THE ROLE OF SAFETY RISK MANAGEMENT IN THE UK RAIL INDUSTRY WHEN DEALING WITH CYBER THREATS

NADIM CHOUDHARY
Ove Arup and Partners Ltd. Resilience, Security and Risk, London, UK.

ABSTRACT

This study will review the literature available on cyber security strategies (generally and those specific to the railway) and compare these against safety methodologies to determine whether there are any overlaps and whether a common risk approach can be used. An assessment will be made on the evaluation of cyber threats in the absence of statistical/historical data and the merits in applying a quantitative approach including consideration of Cost Benefit Analysis (CBA). It is important to note that as the safety and security disciplines have developed independently of each other, the same words (e.g. risk, hazard, threat, likelihood, probability etc.,) have subtle different meanings. The goal of Risk Management seeks to present arguments and/or demonstrations to support assertions that the identified risks have been managed in a way which satisfies the organisation's Risk Appetite and/or the principle of As Low as Reasonably Practicable (ALARP) and CBA.

Keywords: cost benefit, cyber, RAM, reliability, risk management, safety, security.

1 INTRODUCTION

Railways offer a safe and efficient means to transport passengers in the UK. Nevertheless, passengers face risks when travelling on the rail network, whether that be on the London Underground (LU) or the National Rail (NR) which ranges from the minor (slips, trips and falls) to the major (train derailment) risks and must be managed and minimised So Far As is Reasonably Practicable (SFAIRP).

With the changing environment and increasing customer demands, railways are having to upgrade their various operational activities and exploit new technologies to deliver:

1. An increase in the capacity of the railway;
2. More punctual and dependable railway services;
3. Lower unit cost of delivery;
4. Improvements in the safety of the railway;
5. Enhanced passenger experience;
6. Reduced journey times;
7. Greater flexibility to allow service delivery to match demand; and
8. A reduction in the environmental impact measured per unit of activity.

Several high profile projects, such as Crossrail, HS2 and the Thameslink modernisation programme will rely on digital technology to exploit the benefits as detailed above. This exploitation of technology or "digitisation" can include aspects like widespread public Wi-Fi as well as a rail workforce that are able to use mobile devices to deal with track faults. Simply put, the connection of these systems to the outside world presents a new risk – cyber and for the rail industry this is real and growing. Major cyber-security stories have become a recurrent feature on the news. Malware and hacking are now recognised daily global threats to every kind of infrastructure.

ISSN: 2041-9031 (paper format), ISSN: 2041-904X (online), http://www.witpress.com/journals
DOI: 10.2495/SAFE-V8-N1-48-58

In a connected world, the service improvements that technology makes possible also bring with them additional dangers. The London Underground is an example of this, facing increasing demand on its railway system, it has added more trains and therefore runs them much closer together, with digital technology controlling and managing the service. Great news for passengers, but this also means that malware-related incidents or failures have a potentially greater effect on the network and affect a greater number of travellers. And with more rail commuters, the network's need to recover and return the service to normal will be an even bigger priority. Additional impacts on railway stakeholders could include:

1. Disruption to services;
2. Loss of commercial or sensitive information;
3. Reputational damage;
4. Failure to comply with law;
5. Criminal damage;
6. Financial loss, including to the wider UK economy; and
7. Threat to safety of the workforce, passengers or the public, resulting in harm [1].

The seriousness of the threat from cyber is demonstrated by the UK Government adding cyber activity to its list of Tier One threats, alongside terrorism, war and global pandemic. According to a Cabinet Office report, Cyber-crime cost the UK economy £27bn in 2011 [2].

2 THE THREAT

According to Sky News [3], the UK railway network has suffered at least four major cyber-attacks over the last year alone. Sergey Gordeychik, a security researcher at Kaspersky Lab in Moscow has discovered several weaknesses in rail infrastructure. He told Sky News: "Hackers can get access to not only to simple things like online information boards or in-train entertainment, but also to computer systems which manage trains by itself, which manages signals, manage points, and in this case, if they have enough knowledge, then they can create real disaster related to train safety.

In December 2015, power stations in Ukraine were taken offline following a hack. According to a report by Verizon, hackers took control of a water treatment plant, changing the chemical make-up of the water.

Operation Technology (OT) supports physical value creation and manufacturing processes. It therefore comprises the devices, sensors and software necessary to control and monitor plant and equipment. Information Technology (IT), on the other hand, combines all necessary technologies for information processing. Operational systems enable the operational railway to function through controlling such things as train movements, signalling, power, telecommunications, and station management.

During the last decade, most industries have developed and managed OT and IT as two different domains, maintaining separate technology stacks, protocols, standards, governance models and organisational units. However, over the last few years, OT has started to progressively adopt IT-like technologies. Internet Protocol (IP), for example, is gaining acceptance as an all-purpose networking protocol and Windows™ is more and more frequent in a wide range of devices. The convergence of IT and OT will bring clear advantages to companies including cost and risk reductions as well as enhanced performance and gains in flexibility [4].

Operational Technology in the railways has had limited exposure to the growing range of threats (e.g. viruses and other forms of malware) present in the wider IT environment, however this is no longer the case making them vulnerable to cyber-attacks.

The risk from cyber-attack is a product of: vulnerability, or susceptibility to harm; threat or intent to cause harm and likelihood. Determining risk requires an assessment for each of these. The likelihood of an individual or organisation to launch a successful cyber-attack depends on motivation, capability (skills, knowledge and information) and access.

Figure 1 above illustrates a simplistic bow-tie analysis which looks at the threats i.e. the causal factors that could have a varying impact. A number of cyber security activities have to be performed to prevent the manifestation of the identified impact. As an example, people from inside or outside an organisation can be a threat source (those who wish to compromise systems) or threat actors (those who actually carry out an attack). Potential threat sources and actors include criminals, foreign intelligence, competitors, hackers, activists, malware developers, employees and contractors [1].

2.1 The Rail Industry

In order for the rail industry to deliver an available and on time rail service, it has to make use of information technologies and automated computer systems. These systems control train movement, deliver power to the network, support the timetabling and operational planning processes and schedule work activities across the maintenance teams. As is with most industries, every part of the rail business relies in some way on computerised systems and information technologies. In addition, UK rail is introducing the European Rail Traffic Management (ERTMS) system, as part of its ‘digital railway’ plan to modernise signalling infrastructure.

Those systems upon which the rail industry relies are under constant and growing threat. Computer security threats have advanced significantly from early viruses such as Anna Kournikova and Melissa, which caused widespread disruption of email systems at the turn of the century, to sophisticated “digital weapons” such as the Stuxnet virus responsible for damaging centrifuges supporting the Iranian nuclear enrichment programme.

“Railway systems are becoming vulnerable to cyber-attack due to the move away from bespoke stand-alone systems to open-platform, standardised equipment built using Commercial off the Shelf (COTS) components, and increasing use of networked control and automation systems that can be accessed remotely via public and private networks” [5].

Network Rail for example is considered to be part of the UK’s Critical National Infrastructure (CNI) and therefore protecting it from the effects of cyber-attack is a key priority. In addition, NR are also a category 2 provider of CNI, as set out in the Civil Contingencies Act 2004 [6].

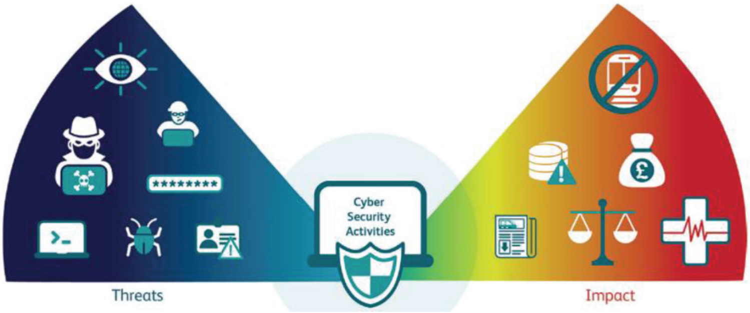

Figure 1: Threats and Impact of cyber security incidents to the railway.

2.2 UK Law

The Health and Safety at Work etc., Act 1974 [7] gives employers a duty to ensure, ‘so far as is reasonably practicable’, the health, safety and welfare of their employees and of any other people affected by their work. This act would cover the threat of cyber and its impact.

3 ROLE OF RISK MANAGEMENT

The purpose of the Risk Management process is to protect the organisation and its ability to perform its mission, not just its IT assets. Therefore, the risk management process should be an essential management function of the organisation.

Risk management is the process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level.

Risk management encompasses three processes: risk assessment (identification and evaluation of risks and risk impacts, and recommendation of risk-reducing measures), risk mitigation (prioritising, implementing and maintaining the appropriate risk-reducing measures recommended from the risk assessment process) and evaluation and assessment (keys for implementing a successful risk management programme).

In the railways, safety and risk analysis tends to focus on operations and maintenance risk and cyber or specifically malicious attacks are not considered as part of the safety case.

Risk Management seeks to present arguments and/or demonstrations to support assertions that the identified risks have been managed in a way which satisfies the organisation’s Risk Appetite and/or the principle of As Low as Reasonably Practicable (ALARP) and Cost Benefit Analysis (CBA). These may include techniques and presentation approaches which include:

1. Independent external testing;
2. Design reviews;
3. Analysis of accumulated log or historical information;
4. Dependency trees; and
5. Goal Structuring Notation.

Management of business risk is a continuous exercise and is part of the risk management approach. Once a risk assessment has been conducted, the risk appetite defined and relevant security measures implemented for an organisation it is important to maintain ongoing management of the business risk as this can change over time due to further identification of vulnerabilities and changes to the threat. Each identified risk can be managed in one of the following ways:

1. Accept – If cost/benefit analysis determines the cost to mitigate the risk is higher than the cost to bear the risk, then the best response is to accept and continually monitor the risk.
2. Avoid – Activities with a high likelihood of loss and impact. The best response is to avoid the activity.
3. Transfer – Activities with a low likelihood of occurring, but with a large impact. The best response is to transfer a portion or all of the risk to a third party by purchasing insurance, hedging, outsourcing, or entering into partnerships.
4. Mitigate – Activities with a high likelihood of occurring, but the impact is small. The best response is to use management control systems to reduce the risk of potential loss [8].

The strategy an organisation wishes to employ is all dependent on their Risk Appetite. As detailed in Reference [9], there are three categories of risk:

- Directly perceptible risk – e.g. climbing a tree, riding a bike, driving a car. This category of risk is dealt with instinctively and intuitively. You don't conduct a formal probabilistic risk assessment before you cross the road.
- Risk perceived through science - e.g. cholera, you need a microscope to see it and a scientific training to understand what you are looking at. Where historic accident data can plausibly projected into the future, actuarial science can inform risk management.
- Virtual risk - the scientists just don't know, or reputable scientists disagree. This is the realm of risk culturally constructed. If science cannot settle an issue it is wonderfully liberating - people, including scientists, are freed to argue from their established beliefs, prejudices and superstitions.

It can be reasonably concluded from the above that safety, reliability and security are risks which are perceived through science and therefore appropriate methodologies have to be employed in order to truly understand the causal factors of risks and their consequences. This then allows for an informed decision to be made and the money that should be spent in line with the ALARP principle.

It is important to note that as the safety and security disciplines have developed independently of each other, the same words (e.g. risk, hazard, threat, likelihood, probability etc.,) have subtle different meanings.

This section of the report will aim to review some of these differences specifically between safety and security as EN 50126 [10] considers Reliability, Availability and Maintainability (RAM) as part of the safety discipline.

3.1 Safety Engineering

Risk is a function of threats, impacts and vulnerabilities. Informed decisions on the appropriate levels of security protection can only be made with a good knowledge of the business risk. A low risk system is likely to require less protection than a high risk system. However, these controls need to be correctly deployed in order to achieve the full security benefit.

Safety in the UK has used the concepts of ALARP and SFAIRP. ALARP also relates to the Common Safety Method – Risk Evaluation and Assessment (CSM REA) [11], which is now required of mainline railways and BS EN 50126 [10]. Any cyber security assessments would now have to ensure that they are completed in a manner compatible with CSM REA.

The figure below illustrates the ALARP principle:

According to the figure above, two extreme regions exist:

- An unacceptable (or intolerable) region where risk can never be accepted; and
- A broadly acceptable region where risk can always be accepted.

To decide whether or not to accept a risk:

- If the risk is in the unacceptable (or intolerable) region – do not accept it.
- If the risk is in the broadly acceptable region – it will not need to be reduced further, unless it can be done so at reasonable cost, however the risk must be monitored to ensure that it remains in that region.

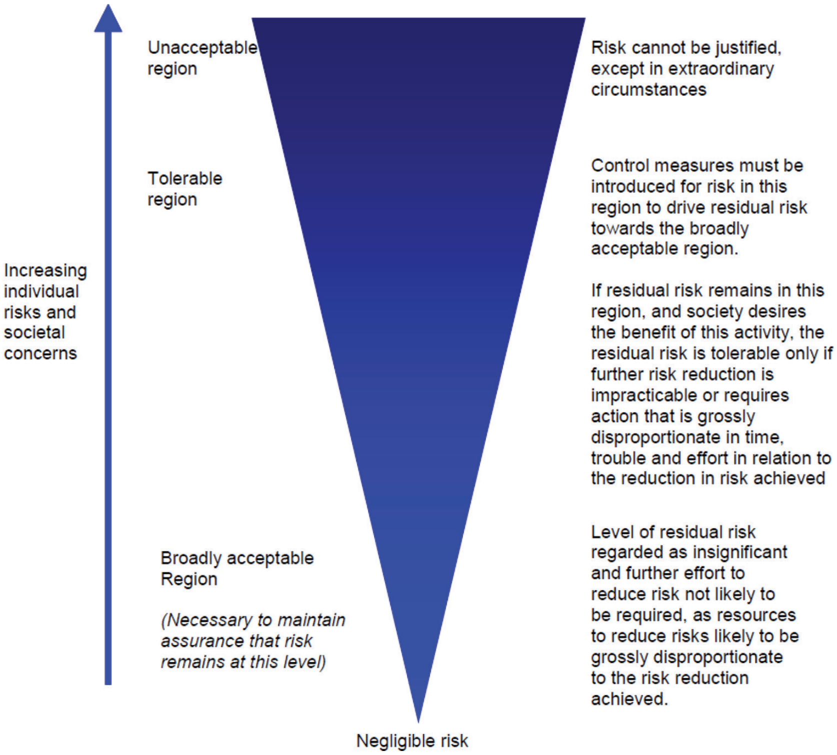
Unacceptable region
Tolerable region
Increasing individual risks and societal concerns
Broadly acceptable Region
(Necessary to maintain assurance that risk remains at this level)
Negligible risk
Risk cannot be justified, except in extraordinary circumstances
Control measures must be introduced for risk in this region to drive residual risk towards the broadly acceptable region.
If residual risk remains in this region, and society desires the benefit of this activity, the residual risk is tolerable only if further risk reduction is impracticable or requires action that is grossly disproportionate in time, trouble and effort in relation to the reduction in risk achieved
Level of residual risk regarded as insignificant and further effort to reduce risk not likely to be required, as resources to reduce risks likely to be grossly disproportionate to the risk reduction achieved.

Figure 2: ALARP Figure.

- If the risk lies between these two regions, it can only be accepted after all ‘reasonably practicable’ steps have been taken to reduce the risk.

3.2 Security Engineering

Cybersecurity focuses on the protection of digital assets (including hardware and information stored, processed or transferred using internet-worked systems). The US National Institute of Standards and Technology (NIST) has identified five key functions necessary for the protection of digital assets [12].

- Identify: Develop an organisational understanding to manage cybersecurity risk to systems, assets, data and capabilities.
- Protect: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure projects. These include Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, and Protective Technology.
- Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. This includes response planning, analysis, mitigation and improvements.

- Recover: Develop and implement the appropriate activities to restore the system capabilities and/or services that were impaired due to a cyber-security event. It includes recovery planning, improvements and communications.

The priorities for the Respond and Recover functions depend on the organisation risk management processes. Darktrace CTO Dave Palmer [3] says “there is no such thing as perfect security – attacks are inevitable so companies should be ready to detect them and respond”.

The ISO/IEC 27000 [13] is a family of standards defined to help organisations keep information assets secure. Among this family, the ISO27001 [14] is the most known standard which provides the requirements for an Information Security Management System (ISMS). ISMS is a systematic approach to managing sensitive information in order to remain secure. ISO 27002 [15] provides guidelines in selecting and implementing controls with the process of implementing the ISMS based on ISO/IEC 27001.

The Centre for the Protection of National Infrastructure (CPNI) and Communications Electronics Security Group (CESG) provide guidance on how organisations can protect against cyber-attacks in 10 steps including Information Risk Management regimes, Secure Configurations, Network Security, Managing User Privileges, Incident Management and Monitoring strategies. In addition, Reference [12] also recommends the use of a risk matrix in the same way that it is done for Safety engineering. Here a 5 by 5 matrix uses terms including Very Low, Low, Medium, High and Very High.

3.3 Reliability Engineering

According to BS EN50126 [8], Quality of Service (QoS) of the railway has to be considered which goes beyond focusing on only individual systems or subsystems. Sometimes, these systems and sub-systems may behave in compliance with their safety cases, however the consequence may be a degraded level of railway performance, in which case, any potential attack would be considered to have been successful.

It should be noted that a succession of ‘fail safe’ scenarios have the potential of producing a higher level system hazard, e.g. cyber-attack affecting the power to the trains which could lead the trains in a ‘safe state’, however they may be stranded in the tunnel, with inadequate ventilation and passengers could start evacuating trains. This would mean that cyber security and its implications have to be considered across the range of railway operating conditions including emergencies.

Generally it is understood that security risk management and specifically the security engineering approaches currently used do not work in compliance with ALARP and SFAIRP, although there is no reason why they cannot be.

3.4 Railway Safety Case

Engineering Safety Management (ESM) is the process of making sure that the risk associated with work on the railway is controlled to an acceptable level. ESM is not just for engineers and can be used for work that involves more than just engineering e.g. cyber security.

In 2005, RSSB launched a new publication on behalf of the industry - How safe is safe enough [16], which tackles some of the long-standing challenges that railway companies face in making consistently safe decisions every day. It brings together a single overview of good practice in making decisions which affect safety.

The objective of 'How safe is safe enough?' is to ensure that the railway industry takes decisions with the proper balance of safety, performance and cost and that are consistent, legal, ethical and workable. It gives the rail industry and other stakeholders a common societal view of what is acceptable, helping companies to meet their legal duties without spending disproportionately on safety.

Any organisation which manages infrastructure or operates trains or stations in the UK must currently write a railway safety case and have it accepted before starting operations. The operator must then follow their safety case.

It is important to note that the legislation makes it clear that infrastructure managers and operators are always entirely responsible for their own actions and must be able to show to the safety authority in their railway safety cases that the safety risk has been controlled.

A typical engineering safety case would demonstrate that all identified risks have been controlled to an acceptable level. It should also show that a systematic approach has been taken in managing safety thus demonstrating that the assessment of risk carried out is valid. In addition, the safety case should consider the effect that the change or product will have on the rest of the railway, including the effect of any changes to operating and maintenance procedures. It is understood that security considerations can have a significant impact on a safety case and where previously this was assessed outside of the common safety framework, this is now being brought back in and considered holistically.

In Reducing Risks, Protecting People [17], the Health and Safety Executive (HSE) suggested that you could use a figure of £1 million (at 2001 prices) as a 'benchmark' – an indication of what it is reasonably practicable to spend to reduce risk by one fatality. 'How Safe is Safe Enough', published by the Rail Safety Standard Board (RSSB), contains full and up-to-date guidance on this and quotes a Value per Fatality (VPF) for 2016 of £1,826,000 [18].

The safety case should be a living document which is subject to review and change as time proceeds. For example, the safety case may change due to important changes to the facility, its mode of operation, or the understanding of safety related issues. It may also change in the light of operating experience or periodic review [19]. If the system remains in its original configuration, the safety case is considered to be valid.

3.5 Cyber Case

For the Cyber security elements, a cyber-security case would need to be developed with documentary evidence to demonstrate to an auditor that the information security management regime is compliant with ISO27001 [14].

In contrast to the Safety case, where it may not require change provided the system remains in its original configuration, a systems security characteristics might change even if the system itself does not. If a new attacker group appears e.g. new types of activists, the threat will change. A vulnerability may be discovered some time later after the system has been installed after having been assessed for safety and security. In both cases, the original system remains unchanged, but the security case and potentially the safety case will no longer be valid because the risks have changed.

An example of the above is that critical train data is transferred trackside using current Wi-Fi technologies, which uses encryption technology. Encryption levels today may be suitable and sufficient, however in the future these could be redundant and thus encryption approaches will need to be reassessed to ensure that the particular encryption solution chosen remains effective.

4 COMBINING SAFETY, RELIABILITY AND SECURITY

There is a perception that safety and security as essentially synonymous, and therefore that the principles of safety engineering are directly applicable to that of security, and vice versa. This is far from reality and the replacement of terminology of ‘safety’ to ‘security; and ‘hazard’ to ‘threat’ will not suffice.

Identifying hazards is the foundation of safety management. Accidents should not only be considered during normal operation, but during degraded and emergency modes as well as at other times such as installation, testing, commissioning, maintenance, decommissioning and disposal.

When identifying hazards for a particular system, there will be a number of causal factors which would lead to the manifestation of those hazards, such as maintenance errors, human errors, and technical failures. Cyber, which previously was not a causal factor that was considered as part of the Safety/Reliability cases and if it was, it was done so outside of the operational context of the railway. Cyber-threats should now be treated like any other discipline in the identification, management and acceptance of system hazards and would be no different in terms of its quantifiable nature (human capability and motivation) as events like extreme weather.

A thorough risk assessment has to be performed which would need to catalogue and assess all IP-enabled assets and associated operating procedures. This part of the process is key in obtaining a better understanding of the risk exposure, thus will allow the further stages to be implemented, namely targeting all subsequent actions in the most appropriate ways.

This part of the process helps to manage rather than avoid all risk, so that organisations can continue to benefit from opportunities in cyberspace.

There has to be an understanding of the threats through identification and evaluation. Possible threats may include: denial of service, targeted attacks, accidental incidents, unauthorised control, malicious code installed on machines, malware infections, phishing or social engineering.

All potential controls that are identified to mitigate against the possible threats have to be proportionate, and not waste resources and going for the belt and braces approach where none are required. Those risks that are evident today may not be present in a few years’ time and in the same manner, there is little benefit in committing resources to mitigate risks that are a few years from maturing – the ALARP principle as discussed above is useful for this level of assessment.

5 ANALYTICAL TOOLS

Key analytical tools such as probabilistic modelling using Monte Carlo simulation, real options, game theory and others have been around for decades.

Uncertainty can be dealt with by using probabilistic modelling. This proves more difficult when dealing with cyber-threats due to the limited amount of published data available (save those that are big enough to make it into the evening news). There is also a perceived complexity of modelling techniques and the garbage in and garbage out syndrome.

As an example, the Channel tunnel fire that closed the tunnel for six months shortly after it opened shouldn’t have happened, according to the event tree analysis produced for the project’s safety assessment, about once every 100 thousand years. The problem with event trees is that they are simplistic. They require feeding with probabilities that are often wild guesses. The real world is infinitely more complicated.

For safety-related systems, there are many probabilistic approaches to computing a residual or tolerable risk, which is underpinned by the concept that there exists a certain probability that these systems will have a dangerous failure over a certain mission time. Dangerous failure can be systematic or random. When it comes to risk analysis, as is mentioned earlier in this study, many concepts from safety and IT security seem very similar. It is very difficult to apply probabilities to IT security and would need to be treated in the same way as systematic failures in the safety domain. This would mean introducing levels of IT security similar to the Safety Integrity Level (SIL) concept.

Any cyber-security measures and procedures considered appropriate to mitigate against terrorists, hackers, hacktivists and cyber criminals must deliver value for money. A robust CBA based on the ALARP principle, where likely benefits are considered to outweigh costs, while maintaining efficient and effective service. Risk Management should be based on the ALARP principle and benefits should focus on improved resilience.

6 CONCLUSIONS

The following conclusions can been drawn from this study:

1. A balance has to be struck between safety and security requirements. It is noted that safety and security are overlapping disciplines, however the end goal is the same, namely to deliver and demonstrate a safe system, which would be in accordance with standards, risk management criteria and railway safety guidelines.
2. Informed judgements have to be made to understand ‘how much’ security is enough, which will be dependent upon the likelihood of a particular security risk being realised and the impact of that realisation. It would also be affected by value for money considerations and the CBA and ALARP principle used in the railways and as detailed in Reference [12] would be appropriate.
3. An organisation would need to be set up to able to adequately, identify, protect, detect, respond and recover from a cyber-security event.
4. NIST 800-30 [12] provides the best guidance in carrying out a cyber-security risk assessment and that all risks have been classified.
5. The principle of ALARP and its triangle that is used in the safety sphere) would need to be followed when assessing cyber-security risks e.g. risks that have been assessed as High or Very High (or equivalent) have been suitably and sufficiently mitigated so as to reduce the risk down to Moderate (or equivalent) or lower.
6. Ensuring that all cyber-security risks identified have been reviewed and classified according to whether they can be related to Safety, RAM or other.
7. Any cyber-security risks identified as safety or RAM related would need to be reviewed by the leads of the appropriate disciplines.
8. Probability cannot be applied to IT security and consideration of the introduction of levels to IT similar to the SIL concept.

ACKNOWLEDGEMENTS

The author would like to thank Ove Arup and Partners Ltd in their assistance in supplying some of the material and images for this paper.

REFERENCES

[1] RSSB – Cyber Security Strategy for Protecting Britain’s Railway – Draft version 0.7, 23 September 2016.

[2] BAE Systems Detica, The Cost of Cyber Crime, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf, February 2012 (accessed 28 February 2017).

[3] Four Cyber Attacks on UK Railways in A Year, available at http://news.sky.com/story/four-cyber-attacks-on-uk-railways-in-a-year-10498558 (accessed 04 May 2017).

[4] Ascent Thought Leadership from Atos White Paper. The Convergence of IT and Operational Technology, available at https://atos.net/content/dam/global/ascent-whitepapers/ascent-whitepaper-the-convergence-of-it-and-operational-technology.pdf (accessed 15 March 2017).

[5] Department for Transport, Rail Cyber Security, Guidance to Industry, February 2016.

[6] Preparation and Planning for Emergencies: Responsibilities of Responder Agencies and others, available at https://www.gov.uk/guidance/preparation-and-planning-for-emergencies-responsibilities-of-responder-agencies-and-others (accessed 15 January 2017).

[7] Health and Safety at Work etc Act 1974, available at http://www.hse.gov.uk/legislation/hswa.htm (accessed 15 March 2017).

[8] A Four Step Risk Approach to Strategy Execution, available at https://erm.ncsu.edu/library/article/risk-strategy-execution (accessed 29 May 2017).

[9] Adams, John, Adam Smith Institute, London, 1999. The Management of Risk and Uncertainty – Risky Business.

[10] Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS). Basic requirements and generic process, BS EN50126-1: 1999.

[11] Common Safety Method for Risk Evaluation and Assessment, Guidance on the Application of Commission Regulation (EU) 402/2013, March 2015, Office of Rail Regulation (ORR).

[12] Improving Critical Infrastructure Cybersecurity Executive Order 13636. Preliminary Cybersecurity Framework, available at http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf (accessed 26 March 2017).

[13] ISO/IEC 27000 Family – Information Security Management Systems, available at http://www.iso.org/iso/home/standards/management-standards/iso27001.htm (accessed 18 January 2017).

[14] ISO/IEC 27002: 2013, Information Technology – Security Techniques – Code of Practice for Information Security Controls, available at http://www.iso.org/iso/catalogue_detail?csnumber=54533 (accessed 15 April 2017).

[15] ISO/IEC 27002: 2013 Information Technology – Security Techniques – Code of Practice for Information Security Controls.

[16] How Safe is Safe Enough? available at http://www.hse.gov.uk/news/judith-risk-assessment/safeenough300712.htm (accessed 15 May 2017).

[17] Health and Safety Executive, Reducing Risks, Protecting People, HSE's decision making process.

[18] Taking Safe Decisions – Safety Related CBA, available at https://www.rssb.co.uk/risk-analysis-and-safety-reporting/risk-analysis/taking-safe-decisions/taking-safe-decisions-safety-related-cba (accessed 01 January 2017).

[19] Office for Nuclear Regulation. The Purpose, Scope and Content of Safety Cases, available at http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf (accessed 04 January 2017).