Safety analysis in a modern railway setting

Barnatt, Neil; Jack, Anson

DOI:
10.1016/j.ssci.2018.08.005

Document Version
Peer reviewed version

Citation for published version (Harvard):
Barnatt, N & Jack, A 2018, 'Safety analysis in a modern railway setting', *Safety Science*.
https://doi.org/10.1016/j.ssci.2018.08.005

Abstract

This paper provides a review of the current approach to risk analysis in the GB railway. It is set against a background of a comparatively high level of perceived safety. The railway is undergoing a modernisation that will result in new operating paradigms which rely on the interconnection of systems and integration of operating processes to obtain efficiencies. There is recognition that in the modern railway environment complexity has increased which has led to questions of whether current methods are still appropriate without modification or support. Conceptually current methods may be usable, but a robust analysis would prove complex and is difficult to demonstrate completeness. There is an understanding that a trade-off is required between complexity created by all the interconnections and the ability of the human engineer to understand. A modified approach is proposed that takes advantage of systems engineering to simplify the problem while at the same time capturing key system risks. There is an outline of the proposed further research to develop the method of analysis further.

Title **Safety analysis in a modern railway setting**

Authors:

Neil Barnatt email:- njb619@student.bham.ac.uk corresponding author

Prof Anson Jack email:- a.c.r.jack@bham.ac.uk

Correspondence address:

Birmingham Centre for Rail Research and Education
School of Engineering
University of Birmingham
Edgbaston
B15 2TT

Safety Science paper

Title **Safety analysis in a modern railway setting**

Abstract

This paper provides a review of the current approach to risk analysis in the GB railway. It is set against a background of a comparatively high level of perceived safety. The railway is undergoing a modernisation that will result in new operating paradigms which rely on the interconnection of systems and integration of operating processes to obtain efficiencies. There is recognition that in the modern railway environment complexity has increased which has led to questions of whether current methods are still appropriate without modification or support. Conceptually current methods may be usable, but a robust analysis would prove complex and is difficult to demonstrate completeness. There is an understanding that a trade-off is required between complexity created by all the interconnections and the ability of the human engineer to understand. A modified approach is proposed that takes advantage of systems engineering to simplify the problem while at the same time capturing key system risks. There is an outline of the proposed further research to develop the method of analysis further.

Keywords: risk, DSM, system, complexity, network, parallelism, simplicity, SRK

1 Introduction

Although the railway in the UK has operated without a major accident for over ten years (Rail Safety and Standards Board 2017) there are worrying questions relating to the appropriateness of traditional methods of risk analysis and the possibility that present good fortune is masking impending problems as technology, the railway and the methods of operation, evolve to satisfy growing demands from the public. A fundamental change in the operation of the railway is taking place through the introduction of a “Digital Railway” (Network Rail 2017), and this creates challenges for traditional approaches to safety analysis. In the new world, some of the ‘slack’ is eliminated from the railway system to get more out of the current assets which may, in turn, reduce traditional safety margins that have been implicitly inbuilt for decades.

While the safety analysis statements in this paper are generally applicable to any railway administration, some underlying assumptions relate to the UK and its legal system which is based on the concept of reasonable practicability. This is in direct contrast to some other European systems that clearly define set levels to be achieved, such as in Germany. The paper is modelled on the UK and the GB segment of the UK in particular. Principally this is to acknowledge the differing regulatory framework in the UK, whilst the majority legislation equally applies to the whole of the UK, there are some differences between GB and other parts of the UK. This matters in the context of the paper, because currently, bodies that are implicitly part of the regulatory framework like the Rail Safety and Standards Board (RSSB) represent the GB mainline rail only. Likewise, statements by the GB safety authority the Office of Rail and Road (ORR) do not apply to other parts of the UK.

Traditional safety analysis of railway systems has focused on the suitability of single systems resulting in individual acceptances. Today systems tend not to operate in isolation if they ever really did. The vogue is for connection of computer-driven systems into a whole railway system that brings new functionality and efficiency. However, when analysing, changing and

introducing these systems, it is not clear that sufficient consideration is given to the interaction between the change and the existing environment.

This paper considers a method of providing a valid analysis by drawing on and combining influences in other operational domains.

2 Safety process models and parallelism

There has been criticism, (Leveson 2011) among others that current methods are serially orientated in their approach, examples such as Failure Modes Effects Analysis (FMEA) and James Reason's Swiss Cheese Model (SCM) are cited. However, these criticisms had already been contested by (Reason, Hollnagel and Paries 2006) through the EUROCODE report, asserting that criticisms of this type were as a result of misconceptions about how to use the SCM and the understanding of its intended limitations. The primary arguments have not changed in the intervening period between the two publications. At the heart of the SCM concept, there are many paths through to an accident and that these merely need to line up (conceptually) for an accident to occur. In later versions of the model, there is a concept of semi-parallelism, because there can be more than one hole in each barrier. Further, these holes vary in size as circumstances change, giving the model a dynamic quality. There has been further criticism from (Leveson 2011), that SCM is not fit to analyse risks because it does not provide the necessary detailed causal analysis. (Reason, Hollnagel and Paries 2006) had anticipated this line of criticism by stating that this was never the intent. It is almost as if Leveson had not read the arguments from Reason and others or at least not accepted them. Similar criticisms of a lack of parallelism can be constructed for the FMEA from the works of (Anleitner 2010). While points of potential failure are identified separately within the FMEA technique, it is clear that there is no intent to imply sequencing. There are other, more relevant, issues concerning the depth of analysis that is required that affect the usability of FMEA in a practical setting.

An interesting facet of current models, in particular Systems Theoretic Accident Model and Process (STAMP) by (Leveson 2011) and versions of SCM is that they give greater weight to the organisational complexity and the operation and governance of a system without an equal emphasis on the technical construction and regular operation. For example, STAMP looks at the organisation starting with government regulation and policy feeding down through the company and eventually coming to the operational level at which point it is combined with the technical system. For the railway industry, much of this organisational sphere is predetermined through regulation and is a fixed framework within which industry has to operate. (Rasmussen 1997) proposes that this type of control is simply treated as another import into the technical analysis of the system, in this case, the railway system.

It is interesting to note that in studies of the usage of safety analysis systems, (Underwood and Waterson 2013), it has been shown that SCM remains popular while Leveson's STAMP approach has not generally been adopted by industry, although it remains an important academic tool. In a different field, outdoor pursuits, there has been further support that STAMP is too complex from (Salmon, Cornelissen and Trotter 2012). Extrapolating from this and previous paragraphs it can be concluded that whatever system is adopted it needs to be simple to apply otherwise it is unlikely to be adopted in the industry.

An interesting fact is that the railway industry guidance, (Rail Safety and Standards Board 2014a), on such matters does not name SCM nor STAMP and instead refers to techniques such as simple cause-frequency-consequence analysis using ranking tables, Fault Tree Analysis (FTA), Failure Modes Effects and Criticality Analysis (FMECA) and FMEA; other previous publications such as (Rail Safety and Standards Board 2007) have taken a similar

approach. Of these techniques, only FTA addresses the issue of combinatory risks. The publications from RSSB, (Rail Safety and Standards Board 2007) and (Rail Safety and Standards Board 2014a), place great store in the hazard identification rather than the analysis of combining risks to gain an overall picture. It could be surmised that the philosophy employed is to identify everything through a first principles review of equipment/process under consideration which can be flawed in a connected world if the focus is on a single or limited set of systems that are undergoing change. The 'identification in isolation' approach which considers each hazard separately is supported in some respects through the legislation as expressed in CSM-REA (Common Safety Method-for Risk Assessment 2013) and the guidance is merely a reflection of this. Overall parallelism, as described by SCM, in the hazard analysis is achieved by default. This is because conceptually, any hazard can occur at any time in these simple table formats. There is no in-built sequencing in this analysis approach because each hazard is dealt with separately; consequently, the effect of parallelism is achieved more by chance than design.

3 Modern systems – computers, parallelism and complexity

The sequential methods may have been appropriate for liquid flow systems, however in a computer-based connected world; hazards can be spread throughout the software of a typical system (Bishop, Bloomfield and Froome 2001). This work cites examples, where errors are introduced as a consequence of corrections to other errors and undocumented features. As a consequence, it is the norm for software-based systems to be used with many latent hazards still present just waiting for the appropriate trigger conditions. Most modern control systems have a computer embedded system within them that performs relatively simple functions controlled through a series of algorithms that mimic more cheaply the physical components that were used in older systems. The shortcomings identified by (Bishop, Bloomfield and Froome 2001) would not have occurred in older systems because of the comparative lack of computerisation and their relative simplicity which relied on the original physical properties. Moreover, in the railway industry standards such as EN50129 (CENELEC 2003), rely on an engineering process which applies a series of methods through EN50128 (CENELEC 2011) to reduce software error rather than a methodical error and hazard elimination approach. The latter approach works through testing, identifying, and a correction process of every possible combination. Therefore, under EN50129 (CENELEC 2003) the best that can be claimed is a statistical reduction in the error and hence hazard population.

With these systematic errors in software, a risk condition is triggered by the satisfaction of trigger values that satisfy a logical condition for the execution of erroneous code. As these computers get connected in parallel through design topologies, many hazards are potentially able to be triggered dependent on a variety of trigger conditions. False confidence is drawn from the fact that testing has not revealed errors, simply because the entire domain cannot currently be completely tested. The understanding of the systems risk is described through an adaption of the Boston Consulting matrix to a risk environment.

		Risk	
		Known	Unknown
Understanding	Known	Specification	General industry knowledge
	Unknown	Design/operation outcomes	Unknown unknowns

Figure 1 Risk and understanding matrix, adapted from Boston Consulting matrix(Bowman 1990)

Figure 1, describes the relationship between understanding and risk. Where a risk is known, and it is understood a specification can be written to eliminate or control the risk. Similarly, risks associated with the design are known but maybe not entirely understood and possibly not tested fully. Some risks exist that are implicitly understood within the rail industry but are not explicitly associated with a particular instance. Likewise, where there is no understanding and the risk is not known testing is unlikely to be undertaken at all. If the size of the specification cell is larger relative to the other cells, the testing is more likely to be successful.

Even where equipment is tested against test specifications the testing will only be as good as the understanding of the system and its specification by the originator of that specification. Even here there could be gaps. The really dangerous area is the unknown unknowns which is an area where hazards can reside undetected. Again, identifying risks on equipment is subjected to the same vagaries such that the analysis is only as good as the understanding of the system. There have been attempts to fill the void with software products, for example in the area of signalling (Duggan and Borälv 2015). Even here the safety models are just reflections of “opinions” of experts. Formal method B (Boulanger 2014) has been applied to metro systems produced by two manufacturers on a limited scale, again it is not used on a wide scale in the industry, perhaps because of the complexity. The claims made by (Boulanger 2014) are limited to assuring the correct translation from the Abstract Machine specification in B to the Implementation specification in B. (Boulanger 2014) acknowledges that it is possible to create a formal specification that is actually incorrect even when the associated proofs assert the specification is right. Furthermore, there is the acknowledgement that external, traditional validation is required to provide the assurance. Therefore, there is little advance on the traditional approaches to software generation and the assertions from Figure 1 are still valid in a formal environment. However, unless the unknown unknowns can be specified the coverage of hazards is likely to be incomplete, and in part, this is linked to a complete understanding of the problem domain.

4 Complexity, understanding and analysis

(Manson 2001), has classified complexity into three types: algorithmic complexity, deterministic complexity and aggregate complexity. Algorithmic complexity refers to the complexity of the calculations, deterministic complexity represents the interactions of the

multiple variables. It is the aggregate complexity which is concerned with how systems are combined to create an emergent behaviour. As a consequence, when analysing the combined system for risk, the algorithmic complexity also increases. As pointed out by (Manson 2001), the complexity can reach a point where the problem is beyond current human understanding to be able to solve manually. This notion of complexity is aligned with the Rasmussen's Skills, Rules Knowledge (SRK) model cited by (Whittingham 2004) where reference is made to the principle of cognitive economy that acknowledges there is a human limit to the assimilation of information and the understanding of implications. The assertion is that human behaviour refines a task to that which involves the least cognitive effort, if possible by employing rules and utilising practised skills. A good deal of safety analysis is rule-based in the sense that methods are laid down about how to undertake the process, an example being Common Safety Method for Risk Evaluation and Assessment (CSM-REA), (Common Safety Method-for Risk Assessment 2013).

Even in an SRK model, the rules and strategies have to be correct to provide a valid answer. This notion is supported by (Reason 1997) who coined the phased of 'mispliance', to refer to the application of a bad rule which will produce an unsafe result. As technology moves on, rules that were good at some point in history can turn bad because the principles that underpin their creation have changed. (Leveson 2011) also asserts this point. An example is the implication that operators of machinery, tools and processes understand how they work. Today that is often not valid as complexity is hidden and often handled by the unseen computer, as happened in the Mulhouse air disaster (Whittingham 2004); only when the system moves out of the normal mode of operation do such flaws become apparent. (Leveson 2011) extends this to argue that the very nature of accidents is changing because the technology and the art of what is possible has advanced. Therefore, by inference, the rules may indeed not be adequate to analyse the risks in a modern setting. (Leveson 2011), in analysing the systems environment, makes the point about appropriateness and links this to complexity indicating that only the simplest systems are understandable. Intuitively this appears to be true, but there needs to be a calibration of what is meant by 'simple'.

The situation is further complicated by emergent behaviours of systems that occur as a result of the interaction between systems, a phenomenon that is highlighted by the International Council on Systems Engineering (INCOSE), (INCOSE 2015), and the resulting ISO 15288 standard (International Standardization Organization 2015). In other words, some features appear at a higher level of integration in a large system that do not even exist to be examined at the lower level. Consequently, the methods of analysis that were outlined in the previous section will largely only cater for the small-scale analysis and other significant hazards could be missed because the processes are not designed to recognise the interconnected emergent properties. There is clearly a need to examine systems at two levels; at the overall system level as well as its various subsystems, to gain a full understanding of its behaviour.

5 Systems

A traditional approach to limiting complexity has been to draw a boundary around the notional system and simplify the description of risk by concentrating on the system boundary rather than the internal operation. A side effect of implementing this scheme is that critical interactions can be missed as details are ignored and the effects are summarised.

An alternative method is to split the whole system into small subsystems; the complexity can then be controlled to facilitate understanding whilst retaining a grasp on the key detail. Therefore, important risks are less likely to have been missed during the analysis process. Without a recombination mechanism, this approach will be limited to either simple problems

or superficial treatment. The recombination after a decomposition should be undertaken selectively, only retaining important details, as outlined below.

A railway system can be thought of as comprising a set of subsystems. The interfaces are either physical, energy or informational. It is clear from observation that an isolated system transmits no risk beyond its boundary. Historically railway systems, such as a signalling or electrical control system, could be regarded as isolated or of limited connectivity through physical contact or energy transfer and therefore analysable through traditional risk analysis methods, for example, FMEA, treating it as an isolated entity. With modern systems, this isolation assumption is no longer valid because designs often connect electronic systems through communication devices. Analysis of the effects of change and hence risk in the overall railway system through these interconnections is analogous to attempts to analyse large complicated computer software. As with software, a complete analysis is not possible with current methods, such as FMEA or FTA, or even Bayesian networks. This is in part a side effect of introducing a relatively complex modelling technique to analyse the detail of a very large-scale problem. As was indicated in the previous section a point is quickly reached where the human analyst cannot comprehend the total of the details.

A related method of analysis used within the GB is the Safety Risk Model (SRM) maintained by (Rail Safety and Standards Board 2014b). This is a retrospective model which indicates the likelihood of selected key risks on a historical basis, and it includes information built from fault trees and event trees described by (Turner, et al. 2002). A positive aspect is that historical knowledge of relationships between the lower level elements is captured and summarised as higher-level hazards. However, given these high-level hazards, again the user is left with the problem of combining these published hazard elements into a coherent whole for the application and making sure that it is customised to reflect risk levels of an application. Consequently, while SRM provides support for the systematic reduction of identified risks, it offers no advance on the Bayesian networks complexity because of the difficulty of creating the application model.

By breaking the total system into small subsystems with interfaces that can be regarded as links a level of understandability can be established. This method aligns with systems theory as proposed by (Phelan 1999). A choice of analysis has to be made between establishing a plain connection between the subsystems and a more complicated connection that reflects the risk propagation properties. Should a plain connection option be selected, then it follows that the effects of the propagation have to be modelled either in the receiving or transmitting subsystem, increasing the complexity of the subsystem risk analysis. Conceptually it is easier to restrict these properties to the links, rather than incorporate them into the internal subsystem models, which is in alignment with complexity theory as described by (Phelan 1999). This theory refers to the overall complex behaviour being driven by a few simple functions of the contributing subsystems, which appeals from the perspective of understandability and analysability. If the functions can be isolated, then the model can be simplified.

Bayesian networks, (Marsh and Bearfield 2008), have been used to describe complex railway systems and their interaction in respect of safety risk. This analysis very quickly becomes complex and labour intensive. Large arrays are created that reduce the understandability of the system under analysis. It is possible to create a network using these techniques, but it would require as much effort as a risk model based on an FTA. As each vertex has a joint probability table (JPT) attached, which encapsulates the different risks at that point, it adds to the complexity of the overall model and hence the analysis. Consequently, for a practical analysis of a railway network which will result in a sizeable

Bayesian network the task has to be undertaken by a computer. As a result, the computer model itself will require effort to construct, and maintenance resource to remain valid when changes occur in the real-world on the railway network.

A linkage approach has been taken by (Parmar and Lees 1987) from the perspective of reliability. In this work, their paper asserted the case for a set of propagation equations, in concept a type of JPT but using physical parameters instead of probabilities. These were used to characterise the linkage between the different parts of the system and how each of the modelled components would modify the entities of interest. This model worked well in the example cited by (Parmar and Lees 1987) because of the fluid flow property of the plant being modelled. However, it is not clear that the assumptions made for the creation of the model would carry over to another type of technology because no evidence was presented in their paper to demonstrate an application in a different industrial environment. It is envisaged that there may be difficulties, where application projects use equipment without the detailed understanding of the transformations of the physical parameters within purchased subsystems; given the method's reliance on the use of physical parameters during system modelling to create the transforms.

To apply this approach to a generic risk model for a railway environment some simplification is necessary. A basic set of properties can be employed which are modelled on a similar system as used by (De Lessio, et al. 2015) in a change propagation model. For the risk environment, the links can be regarded as having one of three properties: an amplifier, a resistor and a carrier. By analysing these links, the propagation of risks can be better understood. A resistor acts to dampen the risk in the following subsystem, whilst a carrier transmits the risk unchanged; finally, an amplifier enhances the risk in the next subsystem in the chain.

To create a generalised model, it is necessary to transform simple chains previously considered into an interconnected network where the nodes (vertices) are the subsystems, and the arcs are the links, partially moving toward the Bayesian network model. To avoid the trap of overcomplexity, a Design Structure Matrix (DSM) can be employed to selectively register the connectivity of the links. DSM is used as an interface technique for systems engineering as documented by (Eppinger and Browning 2012). The links can act as resistor, carrier, amplifier elements, previously described, to enhance or limit the risk in the next subsystem in the chain. The risk once transmitted over the link will, of course, be transformed through the properties of the following subsystem before again being presented at its interfaces for onward transmission should the risk not be mitigated or contained within that subsystem.

The extent of the influence of a change can be described by tracing paths through amplifiers and carriers. Where a resistor is encountered, this is likely to form an effective limit of the influence of a risk through a network, assuming the reduction is substantial. This leads, therefore, to the conclusion that the complexity of a change can be simplified by drawing the system boundary at these points.

Consequently, the outlined methods proposed, DSM, system decomposition into subsystems, and simplification offer the prospect of facilitating analysis of complex systems in sufficient detail to draw safety conclusions, whilst not overwhelming the analyst with the complexity of the analysis.

6 Moving forward

Railways are developed in a commercial world where the requirement to deliver value and reduce timescales is ever present (Office of Rail and Road 2017). The opportunity to develop sophisticated analyses that require a lot of time and effort is not always available to the industry going forward and more practical methods are needed that give an accurate answer quickly, leading to a sufficiently safe outcome. It has been demonstrated in this paper that there are currently weaknesses in existing processes and it has been argued in this paper, that these simple, all-encompassing processes do not exist. The skills do not necessarily exist in the wider industry to be able to undertake these analyses, and therefore the need is to create a tool or method or process that at least, at the user interface, is simple to use and fits within the understanding of engineering practitioners.

An initial proposed research work stream is to use and adapt existing tools and techniques used in other industries and adapt or combine them together for use in the railway environment. The previous sections of this paper provide a number of candidates to be taken forward.

It has been demonstrated that to move forward with risk analysis of modern technology there is a requirement to map out or understand how the phenomena of the unknown-unknowns category is reduced as much as possible. It does not seem appropriate to rely on the procedural methods of current software engineering techniques, as described in EN50128 (CENELEC 2011) for example, to achieve this aim because there is no guarantee that errors will be eliminated. A statistical approach proposed by standards and (Leveson 2011) does not seem very appealing as there is no certainty that particular key hazards are addressed. A possibility that could provide a solution involves controlling the interfaces between subsystems and ensuring that those subsystems are small in concept, even if for practical purposes these are virtual in nature and the physical entity is much larger, constructed from several virtual components. As has been asserted earlier in this paper; as the understandability increases the scope of the unknowns shrinks. This throws more importance on how these subsystems are interconnected as the topology will have an impact on the ability to attenuate risks within the overall system.

An obvious candidate to parcel a railway system up into manageable sections is to use Bayesian Networks. However, it has been shown (Marsh and Bearfield 2008) that these are not without drawbacks, not least the requirement to create JPTs to encapsulate multiple probabilities at each vertex to describe the inter-relationship. This makes for a complex analysis. What is required is a means to simplify the network and to bound the problem. In systems engineering the DSM (Eppinger and Browning 2012) approach has been successfully used to describe interfaces or relationships between entities in a straightforward manner from binary indications to more complex indications. Reading these DSMs is intuitive because they clearly indicate where there is a relationship between two entities on a simple grid matrix, examples are given in a number of contexts by (Eppinger and Browning 2012); consequently, the DSM approach passes the understandability test. The DSM matrices lend themselves to being combined across multiple domains, referred to as Multiple Domain Matrix (MDM), that allows a user to take a readily understandable overview of the system and observe where the major connections exist and by inference the major risk propagation within the wider system. Importantly the overview will enable a sensible boundary to be constructed for the system/operation under consideration by combining and summarising the effects where feasible to constrain the problem to manageable proportions.

Further research is proposed to understand the shortcomings with present methods of safety analysis, including understandability of large-scale applications and the connectivity

problem. An initial objective is to gain a greater understanding of the actual techniques used routinely in the railway industry and to classify those techniques by simplicity, interface inclusion, whole risk and cause-consequence analysis effectiveness.

Consequently, it will be possible to identify where the strengths and weakness lie with regard to the analysis of modern connected systems and integrated operations. It is expected that a parameterised description can be put forward to identify when particular techniques are appropriate on a scale of operational integration and subsystem coupling and integration. Given the need for simplicity, the ideal form of output is a simple infographic for use by practitioners.

Future development will take the idea of connectivity and computerisation to develop the concept of risk propagation across the larger railway system. It is expected that the analysis undertaken will identify the speed of communication as a critical parameter that influences the impact propagation of risks. For example, currently, train consist information and braking allowance is a semi-paper-based activity, whereas moving to the future it is highly likely that it will be totally automated. Consequently, there will be less time to correct errors in the process before they take effect on live systems. Beyond this connectivity is the increasing reliance on other parts of the overall rail system to provide key information for a subsystem which could again increase the propagation properties of risk. Consequently, this could well reveal that crucial safety components are migrating to systems, for instance, business systems, that were previously not regarded as causing any safety risk. This migration is something that is not comprehensively considered in today's analysis, where the focus is on the technical element that has changed in isolation from the whole railway system.

By taking identified techniques, such as FMEAs for example, and combining them with new or clarified insights into the interaction of subsystems in today's railway, it is expected that an improved technique will be created by the authors as part of the research that is simple enough for practitioners to use in today's operational environment.

The proposed approach, using DSM and the identified techniques, will result in a documented process that is supported by simple templates to be filled in by practitioners. To assist with this, a knowledge-based system will be created by the authors to capture the lessons learned from the application. A suitable mechanism for hosting the system will be investigated as part of the research to make certain that the output is useful to industry and academics.

At this early stage in the research, whilst DSM has featured, in this paper as a clear candidate piece in the jigsaw to solve the conundrums set out it should not be looked at as the whole answer. In a sense, DSM has been the 'easy' first piece to identify, but it is not much use on its own without the other pieces. There are further issues such as understandability, encapsulation, systematic parallel paths, temporal continuity and calibration of links to fit into the jigsaw to provide a useable answer. Any final answer will be subject to the test of practicality for practitioners in today's industrial environment.

7 Conclusion

For some of the modern risk analysis techniques, there appears to be an over-emphasis on the role of the management structures and regulation. Because the railway environment is so heavily regulated a concentration on regulation and management structures appears irrelevant to a large extent. Of all the writers on this subject (Rasmussen 1997) appears to have correctly interpreted the reality of a heavily regulated industrial sector by treating this upper tier of the industry as providing a fixed set of requirements to be complied with. This

concept is applicable because it fits into the current regulatory framework for the UK that is set by a series of railway and health and safety regulations. Therefore, it would appear that the greatest advance can be made from refocusing efforts on the technical and operational arena.

It is clear from the analysis in this paper that there are some fundamental problems with risk analysis of modern railway systems as they become more complex and interconnected. These include the perceived assumption that there is a serial association between risks and controls, although it has been shown that this assumption is questionable given the techniques actually used in the industry. Some of the techniques that have been created to solve the perceived shortcomings have not found favour, indicating that they are either not fit for purpose or not readily understood. It could be that the techniques need 'industrialising' transferring them from the academic environment into the industrial landscape. However, it is unlikely that this will be successful given that there is a requirement for reduced costs and greater efficiency in providing rapid and cost-effective change to the railway. It has further been asserted in this paper that simplicity is what is required from practitioners in the railway environment; therefore, any proposed solution, even if it is internally complex or rests on complex theory needs to appear simple to the practitioner user of the system.

The environment is changing to the extent that computers are far more prevalent in modern systems and these systems, in turn, are linked through general communication bearers to other systems forming networks of functional nodes, whether intended or not. It has been shown that taking a pure network approach leads to an over-complex analysis. As the complexity of the analysis grows the chance of missing important risks is increased, and so is the temptation to simplify the modelling.

By applying the proposed scheme, from the research to be undertaken, it is envisaged that the correct balance can be struck between capturing the complexity and simplifying the model. DSM is currently seen as part of the way forward by providing a mechanism to identify the critical links whilst removing other non-important links. By linking this with notions of risk amplification, carriers and resistors, the depth of penetration of risks can be modelled.

8 References

Rail Safety and Standards Board (2017). "10 years after Grayrigg, rail passengers are safer than ever." Retrieved 28/5/17, 2017, from https://www.rssb.co.uk/News/Pages/10-years-after-grayrigg-rail-passengers-are-safer-than-ever.aspx.

Network Rail (2017). "Digital Railway." Retrieved 28/5/17, 2017, from https://www.networkrail.co.uk/our-railway-upgrade-plan/digital-railway/.

N. Leveson, G (2011). *Engineering a Safer World : Systems Thinking Applied to Safety*. London, MIT Press.

J. Reason, E. Hollnagel and J. Paries (2006). *Revisiting the Swiss Cheese Model of Accidents*. Bretigny-Sur-Orge, France, EUROCONTROL Agency.

M. A. Anleitner (2010). *Power of Deduction : Failure Modes and Effects Analysis for Design*. Milwaukee, ASQ Quality Press.

J. Rasmussen (1997). "Risk Management in a Dynamic Society: A Modelling Problem." Safety Science **27**(2/3): 183-213.

P. Underwood and P. Waterson (2013). "Systems thinking, the Swiss Cheese Model and accident analysis:A comparative systemic analysis of the Grayrigg train derailment using the ATSB, AcciMap and STAMP models." Accident Analysis & Prevention **68**: 75-94.

P. M. Salmon, M. Cornelissen and M. J. Trotter (2012). "Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP." Safety Science **50**: 1158-1170.

Rail Safety and Standards Board (2014a). *Guidance on Hazard Identification and Classification*. London, Rail Safety and Satandards Board.
Rail Safety and Standards Board (2007). *Engineering Safety Management (The Yellow Book) Volumes 1 and 2 Fundamentals and Guidance*. London, Rail Safety and Standards Board,.
Common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009 (2013). European Union.
P. Bishop, G, R. Bloomfield, E and P. Froome, K, D (2001). *Justifying the use of software of uncertain pedigree (SOUP) in safety related applications*, Health and Safety Executive.
CENELEC (2003). EN 50129:2003: *Railway Applications - Communication, Signalling and processing systems - safety related electronic systems for signalling*. Brussels, CENELEC.
CENELEC (2011). EN50128:2011: *Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems*. Brussels, CENELEC.
C. Bowman (1990). *The Essence of Strategic Management*. London, Prentice Hall.
P. Duggan and A. Borälv (2015). "Mathematical proof in an automated environment for railway interlockings." IRSE News(217): 2-6.
J. Boulanger (2014). *Formal Methods Applied to Industrial Complex Systems: Implementation of the B Method*. London, ISTE Ltd and John Wiley & Sons inc.
S. M. Manson (2001). "Simplifying complexity: a review of complexity theory." Geoforum **32**: 405-414.
R. B. Whittingham (2004). *The Blame Machine: why human error causes accidents*. London, Elsevier Butterworth Heinemann.
J. Reason (1997). *Managing the Risks of Organizational Accidents*. Aldershot, Ashgate.
INCOSE (2015). *Systems Engineering Handbook : A Guide for System Lifecycle Processes and Activities*. D. Walden, D, J. Roedler G, K. Forsberg, J, R. Hamelin, D and T. Shortell, M. Hoboken, New Jersey, United States of America, Wiley.
International Standardization Organization (2015). ISO/IEEE 15288:2015: *Systems and Software Lifecycle Process*. Geneva, International Standardization Organization.
Rail Safety and Standards Board (2014b). *Safety Risk Model: Risk Profile Bulletin, version 8.1*. London.
S. Turner, D. Keeley, M. Glossop and G. Brownless (2002). *Review of Railway Safety's Safety Risk Model*. Sheffield, Health and Safety Laboratory.
S. Phelan (1999). "A Note on the Correspondence Between Complexity and Systems Theory." Systemic Practice and Action Research **12**(3): 237-246.
D. W. R. Marsh and G. Bearfield (2008). "Generalizing event trees using Bayesian networks." Journal of Risk and Reliability **222**: 105-114.
J. C. Parmar and F. P. Lees (1987). "The Propagation of Faults in Process Plants: Hazard Identification." Reliability Engineering **17**: 277-302.
M. P. De Lessio, M. A. Cardin, A. Astaman and V. Djie (2015). "Process to Analyze Strategic Design and Management Decisions Under Uncertainty in Complex Entrepreneurial Systems." Systems Engineering **18**(6).
S. D. Eppinger and T. R. Browning (2012). *Engineering Systems : Design Structure Matrix Methods and Applications*. London, MIT Press.
Office of Rail and Road (2017). "Economic Regulation." Retrieved 28/5/17, 2017, from http://www.orr.gov.uk/rail/economic-regulation.