Redefining rail systems verification and validation

Bearfield, George; Van Gulijk, Coen; Thomas, Richard James

DOI:
10.1177/09544097221102292

Case Study

Institution of MECHANICAL ENGINEERS

Journal of RAIL AND RAPID TRANSIT

Proc IMechE Part F:
J Rail and Rapid Transit
2022, Vol. 0(0) 1–9
© IMechE 2022
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/09544097221102292
journals.sagepub.com/home/pif
SAGE

Redefining rail systems verification and validation: The safety/security STAIRCASE model

George Bearfield[1], Coen Van Gulijk[2] and Richard James Thomas[3]

Abstract

Safety critical functions of the engineered railway need to perform at levels of integrity that are so high that an acceptable failure rate cannot be demonstrated through testing alone. Where such functions need to be implemented in complex programmable electronic systems certain design, build and test requirements are defined in technical standards and these are deemed to ensure that the correct level of systematic integrity is achieved. These approaches are based on assumptions around how system requirements are managed and delivered which are increasingly challenging to meet in practice. In particular the V&V lifecycle used in functional safety standards and emerging cyber security design standards is idealised. It assumes a top-down cascade of requirements for each delivery project. The approaches have become the de-facto standard internationally and are now mandated to an extent in European railway safety regulations. This paper proposes a different approach: a new lifecycle model that aligns better with the reality of the modern global supply chain and the order in which asset design and project delivery activities are actually undertaken to improve the ability to proactively manage safety.This leads to a fundamental change in the assurance philosophy to bring a simpler and more understandable approach. A framework for applying this approach is set out along with further research objectives to deliver the solution in practice.

Keywords

Railways, railway technology, RAMS, risk analysis, safety/safety engineering, safety-critical software, security, cyber security, safety assurance

Date received: 3 December 2021; accepted: 3 May 2022

Introduction

The railway was traditionally built from electro-mechanical systems whose function was relatively simple.[1] Members of railway staff were also time served, with a general degree of understanding of all aspects of railway function.[2] ‘Because of this there was a good local understanding of the railway’s function, both in normal operation and under failure conditions. On the modern railway, software systems are now being designed in localised pockets of expertise based in key locations around the world.[3,4] For local railway staff systems arrive as ‘black box’–commercial off-the-shelf (COTS) systems[5] and therefore the same degree of understanding does not exist locally. This loss of knowledge and lack of transparency makes it increasingly difficult for those who own and operate the system to build and maintain a high degree of assurance of its safety.

Major accidents can occur on the railway. In order to ensure that railway assets are designed, built and operated safely there are stringent regulations and standards in place. In Europe requirements are set in two high level directives[6,7] which are implemented in the national legislation of each member state. In support of this a number of lower level requirements also exist. One of these is the regulation for the common safety method for risk evaluation and assessment.[8,9] It requires that the responsible party determines whether the introduction of new technology into the railway is a ‘significant’ change. If a change is deemed ‘significant’ then a structured risk management process needs to be applied, evidenced and assessed by an independent body. The legislation recognises that various actors have a part to play in bringing complex railway technical systems into safe operation on the railway network. Asset manufacturers typically act as the responsible party for ‘placing in service’ i.e. for ensuring that the equipment is good as a product and fit to be sold for its intended application. The ultimate user of the equipment must put the system ‘in use’ and ensure that all necessary safety requirements for its operation and maintenance are met in situ. Effective transfer of risk information, and transparency between the actors is critical to the achievement of

[1]Engineering, University of Huddersfield School of Computing and Engineering, Huddersfield, UK
[2]School of Computing and Engineering, University of Huddersfield, Huddersfield, UK
[3]School of Engineering, University of Birmingham, UK

Corresponding author:
George Bearfield, Engineering, University of Huddersfield School of Computing and Engineering, Queensgate, Huddersfield HD1 3DH, UK.
Email: g.bearfield@hud.ac.uk

a safe outcome. The detailed approach to meet these regulatory requirements is set out in a number of specific safety engineering and functional safety standards. The risk management standard for the railway is EN50126 which is in two parts.[10]

The regulatory process includes particular requirements for 'Technical Systems'.[11] The 'technical system' means a product or an assembly of products including the design, implementation and support documentation: typically new signalling systems, or units of rolling stock for example. The development of a technical system starts with its definition and requirements specification and ends with its acceptance; although the design of relevant interfaces with human behaviour is considered, human operators and their actions are not included in the technical system.

The regulation itself is silent on how to meet the requirements associated with the safety functions of the 'technical system.' The most widely accepted technical standard that does so is the railway functional safety standard[12] which is linked to the wider risk management process set out in EN50126. EN50128 is the railway version of the widely adopted process functional safety standard.[13]

The safety lifecycle

The safety engineering approach described in EN50126 and embedded in EN50128 is based upon the application of a 'waterfall' approach to verification and validation. The representation of the cascading process takes on the shape of the letter V (see Figure 1)[14] describes the approach as it relates to software thus:

"Verification: the process of determining whether or not the products of a given phase of the software development cycle fulfil the requirements established during the previous phase. Validation: the process of evaluating software at the end of the software development process to ensure compliance with software requirements."

More informally Boehm describes the terms via two questions. For verification the question is: "Am I building the product right?" For validation the question is instead "Am I building the right product?"

Descending down the left hand side of the 'V' the process describes how the system designer decomposes its requirements to lower and lower levels of abstraction, verifying at each stage that the decomposition is correctly done. Then ascending upwards on the right hand side of the V, each sub-system and lower level design realisation is validated against the appropriately decomposed specification that was previously produced. In this way the presence of design errors that would lead to systematic faults is continually checked for, and their existence minimised. The process is conceptually clear and is based on a number of assumptions that are increasingly under challenge, namely:

- That a design is undertaken under the strong control and authority of a single central design authority.
- That activities happen in a fixed, logical and sequential order.
- And that the competence is in place to fully understand and interpret requirements and their validation evidence, across multiple separate teams and organisations.

Safety architecture of high integrity rail systems

The overall risk management framework defined in the CSM RA encompasses system definition, hazard identification and risk assessment and the definition, implementation and testing of safety requirements. The

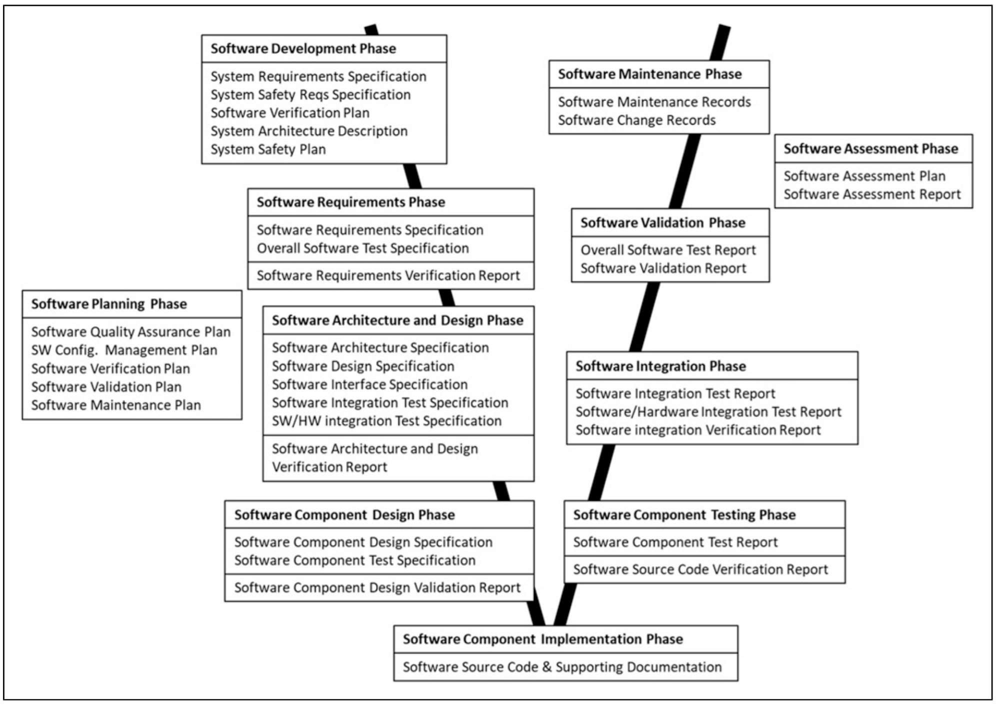
Software Development Phase
System Requirements Specification
System Safety Reqs Specification
Software Verification Plan
System Architecture Description
System Safety Plan
Software Maintenance Phase
Software Maintenance Records
Software Change Records
Software Assessment Phase
Software Assessment Plan
Software Assessment Report
Software Requirements Phase
Software Requirements Specification
Overall Software Test Specification
Software Requirements Verification Report
Software Validation Phase
Overall Software Test Report
Software Validation Report
Software Planning Phase
Software Quality Assurance Plan
SW Config. Management Plan
Software Verification Plan
Software Validation Plan
Software Maintenance Plan
Software Architecture and Design Phase
Software Architecture Specification
Software Design Specification
Software Interface Specification
Software Integration Test Specification
SW/HW integration Test Specification
Software Architecture and Design Verification Report
Software Integration Phase
Software Integration Test Report
Software/Hardware Integration Test Report
Software integration Verification Report
Software Component Design Phase
Software Component Design Specification
Software Component Test Specification
Software Component Design Validation Report
Software Component Testing Phase
Software Component Test Report
Software Source Code Verification Report
Software Component Implementation Phase
Software Source Code & Supporting Documentation

Figure 1. Key steps in the verification and validation development lifecycle (after EN50128).

evidence base that this activity has been done is typically referred to as a 'safety case', although the regulation does not use this term, the particular requirements relating to the safety of 'technical systems' are a subset of these requirements and there are specific approaches to develop and address them.

A revision to the CSM regulation (9) and its associated guidance set out a number of core safety critical functions of the railway. These are listed in Annex 1 of (11) and include for example:

1. Total or partial loss of braking effort.
2. Correct movement authority not enforced by the train.
3. One door being unlocked (with train crew not correctly informed of this door status).
4. One door released and opened in inappropriate areas (e.g. wrong side of train) or situations (e.g. train running).

Each of these functions is set a different severity class [i.e. (a) or (b) in point 2.5.5. in the Annex of the regulation.

> One and 2 above are examples of Category (a) failures, defined as: "a failure that has a credible potential to lead directly to an accident typically affecting a large number of people and resulting in multiple fatalities, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be less than or equal to 10^{-9} per operating hour."

> Three and four above are examples of Category (b) failures and are defined as "where a failure has a credible potential to lead directly to an accident typically affecting a very small number of people and resulting in at least one fatality, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be less than or equal to 10^{-7} per operating hour."

Both random and systematic failures need to be considered. A random failure is a failure whose occurrence is unpredictable in the absolute sense, but is predictable in a probabilistic or statistical sense. This is the domain of traditional reliability engineering. A systematic failure is a failure that is not determined by chance but is introduced by an inaccuracy or design flaw inherent in the system. Such failures occur repeatedly in the same set of circumstances. Software failures are always systematic as they are collections of instructions to a machine. Because there is a large state space of data input and outputs, such errors cannot be exhaustively tested for and may remain undiscovered in a system until a particular set of system inputs arises.

Digital signalling is being rolled out across rail networks[15] and rolling stock platforms are being developed with integrated Train Control and Monitoring Systems (TCMS).[16] The safety critical functions of the railway are now increasingly being delivered by complex, networked programmable systems and software. The approach described in both IEC61508 and EN50128 requires the risk of failure of each safety function to be estimated and failure targets (both random and systematic) to be assigned. The targets are called SILs (Systematic Safety Integrity Levels) and are classified at five levels, from 0 to 4, with the highest requirement being SIL 4 (see Table 1). This level is ascribed to demonstrate an average frequency of dangerous failure of the function of once in between 10^8 and 10^9 hours of operation, when safety functions are operating continuously. An alternative indicative failure rate is also specified for the probability of failure on demand of a safety function.

For systematic software failures, SILs simply indicate which particular software design measures and approaches and roles are deemed necessary to attain the required level. Any practical link between the application of the standard and the failure rate actually achieved is not clearly proven.[17] One critical aspect of compliance to the standards is the design of an appropriate system architecture. Partitioning and duplication of system functions is required in some circumstances to deliver high integrity. A given function is implemented multiple times in different ways. Residual software failures can then be detected and masked by comparing the outputs of these multiple systems to discard outputs that are inconsistent. Different approaches to 'voting' can be used depending on the application requirements. For example, for SIL 4 system functions a 'two out of three' (2oo3) voting system might be required (see Figure 2). Three diverse channels are created to deliver the same specified output, but each is realised independently through separate technology and/or technical expertise.

Such approaches are generally highly recommended for safety critical software and in many cases an essential feature of the system architecture.

Emerging weaknesses of the current approaches

The evidence for mitigating the risk from systematic failures is fundamentally the evidence of robust implementation of a clearly defined and formal waterfall development process for verification and validation. Compliance with this approach is coming ever more critical as digitalisation creates more potential for systematic failures. However rapid technological evolution is undermining a related set of assumptions that underpin the model:

- The model assumes that there is an overarching entity in control of the design. In reality the core platform is usually developed by integrating a range of different sub-systems into the railway, under control of a centralised computer system. The sub-systems are often developed through sub-supplier companies following their own verification and validation approaches independently of the project. The sub-system design is one step further removed than the asset platform design from an understanding of the operational safety requirements. This creates the possibility for miscommunication, misunderstanding, or loss of documented assurance of safety requirements.
- The V & V lifecycle assumes a fixed sequence of activities throughout the design, implementation and

Table 1. SIL levels - (Table from IEC61508 part 1, page 34).

Safety integrity level	Average frequency of a dangerous failure of the safety function (h^{-1}) (probability of failure per hour)
4	$\geq 10^{-9} - < 10^{-8}$
3	$\geq 10^{-8} - < 10^{-7}$
2	$\geq 10^{-7} - < 10^{-6}$
1	$\geq 10^{-6} - < 10^{-5}$

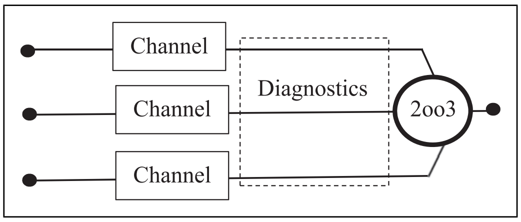

Figure 2. Two out of 3 voting architecture (Diagram from IEC61508 part 6).

test of the system in its entirety. This way of working, the 'waterfall' method, is no longer the default approach in software development which creates a mismatch of method. As already mentioned different parts of the development are undertaken at different times. Also, agile approaches to software development are based on a less structured approach with iterative sprints to build a functional and user centred system.[18]

- The approach of certifying to a SIL level at the sub-system level is sub-optimal. The SIL concept is intended to be applied to functions not systems; the integrity of the function should be assured with respect to a functioning train, in which the sub-system has been integrated and configured for its particular use.
- As regards architectural design of the system, duplication of system hardware requires significant additional work and cost and requires rare, highly skilled resource and expertise. Even if it is possible to have multiple teams of the right level of skill and experience it is difficult to ensure that their design solutions and implementations are truly diverse. Common specifications and design assumptions might be cascaded to these teams and common supply chain elements used will undermine the ability to build a high integrity solution.
- The platform will form the core basis of a wide range of different applications each with its own operational use case. The delivery project requires local adaptations to national standards and local operating rules and constraints. Ultimately safety and security requirements can only be truly and fully understood when a system is considered in its actual operating environment.

Together, these issues create a greater opportunity for systematic failures to exist and remain undetected, and for the effectiveness of assurance to be undermined. It is an accepted principle that engineered systems must be safe and secure by design, [19–22]. However safety and security requirements analysis work often only begins in earnest to meet final authorisation deadlines, rather than proactively, to improve the inherent safety of the product. This approach leads to project delays and increased costs. It also creates the potential for unnecessary residual risk caused by sub-optimal design decisions made under delivery pressure and against a back drop of sunk costs.

Many of the difficulties highlighted above have been raised in other sectors.[23–25] They were tragically evident in the causation of the crashes of the Boeing 737 Max aeroplane in Indonesia and Ethiopia in 2018 and 2019 in which 346 people died. The immediate cause of those accidents was determined to relate to its Manoeuvring Characteristics Augmentation System (MCAS) which was designed to adjust the horizontal stabilizer trim to push the plane nose down so that the pilot would not inadvertently pull the airplane up too steeply, potentially causing a stall. In both crashes it was determined that the MCAS was activated by erroneous indications from its sensors, which were not duplicated in the design to enhance functional integrity. The investigation[26] found that "*the MCAS was not evaluated as a complete and integrated function in the certification documents that were submitted to the FAA,*"

It also found that:

> "The lack of a unified top-down development and evaluation of the system function and its safety analyses, combined with the extensive and fragmented documentation, made it difficult to assess whether compliance was fully demonstrated."

Emerging challenges: Cyber security and safety expectations

In addition to unintentional safety flaws digitalization brings a whole new threat: malignant intrusion of networked systems. The emergence of cyber security vulnerabilities must also be managed in the design, build, operation and maintenance of complex railway technology. Standards and legislation to manage the risks of cyber security have developed with a degree of independence and separation from the systems and approaches to manage safety risk. Security and threat risk management standards have arisen[27–29] which broadly follow a 'plan, do, check, act' management framework and V & V lifecycle of the same type as that specified in the framework described in EN50126/8, and therefore many of the challenges set out here are relevant to cyber assurance as well. More specifically, in the UK, the Department for Transport stresses that all risks must be managed according to the usual legislative safety management and risk acceptance principles: the subset of security issues with safety implications

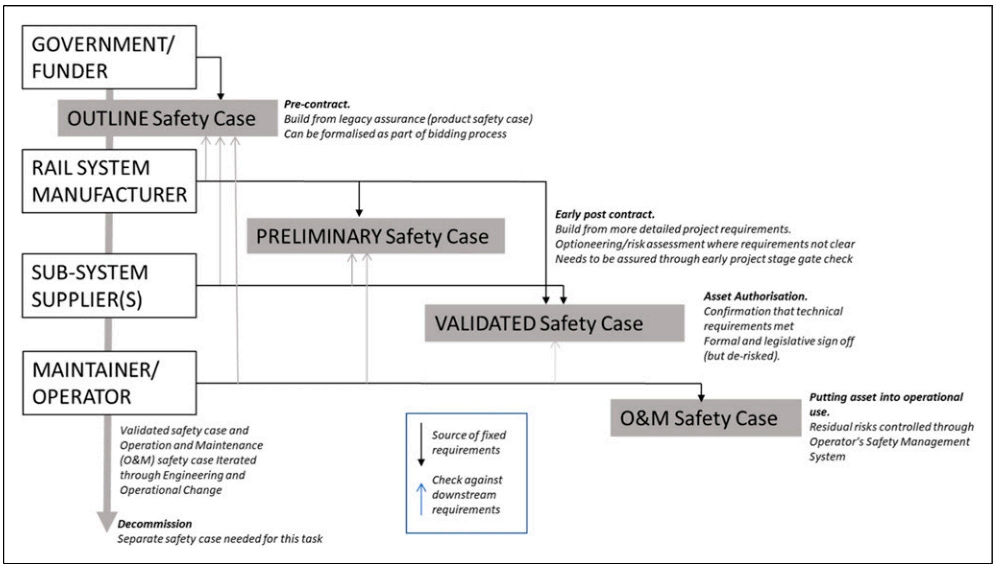
GOVERNMENT/
FUNDER
OUTLINE Safety Case
Pre-contract.
Build from legacy assurance (product safety case)
Can be formalised as part of bidding process
RAIL SYSTEM
MANUFACTURER
PRELIMINARY Safety Case
Early post contract.
Build from more detailed project requirements.
Optioneering/risk assessment where requirements not clear
Needs to be assured through early project stage gate check
SUB-SYSTEM
SUPPLIER(S)
VALIDATED Safety Case
Asset Authorisation.
Confirmation that technical requirements met
Formal and legislative sign off (but de-risked).
MAINTAINER/
OPERATOR
O&M Safety Case
Putting asset into operational use.
Residual risks controlled through Operator's Safety Management System
Validated safety case and Operation and Maintenance (O&M) safety case Iterated through Engineering and Operational Change
Decommission
Separate safety case needed for this task
Source of fixed requirements
Check against downstream requirements

Figure 3. The safety STAIRCASE lifecycle model.

must therefore be considered within existing, mandatory safety assurance activity. This implies a degree of integration in how safety and security requirements are developed and met. However:

- the approaches to architectural design are different: security levels require a zoning approach[28,29] that is different to the concepts of redundancy associated with SIL assurance.
- There are practical and cultural conflicts; good safety culture requires the open sharing of safety information to support learning.[30–32] However there is typically much more secrecy around security information.
- Cyber security risks are characterised by rapid evolution. This manifests in systems design as continual update of software. This rapid update must be reconciled with the need for robust and stable safety systems to minimise the chances of introducing systematic safety failures.
- As risks are being deliberately created by 'threat actors,' traditional safety engineering and reliability methods, based on randomness, may no longer be valid, and the legislative assumption that the person who creates the risk must manage it, flounders.

Some of these challenges are explained in detail in a code of practice produced by the Institute of Engineering and Technology.[32] It should also be noted that railway safety performance has increased significantly over recent years.[33] In this environment there is now comparatively little practical experience of the occurrence of major accidents than in previous decades. Based on the significant work on 'societal concern' (Hoyland, 2018, Bearfield, 2014) it is known that the travelling public has a very low tolerance for rail accidents (Van Gulijk, 2018). The sector needs to ensure that new systems are at least as safe as the more simple and well understood technologies they are replacing, and that the new emergent risks are mitigated as effectively as the old.

Improved model: The safety/security STAIRCASE model

The emerging, technological challenges set out above pose a fundamental challenge to the applicability and assurance of the use of the classical V & V lifecycle model for safety and cyber security engineering. A new model is needed which creates the environment to have meaningful and productive engagement on the emerging risks and design challenges set out here. This paper proposes a revised assurance lifecycle model, the safety 'STAIRCASE' (see Figure 3).

The left-hand side boxes show the different generic organisations responsible for determining the system and its requirements. Each has a different role to play sequentially, in ensuring that robust safety and security requirements are identified and implemented. The blue boxes indicate the type of safety case produced at key project lifecycle phases (the phases are annotated in bold italics). The bold downward lines indicate the source of fixed safety requirements for each safety case. The upwards arrows indicate the source of downstream requirements that need to be checked against the prevailing fixed requirements.

There are some similarities between the concepts set out here and the hierarchical concept of a Generic Product Safety Case; a Generic Application Safety Case and a Specific Application Safety Case as outlined in.[10] Both recognise the fact that V & V activities have layers, different owners, and a natural temporal place. However the STAIRCASE Model is based on the idea that each responsible party must consider all requirements to the level that they are able to, at the point in delivery where they are the lead organisation.

Outline safety case

In the spirit of safety by design, the proposed framework recognises the critical importance of effectively identifying key safety requirements as early as possible, in order to de-risk project delivery and ultimately achieve the best outcome. In particular, the pre-contract safety case creates a commercial incentive to enhance safety and security by design and address the emerging design assurance issues described in this paper and creating additional pressure for these architectures to evolve to meet the rapidly evolving digital assurance risks.

The first significant evaluation of safety should be a part of the tender process, and a basis on which the contract is selected. The safety case would in effect be a first iteration through the risk management process already defined in the CSM RA regulation or its equivalent, focussing on the requirements within the design control of the manufacturer. This should not actually create significant additional work as the 'first of type' platform analysis should provide the bulk of the 'Reference System' evidence that is legally required for subsequent safety demonstrations. Perhaps the most significant change to address is that teams evaluating bids would need the technical competence available to evaluate such safety information at that early stage. Input from experienced operators in the local domain of application is highly valuable here too, as it would be an opportunity to determine whether there were any local application changes needed, prior to the design being frozen. Creating some formal stage-gate here would help to get the right level of engagement early on and create the incentives to make this happen.

Preliminary safety case

With the outline safety case and core argument understood, early project work can focus on identifying any location specific changes or adaptations that might have been missed. This requires early engagement with the future user/operator on operational risks and controls. Clear safety requirements can then be cascaded into the tier 1 and tier 2 supply chain, enhancing compliance, project delivery and assurance.

Validated safety case

The validated safety case should be a relatively defined and simple process associated with the key regulatory stage gate. It should be about gathering the necessary information to evidence the safety argument and provide assurance that all is already in place. The approach makes this a more mechanical process, bringing greater assurance, ensuring that there is a clear audit trail for the safety argument and a solid basis for risk transfer into the operation and maintenance phases.

Fundamentally the approach is based on strengthening the ownership of the whole project at the concept stage, and with the ultimate 'owner' taking overall accountability for the whole assurance process. This should have many benefits as regards getting things right first time, and importantly it should strengthen the overall approach to systems integration, as there is a controlling mind for the process and its application.

Case study: The ETCS cambrian line failure

In 2017, a train driver travelling on the Cambrian Coast line in North Wales, UK reported a fault with the information provided on his in-cab display. Temporary speed restrictions were not being transmitted to several trains under their control. The temporary speed restrictions were required on the approach to seven level crossings to provide level crossing users with sufficient warning of approaching trains so that they could cross safely. The line was equipped with a pilot installation of the European Rail Traffic Management System (ERTMS), a form of railway signalling which transmits signalling and control data directly to the train. Investigation, by the local maintenance staff, found that the signalling system stopped transmitting temporary speed restriction data after it had experienced a shutdown the previous evening. The signallers had no indication of an abnormal condition and the display at the signalling control centre (on the 'poste de GEstion des Signalisations Temporaires' or 'GEST' system) wrongly showed these restrictions as being applied correctly. The UK[37] undertook an investigation. It found that:

- An automated software reset occurred when the equipment requested part of a movement authority that it had previously released for use by another train.
- Temporary speed restriction data was not uploaded to the signalling system after the software reset, because the external database of signaller information had entered a fault condition.
- The system was not designed to provide any indication to signallers that the system had failed.
- The memory used for storing temporary speed restrictions in the Radio Block Centre (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.

A sample of findings from the report have been reviewed against the STAIRCASE method here in order to determine how use of the approach could have prevented or minimised the risk from this incident (see Table 2).

In summary, the failure mode would have been much more likely to be prevented by robust application of the STAIRCASE methodology using competent people. More generally, the STAIRCASE methodology would have created earlier and more rigorous focus on the core safety argument and methodology, bringing a range of wider benefits.

Research and further work

Further work is needed to refine the methodology and to test the approach on a real-world project. This would involve:

Table 2. Review of the benefits of the STAIRCASE model against selected recommendations from the RAIB report into the failure of the ETCS system on the Cambrian line in 2017.

Rail accident investigation branch finding	Improvement with STAIRCASE approach
Only limited amounts of information could be found from the original design work so the investigation needed the supplier to undertake the time consuming task of reverse engineering the GEST sub-system to understand how the system operate	STAIRCASE methodology would have required that original design work and safety argument was available as part of the OUTLINE SAFETY CASE, and was subject to review, prior to contract. The information needed would therefore have been available
Software code which had been part of another product used in Spain was adapted to create the GEST sub-system. Much of the safety case documentation assessed as part of the introduction of the GEST subsystem was based on that prepared for a different project. The use case for this system was different as it was based on track maintenance staff using the GEST terminal, not signallers	The STAIRCASE methodology would have required that this documentation was reviewed and assessed pre-contract. Such review would focus on the system definition and scope, and also on key safety critical functions. Review of 'reference system' arguments and their applicability would be expected to identify key application differences like this
On this other project, the signalling system was reconfigured to store temporary speed restrictions in non-volatile memory	This indicates that the failure mode was able to be recognised. The earlier engagement on the key safety argument here would have likely increased the chances of identifying the failure mode, and ensuring that it was rectified in the design, in particular as it was a relatively simple change that would be very simple to implement at that time. Note that the CSM RA states that a reference system shall have • Similar functions and interfaces as the system under assessment • be used under similar operational conditions as the system under assessment So a competent review would have identified this issue
The ETCS should prevent a train from travelling at more than the permitted speed with a safety integrity level of SIL. [the GEST server failure] resulted in both the failure to upload the temporary speed restriction data to the [signalling system], and the failure to provide the signallers with the correct information needed for them to undertake the human validation. This demonstrated that the two functions were not independent and so the supplied system did not achieve the intended integrity level	The STAIRCASE methodology would enforce a review of the safety argument prior to contract being let. This would focus on the highest risk areas so would certainly look at the robustness of the argument is place to substantiate SIL 4 integrity claims. It is highly likely that a review would have flagged this lack of redundancy
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 ETCS project	The greater availability of information, and the more targeted evidence based stage gates in place for the STAIRCASE method would have increased the chances of it being identified at each subsequent gate, and validated as being in place to substantiate the VALIDATED safety case
The safety related software requirements for the GEST software were insufficiently defined	The STAIRCASE methodology encourages and stresses focus on key architectural safety requirements at the PRELIMINARY safety case stage so that clear requirements can be cascaded to the supply chain, and the more proactive focus would have provided greater assurance that such requirements would be met in practice

- Aligning contracting, governance and assurance to implement the model set out (this could be done voluntarily on a contractual basis, rather than requiring any legislative change). Having said that, should the approach be successfully implemented contractually, it may make sense to review the prevailing legal frameworks to embed it. As the method is based on fundamental principles of good safety engineering this should not, in theory, present a significant challenge.
- Consideration of the optimal safety and security architecture for different rail assets, to support productive discussions on these topics.
- Clarification of the revised, ideal competence requirements needed to support the effective application of the revised model.

Conclusion

Rail Technology is becoming more digitally complex and this is challenging the existing approaches to achieving safety assurance of software driven functions. Meanwhile the travelling public have rising expectations for safety. The processes for building safety integrity need to be effective and transparent and need to drive the right design and assurance behaviours in the real world. The approach presented here provides an avenue of research for addressing these challenges through development of a refined safety and security lifecycle model, that is attuned to real world behaviours and the need for proactive safety analysis and assurance.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iDs

George Bearfield https://orcid.org/0000-0001-5177-4960
Coen Van Gulijk https://orcid.org/0000-0003-4541-2693

References

1. Smith RA. Railway technology-the last 50 years and future prospects. *JRTR: Jpn Railway Transport Rev* 2004; 27: 16–24.
2. Crosby JP. Training and skills requirements for British rail depot maintenance staff. *Proc Inst Mech Eng D: Transport Eng* 1988; 202(2): 119–124.
3. Branch AE. *Global supply chain management and international logistics*. Milton Park, EN: Routledge, 2008.
4. Esposito E and Passaro R. The evolution of supply chain relationships: an interpretative framework based on the Italian inter-industry experience. *J Purch Supply Manag* 2009; 15: 114–126.
5. Wetherholt M. The software assurance of COTS software products. In: AIAA Infotech@ Aerospace Conference and AIAA Unmanned. Seattle, WA: Unlimited Conference; 20099 April 2009.
6. EU. *Directive (EU) 2016*, 2016./798 of the European Parliament and of the Council of 11 May 2016 on railway safety.
7. EU. *Directive (EU) 2016*, 2016./797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (Text with EEA relevance).
8. EC (2015) COMMISSION IMPLEMENTING REGULATION (EU) 2015/1136 of 13 July 2015 amending Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment.
9. EU. *On the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009*, 2013. Report EU No 402/2013.
10. EN50126. Railway applications-the specification and demonstration of reliability. *Availability, maintainability and safety (RAMS)*, 2017.
11. European Union Agency for Rail. *Guideline for the application of harmonised design targets (CSM-DT) for technical systems as defined in EU regulation. ERA-REC-116-2015-GUI*, 2017. Version 1.1, 18/05/2017.
12. EN50128. Railway applications-the specification and demonstration of reliability. *Availability, maintainability and safety (RAMS)*, 2011.
13. IEC 61508-1: 2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems*, 2010.
14. Boehm B. Verifying and validating software requirements and design specifications. *IEEE Softw Los Alamitos* 1984; 1: 1–88.
15. Network Rail. *Digital signalling, long term deployment plan*, 2019. https://www.networkrail.co.uk/wp-content/uploads/2019/06/Digital-Railway-Long-Term-Deployment-Plan-Technical-Report-Executive-Summary.pdf 26 11 20.
16. IEC 61375-2-6. *Electronic railway equipment - Train communication network (TCN) - Part 2-6: On-board to ground communication*, 2018.
17. Griffin DLK and Bearfield G. The use of design targets in harmonisation of safety management in the European rail industry. In: *Risk, reliability and safety: innovating theory and practice - proceedings of the 26th European safety and reliability conference*; 2016, pp. 208–214.
18. Beck K, Beedle M, van Bennekum A, et al. *Manifesto for agile software development*, 2001.
19. Bearfield G. Achieving clarity in the requirements and practice for taking safety decisions in the railway industry in great Britain. *Proc Eur Saf Reliability Conf* 2007; 1: 559–564.
20. Islam G and Storer T. A case study of agile software development for safety-critical systems projects. *Reliab Eng Syst Safe* 2020; 200: 2020.
21. Van Gelder P, Klaassen P, Taebi B, et al. Safe-by-design in engineering: an overview and comparative analysis of engineering disciplines. *Int J Env Res Pub He* 2021; 18(12): 6329.
22. Bearfield G, MacDonald R and Boreham N. The management of engineering change-producing tools and guidance for the rail industry. In: *6th IET professional development course on railway electrification infrastructure and systems*; 2013.
23. Freitas L, Scott WE and Degenaar P. Medicine-by-wire: practical considerations on formal techniques for

dependable medical systems. *Sci Comput Program* 2020; 200: 102545.

24. Naor M, Adler N, Pinto GD, et al. Psychological safety in aviation new product development teams: case study of 737 MAX airplane. *Sustainability* 2020; 12: 8994.
25. Thomas J, Davis A and Samuel MP. Integration-in-totality: the 7th system safety principle based on systems thinking in aerospace safety. *Aerospace* 2020; 7: 149.
26. US Federal Aviation Administration. *Joint authorities technical review, boeing 737 max flight control system*, 2019.
27. EN ISO/BSIEC: 27001. *Information technology. Security techniques. Information security management systems requirements*, 2017, p. 2017.
28. BS EN IEC 62443-3-2. *Security for industrial automation and control systems. Security risk assessment for system design*, 2020.
29. CLC/TSTS: 50701. *Railway applications - cyber security*, 2021, p. 2021.
30. Kriaa S, Pietre-Cambacedes L, Bouissou LM, et al. A survey of approaches combining safety and security for industrial control systems. *Rel Eng Syst Safe* 2015; 139: 156–178.
31. Adjekum DK and Tous MF. Assessing the relationship between organizational management factors and a resilient safety culture in a collegiate aviation program with safety management systems (SMS). *Saf Sci* 2020; 131: 2020.
32. IET. *Institute of engineering and technology/national cyber security centre: code of practice*. Cyber Security and Safety, 2020.
33. European Union Agency for Railways. *Report on railway safety and interoperability in the EU*, 2020.
34. Høyland S. Exploring and modelling the societal safety and societal security concepts – A systematic review. *Empirical Study Key Implications Saf Sci* 2018; 110: 7–22.
35. Bearfield G. *Taking safe decisions and the CSM on risk evaluation and assessment*. IET Seminar Digest, 2014.
36. Van Gulijk C, Hughes P, Figueres M, et al. The case for IT transformation and big data for safety risk management on the GB railways. *Proc IME O: J Risk Rel* 2018; 232(2): 151–163.
37. Rail Accident Investigation Branch. *Loss of safety-critical data on the Cambrian coast line*, 2019. Report 17/2019 Published December 2019.