SECURITY/SAFETY ASSESSMENT WITH THE STAIRCASE MODEL

C. van Gulijk[1,4]*, G. Bearfield[1,3], and R.J. Thomas[2]

[1] *Institute of Railway Research (IRR), University of Huddersfield, Queensgate HD1 3DH,UK.*

[2] *Centre for Railway Research and Education, University of Birmingham, Edgbaston road B15 2TT, UK.*

[3] *Rock Rail, 91 Waterloo Rd, London SE1 8RT, UK*

[4] *TNO Healthy Living, Schipholweg 77, 2316ZL Leiden, The Netherlands*

*Corresponding address (Email: c.vangulijk@hud.ac.uk, +31-629207659)

ABSTRACT

This work addresses the insidious undermining of safety assurance in the railways by sprawling digital networks. Not only does digitalization undermine traditional safety assurance methods, it also provides points of interaction for adversaries. Security assurance therefore is critical of these new digital systems to ensure that no new safety risk is introduced.

Digitalization transforms the railway undertaking, from services, rolling stock, infrastructure and all components within. In train manufacturing, computers used to be localized and independent control units servicing a specific system (say, doors or brakes). Today trains are equipped with overarching, centralized computer control systems for train control and management (TCMS systems). With such systems it becomes increasingly difficult to demonstrably assure safety critical functions for railway systems. Rolling stock is no exception where many facets are now composed of digital systems of systems.

This work explains the first steps for developing a comprehensive approach for the renewal of safety assurance processes to incorporate cyber-physical systems and the cyber security issues associated with them. This work addresses the security landscape for rolling stock OEMs (Original Equipment Manufacturers) whose role has changed from being the primary designers of trains to digital system integrators.

The emerging, technological challenges challenge the classical V & V lifecycle model for safety and cyber security engineering. This paper discusses a revised assurance lifecycle model, the safety 'STAIRCASE' that encompasses four steps in the development of a safety case: 1) the OUTLINE safety case, 2) the PRELIMINARY safety case, 3) the VALIDATED safety case and the O&M safety case.

Keywords: V&V lifecycle model; Safety case; Cyber security; Safety Assurance; Risk analysis

BACKGROUND

The railway is a high-risk industry. It transports large numbers of people at high speeds and there is an ever present potential for disaster. In order to ensure that railway assets are designed, built and operated safely stringent safety regulations and standards are in place. For Europe safety requirements are set in the railway safety directive 2016/798 (EU 2016a) and the rail system interoperability directive 2016/979 (EU 2016b). They are supported by the Common Safety Method for risk evaluation and assessment 352/2009 (CSM RA; EU 2013). The procedures in these documents require that the responsible party determines that novel systems (regardless whether they are introduced for the first time or whether the are a significant change) require a structured risk management process including evidence and assessment 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 and the relationships are carefully set out in legislation. 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, for example a train operating company must put the system 'in use' and ensure that all necessary safety requirements for its operation and maintenance are met and regulatory approval is obtained.

Effective transfer of risk information, and transparency between the actors is critical to the achievement of 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 (EN50126: 2017).

But traditional working methods are challenged by modern supply chains and the ingress of digital systems. They undermine traditional safety assurance methods. Not only does digitalization undermine traditional safety assurance methods, it also provides new entry points and points of interaction for adversaries. Security assurance therefore is critical of these new digital systems to ensure that no new safety risk is introduced. Some of these challenges are explained in a code of practice produced by the Institute of Engineering and Technology (IET, 2020).

Notwithstanding, the deterioration of railway safety performance is simply unacceptable. Railway safety performance has increased significantly over recent years (European union Agency for Railways, 2020). Based on the significant work on 'societal concern' it is known that the travelling public has a very low tolerance for rail accidents (Hoyland, 2018; Bearfield, 2014; 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.

ASSURING RAILWAY SYSTEMS

The regulatory process includes particular requirements for 'Technical Systems' (European Union Agency for Rail, 2017). 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 most widely used technical standard 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).

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, 1984) describes the approach as it relates to software as follows:

"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."

The process is conceptually clear based 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

- The competence is in place to fully understand and interpret requirements and their validation evidence, across multiple separate teams and organisations.

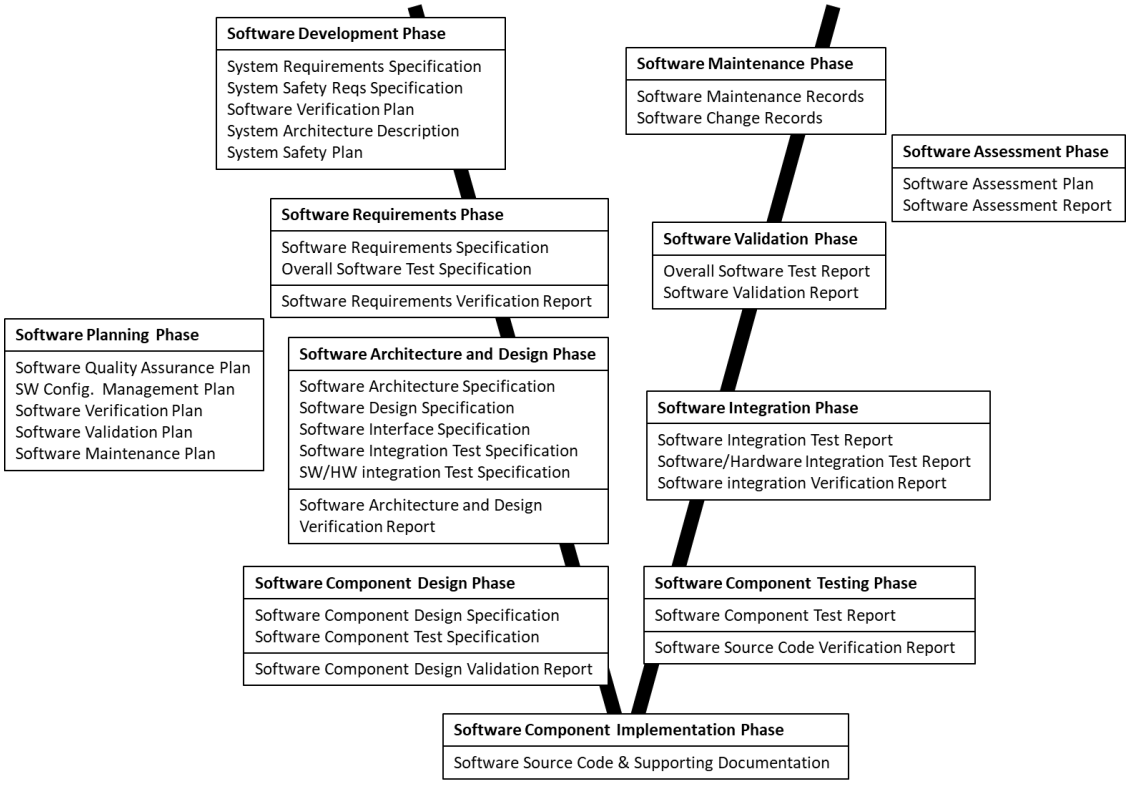

Figure 1: the V model (example for software).

Table 1: Safety Integrity Levels

Safety Integrity Level	**Av. failure freq. safety function**
SIL4	$\geq 10^{-9}$ *to* $< 10^{-8}$ $[h^{-1}]$
SIL3	$\geq 10^{-8}$ *to* $< 10^{-7}$ $[h^{-1}]$
SIL2	$\geq 10^{-7}$ *to* $< 10^{-6}$ $[h^{-1}]$
SIL1	$\geq 10^{-6}$ *to* $< 10^{-5}$ $[h^{-1}]$
(Table from IEC61508 part 1, page 34.)	

ASSURING SAFETY FUNCTIONS

IEC61508 and EN50128 are clear about safety functions for railway systems (see table 1). There are four safety targets or SILs (Systematic Safety Integrity Level) where SIL4 is the highest. This level demands that an average failure frequency is once in between 10^8 and 10^9 hours of operation, when safety functions are operating continuously.

For systematic software failures, SILs cannot be accurately predicted. As an alternative specific software design measures and approaches are prescribed for attaining SIL levels. These can be organisational structures, software development approaches, quality and management processes, validation and verification techniques and requirements, and failure analysis approaches. A specific aspect is the design of an appropriate system architecture. For a train that means the TCMS system which, in many ways, is a train-borne computer system that collects and processes data-streams from components and parts. The number of components can easily be in the dozens but that is rapidly increasing to hundreds. The train even produces data streams that are not directly used in the TCMS systems but are proprietary for sub-system or component manufacturers which are developed by supply-chain partners that use their own verification and validation approaches. AI aggravates the software safety verification because the software changes on its own accord.

Then, the distributed design of sub-systems, and specially the software design of such systems, does not necessarily consider the whole asset. This creates the possibility for miscommunication or misunderstanding of safety requirements. Also, the approach of certifying to a SIL level at the sub-system level potentially ignores common-mode failures and other equipment on the train. As 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.

Together, these issues create a greater opportunity for systematic failures which may remain undetected using traditional verification methods. These issues have been recognised, including by researchers considering how to develop ‘agile’ software approaches to this topic (Islam and Storer, 2020).

ASSURING SOFTWARE FUNCTIONS

With modern manufacturing methods and sub-systems that come with their proprietary data streams. there are a number of potential weaknesses in the application of the functional safety standards described here and their associated SIL requirements.

First, software development is very different from traditional clearly defined and formal waterfall development process in the railways. The basic assumption that hazards are identified at the concept design phase and remain stable is incorrect. Advanced software systems in the TCMS or embedded in software may require software upgrades (patches) on a monthly basis. And when AI is used, the behaviour of the train may change even faster. An idealised waterfall model cannot be applied in such a principled and chronological way.

Second, looking at rolling stock, much of the generic functionality of the system is developed as part of a 'train platform' design. The platform will form the core basis of a wide range of different applications each with its own operational use case. The actual hazards in use will be determined by each use case so it is therefore not practically possible to completely define all necessary safety requirements at the outset.

And third, an tested method for achieving high SIL levels is to design alternative systems: two completely independent systems provide the same function to increase reliability of the function. One sub-system perhaps designing an electro-mechanical device to deliver the function, the second designing a purely mechanical one. But when it comes to developing software functions it is much more difficult to arrive at fundamentally different solutions. Not only does software share similar hardware configurations, but development teams usually have the same skills and use similar design methods.

These propositions are not as far-fetched as they seem. The difficulties highlighted above have been raised in other sectors (Freitas et al, 2020; Naor et al, 2020; Thomas et al, 2020) The US Federal Aviation Administration (2019) which investigated the Boeing 737 Max aeroplane crashes in Indonesia and Ethiopia in 2018 and 2019 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."

SOFTWARE VULNERABILITIES

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. 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, and therefore many of the challenges set out here are relevant to cyber assurance as well.

Integrating safety and security concerns 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. Also, good *safety* culture requires the open sharing of safety information to support learning (Kriaa et al, 2015; Adjekum and Tous et al, 2020; IET, 2020) but security demands secrecy. On top of that,

cyber security risks change quickly so systems require continual updates. And finally, risks are being deliberately created by 'threat actors' which is where traditional safety engineering and reliability methods fail.

STAIRCASE MODEL

A new model is proposed which creates the environment to have meaningful and productive engagement on the emerging risks and design challenges: the 'safety stair-case' presented in figure 2.

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 model assumes that these stages are formalised as assurance stage gates in some way depending on the specific prevailing commercial and legal requirements. The bold downward lines indicate the source of fixed safety requirements for each safety case. The upwards arrows indicate the source of downstream requirements and assumptions that need to be checked against the prevailing fixed requirements. In the spirit of 'safety and security by design' these safety cases are planned for early production and review to minimise project risk associated with late identification of hazards and vulnerabilities. The key change proposed is to shift consideration of the safety case to the pre-contract stage.

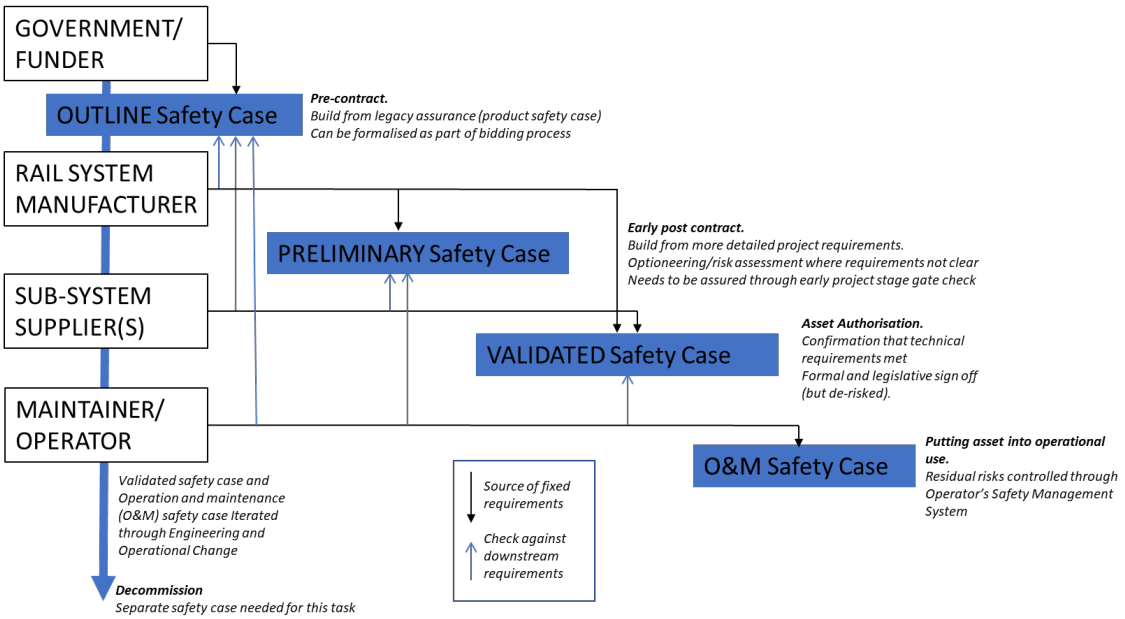

Figure 2: the safety STAIRCASE.

Outline Safety Case

Many solutions are agreed and formalised as part of a project tendering process. The first significant evaluation of safety should therefore be a part of the tender process, and a basis on which the contract is selected. An OUTLINE safety case is therefore needed prior to a contract being set, and should be provided by all bidders as part of the tendering process. 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. Key focus should be on ensuring that the scope of the safety case is clear and complete.

Review of core platform safety case documentation at this stage would ensure clarity about the architecture of the train and the chance to evaluate it early on. It creates a commercial incentive to enhance safety and security by design and address the emerging risks. A critical check is that SIL allocations are clear. Perhaps the most significant change to address is that teams evaluating bids would need the technical competence available to evaluate such safety information early that early stage. It would be very helpful if some formal stage-gate or regulatory oversight were created but strictly speaking, it is not required.

Preliminary Safety Case

Front loading of the safety case work allows the production of a really robust PRELIMINARY safety case early in the project. This means the project can focus on identifying any location specific changes or adaptations that might have been missed in more detail. It also allows early engagement with the future user/operator on operational risks and controls. It allows really clear safety requirements to be cascaded into the tier 1 and tier 2 supply chain, enhancing compliance with safety requirements, project delivery and assurance.

Validated Safety Case

Adhering to current legislative requirements, the VALIDATED safety case should be a relatively defined and simple process. It should be about gathering the necessary information to evidence the safety argument and provide assurance that all is in place and offering it to the regulator with confidence. Often on projects safety is ultimately left to this stage, which may cause serious ramifications for the design of a train when something is amiss. As this is where the key regulatory stage gate occurs, it is also the place suppliers want to de-risk as much as possible. The STAIRCASE 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 phase. The approach also has the potential to reduce project delay risk, by minimising the need for last minute design changes to meet safety requirements or compromises in the safety argument and risk control.

O&M Safety Case

With the VALIDATED safety case in place, stakeholders design their management systems to ensure safe and efficient operation in an O&M safety case. The responsibilities, tasks, controls and residual risks require adequate addressing to achieve operational excellence. Following the STAIRCASE model it is possible that rapidly changing risks require novel procedures for cybersecurity or software patches.

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 this was a significant failing. The line was equipped with a pilot installation of the European Rail Traffic Management System (ERTMS), a form of railway signalling, in 2011. The ERTMS system to transmit 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 GEST system) wrongly showed these restrictions as being applied correctly. The UK (Rail Accident Investigation Branch, 2017) 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.

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 GST sub-system to understand how the system operate. The STAIRCASE methodology would have required that original design work and safety argument to be readily available in the OUTLINE safety case.

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 STAIRCASE would have required that this documentation was reviewed and assessed in the preliminary safety case.

The vulnerability of the system 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.

In summary, it is highly likely that the failure mode would have been prevented by robust application of the STAIRCASE methodology using competent people. More generally, it would have created earlier and more rigorous focus on the core safety.

CONCLUSION

The emerging, technological challenges challenge the classical V & V lifecycle model for safety and cyber security engineering. This paper discusses a revised assurance lifecycle model, the safety ‘STAIRCASE’ that encompasses four steps in the development of a safety case: 1) the OUTLINE safety case, 2) the PRELIMINARY safety case, 3) the VALIDATED safety case and the O&M safety case. The authors believe that the approach forces manufacturers and other stakeholders to think more carefully about safety and (cyber) security and is better equipped to deal with complex data systems and rapidly changing software. The approach does not brutalize current assurance methods as the validated safety case remains. It could be beneficial if some form of regulatory oversight could be added but strictly, that is not necessary.

REFERENCES

- 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.
- Bearfield G (2014), Taking safe decisions and the CSM on risk evaluation and assessment. *IET Seminar Digest*.
- Boehm B (1984). Verifying and Validating Software Requirements and Design Specifications, *IEEE Software; Los Alamitos Vol. 1*, Iss. 1.
- BS EN ISO/IEC 27001:2017 (2017) Information technology. Security techniques. Information security management systems requirements.
- BS EN IEC 62443-3-2:2020 (2020) Security for industrial automation and control systems. Security risk assessment for system design.
- EN50126: 2017 (2017) Railway Applications-The Specification and Demonstration of Reliability. Availability, Maintainability and Safety (RAMS)
- EU (2016). Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety.
- EU (2016). Directive (EU) 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).
- EU (2013). On the Common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009. Report EU No 402/2013.
- 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
- European Union Agency for Railways (2020), Report on Railway Safety and Interoperability in the EU.
  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
- Høyland S (2018) Exploring and modeling the societal safety and societal security concepts – A systematic review, empirical study and key implications *Safety Science* Volume 110, Part C, December 2018, Pages 7-22
- IEC 61508-1: 2010 (2010) Functional Safety of Electrical/ Electronic/Programmable Electronic Safety-Related Systems.
- IEC 61375-2-6:2018 Electronic railway equipment - Train communication network (TCN) - Part 2-6: On-board to ground communication.
- IET (2020) Institute of Engineering and Technology/National Cyber Security Centre: Code of Practice: Cyber Security and Safety, 2020
- Islam G and Storer T (2020) A case study of agile software development for safety-Critical systems projects, *Reliability Engineering & System Safety, Volume 200, 2020.*
- 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.
- 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.

- Rail Accident Investigation Branch (2019) Loss of safety-critical data on the Cambrian Coast line, 20th October 2017, Report 17/2019 Published December 2019.
- 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.
- TS CLC/TS 50701:2021 (2021) Railway Applications - Cyber Security.
- US Federal Aviation Administration (2019): Joint Authorities Technical Review, Boeing 737 Max Flight Control System, October 11th 2019.
- Van Gulijk C, Hughes P, Figueres M, El-Rashidy R & Bearfield G (2018) The case for IT transformation and big data for safety risk management on the GB railways, Proc. IME Part O: Journal of Risk and Reliability Volume 232, Issue 2, Pages 151-163.