We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900
Open access books available

185,000
International authors and editors

200M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



Chapter 3

Application of Cognitive Systems Engineering Approach to Railway Systems (System for Investigation of Railway Interfaces)

Sanjeev Kumar Appicharla

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/61527

Abstract

This chapter presents the results of a cognitive systems engineering approach applied to railway systems. This application is through the methodology of 'System for Investigation of Railway Interfaces – SIRI'. The utility of the chapter lies in highlighting errors in the current approaches to safety risk management.

Keywords: Cognitive systems Engineering, Systems safety engineeering, Human factors engineering, Risk and Decision Making

1. Introduction

This chapter presents the results of a cognitive systems engineering approach to safety, 'System for Investigation of Railway Interfaces – SIRI'. The objectives of the application are to show:

a. How current methods to model, analyse, and manage safety risk do not facilitate learning lessons from past accidents;

b. How the use of heuristics by decision makers induce biases into the Committee-based decision-making process;

c. How failure of understanding amongst railway practitioners manifests when the attributes of reliability, availability, maintainability, and safety (RAMS) are treated as independent parameters of a signalling system.

INTECH
open science | open minds

© 2015 The Author(s). Licensee InTech. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The above failings are demonstrated by means of a case study of Cambrian European Railway Train Management System – ERTMS – level crossing incident investigated by UK's Rail Accident Investigation Board(RAIB) in Jan 2012.

RAIB noted that a deviation to a safety critical requirement to interlock the function of the barriers with the function of train protection (braking system) was granted by the Signalling Standards Committee to the duty – holder organisation – Network Rail, without asking for a human factors analysis or risk assessment to support the deviation request. This incident occurred at the automatic barrier locally monitored type level crossing (ABCL). This chapter provides the causal factors behind the decision to grant a deviation to safety critical requirements.

This chapter draws upon author's papers peer reviewed and published in the proceedings of the IET International System Safety Conferences since 2006, and publicly available literature [2, 3, 4, 7, 9, 11, 12].

The rest of the chapter is organised in this way: Section 1 provides the abstract of the chapter; Section 2 shows why wrong-but-popular approaches to safety risk management persist in the railway domain; Section 3 presents a case study using the SIRI methodology to help understand its application; Section 4 provides conclusions on subject matter of the chapter. Section 5 provides acknowledgements. Section 6 provides the references.

2. Explanation for persistence of wrong-but–popular approaches to safety risk management: Doing the wrong thing right

> OM. What instructions did the Blessed Lord give: Be compassionate. Be controlled. Be charitable.
>
> Sri Adi Śhankarāchārya, 8th Century AD, Brihadaranyaka Upanishad
>
> Translated by Prof V. Roebuck [79]
>
> Everything is fine today that is our illusion.
>
> Voltaire, quoted by Douglass W. Hubbard [29]
>
> We have inherited the neural mechanisms that evolved to provide ongoing assessment of threat level, and they have not been turned off. Situations are constantly evaluated as good or bad, requiring escaping or permitting approach. Good mood and cognitive ease are the human equivalents of assessments of safety and familiarity.
>
> Nobel laureate and psychologist, Prof Daniel Kahneman (pp. 90) [36]

OM is the sacred symbol to denote Brahman in the Hindu religious literature. More information can be gained about the nature and meaning of the symbol from reading Prof Roebuck's writings [79]. Prof Charles Perrow, originator of Normal Accident Theory, recounted the

http://dx.doi.org/10.5772/61527

abnormal blessings he had received from his co-researchers in his preface to second edition of his book. Author speculates that Prof Charles Perrow did not know the source of abnormal blessings for the success of Normal Accident Theory as he may have thought he had not prayed for its success [49, 79]. In his survey of risk assessment theories and practices, Charles Perrow did recognise the work of cognitive systems engineering experts and various kinds of rationalities but opinied that these view points did not recognise the role of power in and of organisations (pp. 379) [79]. Interpretating the reality of accident causal factors and represent them by means of fault free fault tree analytical representation to show errors in the systems engineering steps, in the professional opinion of the author, helps mitigate the problem of discounting power of subject matter experts, and risk assessors in generating biased risk information in producer and client, systems engineering and regulatory organisations (pp.65) [52].

From the vast literature on risk on the perspective of risk rationality in human affairs, it is easy to think of four types of rationalities: omniscient rationality, which is enjoyed by political economists like Nobel laureate Gary S. Baker, "bounded" or limited rationality advanced by organisational decision scientist is and some risk assessors like Nobel laureate Herbert A. Simon, irrationality as advocated by behavorial economists like Noble laureate Daniel Kahneman, reluctant rationality of participants in making choices and displaying regret after the fact who may regard false negative alarms (near miss incidents) as reliablity events [36, 62]. Typical example being NASA managerial judgements on the Challenger launch decision.

Neuro-scientists have identified human brain regions associated with emotional and cognitive side of information processing activity when an individual processes a risky stimulus [36, 50]. Studies cited by Nobel laureate Daniel Kahneman, Peter N.C. Mohr, and his co-workers draw attention to the fact that decision maker(s) when engaged in the tasks of revealing preferences or answering queries on uncertain situations such as questions on lottery, risk assessment, and risk management do consult their emotions, and these decisions can be called decisions under risk. Decision theorists like psychologists, philosophers, statisticians, and economists approach decision making in a mathematical manner and are not prone to emotions and framing effects felt in the case of non-decision scientist(s) asserted in these research papers. The idea of risk as a rare event with odds of 1 in 400 or more with a consequence probability of 0.249% is possible is acknowedged by Prof David Hand, an expert statistician [26]. In other words, definition of rare events and estimation of the odds of their occurrence by expert statisticians may be prone to error is the thesis advanced by Prof David Hand. Evidence for this thesis is drawn by Prof David Hand from the case study of Sudden Infant Death Syndrome. Sir Roy Meadow's expert evidence led to erroneous legal prosecution of Sally Clarke. Rare event of train and vehicle collision on the Great Britain railway track was experienced by the members of the same family in the UK within a span of 15 years is cited as well [26]. The mean expected rate for such random events to occur as per Poisson's distribution is 0.741%. It is tempting to arrive at a conclusion that operational reliability of the railway is very high, i.e. 99.25% based upon the foregoing metric. Most pre–university students learn about stastitical distributions in their final year of secondary school leaving stage. Students of risk management can easily be laid into error if they are not careful in their thinking when making risk judgements that involve casual inferences (pp. 166–67) [36]. The litmus test for any student of decision making

and risk management is the case of NASA Space Shuttle Accident in 1986. This case study alone poses challenge to statistical and rational decision theory, learning from past failure incidents, theories of control, system safety, and risk management [5, 36, 49]. The signal of less than adequate design shuttle vehicle flown by NASA and supported by its supplier, Morton Thiokol, till the pre-launch decision was obscured or buried under the noise generated by the hindsight observations of NASA manager's pre-launch decision [5]. To its credit, NASA, Langley Research News hosts the book on its website written by former Morton Thikol engineering director, Allan Madonald, who had a change of heart without any apparent reason on the pre-launch decision day and went along with engineer Roger Boisjoly who was opposed to the launch decision [5], [55]. Risk management expert Douglass Hubbard is of the view that Bayesian risk analysis may have helped in the case of NASA Challenger decision situation where the failure data was scanty [29]. Bayesian risk analysis can certainly help if prior information of categorial variables is available in the odds form and likelihood ratio of positive and negative rates are known as well. But we 've bear in mind Prof James Reason's thesis that most of us are not intutive bayesians [55]. Once Johann Wolfgang von Goethe observed that it is much easier to recognize error than to find truth; the former lies on the surface, this is quite manageable; the latter resides in depth, and this quest is not everyone's business. No accident researcher has the luxury of verifying correspondence between ideas of managerial oversight and risk seeking behavior apart from relying upon lessons learn from behavioral science risk literature (pp. 228) [53, 54].

The thesis advanced in the research papers in the area of cognitive psychology is that people who resist intutive responses to following bat–ball question do not need to reflect on the question again. The bat-–ball puzzle is as under. This question is to be answered in an intutive manner without solving it on a paper.

A bat and ball costs £1.10.

The bat costs one dollar more than the ball.

How much does the ball cost?

The intutive answer is 10 cents. Many thousands of university students have answered the bat–ball question. More than half of the undergraduate students at Harvard, MIT, Princeton gave the intutive–incorrect –answer.

The failure rate at other American universities is even more higher at 80% (pp. 44–45) [36]. The correct answer is 5 cents. Perhaps, a distinction between intelligence and rationality is needed is the suggestion made by these researchers (pp. 49) [36].

The author observes that intutive errors in decisions made by these undergraduate students cannot be explained by saying that these students are not skilled mathematicians. The author speculates that the psychological mechanisms involved in the perceptual and cognitive decision process by experimental subjects are as follows; mentally formulating the equations to represent the quantities of prices involved, and then subtracting the equations to identify one of the single unknown and arrive at its value by halving it. The difference between those who get the right and wrong answers is simply this: failure to divide in the final equation.

http://dx.doi.org/10.5772/61527

These errors are attributed by cognitive psychologists to the property of overconfidence of subjects who answer the question as 10 cents. From the science of cybernetics perspective, the purpose of the bat–ball question is to trigger thinking activity on decisions on safety-related control systems where the safe state of the system cannot be perceived by sight and failures in risk management and safety assurance process are likely [12, 28, 44, 57].

When author compares and evaluates the foregoing behavorial science research findings against the research findings published within system safety research domain, then another type of culture of decision-making emerges. Complexity of a socio-technical system became the focus of attention of system safety researchers during the 1980s. Prof Charles Perrow (1984) argued that complexity of organisations and tight-coupling of systems render it difficult to foresee how rare accidents can occur. The problem of complexity poses serious challenge to formal system safety management processes. Evidence is available to show that the counter thesis of Normal Accident Theory namely, High Reliable Organisations, is negated by John Bushby's case study of two British railway accidents [16]. James Reason (1990) whilst advancing a general view of accident causation in complex systems in the form of Swiss Cheese Model observed that system (normal) accidents have their origin in latent failures (fallible decisions) in supervisory control systems made at the corporate management, designer(s), and line management levels. He noted that identifying latent errors is a challenge faced by human factors researchers concerned with preserving the safety of complex, high-risk systems (pp. 199–216) [55]. Further, the author accepts Prof James Reason's idea of latent error that it is intimately bound up with the character of technology and accepts that tackling latent errors by identifying resident pathogens is the most effective way to improve the safety of complex systems (pp. 174) [55]. Prof Jens Rasmussen (1994) and his co-workers raised the question: are managers willing to spend the effort required for effective risk management? They argued senior managers like chief executive officers (CEOs) may not possess competence to deal with discipline of system safety management as they are usually drawn from finance or legal background (pp.159) [52]. System safety practitioners are to be found at lower levels in organisation in situations where the mean time between fatal accidents is large and the tenure of CEOs is short. In other words, CEOs do not get feedback on their performance in the field of system safety risk management. Further, they argued that Prof James Reason's approach will encounter problems if large number of 'less than adequate' conditions or decisions are identified from the past accidents using causal trees included in the Management Oversight and Risk Tree by William Johnson. However, applicant shows how the problem of representing various less than adequate latent failures by way of fault tree representation, taking into account the less-than-adequate decisions, is shown by the case study later on. This will show where interventions may be necessary.

It is common to observe three strategies to manage risks of fatal accidents [2, 52]. The strategy of emperical safety control used in the traffic and work domain is based upon 'safety on the average' for high-frequency and low-consequence traffic accidents. The problem with the strategy is that these measures may be degraded if the organisation is under economic pressure. Author finds that Network Rail's approach to change the specification of a signalling cable without checking for unsafe conditions that may be generated during operations is one example from the railway domain of this tendency to buckle under economic pressure as it

was done in 2011. Risk management strategy of making design improvements after learning lessons from investigation of medium size, infrequent accidents is practised within the railway and aircraft domains. The third, risk management strategy followed is through the control of hazards based upon use of multiple barriers or defences as in the nuclear domain based upon predictive risk analysis (pp. 35–159), [52]. Prof Trevor Kletz argued that organisations suffer from lack of memory in 2003 [38]. An UK Health & Safety Executive (HSE) Publication HSG 238 argued that safety-related control systems are bound to fail if the errors in the specification, design, testing, commissioning phases (lifecycle factors) of control systems are not checked and corrected [72, 73 ,74, 75]. Prof Nancy Leveson presented a new control systems engineering method, named STAMP, for accident analysis, which included representations of legal, socio-technical systems as well [40]. Knut Rygh, Chief System Safety Engineer, Accident Investigation Board, Norway, stated in 2005 publication that it is an establised fact that a systematic safety assessment is an accident investigation before the accident occurs (pp. 90–108) [63]. It follows from the foregoing research facts that an occurrence of incident or an accident implies that system safety case which documents the results of potential accident has either failed to investigate the potential hazard in a thorough manner or system case documentation ignored the hazard that could occur in the operations or lessons learnt from past accidents were forgotten or unknown dangerous unforeseen mode of operation has occurred or incident reporting system has failed or failures in risk management process were ignored or the independent safety analysts organisation has used the safety target of Mean Time to Unsafe Failure for safety case without using HAZOP + Fault Tree Analysis in the safety analysis of complex systems [29, 33, 34]. Prof Derek Hitchins (2007) stated that systems engineering cannot be carried out by the method discovered by Rene Descartes; dividing the problem space into its parts to analyse the parts and a holistic method as a frame of reference is necessary [28]. Following the financial crisis in 2007/2008, the idea of Black Swan event was popularised by Prof Nicholas Taleb [36]. Prof John Adams (2009) argued that economics of safety is a debate that is not settled as moral attitudes towards risk management are not stable; they depend upon the individual or social cultural perspective invovled in the debate [1]. Nobel laureate Daniel Kahneman (2011) argued that senior executives lack robust decision-making process and are prone to committing same errors like others as well [36]. Further, most railway, household kitchen, and weapons system projects fail to attain their objective due to planning fallacy as noted by him drawing upon the evidence of 2005 Oxford study. Prof David Hand (2015) argued using the evidence of 2008 financial crisis that risk inherent in the finance operations is better handled by Cauchy distribution as the decision-making framework of Gaussian means and variance leads to under-estimation of fat-tail risk events. During the financial crisis in 2008, it was revealed that Goldman Sachs's Chief Financial Officer (CFO) reported 25 standard deviation events occuring in a row in their operations [26]. Readers may wish to look up the probability of 25 Sigma event on the freely available online website – Wolfram Computational Engine. This works out to be 6.113 E-10^{-138} or a chance event of obtainning a head in all tosses of 456 fair coins. These rare events have occurred several times during the course of the past two decades. This failure in understanding risk is labelled in the safety risk literature as latent error. If latent errors are not cognised, then there is no way to address them. Therefore, switch to Bayesian risk management is required. However, Prof David Hand's work illustrates how abuse of statistics can occur [26].

http://dx.doi.org/10.5772/61527

The following are the definitions for latent and active errors.

Definition: Active errors are human errors, whose effects are felt almost immediately. For example, a road user may enter a level crossing space when it is not safe to do so due to wrong-side failure of the level crossing as in the case of the Herefordshire level crossing accident in 2011 [2, 11].

Definition: Latent errors are human errors whose adverse consequences may lie dormant within the system for a long time, only becoming evident when they combine with other factors to breach system (production) defences. For example, wrong-side failure event of the level crossing caused by the signaller who raised the barrier needed a conjuction of events of lack of approach locking and a road user entering the crossing space simultaneously to manifest the Herefordshire level crossing accident in 2011 [2, 11]. The independent accident investigating organisation, RAIB, reasoned, by way of counter-factual reasoning, that if the level crossing were to be fitted with approach locking facility, then the signaller would have been prevented from raising the road barriers, after they have been lowered. The causal statement was accepted by all organisations invovled in the situation according to the intutive frame of reference in the language of Prof Jens Rasmussen. Rather than questioning the scenario as to why the train did not stop at the level crossing signal fitted with Train Protection Warning System (TPWS) when stop signal was replaced, RAIB remained satisfied with the answer they found [2]. Based upon behavorial research discussed earlier, lack of cognitive reflection is implied and author concludes that this is a sign of irrationality. In human error terms, this act of omission can be called violation by element and duty holder as well.

Now, let us look at the other reasons for failures to recognise latent errors. First, lack of familiarty with the cognitive system engineering approach advocated by Prof Jen Rasmussen and his co-authors in the railway domain signalling and telegraph, human factors, safety and risk experts [52, 54]. Consequence of the lack of familiarity is the exclusion of certain stakeholders organisations' contribution to risk. Prof Jens Rasemussen's approach demands that cognitive system analysis shall include all stakeholder organisations and their contribution (positive or negative) towards system safety performance must be represented. These contributions are captured by way of a graphical representation in the form of Accimap [32, 52, 54]. Evidence for the lack of familiarity of contribution of human errors in management field can be seen in the case of the popular quantitative risk assessments made up of fault and event tree model. These representations are used by industrial practitioners for identifying accident precursors to safety risk, but do not include latent errors [24, 56]. The latent errors are errors committed in the areas of risk policy, domain-specific safety standards, which are industry consensus standards, and ignore errors in system design, risk assessments, independent safety assessments and reviews, and risk management that lead to less than sub-optimal diagnosis of potential or actual hazards. And as a result, risk assessors and managers pay less attention to less than adequate barriers for controlling hazards can be seen from the documentation on hazard analysis, modelling, risk analysis, and management of individual and societal risk concerns [17, 24, 60, 61, 72, 74, 75, 77]. Recommendations from the UK HSE Guidance on safety relevant control systems are not followed in these documents [73, 74]. When accidents do occur, front-line staff or members of public get blamed for less than adequate designs with which

these actors have to grapple as it can be seen in the case of assertion made in the publication by a team of railway signalling and train driving managers and this blame culture was investigated as well [25, 80].

All psychologists hold the thesis that human mind cannot estimate the probabilities or likelihood of rare events which lie between the interval of zero to one percentile and ninety-nine percentile of distribution of probabilities and errors in judgements arise due to basic inability in human thinking (pp. 315) [36]. Misconceptions of chances and lack of recognition of co-variation do occur in the railway industry is asserted by the author following Prof James Reason's work. For example, collision of a train with a vehicle on the track was regarded as once-in-a million kind of chance event by a member of public is cited by Prof David Hand [26]. The author found that the probability of Hixon level crossing accident was reckoned by S. Hall, a British Rail signalling expert (1991)to be one in a million kind of chance event [2, 11]. However, the RSSB (formerly Rail Safety and Standards Board) Report tells a different story of high likelihood of more than ten collisions events per year [59]. If readers think that progress may have been made since 1990s, then they will be disappointed to read that errors in risk modelling by Network Rail/RSSB All Level Crossings Risk Model were reported in the UK House of Commons Report in 2014 [71]. Combining two pieces of information such as RSSB's statistical data with the causes identified in the RAIB accident reports poses a problem of inferrring causes of level crossing accidents. This problem is logically equivalent to the problem of applying Bayes rule to the taxi-cab problem cited in the risk literature (pp. 166–167) [36].

Second explanation is that the majority of railway domain experts, i.e. engineers and managers, are not aware of errors in their statistical, economical, logical, ontological, and cosmological reasonings of railway accidents [26, 32, 36, 42, 50, 55, 67].

For example, if reliability, availability, maintainability, and safety properties of systems and human actors forming part of a given social-technical system are considered in an unified manner, then it is clear they are not to be treated as independent parameters as it is assumed in classical economical theories is demonstrated by sociologist Prof Charles Perrow and system safety theorist Prof Nancy Leveson as well [40, 49]. Prof Charles Perrow argued that errors in sub-systems in the system lifecycle factors may interact in unforseen ways; and as a result of these unwanted interactions, risk of an accident cannot be foreseen and pre-determined. Therefore, some high-risk technologies like nuclear plants that are prone to acccidents should be avoided. Rare events like nuclear power accidents require more time to manifest not withstanding the claims of risk assessors and managers to the contrary [13, 17, 49, 57]. The author found this reasoning to be true in the cases of NASA Space Shuttle Challenger and Japanense Nuclear accidents where errors in risk assessment led to under-estimating of fatal risk in terms of its likelihood [5, 6]. RSSB does not apply the requirements in the risk guidance from cognitive perspective issued to the industry to itself and fails to identify risk in its management systems are shown by the case study in the paper [58, 59, 60, 61].

The author is led to the insight on human and scoial cognition, drawn from works of Nobel laureates Herbert A. Simon, Daniel Mcfadden, and Daniel Kahneman, that cognitive errors in information processing activity do exist [36, 42, 55, 67]. Insight drawn from the work of Nobel laureate, Herbert Simon (1978), is that the fundamental limitation of human cognition

http://dx.doi.org/10.5772/61527

in organisational context gives rise to *satisficing behaviour*: tendency to settle for satisfactory rather than optimal courses of action; this is discussed in the text on the topic of bounded rationality in Section 3.3.1 of the Chapter 2 on cognitive science tradition by James Reason [55]. In the same text, Reason observed that this is true for both individual and collective decision making and cites Cyert and March (1963) who demonstrated organisational planners are inclined to compromise their goal setting by choosing minimal objectives rather than those likely to lead to best outcome. Organisational behaviour needs to become the focus of attention [15]. Two examples of the necessity to focus on this social tendency to compromise goals can be read from the evidence of failure of the High Speed 2 Business Case in the UK House of Lords Economics Affairs Committee Report and failure in the case of Chinese ERTMS Train Crash [14, 68].

Third, Prof James Reason advanced the idea of controlling safer operations by identifying the pathogens hidden in the senior and line management decisions and practices that feed into psychological precursors of unsafe acts is the best way of controlling safer operations [55]. These hidden pathogens are best discovered, as per the author's knowledge, by using the Management Oversight and Risk Tree to include human failings in risk assessment, risk management, engineering management, and investment management. This idea is supported byProf Jens Rasmussen as well. The problem of determining the risk in a qualitative or quantitaive manner is subject to professional biases is noted by Prof David Ball in the UK HSE Research Report 034 on how to understand and respond to the societal concerns. He observed that a risk management strategy cannot be promoted without a belief that one way of life, or one way of sharing risks and costs, is better than another [73]. Questions of will to impose harm on others and acting under ignorance are philosophical questions if we disregard the legal and bounded rationality perspective for a moment [66, 67]. Acting upon information generated by FN curves by means of RSSB's Safety Risk Model or FN curve data analysis without taking into account decision-making under uncertainty is an error is noted by Prof Andrew Evans in his study of transport accidents. The literaruture by Prof Andrew Evans shows how FN curves are constructed [76].

The HSE Report 034 had emphasised the need to incorporate plural views into decision making, while acknowledging that these will be based substantially on beliefs, values and ways of categorising the world, rather than upon objective information [73]. Role culture plays an important role is shown by Prof John Adams as well. In other words, bias will unavoidably be encountered, and ultimately the question may well come down to choosing one form of bias over another. Further, the following features characterise risk-based decision-making:

- not all values are equal – some can be more thoroughly justified than others (moral philosophy) and some – when applied – produce better practical results than others
- a risk management strategy cannot be promoted without having an opinion that one way of life is better than another.
- risk management is essentially political – the only honest and open way forward is to admit this and embrace it

The Skills-Rules-Knowledge taxonomy advanced by Prof Jens Rasmussen is applicable to the co-operative archictecture of work which is applicable to the current regime of risk management within the Europe as well [53, 54, 55]. Duty of co-operation is mandated by the UK Rail Regulator as well [46]. Contrary to the advice that emerges from reading the management literature that safety and production planning should not be placed lower than finance and planning activity in the hierarchy of management concerns, it is common place to find economic concerns being prioritsed ahead of the safety concerns in the industrial context. From cognitive science perspective, this act of compromising safety is a violation (pp. 206), [55].

The cognitive biases and information processing flaws were identifed by Prof Andrew.P. Sage as well. These flaws affect information formulation for acquisition, analysis, and interpretation. These can be read from the works of Prof Andrew P. Sage [47]. These flaws are based on those identified in the works of 1974 Daniel Kahneman and Amos Tversky's paper [36].

The following are the biases that have come to the author's attention as a result of his own research on system risk assessment and management.

1. *Incomplete data*. Failure to include uncertainty in the scientific estimates of reliability, availability, and maintainability of digital signalling systems including communication systems as a whole. I know the report is damning, and it may be based upon solid evidence, but how sure are we? We must allow for that uncertainty in our thinking.

2. *Defence-in-depth fallacy*. Fallacy on the part of computing science experts who entertain the idea that graceful degradation of automated information processes (fault tolerant architecture) shall be fail safe as the automated system is designed to stop the process under control if in doubt over the data (how the computer will doubt its input data, its own logic, and the outputs it generated if it has no access to real world like human beings is not questioned?);

3. *Affect Heuristic and/or planning fallacy*. The transport programme has large benefits and no major costs. I suspect the affect heuristic. No one pays attention to the fact of failure of 90% of the large railway projects to attain the cost, and passenger targets has been cited in a 2005 study. The great and good in the company are agreed with the programme mission and they like their plans. I suspect *Affect* and *satisficing heuristic and planning fallacy* [36].

4. *Narrative fallacy*. The consulting engineer is learning too much from the recent £1 billion project success, which is too tidy. The engineer has fallen for a *narrative fallacy.*

5. *Out of mind out of sight bias*. The fault tree and event tree analysis of the train crashes do not show any management and technical errors. I suspect '*out of mind out of sight bias'.*

6. *Blame Game.* The train failed in the tunnel. The communcation between the trackside and train-based equipment did not take place in the degraded scenario due to operator error. The computer simulation did not test this scenario. I smell the 'blame game'.

7. *Gambler's fallacy*. Clear-cut information about the probablity of an event is not taken into account because people believe that chance is a self-correcting process, such that a

http://dx.doi.org/10.5772/61527

deviation in one direction will necessarily be followed by a deviation in the opposite direction. 'The shares have been falling for the railway firm, it is time to buy as the trend will reverse'. Gambler's fallacy can be seen as a factor in the explanation of Saint Petersburg paradox described in the literature.

The expected value of the game as a sum of the product of probability of loss or gain multiplied by the values of the outcomes considered by the decision maker(s) or taker(s) is poor psychology is noted by Nobel Laureate, Daniel Kahneman. These type of erroneous arguments can be seen in the case of level crossings [25].

8. *Illusion of Invincibility bias*. The supplier has announced a new train protection system which is designed to be fail safe and uses mutliple but redundant channels for information processing. Full moon effect on information processing is not recognized. I suspect 'Illusion of invincibility bias'.

9. *Expert's Subjective Risk Bias*. The supplier has furnished us the risk register for the anticipated risks. The hazard mitigation method is noted by the domain experts, but the method of hazard control is insufficent for the risk. I suspect 'Expert's Subjective Bias'.

Allais paradox: Norms of Expected Utility Theory and axioms of Rational Choice were violated due to certainty effect by expert statisticians and future Laureates in Economics in the following decision situation is cited by Laureate economist Daniel Kahneman (pp. 310–321) [36], (pp. 39) [55].

Decision I: choose 61% of £520,000 or 63% of £500,000

Decision II: choose 98% of £520,000 and 100% of £500,000

10. *Railway Senior Managers's Fallacy.* The train driver has the ultimate responsibility for the safety of the train and passengers and has to comply with signal commands. We have robust systems for recruiting, training, developing, and certifying the train staff. Our operating rules and regulations are robust. The train drivers can handle the emergency and normal situations with cognitive work load.

11. Our experience has shown that signalling systems are functioning correctly after the accident. I suspect 'Senior Manager's Fallacy'.

12. *Railway Engineer's fallacy*. Human intuitions are prone to errors and mistakes. Train driver's response is too slow for attaining productivity target. Let us automate the train driving task. I suspect 'Engineer's fallacy'.

13. *Instrumentalism Fallacy.* Give a small boy a hammer, and he will find that everything he encounters needs pounding. I suspect instrumental fallacy.

14. *Geometer's Fallacy.* Noble laureate and a physicist, Albert Einstein, in his phenomenalogical experience wrote that old geometers like Euclid dealt with conceptual objects (straight line, point, surface) but not really with space, such as was done later in Descartes's analytical geometry [20]. We must be careful of the lack of connection between geometry and physics. I suspect Geometer 'Engineer's fallacy'.

15. *Measurement Fallacy.* Risk not measured is not managed. Let us quantify the risk of rare events according to Poisson method and justify that it is acceptable as the greater good of the society is served by ignoring so-called wider human factors. I suspect Measurement Fallacy.

16. *Concrete Jungle Fallacy.* European and American city dwellers have a much higher percentage of rectangularity in their environments than non-Europeans and so are more susceptible to Muller-lyer illusion. Muller-lyer illusion occurs when two lines of equally long parallel lines with arrow tails placed at the end visually appear longer.

17. *Coherence Bias.* The plan to implement the requirements as a decision rule has been agreed by domain experts. But this plan fails to meet the decision criteria for cognitive adequacy and safety requirements. Warnings about the inadequacy are dismissed as soon as raised. The operator's inattention due to distractions in the environment to execute the task is ignored. I suspect group–think bias [4, 36].

18. *Fault and event tree analysis bias.* Goldman Sach's (error cited earlier) bug is not acknowledged by mechanical approach to change management in organisations without paying attention to the nature and behaviour of organisations and blindly relying upon methods like fault and event trees are prone to error [13, 16, 17, 25, 55, 65, 78].

Some of the above latent human factors that may contribute to any of the potential ERTMS accident was noted by Sanjeev Appicharla in 2013 [6, 8]. The author refers the reader(s) to an excellent online 2010 report by Felix Redmill in the computing science domain on how to judge if the safety risks are ALARP via a decision-making process [57]. There is no unanimous agreement on the use of ALARP principle as per the UK House of Lords Report [77]. However, the Redmill's 2010 Report does not take into account all errors in information processing of choices revealed to us by economists and psychologists in general and Nobel laureates, Herbert A. Simon, Daniel Mcfadden, and Daniel Kahneman in particular [36, 42, 67]. The author does not subscribe to the idea automated risk assessement tools such as genetic alogrithms are of help. Readers may note that SIRI methodology is a engineering methodology to assist system and safety analysis of engineered systems by taking into account success and failure scenarios and based upon the theory of decision-making under uncertainty in the data and decision-making process [35, 37]. The challenges posed by problems of complexity, causality, overconfidence, human error, hindsight and outcome biases, bounded rationality, economic choices, cognitive limitations, out of sight out of mind bias, halo effect, omissions and oversight has to be met by any methodology to be used for decision making for the assurance of system safety risk management of complex engineered systems [55].

In this section, idea as to why some wrong approaches to safety risk management relying upon risk-benefit analysis or fault and event tree analysis or reactive risk management persist was discussed.

In the next section, the case study of ERTMS Cambrian Safety Critical Incident is taken up to show how the foregoing concepts are logically demonstrated in the case study of Cambrian ERTMS Safety Critical Incident.

http://dx.doi.org/10.5772/61527

3. Analysis and modelling of cambrian ERTMS safety critical incident

To manage the hazardous (potential or actual) situations, the different steps followed in the system and safety analysis as per SIRI methodology are as follows [3].

a. Developing description of an operational railway (system modelling process through architecture context diagrams, operational process diagrams, parameters diagram, and/or event causal flow analysis and agree emergent properties). This activity is usually carried out within a team and process is used to elicit domain knowledge through representation of diagrams such that a validated design or concept diagram is taken as input to the next stage of the SIRI methodology;

b. Identifying hazards (hazards identification process through hazard and operability (HAZOP) study, a team-based acitivity by HAZOP Chair);

c. Modelling accident scenarios (causal analysis process through Energy and Barrier Trace Analysis to identify harmful energy sources, victims, and barriers; failures of barriers detected through the application of Management Oversight and Risk Tree questionnaire and compare results with Skills–Rules–Knowledge Framework and Swiss Cheese Model to identify latent errors and develop the Hazard and Causal Factors Analysis Report. These tasks are to be carried by HAZOP Chair and Secretary)

d. Performing risk assessment and developing countermeasures (risk assessment process through Bayesian risk analysis and/or binomial distributions or Cauchy distributions to work out base rates, these results may be needed to be incorporated with MORT Analysis. Risk analyst and HAZOP Chair)

e. Preparation of impact assessment and documentation of results and release for stakeholders' consultation or peer review (impact assessment process, HAZOP Chair and MORT Analyst)

The last three steps may involve iterative process between them; processing of developing understanding may require intermediate stages to store the results on a draft version to revisit the branches of Management Oversight and Risk Tree (MORT) questions from engineering and risk management perspectives. A red, green, amber light marking system may be needed as each sequence of energy transfer process may need to be revisited. Further, as the original Management Oversight and Risk Tree in 1974 was developed with an understanding that at the design phase engineers and their managers will be able to perceive, concieve, and act upon the identified hazards before the close out of the design process [35, 37]. However, as the railway domain does not use the concept of affordance of harm from the system as a design criterion as required by human factors engineering process, it is necessary to consider various heuristics used by designers and operators and resulting biases that may arise at the design as well as operational time in the risk assessment, safety verification, and valdiation phases [5, 6].

It is assumed that HAZOP Chair and Risk Analyst roles will be performed by competent persons. In terms of meeting systems engineeering and safety standards set by engineering

institutions such as Institution of Electrical and Electronic Engineers – IEEE std 1220 or International Electro-technical Commission – IEC 61508 or sector-specific European Committee for Electro-technical Standardisation – CENELEC 50126, the two stage processes of system and safety analysis can be complied and implemented with the help of SIRI methodology [6].

To produce a model of an operational railway, the model should be able to reflect the real world closely. The operational railway includes several interfaces in all operational circumstances:

a. Man–machine interface (driver–line signals, signaller–automatic route setting, driver–train, etc.)

b. Machine–machine interface (interlocking – lineside signals, ATP-train brake, ERTMS-interlocking, ERTMS-fixed and mobile telephony, mobile telephony to ETCS, etc.)

c. Man procedures (operational procedures, work instructions, etc.)

d. Organisational interfaces (safety standards, failure management, hazard control between duty holders, between duty holders and industry bodies, between various types of organisations)

However, the present modelling languages suffer from a disadvantage in the sense that they tend to superimpose their own order on existing systems and fail to capture the rich partial order present in the system.

The application of the SIRI methodology to the incident situation under study is described. The RAIB Accident Investigation Report is used as the input document alongside the MORT (2002) questionnaire.

The RAIB Summary is reproduced here.

Shortly before 22:00 hrs on Sunday, 19 June 2011, a passenger train, travelling from Aberystwyth to Machynlleth, ran onto the level crossing at Llanbadarn while the barriers at the crossing were raised, and came to a stop with the front of the train about 31 metres beyond the crossing. There were no road vehicles or pedestrians on the crossing at the time. The immediate cause of the incident was that the train driver did not notice that the indicator close to the crossing was flashing red until it was too late for him to stop the train before it reached the crossing. Factors behind this included the driver's 'Increased work load' (his need to observe a screen in the cab at the same time as he should also be observing a lineside indicator), the design of the equipment associated with the operation of the level crossing, and the re-setting of the signalling system on board the train before it could depart from Aberystwyth. An underlying cause of the incident was that the signalling system now in use on the lines from Shrewsbury to Aberystwyth and Pwllheli does not interface with the automatic level crossings on these routes.

The RAIB has made six recommendations, three directed to Network Rail, two to Arriva Trains Wales, and one to the Rail Safety and Standards Board. These cover the development of engineering solutions to mitigate the risk of trains passing over automatic crossings which have not operated correctly; changes to the operating equipment of Llanbadarn crossing; the

http://dx.doi.org/10.5772/61527

processes used by railway operators to request permission to deviate from published standards; the operational requirements of drivers as trains depart from Aberystwyth; and the way in which drivers interact with the information screens of the cab signalling used on the Cambrian lines.

3.1. System analysis diagram

To enable, visualise, and reason about risk manager behaviour in general operating situation within the real world, the author has prepared an adapted version of diagram of Prof Jens Rasmussen's Skills-Rules-Knowledge Framework within Cognitive Science tradition. The diagram does not show actual mental world of an individual, but it is a model or a representation to be used by SIRI Analyst to reason about certain behaviour in philosophical, teleological, cultural, and scentific traditions of thinking and reasoning reflected in the literature on risk. However, it should be noted that this model does not reflect real truths. As Prof David Hand has written, one must revert to religion or pure mathematics for learning absolute truths [26]. It only shows a frame to reason about heuristics which allows response (automatic or reasoned) to the questions on risks or operator's actions in the real danger situation as well as shortfalls in risk or investment actions reasoned in the mangerial thinking.

To enable easy comprehension of the context of the UK railway industry operations, a system diagram is prepared. This is shown in Figure 1. This is an architectural context diagram (ACD) showing stakeholder organisations involved in the context of the Cambrian ERTMS Incident. From a systems engineering perspective, organisations forming part of the railway system are Network Rail and Passenger or Freight operating (not shown in the figure) companies, European Railway Agency, RSSB, RAIB are system supporting organisations whereas Department of Transport is the ultimate owner of the UK Railway System. Office of Rail Regulator, ORR, is a regulatory organisation. Element organisations like Alstom, Siemens, Ansaldo, Bombardier, Invensys, and Thales that supply signalling solutions are represented as contractors. Professional engineering societies which train, license, and certify individuals to meet the railway industrial needs are not represented in the diagram, but are recognised as institutions contributing to human capital development and as consequence to risk management as per Noble laureate and economist, Gary Becker's perspective [62]. Notified bodies or project safety organisations are treated as entities acting as contractors providing safety auditing, assessment, advice, and accreditation. The brief details of European Process validation and certification process is defined in the Section 5.5.3 of the uic Compendium on ERTMS [81].

From system analytical perspective, the definition of an organisation offered by Nobel Herbert Simon that organisations are adaptable systems made up of physical, technical, and human resources and exhibit what is known as 'satisficing behaviour' is accepted in this chapter [67]. The solid red lines in the above figure indicate safety critical interfaces and functions and dotted red line indicates influences emerging from accident investigations. Symbol 1 indicates ORR is legally independent of the Secretary of State. Symbol 2 indicates Passenger Focus is an independent body set up by the UK Government to protect the interests of passengers.

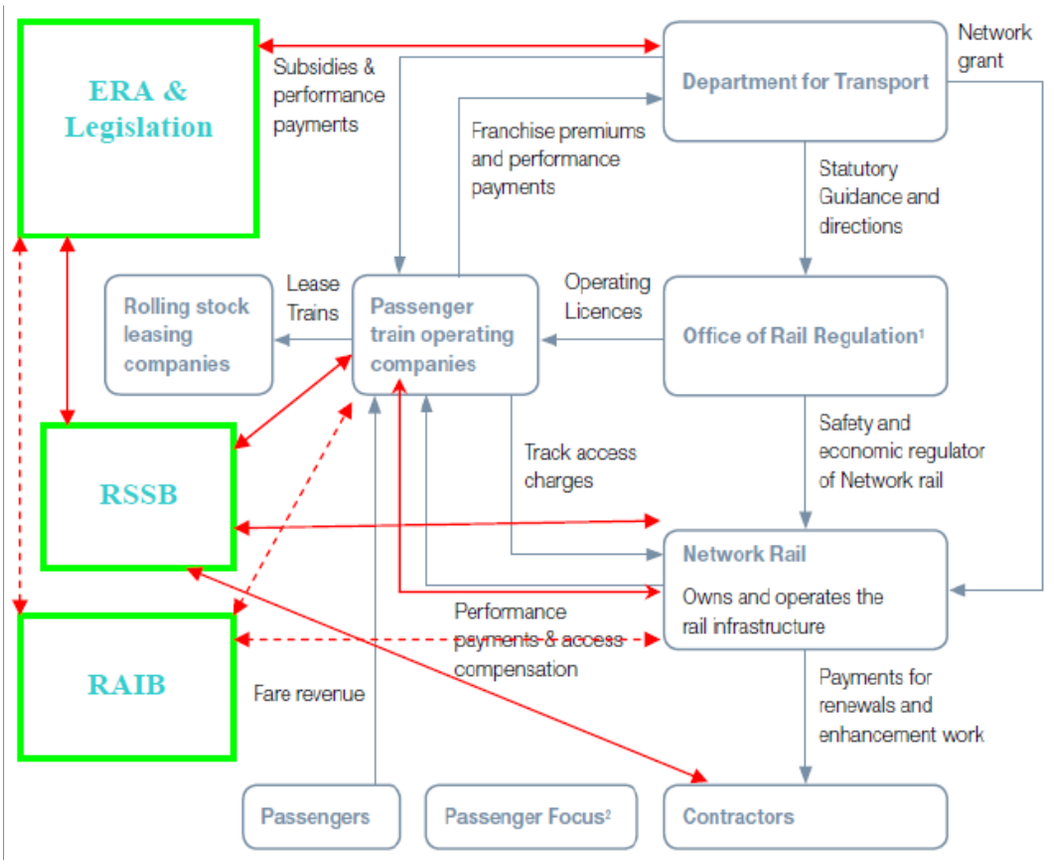


Figure 1. Architecture Context Diagram of the Railway Industry. Adapted from the UK National Audit Office Report (The UK National Audit Office 2010).

3.2. Hypothetical HAZOP study

The description of hazard identification and analytical methods used in the SIRI methodology is available in the published litearture. It is a hazard identification technique promoted by the UK Intuition of Chemical Industry in the early 1970s [17].

From the information gathered from the summary section, paragraph 95 and 177 of the RAIB Report, the critical interface between stakeholder organisations, Network Rail, the owner of the rail infrastructure and Arriva Trains Wales (ATW), the passenger train operating company at the operational time is the interface between driver's eye ball and the driver crossing indicator [51]. This is identified as Driver_ Perception of the Driver Crossing Indicator (DCI) and is the emergent property to be conserved in this study and operations as well.

The indicator was flashing red giving dynamic information to the train driver, but driver's response was delayed and the train did not stop ahead of the level crossing, indicating a safety critical deviation. From the SIRI methodological perspective, after Driver_ Perception is a safety critical deviation as the event of driver perception occurred after the braking point despite stopping ahead of the crossing space. Reading of the para 100 and subsequent text of RAIB Report suggests that signaller made mistake in setting the routes which led to a timing sequence problem, leading to the event of the opening of the barriers prior to the event of train

http://dx.doi.org/10.5772/61527

passing over the crossing space. The chain of events leading from this pre-cursor event is not discussed as the parameter of interest in the hypothetical HAZOP study is Driver_ Perception of the Driver Crossing Indicator in the sequence of events desired and its late occurrence. Suffices to note that signaller's error is a latent error and it is clear that human factor analysis of the signaller's task post implementation was not carried out. This is a latent error from the Common Safety Method's perspective as well [11].

Moreover, the design intent of ERTMS signalling automatic train protection (ATP) system is to provide the signal to programmable electronic system giving information on safe speeds and stopping points in Full Supervision (FS) Mode [82]. Thus, from the ERTMS signalling system function perspective, the emergent property which is to be conserved by trackside sub-system to on-board train system critical interface is Provide_ Signal.

But the national signalling infrastructure and human factors are excluded from the scope of Signalling Supplier's Consortium's (UNISIG) safety analysis. Further, the Compendium on ERTMS notes in Section 8.3.2 that the Index 47 document contained in the Chapter 6, risk analysis performed by two member states resulted in different interpretations of the hazard lists [82]. Given the fact that certain signalling entities and human factors are excluded, then the questions on the purpose of the European Train Control System(ETCS) *to provide the train driver with information to enable drive the train safely and to enforce respect for this information is* not satisfied if Driver _Perception _ Crossing Indicator is not included in the movement authority information. This discovery should provoke thoughts on the requirements management process used in the programme management of ETCS programes. This incident has shown that the design intent as per RGS GE/RT 8026 was not met [51].

The sample HAZOP worksheet for automatic train protection system adapted from the IEC 61822 standard for HAZOP study is shown in Figure 2. From reading the text in the para of the RAIB investigation, para 157 it is clear that the movement authority across the crossing was issued without stopping information ie No _ Provide_ Signal [51]. From this hypothetical HAZOP study and RAIB information, it is clear that trackside sub-system was not configured for the emergent property Provide_ Signal at the ABCL Level Crossings. If a real HAZOP study were to be conducted, then this failure may provoke thinking about the adequacy of study of failure scenarios and barriers as well.

Absence of the road user at the crossing space averted the potential accident. The real accident, if it had occurred, may have led to a range of outcomes with the loss of life as well as public and media outrage, if too many fatalities had resulted from it.

Figure 3 shows the schematic diagram of Llanbadarn ABCL facility. This figure may have to be zoomed to 180% or above to gain visual clarity. At the minimum, actions as planned under the risky scenario of raised barriers and stopping train front stopping 31 metres beyond the crossing space would have certainly resulted in a collision between the road and the rail vehicle, given the present understanding of laws of physics [48].

The absence of road user at the same time when the train passed the ABCL crossing space in error is judged by the SIRI analyst to be an 'act of God', as the intention of all stakeholder organisations such as regulating, specifying, developing, designing, manufacturing, supply-

STUDY TITLE: AUTOMATIC TRAIN PROTECTION SYSTEM								SHEET: 1 of 2		
REFERENCE DRAWING No.: ATP BLOCK DIAGRAM				REVISION No.: 1				DATE:		
TEAM COMPOSITION: DJ, JB, BA								MEETING DATE:		
PART CONSIDERED:				INPUT FROM TRACKSIDE EQUIPMENT						
DESIGN INTENT:				TO PROVIDE SIGNAL TO PES VIA ANTENNAE GIVING INFORMATION ON SAFE SPEEDS AND STOPPING POINTS						
No.	Element	Characteristic	Guide word	Deviation	Possible causes	Consequences	Safeguards	Comments	Actions required	Action allocated to
1	Input signal	Amplitude	NO	No signal detected	Transmitter failure	Considered in separate study of trackside equipment			Review output from trackside equipment study	DJ
2	Input signal	Amplitude	MORE	Greater than design amplitude	Transmitter mounted too close to rail	May damage equipment	Checks to be carried out during installation		Add check to installation procedure	DJ
3	Input signal	Amplitude	LESS	Smaller than design amplitude	Transmitter mounted too far from rail	Signal may be missed	As above		Add check to installation procedure	DJ
4	Input signal	Frequency	OTHER THAN	Different frequency detected	Pick up of a signal from adjacent track	Incorrect value passed to processor	Currently none		Check if action is needed to protect against this	DJ
5	Antennae	Position	OTHER THAN	Antennae is in other than the correct location	Failure of mountings	Could hit track and be destroyed	Cable should provide secondary support		Ensure that cable will keep antennae clear of track	JB
6	Antennae	Voltage	MORE	Greater voltage than expected	Antennae short to live rail	Antennae and other equipment become electrically live			Check if there is any protection against this occurring	DJ

Figure 2. Sample HAZOP worksheet for ATP system.

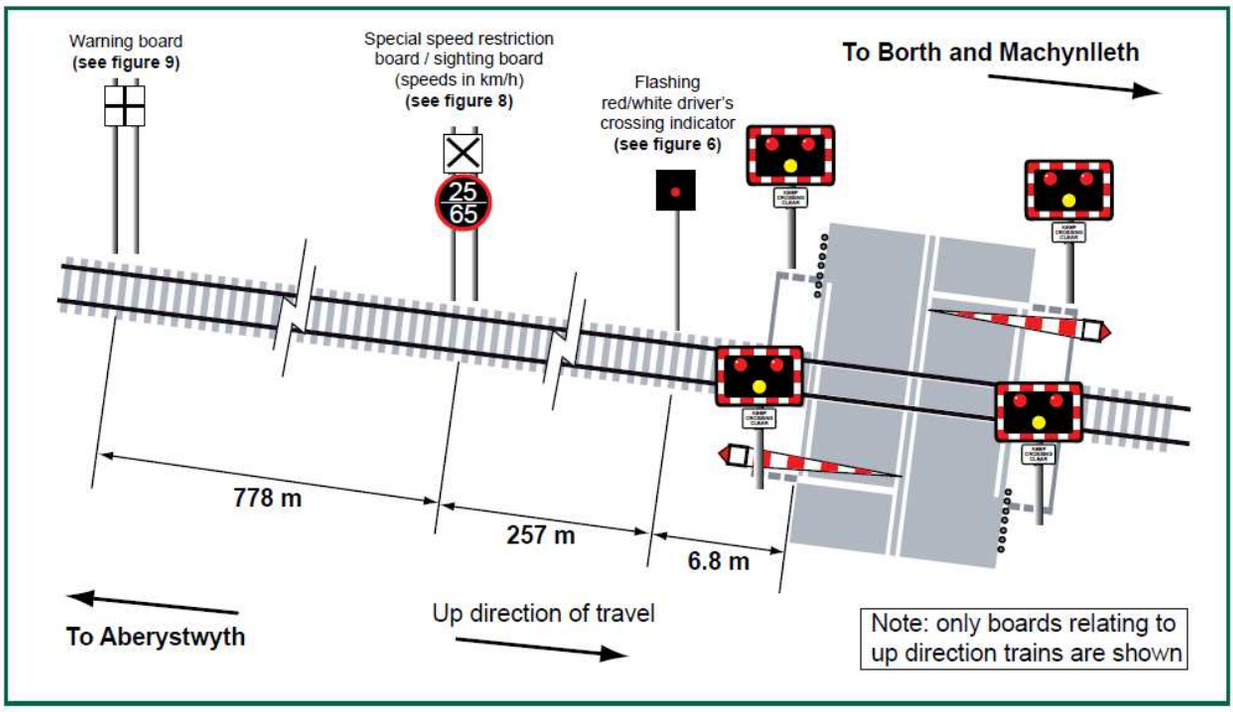


Figure 3. Schematic diagram of Llanbadarn ABCL.

ing, utilising, and maintaining the ABCL design is to allow road users (without committing an error) to pass through the crossing space when barriers are raised.

Non-provision of engineered safety feature in the contemporary ABCL design is a signalling engineering induced (latent) error at the RSSB Standards Committee Level whereas driver's delay in departing and arriving at the strike in point may be signaller (active) induced error.

http://dx.doi.org/10.5772/61527

The SIRI methodology adopts a system-induced error approach; and therefore, it is necessary to look at errors from a holistic perspective. The lack of compatability of requirements between Railway Group Safety Standard GE/RT 8026 and European Norm for ERTMS/ETCS System is a glaring omission in the area of railway safety risk management [46]. It shows intelligence failure on the part of all organisations. This type of failure was investigated in the GB Railway domain in 1976 by Barry A. Turner as well [78].

3.3. System safety analysis: Application of Energy Barrier Trace Analysis – EBTA, Skills–Rules–Knowledge (SRK) and Management and Oversight and Risk Tree (MORT) methods

Management and Oversight and Risk Tree (MORT) is an analytical technique for identifying safety-related oversights, errors, and/or omissions, or assumed risks that lead to occurence of an incident or accident [17, 35]. The MORT diagram uses of the logic of fault tree. It contains two main branches. One related to control of technical factors denoted by letters SB, SD, etc., which are leaves of the causal tree and representing system life-cycle factors. Another branch relates to management branch denoted by letters such MA, MB. Leaves within these branches are noted by lower case letters a1, b2, etc., which relate these events to questions listed in the MORT User Manual [17, 35].

The MORT Report contains following acronyms:

LTA: less than adequate

DN: did not

FT: failed to

HAP: hazard analysis process

The description of the concept of operations is drawn from the ORR documentation, RSSB Railway Group Standards, and is based upon the author's past experience of chairing HAZOP study at RSSB for generic ABCL facility and described using the generic Event Causal Factors (ECFA) analysis chart. This is shown in Figure 4. This may be required to enlarge till 180% to gain visual clarity on the computer screen.

The description of the expected event sequence to form a coherent description uses a particular notation of ECF analysis. The criteria to be used to read the event sequence diagram follows.

- Events must describe an occurrence, not a condition,
- Events must be described with at least one noun or verb,
- Occurrences must be precisely described,
- Events must describe one discrete action,
- Events are enclosed in rectangles and connected to other events as a forward chain using horizontal arrows,
- Conditions are enclosed in ovals and are connected to events by vertical arrows,
- Events should range from beginning to end of the particular method of operation,

- Each event should be derived from the one preceding event save for initiating event,
- Colour coding is used to distinguish infrastructure manager (IM), railway undertaking or train operating (RU) domain, and user domain,
- Events are labelled with number or letters to identify the sequential flow of events in respective duty holder domain.

The Concept of Operations describes the operational scenario when the train is approaching the warning board and the train driver is in vigilant mode of information processing. However, the desription of the incident RAIB (paragraph 110) informs that the event of approaching the warning board was delayed due to train entering Staff Responsible, SR, mode [70]. The ABCL being located near the station inserted a delay in the normal specification of the ABCL task analysis, and no separate task analysis was performed by the Railway Understaking (RU) in question. The time to approach to the level crossing space is specified in the form of a time interval and no account was taken in the variation in the time for the tasks to be performed by the train driver due to differernt operating modes was undertaken by RSSB before granting deviation to the safety critical requirements specified in the Railway Group Standard – RGS GE/RT 8026 [51].

This is a latent error embedded into the system where engineering and organisational errors are committed. This is an instance of *Railway Senior Managers and Engineer Fallacies*. Further, this latent error refutes the European Railway Agency, and RSSB's idea that the management and regulation of the railway is designed to ensure that – if each transport operator meets its obligations with respect the safety of its own operation and the state also fulfils its duties – then the sum of the parts will lead to a whole that is safe. Further, the RSSB statement does not fit the idea of systems thinking that whole is more than sum of its parts. This idea is entertained by system engineers as well as human factors specialists. Moreover, this error does not align with the Best Practice of Decisions Under Risk of Prospect Theory, which is acknowledged by RSSB in its July 2014 document [6]. Given the nature of the latent error, it is clear that this decision not to conduct workload assessment is a violation from RSSB's own Best Practice for Human Factors Risk and Safe Decision Taking [58, 61].

Given the Concept of Operations diagram which the author has developed, introducing timing analysis into the scheme is not a difficult issue if the data from the human factors engineering is included as well. From the direct inspection of events sequence described in the diagrams shown in the Figure 4, the expected event labelled E-IM-13 in the Network Rail domain flashing white aspect, and contrary to the expected event labelled E-RU-6 in the Arriva Train Wales domain, the red light was perceived, suggesting that the barriers were raised and an obstruction may be expected in the path ahead of the train.

Realising this fact, train driver applied brakes but the train did not stop short of the crossing. Since this constitutes a safety critical deviation, it is necessary to inquire further as to why the driver's response was slow and what shaped that behaviour. The train driver's action was a skill-based error type where the spatio-temporal response was delayed [12, 36, 55, 52].

http://dx.doi.org/10.5772/61527

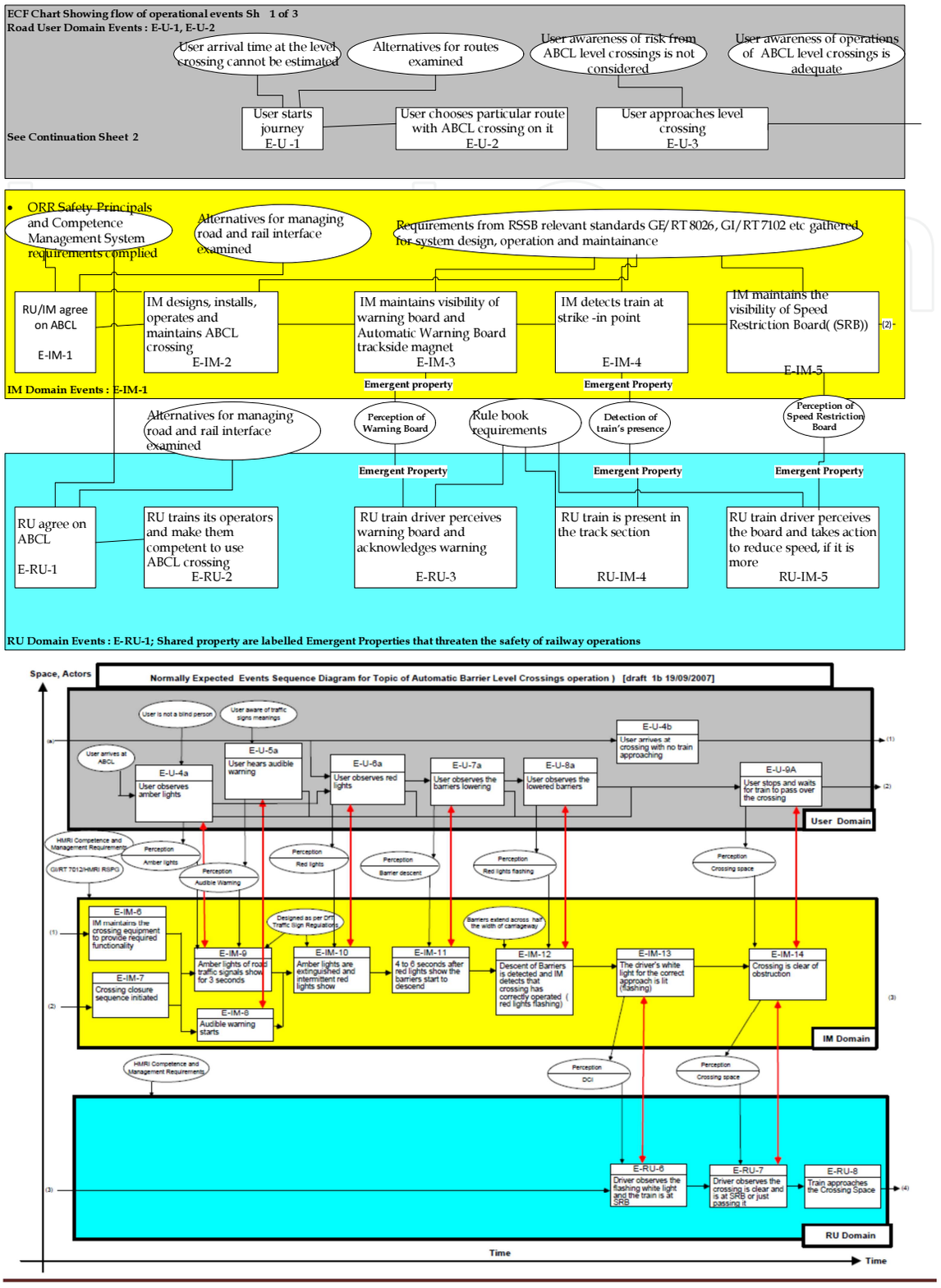


Figure 4. Representation of the concept of operations of ABCL Facility signalled by traditional lineside signalling

3.4. Energy barrier trace analysis

From the RAIB Report(s), the information available from the stakeholder organisations websites, the following worksheet is generated. This worksheet forms the starting point of the root cause analysis.

Harmful energy flow or harmful agent, adverse environmental condition SB1	**Target vulnerable person or thing SB2**	**Barrier and controls to separate energy and target SB3**
Kinetic hazard (train movement into the crossing space) when barriers are raised	None present at the time of incident	ERTMS Cab Signalling (not provided with movement and braking information when approaching level crossings) does not apply to national signalling infrastructure *(incomplete data for safety analysis).* Latent error: *status quo bias*
		Restriction on train speed (not provided with information at level crossings). Latent error: *status quo bias*
		Obstacle detection (not provided). Latent error: *habit bias*.
		Lifting barriers (provided) but not inerlocked with train movement. Latent error: *habit bias*.
		Approaching locking (not identified in the RAIB report). Latent error: *habit bias*.
		Interlocking system (did not provide function of locking barriers with train braking function). Latent error: *illusion of validity of driver's expertise.*
		Did not provide bridges, underpass, etc. Latent error: *illusion of control.*

Table 1. For Energy Barrier Trace Analysis (EBTA) worksheet

Logic of combinations may be applied to the following table. The author does not agree to the Pearson's idea that causation and correlation can be inferred in the same way [23].Credit to

http://dx.doi.org/10.5772/61527

God is given at the user level crossings where no indication of approaching train can be percieved or passenger manages to escape the accident [73, 74]. Otherwise, the table indicates that level crossings are accidents waiting to happen. This table can be interpreted again using the Prof James Reason's Swiss Cheese Model as well. The ECFA activity yields information on unsafe acts. But the precursor information on regulatory, organizational oversights is available from the EBTA and MORT charts.

It is clear from the foregoing particular description of the ABCL incident by RAIB, an ineffective system was deployed. The method of application of the MORT under the SIRI Methodology has been described in 2011 and 2012 [2, 6, 7, 9]. Call for replacement for bridges is not met easily due to failure on the part of social actors to percieve the risk correctly. Further erroneous interactions between distant components of Route Management System and level crossings user's intention leading to fatality at the level crossing site are noted in the accident literature [70].

To consider how and why the hazardous system was deployed and safeguards were not provided, it is necessary to apply the MORT questionnaire, as an organisation framework, to the RAIB report and related literature to arrive at all factors involved in contributing to the incident. MORT audit questionnaire is freely available online at www. nri.eu.com [35, 37].

3.5. Information on hazard causal factors: SIRI MORT representation

The application of MORT audit questions (2002 version) and the elicited following responses are characterised as human errors [35, 37]. Readers are requested to enlarge the images to make them readable. The Lessons learnt from the 2011 Incident and evidences drawn from the RAIB Report 11/2012 and 2010 RSSB Road and Rail Interface Report are described together with the evidence to support the reasoning in the form of a fault tree representation. The MORT Causal Trees for engineering and managerial are represented in Figure 5, Figure 6, and Figure 7. The hueristics and biases shown are not mapped to organisations involved in Figure 5. Such mapping may be carried out with the available information. The information contained in the MORT Top Tree derives from the managerial and engineering branches and evidences from the requirements for safety management system, generation, operation and maintenance of system safey case from UK and European Commissions Norms.

The inspection of the above diagram shows that how the hazards, and heuristics and biases involved in safety risk information processing at the knowldege -based level with a potential of loss of 32 lives with 99% probability as per standard Cauchy distribution with statistical median of 0.72 fatality per 1,000 ABCL level crossings and scale factor equal to 1 were not analysed. The neglect of base rates can be seen from the HS2 Risk Report [27]. Fault within fault tree analysis labelled as out of sight out of mind bias is self evident in this case study.

The mean weighted fatality rate of 0.72 fatalities for road vehicle passengers is taken from RSSB Report dated 2010 [60]. The basis of the calculations and more elaboration of the causal tree follows.

The information on the hazard causal factors will be appreciated when the information is placed in the frame of reference using the concept of operations diagram (see Figure 3).

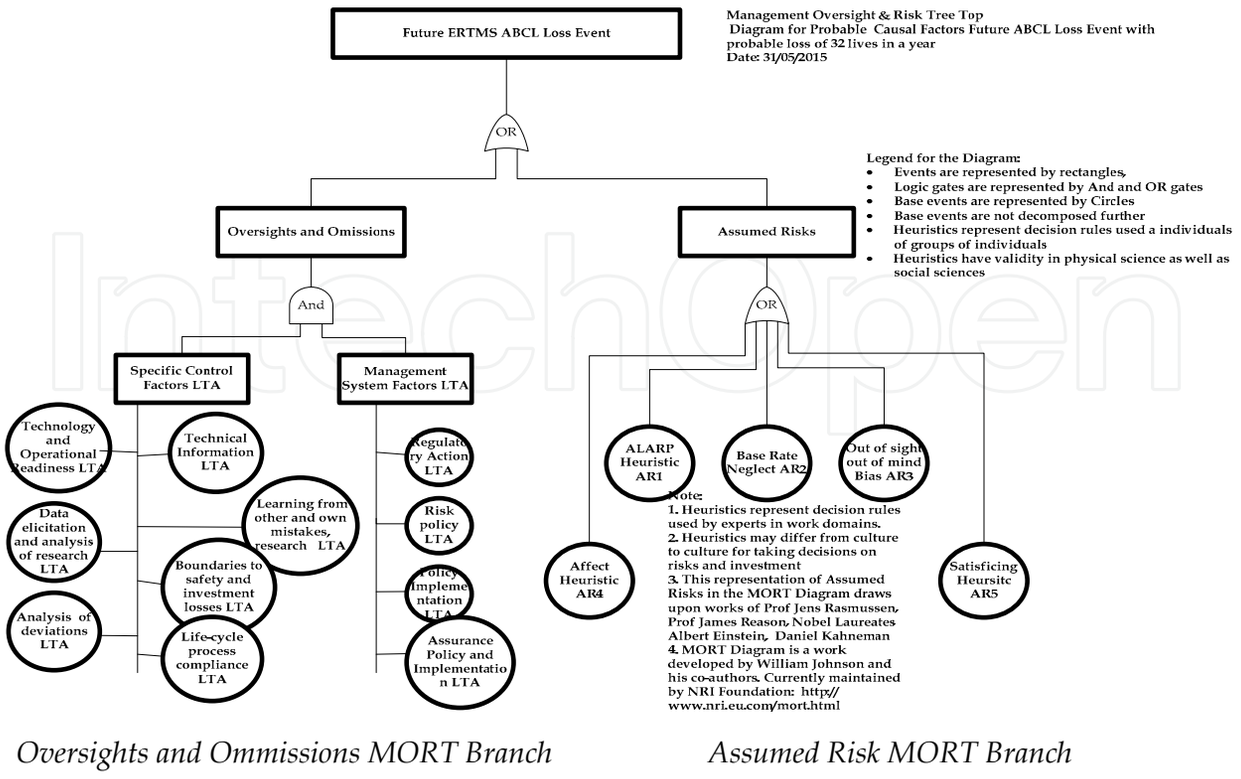


Figure 5. SIRI MORT Top Tree (Page 1)

It should be noted that ERTMS Safety Experts do acknowledge that Command Control & Signalling Technical Interoperability Specification (TSI) cannot itself gaurantee the safety of system since the National Part of Signalling System and an interface to it is outside the TSI Scope (pp. 206) [82]. The way to integrate man–machine interactions, operational rules, or non-inter-operability technical components into system safety analysis, as per the European Railway Agency, is to treat the safety performance of inter-operable constituents as a fixed factor and derive safety requirements for the non-TSI constituents. ERA arguments is that top down decomposition and allocation of probabilities ignores the human factors in risk assessments, fault tree analysis, and allocation of physical, human and social capital. The Consensus decision making process adopted at the RSSB Signalling Standards Committee level does not use any system analysis to detect conflicts between various types of requirements which give rise to human factor concerns. In other words, Group think bias due to assignable causes or optimism fallacy can manifest in such decision settings due to systematic human failings in lack of systems engineering process in specification of safety requirements, risk analysis & modelling and human factors investigation. ERA is aware of incompleteness of the generic risk analysis but RSSB does not include human factors concerns.

Less than adequate competence of professional heads of signalling, risk assessment, independent review, operations, human factors, safety, and systems engineering disciplines at regulatory, safety, duty-holder, supplier and validation organisations is a natural conclusion that can be drawn from the case study. The Greek philosopher, Plato once asked who will

http://dx.doi.org/10.5772/61527

guard the guardians via Glaucon who thought it was absurd to consider their oversight (Plato's Republic). This was the original thesis stated by author in his 2006 publication [3]. The European Process for SafetyAuthorisation as defined in by Peter Winter in the UIC Compendium on ERTMS in 2009 for the safety certification did not assure the safety operability albiet technical inter-operability of components has been attained (pp.128) [81]. Identifying, interpretation of current state, evaluating of options, identification of target (safe) state, specifying the safety goal for the Cambrian ERTMS Implementation which forms five crucial stages of decision making of Skills-Rules-Knowledge Decision Model were less than adequate. The work groups invovled did not have the interest of public safety at the heart of their decision making activity (pp. 369) [49]. Management Oversight and Risk Tree's decision model provides the idea that noise generated by political rhetoric overshadows the signal of less than adequate design of level crossings. Author has observed the tendency on the part of safety organisations to club several safety and human factors engineering technqiues such as Hazop, Fault and Event Tree Analysis, Operator Task Analysis to conduct safety critical analysis and has raised this concerns with Chair of Human Factors Working Group of UK INCOSE set up recently [6]. The feedback on this document is awaited. However, the safety case for ERTMS/ETCS is difficult to generate using the existing safety management methods was argued by the author at RSSB in January 2010 [10].

Incomplete system definitions cannot be used for system safety analysis is learnt from the the literature of control systems engineering from the UK HSE Guidance Note HSG238 as well [73]. However, this vital fact has been omitted by RSSB research managers is learnt from reading this research paper published in 2011 [22]. In other words, if operator error and signalling technical error are contributory causes (ignoring latent errors) then to attain SIL4 target for the overall system, the state of being at risk due to technical and signalling equipment failure has to exceed one chance per hundred billion opportunities per hour. This is under the assumption train driver's behavior is logically equivalent to a low demand SIL2 system from past data and including effect of immutable human nature discovered by David Hume. [65, 66, 80].

In other words, human error rate has to exceed SIL4 level if we include latent errors as well. The question of conjunction fallacy naturally arises if the final cause of the hazard is to be investigated together with its material (national signalling failure rate), formal (failure rate of risk management system), and effective causes (failure of human factors), as per Prof Jens Rasmussen's idea of Aristoteleian causal representation as applied to hazardous events and theory of probability as well (36), (pp. 53) [53]. Thus, the idea of fat tail risk has escaped the attention of ERTMS specification writers, European Rail Agency safety experts, and safety risk experts at GB rail national safety bodies and duty-holders. This social phenomena is not new. Aircraft industry shows similar tendecies as well [13, 49].

The meaning of hazards management is restricted to storing information on databases rather than eliminate hazards can be seen from a metro railway project Report in 2009 [30]. Further, the idea of conjunction of random failure events of redundant information processors has been paid attention, but fat tail risk problem showing up as group-think bias is not entertained in the risk literature by ERTMS designers, regulators, duty-holders, and standard bodies as noted

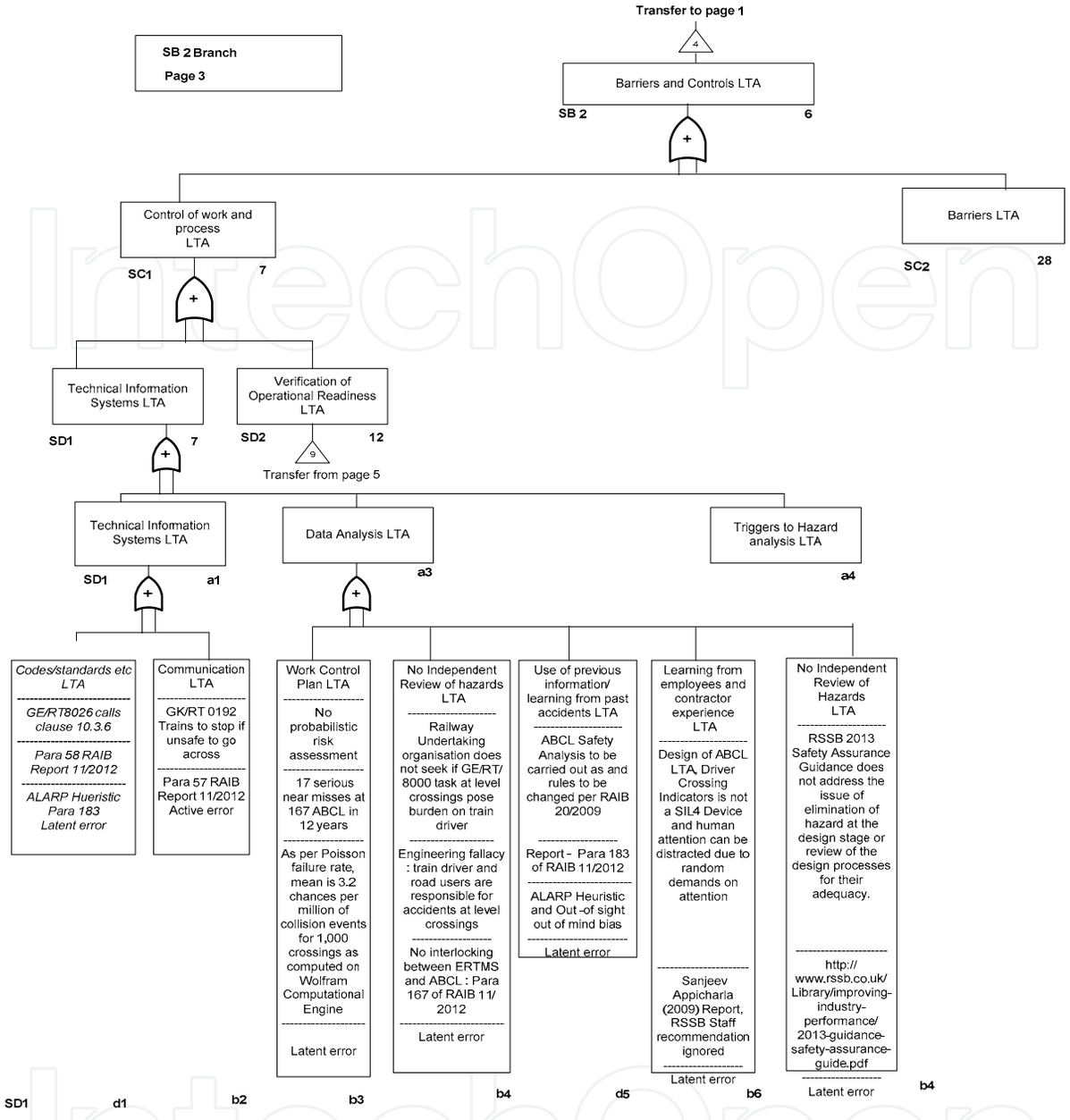


Figure 6. SIRI MORT SB2 Branch.

byNobel laureate Daniel Kahneman and Sanjeev Appicharla [4, 36]. Review of RSSB Safety Risk Model in 2012 did not refer to the errors that could occur in the usage of Bow-tie models as it has been shown in the accident investigation of loss of military aircraft, Nimrod in the Nimrod Report in 2009. Accident pre-cursor models do not include managerial, and engineering oversight and tendencyto assume risks can be seen from this review. Less than adequate technical review of fault tree analysis can be seen from this reference [24]. Further, the Review Report did not raise concerns over the subject matter experts using normalising constants in the risk equation as highlighted by Prof Paul Slovic [25, 36, 78]. Further, the familiar short-cuts have been taken to selecction of goals, task and execution of decision process as per Prof Jens

http://dx.doi.org/10.5772/61527

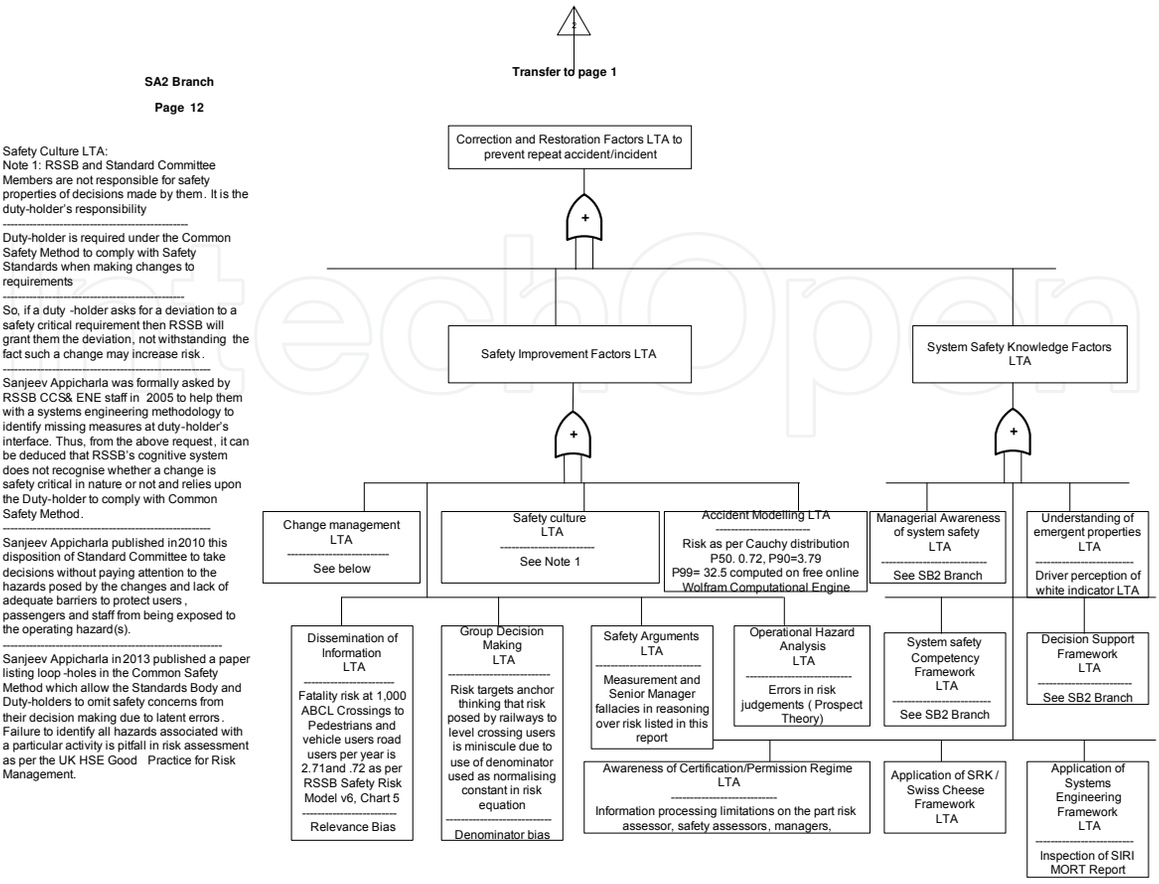


Figure 7. SIRI MORT SA2 Branch.

Rasmussen's SRK model of eight stage process of decision making and the potential hazard of train colliding with a road vechicle was not recognised by senior managers as per Prof James Reason's Swiss Cheese Model. The tendency not to eliminate risk within British Railway days is noted by risk and regulation expert, Prof Hutter [41].

The MORT results have shown the relevent hueristics and resulting biases incorporated into the MORT analysis shows a different risk picture than the expert railway safety and economic managers can imagine. An integrated analysis of quantified risk assessment, wider human factors via Swiss Cheese Model, and decision errors at the knowledge -based level called latent errors to show resident pathogens via cognitive systems engineering approach in an application of MORT is a novelty. This need is stated in RSSB Research Project calling for formal procedures to be applied to the task of assessment of rules and staff of RSSB as well [19, 2–11]. The decisions taken by various organisations show that these stakeholder organisations were not optimising safety for the road users, passengers, and staff.

The incident occurred as RSSB/Network Rail did not consider inclusion of level crossing functionality into the Cambrian ERTMS Automatic Train Protection System. The decision-making process used by RSSB Signalling Standards Committee for deciding upon the implementation of mandatory safety requirements specified within the Railway Group Standards was less than adequate as it failed to take into worst-case scenario of risk possible and the EU

Techncial Specification for Inter-Operability did exclude the functionality. The hazard analysis process used to close out the hazards failed to take into account wider and local human factors due to this exclusion [49, 55, 69]. Further, linear interaction between Design of the System with Operator (train driver and level crossing user) is not an hidden interaction in the work situationand therefore, from a complex systems persective, the ABCL Incident is simply a component failure accident [55].

4. Conclusion

The reasons for persisent use of wrong-but-popular approaches like cost-benefit analysis, and fault and event tree models for safety justification, identification of accident pre-cursors, and management of safety risk through independent safety assessment approach were presented in the chapter.

The Cambrian ERTMS case study has identified all engineering, managerial, organisational, and regulatory actions which have contributed to the ERTMS Safety Critical Incident using the SIRI methodology. The case study showed various heuristics and biases that were active in the railway industry. This is a novel use of hueristics and biases appraoch within the cognitive systems engineering tradition without omitting any stakeholder organisation in the SRK, MORT, and SCM analysis.

Acknowledgements

The author expressed thanks to the InTech publishers for invitation to contribute to the book. The author expresses thanks to anonymous reviewers for pointing out drafting and typographical errors in the text. Thanks are due to MORT team as well. Thanks are due to near and dear ones in the family as well. It is difficult to name every individual and organisation that has helped directly or indirectly in the production of case study.

Author details

Sanjeev Kumar Appicharla[1,2*]

Address all correspondence to: appicharlak@ yahoo.co.uk

1 Institution of Engineering and Technology, UK

2 International Council on Systems Engineering, UK

http://dx.doi.org/10.5772/61527

References

[1] Adams J. Risk Management; the economics and morality of safety revisited. Safety Critical Systems: Problems, Process and Practice. Brighton: Springer, 2009. 23–37.

[2] Appicharla S. Analysis and modelling of the Herefordshire accident using MORT method. International System Safety Conference. Birmingham: IET London, 2011. 10.

[3] Appicharla S. System for invesitgation of railway interfaces. International System Safety Conference. London: IET, London, 2006. 10.

[4] Appicharla S. System for investigation of railway interfaces. International System Safety Conference. Manchester: IET, London, 2010. 6.

[5] Appicharla S. Analysis and modelling of NASA space shuttle Challenger accident using management and oversight risk tree. 7th IET International System Safety Conference. Edinburgh: IET, 2012. 8.

[6] Appicharla S. Literature on Swiss Cheese Model and application to accident analysis and safety investigations, Unpublished draft September 2015.

[7] Appicharla S. Analysis and Modelling of the Fukushima Nuclear Accident 2011 using System for Investigation of Railway Interfaces. Cardiff: Eigth IET International System Safety Conference, 2013.

[8] Appicharla S. Revisting Avilability, Emotions, Risk. London: Upublished Draft, 2014.

[9] Appicharla S. System for investigation of railway interfaces. In: Reliabiity and Safety in Railways, 144–192. Crotia: http://www.intechopen.com/, 2012.

[10] Appicharla S. Safety Case for ERTMS/ETCS Signalling System, RSSB Unpublished draft,2010.

[11] Appicharla S. Technical Review of Common Safety Method using System for Investigating Railway Interfaces(SIRI) Methodology. Cardiff: IET International System Safety Conference 2013, 2013.

[12] Ashby WR. The nervous system as a physical machine with special reference to origin of adaptive behaviour. Mind New Series (Oxford University Press for the Mind Association) 56, no. 221 (1947): 44–59.

[13] Lawrence, B. Dr. A380 Aircraft Safety Process. London: IET System Safety Conference, 2006.

[14] Branigan T. Chinese anger over alleged cover-up of high-speed rail crash. 2011 July 2011. http://www.guardian.co.uk/world/2011/jul/25/chinese-rail-crash-cover-up-claims?INTCMP=SRCH (accessed Feb 18, 2013).

[15] Buchanan D, Andrej H. Organisational Behaviour, an introductory text. Hemel Hampstead: Prentice Hall, Europe, 1985.

[16] Busby J. Failure to mobilise in reliability seeking organisations; two cases from the UK railways. J Manag Stud (Blackwell Publishing Limited) 2006;43(6):022–2380.

[17] Clifton, E. II. A. Hazard Analysis Techniques for System Safety. New Jersey: Wiley& Sons, 2005.

[18] Daniels K, Jane H. Strategy Reader: A Cognitive Perspective. 2nd Edition. Oxford: Blackell Publishers, 1998.

[19] DNV Consulting. T220, Applicability of Formal Safety Assessment Process Approach to Rules and Standards Development within the Railway Industry. London: RSSB, 2004, 28.

[20] Einstein A. Relativity. London: Routledge, 1916–1952/2000.

[21] European Commission Directorate General For Transport. Master Plan for Development and Pilot Installations of the European Rail Traffic Management System. Brussels: European Commission, 1996.

[22] Bearfield GJ, Short R. Standardising safety engineering approaches in the UK railway. The Sixth International System Safety Conference. Birmingham: The Institution of Engineering and Technology, 2011. 5.

[23] Gopnik A, Laura S. Causal Learning, Psychology, Philosophy, Computation. New York: Oxford Unviersity Press, 2007.

[24] Haddon-Cave, Sir Charles. The NIMROD Review. An Independant Review into the Broader Issues Surrounding the Loss of the RAF NIMROD MR2 Aircraft XV 230 in 2006, London: Her Majesty Stationary Office, 2009, 587.

[25] Hall S, Van Der Mark P. Level Crossings. Hersham: Ian Allan Publishing, 2008.

[26] Hand, David. The Improbability Principle. London: Penguin, 2015.

[27] High Speed Two (HS2) Limited. High Speed Rail Cost and Risk Model. RisK Report, London: High Speed Two (HS2) Limited, 2009.

[28] Hitchins D. Systems Engineering. Chichester: John Wiley & Sons, 2007.

[29] Hubbard DW. The Failure of Risk Management. First. New Jersey: John Wiley & Sons, 2009.

[30] Hughes D, Saeed A. Hazard management. Hazard Management, System Safety-Critical Systems: Problem, Process, and Practice, Springer, Proceedings of the 17th Safety Critical Systems Symposium, Brighton, UK. London: Springer, The Safety-Critial Systems Club, 2009. pp. 23–37.

[31] Reason J, Hollangel E, Paires J. Revisting the « Swiss Cheese » Model of Accidents. Accident Model discussions, BRUXELLES: Eurocontrol Agency, 2006.

[32] Rasmussen J, Svedung I. Graphical representation of accident scenarios: mapping the system structure and causation of accidents. Safety Sci 2002;40:397–417.

[33] Camargo JB Jr, Almeida JR Jr. The safety analysis case in the Sao Paulo metro. Towards System Safety. London: Springer, Safety-Critial Systems Club, 1999. 110.

[34] Johnson CW. Reasons for the failure of incident reporting in the healthcare and rail industries. Proc Tenth Safety-Critical Syst Sympos. London: Springer-Verlag, 2002. 31–57.

[35] Johnson WG. Management Oversight and Risk Tree SAN 821-2. Washington D.C: US Atomic Energy Agency, 1974.

[36] Kahneman D. Thinking Fast and Slow. London: Penguin Group, 2011.

[37] Kingston J, Nertney R, Frei R, Schalllier P, Koornef F. Barrier analysis analysed from MORT perspective. PSAM7/ESREL '04 International Conference on Probabilistic Safety Assessment and Management. Berlin: Springer-Verlag, London, 2004.

[38] Kletz T. Lessons from Disasters-How Organisations Have No Memory and Accidents Recur. 2003. Rugby: Institution of Chemical Engineers, 1993.

[39] Janis LI, Mann L. Decision Making. New York: The Free Press, 1977.

[40] Nancy L. The need for new paradigms in safety engineering. Safety-Critical Systems: Problems, Processes and Practice. London: Springer-Verlag London Limited, 2009. pp. 3–20.

[41] Hutter MB. Regulation and Risk. Oxford: Oxford University Press, 2001.

[42] McFadden D. Economic Choices. 08 December 2000. http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2000/mcfadden-lecture.pdf (accessed March 09, 2015).

[43] Nagrath IJ, Gopal M. Control Systems Engineering. New Delhi: Wiley Eastern Limited, 1982.

[44] Nicholson M, Rae A. IRSE guidance on the application of safety assurance processes in the signalling industry (May 2010). Safety Critial Systems Club Newsletter (Safety-Critical Systems Club) September 2010;20(1):14–19.

[45] Office of Rail Regulator. Level Crossings, A guide for managers, designers and operators, Railway Safety Publication 7. London: Office of Rail Regulator, Aug 2011.

[46] ORR. ORR guidance on the application of Common Safety Method on Risk Evaluation and Assessment. London: ORR, December 2012.

[47] Sage P, Prof Andrew. Chapter 26: Systems Engineering: Analysis, Design, and Information Processing for Analyssis and Design. Mechanical Engineers' Handbook. Edited by Myer Kutz. John Wiley& Sons.Inc, 1998.

[48] Penrose R. The Road to Reality. London: Jonathan Cape, 2004.

[49] Perrow C. Normal Accidents. 1999. New Jersey: Princeton University Press, 1984.

[50] Peter N, Mohr C, Biele G, Hauke RH. Neural processing of risk. J Neuro-Sci 12 May 2010. http://www.jneurosci.org/content/30/19/6613.short (accessed March 12, 2015).

[51] RAIB. Investigation Into Llabardarn Crossing, 01/2012. Derby: HMSO, June 2012.

[52] Rasmussen J, Pejtersen AM, Goodstein LP. Cognitive Systems Engineering. First Edition. New York: John Wiley& Sons, Inc, 1994.

[53] Rasmussen J. Information Processing and Human -Machine Interaction: An Approach to Cogntive Engineering. Amesterdam: Elsevier Sciences, 1986.

[54] Rassmussen J. Risk management in a dynamic society: a modelling problem. Safety Science (Elsevier Science Limited) 1997;27(2/3):183–213.

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

[56] Redmill F. ALARP Explored No. CS-TR-1197. New Castle: University of Newcastle upon Tyne, 2010.

[57] Rosenbluth A, Wiener N, Bigelow J. Behaviour, purpose, teleology. Philos Sci 1943 Jan;10(1):18–24.

[58] RSSB. Good Practice Guide on Cognitive and Individual Risk Factors,RS/232 Issue 1. London: RSSB, 2008.

[59] RSSB. Road Rail Interface Report. London: The GB Railway Industry, 2010.

[60] RSSB. T169, Risk in Management Systems. London: RSSB, 2004.

[61] RSSB. Taking safe decisions. RSSB Risk Analysis-And Safety Reporting. July 2014. http://www.rssb.co.uk/Library/risk-analysis-and-safety-reporting/2014-guidance-taking-safe-decisions.pdf (accessed March 20, 2015).

[62] Becker S. G. Human Capital. 3rd. Chicago: The University of Chicago Press, 1964.

[63] Safety-critical Systems Club. Proceedings of the Thirteen Safety Critical Systems Symposium. System Safety, London : Springer, 2005.

[64] Schlosser E. Command & Control. London: Penguin Books, 2014.

[65] Schopenhaeur A. On the Principle of Sufficient Reason. Translated by Karl Hillebrand. New York: Prometheus Books, 1813/2006.

[66] Schopenhaeur A. World as Will and Representation. Translated by R.B. Halldane and J. Kemp. London : Kegan Paul, Trench, Trubner & Co; Ltd, 1818.

[67] Simon H. Theories of bounded rationality. In: Decision and Organisation, pp. 161–176. North Holland Publishing Company, 1972.

[68] The House of Lords Economic Affairs Committee. The Economics of High Speed 2, HL 134. Economic Report, London: UK Parliament, 2015.

[69] The Human Factor. 17 October 2014. http://www.vanityfair.com/news/business/2014/10/air-france-flight-447-crash (accessed March 04, 2015).

[70] The RAIB, Fatal Accident at Motts Lane Level Crossing, HMSO January 2014.

[71] The UK 2010 Parliament Transport Select Committee. Safety at level crossings Report 680 dated 7th March 2014. London: House of Commons, HMSO, 2014.

[72] The UK Health and Safety Executive. Research Report 034: Understanding and Responding to Societal Concern. Norwhich : Her Majesty's Stationery Office, 2002.

[73] The UK Health and Safety Concern. Out of Control. Safety Report, Norwich: Her Majesty Stationary Office, 2003.

[74] The UK Health and Safety Concern. Reducing error and influencing behaviour. The UK HSE. 1999/2009. http://www.hseni.gov.uk/hsg_48_reducing_error_and_influencing_behaviour.pdf (accessed Jan 25, 2013).

[75] The UK Health and Safety Concern. Transport fatal accidents and FN curves. Safety related, Norwhich: Her Majesty's Stationery Office, 2003.

[76] The UK Parliament House of Lords Select Committe on Economic Affaris. Government Policy on the Management of Risk, Fifth Report. London: House of Lords, 2005–06.

[77] TTAC Limited. Review of LU and RSSB safety risk models. Office of Rail Regulator. September 2012. http://orr.gov.uk/__data/assets/pdf_file/0019/5059/ttac-safety-risk-models-review.pdf (accessed October 30, 2012).

[78] Turner BA. The organisational and inter-organisational development of disasters. Adminstrative Science Quaterly (Johnston School of Management, Cornell University) 1976;21(3):378–97.

[79] Valerie R. The Upanishads. London: Penguin Books, 2003.

[80] Whittingham RB. The Blame Machine. Burlignton: Elsevier Butterworth-Heinmann, 2004.

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

IntechOpen

IntechOpen