’s attention, whether for real world incidents that had happened, or reasonably foreseeable ones. I – and I suspect others – started to ask ourselves: “how would we know this had happened?” thus meeting the monitoring and reporting element of the Rec, and also framing the incident within our own operational and technical experience. (Note that, although the ‘reasonably foreseeable scenarios’ themselves are not widely distributed, the approach is presented in podcasts and webinars, referenced later in this paper).

This need for people to be aware and able to report what they see, even if based on incomplete information capture, is part of the activity needed to address safety learning (‘improve the capture’ in the language of the Rec). RAIB also noted the importance of considering all reasonably foreseeable circumstances (circumstances can be taken as another term for scenarios) when developing a software system [9]:

“It is fundamental that the process of digital design is robust enough to ensure that software-based systems operate correctly in all reasonably foreseeable circumstances. In this case, the people operating the railway did not know that there was anything amiss. Digital railways need to detect when they have failed and report this to those who need to know: in this case, the signallers”.

A parallel programme of work was also facilitated by RSSB to gather similar case studies across rail and other sectors [10], and to analyse and frame them within the V-cycle, delivering the case study message within a podcast format. A digital safety webinar was used to increase understanding of the importance of considering reasonably foreseeable scenarios and also the value of taking a cybersecurity perspective on train operations [11]. The concept of a ‘digital train’ played a key part in raising awareness and understanding of how complex software-based systems are an integral part of a transport system’s operations. All

three webinar speakers met the wider engagement and communications challenge embedded in Rec 3. All of the material was made publicly available on RSSB’s website [fig 4] as part of steps towards ‘developing digital competency’ and linked to from the Network Rail public facing page [8]. I think we got better as we went along. My favourite podcasts are the Cambrian and other case studies in a suite of four podcast episodes. The ‘introduction to digital safety’ one includes my Kazakhstan and space adventures too, which apparently made the software topic a bit more interesting.

Developing Digital Competency

24/03/2021



As the railway continues to develop and embed digital technologies, it becomes increasingly important to report and understand near misses and accidents with a digital component.

In response, RSSB has created free online material to develop greater understanding of complex software-based systems. This material support industry’s response to the RAIB Cambrian recommendations and raises awareness of digital asset integrity topics.

Cambrian incident - case studies from other sectors and 4 podcast episodes	▼
Reporting and learning from digital incidents - 3 blogs	▼
The NIS regulations - 2 podcast episode	▼
An introduction to digital safety - podcast	▼
Digital asset integrity, understanding a digital train - 1 webinar	▼

To find out more about other sectors and how their learning points on causal factors can be used in the railway, please read these aerospace, energy, medical and transport case studies.

Access case studies ➤

Fig 4 A public resource designed to support development of digital competency [11]

At the time of writing, the RAIB Cambrian recommendation’s ‘wider industry’ programme of work continues, including using the causal factor analysis from Rec 3 to act in effect as inspiration for “design requirements” for development of a strengthened lifecycle approach to procurement of complex software-based systems to meet Rec 1.

And, at an industry-wide level, awareness of this issue, along with an increasing call to action, continues to grow, with RAIB’s Chief Inspector stating, “demonstrating digital system safety can be difficult but it doesn’t mean we shouldn’t try and master the problem” [12].

What else can be done – and is there another challenge to meet?

My perspective is that it's clear that the rail industry is stepping up in responding to this important incident, and that further progress will be made, noting it is 'reactive progress' as it is reacting to an incident. Improvements in the implementation of the V-cycle, combined with increased awareness at technical and procurement level as to how things could go wrong, can clearly improve the overall management of complex software-based systems. Greater awareness and use of existing safety frameworks, maturity models, standards and guidance all provide a 'thinking and doing' roadmap.

But is it enough as it is?

Perhaps more provocatively, this parallel question can also be asked:

"Could a proactive cybersecurity perspective have helped modify the pathway to this incident?"

Or, put differently, if a cybersecurity risk assessment had been carried out, could it have identified (design and operational) vulnerabilities which, if addressed, would have truncated or interrupted the steps between design vulnerabilities and realisation of the potentially unsafe situation with the temporary speed restrictions?

I also think that this question cuts to the heart of the challenge involved in complex software-based systems, well as being nothing less than an enormous can of (potentially tasty) worms, which is only just starting to be opened. As outlined in the recent seminar IET Code of Practice on Cyber Security and Safety [13, 14], considering both safety and cybersecurity is not a simple problem space and there is no one size fits all.

The speakers at the launch outlined various challenges, including the clear view expressed that you could do a safety risk assessment or a cybersecurity risk assessment, not a combined one (at least not at this time). The very few people who have the skill set to do both have to choose which hat to wear. Despite this, they stressed that steps must be taken to move things forward, as "increasing connectivity is driving complexity", not only at the technical level, but the organisational structures and cultures around the systems themselves. It's perhaps stating the obvious, but the skills and mindsets that people have need to be broadened in order for the industry to have a better chance in managing these domains and changes.

For me, my personal view is yes to a cybersecurity risk assessment, and I'll be bold in saying that I think that a high-level screening from a cybersecurity perspective should be carried out for all complex software-based systems. At a minimum, it could identify additional design and operational requirements. It certainly gets people to put their thinking caps on; I saw how the three cybersecurity speakers in the 'digital asset integrity' webinar 'cut through' to the heart of creating a real world 'here today' mindset for complex software-based systems.

We could – and I think should? – move to the position of a systems led cybersecurity review being a default starting point. And then, depending on the findings, it is then an "Opt-out" decision point for more detailed follow on cybersecurity reviews, rather than having to make the case for an "Opt-in" cybersecurity risk assessment at the start. I also think that a 'basics' approach around case studies is where we need to start, having seen the power of the format used in both public domain and restricted access discussion formats.

Finally - a call to action for SCSC members?

In my mind there is no doubt as to the size of the task ahead in implementing the scope of the Cambrian RAIB recommendations that engage the wider industry on complex software-based systems. A bit like painting the Forth Bridge, I suspect the principles behind it will never be closed off, as changes in digital systems, both scope and reach of deployment, will be ongoing, and it is hard to predict the future fully.

My personal vision, having had the benefit of working across multiple sectors across many years, is that we – as individuals and as a SCSC community – should continue to seek, wherever possible, the opportunity to frame and exchange case studies and lessons learned. We know that it is not only 'what we say' but 'how we say it' that can increase the effectiveness of the message and how it lands, sticks and creates action. I found that in working on the RSSB podcasts that analysis of causal factors of complex software-based system incidents across multiple sectors certainly found common themes, and the use of podcasts was able to reach audiences that might not normally read a long accident report, or shorter brief. I'd encourage others to give it a try. You don't need to be a media star, frame it as a conversation! For some more handy tips, there is much practical experience in the SCSC community; I also presented some ideas, blending politics and everything else, at this year's Safety-Critical Systems Symposium [15].

As for other sectors, to work on staying ahead of the complex software-based systems curve, the rail sector can and does continue to learn. Sharing case studies, particularly in the template provided, does seem to provide a way to increase collective thinking and awareness. In terms of seeking inspiration, there's no harm in looking at what I call a 'snag list' taken from the IET Code of Practice on Cyber Security and Safety [13] (fig 5).

Section 2 Challenges at the intersection of safety and security

- 2.1 Reasonably practicable risk reduction is not easily defined for cyber security
- 2.2 Perceived conflict of objectives and expectations
- 2.3 Lack of common language
- 2.4 Different engineering perspectives
- 2.5 Quantitative vs qualitative assessment of likelihood
- 2.6 Porous system boundary
- 2.7 Dynamic nature of cyber security; static nature of safety analysis
- 2.8 Tensions over maintenance of cyber security
- 2.9 Different risk paradigms
- 2.10 Different risk control philosophy

Fig 5 Ten challenges to consider when preparing a 'reasonably foreseeable scenario' for a complex software-based system? [13]

And to wrap up...What is my call to action? I hope I've made a strong case for sharing case studies, using the template and formula presented here, and also the parallel importance of considering how the engagement and communications can be delivered in order to achieve impact. I've also extended a suggestion for next steps in the development of case studies by incorporating safety and cybersecurity. I would now like to open a discussion on how the SCSC community could help build on this work so please get in touch with myself (emma.taylor@scsc.uk) and Stephen Bull (stephen.bull@scsc.uk) to share your thoughts.

References

- [1] Annex B of Service Assurance Guidance Version 2 [SCSC-156A], The SCSC Service Assurance Working Group [scsc.uk/scsc-156A](https://www.scsc.uk/scsc-156A) Feb 2021
- [2] Annex H of Data Safety Guidance Version 3.3 [SCSC-127F], The SCSC Data Safety Initiative Working Group [scsc.uk/scsc-127F](https://www.scsc.uk/scsc-127F) Feb 2021
- [3] Report 17/2019: Loss of safety critical signalling data on the Cambrian Coast line: www.gov.uk/raib-reports/report-17-2019-loss-of-safety-critical-signalling-data-on-the-cambrian-coast-line. Accessed 1st May 2021.
- [4] Handling RAIB recommendations: www.orr.gov.uk/monitoring-regulation/rail/promoting-health-safety/investigation-enforcement-powers/handling-raib-recommendations. Accessed 1st May 2021.
- [5] RAIB Report: Loss of safety critical signalling data on the Cambrian Coast line on 20 October 2017: www.orr.gov.uk/sites/default/files/2020-12/raib-cambrian-coast-line-2020-12-18.pdf. Downloaded 1st May 2021.
- [6] Annex B: Glossary of terms used in RAIB reports: www.orr.gov.uk/sites/default/files/om/glossary-of-terms-used-in-raib-reports.pdf. Accessed 1st May 2021.
- [7] Report following railway power disruption on 9th August 2019: [www.orr.gov.uk/me-dia/10752/download](https://www.orr.gov.uk/media/10752/download). Accessed 1st May 2021.
- [8] Improving Railway System Safety: safety.networkrail.co.uk/improving-railway-system-safety/. Accessed 1st May 2021.
- [9] RAIB Annual Report 2019: assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/886627/AR2019_200521.pdf. Accessed 1st May 2021.
- [10] Learning from Other Sectors, www.rssb.co.uk/safety-and-health/learning-from-experience/accident-investigation-and-learning/learning-from-other-sectors, Accessed 10th May 2021.
- [11] Developing Digital Competency: <http://www.rssb.co.uk/en/safety-and-health/learning-from-experience/accident-investigation-and-learning/developing-digital-competency>. Accessed 1st May 2021
- [12] S French, The True Needs of End Users in Safety-Critical Software-Based Systems Design, RTM, https://mag.railtechnologymagazine.com/display_article.php?id=3954332&view=697292.
- [13] IET Code of Practice for Cyber Security and Safety: theiet.msafocus.com/k/Iet/code_of_practice_for_cyber_security_and_safety. Accessed 1st May 2021.
- [14] Code of Practice: Cyber Security and Safety Webinar: webinars.on24.com/theIET/CyberSafetyCode. Accessed 1st May 2021.
- [15] Taylor E A (2021) Influencing for Safety and Risk: A Novel Toolkit, Systems and Covid-19, Proceedings of the 29th Safety-Critical Systems Club Symposium Virtual Conference, 9th–11th Feb 21.

Image attribution: lead image: ID681094 © Paul Neyman. Fig 1, 2 and 3 from the RAIB accident report [3], fig 4 from RSSB website [10]

Dr Emma A Taylor CEng FIMechE FSArs

Emma is a safety engineer with 30 years of experience across space, energy and transport. This article is written in a personal capacity and references only public domain work done whilst she was at RSSB, as the RSSB lead for implementation of the Cambrian ERTMS Recs. During this project she worked closely with colleagues at RSSB and rail industry stakeholders, including Network Rail and the National Cyber Security Centre (NCSC) and would like to acknowledge the valuable contribution made by them in producing the public domain outputs. The views she expresses on the use of a cybersecurity risk assessment to assess complex software-based systems, and the blended approach to generation of future case studies, are personal, and do not form part of the industry's response to the Cambrian Recs. She is now Head of Digital Safety at a leading rail cybersecurity solutions company, RazorSecure, and is also a Past Chair of the Safety and Reliability Society, and a member of the SCSC Steering Group.

The opinions expressed here are for discussion only and should not be taken as the basis for regulatory, legal, commercial or technical advice.