6

System for Investigation of Railway Interfaces (SIRI)

Sanjeev Kumar Appicharla
[1]*Institution of Engineering and Technology*
[2]*The International Council on Systems Engineering, UK*

1. Introduction

This chapter presents an abstract system framework called ''System for Investigation of Railway Interfaces'' (SIRI), to study potential or past railway accident(s). The aim of the study is to learn about the multiple causal factors (elements or conditions) which represented together can be called a cause leading to the undesired state called potential or accident situation. Safety studies like SIRI can be used in conjunction with the quantitative risk estimation method (PRA) to help highlight or uncover decisions leading to assumption of unreasonable risk or human error in engineering and management factors needs to be studied. Author accepts the viewpoint of George E.Apostolakis on the utility of quantitative risk analysis (QRA) or probability risk analysis (PRA) techniques in general (E.Apostolakis 2004). The questions of human error and organisational learning are clarified later in the chapter in the context of acceptance of QRA method.

The SIRI Framework uses *synthetic* mode of thinking as opposed to *analytical* mode of thinking. Analytical mode of thinking is like decomposing water which does no longer contains anything liquid and has taste. The SIRI Framework synthesises multiple study methods into a cohesive process represented as a system. The study methods used in stages to arrive at the decision of a potential accident situation in an unambiguous manner are Hazard identification method (HAZOP), Event Causal Factor Analysis (ECFA), Energy Barrier Trace Analysis (EBTA), accident investigation technique (MORT), and cognitive human factors framework (SRK) and systems thinking integrated into a cohesive system framework. This is to facilitate the conceptual work of defining an operational system and inquiry into causal factors (individual, technical and organisational factors) to get an unambiguous feedback on the potential or actual accident situation. In this way, it is hoped that decisions, which might take operational situation outside the safe envelope due to groupthink bias or individual decision maker bias, may be detected at the planning stage or pre-design stage itself. Readers can gain access to the MORT user manual and related information from the NRI Foundation (Noordwijk Risk Foundation 1998). Need for analytical framework or multiple study methods are noted in the safety literature, but author wishes to cite two articles in support (Hovdon, Storseth and Tinmmanvisk 2011), (Hale, P.H.Lin and Roelen 2011).

This paper verified two theses accepted within the SIRI Framework. First, fallible decision making is the starting point of the accident sequence and is connected with the failure of foresight and/or not heeding warning signals, or where hindsight bias or groupthink bias dominates or lessons learnt are not applied or no lessons are learnt or not performing system safety analysis (B. A. Turner 1976), (J. Reason 1990), (Johnson.W.G 1974), (Wei 2008), (Kletz 2002). Second, it is possible to gain insight into the hazardous conditions or events that pre-disposes a normal act into an unsafe act in conjunction with local less than adequate defences in a complex system (Johnson.W.G 1974), (Briscose .G 1990), (IEC 2001), (Kingston, et al. 2004). Knowledge of past outcomes is not necessarily a good guide to future outcomes was established by Fischoff (1975) and this phenomenon was named as *hindsight bias.* The effect of *hindsight bias* and its two forms is cited by James Reason in his study of human error (J. Reason 1990). The concept of *impossible accident,* promoted by Wagenaar and Groeneweg (1988), is used to convey the idea that accidents appear to be the result of highly complex coincidences which could rarely be foreseen by the people involved (J. Reason 1990). The SIRI analyses of the Herefordshire Accident show that notion of *impossible accident* is not true in the case of level crossing accidents. Why? Because people involved in the decision making situation are prone to group think bias and prone to blame others in the projects and/or different organisations and rarely look at own actions which lead to bad policy or decision making (Goodwin 2006), (Whittingham 2004), (Weyman 2006), (S. Appicharla 2010), (S. Appicharla 2011). Re-evaluation of data and hypothesis is necessary to avoid confirmation bias. This can be seen in the case of scientists who assumed that the thesis nothing can travel faster than light. This thesis was falsified in the OPERA experiment. The summary of this OPERA experiment can be found in the science and technology section of the Economist (The Economist 2011). The two ideas learnt from Albert Einstein are: a) that time sequence of events experienced cannot be equated with the order of experience in time in the context of acoustical and visual experience; and b) physicists endeavour to eliminate psychical element from the causal nexus of existence (Einstein 1920). Contrary to the physicist(s) approach in the Einstein tradition, it is necessary to include psychical element and conduct the evaluation of technical as well as organisational aspects individually and re-evaluate them together in the safety studies (both accident investigation and project safety studies). However, no such re-evaluation was seen on the part of UK railway signalling industry in the case of the Herefordshire accident cited in this chapter. Author presented the Herefordshire railway accident case study based upon the principles of line side signalling perspective to verify the thesis accidents are due to ''satisficing behaviour'' displayed by the railway organisations. No case study is presented from a cab signalling perspective as an incident on a level crossing installed on the ERTMS signalled railway is under RAIB investigation. Details are given in the chapter later on.

The main thrust of this chapter is on the topic of taking a 'system approach to railway Safety' and is designed to:

a. help railway signalling engineers and managers utilise the framework as an independent system safety analysis methodology to help identify potential accident scenarios (system hazard) , detect and analyse the hazard causal factors and enable take preventive actions;
b. help post-accident/incident investigators utilise the framework to facilitate learning of lessons and help draw correct conclusions from a single event (incident or accident)

which occurred in the recent or remote past to identify and verify the thesis that conjunction of management and engineering oversights and/or omissions or the undue acceptance of risk were the causal factors behind the occurrence of the incident or accident.

The conceptual basis of the chapter is based on author's three published papers in the IET International System Safety Conferences and unpublished consultation commentary provided to the UK statutory body, the UK Law Commission in October 2010 (S. Appicharla 2006), (S. Appicharla 2010) (S. K. Appicharla 2010), (S. Appicharla 2011). Author's work experience, and learning from the past RSSB Research projects and study of related literature from domain of systems engineering, decision making, risk management, accident analysis and investigation, psychology, mathematics and philosophy have also provided necessary inputs. The concepts associated with the 'system approach to safety' which author wished to promote in conjunction with interested members of public are publicly available on the Wikipedia website (Wikipedia 2011). Demand for system approach is described in the safety literature as well (Elliot 1999).

This chapter highlights the application of the third step of the SIRI Framework. The aim is to support efforts to identify system hazard(s), and select amongst alternative solution(s) to deal with the identified hazard(s). Earlier application stages of the SIRI Framework were elaborated in the IET International System Safety Conference publications in 2006 and 2010 (S. Appicharla 2006), (S. Appicharla 2010)

The process of dealing with the hazards that arise with the implementation of the selected option can be dealt with by applying the same procedure or the procedure developed by Stephen Derby and Ralph Keeney (L.Derby and Keeny 1981). Stephen Derby and Ralph Keeney argued that the question of 'how safe is safe enough' cannot be answered using the subjective utility criteria (experts judgement) or using risk quantified in 10^{-7}/person/year risk or by performing value trade-off analysis as they do not satisfy the needs of collective decision making. They reckon that collective decision making is a problem riddled with ethical constraints. Any analysis of decisions on acceptable risk must ponder on social, technical, political and ethical dimensions. A similar observation has been made by the Royal Academy of Engineering on the matter of engineering ethics in practice. They have issued a long and short version of documents discussing the complications involved and the short version was accessed by author (The Royal Academy of Engineering 2011). Author has noted that there is a growing interest in the subject matter of philosophy in engineering domain.

The rest of the chapter is organised in this way. Section 2 defines the concepts used in the SIRI Framework. Section 3 presents a case study using the SIRI Framework to help understand its application. Section 4 states the problem statement which the solution has addressed. Section 5 summarises and draws conclusions on subject matter of the chapter. Section 6 acknowledges the help received from others. Section 7 provides the references.

2. Definitions of concepts in the SIRI framework

2.1 Cognitive systems engineering, affordance of harm and reality

The notions of ''system'' and 'systems engineering' are used in the way as they are defined by Benjamin Blanchard (Benjamin.S.Blanchard 2004). Systems engineering is taken to mean

the orderly process of bringing a system into being. A ''system'' comprises a complex of combinations of resources (in the form of human beings, materials, equipment, software, facilities, data, information, services, etc.) integrated in such a manner as to fulfill a designated need.

A system is developed to accomplish a specific function, or series of functions, and may be classified as a natural system, human- made system, physical system, conceptual system, closed-loop system, open-loop system, static system, dynamic system, and so on. Readers can refer to the work of Benjamin S. Blanchard and Wolter J. Fabrcky to learn the distinctions between analytical and synthetic mode of thought (J.Fabrcky and S.Blanchard 2005). For want of physical space, author cannot reflect upon the two modes of thinking in this chapter.

Author got familiar with the application of system approach in the social science field from reading the works of an economist, F.A. Hayek apart from its application in the thermodynamic field[1] and has argued an application in an unpublished paper in 1998 (S. Appicharla 1998). Subsequent to this, author has learnt that Herbert A.Simon's concepts of ''bounded rationality'' and ''satisficing behavior'' have influenced the works of Irving L. Janis, Barry Turner, Charles Perrow and James Reason as well (L.Janis and Mann 1977), (B. A. Turner 1976), (Perrow 1984), (J. Reason 1990). Herbert A. Simon's work was influenced by F.A. Hayek's concepts is gathered from the quote by Herbert Simon that no one has characterized market economy better than F.A.Hayek. Gary Baker, an empirical economist, acknowledges the influence of F.A Hayek in his work on Human Capital but notes that centrally planned and other such economies that do not make effective use of markets and prices raise co-ordination costs thereby reduce incentives for investments in specialized knowledge. Baker states that F.A. Hayek stated that… the problem of a rational economic order is….the utilization of knowledge which is not given to anyone in totality (Baker 1964). The division of labour is greater, in economies that make effective use of prices and markets to co-ordinate tasks and skills across firms. However, the case study presented in this chapter found that market economy destroys divine capital (it is assumed in this chapter that life is the work of divine capital) and no necessary investment into human capital is needed to prevent this destruction from occurring. In other words, as Charles Perrow argued the cost of transactions are borne by the wider society (Perrow 1984).

The concept of *cognitive systems engineering* is introduced by members of human factors engineering community, as an approach to describe and analyse man-machine systems. Daniel Woods, ERIK Hollnagel (1983) described the concept in a paper titled, ''cognitive systems engineering; new wine in new bottles'' (Hollnagel and David.D 1983). In that paper, they quoted Criak (1943) who remarked: ''If the organism carries a "small-scale model" of external reality and of its possible actions within its head, it is able to try out various alternatives, conclude which is the best of them, react to future situations before they arise, utilize the knowledge of past events in dealing with the present and the future, and in every way to react in a much fuller, safer, and more competent manner to the emergencies which face it''. An extension of this idea that a machine must possess a logical model of its

[1]Examples of system approaches such as heat flow balance modelled as differential equations can be gathered from standard text books on control systems engineering or from text books on Bayesian mathematical functions.

environment in multiple levels was discussed in the paper by Erik Hollnagel and David.D. Woods.

Prior to this, Barry A. Turner relying upon a similar concept of collective adoption of simplified assumptions into a framework of 'bounded rationality' helped deduced the fact that large scale intelligence failures are seen to occur in the organisational and inter-organisational practices prior to the occurrence of disaster. Drawing upon three case studies of public inquiries in United Kingdom, Turner hypothesized that a set of cultural beliefs about the world and its hazards in the social context and associated pre-cautionary norms set out in the laws, codes of practice, mores and folkways are the starting point of events in a process made up of 6 stages ending up with cultural re-adjustment. One of the public inquiry studied was the Hixon accident which is relevant in the railway context (B. A. Turner 1976). Earlier to this period, the concepts of organism, adaptive behavior and regulation in an environment were studied by Ashby (W. Ashby 1960), (W. Ashby 1960), (Ashby and Conant 1970). The concepts of representation of external reality as an object and the four roots of the principle of sufficient reason were discussed by Arthur Schopenhauer (Schopenhaeur 1820/2006). These set of ideas were followed by Leo Tolstoy (Tolstoy 1887/1930), and Alfred North Whitehead (Whitehead 1927/1978). Alfred North Whitehead traced the origin of these concepts back to the Buddhists whereas Arthur Schopenhauer traced the origin of these concepts back to the Upanishads. The principle Upanishads were translated from Sanskrit to English by Valerie Roebuck (Valerie 2003). Valerie Roebuck in the contemporary period traces the origin to pre-buddhistic Upanishad era in the fifth or sixth centuries BCE (Valerie 2003). Author has learnt from Jens Rasmussen and others that the concept of system coming into being can be traced back to ancient Greek times represented by Aristotelian notion of causation ((Rasmussen, Pejtersen and Goodstein 1994). The concepts of self or soul and external reality are mentioned by Aristotle in the ancient Greek times in the book VII on Politics (Aristotle 323 BC/1951).

The concepts of the Platonic world of mathematical forms such as squares, cubes, circles, spheres etc were recognized to be distinct from the corresponding approximate entities (substantial forms) in contemporary Greek physical world,and giving considerations to them in abstract form may give rise to a doubt whether the Platonic world of mathematical forms is 'real' (Penrose 2004) (Plato 375 BC/1995). However, these doubts can be dispelled when the fact that RSA algorithm relies on mathematics to support electronic communication between sender and a recipient in the public domain in modern communications is recognized (Singh 2001). The idea of relativity of time can be gathered from the BBC news headline that engineers can learn from the way slime mould searches for food resembled the 100 year old Tokyo rail network and the way it solved the problem of finding an efficient way through the maze (The BBC 2010). Mathematics cannot determine absolute motion since everything determined by it ends in relations by stating perfect equivalence between theories as in astronomy is a fact noted by G.W. Leibniz in his New System of the Nature (G.W 1695/1998).

According to Benjamin S. Blanchard and Wolter J. Fabrcky(2006), social groups organizing themselves possessing inherent abilities and the knowledge to maintain its stock of technology can be said to have civilization. They assert that modern civilizations possess pervasive and potent technical systems that provide products, systems, structures and services. In this sense, author asserts that both ancient and modern civilizations possessed potent technical systems

that can afford harm and benefits in the way they followed the norms. As an example, in the ancient Vedic civilizations, people carried out the sacrificial ceremonies which belong to the ritualistic portion of the Vedas to the letter without comprehending the spirit of sacrifice. This is learnt from reading the verses 3.10 to 3.13 of the Bhagavad Gita as translated and commented by Swami Nikhilananda (Nikhilananda 1944). It is accepted in this paper the truth which is stated in the Upanishad that there are three kinds of adversity: fever, headaches etc arising from disorder of the body(internal) , arising (from) external objects, such as tigers, snakes; arising from the action of great cosmic forces, such as those cause rain, storms, or earthquakes. Similarly, prosperity is of three kinds (Nikhilananda 1944). For explanatory purposes, it is assumed that the actions cause results (the desired or undesired) observed which arise from the combination of three causes acting together: material cause, efficient cause and formal cause to give rise to the final cause (the desired or undesired) effect. This is Aristotle theory of causation (Aristotle, Ethics 350BC/1955). The Aristotle theory of causation bears a very close resemblance to the deductive science of Gunas (three modes of material modifications) articulated in the fourteenth chapter of the Bhagavad Gita and reading of the verse 3.27 which states that all work is performed by Gunas of Prakriti and the idea that Self is an agent is false knowledge (Nikhilananda 1944). Scientists and philosophers citing or drawing inspiration from the Sacred Scriptures is not an uncommon phenomenon. Sir Issac Newton held the view that both Nature and Scripture were presentations of God's message to man, which was to be learned scientifically or through the study of God's revelation as presented in the Bible and/or Koran. Newton in his Principia Mathematica, offered a version of the argument of design to show that we (critical reader may disagree) could know of God scientifically (Popkin H. R 1969).

Some examples relevant to the misery faced by the railway customers can be comprehended from the real world examples. Reading the news items about signalling cable thefts or the rats eating away the signalling cables, lightning causing signalling circuits to fail highlight nature of problems faced (Wainwright, 21 September 2011), (The BBC News, 27 September 2011), (The BBC News, 12 August 2011). To prevent erroneous conclusions that can be drawn based on the foregoing that wireless or radio communication based signalling systems provide better safety and security, a process with a pattern similar to the SIMILAR process is needed. The customer or beneficiary can be assumed to be members of local or wider society. Author had conceived the SIRI Framework in response to a request from the signalling engineer's request to help identify the duty-holder interfaces. The problem statement author started working from is given in the section 4.

2.2 Systems thinking process

A.Terry Bahill and Bruce Gissing asserted that humans (as individuals, on teams, and in organisations) employ simple processes to increase their probability of success. They argued that Peter Senge's Fifth Discipline, Shewart's Plan-Do-Check-Act cycle, Covey's 7 habits of highly effective people, Katzeban and Smith's The Wisdom of Teams, INCOSE Fellow Consensus on Systems Engineering Process and IEEE 1220 Systems Engineering Process shares the common roots of the SIMILAR process. These processes were mapped to the SIMILAR process to show them sharing common roots in systems thinking in the IEEE article (Gissing and Bahill 1998). Thus, the SIMILAR process would serve as a comparative benchmark for the SIRI Framework.

The SIMILAR process is stated in a very brief manner. A picture of the SIMILAR process is shown in Figure 1. It is concerned with logically consistent and effective means of planning and problem solving. The process starts with the stage of developing a system in an engineering environment to address the current deficiency and description of what function must be done or satisfied by the system. At this stage *what is* determined. This is State the Problem stage. With completion of the problem definition stage, the process moves to the Investigate Alternatives where the functional alternatives are searched to satisfy the problem statement. After the match has been made between the need and the solution to satisfy the need, a model is developed and is analysed to determine what is *to be*. At the Integrate Stage, the developed model or simulations etc are checked for the compatibility with the sub –systems to assure that interfaces exist between sub-systems for transferring the outputs/data/information as the case may be.

Inherent feedback loops between inter-connected sub-systems must be checked to minimize the exchange. Architects of the SIMILAR process assert that well-designed systems integrate sub-systems such that they contribute to whole direction of the system. Launch the System means running the system and producing the outputs. Assess Performance is the stage where the metrics are used to measure the performance. Terry Bahill and Bruce Gissing did not mention the qualitative aspects at this stage, but author reckons that both quantitative and qualitative aspects must be taken into account. The Re-evaluate is the feedback stage at each of the process stage to assess and evaluate the performance. Terry Bahill and Bruce Gissing reckon that repeated application of the process to systems, sub-systems, components in an iterative manner produces outputs similar to a fractal process. Further, the Re-evaluate Stage runs parallel to the main work streams of the SIMILAR process. Author wishes to clarify that the representation of the SIMILAR process does not represent causality. It should be noted the notion of causality applies to physical systems rather than social systems.

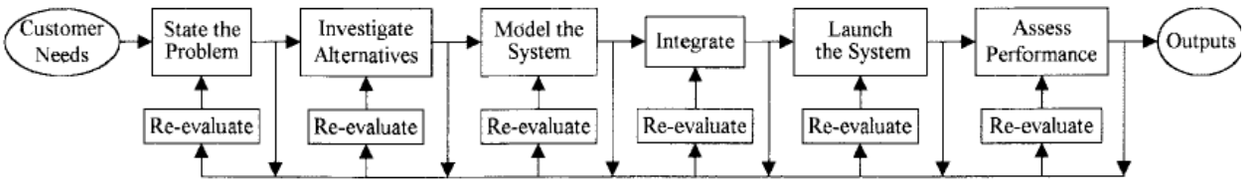


Fig. 1. A graphical representation of the SIMILAR process.

The perception and definition of a particular system, its architecture and its constituent elements depend on an observer's interests and responsibilities. One person's system - of - interest can be viewed as a system element or product in other person's system - of- interest. Conversely, it can be viewed as being part of the environment of operation for another person's system of interest. The basic definition of a system at the modelling stage can give rise to disputes. Mathematically inclined people would not agree to a definition of a system given in the new formed (during 1970s) soft systems engineering tradition (I.Mitrani 1982). The notion of a system and its definition can give rise to multiple interpretations can be evidenced from a recent publication in the UK railway domain as well (G.J.Bearfield; R.Short September 2011). However, author notes and agrees with I.Mitrani observation that motivation for modelling objective (from any kind of modelling activity) is that process of observing and learning from the real system in operation is too difficult, too hazardous or too expensive. This is the case

when a system is not yet built. Alternatively, the objective may be to assess the performance of the effect of a proposed major changes in an existing system (for example, addition of European train control systems, moving block systems, renewal of fixed block signalling etc).

The SIMILAR process does provide a basis on which such problems can be sorted out by describing a new process bench marked to a tested and agreed systems thinking process model. This is line with the thoughts of the architects of the SIMILAR process. Given that human behavior is fragile and fallible in nature, it is necessary that a systematic method that can transcend or overcome the errors in faculties of perception, cognition and judgments based upon limited, narrow professional expertise is necessary.

The SIMILAR process appears to cater to that need. However, in the case of safety problems, no stakeholder is in a position to outline the problem in a manner as it is expected by the SIMILAR process. Further, it is a matter of every day experience that man –made and natural system (s) do produce unwanted outcomes in the form of incidents or accidents. However, the SIMILAR process calls for multiple methods to be used is evidenced from the graphical representation of the process in the Fig. 1.

Many accident investigators or researchers have used models or methods to explain 'what' happened afterwards. However, system developers, owners and operators and maintainers are more interested in learning lessons and taking preventive actions in a cost effective manner. This paper presents a proactive approach by revealing the gaps in the knowledge of parameters that sit on the boundaries of the systems, sub-systems and components. These give rise to notion of a 'system hazard' which given the rights conditions can escalate to an accident.

From an energy perspective, harm arises from inherent danger in the sources of energy which have not been diverted into safe channels in the performance of work and its unsafe flow of energy is triggered by a change in the circumstances due to lack of awareness and/or risk taking behavior on the part of social elements of the system. Energy is a necessary ingredient for attainment of success of any system of work. This perspective focusses attention on the organisational factors, workplace factors and the individual factors and the state of barriers in the analysis of the sequential progress of accident sequence. The decisions taken at the work group level (or organisational level) provide for latent failure pathway if the hazard is not recognized at the planning of the work or in the standards that regulate the work processes. The Swiss Cheese Model SCM is used to trigger the analyst's awareness to check for organisational factors in the M Branch of the MORT analysis.

James Reason (2007) in his 18th Westminster Lecture on 'recurrent patterns in transport accidents' stated that there are three levels of accident contributors: universals (the ever present tension between protection and production), conditions and causes (the local factors that combine with certain conditions to breach defences in unforeseen and unforeseeable ways) (Reason J. , 2007). Reason's lecture was intended to pose more questions than provide answers. He noted that answers to the 'why' question are often found well 'upstream' in both time and space from the event: indicting the organisation, the regulator and sometimes the entire transport system. Author could not determine why this method of explanation should not be pursued from Reasons' perspective. Author's speculation in this area is that James Reason does not think re-engineering of a social technical system is a legitimate and feasible activity. Author notes that social technical system is a small part of wider geographical society which is greater than a local social technical system.

Author thinks that James Reason's research is countered by 17th Westminster Lecture given by Phil Goodwin on 'determination' and 'denial: the paradox of safety research and traffic policy (Goodwin, 2006). He gave three arguments for not taking action aimed at improving safety in the case of road transport. First, the trends will take care of the problems. This is the idea that the technical advance will solve all problems. Second, road driver behavior is unsafe and cannot be influenced. This is an example of 'law of unintended consequences'. And third, reducing collisions in one place is not due to anything due to human intervention, but a random effect counteracted by increases somewhere else. In the extreme form, this is an example of the view that universe operates randomly, and human agency is ineffective. He concluded his lecture by saying that his research led to the recurrent conclusion that the effects of policy on behaviour are bigger than has been conventionally assumed –behaviour does change, and substantially. This has been obscured from general awareness by biases in the form of data and models which have been influential, which has led to a continual underestimate of the potential both for making things better by good policies and making them worse by misguided policies (Goodwin 2006). The role of various biases in the failure of Incident Reporting Systems in UK has been studied by Chris Johnson (C. Johnson 2002). Author wishes to argue that the 'SIRI Framework' and 'STAMP' accident models fall under this category of models for safety improvement from cosmological perspective(analysis of cause-effect relations) (S. Appicharla 2011) (N. Leveson 2011).

Author notes that accident modelling from ontological perceptive (analysis of what is – ought to be relations) is studied by Why Because Analysis method which is advanced by Peter Ladkin based upon David Hume's philosophy (Ladkin 1995).

Fig. 2. A reference Model for Accident Analysis. Sourced from (Wkipedia 2011).

With basic notion(s) outlined above, the mapping of the SIMILAR process onto the SIRI Framework is provided in the Table 1. This is to argue the case that without sacrificing the core notions of the SIMILAR Process, it is possible to establish identity between two systems thinking processes. Author has learnt that the notion of systems thinking was part of the deliberations when Management Oversight and Risk Tree (MORT) was being developed by William Johnson and his team. Both concepts of system as composite entity made up of entities and as a systematic method for investigation as well were noted in the original MORT

documentation (Johnson.W.G, 1974). Prior to this notion of system made up of barriers, threats, regulator and essential variables was articulated by Ashby (Ashby W., 1956/1999), (Ashby W., 1960) (Ashby and Conant 1970). The SIRI Framework does re-use several of these concepts developed by Ashby and MORT team. Ashby used the example of adaptive behavior on part of a train driver in his treatise on Design for a Brain (W. Ashby 1960).

Claiming completeness of knowledge is a herculean task; however, using the principles of abstraction, refinement and information presentation in a careful manner, UK railway industry can make a claim that railways are safe to operate even under changing conditions. This is achieved by detecting all safety critical deviations possible in the system at the operational time and ensuring that safeguards are available to prevent those variations escalating into accidents. Author rejects the idea of safety case approach based upon formal approaches such Bayesian belief networks or compliance with railway CENELEC norms is sufficient unless the safety and electro-magnetic compatibility (EMC) is designed into the technical or operational systems based upon understanding[2] (B.Bateman, S.W. Hatton 2006), (Hughes,D , Saeed A, 2009). The idea that TBTC command for service braking distance function can be given lower safety integrity level SIL 2 than the TBTC command for emergency braking distance SIL 4 can be seen in the paper by S.D.Turner and a safety case has been prepared and accepted on that basis (S. Turner 2011). The way SIL targets are assigned to the command functions appear to be correct at first sight. However, a bit of thinking would reveal that if the output command for service brake function has failed then it is clear from the logic of IEC 61508 to note that distance computation or information available on train location is in error at the input stage of processing or algorithms for speed and location determination are in error. Over time, the distance to a danger point from a reference point on the physical track space at which the following train must necessarily stop does not always grow in size. Common cause failure analysis (CCFA) is a must as single point failure (SPF) destroys independent redundant designs is noted fact in the safety literature (Clifton 2005), (The UK Health and Safety Executive 2003) . In line with author's argument, a paper by Tim Kelly calls for a cautionary approach when preparing safety cases (Kelly 2008). EMC must be designed into system is argued by Armstrong (Armstrong 2006). Interpretation is necessary when safety cases are prepared strictly in accordance with the CENELEC norms is noted by an independent safety assessor (Skogstad 1999). Author asserts that analysis of safety property in the form of safety cases cannot be like banker's note which is issued by a firm which has nothing other than paper obligations to back it with. The notion of comparing safety case analysis with a banker's note is gained reading from of text on the page 123 of Arthur Schopenhauer's book (Schopenhaeur 1820/2006).

2.3 Emergent property, perceptions, causation, system safety viewpoint

The SIRI Framework adopts the cognitive science tradition of Rasmussen's skill-rule-knowledge framework and argues that measures to eliminate affordances for errors and harm are feasible in the railway context. The term affordance refers to the basic properties of

[2] Understanding is a technical term denoting a faculty which means causation from David Hume's perspective and this definition is accepted in this chapter. The Bayesian Belief Network, if used, should model engineering and managerial factors as well to meet the requirements of the risk management model advanced by Jens Rasmussen (Rassmussen 1997).

objects that shape the way people react to them. An artefact that is well designed should, through appropriate use of invariant features, make obvious what is for and how it should be used. Author is of the view point that the signalling systems and railway infrastructure in the context of rail-road interfaces or man-machine interfaces should be designed for errors assuming that active human errors do occur and eliminate error inducing situations from operations (J. Reason 1990), (S. Appicharla 2010). From a human factor perspective, a 24 element model made up of 5 elements of perceptive organ system, 5 elements of sensory motor organ system, 4 elements of cognitive system with 5 elements of vital systems of respiration etc is used to represent the human element in the context of an operational environment. This is a universal model which is supported in the domain of systems engineering, philosophy, behavioral science as well found in ancient Sanskrit texts like Kausitaki Upanishad III (Valerie 2003).

The SIRI Framework through the application of HAZOP/EBTA/ECFA/MORT studies is able to focus attention of the analyst on the where the cognitive mis-match between the task and the person is occurring or could occur by taking into account the organisational and inter-organisations perspectives and their impact on it. The concept of affordance of harm directs attention to the areas where the lack of awareness is creating safety problems. Affordance in Gibson's ecological approach is the direct perception –action mode of cognitive control which is depending upon a human being actively engaging in a goal directed activity in contrast to a human passively making judgments about a given environmental situation as in the case of knowledge based sematic interpretations(e.g. of a work of art). Jens Rasmussen cited two comments from Gibson (1988) as being relevant-''affordance links perception to action'' and ''learning about affordances entails explanatory activities'' (Rasmussen, Pejtersen, & Goodstein, 1994). This is demonstrated through a simple example.

Engineers experienced in the area of design of power distribution systems can grasp the concept of affordance for harm by studying the case of electrocution of several farmers when working on agricultural watering systems. This case study by Casey (1993) was cited by Jens Rasmussen (Rasmussen, Pejtersen, & Goodstein, 1994). When moving the system from one location to another, apparently some workers occasionally raised the 38-ft. long thin-walled pipes to a vertical position and touched the high voltage lines. No one expected farmers to raise the long pipes to a vertical position for transporting them to the next field. Only after analysts actually visiting the location and interviewing people did it become clear that farmers usually raised the pipes to a vertical position to release rabbits hiding in the pipes and lethal consequences resulted when done below the high voltage lines. Thus, it is argued in the case study that it demonstrates the limit of empirical safety control and the expresses the need for shorter pipe lines as defence against electrocution under high voltage lines. The idea of teaching about human error categories was refuted as a barrier (Rasmussen, Pejtersen, & Goodstein, 1994).

From the perspective of Energy Trace and Barrier Analysis(EBTA), the transfer of energy across the air-gap was, in the case of agriculture water system, triggered by reduction in the distance between the charged conductor and pipe which raised the potential difference above the natural dielectric strength of air acting as an insulator (barrier). The design failure in the situation was not to provide earth-wire grid beneath the overhead conductors to safe guard against the charged conductors falling to the ground or objects lifted up to them. The accident situation would manifest in the SIRI Framework when the designer's emergent

property of Sustain_ the Dielectric Strength would be tested against possible variations during the HAZOP study. The application of guide word-No or Less would reveal the potential accident to reveal the farmer's lack of perception of electrocution hazard (system hazard) and the failing barrier of safe distance (height) above ground.

The dynamic interfaces between the system hazard, barrier and potential accident form the essence of the SIRI Framework. The loss of protection to the farmer together with dis-functional interaction between S branch (technical system) and M branch (risk management factors) of the MORT would be revealed at the ECF/EBTA/MORT stage of analysis. The design engineer's knowledge of clearance and creepage requirements for protecting against earth potential rise for touch, step and transferred voltages for various working conditions and states of environment would be tested during the HAZOP and EBTA studies. Inspection of author's log book from initial days of work experience reveals that awareness of such conditions is essential competence on the part of the electrical power engineer and is still a valid idea as evidenced by entry on the public data base (Wikipedia 2011). This pattern of reasoning leads to ''how'' question implicating conjunction of technical failures in the planning stage and local influences at the sharp end of operations. The 'why' question implicating the engineering and management factors would be revealed from the use of question set in the M branch of MORT studies.

The IEC 15288 noted in the Annex D (informative section) the essential concept which the International Standard is based upon (ISO/IEC 2002). It noted that humans contribute to performance and characteristics of many systems for numerous reasons, e.g. their special skills, the need for flexibility, for legal reasons. Whether they are users or operators, humans are highly complex, with behavior that is difficult to predict, and they need protection from harm. Author notes that the rational actor model assumed by behavioral school of economics is refuted implicitly in the Annex D of the IEC 15228 Standard. Why? Because the empirical theory of human capital propounded by Gary S.Baker, assumes that investments into human capital usually are rational responses to a calculus of expected costs and benefits (Baker, 1964). Case study in the paper would show that this assumption is not true in the case of the UK railway signalling industry and the concept of 'bounded rationality' developed by Herbert A. Simon and acknowledged by James Reason persists (J. Reason 1990).

The foregoing notions require system life cycle process to address human element factors in the area of human factors engineering, system safety, health hazard assessment, man power, personnel and training. These issues are addressed by particular activities and iteration in the life cycle, and are described in more detail in ISO 13407 and ISO/TR 18529 (ISO/IEC 2002).

The concept of emergent property is important to be grasped in the context of systems thinking. An emergent property is a property which a collection or complex system has, but which the individual members do not have. Three examples are given to illustrate the concept. First, ammonia is a gas and so, is hydrogen chloride. When both gases are mixed, the result is a solid. The property is not possessed by either of the reactant. Second, carbon, hydrogen and oxygen are tasteless but the particular compound, sugar', has characteristic taste possessed by none of them. Third, The twenty (or so) amino-acids in a bacterium have none of them possess the property of being 'self-producing', yet the whole with some other substances has this property (Ashby W. , 1956/1999).

The SIMILAR Process	The SIRI Framework
State the problem	Derive the Emergent property using signalling layout, system diagrams and stakeholder's consensus on the norms
Investigate Alternatives	Assess the variations in the selected emergent property of the user and identify the potential accident situation using the HAZOP study
Model the System	Construct the narrative of expected operations using the ECF notation. If the potential danger situation is identified in the HAZOP study, then identify the trigger from the ECF diagram using MORT Decision Model in the operational situation.
Integrate	Generate EBTA diagram and perform MORT analysis , identify the interfaces between the potential hazard, barriers (missing) and targets, and decide upon the root of the problem using MORT accident process model
Launch the System	
Assess Performance	Compare with SRK model with Jens Rasmussen SRK Decision ladder and Reason's SCM and prepare the SIRI Hazard Causal Analysis Report
Re-evaluate	Release to stakeholders for consultation and peer review

Table 1. The SIMILAR Process mapped onto the SIRI Framework.

It is noted by author that concept of 'emergent properties' is not easily understood in the UK railway signalling domain. Author found a paper by E.Goddard which considered the subject of emergent properties in a very brief manner in the context of mass transit systems. But E. Goddard did not go far enough to include the concept of affordance of harm or system safety as an essential property of the railway system (Goddard, E 1998). Based on the concept of emergent properties, author rejects the J.S.Mill explanation perspective that it is possible to reason the property of the whole from the properties of parts.

This view of J.S.Mill is countered by Chris Johnson in the discussions on the theme of complexity following the workshop held on Complexity in Design and Engineering during March 2005 (C. Johnson 2006). Author has noted that the contents of the document by Chris Johnson were not peer reviewed. However, latest research from the behavioral science domain indicates that 90% population of the human subjects tested by researchers did not confirm to the expectations of the ethical theory of utilitarianism promoted by J.S.Mill and Bentham. The goal of this ethical theory is encapsulated in Bentham's aphorism that "the greatest happiness of the greatest number is the foundation of morals and legislation. The results published in Cognition were cited in the science and technology section of the Economist (The Economist 24 September 2011)". Author's assertion is that the idea of utilitarianism and associated ALARP judgments without taking into account the concept of unreasonable risk is verified by this research which generated the evidence that the antisocial personality traits predict utilitarian responses to moral dilemmas. The principle of correspondence has been used to draw similarities between control group and non-control group of human subjects in the laboratory conditions and outside of it. On comparison of ideas between Mill's theory of causation and the Aristotelian theory of causation, it appears that Aristotelian theory is more logical (M.Copi and Cohen 1998).

A key insight from the systems theory is that different individuals and organisations within a problem domain will have significantly different perspectives based on different histories, cultures, and goals. These different perspectives need to be integrated and accommodated if effective action is to be taken by all the relevant agents (Chapman 2004). But hope of acquiring true information from all the agencies to learn about the local as well as global interactions, from a top-down perspective is remote, and therefore, a bottom-up approach with no accident is acceptable policy is adopted to reflect upon the disturbing causes leading to system hazard and efficient barriers to eliminate them from operations. The idea of bottom-up approach in safety literature has been thought of by John Adams as well (S. Appicharla 2006), (Adams 2009). However, in contrast to John Adams approach, author does not recommend a safety action to be legislated as an effective procedure in the absence of efforts to detect policy and regulatory oversights and omissions that are occurring and impacting the standards in an adverse way (S. Appicharla 2010).

Literature in the decision making domain often calls upon readers to imagine typical scenarios to draw their attention to the subject matter. These may involve an imaginary scenario of tough decision making on the part of an old and poor clerk to replace an old worn out coat and trigger an action to start saving for a new coat. Under the critical judgment of a young tailor, old and poor clerk needs to depart from a previous approach of incrementally repairing the patches of the worn-out coat. This school of thought may lay emphasis on the concept of psychological stress upon decision making in conflict situations

(L.Janis and Mann 1977). Sociologist(s) may demand the reader to consider the plight of a person who misses a crucial interview due to a coincidence of foreseeable but imaginary events or circumstances (Perrow 1984). Other researchers in business decision analysis would like to focus attention away from black swan events which are impossible to predict. Instead, they offer advice on risk management and recommend try to reduce the impacts of the threats we don't understand (Taleb, Goldstein and W.Spitznel 2009).Some authors, would like the readers to consider the fact that human information processing might be subject to various kinds of biases due to use of thumb rules (heuristics) and due to things like representativeness, anchoring, and availability effects (Tversky and Daniel 1974).The process of multiple valued decisions requiring trade off approach developed by Benjamin Franklin of assessing pros and cons of any given situation as he called it as moral or prudential algebra is another perspective on the decision problem. This method is cited by (L.Janis and Mann 1977).All of these articles may direct the attention towards a process called humble decision making. Successful decision making is all about avoiding decisions with no sense of overarching purposes reckons another researcher in decision making (Etzioni 1989). In the medical health sector, Gerd Gigerenzer and J.A.Muir Gray argue that inability to make informed decisions by the doctors and patients using the laws of conditional probability wastes lot of public money. They urge that better use of condition probabilities and statistics would help the matters in the case of delivering patient care in a more economical way (Gray 2011). Charles Handy noted in the chapter on the 'working of groups 'that it has been shown in experimental studies that groups who attack a problem in a systematic manner perform better than groups who 'muddle through' or 'evolve'. He suggests that the decision making procedure is also of great importance (Handy C., 1999). The same suggestion is made by Derby and Keeney that there is no single solution to the how safe is safe enough problem and social, political and ethical aspects of the problem must be addressed by the analysis explicitly (L.Derby and Keeny 1981). In the wake of Japanese earthquake disaster, few observers like Ekekwe call for better risk communication (Ekekwe 2011).

As detecting subtle influences on decision making which cause behavior (rational or irrational) is an elusive phenomenon, the decision principle embedded in the SIRI Framework is the inherent safe design principle for the whole system. Thus, the system is biased towards no accident policy. Author notes that biases can be seen even in the case of founding father of modern economics, Adam Smith and other economists.

Adam Smith writing in Wealth of Nations in the chapter IV on the origin and use of money stated that once division of labour being established, every man lives by exchanging, or becomes in some measure a merchant, and the society itself grows to be what is called a commercial society.

Further, after elaborating that barter trade must have been in place before the origin and use of money, he notes that in a village in Scotland during his time, it was not uncommon for a workman to carry nails instead of money to the baker's shop or the ale house. Adam Smith, it is reasoned by author, thought it is odd on the part of nailer to do that. This is reasoning is validated by commentary of a later editor of the Wealth of Nations in 1805. The commentator gave explanation of this fact in this manner: Factors furnish the nailers with materials, and during the time they are working give them credit for bread, cheese, and chandlery goods which they pay for in nails when the iron is worked up. The fact that nails

are metals is forgotten in the text the following paragraph. At another place, Adam Smith remarked in the chapter on real and nominal price that at the same time and place, money is the exact measure of the real exchangeable value of all commodities (Smith 1776/1937). Author finds price system to be invalid and untrue in the case of ordinary commodity like jam. On a comparative basis, a brand can be cheaper on the supermarket shelves even after being better on account of energy and fat content. The difference in price cannot be attributed to time it takes to make them as David Ricardo (1772-1823), asserted in labour theory of value. Another instance of an assumption made by economist(s), which author finds is invalid and not true is on the need for a government.

Max Lernet, editor of 1937 edition wrote that Adam Smith assumed that there is 'divine hand' which guides each man in pursuing his own gain to contribute to social welfare and therefore, government is superfluous except to preserve order and perform routine functions. Author contends that this assumption is negated by the David Hume's picture of a man not as a religious creature, nor as a machine, but as a creature dominated by sentiment, passion and appetite (Hume 1739/1984). E.L.Woodward in his History of England wrote about new types of business-men arose who were' without scruple and without pity'-free, but lacking in any sense of obligation to their fellow men (Brown 1958). This mode of thought of sense of self within a community agrees with the thought of devotionalism or Bhakti Yoga expressed in texts like the Bhagavad Gita(BG) –with its emphasis on 'service', 'grace', 'humility', and 'love'. This devotion is often compared to the anvil in a black smith's shop in the Vedanta literature. In spite of repeated blows the anvil remains unshaken is learnt from the verse 10.7 of the BG (Nikhilananda 1944) . This thought appears to contradict the Vedic saying of prey-predator logic of eater is eaten away is noted by another Sanskrit Scholar, Wendy Dongier (Manu unknown/1951). The point of these discussions is that for each and every thesis, it is not difficult to find a contradiction in the form of anti-thesis which were called Antimonies by Immanuel Kant. Both antimonies which can be validly proven and since, each makes a claim that is beyond the grasp of spatiotemporal, neither can be confirmed or denied by experience (McCormick 2005). The way to resolve Antimonies is to grasp the Principle of Sufficient Reason. The Principle of Sufficient Reason is expressed generally by the idea that our knowing consciousness, which manifests itself as outer and inner sensibility (or receptivity) and as understanding and reason, subdivides itself into Subject and Object and contains nothing else is accepted in this chapter. To be the Object for the Subject and to be our representation are the same thing. All our representations which may be determined apriori and on account of which nothing existing separately and independently, nothing simple or detached can become an Object for us. This concept is due to Arthur Schopenhauer (Schopenhaeur 1820/2006).

Unless, we represent an idea to ourselves we cannot compute. A cognitive animal, which carries in it a model or image of the environment, is a sort of animal which can form ideas about environment and process information. In other words, cognition is a computation on a representation. Let us consider the issue of external world which contains many diverse features, and objects which cannot occupy the tiny size of human brain. Therefore, it is reasonable to assume that we store image copies of these objects or subjects which we derive out of experience (S. K. Appicharla 2010). From the forgoing, it is argued that reasoning from an economic point of view is fallible in some sense and does not provide a coherent, valid, logical and consistent explanation. On the contrary, the spiritual perspective as

expressed in the Vedanta texts is more rationale and valid in the modern context as well. This viewpoint finds supported by Arthur Schopenhauer (Schopenhaeur 1820/2006). Author notes that Adam Smith wanted to attack the feudal and mercantilist institutions of his age. Author learns from the BG Verse 5.18 that wisdom lies in seeing the same in all – wether it be a brahmin endowed with learning and humility, or a cow or elephant or a dog or an outcaste. This verse suggests to the author that subjective biases can enter into safety assessments due to economic or social evaluations and therefore, a sense of equality is necessary when dealing with the question of energy that is harmful.

It is noted by the author that Hume's perspective and Kantian perspective on causation is challenged by Schopenhauer (Schopenhaeur 1820/2006), (Wicks 2007). David Hume accepted that reasoning about cause-effect relations results in a sequence of events whereas Immanuel Kant reasoned that a sequence of events presupposes cause-effect relation. However, Arthur Schopenhauer argued that empirical reality is a complex of space and time in which objects (things which are represented) co-exist with the subject (the representer) in space. For example, when a substance catches fire, for instance, this state of ignition must have preceded by a state which is made up of conjunction of affinity to oxygen, of contact with oxygen, and of a given temperature. Ignition must necessarily follow upon this state and as it has just taken place that cannot always been there, but must on contrary, have only supervened. This supervening is called a change. Therefore, law of causality applies exclusively to changes.

Arthur Schopenhauer argued an explanatory account of anything does involve reasoning by a human subject using the connection of four independent kind(or parallel) of objects of material things(law of causality) , abstract concepts(law of logic) , mathematical and geometrical(law of mathematics and space), and psychological motives(law of intention).

From author's perspective, these connections form the basis of motivation in seeking explanation of multiple factors for hazard occurrence and present true explanation of accident phenomenon.

The early railway companies seemed satisfied with a philosophy that a big steam engine at the front of a train could easily push a horse-drawn vehicle on a crossing out of its way (Hall.S & Mark, 2008). No decision was enforced on the railway companies to avoid or eliminate the danger. It is a regrettable fact of phenomenal reality that Hume's perception of a man dominates the social psychological perceptive. If any examples of divinity are to be seen in the railway world then one can observe it in the personalities of Col.W. Yolland, Captain Laffan, Captain Sir H.W.Tyler and several others who were actively involved in promoting railway safety in the period between 1851-1871. These individuals promoted the concepts of interlocking the signals and points, blocking the route and braking as essential principles of railway safety. However, the concept of braking distance was taken for granted by them.

An expert in the UK railway domain thinks differently from a lay person on the matters of risk is demonstrated by the RSSB Research report T517 (Risk Solutions 2006). Author has found this observation to be valid even in the case of safety experts. Author inquired from his lecture audience on 21 September 2011 as to whether they saw one or two women in the Figure 3. Author was surprised to learn that at least two persons out of about 12-15 persons in the room did not re-cognize both woman figures in the picture. Author did not perform

any further examination to make both groups to communicate with each other to establish reasons for not seeing the double figures. The audience was made up of railway and road safety experts at the sixth IET International System Safety Conference held at Birmingham (S. Appicharla 2011).

Fig. 3. The picture shows an old crone or a 19th century young girl, depending upon the perspective of person looking at the picture.

As Charles Handy noted that the order of presentation of information is important in the case of perception. He noted that people who were first conditioned to see young girl first saw young girl but did not see the old woman and vice versa (Handy 1999). The idea which author wants advance from his foregoing observation is that it is a case of selective perception of objective evidence rather than a framing effect and this may bias the safety assessor or safety authorities as well. Why? Because all cases of human perception involve selective perception and therefore, it is necessary that perceptual illusions and cognitive errors are eliminated to grasp the reality of the hazard situation. Mirage is one example of perceptual illusion (S. K. Appicharla 2010). The point of the above figure perception is to make clear that consciousness is spatially multiple but in temporal terms it has unity which has been stated by Baroness Susan Greenfield (Graham Walker 2007). The argument advanced by Baroness Susan Greenfield is that there are two requirements for the consideration of morality from a scientific perspective. These are a sense of self and a sense of consequences of one's action. In line with Roger Penrose's thinking, Baroness Susan Greenfield argues that synthetic brains will never be conscious because they do not have, amongst other things, intuition or common sense. It is clear from the foregoing brief discussion that the R.L. Maguire's assertion that everyone has same mental model of safety or accident investigation is not true (R.L.Maguire and Brain 2006). Author accepts Ashby's assertion that every creature has same physical brain is both acceptable and true (W. Ashby 1960).

Unless, the idea of treating 'a person as a machine' is abandoned, the concept of taking the systems view of the self cannot take root in our consciousness. This idea is borrowed from Lynn M. Rasmussen (2004). Lynn M. Rasmussen states that the idea of the systems view of the self with its simple description of surrounding systems, purposes, functions, and

processes, shows us how we are all the same, that everyone is "like us." It transcends belief systems that divide us, links our inner functions with universally held values and ideals, and gives us a clear means for increasing our own consciousness and the consciousness of people of the systems in which we live (M. Rassmussen 2004). The UK railway industry body, RSSB, did conduct research into the topic of ethics in relation to safety is noted by author (Elliott 2003) (Wolff 2002). However, the research findings were not reflected upon by the industry.

This pattern of thought aligns with concepts of systems thinking as they are represented in the systems engineering standard, IEC15288, Annex D (ISO/IEC 2002). However, author would like to raise a concern here that this idea of relative self does not by itself extend to Karl Marx's worldwide view of dialectical materialism (Rupert Woodfin 2004).

To overcome the limitations imposed due to cognitive economy, system thinking is deployed to consider the emergent property of system safety by becoming aware that two kinds of awareness are present in the process of empirical perception. According to the system of Vedanta philosophy which this chapter accepts is that any object which is conditioned by the law of cause and effect is not absolutely real; for every effect is a change brought about cause, and every effect is temporary. According to the system of Vedanta philosophy the unreal never is. The real never ceases to be. The only Reality is the Atman, Consciousness, which is unchanging Witness of changes in the relative world(Samsara). The Absolute Reality is not conditioned by causality as stated in the Bhagavad Gita verse 2.16 (Nikhilananda 1944).

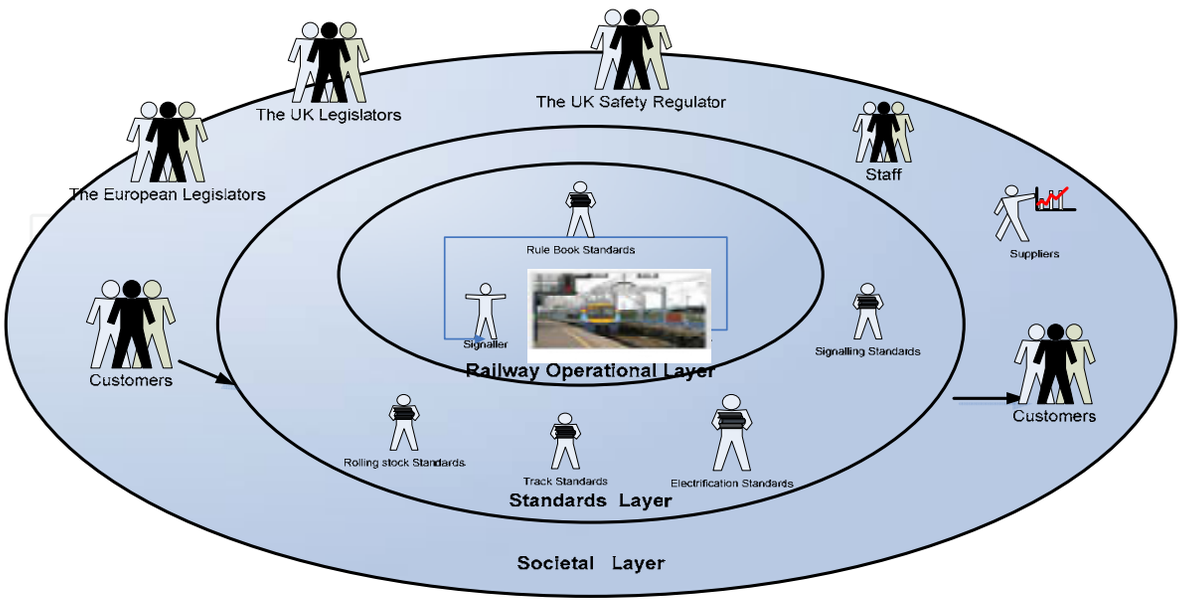


Fig. 4. A layered view of the UK non- ERTMS Railway Transportation Process

A schematic example of the multiplicity and complexity of perceivable systems –of –interest in the traditional UK railway operational situation and its context is given Figure 4. This schematic shows:

a. importance of defined boundaries that encapsulate meaningful needs and practical solutions;
b. layered perception of the system physical structure ;
c. an entity or element at any level of the layers can be viewed as a system;
d. a system comprises of a fully integrated, defined set of sub-ordinate systems,
e. characteristics properties of a system boundary arise from the interactions between system elements;
f. humans can be viewed as users external to a system (e.g railway user) or as elements within that system (e.g. train drivers or signallers) or as regulators or controllers of the system (e.g ORR/DfT) or as suppliers (e.g. signalling or rolling stock suppliers)
g. a system can be viewed in isolation as entity, i.e. as a product or as an ordered collection of functions capable of interacting with its surrounding environment, i.e a set of services
h. rules and regulations in the form of standards constitute a system with explicit purpose of documented and agreed procedures governing the interactions (lateral and vertical) within and across railway organisations, which can be used to support the self-regulation of system safety by the duty holders directly.

Terry Bahill and Steven Henderson (2005) discussed 23 famous failures and identified putative cause of those failures of system designs in terms of important system engineering categories of requirements development, requirements verification, requirements validation, system verification and validation where these activities were done correctly and incorrectly. They discussed that the Tacoma Narrows Bridge disaster can be taken as relevant to the railway domain was a case of system validation error. Validating a system means building the right system: making sure that the system does what it is supposed to do in its intended environment. They did not advance any scheme or framework by which the safety failures could have been foreseen. They hoped that the model System Requirements Classification Model (SCRM) and its divisions would help to improve understanding and compliance in the five systems engineering tasks (Bahill and J.Henderson 2005). Author learnt that 64% of the failures studies were B1category of unverified or invalidated systems with valid requirements but poor design realisation. Examples of this type of system design are the Tacoma Narrows Bridge disaster or war in Vietnam and Super Conducting Super Collider. 12% of the failures belonging to the B2 category of system designs which fail to adhere to their designs or fail to satisfy stakeholder needs in the process. System designs of this type are Mars Climate Orbiter and Titanic. This research can be taken to support the idea of Groupthink bias as a crucial factor in the 76% of the cases studied.

From a systems engineering perspective, in accordance with the IEEE 1471, it is assumed that each stakeholder would hold a perspective relative to the system behavior, its elements and/or attributes (W.Maier, Emery and Hillard 2004). In addition to traditional Three Viewpoints of Requirements, Structure and Allocation of the Hatley Pirbhai Method, the system and related concepts are defined in the Viewpoint Method as indicated in Table 2.

Viewpoint Name : Safety Analysis and Requirements.
Stakeholders: HAZOP Chair, HAZOP study members, MORT/ECF/SRK Analyst(s), Concept/Functional System Design Team, Operational and MaintenaceTeam, Risk Management Team, Human Factors Engineering team, Rolling Stock engineers, Signalling engineers, Track Engineers, Operational and Maintenace Staff, Accident Investigators, Data team, Configuration team, Electrification Team, Hazard Analysis Team, Asset Engineer, Software Team, Safety Policy Team, Reliability Team
Concerns: Potential or actual accidents, Root Causes, Hazards, Barriers, Targets, Controls Factors, Management System Factors, Energy Flows, Vulnerability, System elements, Interfaces, Behavior, Biases, Safety Risk, Data Analysis
Modelling Language: Entity Relationship diagrams, SIRI Diagrams

Study Methods: HAZOP/Managmenet and Oversight Risk Tree /Events Causal Factors Analysis/Engery Barrier Trace Analysis.

Consistency and Completeness Analysis Methods: Documented series of consistency rules and compliance of the safety studies with the basic concepts defined in the standards and guidelines such as IEC 61508/IEC 61882/IEC 15288/UK HSE Guideline 238/ BS EN 50126/IEEE-STD-1233. Some of the rules and process may seem redundant but it is necessary to assure that different persons check of the same rules inside and outside railway domain provide diverse means of checking the reports produced by the SIRI Framework. The underlying concept is to perceive the harm afforded by the system. (IEC 2001).

Table 2. System Safety Analysis and Requirements Viewpoint

3. SIRI case study: Herefordshire level crossing accident

The analysis started with the recording of facts connected with the accident which is treated as the top event or loss event in the MORT diagram.

3.1 RAIB report on herefordshire level crossing accident

The UK rail accident investigation agency, Rail Accident Investigation Branch (RAIB), published results of its findings into the Herefordshire level crossing accident in February 2011. This accident occurred on 16 January 2010 when a passenger train collided against two cars at the Infrastructure Manager(IM) staff managed manually controlled barrier type of level crossing. A woman passenger in one of the cars died as a result of this collision at the hospital while the car driver was seriously injured (RAIB 2011). The occupants in the other car suffered no injuries. Fig. 5 shows a BBC photo of the accident scene at the time when the barriers were up and the red lamp was lit.

The RAIB accident investigation process identifies, as a general procedure, a causal structure of an accident made up of immediate cause, causal and contributory factors, and underlying factors. This structure explains how a particular accident came into being. In this particular accident, the report identified several causal factors.

The immediate cause of the accident was the signaller located in the adjacent signal box who raised the barriers when train IV75 was approaching the MCB type of crossing allowing the

cars to move in the path of approaching train 1V75. The causal and contributory factors that led to the accident identified were a) unrecovered human error in the operating situation caused by signaller being distracted by a call from a user of a User Worked Crossing (UWC) and engaged in monitoring the progress of another train ; b) working out the time available to allow sheep movement across UWC; c) mentally distracted to work out the rules by which UWC situation to be managed; and d) the lack of engineering safeguard such as approach locking to protect against signaller's error.

The possible underlying factor stated in the report was the absence of requirements to consider safety benefits of such a measure in the Group or company standards (industry requirements) or in the UK Government regulations.

Finally, there were no cues available in the operating situation which could draw signaller's attention to the fact that danger was imminent in the operating situation. A further reading of the report reveals information that RAIB found the lack of regular communication between the operational risk team and the signalling team within the Infrastructure Manager (IM) organisation, Network Rail. This communication failure compounded the problem of determining the true level of risk. Human error that could occur in the level crossing situation was not included in the risk calculations due to the lack of regular liaison.

Fig. 5. A BBC photo of accident scene. Accessed on http://news.bbc.co.uk/1/hi/england/hereford/worcs/8465412.stm

3.2 SIRI event causal factors, energy barrier trace analysis and MORT analysis

The actual pre-cursor events which were triggered the crash are shown in the hand sketch using the Event Causal Factor notation in Fig 7. Author has used hand sketches for the analysis of the accident situation in the tradition of soft systems engineering started by Peter

Checkland (Checkland 2000). This diagram can be created using Microsoft Visio as well. The oval shapes denote conditions (perceptions or abstract rules) connected to the events and one to many and many to one relationship are shown on the diagram. To facilitate ease of comprehension, conditions which extend over time are shown in dotted lines. The analysis begins with the situation which is normative pattern/ situation of functional sequences of events. User arriving first at the level crossing, the train later (bearing in mind relativity of time at play) and train departing first and user leaving the crossing, later. This forms the core operational layer of the Railway System which is regulated by the Standards Layer which is surrounded by Societal Layer (refer to Fig. 4).

The emergent properties involved in the actions taken by various people involved in the accident situation which were directly connected in the perception –action mode in the sense of affordance are as follows:

a. Car driver's action of perceiving (event UD/E/2) the lifting barrier afforded the information that it is safe to go across the crossing space after having waited for the barrier to lift(event UD/E/1). This is in line with the connection between perception and action mode advanced by Gibson.
b. Train driver's perception of the Stop signal ML 42 changing aspects (RU/E/2) afforded the information that it is not safe to go as train driver became aware that some obstruction is expected. The action of brake application is directly connected to the perception as argued by Gibson.
c. Signaller's perception of the lifting barrier and the train (IM/E/3) afforded the information that there was an error on his part which could not be recovered despite his best intentions. This is in line with the connection between perception and action mode advanced by Gibson.
d. Despite the application of the service and emergency brake, the event in the RU domain (RU/E/3) occurred affording the information to analysts or observers that signalling distance beyond the Stop Signal ML 42 was less than adequate for the train to stop relative to the train speed. This is an indirect inference which is not directly perceived by us (author + reader). This is based upon the expected engineering and cultural norms that a signal shall be provided with a sufficient braking distance in case of emergency conditions obtaining in the operations.

Based upon the above four premises, it is reasoned that affordance of harm was due to failure to provide adequate braking distance at the Stop Signal ML42. By the method of counter factual reasoning, it can be deduced that three elements of information went missing in the System failure scenario case. User was not afforded information as to whether it is safe to cross or not? The signaller had no direct access to the information as whether the train passed the crossing space or not directly from the environment. The train driver had no direct access to information at a point in space from where the train could have been braked to safety. The RAIB report provides complete information with respect to the signaller's error.

The analysis of the operational scenario depicted in the ECF diagram requires from a behavioral science perspective application of the generic human factors framework of Jen Rasmussen Skill-Rules-Knowledge (SRK) or the MORT decision model of the accident process. Fig. 6 shows the MORT decision model which author used for making decisions.

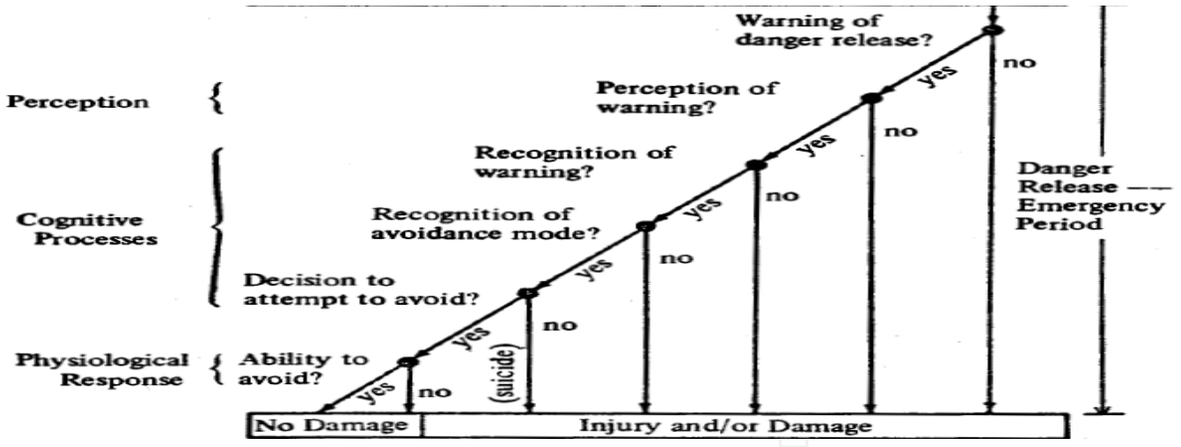


Fig. 6. A decision model of the accident process inherent in the MORT method.

The same model of the accident process can be used to represent danger at the design decision stage where decisions are taken to assume risk by calculation or by ignoring harmful safety outcomes where the end product of such decision making is that potential danger is embedded into the operational situation.

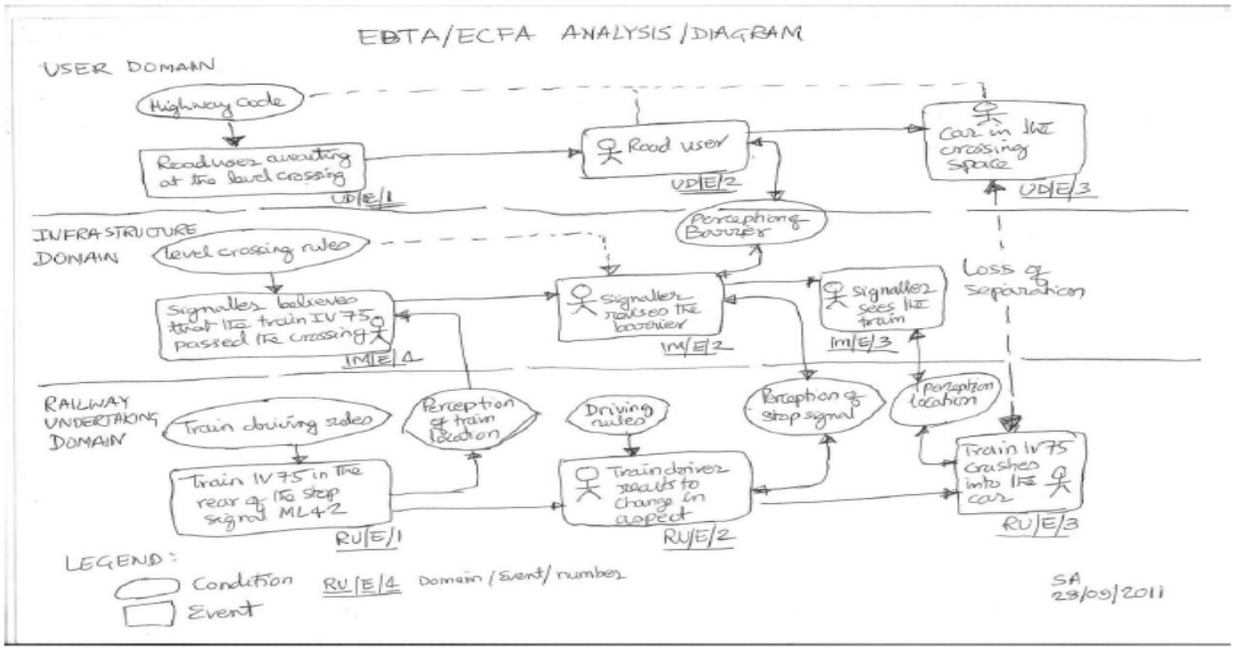


Fig. 7. A hand drawn sketch showing the pre-cursor events and conditions leading to the Herefordshire Crossing Accident on 16th January 2010. This is based upon the Schopenhauer's method of explanation discussed in section 2.1.

Based upon the perspective of energy barrier trace analysis (EBTA), author has listed barriers and controls for the purpose of evaluation of the alternatives which can protect the road user. These have been collected as part of the desk -top search of the ORR and other railway websites for the initiatives underway. These are shown in

Table 3. An evaluation of these barriers is conducted using the MORT questionnaire and as per the flow chart for conducting the investigation in the MORT User Manual. This is freely available for downloading from the NRI website (Johnson.W.G 1974). The results of the MORT application are stated in the Table 4 as per the instructions in the literature available (Gunderson 2005).

Harmful Energy Flow or harmful Agent, adverse environmental condition SB1	Target Vulnerable person or thing SB2	Barrier & Controls to separate Energy and Target SB3
Kinetic hazard (train movement into the crossing space) when it is occupied	Car drivers and passengers	Full service braking distance
		Restriction on train speed
		Obstacle detection
		Lifting barriers
		Road traffic light signals
		Active audio-visual alarms
		Passive visual signs
		Approaching locking
		Interlocking system
		Railway Protective signal
		Bridges, underpass etc
		radio communication systems to private user worked crossing users

Table 3. Energy Barrier Trade Analysis

MORT Branch Description	Problem statement/comments	Evidence
S/M Oversights and Omissions		
Specific Control Factors LTA	SA1: A passenger killed in Herefordshire Level Crossing Accident when a train IV75 struck two cars at Morten –on-Lugg near Hereford. The movement of the train 1V75 into the crossing space when the car is in the crossing space is regarded as not being functional part of the level crossing when considered as an Operational System. The judgement that a blame culture is prevailing the UK railway industry is deduced from the fact that full service braking distance is not provided at the Stop Signal ML42 to facilitate train braking to halt before entering the crossing space in hazardous situation. Such a requirement is not stated by the Accident investigator, the Regulator, the Infrastructure Manager, the Railway Undertaking and the Standards body which form the Social Layer. The Office of Rail Regulation (ORR) is the independent safety and economic regulator for Britain's railways. Following is the extract from the Office of Rail Regulator Website (The Office of Rail Regulator 2008): The on-going safety of level crossings ultimately depends on you, the users recognising the hazard and obeying instructions. The UK's level crossing safety record is among the best in the world. Over a third of all accidents involving a train are at a level crossing. 95% of the train accident risk arises from incorrect use of crossings by road vehicle drivers, such as attempting to 'beat the barriers' or run red lights. Less than 5% of train accidents at level	1. The RAIB Report Summary. (The RAIB 2011). 2. The train driver applied full service braking is evidenced from the paragraph 80, 156 of the RAIB report. 3. More than 8% of accident risk is within the industry control at level crossings is stated by the RAIB (paragraph 167). This data contradicts the ORR information given in the adjacent column. 3. The risk of an accident involving a train and vehicle does not fall into Assumed Risk Category under the MORT Questionnaire as risk to be properly assumed it has to meet the decision criteria of adequacy of cost-benefit analysis, uncertainty about risk themselves, tolerability of risks, adequacy of information and interpretation provided to the person making decision, and finally whether decision to assume risk was made by an appropriate person. This question set can be seen from page 46 of the NRI MORT User Manual. 4. The signaller error is a skill-based performance error. The road user error is a rule-based performance error.

MORT Branch Description	Problem statement/comments	Evidence
	crossing are as a result of a level crossing failure. Pedestrian fatalities and major injuries are most associated with footpath crossings and automatic half barriers (a type of level crossing).	
SA2: Stabilisation and Restoration LTA	Not considered due to the nature of the MORT desk top study. It is assumed that these branch events were adequate.	The RAIB Report Summary.

SB3 Branch Events LTA: : This branch is judged as being less than adequate (LTA) due to the following reasons

	SD1 Technical Information Systems LTA	The RAIB report detailing lack of approach locking in paragraphs 95,130 and 136.
	b1.Knowlegde LTA d1. Application of knowledge from codes and manuals LTA	
	d2. Was the list of experts(to contact for knowledge) adquate	Page 15 of Level crossings (Hall.S and Mark 2008).
	d3. Was any existing but unwritten knowledge about the work flow/ process known to the ''action' 'person?	The RAIB report paragraphs 35, 80, and 89 citing the events of signal aspect change and application of full service braking.
	d4. Was there research directed to the solution of known work flow/process problems and was this adequate?	
	Action person is the individuals (or individuals) undertaking the work task/process.	The RAIB report paragraph 15, 35,48,79,95 and 133. Paragraph 38 provides clear indication that ML42 and ML5 are protective signals in opposite directions. ML5 and ML42 fitted with the TPWS indicate that TPWS were fitted (at least at this location) without paying attention to the fact the fitting TPWS toML43 does not provide any safety benefit.
	The signalling engineering renewal works did not use approach locking to prevent the raising of barriers.	
	Rule 119 of the Rule Book did not indicate how the Gate keeper of level crossing would satisfy himself that no train is near before opening the gates to the road traffic.	The list of research projects conducted by RSSB can be accessed from their website freely at the following URL:
	The signalling engineering renewal works in 2009 did not provide sufficient braking	

MORT Branch Description	Problem statement/comments	Evidence
	distance at the stop signal ML42 as the RAIB report stated that the braking system on the train was functional, and the driver of the train IV75 applied full service braking when Stop Signal ML42 changed status. No SPAD risk is considered when the installation of the TPWS equipment at ML 43 and ML5 signal in 2003 was considered. This clearly indicates that there was awareness among the project signalling engineers that ML42 did not have sufficient braking distance. Either this information was either not shared with higher management or management has accepted that fact that engineering or management error cannot be compensated. The industry body, RSSB, and the European body, UIC conduct huge amount of research. None of the research had identified non-provision of sufficient braking distance as a risk factor at the MCB type of crossing. The SD1 branch is set to LTA based upon the foregoing problem set.	http://www.rssb.co.uk/SiteCollectionDocuments/pdf/reports/research/T907_guide_final.pdf The European research efforts can be accessed from the UIC Website freely at the following URLs: http://www.uic.org/com/article/european-commission-workshop-on?page=thickbox_enews http://www.iva.ing.tu-bs.de/levelcrossing/selcat/ All of the above represent knowledge based performance errors.
	<u>d5. Previous Investigation and Analysis LTA</u> <u>b4. Independent organisation and person review the work/process to identify high potential hazards LTA.</u> The signalling engineering renewal works did not consider the operational scenario during the project planning stage in which the train might encounter the stop signal being replaced to danger after passing the distant signal for the crossing in the clear position. An identical accident took place on 22 September 1965 at Roundstone level	1. Stanley Hall and Peter Van Der Mark give detail of the similar occurrence and note that this typical of several accidents of this type in pages 33-4, (Hall.S and Mark 2008). 2. The RAIB paragraphs 157 to 167 detailing risk due to manual operations. The RAIB observation that AHB are safer in comparison to manually operated barrier crossings is

MORT Branch Description	Problem statement/comments	Evidence
	crossing near Angmering, on the Brighton to Portsmouth line Col Reed, who led the public inquiry into the Roundstone accident did not consider the psychological pressure felt by crossing keeper and falsely believed that automatic half barriers would provide safer alternative. He did not inquire whether the sufficient braking distance was available. In this occurrence, the signaller lifted the barrier under the distraction from once in 20 year kind of an event, user (farmer) of the adjacent level crossing distracted the attention of the signaller. The RAIB notes 12 near miss incidents and 37 incidents of user abuse. Author had reviewed the work of ABCL/AHB level crossings as a HAZOP Chair and made the results available in the public domain.	contradicted by data given by Stanley Hall and Peter Van Der Mark on page 78 that between 2000 and 2006 16 fatalities have occurred on the AHB level crossings and none have occurred on MCB type of crossings (Hall.S and Mark 2008). 3. The risk data provided by RSSB in the Annual Performance Report in the form of histogram shows that user worked crossings and Active (automatic controlled crossings) pose more risk than manually controlled barrier or gated crossings (RSSB 2010/11). 4.Past MORT study showed that group think bias has an adverse impact on the safety outcomes (S. Appicharla 2010). All of the above represent knowledge based performance errors.
	The signalling engineering renewal works interpreted the term 'absolute' in the Absolute Block System to mean that only one train in a section is permitted between signal boxes on the same line at the same time. This interpretation did not include crossing space as a part of the line or route where trains and vehicles and/or passengers can be on the line at the same time on the crossing space. The signalling engineering works did not provide overlap or safety margin according to the Absolute Block Regulation 3.4 of BR	Chapter 13, pages 48-53 discusses the Absolute Block System Rules and Regulation of the Modern Signalling Handbook (Hall 2010). All of the above represent knowledge based performance errors.

MORT Branch Description	Problem statement/comments	Evidence
	300062/2, 1992	
	The civil engineering works did not provide bridges or underpass according to the section 13 of the Railway Regulation Act 1842. The 1842 Act also gave the Board of Trade powers in Section 13 to authorise companies to construct bridges in place of level crossings at their own expense, although it should be noted that it did not give the Board of Trade powers to compel them to do so.	Page 7 of Level Crossings (Hall.S and Mark 2008). All of the above represent knowledge based performance errors.
	The civil engineering, signalling engineering works and operations departments of the erstwhile BR organisation did not find satisfactory solution to problems of reduction of manning costs at the gated crossings, reduction of delays to road traffic and to improve safety as they adopted unsafe automated half barrier crossings According to study published by Andrew Evans (2010), on automated crossings accidents rates are higher because the primary responsibility for the safe operation of automatic crossings rests with road users in observing the warnings indicating approaching train. But in this accident, loss of protection took place as the train did not come to stop before striking the cars.	Chapter 7 of Level Crossings details the major reappraisal of level crossing policy (Hall.S and Mark 2008). The accident process theory developed by Stott and used by many accident investigators in the level crossing risk studies is rejected by author in his previous publication (S. Appicharla 2011). All of the above represent knowledge based performance errors.
	The civil engineering works, signalling engineering works and operating rules and regulations did not specify restrictions on train speed when the route contained the hazard of stop signal being placed to danger in the Absolute Block Signalling system. Active human error in the ABS was perceived for the first time in January 1885 when a signalman gave 'Train out of Section' bell signal to the previous signalman before the train cleared out of section.	Page 52, The North Staffordshire Railway Accident near Stroke on Kent, January 1885 and The London, Chatham& Dover Railway Signalling Arrangements (Hall, Railway Detectives 1990). All of the above represent knowledge based performance

MORT Branch Description	Problem statement/comments	Evidence
		errors.
	The signalling engineering works did not consider any hazard review of the UWCs type level crossings which have potential to distract the signaller from monitoring the progress of trains. This type of error which has occurred is similar in nature to signaller error that emerged in the context of track worker safety HAZOP workshops author has chaired in 2006. This HAZOP workshop demonstrated that signalling engineers possess false beliefs about the equipment performance and outcome of the degraded scenarios. The results of HAZOP study were published in 2010 by (S. Appicharla 2010). In the case of Herefordshire accident signaller's error is located at the skill based level where the necessary condition for the occurrence of a slip of action is the presence of the 'attentional capture' associated with either distraction or preoccupation. The actions of road user, train driver and signaller in the SB2 branch are judged adequate as per the cognitive science tradition. All active human errors were triggered by external causes.	Rule 119 of the Rule Book did not indicate how the Gate Keeper of level crossing would satisfy himself that no train is near before opening the gates to the road traffic. The common belief that as long as the rules were followed, safety would be maintained is also seen in the case of the Astra Train crash in 2000 (Halvorsrud 2002). Author from the Norwegian Railway Inspectorate reported that the signalling engineers and technicians reacted with disbelief to the suggestion that re-engineering of the signalling system is necessary. Why? Because railway signalling systems are assumed to be fail safe and it just not fail unsafely. The defective historical rule 119 and defect in the signalling layout and planning are likely to provoke similar reactions of dis-belief to the idea re-engineering of the signalling system and operational rules is necessary as it can be seen from this study.

M Branch Events: This branch is judged as being less than adequate (LTA) due to the following reasons.

Problem statement/comments	Evidence
From the perspective of organisational behaviour, management control is the process through which plans are	1. As per the SIMILAR process discussed in the section 2.2. 2. Barry A. Turner (1976)

MORT Branch Description	Problem statement/comments	Evidence
	implemented and objectives are achieved by setting standards, measuring performance, comparing with actual performance and then deciding necessary corrective action and feedback. However, it is important that standards should prioritise safety. Case studies of King's Cross Underground fire published by Reason (1990) and discussions on automatic train protection system by Whittingham (2004) do not lay emphasis on why policies failures in safety matters continue to occur.	published his findings on the problem of failure of foresight. Refer to section 2.2.1.
	No lessons have been learnt from Barry A. Turner study of the Hixon Accident.	
Policy LTA	The ORR guide on level crossings did not call upon the duty holder organisations (RU/IM) to provide full service braking distance when the stop signal is replaced to danger in the MCB type protected crossings or barrier crossings with obstacle detection As the ORR guide did not ask for full service braking distance at the protective signal, this is considered as a causal factor. When signalling schemes with full service braking distance at level crossings or changes to line speed or constructing bridges or underpass etc when proposed (as a risk reduction measures) these proposals must meet the process requirements defined by ORR as below. As these measures are technically and practically feasible as per MORT terminology and therefore, they are not logged as Assumed Risks in the MORT study. Further, the concept of duty of care from engineering perspective demands safety must be designed into operations. The definition of Risk and Hazard which is accepted in the UK Case Law is noted by	1.COMMISSION REGULATION (EC) No 352/2009 of 24 April 2009 on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of Directive 2004/49/EC of the European Parliament and of the Council contradicts the UK HSE Case Law 5. The conflict of philosophy between European Union legislation for inter-operability certification and United Kingdom case law, rules and regulations is noted by Andrew Rae and Mark Nicholson (Nicholson.M and Rae.A Septembe 2010). 2. ORR, Railway Safety Publication 7, Guide for level crossing managers, designers and operators does not call for sufficient braking distance to

MORT Branch Description	Problem statement/comments	Evidence
	author and there is a unresolved problem between the UK Case Law definitions and EU legislations on inter-operability, Safety Directive (Appicharla S. , 2010).	be provided in case stop signals are replace to danger after showing clear aspect. (The Office of Rail Regulator 2011)
SFAIRP 'so far as is reasonably practicable' Policy	The ORR internal policy guidance on safety related investment decisions did not expect the duty holder to perform cost benefit analysis when the risk reduction action is to be taken based upon the relevant good practice as a baseline. When the relevant good practice is not good enough it recommends rough CBA to be undertaken and along with a correction for 'optimism bias'. This is to make adjustments for overconfidence in the project estimates to account for cost overruns in capital projects. Where risks are difficulty to quantify, the guidance documents suggests using qualitative techniques such as structured workshop assessments supported by expert judgement. The RSSB guidance on taking safe decisions uses reasonably practicable policy. The argument advanced is that predicting accident risk in inherently uncertain. Similar accidents may give rise to different fatalities: 31 fatalities (Ladbroke Grove) or 7 fatalities (Southall) and therefore, low frequency high fatality accidents cannot be predicted. Quantitative risk assessment is considered to be useful as high frequency and low fatality incidents can be easily predicted as there is plenty of historical data. This argument is not in accordance with the best practice of safety management. When the information is uncertain, the precautionary principle should be invoked. The principle of inherent safe design of signalling or any other engineering works is perceived but not cognised.	1. This document can be accessed here. http://www.rail-reg.gov.uk/upload/pdf/risk-CBA_sdm_rev_guid.pdf. 2. The scrutiny of account the engineering safety management process followed by the UK railway industry which is biased towards operational reliability by taking into the number of years of reliable operation. The Yellow book does not contain any process for performing system hazard causal factor analysis as identified in the informative clause, 4.4.2.12 of BS EN 50126 (CENELEC 1999). 3. E.L.Woodward in his History of England wrote about new types of business-men arose who were' without scruple and without pity'-free, but lacking in any sense of obligation to their fellow men (Brown 1958). 4. R.B.Whittingham (2004) argued in the page 188 that there is a lack of will to make necessary investment into automatic train protection by the railway industry using arguments of high cost of ATP

MORT Branch Description	Problem statement/comments	Evidence
	It may be argued that the recent commitment by the railway industry to install ERTMS removes this concern. Author wishes to draw readers' attention to the fact ERTMS technology cannot be considered as a barrier in the same sense as TPWS. This judgement is arrived at by reading the technical review of the ETP project by the UK HSE Research Report 0067 (2003) where the reviewers have expressed concern that all potential accident scenarios have not been examined. Further, the recent incident which occurred at the level crossing at Llanbadarn, near Aberystwyth, Dyfed, on the ERTMS signalled railway between Aberystwyth and Machynlleth, on Sunday 19 June 2011 has drawn author's attention. This incident raises a concern that integration and commissioning of national signalling elements into the Inter-operable sub systems to form a coherent and consistent operational system may not have been preceded by any hazard and safety analysis. Selective attention to optimism bias without considering other biases which can operate in the decision making process is a policy error. Author has already published the results of past HAZOP and MORT studies which show that expert judgement is compromised by group think bias in 2010 (Appicharla S. , 2010). The question of blind spot does not arise as information and cognition of that fact that signal ML42 did not give sufficient braking distance has been there since 2003. Thus, question set is marked LTA	per fatality averted but the situation is exacerbated by a lack of consistent policy by successive governments (Whittingham 2004). Author accepts the definition of internal and external causes of human error defined by Whittingham (S. Appicharla, Analysis and modelling of the Herefordshire Accident using MORT Method 2011) 5. Blame culture prevails in the parts of the UK railway industry is noted in the following paper on Organisational Dynamics and Safety Culture in UK Train Operating Companies (Weyman 2006). 6. The railway projects do not consider all accident scenarios and include safety concerns is seen from the following papers on the Train Protection - Technical review of the ERTMS Programme Team report, The UK HSE Reserach Report 067 and performance of ERTMS system. (The NEL Consortium 2003), (D. Hicks 2004). 7. Risk in management systems is a cause for concern is concluded in the RSSB Research Project T169 (Ansper Consulting 2004). 8. Error in policy is a knowledge based performance error.

MORT Branch Description	Problem statement/comments	Evidence
MA2. Implementation of Policy LTA	ORR notes in its annual assessment, ''Safety - weaknesses in Network Rail's safety culture have been recognised including the exposure of flawed injury reporting. ORR is often frustrated by the slow pace of necessary safety improvements, and a number of enforcement notices followed failure to make timely progress''. This admission by ORR (ORR/14/11) suggests failure in general to the lack of thinking about alternative counter measures for minimising the problems. The question of budgets LTA does not arise as Network Rail is a profit making enterprise with annual profit after tax of £313 million in the year 2010-11. This profit can fund replacement of public level crossings and implement communication systems for the private level crossings in the signal box area. A rough estimate of £1 million per unit bridge cost is assumed. The case of private level crossings can be solved by a communication system which can activate and communicate train arrival message to this set of users. Argument from social cost benefit analysis does not arise as it is evident that there is no shortage of funds for investment and the risk falls into intolerable zone. Failure to set an example by ORR is reflected from the above admission. Thus, this question set is marked LTA.	ORR Annual Assessment Report. All ORR documents can be freely accessed from their website directly. This represents knowledge based performance error.
MA3. Risk Assessment and Control System LTA	This branch is judged as being less than adequate due to the following reasons.	
	•MB1 Hazard Analysis Process LTA	RAIB Report paragraph 167.
	The like for like replacement project in 2009 did not recognise the need for hazard analysis to identify potential accident scenarios. The RSSB and Network rail risk	This represents knowledge based performance error.

MORT Branch Description	Problem statement/comments	Evidence
	assessment process did not include the task of hazard analysis. The RSSB Topic Report says that, ''level crossings are safe when used correctly. Over 90% of risk in the previous ten years has resulted from user misuse in the form of error or violation (the remainder being due to other causes, such as equipment failure, reduced visibility or railway operator error). The analysis of S branch suggests hazard causal factors such as less than adequate control of work process are not modelled in the accident risk equation and therefore, answers to this set of questions are set to LTA.	
	• MA3.Standards LTA There are no requirements to consider alternatives to current work process controls (approach locking) suggested in the Railway Group Standards or NR Company Standards or in the ORR Government Regulations. This conclusion is based upon examination of the ORR Risk Profile Topic Strategy for Level Crossings, HMRI Safety Principles 4 and 23 and Railway Group Standard GI/RT7012. The RGS GI/RT 7012 did not contain any requirement for the full service braking distance to be provided at the protective signal. It is noted that it sets a limit between 50m to 600 m for the stop signal's location from the crossing space but it does not specify whether it applies when the stop signal replaced to danger for the crossings operated by IM staff. The ORR Guidance on level crossings did not call for full service braking distance to be provided in the case of barrier crossings operated by Infrastructure Manager Staff. The guidance does not consider the fact	1.The Railway Group Standard GI/RT7012 (RSSB 2010) 2. ORR Risk Profile Topic Strategy for Level Crossings (Office of Rail Regulator 2008-09 to 2009-10) and ORR Guidance on Level Crossings (Office of Rail Regulator Aug 2011) A paper by X. Quayzi (2011) argued that bounded rationality biases our decision making and leads us to a false sense of safety when using best practices. We are naturally inclined to use best practices without taking a critical view of culture, regulatory systems not defined in the best practices. This approach could lead to an increase of the level of risk (Quayzi 2011).

MORT Branch Description	Problem statement/comments	Evidence
	when a train passes the protective signal at Stop it might lead to an accident scenario. However, provision of full braking distance in other type of crossings is defeated due combination of the driver error and road user error. To be useful, where protecting signal is provided, it is necessary to provide full service braking distance with TPWS protection. • Data Analysis LTA From the inspection of the data in Figure 8 and Figure 9, modelled by Andrew Evans of Imperial College, London show that the trend of high frequency and low fatality events continues and reveals that risk is not ALARP. The statistical overall frequency of accidents is estimated to be 2.63 per year in 2009 causing 3.71 fatalities per year. The product of two figures gives 9.73 accident fatalities per year. The corresponding figure for 1967-2007 was 10.321. This is unreasonable risk as per ALARP classification of risk and does not meet policy requirements for risk management from ALARP perspective as per the guidance clause 3.7 and 3.8 listed on the Guidance Note on the website (The UK Health and Safety 2003). It is vital to consider decision errors in statistical process control domain where it may lead to a situation where vital clue about the phenomena under observation may be missed and out of control process is continued in the operations. The RAIB report provides the evidence that risk analysis was LTA. The risk analysis did not cover information about human error in the operating situation. Further, that the risk analysis procedure used by IM internal procedure for risk assessment i.e. All Level	1. RAIB Report paragraphs 55, and 147 to 155. 2. Reading of the following paper reveals that possible wrong side failure of barriers was not foreseen. The idea of condition monitoring using the fault tree and FMEA techniques detected only one third of the failures and none of the detected failures were causal factors in this accident (Roberts, Márquez and Tobias 2010). 3. The Infrastructure Risk Modelling (IRM) undertaken by Railtrack, predecessor of Network Rail in 1997 did consider the dangerous failures in the consequence analysis and this modelling showed that some branches of the event tree did not contain any safety barriers and directly led to accident scenario due to automatically failure of barriers in the case of CCTV/AHB level crossings. But the modellers and analysts of the event trees did not consider engineering and managerial errors as types in

MORT Branch Description	Problem statement/comments	Evidence
	Crossings Risk Management Model (ALCRM) did not generate any trigger for hazard analysis is evident from the RAIB Report. In 2009, a mean of about 5 per cent of fatal accidents were at railway controlled crossings, 52 per cent were at automatic crossings, and 43 per cent were at passive crossings.	the fault or event tree analysis and restricted themselves to operator or user error which appear as external causes to the engineers and managers involved in the decision making on the standards and facility designs. The IRM later developed into the Safety Risk Model (SRM) which was reviewed by the Health and Safety Laboratory (HSL) in 2002 and noted that root causes of human error are not modelled in the SRM. The report noted a concern that SRM fault tree modelling might not support a detailed assessment of root causes of some failures. The report did not express any concern that engineering and management errors are not considered in the pre-cursor model. (Human Factors Group, Health and Safety Laboratory 2002). The above comments show that probabilistic risk assessment was less than adequate to show contribution made by human failures in engineering, management and organisation levels. The event tree analysis in the context of nuclear power is discussed by James Reason (J. Reason 1990).

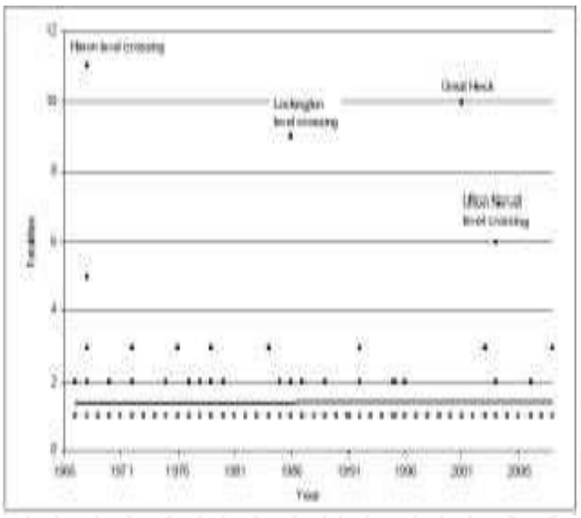


Fig. 8. Fatalities in collisions between train and road vehicles collisions 1967-2009. Source: Andrew Evans (Evans 2010)

MORT Branch Description	Problem statement/comments	Evidence

Accident Location	Estimated rate of change in accidents per train-km (with standard error)	Accidents per year in 2009	Fatalities per accident	Fatalities per year in 2009
At level crossings		2.39		3.37
Not at level crossings		0.25		0.35
All	−3.2% (se 0.6%) p.a.	2.63	1.41	3.71

Fig. 9. Fatalities in collisions between train and road vehicle in 2009. Source: (Evans 2010).

-b1Technical Information LTA -b2Defintion of ES& H goals LTA -Trigger to Hazard Analysis LTA -Sensitivity LTA	The flow chart used for the decision making in the IM organisation on the proposed changes did not draw any attention to the hazardous nature of the activity. The existing method of ALCRM is insensitive to changes in the real circumstances concerning pre and post-accident risk modelling are facts read from the RAIB report (paragraphs 55,149,150). The need to perform hazard causal analysis along with risk analysis is stated in the IEC 61508 at phase 3 before the allocation of requirements. This basic safety standard can be used for non-programmable technologies as well. A paper published by another railway administration regulated by the ORR gives an instance of this kind of conceptual error of not considering system hazard factor casual analysis. Conceptually, BS EN 50126 describes the idea of hazard causal factors analysis in clause 4.4.2.12, Figure 7 of the standard, but this analysis is not mandatory for the regulatory or system development process. The UK Railway Safety Risk Model does not integrate the fault tree and event trees correctly as it is required for the proper estimation of the risk. The top event of the	1. The concepts of system, system hazard, and probabilistic risk analysis are not understood in the UK railway industry. This acknowledgement is made in a paper presented by G.J.Bearfield and R, Short of RSSB and Atkins Rail in September 2011 (G.J.Bearfield; R.Short September 2011). 2. The RAIB Report Paragraphs 55,149,133 and 150. 3. Hazard Management with DOORS: Rail Infrastructure Projects (Hughes,D , Saeed A, 2009). Hazard management is taken to mean management of hazard log rather than concrete action to eliminate the unsafe situations. Metro railways undertake multi-method of analysis is learnt from the published literature on São Paulo Metro (Joao Batista Camargo Junior 1999).

MORT Branch Description	Problem statement/comments	Evidence
	fault tree is used as an input to the event tree in the case of the Railway Safety Risk model. This conceptual error does not arise with other PRAs where there is correct integration. The Installation of the TPWS equipment at ML 43 and ML5 signal in 2003 clearly indicates that there was awareness among the project signalling engineers that ML42 did not have sufficient braking distance. This information was either not shared with higher management and management failed to act or was suppressed locally. Lack of communication between the risk team and the signalling team is noted in the RAIB report. Thus, answers to risk data analysis, setting of EH& S goal setting, trigger to hazard analysis etc in this sub-section are set to LTA.	4. The Infrastructure Risk Modelling carried out by Railtrack using the Cause Consequence Analysis method the scenario crossing open before train has passed is recognised as an accident scenario (automatic function) with no barriers in place to safe guard road user life in the case of manually controlled barrier crossing CCTV type (Ref Railtrack/S&S/IRM_CCA/18 dated March 1998). This document can be searched on the web using the above reference.
•Safety Program Review LTA	ORR guide did not call up for any safety program review in the guide. There is no evidence provided in the RAIB report which gives the assurance that a safety program review exists in the IM/RU organisations. British railway did not have any cohesive plan for safety management is gathered from David Maidment's account (Maidment 2002). The details can be seen at this URL: http://www.davidmaidment.com/railways.htm. In hindsight the claim made by David Maidment is wrong as BR did not implement MORT method even after being aware of its existence. This fact Is cited in the literature (S. Appicharla 2011). Thus, MA3 branch events are set to LTA.	There is no single, clearly defined assurance process and formal safety assessment in the railway industry is concluded in the RSSB research reports T219 (DNV Consulting 2004) and T220 (DNV Consulting 2004).

MORT Branch Description	Problem statement/comments	Evidence
Conclusion	This paper verified the MORT thesis that the Herefordshire accident occurred because affordance of harm posed by MCB level crossing was not eliminated by the signalling layout, less than adequate signalling rules, less than adequate operational rules due to oversights and omissions. The MORT study concluded and reconfirmed that safety critical decision making suffers from individual as well as group think bias. Internal decisions taken by the industry attribute human error to external causes and this attribution provides a latent pathway to erode the barriers as per the SCM. The safety interventions can be initiated if the two proposals of bridges replacing public level crossings, radio communication with the private crossing users (UWC and other private crossings) can be established to provide information on the arrival of trains at the crossing space. Obstacle detection without provision of stopping distance for the train is not design which complies with inherent safe design principle.	1.The MORT and Swiss Cheese Model 2. Latest experiment published in the in the journal of Experimental Social Psychology reveals that society looks upon the role of producer with respect and admiration and looks down the role of worker (The Economist 2011). Society rewards risk taking but punishes safety risk taking is the inference author draws from the demands for public inquiries after every major accident. If human agency causes accidents, then human agency can prevent them as well. The idea that latent errors that precede a major disaster in defended systems is analogue to resident pathogens in the human body is refuted by this case study as there were no multiple defences in the design of the operational system. The notion that fallible decision making cannot be detected is not true is learnt from this case study.

Table 4. MORT Table for the explanation of the Herefordshire Level Crossing Accident

4. Problem Statement

Problem Statement electronically created 13 December 2005

How do we identify the Interfaces?

4.1 Background

The standards strategy is centred around the filter process which takes existing measures and determines whether they are defining a duty holder interface. The assumption is that within our existing standards all the interfaces are sufficiently defined.

Within CCS & ENE the feeling is that this assumption is not valid. Many duty holder interfaces are either not covered or at best implied. If the existing measures where the only source of material for the new standards the fear is that many gaps would be left.

What is required is a means of identifying all the relevant interfaces with a high level of confidence that omissions do not exist. Modelling of the railway systems is proposed as the means of achieving this. Furthermore, modelling may offer additional benefits. Note that modelling may not be the only means of achieving the objectives.

4.2 Solution objectives

The primary objective is to identify all interfaces (at the product level) between duty holders for each part of the CCS & ENE railway disciplines. These must be sufficiently detailed to ensure that all known technology implementations are described. In some cases the various technologies will create different interfaces and therefore need separate means of identification, in some cases the known technology solutions will not require to be identified separately.

Where the choice of technology creates different interfaces, it will be helpful (but not immediately essential) to represent a non-technology dependent system since this would appear to provide assistance for the future development of new solutions.

As a secondary objective, it may be helpful if the solution could provide assistance with the safety justification needed. Achievement of this objective is not essential.

4.3 Exclusions

It is not anticipated that the wording or the measurement values of the final control measure will be generated by the solution.

5. Conclusion

This chapter advanced presented a framework for the conduct of independent accident analysis and system safety analysis and assessment by taking cognitive systems engineering perspective in response to a problem statement expressed in 2005. This takes into account organisational, technical, individual and regulatory factors. The application of the SIRI Framework to the case study of Herefordshire level crossing accident showed groupthink bias is active in UK railway industry. Why? Because material cause (less than adequate signalling rule regarding stop signal location), efficient cause (less than adequate operational rule 119) and formal cause (managerial policy of relying on numerical risks and their pre-cursors and subject expert information and decision based upon a false erroneous grasp of ALARP principle) have been demonstrated in the case study presented in the chapter. Thus, it is necessary that re-engineering action on the current signalling system,

rule-making and procedures of decision making is taken to manage the rail-road interface safety. This is to tackle the problem of group think and individual bias which has negative impact upon safety outcomes.

6. Acknowledgment

Author wishes to acknowledge the efforts of following organisations and/or individuals for their indirect help rendered in the preparation of this paper.

- The MORT team and supporting team at the Noordwijk Risk Initiative Foundation, Netherlands, for hosting MORT related documentation.
- The Trustees of the estate of Dr. W. Ross Ashby for making available Ashby's documentation.
- The team(s) at the Health and Safety Executive, United Kingdom for making available HSE related research reports.
- The team(s) at the Delft University, Netherlands, and their collaborators for the invitation to submit a paper.
- Reviewers for their helpful suggestions and comments.

7. References

Adams, J. "Risk Management: the Economics and Morality of Safety Revisited." London: Proceedings of Safety-Critical Systems: Problems, Process and Practice, 2009. 23-37.

Ansper Consulting. *T169, Risk in Management Systems.* London: RSSB, 2004.

Appicharla, S. "Analysis and modelling of the Herefordshire Accident using MORT Method." *The 6th IET International System Safety Conference.* Birmingham: Institution of Engineering and Technology, 2011. 10.

—. "System for Investigation of Railway Interfaces." *The 5th IET International System Safety Conference.* Manchester: Institution of Engineering and Technology, 2010. 6.

—. "System for Investigation of Railway Interfaces." *The 1st IET International Conference on System Safety.* London: Institution of Engineering and Technology, 2006. pp.7-16.

Appicharla, Sanjeev. "Economy, a thermodynamic perspective." *Unpublished Manuscript.* New Delhi, 12 December 1998.

Appicharla, Sanjeev Kumar. *Response to the Consultation on Level Crossings , UK Law Commission .* London: Unpublished draft, 2010.

Aristotle. *Ethics.* Translated by J.A.K.Thompson. Aylesbury : Penguin Classics, 350BC/1955.

—. *The Politics.* London: Penguin Classics, 323 BC/1951.

Armstrong, K. "Why EMC Testing is Inadequate for Functional Safety -and what should be done Instead." *The 1st IET International Conference on System Safety.* London: Institution of Engineering and Technology, 2006. pp.179-83.

Ashby, W.R. *Introduction to Cybernetics.* London: Chapman and Hall Ltd, 1956/1999.

—. *The Design of a Brain.* London: John Wiley & Sons, 1960.

Ashby, W.R., and C.R Conant. "Every Good Regulator of a System must be model of the System." *International Journal of System Science* Vol 1, No.2 (1970): 89-97.

B.Bateman, S.W. Hatton. "The Increasing Role of Structured Methods in Arguing Safety." *1st IET International Conference on System Safety.* London: Institution of Engineering and Technology, 2006. pp.158-63.

Bahill, A.Terry, and Steven J.Henderson. "Requirements Development, Verification, and Validation Exhibited in Famous Failures." *Systems Engineering* (INCOSE and Wiley Subscription Services) 8, no. 1 (2005): 1-14.

Baker, Baker S. *Human Capital* . London: The University of Chicago Press, 1964.

Benjamin.S.Blanchard. *Systems Engineering Managment.* Vol. 3rd Edition. New Jersey: John Wiley& Sons,Inc, 2004.

Briscose .G, J. *MORT Based Risk Managment.* Idaho Falls: System Safety Development Centre, 1990.

Brown, J.A.C. *The Social Psychology of Industry.* Middlesex: The Penguin Books, 1958.

CENELEC. *EN 50126 Railway applications- The Specification and demonstration of Reliability, Availability, Maintainability and Safety Speicification* . Brussels: CENELEC , 1999.

Chapman, J. *Systems Failure.* London : Demos, 2004.

Checkland, Peter. "Soft Systems Methodology." *Systems Research and Behavorial Science*, 2000: pp.11-58.

Clifton, Ericson II . A. *Hazard Analysis Techniques for System Safety.* New Jersey: Wiley& Sons, 2005.

D. Hicks. "Performance modelling for the National ERTMS Programme (NEP)." *The IEE Seminar Railway System Modelling.* London: The Institution of Electrical Engineers, 2004. 61-74.

DNV Consulting. *Review of the efficacy of the safety assurance processes in preventing catastrophic accidents.* London: The RSSB, 2004.

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

E.Apostolakis, George. "How Useful is Quantative Risk Assessment." 24, no. 3 (2004): Risk Analysis .

Einstein, Albert. *Relativity.* London: Routledge, 1920.

Ekekwe, Ndubuisis. *Better Risk Communication.* 11 May 2011. http://blogs.hbr.org/cs/2011/05/better_risk_communication.html (accessed September 29, 2011).

Elliot, John. "Systems Approach to Safety-related Systems." London: Springer-Verlag London Limited, 1999. 75-98.

Elliott, Chris, Taig,T. *T230 a Ethical Basis of Rail Safety Decisions.* London: RSSB, 2003.

Etzioni, Amitai. "Humble Decision Making." *The Harvard Business Review*, 1989: 122-26.

Evans, Andrew. "Fatal accidents at railway level crossings in Great Britain: 1946-2009." *Accident Analysis and Prevention*, 2011: 1837-1845.

—. "Fatal Train Accidents on Britain`s Main Line Railways: End of 2009 Analysis ." *Center for Transport Studies, Imperial College London* . March 2010. http://www.cts.cv.ic.ac.uk/html/ResearchActivities/publicationDetails.asp?PublicationID=1330 (accessed October 04, 2011).

Fischhoff, Baruch. "Setting Standards : a Systematic Approach to Managing Public Health and Safety Risks." *Management Science* 30, no. 7 (1984): 823-43.

G.J.Bearfield; R.Short. "Standardising Safety Engineering Approaches in the UK Railway ." *The Sixth International System Safety Conference.* Birmingham: The Institution of Engineering and Technology , September 2011. 5.

G.March, James, and Zur Shapira. "Managerial Perspectives on Risk and Risk Taking." *Management Science* (The Institute of Management Science) 33, no. 11 (1987): 1404-418.

G.W, Leibniz. *Philosophical Texts.* Translated by R.S.Woolhouse and Richard Franks. London: Oxford University Press, 1695/1998.

Gissing, Bruce, and A.Terry Bahill. "Re-evaluating Systems Engineering Process Using Systems Thinking." *Systems Engineering* (The Institution of Electrical and Electronic Engineers) 28, no. 4 (November 1998): 516-27.

Goddard, E. "Supervision and operation of mass transit system." *Seventh Vacation School on Railway Signalling and Control Systes.* Glasgow: The Institution of Electrical Engineers, 1998.

Goodwin, Phil. *Determination and Denial: The Paradox of Safety Research and Traffic Policy* . London: The 17 thParliamentary Lecture on Transport Safety, PACTS , 2006.

Graham Walker. "The Science of Morality ." Edited by Graham Walker. London : RoyaL College of Physicians, 2007. 130.

Gray, Gigerenzer and J.A.Muir. *Better Doctors, Better Patients, Better Decisions; Envisioning Health care.* Cambridge, MA: MIT Press, 2011.

Gunderson, Scott. "A Review of Organizational Factors and Maturity Measures for System Safety Analysis." *Systems Engineering* 8, no. 3 (2005): 234-44.

H.Popkin, Richard, and Avrum Stroll. *Philosophy* . Oxford: Butterworth Heinemann, 1969.

Hale, Andrew., P.H.Lin, and A.L.C Roelen. "Accident Models and Organisational Factors in air tranport: the need for multi-method models." *Safety Science* 49 (2011): 5-10.

Hall, Stanley. *Modern Signalling Handbook.* Skipton: Ian Allan, 2010.

—. *Railway Detectives.* London : Ian Hall, 1990.

Hall.S, and Peter Van Der Mark. *Level Crossings.* Hersham: Ian Allan Publishing, 2008.

Halvorsrud, Gunhild. *The Asta Train Crash, its Precursors and Consequences, and its Investigation.* London : The Safety-Critical Systems Club, Springer , 2002.

Handy, C. *Understanding Organisations.* 4th. London: Penguin Books, 1999.

Hollnagel, EriK, and Woods David.D. "Cognitive Systems Engineering: a New Wine in New Bottel." *International Journal of Man-Machine Studies* 18 (1983): 583-600.

Hovdon, J, Storseth, and R,N Tinmmanvisk. "Multilevel Learning From Accidents: Case Studies from Transport." *Safety Science* 49 (2011): 98-105.

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.

Human Factors Group, Health and Safety Laboratory . *Review of Railway Safety's Safety Risk Model, HSL/ 2002/06.* Sheffield: The UK Health and Safety Executive, 2002.

Hume, David. *A treatise of Human Nature.* 1984. London: Penguin, 1739/1984.

I.Mitrani. *Simulation technqiues for discrete event systems.* Cambridge: The Press Syndicate of the Cambrigde University Press, 1982.

IEC. *61508: Funtional Safety of electrical/electronic/programmable electronic safety- related systems.* Brussels: International Electro-technical Commission, 2001.

IEEE Computer Society. *IEEE 1220 Standard for Applicationn and Management of the Systems Engineering Process.* The Institute of Electrical and Electronics Engineers, 1998.

ISO/IEC. *System Engineering- System life cycle ISO/IEC 15288.* International Standard, Brussels: The International Elecctro-Technical Commission, 2002.

J.Fabrcky, Wolter, and Benjamin S.Blanchard. *Systems Engineering and Analysis.* Prentice Hall, 2005.

J.M.Coulson, and .J.F.Richardson. *Chemical Engineering*. Oxford: Pergamon, 1965.

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

Joao Batista Camargo Junior, Jorge Rady de Almeida Junior. "The Safety Analysis Case in the Sao Paulo Metro." *Towards System Safety* . London: Springer, Safety-Critial Systems Club , 1999. 110.

Johnson, C.W. "Reasons for the Failure of Incident Reporting in the Healthcare and Rail Industries." *Proceedings of the Tenth Safety-critical Systems Symposium.* London: Springer-Verlag, 2002. 31-57.

Johnson, Chris. *What are Emergent Properties and How Do They Affect Engineering of Complex Systems.* Exploration, Glasgow: Glasgow University, 2006, 14.

Johnson.W.G. *Management Oversight and Risk Tree SAN 821-2.* Washington D.C: US Atomic Energy Agency, 1974.

Kelly, Tim. "Are Safety Cases Working?" January 2008: 5.

Kingston, John., Robert Nertney, Rudolf Frei, Philippe Schalllier, and FloorKoornef. "Barrier Analysis Analysed from MORT Perspective." *PSAM7/ESREL '04 International Conference on Probabilistic Safety Assessment and Management.* Berlin: Springer-Verlag, London , 2004.

Kletz, T. "Accident Investigations-Missed Oppurtunties." *Components of System Safety.* London: Springer-Verlag London Limited , 2002.

Kletz, T, D Mansfield, and L Poulter. *Improving Inherent Safety, OTH 96521.* Sheffiled: The UK Health & Safety Executive, 1996.

L.Derby, Stephen, and Ralph Keeny. "How Safe is Safe Enough." *Risk Analysiss* (Wiley & Sons) 1, no. 3 (1981): 21-24.

L.Janis, Irving, and Leon Mann. *Decision Making.* New York: The Free Press, 1977.

Ladkin, Peter. *Why Because Analysis* . 1 January 1995. http://www.rvs.uni-bielefeld.de/ (accessed Septmeber 13, 2011).

Leveson, N. "The Need for New Paradigms in Safety Engineering ." *Proceedings of the Seventeenth Safety- Critical Systems Symposium.* Brighton,UK: Springer-Verlag , 2009. 3-20.

Leveson, Nancy. "A New Accident Model for Engineering Safer Systems." *Safety Science* 42, 2003: 237-230.

Leveson, Nancy. "Applying Systems Thinking to Analyse and Learn from Events." *Safety Science* (Elsevier), 2011: 55-64.

—. "The Need for New Paradigms in Safety Engineering." *Safety-Critical Systems: Problems, Processes and Practice.* London: Springer-Verlag London Limited, 2009. pp. 3-20.

Lovallo, Dan, and Daniel Kahneman. "How Optimism Undermines Executives' Decisions." *Harvard Business Review* , July 2003: 8.

M.Copi, Irving, and Carl Cohen. *Introduction to Logic.* New Delhi: Pearson Education, 1998.

Maidment, David. "System Safety: challenges and pitfalls of Intervention." *New Technologies and Work* . Oxford : Elsevier Science, 2002.

Manu, Sage. *Laws of Manu, Manu Smrithi.* Translated by Wendy Donhier with Brian Smith. London: Penguin Classics, unknown/1951.

McCormick, Matt. *Immanuel Kant: Metaphysics.* 30 June 2005. http://www.iep.utm.edu/kantmeta/ (accessed October 2011, 2011).

NEP. *National ERTMS Programme Report.* London : National ERTMS Programme Team , 2003-2004.

Nicholson.M, and 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) 20, no. 1 (Septembe 2010): 14-19.

Nikhilananda, Swami. *The Bhagavad Gita.* New York: Ramakrishna-Vivekananda Center, 1944.

Noordwijk Risk Foundation. *the NRI Foundation website.* 1998. www.nri.eu.com (accessed September 29, 2011).

Office of Rail Regulator. *HMRI's Risk Profile Topic Strategy for Level Crossings.* 2008-09 to 2009-10. http://www.rail-reg.gov.uk/upload/pdf/RPT-levxings.pdf (accessed October 04, 2011).

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

Penrose, Roger. *The Road to Reality.* London: Jonathan Cape, 2004.

Perrow, Charles. *Normal Accidents.* 1999. New Jersey: Princeton University Press, 1984.

Plato. *The Republic.* Translated by Desmond Lee. London: Penguin Books, 375 BC/1995.

Popkin H. R, Stroll,A. *Philosophy.* Oxford: Butterworth Heinemann, 1969.

Quayzi, X. "Are Best Practises Really Best Practises." *The Sixth International System Safety Conference* . Birmingham : The Instituion of Engieering and Technology , 2011. 4.

R.L.Maguire, and C.J. Brain. "History and Perception of the Language Used in the Safety Domain." *The 1st IET International Conference on System Safety.* London: Institution of Engineering and Technology, 2006. 196-01.

Rae, Andrew. *Safety Decision Making Using Cost-benefit Analysis* . Newcastle,UK: Safety Critical Systems Club Newsletter, 2010.

RAIB. *Fatal accident at Moreton-on-Lugg, near Hereford, 16 January 2010.* Accident Report 04/2011, The RAIB, UK Department for Transport, 2011.

Railway, Board British. *Group Standard GH/CZ0002* . Derby: The British Railway Board, 1993.

Rasmussen, J. *Information Processing and Human-Machine Interaction.* New York: Elsevier Science, 1986.

Rasmussen, J, A M Pejtersen, and L P Goodstein. *Cognitive Systems Engineering.* New York: John Wiley& Sons, Inc, 1994.

Rassmussen. "Risk Management in Dynamic System: A Modelling Problem." *Safety Science* (Elsevier Science Limited) 2/3 (1997): 183-213.

Rassmussen, J. "Risk Management in a dynamic society: a modelling problem." *Safety Science* (Elsevier Science Limited) 27, no. 2/3 (1997): 183-213.

Rassmussen, M.L. "A Systens View of The Self." *The 48th Annual Meeting of the International Society for the Systems Sciences.* The International Society for the Systems Science, 2004.

Reason, J. *Human Contribution: Unsafe Acts, Accidents and Heroic Recoveries.* Surrey: Ashgate Publishing , 2008.

—. *Human Error.* 17th. New York: Cambridge University Press, 1990.

Reason, James. *Recurrent Patterns in Transport Accidents: Conditions and Causes.* London: 18 th Parliamentary Advisory Council for Transport Safety, 2007.

Ring, Jack. "Towrds an Ontology of Systems Engineering ." *Insight* , April 2002: 19-23.

Risk Solutions. *Development and Calibration of Model for Guaging Societal Concern for the Railway Industry.* London: The RSSB , 2006.

Roberts, C, F P G Márquez, and A M Tobias. "A Pragmatic Approach to the Condition monitoring of Hydraulic Level Crossing Barriers." *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit,.* Birmingham: The Sage Publications , 2010. 605-10.

Robinson, D & Garrat. *Introducing Ethics.* London: Icon Books Limited, 2008.

Roland, Harold E., and Brian Moriarty. *System safety engineering and management* . Danvers. M.A: John Wiley& Sons, 1990.

RSSB. *Annual Safety Performance Report 2010/11.* London: RSSB, UK, 2010/11.

—. *Requirements for Level Crossings.* 06 Feb 2010. http://www.rgsonline.co.uk/Railway_Group_Standards/Control%20Command%20and%20Signalling/Railway%20Group%20Standards/GIRT7012%20Iss%201.pdf (accessed October 04, 2011).

Rupert Woodfin, Oscar Zarate. *Introducing Marxism.* Royston: Icon Books Ltd, 2004.

S.Baker, Gary. *Human Capital.* 3rd. Chicago : The University of Chicago Press, 1964.

S.Blanchard, Benjamin, and Wolter J.Fabrcky. *Systems Engineering and Analysis.* Prentice Hall , 2006.

Schopenhaeur, A. *On the Principle of Sufficient Reason.* Translated by Karl Hillebrand. New York: Prometheus Books, 1820/2006.

Singh, Simon. *The cracking codebook.* London: Harper Collins, 2001.

Skogstad, Øystein. *Experiences with Safety Case Documentation According to CENELEC Railway Safety Norms.* London: The Safety-Critical Systems Club, Springer, 1999.

Smith, Adam. *Wealth of Nations, The Nature and Causes of the Wealth of Nations.* New York: Modern Library, 1776/1937.

T, Taig., and Elliot.C. *Ethical Basis of Rai Safety Decisions.* London: RSSB, 2003.

Taleb, Nassim N., Daneil G. Goldstein, and and Mark W.Spitznel. "Six Mistakes Execuives Make In Risk Managment." *Harvard Business Review*, 2009.

The BBC. "Engineers can learn from slime." *The BBC.* 22 January 2010. http://news.bbc.co.uk/1/hi/8473316.stm (accessed October 03, 2011).

The BBC News. *China train crash: Design flaws to blame - safety chief.* News, Unknown: The BBC News, 12 August 2011.

The BBC News. *'Rats' cause misery for London King's Cross commuters.* unknown: The BBC News, 27 Septmber 2011.

The Economist. "Difference Engine: Disaster waiting to happen." 16th September 2011. http://www.economist.com/blogs/babbage/2011/09/reliability-grid (accessed September 17, 2011).

—. "The Deepwater Horizon Report." *Economist*, 13th January 2011.

The Economist. *Goodness has nothing to do with it.* Unknown: The Economist, 24 September 2011.

—. "So long, and thanks for all the quarks, Science and Technology section." 1-7th October 2011.

—. "All power tends to corrupt." *The Economist*, 1st-7th October 2011: 87-.

—. "Left to their own devices,Medtronic and the woes of America's medical-technology industry." *The Economist*, 10th September 2011.

The NEL Consortium. *Train Protection - Technical review of the ERTMS Programme Team report, The UK HSE Reserach Report 067.* Norwhich: The UK Health and Safety Executive, 2003, 54.

The Office of Rail Regulator . *ORR, Railway Safety Publication 7, Guide for level crossing managers, designers and operators.* The UK Office of Rail Regulator , 2011.

The Office of Rail Regulator. *Facts & figures on Level Crossings.* 25 January 2008. http://www.rail-reg.gov.uk/server/show/nav.1568 (accessed October 04, 2011).

The RAIB . *Investigation into an incident at Llanbadarn level crossing, 19 June 2011.* 19 June 2011. http://www.raib.gov.uk/publications/current_investigations_register/110619_llanbadarn.cfm (accessed September 29, 2011).

The RAIB. *Fatal Accident involving a Train Driver Deal, 29 July 2006.* Derby: The RAIB, 2006.

The RAIB. "RAIB Accident Report 04/2011, Fatal accident at Moreton-on-Lugg, near Hereford, 16 January 2010, Accessed on 15th June 2011." Derby, 2011.

The Royal Academy of Engineering. *Engineering Ethics in Practice: Short Version.* August 2011. http://www.raeng.org.uk/societygov/engineeringethics/pdf/Engineering_ethics_in_practice_short.pdf (accessed October 07, 2011).

The UK Health and Safety. "Assessing compliance with the law in individual cases and the use of good practice." *The UK Health and Safety Executive.* 2003. http://www.hse.gov.uk (accessed 10 04, 2010).

The UK Health and Safety Executive. *Why Control Systems Go out of Failure.* The UK Health and Safety Executive, 2003.

Tolstoy, Leo. *My Confession and the Spirit of Christ's Teaching.* London: Walter Scott, Limited, 1887/1930.

Turner, Barry A. "The organisational and Inter-organisational Development of Disasters." *Adminstrative Science Quaterly* (Johnston School of Management, Cornell University) 21, no. 3 (1976): 378-97.

Turner, S.D. "Jublilee Line Upgrade From Cross Acceptance to Revenue Service." *The 6th IET International System Safety Conference.* Birmingham: Institution of Engineering and Technology, 2011. 7.

Tversky, Amor, and Kahneman Daniel. "Judgement Under Uncertainty: heuristics and biases." *Science*, 1974: 1124-31.

Valerie, Roebuck. *The Upanisads.* London: Penguin Books, 2003.

W.Maier, Mark, David Emery, and Rcih Hillard. "ANSI/IEE 1471 and Systems Engineering." *Systems Engineering* (INCOSE and Wiley Subscription Services) 7, no. 3 (2004): 257-70.

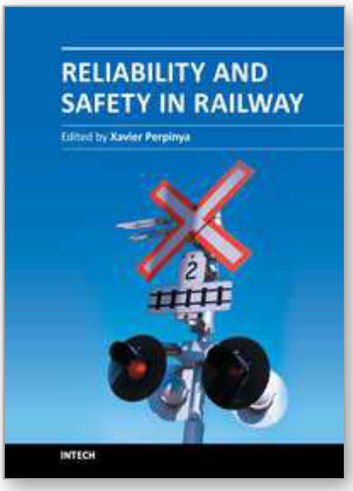
Wainwright, Martin. *Two arrested over railway cable theft on east coast mainline.* The Guardian, 21 September 2011.

Wei, Choo Chun. "Organisational Disasters, Why they happen and how they may be prevented." *Management Division* 46, no. 1 (2008): 32-45.

Weyman, A & Pigdeon, N & Jeffcott, S & Walls, J. *Organisational Dynamics and Safety Culture in UK Train Operating Companies.* Norwich: UK Health and Safety Executive, 2006.

Whitehead, Alfred North. *Process and Reality.* 1985. New York: The First Free Press, 1927/1978.

Whittingham, R.B. *The Blame Machine.* Burlignton: Elsevier Butterworth-Heinmann, 2004.
Wicks, R. *The Stanford Encyclopedia of Philosophy.* Edited by Edward N. Zalta. 17 Nov 2007. http://plato.stanford.edu/archives/win2010/entries/schopenhauer (accessed September 05, 2011).
Wikipedia. *Earth potential rise.* 4 May 2011. http://en.wikipedia.org/wiki/Earth_potential_rise (accessed September 18, 2011).
—. *System safety.* 21 June 2011. http://en.wikipedia.org/wiki/System_safety (accessed September 25, 2011).
Winter, Peter. *Compendium on ERTMS.* Hamburg: DVV Media Group GmbH, 2009.
Wkipedia. "Swiss Cheese Model." *Wkipedia.* 15 September 2011. http://en.wikipedia.org/wiki/Swiss_cheese_model (accessed September 25, 2011).
Wolff, J. *T230b Railway Safety and Ethics of Tolerability of Risk.* London: RSSB, 2002.



Reliability and Safety in Railway

Edited by Dr. Xavier Perpinya

ISBN 978-953-51-0451-3

Hard cover, 418 pages

Publisher InTech

Published online 30, March, 2012

Published in print edition March, 2012

In railway applications, performance studies are fundamental to increase the lifetime of railway systems. One of their main goals is verifying whether their working conditions are reliable and safety. This task not only takes into account the analysis of the whole traction chain, but also requires ensuring that the railway infrastructure is properly working. Therefore, several tests for detecting any dysfunctions on their proper operation have been developed. This book covers this topic, introducing the reader to railway traction fundamentals, providing some ideas on safety and reliability issues, and experimental approaches to detect any of these dysfunctions. The objective of the book is to serve as a valuable reference for students, educators, scientists, faculty members, researchers, and engineers.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Sanjeev Kumar Appicharla (2012). System for Investigation of Railway Interfaces (SIRI), Reliability and Safety in Railway, Dr. Xavier Perpinya (Ed.), ISBN: 978-953-51-0451-3, InTech, Available from: http://www.intechopen.com/books/reliability-and-safety-in-railway/railway-system-safety

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen