Transformation of cyber security/safety assurance

Bearfield, George; van Gulijk, Coen; Parkinson, Simon; Thomas, Richard J

Transformation of Cyber Security/Safety Assurance

George Bearfield[1], Coen van Gulijk[1], Simon Parkinson[1], Richard J. Thomas[2]

[1] Institute of Rail Research, University of Huddersfield, Huddersfield, United Kingdom
[2] Birmingham Centre for Railway Research and Education, University of Birmingham, Birmingham, United Kingdom
Corresponding Author: TBC (Sharon.Jones@RSSB.co.uk)

Abstract

In the past decade rapid digitalisation of railway assets - including signalling and rolling stock - has occurred in parallel with a rising cyber security threat to critical national infrastructure. Rail safety requirements remain stringent and legacy standards for delivering safe, high integrity, complex digital systems exist. Security standards are emerging which implement some of the same principles of design and assurance as these safety standards, but do not do so in an integrated way with the safety discipline. There are two fundamental challenges emerging. The first is that safety design requirements and security design requirements have parallel principles and constraints related to segregation and partitioning of systems and networks in the design, but no proven good practice exists for how to meet both sets of requirements in an integrated way for any given asset. The second is that the verification and validation 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. It is increasingly difficult to meet these requirements in practice. This paper explains the many challenges in order to inform subsequent research, standardisation and industry activity needed to address them.

Keywords: Cyber Security, System Safety, Railway, Functional Safety

1. Introduction

Functional safety of software driven systems is an increasing challenge for the rail industry [1]. For example 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. The temporary speed restrictions that were required to safely traverse the level crossing were not implemented. The [1] undertook an investigation and found a range of failures with the way that the safety of what was a software driven system had been designed and delivered across the full variety of engaged organisations. Similar failings were 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. The US Federal Aviation Administration investigation) [2] 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."* Many of the difficulties highlighted above have been raised in other sectors [3][4][5].

Over the past 10 years, cyber security has become a dominant concern across the railway. For example, advances in railway rolling stock have moved towards platform-based architectures, with the ratification of ISO 61375 (the Wired Train Bus) providing a heterogeneous network in which systems are no longer connected with point-to-point connections, but instead uses a common network to communicate across all systems of systems. This increases the 'attack surface', where a software defect, exploited by an adversary, on one component can have serious consequences. This might, in some cases, create risks that were not considered as part of the asset 'safety case'. The role of the rail asset manufacturer has also fundamentally changed from having authority across all components fitted to the vehicle to one of being a system integrator, meaning that they have reduced control over the functionality of systems and components, in particular in the way the customer (and manufacturer) requirements are designed and implemented in software. This presents a new risk that the requirements have not been implemented correctly, where safety assurance now becomes a costly and difficult process due to the high level of inter-connectivity between. Safety and cyber security are no longer independent topics. A combined approach is increasingly required throughout their delivery.

3. Standards and Regulation

The application of robust system safety engineering techniques is necessary to meet regulatory requirements for railway safety. The detailed approach to meet such requirements is set out in a number of specific safety engineering and functional safety standards. The regulatory process in Europe includes particular requirements for 'Technical Systems' [6]. 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 (EN50128:2011) 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 (IEC61508-1:2010).

3.1 The Verification and Validation 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). Boehm [7] 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?".

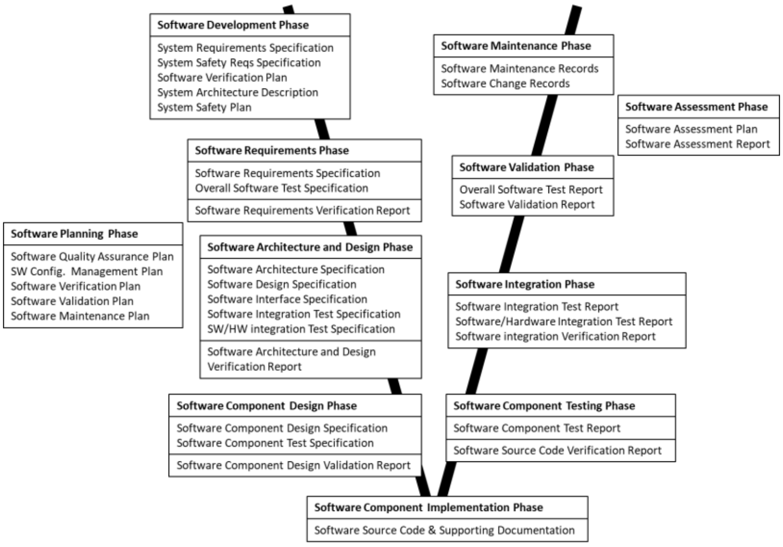
Software Development Phase
System Requirements Specification
System Safety Reqs Specification
Software Verification Plan
System Architecture Description
System Safety Plan
Software Maintenance Phase
Software Maintenance Records
Software Change Records
Software Assessment Phase
Software Assessment Plan
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: Verification and Validation lifecycle from EN50126

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; activities happen in a fixed, logical and sequential order and the competence is in place to fully understand and interpret requirements and their validation evidence, across multiple separate teams and organisations.

3.2 Functional Safety

The standards require a 'functional safety' approach. The railway can be decomposed into its safety critical functions (e.g. Total or partial loss of braking effort, whole train) EU [8] define each of these functions and assign each a different severity class. Broadly these set different levels of safety integrity that must be built into the functions. 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.

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.

Safety Integrity Level (SIL)	Average frequency of a dangerous failure of the safety function [h^{-1}] (Probability of failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

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

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 (Griffin and Bearfield, 2016). 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.

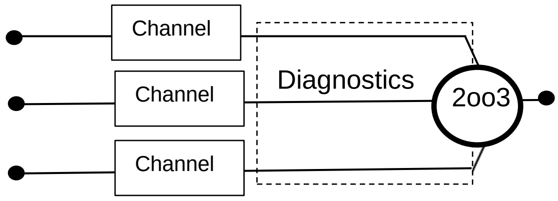

Figure 1: 2 out of 3 voting architecture (Diagram from IEC61508 part 6)

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

3.3 Cyber Security

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 in parallel with the systems and approaches to manage safety risk. Security and threat risk management standards have arisen (BS EN ISO/IEC 27001:2017, BS EN ISO/IEC 62443-3-2:2020, TS CLC/TS 50701: 2021) 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.

The technical standard TS 50701 also has a concept of Security Levels which is similar in concept to the Safety SIL approach, though different in the detail. It states that the security level is a: *"measure of confidence that the zone, conduit or a component thereof is free from vulnerabilities and functions in the intended manner".*

The specification defines architectural design constraints on rail assets, based on the concepts of zones and conduits. It defines a zone as a: *"grouping of logical or physical assets based upon risk or other criteria, such as criticality of assets, operational function, physical or logical location, required access (e.g. least privilege principles) or responsible organization."* It also states that: *"The definition of zones includes measures for encapsulation of functionality to keep a particular service alive in case of an incident in another zone; the same way as capabilities to isolate an incident by closing the gateways to the infected zone."*

TS50701 defines a conduit as a: "logical grouping of communication channels, connecting two or more zones, that share common security requirements." It states that the zone model applied depends on the threat risk assessment and the target architecture of each railway operator. It requires that communication and human interactions in high criticality zones are monitored, logged and stored for forensics at least at the subsystem boundaries. It also requires that security devices between zones with different criticality that protect the zone with the higher criticality should be managed by the responsible organization of the higher criticality zone. Higher criticality zones are required to consider inputs from lower security zones as potentially hostile.

4. Two fundamental weaknesses

There are two fundamental challenges emerging. The first is that safety design requirements and security design requirements have parallel principles and constraints related to segregation and partitioning of systems and networks in the design, but no proven good practice exists for how to meet both sets of requirements in an integrated way for any given asset. Note that, for example, 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. It is increasingly recognised that the subset of security issues with safety implications must therefore be considered within existing, mandatory safety assurance activity.

The second is that the verification and validation 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.

4.1 Parallel architectural requirements

Any architectural design requires trade-offs and optimisations. The fundamental principle to address here is that the safety impact of cyber security risks and vulnerabilities is itself a critical input to the cyber security risk assessment. The cyber security architectural constraints for segregation and those for safety partitioning and independence therefore needs to be considered in an integrated way to find an optimal solution, that minimises downstream risks. However the approaches to architectural design are different: security levels require a zoning approach (BS EN ISO/IEC 62443-3-2:2020, TS CLC/TS 50701: 2021) that is different to the concepts of redundancy associated with SIL assurance.

Effective compliance with the complex task of architectural design can be further hindered by the practical difficulties of meeting the SIL architectural requirement. 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.

Another factor that may hinder a common approach is that 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. It is also the case that 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 (IET, 2020). These issues create a greater opportunity for systematic failures and cyber vulnerabilities to exist and remain undetected, and for the effectiveness of assurance to be undermined, particularly in the absence of a unified approach.

4.1 V&V lifecycle to deliver safe and secure rail assets.

The evidence for mitigating the risk from systematic failures and cyber vulnerabilities is fundamentally the evidence of robust implementation of a clearly defined and formal waterfall development process for verification and validation in accordance with the relevant standard. 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. In summary:

- 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. This creates the possibility for miscommunication, misunderstanding, or loss of documented assurance of safety requirements.
- 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.
- 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.

- The V&V lifecycle approach requires free and open sharing of informational across organisational boundaries as a project to deliver a rail asset progresses. There are practical and cultural conflicts; good safety culture requires the open sharing of safety information to support learning [9][10][11]. However there is typically much more secrecy around security information.

5. The Way Forward: Managing Safety and Cyber Security Risk

It is increasingly difficult to meet these requirements in practice and the reference frameworks are increasingly less fit-for-purpose. The railway industry has to move toward to frameworks where safety and cyber safety are integrated effectively and efficiently. One framework that requires revision is the traditional V&V lifecycle. (Figure 1). The strong safety-focus needs to shift to the integration of cyber risks. This is a significant challenge because safety experts and security experts have very different backgrounds and work from very different frameworks. Perhaps the best 'first step' is not to fundamentally change the legislative frameworks but to bring them forward in the design process. That is to say, rather than creating safety and security cases to prove that train complies with current regulations to Develop a set of overarching safety and security architectural constraints, that recognise the optimal trade-offs between functionality, network connectivity, and high safety integrity, for the variety of rail assets.

Equally, and perhaps even more importantly, the technical design of the hard- and software has to be designed to assure cyber safety and security at the same time. This requires a different design approach of railway equipment. Moving away from a safe design adding cyber security as an add-on, working toward an integrated approach where the system's digital infrastructure is designed with cyber-security measures in situ. Manufacturers are working toward this future but as long as legislative frameworks maintain the traditional V&V life-cycle the incentive to modernize cannot come to full fruition. The authors are involved in several initiatieves to move the field forward in re-engineering the Verification and Validation lifecycle, to minimise the challenges to its practical application set out in this paper..

References

[1] European Union Agency for Cyber Security. (2020). Rail Cybersecurity – Security Measures in the Railway Transport Sector. ENISA. Available: https://www.enisa.europa.eu/publications/railway-cybersecurity

[2] US Federal Aviation Administration (2019): Joint Authorities Technical Review, Boeing 737 Max Flight Control System, October 11th 2019.

[3] Freitas L, Scott W E, Degenaar P, (2020) Medicine-by-wire: Practical considerations on formal techniques for dependable medical systems, Science of Computer Programming, Volume 200

[4] Naor M, Adler N, Pinto GD, Dumanis A (2020) Psychological Safety in Aviation New Product Development Teams: Case Study of 737 MAX Airplane. Sustainability 2020, 12, 8994.

[5] Thomas, J, Davis A, Samuel M P (2020) Integration-In-Totality: The 7th System Safety Principle Based on Systems Thinking in Aerospace Safety. Aerospace 2020, 7, 149.

[6] European Union Agency for Rail (2017) Guideline for the application of harmonised design targets (CSM-DT) for technical systems as defined in EU regulation. ERA-REC-116-2015-GUI, Version 1.1, 18/05/2017

[7] Boehm B (1984). Verifying and Validating Software Requirements and Design Specifications, IEEE Software; Los Alamitos Vol. 1, Iss. 1.

[8] EU (2013). On the Common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009. Report EU No 402/2013.

[9] Kriaa S, Pietre-Cambacedes, L Bouissou M and Halgand Y (2015) A survey of approaches combining safety and security for industrial control systems. Reliability Engineering & System Safety; Volume 139: July 2015: Pages 156-178.

[10] Adjekum D K and Tous M F (2020) Assessing the relationship between organizational management factors and a resilient safety culture in a collegiate aviation program with Safety Management Systems (SMS), Safety Science, Volume 131, 2020.

[11] IET (2020) Institute of Engineering and Technology/National Cyber Security Centre: Code of Practice: Cyber Security and Safety, 2020