World Academy of Science, Engineering and Technology
International Journal of Industrial and Systems Engineering
Vol:16, No:11, 2022

Case Study Analysis of 2017 European Railway Traffic Management Incident: The Application of System for Investigation of Railway Interfaces Methodology

Sanjeev Kumar Appicharla

Abstract**—**This paper presents the results of the modelling and analysis of the European Railway Traffic Management (ERTMS) safety critical incident to raise awareness of biases in systems engineering process on the Cambrian Railway in the UK using the RAIB 17/2019 as a primary input. The RAIB, the UK independent accident investigator, published the Report- RAIB 17/2019 giving the details of their investigation of the focal event in the form of immediate cause, causal factors and underlying factors and recommendations to prevent a repeat of the safety-critical incident on the Cambrian Line. The Systems for Investigation of Railway Interfaces (SIRI) is the Methodology used to model and analyse the safety-critical incident. The SIRI Methodology uses the Swiss Cheese Model to model the incident and identify latent failure conditions (potentially less than adequate conditions) by means of the Management Oversight and Risk Tree technique. The benefits of the SIRI Methodology are threefold: first is that it incorporates "Heuristics and Biases" approach, in the Management Oversight and Risk Tree technique to identify systematic errors. Civil engineering and programme management railway professionals are aware of role "optimism bias" plays in programme cost overruns and are aware of bow tie (fault and event tree) model-based safety risk modelling technique. However, the role of systematic errors due to "Heuristics and Biases" is not appreciated as yet. This overcomes the problems of omission of human and organisational factors from accident analysis. Second, the scope of the investigation includes all levels of the socio-technical system, including government, regulatory, railway safety bodies, duty holders, signalling firms and transport planners, and front-line staff such that lessons learned at the decision making and implementation level as well. Third, the author's past accident case studies are supplemented with research pieces of evidence drawn from the practitioner's and academic researchers' publications as well. This is to discuss the role of system thinking to improve the decision making and risk management processes and practices in the IEC 15288 Systems Engineering standard, and in the industrial context such as the GB railways and Artificial Intelligence (AI) contexts as well.

Keywords**—**Accident analysis, AI algorithm internal audit, bounded rationality, Byzantine failures, heuristics and biases approach.

I. Introduction

IN this section, we examine the summary information relevant to the safety critical incident stated in the RAIB 17/2019 document [1]. The Rail Accident Investigation Branch (RAIB) claims in the preface of its Report 17/2019 that its investigation is to improve railway safety by preventing future railway accidents or by mitigating their consequences [1]. They noted that the RAIB's findings are based on its own evaluation of the evidence that was available at the time of the investigation to them. Further, the author notes that the RAIB observations of evidences led them to findings and these were intended to explain what happened, and why, in a fair and unbiased manner [1].

In the Summary of the RAIB Report, it is stated, "During the morning of Friday 20 October 2017, a train driver travelling on the Cambrian Coast line in North Wales reported a fault with the information provided on his in-cab display. As signalling staff at the control centre in Machynlleth investigated this report, they became aware that 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" (Clause 4) [1].

The RAIB (2019) Report stated, "In 2011, the Cambrian lines were equipped with a pilot installation of the European Rail Traffic Management System (ERTMS), a form of railway signalling. The ERTMS system provided on the Cambrian lines removed the need for signals along the track by transmitting signalling and control data directly to the train. This transmitted data is used to enforce the permitted speed and display both movement authority (Permission to travel along a specified part of the railway), the incident and other information, including temporary and permanent speed restrictions, on a screen in front of the driver safely" (Clause 5) [1]. However, the RAIB (2019) Report stated that: "Subsequent investigation, by the local maintenance staff, found that the signalling system stopped transmitting temporary speed restriction data after it had experienced a shutdown and restart at around 23:10 hrs the previous evening. The signallers had no indication of an abnormal condition and the display at the signalling control centre wrongly showed these restrictions as being applied correctly safely" (Clause 6) [1].

The RAIB Report (2019) on the re-use of certified signalling equipment, thus: "The ERTMS signalling implemented on the Cambrian lines, although new to Network Rail infrastructure,

Sanjeev Kumar Appicharla is with Institution of Engineering and Technology (IET), UK (e-mail: appicharlak@yahoo.co.uk).

was based on equipment already in operation elsewhere in Europe. Implementation in the United Kingdom (UK) was partly reliant on product validations already achieved in Europe, with the differences required for the Cambrian lines being subject to a full approval process in accordance with UK procedures safely" (Clause 19) [1].

The RAIB (2019) stated, "A temporary speed restriction is applied when a short-term reduction is required to the maximum permitted line speed at a specified location. Temporary speed restrictions are marked by trackside signs in areas with traditional trackside signalling. For in-cab signalling areas, such as the Cambrian lines, trackside signs are not provided because the temporary speed restrictions should be included in the permitted speed provided to the driver by the DMI. In both types of area, the railway Rule Book (RSSB document GE/RT80003) requires train drivers to make themselves aware of temporary speed restrictions in the weekly operating notices issued to them" (Clause 19) [1].

The rest of the paper is structured as follows: Section II introduces the brief history of development for the ERTM System development and its application and related safety regulations in the UK. The periods are (1) 1758 -till 1986 -1995. (2) 1996-2002; (3) 2003-2007; (4) 2006-2020; and, (5) 2020-2021. The summary of the RAIB conclusions of their investigation is presented and the requirements of the Safety Management System are presented as well. Section III presents the application of the methodology to case study review. Section IV presents the results. Section V provides the conclusions on the lessons learnt.

II. The Very Brief History of Development to the ERTMS/ETCS Technology

Stanley Hall (1990) documents the history of Her Majesty Railway Inspectorate (HMRI) in its 150 years of existence till 1990. In the same year, Prof. James Reason published his seminal work entitled, "Human Error" and the "Swiss Cheese Model" [2], [3]. Reason et al. stated, "All complex systems contain such potentially multi-causal conditions, but only rarely do they arise thereby creating a possible trajectory for an accident. Often these vulnerabilities are "latent", i.e., present in the organisation long before a specific incident is triggered. Furthermore, most of them are a product of the organisation itself, as a result of its design (e.g., staffing, training policy, communication patterns, hierarchical relationship,) or as a result of managerial decisions" [3], [4, p.2].

The brief background to The European Rail Traffic Management System (ERTMS) is provided by Lochman and the history is detailed at a length in a M.Sc. Thesis by Simon Paye, which is made freely available on the Web. These texts may be consulted for learning greater details of how chaotic design and development efforts coalesced into a cohesive effort [5], [6]. Paye (2010) noted that previous studies (see [5]) have shown that most of the interests and endeavours are geared to a particular subset of railways: the signalling subsystem [6]. With its countless installations and rules that inform train drivers and command line switches, the signalling subsystem is undoubtedly the most fragmented element in the European railway area: there are more than twenty different signalling systems (DG-TREN, 2005:2). This important diversity of signalling subsystems is the major obstacle to the interconnection of the national networks. Being aware of that, the Commission launched in the late 1980s an ambitious industrial project, called ERTMS (European Rail Traffic Management System) with the objective to replace the manifold national signalling systems by a single, European system effort [5], [6]. The functional aim of the European Rail Traffic Management projects was to enhance cross-border interoperability and signalling procurement by creating a single Europe-wide standard for railway signalling through Directives and "High level standardisation" with a top-down approach. The structure of the programme is detailed in a brief manner [5], [6]. The Structure of the EU Rail Traffic Management programme contains three basic elements as follows (Chapters 2, 3, 4, 5, 6) [5]:

1. Traffic Management Layer, Europtirails: The operation management level comprising of functions and means necessary for reliable and safe running of trains on the railway infrastructure. The main functions are monitoring, tracking, and tracing cross-border trains for ensuring transparency on corridors, optimising the disposition of trains and the logistical chain for reducing the delays on international trains; optimising capacity offer in perturbed scenarios. Passenger information services and train location information perform ace regime. For greater details see the chapters cited.
2. GSM-R (Global System for Mobiles - Railway): The communication system for exchanging safety relevant data between infrastructure and trains. The public standard – "Global System for Mobiles" was adapted for the railways needs. For greater details see the chapters cited.
3. ETCS (European Train Control System): The signalling element of the system which forms the interface between the infrastructure and trains. The signalling system is supposed to optimise performance close to the limits of dictated by physics of guided system. Towards this end, it uses telematic technology which allows for train warning, train protection and train control functions.

III. Application of SIRI Methodology

The most effective way of managing safety, according to the Management Oversight & Risk Tree (MORT) philosophy, is to make it an integral part of business management and operational control [7]. This philosophy finds support from a key insight from systems engineering perspective. RSSB Research Report T169 comments in the section on systems engineering, thus, "systems thinking predicts that individuals will not change their mode of thinking or operating within the world until their existing modes are proved beyond doubt, through direct experience, to be failing". This is an independent conclusion arrived in the RSSB Research Report in 2004 (Section 4.3.3.1.1) [8].

Another point to bear in mind when performing MORT analysis is that the order in which evaluation is carried out is important. For example, simple mathematical expression 2+3x5

when evaluated might give rise to different results of 25 or 17 depending upon the punctuation carried out. For example, if the expression is punctuated thus, (2+3) x 5 the result denotes 25 or 17 when the expression is punctuated as 2+(3x5). This example is motivated by a simpler example in [9, p.350]. "Ambiguity" bias is an example in the problem-solving context can be generalised from this example [9], [10].

Let us consider the problem of multiplications. Let us multiply 113 by 9. This can be carried out in an intuitive manner. But to multiply CXIII by IX in the old Roman numerals we find it far more cumbersome [9, p.343]. Though, we know the answer, anchored by this number, we cannot still carry out computation without the aid of a device such as an Abacus (see foot-note 2) [9, p.343]. The advantage of the Indo-Arabic numerals as a full adequate symbolic language enables us to manipulate statements and arguments more efficiently and more easily than before [9, p.343]. The addition of the numeral 'zero' to include in as an actual number in the list of natural numbers and role of natural numbers is clear and unambiguous. The mathematical operations using the natural numbers are independent of the nature of the geometry of the world. This discovery is traced back to the Hindu mathematicians of India, starting with Brahma Gupta in 7th century followed up by Mahavira and Bhaskara in the 9th and 12th century respectively is learnt from the work of Nobel laureate, Prof. Sir Roger Penrose. The insight that the mathematical operations using the natural numbers are independent of the nature of the geometry of the world is learnt as well [11, p.63].

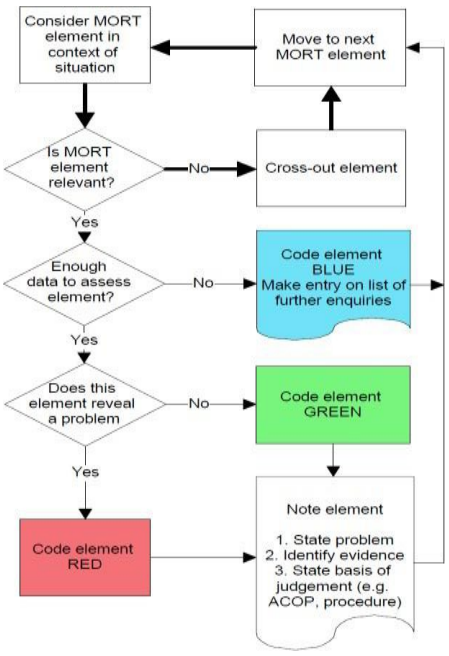

Fig. 1 MORT Flow chart [12]

Reasoning about what was lacking in S branch need to be evaluated first and then M branches in the MORT logic tree should be evaluated later. This order is essential as the consequences of the fatal accidents are not reversible. Further, the calculus of probabilities, which has an impact on safety critical decision making such as calculating mean time between failures of systems, must be kept in mind. The topic of calculus of probabilities is discussed in detail by Poincare (pp.183-210) [7]. Appicharla's limited search on the internet for past application of MORT to the UK railways produced two documents. One is an accident handbook produced by Chris Johnson. Second, a British Railway Board (BRB) document bearing number GH/ZC0002 dated Nov 93 Revision A hosted by RSSB. The author has already referenced Chris Johnson's work in his earlier work published in 2006 which is cited by Appicharla [18]. The BRB document lists various terms used in connection safety terminology which mentions MORT technique. However, no application of the MORT method by the BRB is known to the author. A formal approach to system safety engineering in 1993 did get initiated by the BRB, but on privatisation, the effort seems to have been overtaken by the turn of events [7].

Originally, MORT was used as an accident investigation method. It combines the technical, managerial and human factors aspects into a single analysis method and serves as an aid to discover errors before operations and can be applied in three steps as follows [12].

THE ANALYST SEEKS TO DEFINE THE EVENT TO BE ANALYSED IN TERMS OF TARGETS AND BARRIERS AND CONTROLS. THIS STEP IS SUPPORTED BY A PROCEDURE CALLED ENERGY TRACE AND BARRIER ANALYSIS (ETBA). THE FORMAT FOR RECORDING THE RESULTS OF ETBA ANALYSIS IS SHOWN IN

Step1. TABLE I. The necessary information on how to perform this procedure is given in the user manual [12]. The author has filled the table using the information given in the ORR Guide document (see [13]) and the RAIB Report (see [1]).

Step2. The MORT analyst looks at how the energy exchange took place producing injuries.

Step3. The MORT analyst evaluates the hypothesis that unwanted energy flow was the result of how the activity was managed by local as well as upstream management. Here, the MORT question set and pre-defined logic tree helps the analyst to inquire and reflect upon the events in the accident sequence.

S/M Oversights and Omissions: SA1: The RAIB Report [1] noted, in the Summary, thus: "On the morning of 20 October 2017, four trains travelled over the Cambrian Coast line, Gwynedd, while temporary speed restriction data was not being sent to the trains by the signalling system. No accident resulted but a train approached a level crossing at 80 km/h (50 mph), significantly exceeding the temporary speed restriction of 30 km/h (19 mph) needed to give adequate warning time for level crossing users. The line has been operated since 2011 using a pilot installation of the European Rail Traffic Management System (ERTMS) which replaces traditional lineside signals and signs with movement authorities transmitted to trains. These movement authorities include maximum permitted speeds which are displayed to the train driver and used for automatic supervision of train speed" [1].

TABLE I
ETBA FOR THE CAMBRIAN LOSS OF SAFETY DATA INCIDENT [1], [7], [13], [14]

SB1: Harmful energy flow or Adverse agent or environmental condition	SB2: Target: Vulnerable person or thing	SB3: Barriers & Controls to Separate energy and target
Kinetic hazard, ERTMS train moving into crossing space in excess of the permitted speed	Level crossing users, vehicles and animals	Less Than Adequate (LTA) ALARP Principle LTA ROGS Regulation (2006) and ERA regulations (2004) LTA Railway Group Standards LTA CENELEC Standards LTA Change Management LTA System definition LTA Risk Management LTA RU/IM Safety Management System LTA Swiss Cheese Model application LTA Risk Assessment LTA Risk Assessment Review LTA System Assurance Management LTA Competence Management LTA Learning lessons from past failures

A. MORT Code SB3. Barriers and Controls LTA

As per the MORT User Manual, this MORT branch considers whether adequate barriers and controls were in place to prevent vulnerable persons and objects from being exposed to harmful energy flows and/or environmental conditions [12].

Barriers are purely protective. They need to be designed to fit the characteristics of the energy flows involved and the targets that could be exposed. Examples include machinery guards, Personal Protection Equipment (PPE), firewalls, blast walls and pipe-work integrity. Controls are "controls of work and process" which may also serve to offer protection [12]. Examples include safe operating procedures, toolbox talks, permits to work and isolations. As per the Swiss Cheese Model application (2006) to the UBERLINGEN Accident Analysis, ICAO and other levels of socio-technical system can be invoked in the analysis [4]. However, a ERTMS Study (2018) found in the Netherlands that the ERTMS Architecture is not so well understood and makes it difficult to understand find a root cause for each hazard (see [15]). Further, barrier analysis is to include the human and organisational factors as well [16]-[18].

1) SC1. Control of Work and Process LTA

This branch considers the adequacy of the control system for the work activity or process in question [12]. Six aspects of the control system are considered:

- Technical information systems [SD1]
- Verification of operational readiness [SD2]
- Inspection [SD3]
- Maintenance [SD4]
- Supervision [SD5]
- Supervision support [SD6]

a) SD1 Technical Information Systems LTA

This branch is about the adequacy of the information system designed to support the work/process in question. This is considered in three ways:

- Providing information about the technology, activities and materials deployed; examples – Toolbox talks, formal operator routines, task work pack containing necessary information on codes, standards and safety critical issues.
- The monitoring systems that measure the behaviour and efficiency of the "work flow process";
- Actions triggered by the results of the monitoring process (e.g., triggering of Risk analysis).

(1) a1. Technical Information LTA

(a) b1. Knowledge LTA

(i) d1. application of Codes and Manuals

- Were the work/process and related issues adequately addressed by codes and manuals; and,
- Did individuals making decisions adequately apply the knowledge from codes and manuals?

The RAIB Report 17/2019 stated in the clause 118, thus "these shortcomings should have been recognised within the client role required by the EN501xx series of European standards current during the Cambrian ERTMS development (paragraph 37). This is supported by RSSB guidance note GEGN8650, which provides assistance for clients procuring high integrity software. Although published in March 2017, the interpretation of client responsibilities is based on parts of the EN501xx series which were unaltered from the version applicable during the Cambrian ERTMS development" (Clause 118) [1].

The SCM/MORT Analyst observation #1 on the adequacy of individuals making decisions adequately apply the knowledge from codes and manuals, is this : "The evidence from ERTMS signalling safety expert that the safety standards like the CENELEC 50129 failed to provide a proper foundation for risk analysis is noted in the ERTMS literature published by the UIC, a major stakeholding organisation and clients like DB, Network Rail and SNCF took over the responsibility to specify the safety goal and target to the signalling suppliers (pp.204-205)" [19]. Thus, the UNISIG document 091 (2015), (a mandatory specification) and its earlier versions since 2001 took account the role of temporary speed restriction and passed on the responsibility of track side engineering issues to the national implementation team. Therefore, despite the less than adequate safety standard, CENELEC 50129, the authors of the UNISIG document 091 were clear about the risk contributors and specified the tolerable hazard requirement in the Clause 9.4, thus, "The complete ETCS Trackside System Deployment process is not part of ETCS, but shall be of a quality that is appropriate to the required safety level. See further paragraph 4.6.1.1". (Background information is provided by Subset-088 Part 3, paragraph 12.6.4.1) [20].

Clause 4.6.1.1. of the UNISIG document 091 (2015), (a mandatory specification), reads, thus: "the safety performance of the system where ETCS is applied is crucially dependent not only upon the performance of ETCS itself, but also upon the quality of data from sources external to ETCS, transferred to

ETCS. Therefore, requirements are placed on the corresponding processes where necessary. These requirements demand that the process being adopted shall be of a quality level that is appropriate to the required safety level". This should be interpreted to mean that [20]:

- the criticality of the data needs to be determined from an overall railway system safety perspective.
- the process in question must be examined in detail to identify where there are potential threats to the accuracy of the process and measures are put in place to minimise these threats to the required safety level, taking into account the functional properties of ETCS and the safety integrity requirements specified in the present document.

The SCM/MORT Analyst observation #2 on the Safety Requirements for the Trackside Subsystem" are less than adequate. The evidence for the claim is the Clause 12.6.4 of the Subset 088, Part 3(2019), and it reads thus: "Integrity Requirements for the ETCS Trackside System Deployment for the Trackside Subsystem". Clause 12.6.4.1 of the Sub set 088, Part 3(2019), reads thus: The hazard rate for the trackside system visited by a train in the reference mission, less those items forming the non-trusted parts of the transmission system, must be shown not to exceed THRtrackside = 0.67 * 10^{-9} dangerous failures per hour (clause 9.4) [20].

"Where the dangerous failure is defined as: Failure to provide information to the on-board supervision in accordance with the data advised to the trackside from external entities" [20].

Note: External entities include the assumption that the on-board provides correct information to the RBC in level 2. If this is not the case, it shall be considered as part of the on-board hazard detailed in 12.3.1.2 [20].

RAIB Clause 104 reads thus "The Cambrian version of "G 'poste de GEstion des Signalisations Temporaires' (GEST is based on the product produced for the LGVEE project. The LGVEE product meets safety requirements and achieves the required SIL 2 integrity level. This safety report demonstrates that the modifications to the LGVEE product maintain the safety integrity level of the products, and that the appropriate safety analyses have identified the safety requirements on the operating environment necessary to maintain the safety of the GEST in generic Network Rail applications to an acceptable level. The Trackside ERTMS and Signalling System Safety Case demonstrate that the overall specific application design and configuration for Cambrian is safe, that the defined data preparation processes have been followed, that adequate testing has been carried out, and that the safety requirements have been met" [1].

RAIB Clause 71 reads thus: "The CCS-TSI refers to technical documents prepared by a European rail industry working group (UNISIG) which contain detailed technical requirements for ERTMS systems" [1].

The safety requirements for ETCS level 2, as applied on the Cambrian scheme, were set out in UNISIG SUBSET-091 version 2.2.11, dated 10 August 2005, and included:

- 4.2.1.6 'The role of ETCS ... [is] to provide the Driver with information to allow him to drive the train safely and to enforce respect of this information.'
- 4.2.1.8 'The Core Hazard for the reference architecture is defined as exceedance of the safe speed/distance as advised to ETCS'.
- 4.2.1.9 'The maximum allowed rate of occurrence for the core hazard ... [is] 2.0*10^{-9}/hour/train. This is the maximum Tolerable Hazard Rate (THR) for ETCS, denoted as THRETCS'.
- 8.1.1.1 'The safety integrity level will be derived from the different tolerable hazard rates. For Hazard Rates of <10^{-9} dangerous failures per hour, a SIL 4 process will be applicable'.
- 8.1.1.3 'The dangerous failure for the ETCS trackside equipment is defined as failure to provide information to the ETCS onboard supervision in accordance with the data advised to the ETCS trackside from external entities.
- 9.2 'The collection, interpretation, accuracy and allocation of data relating to the railway network shall be undertaken to a quality level commensurate with the SIL 4 allocation to the ETCS equipment'.

RAIB notes, "Taken together, these requirements mean that the ETCS should prevent a train from travelling at more than the permitted speed with a safety integrity level of SIL4. UNISIG SUBSET-091 does not include an exemption for temporary speed restrictions" (Clause 71) [1].

The SCM/MORT Analyst observation on the "GEST 2" is that as per the apportioned figure of THR, the failure rate of the THR trackside works out to one failure per 100,000 hours per annum. Or a trackside sub-system failure should be seen once in 100,000 years. This corresponds to SIL-0 level rather SIL-2 level. As per SIL-2 level, a failure is to be seen once in a million years [21].

Based upon the above observation of last paragraph, SCM/MORT Analyst observation #3 is that the Knowledge of UNISIG and RAIB experts of the IEC 61508 standard is answered LTA.

(b) d2. List of Experts LTA

Based upon the evidence of UNISIG sub-set 091 and 088, and RAIB clauses cited above, the SCM/MORT Analyst observation #4 is that the question is set to LTA [20].

(i) d3. Local Knowledge LTA

Based upon the evidence of failure node at knowledge-based behaviour level of human performance (see Clause 6.3, [3]), omission of the track side fault tree contribution to the overall fault tree analysis is an instance of "Out of sight out of mind" bias [3]. And this is not in compliance with the Office of Rail and Road Regulator (ORR) Guidance on Safety Management System (SMS) requirements for risk assessment process (see Clause 4.8, [13], (pp.204-205) [19]. Readers may have to consult the Chapter 2 and Chapter 3 of the Prof. James Reason's work (1990) to learn how the "Heuristics and Biases" approach was developed to identify failures at various levels of Jens Rasmussen's performance levels [3].

Based upon the evidence, the SCM/MORT Analyst observation #5 as an answer to the question is set to LTA.

(ii) d4. Solution Research LTA

Based upon the evidence of Jens Braband (2009) (cited in section 8.1.3, [19]) and analysis carried out in the UNISIG subset 091 (2015) and 088 (2019) (see [19]) documents, the top-down decomposition of safety integrity targets did not understand the pitfalls of task performance errors and how they may induce errors into staff performance at the local sites (for example, signallers and the train drivers in this case). Further the concept of "Bounded rationality" assumed by Nobel prize winning cognitive psychologists due to which limited information processing is found in real world rather than omniscient rationality assumed by the economists leads to the conclusion that solution search will be limited rather exhaustive search to solutions to the problems faced [3], [10]. Please refer to the MORT Fault tree branch SD5, f6 node to learn more about this observation. Thus, it is clear that SCM/MORT Analyst observation #6 is that the question is set to LTA.

b) SD2 Operational Readiness Review

This branch considers the adequacy of efforts to ensure that work/process or site was ready to be used or occupied. If operational readiness was not assured, control of the work/ process may have been inadequate. We consider readiness in terms of: plant/hardware; procedures/management controls; personnel, and software (added to the MORT question set):

a1. Verification of Operational Readiness LTA

This branch considers whether verification of the operational readiness of the facility and work process was adequate.

RAIB Clause 79 reads thus: "The vulnerability of the system to a single point of failure had neither been detected nor corrected during the design, approval and testing phases of the Cambrian ERTMS project" [1].

b1. Did not Specify Check

- Was an operational readiness check specified for this work/ process?
- Would an adequate operational readiness check have identified the problem in question?

RAIB Clause 80 reads thus: "taken together, the factors described in paragraphs 46 to 78 resulted in a system which was intended to have a high level of safety integrity, but did not achieve this following the rollover of the Radio Block Centre (RBC)" [1]. These shortcomings had neither been detected nor corrected during the design, approval and testing phases of the Cambrian ERTMS project due to a combination of the following:

a. the safety related software requirements for the GEST software were insufficiently defined (paragraph 81);
b. the hazard analysis process did not identify, and so failed to mitigate against, the GEST software thread failure mode (paragraph 88);
c. the validation process did not ensure that the safety requirement for the correct display of temporary speed restrictions was met (paragraph 94); and,
d. GEST was accepted into service without the production of a generic product safety case (or equivalent); had such a process been followed rigorously, it would probably have exposed the shortcomings in the software design (paragraph 99), (Clause 80) [1].

b2. Readiness Criteria LTA

RAIB Clause C26 reads thus: "While attempting to identify the reasons for the loss of temporary speed restrictions from the RBC on 20 October 2017, a sequence of testing was improvised by the Network Rail signalling technician and AnsaldoSTS maintenance support engineer, as maintenance documentation gave no guidance on this topic. Their testing sequence was intended to identify the location of the fault causing the loss of temporary speed restrictions. The sequence followed is shown in Table C1" [1].

The SCM/MORT Analyst observation #7 is that the client technician and supplier maintenance support engineer, created a procedural specification to re-create the fault and generate a solution to the safety problem and this was in fact overlooked by the Ansaldo STS design team and the safety team did not specify the readiness criteria for the GEST software during the design and development stage. Thus, the question is set to LTA.

- b3. Verification Procedure LTA
- b4. Competence LTA
- b5. Follow-up LTA
- a2. Technical Support LTA:
- a3. Interface between Operations and Maintenance or Testing Activities LTA:
- SD3. Inspection LTA
- SD4. Maintenance LTA
- a1. Planning Process LTA:
- b1. Specification of Plan LTA:
- c1. Maintainability (Inspectability) LTA:
- c2. Completeness of the Plan LTA
- c3. Co-ordination LTA
- c4. Competence LTA
- c5. Analysis of Failure LTA

RAIB Clause 27 reads thus: On 20 October 2017, the morning after the rollover, passenger train services started at 07:17 hrs and, when the first three trains passed over the line with the missing temporary speed restrictions, none of the drivers reported problems with the speed indication displayed on their DMIs [1].

RAIB Clause 28 reads thus: "The fourth train over the affected line was the 08:52 hrs Machynlleth to Pwllheli service with the reporting number 2J035. At around 10:02 hrs, train 2J03 passed through a 30 km/h (19 mph) temporary speed restriction at approximately 80 km/h (50 mph) while travelling between Barmouth and Llanaber. The temporary speed restriction had been applied at this location since 2014 to provide level crossing users with sufficient warning of approaching trains so they could cross safely" [1].

RAIB Clause 29 reads thus: "After passing through this restriction, the driver of train 2J03 reported a fault with the information provided to him by his driver machine interface (DMI). While investigating this report, a signalling technician at the Machynlleth control centre discovered that temporary speed restriction information was not being transmitted to any of the trains on the Cambrian lines" [1].

RAIB Clause 30 reads, thus: "The signalling technician

initiated an RBC reset (software restart) at around 10:11 hrs, intending that this would cause an automatic reloading of the temporary speed restrictions from the GEST sub-system into the RBC. This did not resolve the problem, so the signalling technician reset the GEST server and initiated another RBC reset. At around 11:51 hrs, and after several further unsuccessful attempts to cause an automatic reload of the temporary speed restrictions, the signalling technician contacted the AnsaldoSTS support engineer to request assistance. By this time, signallers and train drivers had reverted to using a procedure-based system of verbal and written instructions to continue the train service" [1].

RAIB Clause 31 reads thus: "While restoring normal working after trying other options, the support engineer advised the signalling technician to delete information contained within a database from the GEST sub-system. This instruction required all temporary speed restriction information to be manually re-entered into the GEST terminal and then transferred to the RBC by the GEST software. The manually entered restrictions displayed correctly on the GEST terminal, and upload to the RBC was verified by a test train which passed through the area at reduced speed while the driver confirmed that the restrictions" were displayed on the DMI. During this activity to return the system to normal service, event and data logs containing information relating to the system were not saved and were subsequently overwritten. Normal operation was resumed at 15:50 hrs" [1].

RAIB Clause 73 reads thus: "temporary speed restriction data was not retained in the RBC during a rollover because it was held in volatile memory. To avoid the need for this data to be manually reloaded, the GEST sub-system was programmed to detect an RBC rollover and automatically send the RBC a copy of the temporary speed restriction data stored in the GEST memory. However, because the GEST sub-system was designed to meet a SIL2 safety integrity level, the AnsaldoSTS designers incorporated an additional check intended to meet the specified requirements. This additional integrity check was performed with a human visual cross check undertaken by the GEST operator. This method of validating the integrity of transmitted data was reliant on the process which gives feedback to the operator, in this instance the display of temporary speed restriction data on the GEST terminal, being independent from the upload process" [1].

RAIB Clause 74 reads thus: "The GEST server entering issue mode due to failure of the Operations thread on 19 October 2017 resulted in both the failure to upload the temporary speed restriction data to the RBC (paragraph 46), and the failure to provide the signallers with the correct information needed for them to undertake the human validation (paragraph 51). This demonstrated that the two functions were not independent and so the supplied system did not achieve the intended integrity level" [1].

RAIB Clause 146 reads thus: "Shortly after the incident, a new control centre instruction was issued at Machynlleth. This required all temporary speed restrictions to be entered manually, and verified by a test train, before normal operations were resumed after a rollover. It has since been revised to require a rollover to be followed by a second, manually triggered reset, during which the correct uploading of temporary speed restrictions is checked and then independently verified by signalling centre staff using the SILAM data logger. In addition, local maintenance staff carry out a daily verification that temporary restrictions are being transmitted to trains" [1].

Based upon the foregoing evidence and the evidence in Appendix C on the part of RAIB, the MORT Analyst observation #8 to the SD3, SD4 and SD 5 branches question(s) are set to LTA. MORT Analyst notes that the maintenance support provided by Ansaldo STS maintenance engineer was critical to the restoration of operations.

B. M— Management System Factors LTA

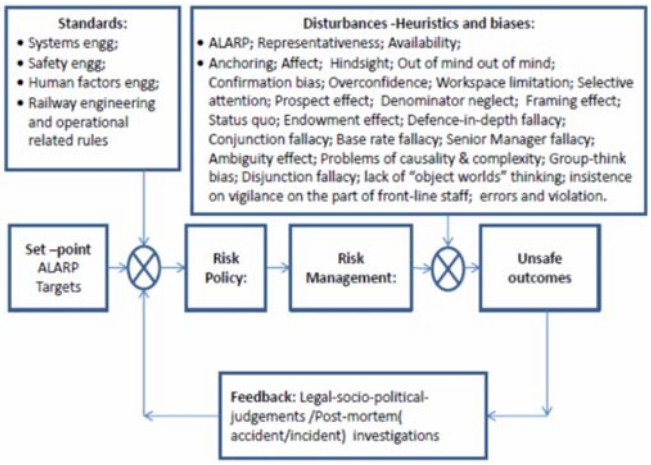

Fig. 2 The SIRI Model of Societal Risk Management [14]

The Management System factors branch considers the design, planning or policy formulation processes that may have contributed to the incident or accident and its consequences. Here you will consider, in the light of what you have revealed through S-branch analysis of this accident, which aspects of the management system allowed the S-branch factors to be LTA. MORT assumes that all issues in the S-branch are tied to issues in the M-Branch. The relationship between these is such that the M-branch designs and governs the S branch. The emphasis here is on processes rather than people. There may be several instances where a function in the "M" branch is the responsibility of a person who does not have "manager" as part of their title or job-description [12].

1) MA1. Policy LTA

Policy refers to a specific policy subject identified during previous analysis. You will need to bear this subject in mind when considering the questions below. Concerning a specific policy subject:

- was the policy clearly stated?
- was the policy up-to-date?
- was policy formulation adequate?
- was the policy of sufficient scope to address the major issues and problems likely to be encountered?
- was this policy adequately integrated with other policies?

2) MA2. Implementation of Policy LTA

a) a1. Planning Process LTA:
b) a2. Execution of Policy Implementation Plan LTA:

3) MA3. Risk Management System LTA

a) MB1. Risk Management Policy LTA
b) MB2. Implementation of Risk Management Policy LTA
c) MB3. Risk Analysis Process LTA
d) MB4. Risk Management Assurance Programme LTA
e) MB5 Review of Risk Management System LTA

Evidences for the above MORT hypotheses are provided hereafter:

(1) Understanding Systems Engineering Standards LTA

RAIB Clause 116 reads thus "Network Rail input did not include effective client role checks to identify the design process shortcomings" [1].

RAIB Clause 117 reads thus "The processes defined in the European standards for the procurement of high integrity systems such as the Cambrian ERTMS system, require the client to be involved in the development of the system (paragraph 37). Network Rail's role therefore included the review and acceptance of the GEST safety case, including the associated system requirements specification and software requirements specification, prepared by AnsaldoSTS" [1].

RAIB Clause 118 reads thus "The RAIB's view is that these shortcomings should have been recognised within the client role required by the EN501xx series of European standards current during the Cambrian ERTMS development (paragraph37). This is supported by RSSB guidance note GEGN8650, which provides assistance for clients procuring high integrity software. Although published in March 2017, the interpretation of client responsibilities is based on parts of the EN501xx series which were unaltered from the version applicable during the Cambrian ERTMS development" [1].

RAIB Clause 119 reads thus "GEGN8650 stresses the importance of the client playing an active part in the production and review of requirements in the early stages of the software development. GEGN8650 identifies common issues which, if left unresolved, can lead to faults in the final software product. These include omissions in the requirements, incorrect specification of the software architecture and a lack of design in the code to deal with erroneous or unexpected parameters" [1].

Omission of System Engineering standard IEC 15288 that RAIB 27/2009 (2009) noted itself by the RAIB as a standard for managing safety critical software is omitted in the RAIB 17/2019 report [22]. The RAIB (2009) Clause 182 reads thus: "In addition to the analysis of previous specific events described above, the RAIB considered to what extent the use of RRVs and trailers on Network Rail conformed to BS ISO/IEC 15288:2002, 'Systems Engineering – System life cycle processes. This standard describes a common framework for system life cycles from conception through to disposal, and the different stages and their purpose are in Appendix G. The RAIB has taken the RRV system to include the machines/trailers themselves, the people who will operate and maintain them, and the procedures that govern the system" [22]. This gives support to the idea that RAIB and GB Railways suffer from problems of complexity and are unable to adopt a Systems thinking approach to overcome it [18], [23], [24]. This is due to "status quo" bias [3].

Findings of review of Sir Peter Hendy (2015) presented: "Signalling resource, needed in respect of replacement and renewal and as a necessary precursor to electrification, is in short supply. Network Rail and its suppliers need to redouble their efforts to recruit apprentices and engineers to complete these works. In addition, Network Rail needs to employ more senior staff in a very competitive market to effectively deliver works paid for by public funds" [25]. Further, Hendy found: "The Great Western Electrification programme will electrify the main line from Maidenhead to Wales and will deliver faster and smoother journeys to passengers as well as being more environmentally friendly. The project requires extensive work to be carried out on the signalling system along the route to allow for the safe movement of trains following electrification. The signalling also needs to be protected from interference of the high-voltage electricity which is used to power the trains. This signalling work is usually undertaken prior to electrification. There has been an acknowledged shortage of suitably skilled people available in the supply chain to undertake the necessary signalling work along this route as they are undertaking many other signalling renewals around the UK. In order to maintain momentum and not cause delays to the programme, Network Rail took the decision to change the sequence of construction and to start piling (the digging of holes) in preparation for the gantries that will hold the electric wires before carrying out the signalling works. The signalling system on the Western Mainline was buried beneath the ballast in the 1970s to prevent it being stolen or vandalised. There were no accurate maps of where the signalling cables were buried. This means that the location of the cables was uncertain. As our contractors started mechanical piling, on two occasions buried cables were hit. These cables were cut, resulting in significant costs being incurred and unacceptable disruption being caused to passengers. To avoid this happening again, a new practice has been introduced whereby trial holes are dug by hand to locate the cable to make sure that piling will not impact the operational railway. There are over 16,000 piles to be installed throughout this route. This additional work adds significant delay and cost to the electrification of Great Western" [25]. Kahneman noted that the Railway Planning process suffers from "planning fallacy" and discussed *Method of reference class forecasting* advanced by Flyvberg to improve the planning [10, pp.250-251].

The SCM/MORT analyst observation #9 on the Hendy Review and the long quotation cited in the previous paragraph as evidence is that Pitfalls in risk assessments and Interface management concerns between the signalling and electrification disciplines were not understood by concerned railway engineers and managers is concluded [23], [26].

(2) Understanding of Site-Specific Information and Risk Assessment LTA

The SCM/MORT analyst observation #10 on the culture of less than adequate systems engineering and risk management is concluded based on the evidence available: Prof Anson Jack and his doctoral student, Neil Barnatt admitted thus: "The current (added, here) situation is further complicated by emergent behaviours of systems that occur as a result of the interaction between systems, a phenomenon that is highlighted by the International Council on Systems Engineering (INCOSE 2015), and the resulting ISO 15288 standard (International Standardization Organization 2015). In other words, some features appear at a higher level of integration in a large system that do not even exist to be examined at the lower level. Consequently, the methods of analysis that were outlined in the previous section will largely only cater for the small-scale analysis and other significant hazards could be missed because the processes are not designed to recognise the interconnected emergent properties. There is clearly a need to examine systems at two levels; at the overall system level as well as its various subsystems, to gain a full understanding of its behaviour" [27].

(a) Integration of Risk Management and Business Policy LTA

The SCM/MORT analyst observation #11 on the inclusion of human and organisational factors in system analysis LTA is concluded on the basis of evidence of human factors engineering academics who worked in the GB railways domain like evidence of Ryan and Mearns was presented in the paper earlier showing lack of inclusion of these concerns into business policy [16], [17].

Omission of the ISO Risk management standard and guidelines from the incident analysis is observed [28]. This is due to "out of sight out of mind bias" [3].

(b) Engineering Risk Management LTA

Review of Sir Peter Hendy (2015) found on the theme of engineering approach to systematic capture and management of risks that the technical risks identified were considered manageable. The technical risks identified were the risks affecting deliverability: a) insufficient competent engineering resources; b) inadequately defined scope at Guide to Railway Investment projects (GRIP 3); c) late changes to engineering scope [25, p.35].

Withdrawal of Yellow Book, a defective engineering management standard in the era of multiple causal factors analysis and lack of inclusion of human and organisational factors, lack of system approach to organisational analysis and work systems is further evidence of the lack of a suitable engineering risk management strategy as per the ORR Guidance (see Clause 2.2, [13]), the ORR Risk Management Model RM^3 and CENELEC standard 50126 as well [13], [29], [30].

Failure of EC SAMRAIL and SAMNET projects to instil safety culture is further evidence for lacking capability to understand complex systems and the roles risk averse and risk-taking behaviour play in the risk management domain is not recognised by domain experts. This is noted by safety researchers who worked in the domain [4], [10], [31]- [33].

Fox and RAIB Chief Accident Investigator did not examine the role of these behaviours in their studies of Canadian and the British accidents despite discussing the role decision-making plays in the safety management systems [10], [34], [35]. And ORR did not note that the omission of the human and organisational factors from the risk assessment of the Crossrail risk assessment is a cause for safety concern [36]. This is due to less than adequate "mental model" of the problem situation or problems due to complexity or anchoring heuristic leads to underestimation of risk in a complex system due to errors in decision making and (see chapters 2 and 3) [3], (see Appendix A) [10], [37].

The SCM/MORT analyst observation #11 on the competence of engineering management staff and strategy planning is LTA.

(c) Regulatory and System owner awareness of Common Safety Method: Risk Assessment LTA

The MORT analyst observation on the adequacy of senior management level competence on engineering management of safety critical projects or the application of Common Safety Method for Risk Assessment is drawn from the following evidence:

From: Anson Jack <email redacted>
To: Sanjeev Kumar Appicharla
Thu, 8 Oct 2020 at 09:05

Dear Sanjeev
Good to hear from you – I hope you are well.
When I sent this email to you, I was doing so as a director of RSSB and not in my personal capacity.
So far as I am personally concerned, I can see no reason why you should not use the document that you attached to this email in any presentation that you make. However, if you feel constrained by the requirements, I set out in the email of 2007 I suggest that you approach RSSB.
With best wishes
Anson

Professor Anson Jack FCILT FSaRS MA(Oxon)
Birmingham Centre for Rail Research and Education
School of Engineering
University of Birmingham
Edgbaston
B15 2TT
United Kingdom

From: "appicharlak@yahoo.co.uk" <appicharlak@yahoo.co.uk>
Reply to: Sanjeev Kumar Appicharla <appicharlak@yahoo.co.uk>
Date: Wednesday, 7 October 2020 at 18:14
To: "Anson Jack (Civil Engineering)" < email redacted >
Subject: Re: CSM Technical Note

Prof Anson,
I need your permission to the email below to share in the Final Paper I am due to present at the 2020 International System Safety Conference.

Since the DFT and ORR have accepted it without knowing the pitfalls of the CSM-RA which I have noted in my 2013 Application, it forms one of the latent errors on the part of the DFT and ORR.

Thanking you in advance,

Regards

Sanjeev Kumar Appicharla

On Thursday, 6 May 2010, 13:35:59 BST, Sanjeev Appicharla <sanjeev.appicharla@rssb.co.uk> wrote:

From: Jack Anson
Sent: 28 February 2007 20:42
To: Allan Jeff; Appicharla Sanjeev
Subject: FW: CSM Technical Note

The references to system design in here may be of interest to Sanjeev' in the context of the paper on SIRI you are developing.

Not to be quoted from please as it is a document within the regulatory community that DfT have shared.

Note also that DfT and ORR do not agree with the position set out in the paper!

Anson

From: Marks Marie
Sent: 28 February 207 11:59 To: Amanda Whyte (E-mail); Andrew.MCNAUGHTON2@networkrail.co.uk; Andy Doherty (E-mail); Carol Baker (E-mail); Caroline Wake; Chris Carr; Clare Freeman (E-mail); Gill Dixie; Grenardo Tracee; Jack Anson; Jonathan Ellis; Julian Lindfield; Keith Rose (E-mail); Keith Watson (E-mail); Louise Shaw (E-mail); Marks Marie; Milligan Adam; Nicola Carolan; Richard Gostling (E-mail); Richard Lockett (E-mail); Robert Gardner; Sharpe Andrew; Stephen Barber; Tim Gilbert; Walters Taela
Subject: FW: CSM Technical Note

Dear all,

As promised at ISCC, please find attached (from Caroline Wake) the ERA technical note re CSMs and interoperability.

Kind regards,

Marie

The SCM/MORT analyst observation #12 is on the lack of awareness of other biases listed in the paper at the Office of Rail Road Regulation: The Office of Rail Road Regulation (2015) internal policy guidance on safety related investment decisions did not expect the duty holder to perform cost benefit analysis when the risk reduction action is to be taken based upon the relevant good practice as a baseline. When the relevant good practice is not good enough it recommends rough CBA to be undertaken and along with a correction for 'optimism bias'. This is to make adjustments for overconfidence in the project estimates to account for cost overruns in capital projects. This document can be accessed here [38]. Readers need to see chapter 2 and chapter 3 as well [3].

(3) Expert Judgement LTA: Group Think Bias

Where risks are difficulty to quantify, the guidance documents suggest using qualitative techniques such as structured workshop assessments supported by expert judgement. We already published the results of past HAZOP and MORT studies which show that expert judgement is compromised by group think bias in 2010b [18]. This is further evident from engineering safety management process followed by the UK railway industry which is biased towards operational reliability by taking into the number of years of reliable operation [39]. The Yellow Book does not contain any process for performing system hazard causal factor analysis as identified in the informative clause, 4.4.2.12 of BS EN 50126 [30], [39]. The RSSB guidance (2014) on taking safe decisions uses reasonably practicable policy. The argument advanced is predicting accident risk in inherently uncertain. Similar accidents may give rise to different fatalities: 31 fatalities (Ladbroke Grove) or seven fatalities (Southall) and therefore, low frequency high fatality accidents cannot be predicted. Quantitative risk assessment is considered to be useful as high frequency and low fatality incidents can be easily predicted as there is plenty of historical data. This argument is not in accordance with the best practice of safety management. When the information is uncertain, the precautionary principle should be invoked. The principle of inherent safe design of signalling or any other engineering works is perceived but not cognised [7]. The ERTMS system architecture is not well understood by the (87%) of railway domain experts (section 7) [15]. Thus, Expert Judgement LTA is concluded.

(4) Safety Investment into Automatic Train Protection LTA

The SCM/MORT analyst observation #13 on the culture of safety investments: Whittingham argued that there is a lack of will to make necessary investment into automatic train protection by the railway industry using arguments of high cost of ATP per fatality averted but the situation is exacerbated by a lack of consistent policy by successive governments [40, pp.188]. Mental accounting bias as suggested by Nobel laureate Prof Richard Thaler is inferred here [10, p.343]. McDermott et al. stated that systems engineers are also prone to cognitive biases and this needs to be addressed to enable investment into train protection [41].

(5) System Assurance Management LTA

The SCM/MORT analyst observation #14 on the culture of less than adequate system assurance management: RAIB clause 149: reads, thus: "Ricardo Rail/Ricardo Certification has stated that it has revised its assessment processes as part of the work necessary to become a UKAS accredited independent safety assessment service. The revised processes also incorporate the changes required by the Common Safety Method for Risk Evaluation and Assessment (Commission Regulation (EU) 402/2013) in April 2013" [1]. The author noted that this is not true as there is no method to carry out explicit risk assessment after the withdrawal of the Yellow Book as per Dr. George Bearfield, the then SSB Safety Manager and ex Chief Inspector HMRI [42]. This is a "mis-representation bias" and is due to representativeness heuristic (see Appendix A) [10].

The RAIB (2019) accepted that Independent Safety Assessor Modifications to these assessment processes mean they are more systematic in confirming that there is evidence that safety requirements have been met by ensuring following activities in

the performance of CSM-RA (Clause 149) [1]. However, failure types noted in the research by the author n this paper suggest that the RAIB acceptance is pre-mature [7], [14].

a. all reasonably foreseeable hazards are identified;
b. assumptions that underpin the safety behaviours of systems are identified and defined/written down (in system definitions); and,
c. evidence is sought for the implementation of all safety requirements associated with hazards.

(6) System Definition LTA

The SCM/MORT analyst observation #15 on the culture of less than adequate system definition: The European Commission Directorate General for Transport Master ERTMS Development Plan (1996) did not specify how system safety analysis will drive safety requirements [43]. This is "Anchoring" bias [10]. The patchy development of the ERTMS is given by Lochman [5], [19].

The ESROG working Group (2000) did not identify a system definition including individual, technical and organisational factors as required by the initial stage of the Common Safety Method [44].

RSSB (2011) admitted in a paper its inability to define the system including software, but a generic hazard list will suffice [42]. Further, the concept of "Bounded rationality" assumed by Nobel prize winning cognitive psychologists due to which limited information processing is found in real world rather than omniscient rationality assumed by the economists leads to the conclusion that solution search will be a limited rather exhaustive search to solutions to the problems faced due to satisficing heuristics [3], [10].

In a Lessons Learnt Report to the ORR (2012) it was noted that the operation concepts should reflect all degraded and non-TSI modes of operation from all human perspectives. Clear system recovery path should be set out and used to inform system reliability calculations [45]. In response to the 2012 Report, RSSB (2012) advised that the Operation Concepts were currently at a conceptual level and a system engineering approach would be used to be develop detailed requirements. RSSB does not understand the role of latent failures and systems engineering concepts was published by Appicharla in 2010b, 2013 and 2017 as well is the MORT analyst observation #17 [18], [44], [45].

(7) System Risk Assessment Review LTA

RAIB Clause 14 reads thus: "Network Rail chaired and employed the discipline experts which formed the System Review Panel (SRP). The SRP determined the acceptability of the safety case documents submitted to it by the Cambrian ERTMS project team, taking account of the issues that had been identified by the ISA" [1]. The SCM/MORT analyst observation #16 based upon the foregoing is the less than adequate understanding of process steps in the risk management domain.

(8) Learning Lessons from past Failures LTA

The SCM/MORT analyst observation #17 of Learning Lessons from past failures LTA: RAIB Clause 146 reads, thus: "Shortly after the incident, a new control centre instruction was issued at Machynlleth. This required all temporary speed restrictions to be entered manually, and verified by a test train, before normal operations were resumed after a rollover. It has since been revised to require a rollover to be followed by a second, manually triggered reset, during which the correct uploading of temporary speed restrictions is checked and then independently verified by signalling centre staff using the SILAM data logger. In addition, local maintenance staff carry out a daily verification that temporary restrictions are being transmitted to trains" [1].

NAO (2006) Report stated a sweeping train to check the track status free of being occupation to overcome the defects in the axle counter technology [46]. The same idea is implemented by Network Rail in the case of event of Loss of temporary speed restriction data can be safety. Halcrow (2012) Report on Lessons Learnt from ERTMS, Recommendation 2 reads thus: A robust system engineering approach is developed to ensure a comprehensive mapping between specifications (TSI+others) and operating requirements. NR stated that Thameslink already had a system engineering approach which would be taken forward with the national programme [45], [47]. Research by the UK HSE is neglected by the RAIB as well as Halcrow [48]. No lessons are learnt from NIMROD Failure of Safety Case or failure of safety engineering tasks [49]. The RAIB Report 17/2019 [1] takes no cognizance of the Thameslink systems engineering capability suggesting that the capability is either non-existent [47] or Network Rail experts suffer from overconfidence bias. [10]. LTA Learning Lessons are concluded.

(9) Safety Management System LTA

The SCM/MORT analyst observation #18 of Safety Management System LTA: RAIB (2017) states the defects in the safety management system and safety culture observed in the accidents it surveyed [35]. But RAIB fails to apply its knowledge base to this incident is a concern. Risk in management systems is due to "availability" heuristic. "Out of sight mind" bias and lack of application of "decision making under uncertainty" in risk assessments are not included in the RU or IM SMS to form a stage-based reviews or decision making. Evans recommended that application of "decision making under uncertainty" is required in the study of societal risk and biases in decision making need to be considered [8], [50]-[52].

(10) Oversight, Internal Auditing and Review LTA

The SCM/MORT analyst observation #19: The RAIB Report 17/2019 fails to state any internal auditing reviews of the Cambrian Project Team. Further, the RAIB is silent on the competence of operational, management and front-line staff and focused its attention only on single point failure without looking into how the programme and general management and safety management system failures contributed to the failure of pilot project as it had stated in 2017 [1], [4], [35]. This is due to "confirmation" bias [3]. The ABIN Method analysis of the Interim Report has failed to include these factors is the evidence

[53].

Smart et al., at Google (2020), in their lessons learnt exercise from the aviation industry, have noted that accident statistics and safety target of one in billion per use maximum failure probability reveal a remarkable safety record approaching an engineering marvel. The aircraft and engine manufacturers, airlines, governments, regulatory bodies, and other industry stakeholders have contributed to this safety record over a number of years. The complexity of the modern avionic system had increased drastically with about 13 million lines of code for Boeing 787 aircraft. But they noted that the recent Boeing 737 MAX accidents indicate, safety is never finished, and the qualitative impact of failures cannot be ignored—even one accident can impact the lives of many and they rightfully acknowledged the crashes as a catastrophic tragedy. In a like manner to Nobel laureate Prof. Daniel Kahneman, (see [10]) they draw attention to the fact belief in small numbers and failure to recognise the fact that element probability in fault scenarios in a complex system can lead to a disaster if active measures are not taken to mitigate the risk. Due to lack of vigilance, there is a danger that complex systems drift into failure [54].

Smart et al. further argued on the limitations of internal audit due to biases on the part of auditors, part of the AI systems developers, and social biases in its larger socio-technical system, are challenging in nature and are not addressed systematically in the literature. However, learning from the regulatory dynamics in the financial, aviation, chemical, food, and pharmaceutical industries suggest that internal audits are only one important aspect of a broader system of required quality checks and balances [54]. In other words, defence in depth policy is needed.

The idea of Byzantine fault discussed by computer scientists may be generalised to state the idea that an accident may indicate different things to different professionals and it is necessary that system ideas are shared through the use of systems engineering architecture concepts. The IEC 15288 systems engineering standard supports creation, modification and changing of such system architecture. Appicharla developed such a language and helped domain engineers express it [31], [54]. However, Appicharla through the application of SIRI Methodology learnt that domain engineers and senior managers involved in safety related decision-making activity are prone to group think bias [18]. Traditional risk assessments are based on causal chains and event analysis, failure reporting and risk assessments, calculating historical data-based probabilities. This approach has strong limitations in analysing complex systems as they treat the system as being composed of components with linear interactions, using methods like fault trees and event trees, and have mainly a historical failure data perspective [55].

IV. Results

The application of SIRI Methodology revealed the errors in the S and M branches involved in the MORT Logic Diagram. The results include human and organisational factors and provide a big picture of the risk management problem than the M.Sc. Thesis of Marius Wold Albert (2019) of NTNU [53]. Marius Wold Albert (2019) studied the same accident from the STAMP/CAST and ABIN Method based upon the interim RAIB Report is to be noted.

V. Conclusions

The research paper presents the results of the application of systems engineering approach and a method for identification of the latent factors and underlying heuristics and biases at various levels of socio-technical system involved in contributing to the system failure.

Acknowledgments

We express gratitude to the Reviewers and the Organising Committee to accept the lengthy paper. We extend gratitude to the organisations (especially, the NFI Foundation) and research scholars who made their research output available freely to our requests on the research gate.net. We express gratitude to Mr Cherian P. Thomas Managing Director, Aethos Business and Mr N.P Rao, CEO Pegasus Consulting for their help in reviewing the presentation slides.

References

[1] RAIB, "Report 17/2019: Loss of safety critical signalling data on the Cambrian Coast line, 20 October 2017," 19th December 2019. (Online). Available: https://assets.publishing.service.gov.uk/media/5df8fa1be5274a08de86827d/R172019_191219_Cambrian_Coast_line.pdf (Accessed 5th January 2020).

[2] S. Hall, The Railway Detectives: 150 year old saga of the Railway Inspectorate, London: Ian Allen, 1990.

[3] J Reason, Human Error, 17th ed., New York: Cambridge University Press, 1990.

[4] J. Reason; E. Hollangel; J Paires, "Revisiting the « Swiss Cheese » Model of Accidents," Eurocontrol Agency, BRUXELLES, 2006. (Online). Available: http://www.eurocontrol.int/eec/gallery/content/public/document/eec/report/2006/017_Swiss_Cheese_Model.pdf. (Accessed 2011 September 2011).

[5] L. Lochman, "Background on ERTMS," in *Compendium on ERTMS - European Rail Traffic System*, 2009 ed., Hamburg, EUrail press, DVV Media House, Hamburg, 2009, pp. 31-50.

[6] P. Simon, ""Standardizing European Railways: A Supranational Struggle against Persistent National Languages and Emergent Local Dialects"," Flux, Vols. 79-80, no. 1, pp. 124-136, 2010.

[7] S. Appicharla, "Modelling and Analysis of Herefordshire Level Crossing Accident using Management Oversight and Risk Tree (MORT)," IEEE, 21st September 2011. (Online). Available: https://ieeexplore.ieee.org/abstract/document/6136924 (Accessed 23rd January 2012).

[8] Oldfield, Professor Agi; Ltd, Anser Conspectus, "RSSB Report: T169 – Risk in Management Systems Rev 2," RSSB, London, 2004.

[9] I. M. Copi and C. Cohen, Introduction of Logic, Low Price Edition, 2001 ed., Delhi: Pearson Education, 1998.

[10] Nobel laureate, Prof Daniel Kahneman, Thinking Fast and Slow, London: Penguin Group, 2012.

[11] Nobel laureate, Sir Roger Penrose, The Road to Reality: A complete Guide to the Laws of Universe, 2004 ed., London: Jonathan Cape, 2004, p. 1049.

[12] The Noordwijk Risk Initiative Foundation; Royal Dutch Navy, "NRI MORT User's Manual," 20 December 2009. (Online). Available: http://www.nri.eu.com/NRI1.pdf (Accessed 16th March 2017).

[13] The Office of Rail and Road (ORR), "Guide to ROGS: The Railways and Other Guided Transport Systems (Safety) Regulations 2006 (as amended)," ORR, London, 2020. (Online). Available: https://www.orr.gov.uk/sites/default/files/2020-11/rogs-guidance-

october-2020.pdf (Accessed 23rd December 2020).

[14] S. K. Appicharla, "RSL 024 and RSL 013: Written Evidences for the UK Transport Select Committee's Railway Safety Inquiry," 09th January 2017. (Online). Available: https://old.parliament.uk/business/committees/committees-a-z/commons-select/transport-committee/inquiries/parliament-2015/rail-safety-16-17/publications/ (Accessed 31st May 2020).

[15] Katja Schuitemaker; Heidi van Spaandonk; Marco Kuijsten; Mohammad Rajabalinejad, University of Twente (UT), Utrecht, the Netherlands (UN), "Evaluating Key Factors Influencing ERTMS Risk Assessment: A Reference Model," International Journal on Advances in Systems & Measurements, vol. 11, no. 1,2, pp. 22-35, 2018.

[16] Kathryn J. Mearns, Wood PLC, Aberdeen, UK, "Safety Leadership and Human and Organisational Factors (HOF)—Where Do We Go from Here?" in Human and Organisational Factors: Practices and Strategies for a Changing World, Toulouse, France, Springer Open, 2020, p. 138.

[17] Ryan, Brendan, the Nottingham University, ""Accounting for differing perspectives and values: the rail industry." In Human and Organisational Factors, Springer, Cham, 2020.," in Human and Organisational Factors, Practices and Strategies for a Changing World, Toulouse, France, Springer Briefs in Safety Management, 2020, pp. 5-13. (Online). Available: https://link.springer.com/book/10.1007%2F978-3-030-25639-5 (Accessed 23rd August 2020).

[18] S. Appicharla, "System for Investigation of Railway Interfaces," in The Fifth IET International System Safety Conference, Manchester, 2010b. Online). Available: http://ieeexplore.ieee.org/document/5712351/ (Accessed 3rd August 2021).

[19] D. P. Winter, "Compendium on ERTMS", Hamburg: DVV Media Group GmbH, 2009.

[20] UNISIG, "SUBSET-091: Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2, version 3.4.0," UNISIG, Brussels, 2015. (Online). Available: https://www.era.europa.eu/sites/default/files/filesystem/ertms/ccs_tsi_annex_a_-_mandatory_specifications/set_of_specifications_2_etcs_b3_mr1_gsm-r_b1/index027_-_subset-091_v340.pdf. (Accessed 30th March 2020).

[21] International Electrotechnical Commission Contributors, "Functional Safety and IEC 61508," 2010. (Online). Available: https://webstore.iec.ch/publication/22273 (Accessed 18th September 2019).

[22] RAIB, "Report 27/2009: Investigation into runaways of road-rail vehicles," October 2009. (Online). Available: https://assets.publishing.service.gov.uk/media/547c901ee5274a428d000173/R272009_091029_RRV.pdf (Accessed 3rd October 2019)

[23] BS ISO/IEC 15288: 2002, Annex D, System Concepts, London: International Electro-technical Commission /BSI London, 2002.

[24] P. N. Leveson, "A New Accident Model for Engineering Safer Systems," Safety Science, vol. 42, no. 4, pp. 237-230, 2004.

[25] Sir Peter Hendy, Chairman, Network Rail, "Report from Sir Peter Hendy to the Secretary of State for Transport on the replanning of Network Rail's Investment Programme November 2015," Network Rail, London, 2015. (Online). Available: https://www.networkrail.co.uk/wp-content/uploads/2019/06/hendy-report.pdf (Accessed 31st May 2021).

[26] Dr Sandra Gadd, Dr Deborah Keeley, Dr Helen Balmforth, Health & Safety Laboratory, "Good practice and pitfalls in risk assessment," HMSO, Norwich, 2003. (Online). Available: https://www.hse.gov.uk/research/rrpdf/rr151.pdf. (Accessed 29th May 2021).

[27] J. Prof Anson and N. Barnatt, "Safety analysis in a modern railway setting," Safety Science, pp. 177-182, 2018. (Online). Available: https://www.sciencedirect.com/science/article/pii/S092575351731130X (Accessed 25th August 2019).

[28] Technical Committee ISO/TC 262, Risk management., "ISO 31000(en) Risk management — Guidelines," February 2018. (Online). Available: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en (Accessed 15th April 2021).

[29] ORR, the Office of Rail and Road, "Risk Management Maturity Model (2019) Amended 2020," ORR, 2019. (Online). Available: https://orr.gov.uk/__data/assets/pdf_file/0013/2623/risk-management-maturity-model-rm3.pdf (Accessed 9th July 2020).

[30] CLC/Tc 9X " Electrical and electronic applications for railways, "BS EN 50126 Part 1: Railway applications —The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)," 2020. (Online). Available: https://shop.bsigroup.com/ProductDetail?pid=000000000030411381 (Accessed 3rd August 2021).

[31] S Appicharla, "System for Investigation of Railway Interfaces," US IEEE, 7th June 2006. (Online). Available: http://ieeexplore.ieee.org/document/1662220/ (Accessed 2015 December 2015).

[32] European Commission Fifth Framework programme, "D2.9.1: Synthesis of SAMRAIL findings," The European Commission, Brussels, 2006European Commission Fifth Framework programme, "D2.9.1: Synthesis of SAMRAIL findings," 2006. (Online). Available: https://trimis.ec.europa.eu/sites/default/files/project/documents/20060727_155616_03705_SAMRAIL_Final_Report.pdf. (Accessed 24th April 2019).

[33] WS Atkins Rail Limited, UK, "European Commission Fifth Framework programme: SAMRAIL/SM/D2, D2.9.1: Synthesis of SAMRAIL findings," 8th December 2004. (Online). Available: https://trimis.ec.europa.eu/sites/default/files/project/documents/20060727_155616_03705_SAMRAIL_Final_Report.pdf (Accessed 11th February 2020).

[34] Kathleen Fox, MSc in Human Factors and System Safety, Lund University, Sweden, How has the implementation of Safety Management Systems (SMS) in the transportation industry impacted on risk management and decision-making? Lund, Scania, Lund University, Sweden, 2009. (Online). Available: https://www.humanfactors.lth.se/fileadmin/_migrated/content_uploads/thesis-2009-Fox-Impact_of_SMS_on_Risk_Management_and_Decision_Making.pdf (Accessed 29th May 2021).

[35] Simon French, Chief Inspector of Rail Accidents, Tabitha Steel, Human Factors Specialist, Rail Accident Investigation Branch, United Kingdom, "Discussion paper 20: The Investigation of Safety Management Systems and Safety Culture:" in The Roundtable on Safety Management Systems, Paris Cedex 16, 2017. (Online). Available https://www.itf-oecd.org/sites/default/files/docs/investigation-sms-safety-culture.pdf (Accessed 23rd August 2020).

[36] S. K. Appicharla, "Cross Rail Train Protection (Plan B) - Railway Safety Regulations," ORR, 27th October 2015. (Online). Available: https://orr.gov.uk/__data/assets/pdf_file/0004/19894/crossrail-exemption-application-consultation-sanjeev-kumar-appicharla.pdf. (Accessed 18th May 2019).

[37] Prof Philip N. Johnson-Laird, Department of Psychology, Princeton University, Princeton, NJ 0854, "Mental models and human reasoning," Proceedings of the National Academy of Sciences, vol. 107, no. 43, pp. 18243-18250. (Online). Available https://www.pnas.org/content/107/43/18243 (Accessed 26th October 2010)

[38] Office of Rail Road Regulation, "Internal guidance on cost benefit analysis (CBA) in support of safety-related investment decisions," Office of Rail Road Regulation, London, 2015.

[39] Ali Hessami, John D. Corrie, Roderick Muttram, Roger Aylward, Brian Clemenston, Robert A. Davis, Bruce Elliott, Eddie Goddard, Chris Thompson, Dee Razdan, J. Irwin, Terry George, Andy Doherty, Yellow Book, London: Railtrack on behalf of the UK Rail Industry, 2000.

[40] R. Whittingham, The Blame Machine, Oxford: Elsevier, 2004.

[41] McDermott, Thomas A., Dennis J. Folds, Leonie Hallo, "Addressing Cognitive Bias in Systems Engineering Teams," INCOSE International Symposium, vol. 30, no. 1, pp. 257-271, July 2020.

[42] Dr. G.J. Bearfield; R. Short, "Standardizing Safety Engineering Approaches in the UK Railway," in The Sixth International System Safety Conference, Birmingham, 2011.

[43] The European Commission Directorate General for Transport, "The Master Plan for Development and Pilot Installations of the European Traffic Rail Management System Doc.189/96," The European Commission, Brussels, 1996.

[44] S. Appicharla, "Technical Review of Common Safety Method using System for Investigating Railway Interfaces (SIRI) Methodology," in 8th IET International System Safety Conference incorporating the Cyber Security Conference 2013, Cardiff, UK, 2013. (Online). Available: https://ieeexplore.ieee.org/document/6725790 (Accessed 3rd August 2021).

[45] Halcrow Group Limited, "(CH012 Final Report National ERTMS Lessons Learnt Review Report," 4th April 2012. (Online). Available: https://orr.gov.uk/__data/assets/pdf_file/0005/1985/reporter-ertms-lessons-learnt.pdf (Accessed 26th October 2019).

[46] Sir John Bourn, The Comptroller and Auditor General, NAO, "The Modernisation of the West Coast Main Line," The HM Stationery Office,

London, 2006. (Online). Available: https://www.nao.org.uk/wp-content/uploads/2006/11/060722.pdf (Accessed 22nd August 2019).

[47] Obi Ozonzeadi, Development Manager –Network Rail, Governance for Railway Investment Projects (GRIP) application for Thameslink Programme, London: Thameslink Programme, 2018. (Online). Available: https://uhoun19qey9384ovv24t33c1-wpengine.netdna-ssl.com/wp-content/uploads/2018/10/GRIP-application.pdf. (Accessed 12th June 2021).

[48] The NEL Consortium, "The UK HSE Research Report 067: Train Protection - Technical review of the ERTMS Programme Team report," The UK HSE, HMSO, Norwich, 2003. (Online). Available: http://www.hse.gov.uk/research/rrpdf/rr067.pdf (Accessed 6th August 2013).

[49] Sir Haddon Cave, QC, "THE Nimrod Review," 28th October 2009. (Online). Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/229037/1025.pdf (Accessed 25th December 2019).

[50] Atsuo Murata; Tomoko Nakamura; Waldemar Karwowski, "Influence of Cognitive Biases in Distorting Decision Making and Leading to Critical Unfavourable Incidents," Safety, vol. 1, no. 1, pp. 44-58, 2015. (Online). Available https://www.mdpi.com/2313-576X/1/1/44 (Accessed 3rd August 2021).

[51] T. T. &. M. Hunt, "Review of LU and RSSB Safety Risk Models," ORR, London, 2012. T. T. &. M. Hunt, "Review of LU and RSSB Safety Risk Models," 2012. (Online). Available: https://orr.gov.uk/__data/assets/pdf_file/0019/5059/ttac-safety-risk-models-review.pdf. (Accessed 6th May 2019).

[52] P. A. Evans, "Transport Fatal Accidents and FN Curves," HMSO, Norwich, London, 2003. (Online). Available: https://webarchive.nationalarchives.gov.uk/20101111125221/http://www.rail-reg.gov.uk/upload/pdf/rr073.pdf (Accessed 12th June 2019).

[53] Marius Wold Albert, MSc NNTU, "A case study to investigate accidents involving the European Rail Traffic Management System (ERTMS): Investigation of complex accidents in the digitalised railway sector," 2019. (Online). Available: https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2634920/Albert%20Marius%20Wold.pdf?sequence=1&isAllowed=y (Accessed 11th June 2021).

[54] Andrew Smart et al, Google, "Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing," in FAccT: Fairness, Accountability, and Transparency, Barcelona, Spain, 2020. Online. Available: https://dl.acm.org/doi/10.1145/3351095.3372873 (Accessed 30th March 2021).

[55] Prof T. Aven; University of Stavanger., "Risk Assessment and risk management: review of recent advances on their foundations," European Journal of Operations Research, vol. 253, no. 1, pp. 1-13, 16th August 2016. (Online). Available https://www.sciencedirect.com/science/article/pii/S0377221715011479 (Accessed 30th April 2019).