RAIL RISK BEST PRACTICE - CROSS SECTORAL LESSONS TO BE LEARNED?

Paul Bews [(1)] Mercedes Gonzalez-Palacio [(2)] Mark Davis [(3)] Andrew Herd [(4)]

[(1)] Booz Allen Hamilton, Apollolaan 151, 1077 AR Amsterdam, Nederlands
[(2)] Booz Allen Hamilton, Savoy Court, The Strand, London, UK
[(3)] Booz Allen Hamilton, Mclean, VA, USA
[(4)] Booz Allen Hamilton, Keplerlaan 1, 2201 AZ Noordwijk, Nederlands

ABSTRACT

What does one of the oldest forms of public transport have to offer one of the newest? This paper examines this question by comparing the various best practice approaches to risk assessment within the rail industry to that of the spaceflight industry. By examining risk assessment and risk management approaches to public-accountable operations, specific techniques and processes that present sectoral best-practice can be presented.

Specifically, the paper explores common tools and methods used to conduct and implement risk assessment, comparing these with the approaches adopted within specific space agencies involved in human spaceflight. Additionally, this paper highlights any substantial differences, such as the use of primarily quantitative methods by the railway sector and the use of qualitative methods by the spaceflight sector, and proposes which unique risk assessment method would provide a best fit for adoption by these agencies.

Finally, an overview of the existing safety assessment and management approaches for human spaceflight are provided, with the end result being an explanation of the different ways to approach vehicle and payload risk management/assessment.

1. INTRODUCTION

Over the past century public support of and demand for accessible forms of transport have influenced the development and operations of these transport services.

Due to catastrophic incidents, primarily over the past 20 years, the public transport industry (amongst others – in the oil industry for example) has been driven down a path of becoming a leader in the development and utilisation of risk assessment and risk management techniques. This is in no small part due to their public accountability for their service provision and due to the direct public impact when such a catastrophic incident occurs. However this accountability has not been direct public pressure to specifically adopt risk management techniques, purely to increase reliability and safety of the transport service itself. This is demonstrated through the public acceptability of different levels of risk for various forms of transport. For example the public put themselves at a higher risk by driving a car than when the public purchase a ticket for a service such as the train or indeed a plane journey.

Spaceflight in recent years has also experienced a number of catastrophic events. In response to these events there has been both a high level public awareness and agency response. Public "involvement" in the aftermath of the Columbia accident, was direct, as shuttle debris fell over a wide area. More than 2,000 debris fields were found in sparsely populated areas southeast of Dallas from Nacogdoches in East Texas, where a high amount of debris fell, to western Louisiana and the south-western counties of Arkansas [1]. Data was collected from these sites for the investigation, data that would ultimately be used to ascertain the flight-worthiness of subsequent launches of the National Aeronautics and Space Administration (NASA) space shuttle.

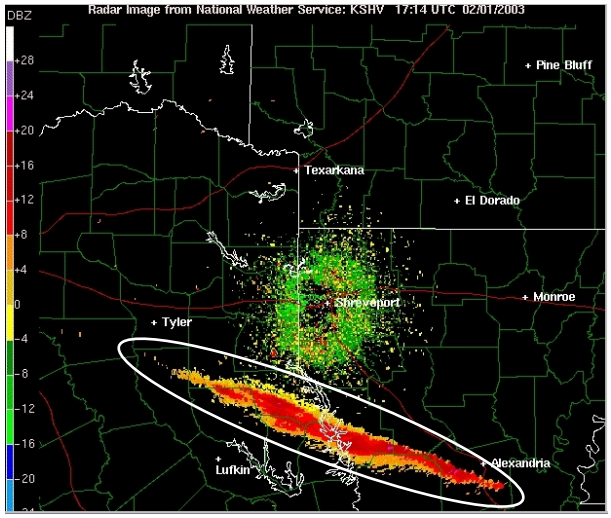

Figure 1 Columbia debris (circled) detected by National Weather Service radar over Texas and Louisiana.

However public involvement in spaceflight has become all the more direct with fee-paying "tourists" visiting the International Space Station. For a slightly lesser amount members of the public can experience spaceflight on commercial vehicles. Spaceflight thus has been firmly (and rapidly) seated in the public domain, demonstrated by the existence of space tourism commercial enterprises such as Space Adventures (Soyuz-based) and Virgin Galactic.

In this regard spaceflight is moving towards sectors that exist firmly in (are reliant upon, utilised by and are accountable to) the public domain. This public dimension, in turn will affect the spaceflight sector in terms of the use of hazard control and risk assessment best practice approaches to control hazards. It would therefore appear credible that sectors operating in the public domain could offer specific and relevant insights into best practice examples. After all, the common objective is safe and reliable transportation, and domains other than spaceflight have an extensive record and experience on success and failures. The primary purpose of this paper therefore is to give some specific examples and highlight the benefits of looking at best practice used in a related transport service industry, i.e. the rail industry, which could be used within the spaceflight sector.

The basic principle behind the ideas put forward in this paper is that any safety considerations for a transportation system should be made looking at the history and previous experience of other industries. Moreover, that they should be made in the context of the safety levels that exist within the current environment or safety levels that are socially or politically tolerable within this environment.

As spaceflight becomes more of a public proposition, the space industry have a responsibility to ensure an adequate balance is achieved between affordability (or best-use of tax funds) and safety. The spaceflight industry is faced with providing an approach that will allow for the setting and demonstration of safety requirements and targets at publicly tolerable levels. This will involve the deploying of safety risk management strategies for the space transportation industry as a whole. This would also need to include the space tourism spaceflight sub sector.

This may not necessarily mean a major departure to the approach already established within the spaceflight sector, or indeed any kind of dilution in overall safety standards. It may however mean that a more focussed adoption of a risk-based approach to the setting of values used within these safety standards. This in turn requires for the adoption of risk assessment and risk management approaches that provide by analysis and demonstration that these values, and hence these standards, have been achieved.

Commercial industries, traditionally accountable to financial shareholders have needed to be in a position to demonstrate a robust approach to risk has been taken in order to sustain financial investment. Those industries with a high level of public accountability (or relying on the buying public) also have had to adopt robust and efficient risk management approaches in order to secure (and maintain) both financial and public backing.

However risk assessment in itself has not proved sufficient to ensure success within key public transport service industries. Risk assessment and risk management however has provided the highest benefits and provided instances of sectoral best practice. The underlying theme therefore is that risk assessment is not an end in itself; the management of risk is. This paper details some lessons learned and some best practice techniques from the rail sector that illustrate how this subtle objective has come more to the forefront of the way safety and risk is being effectively addressed.

1.1 Risk Assessment General Approach

Whilst this paper does not intend to set out or even seek to define risk assessment approaches, it is beneficial to examine risk assessment approaches utilised by commercial industry and public organisations involved in the provision of transport services (including infrastructures) used by the general public.

Risk simply put is the combination of the impact, or severity, of a particular event and the probability, or likelihood, of this event occurring. The risk quantity is therefore the product of these two entities. Event impact being given a number (on a set or declared scale) and probability given as a percentage or classification based on the likelihood of an event occurring.

The challenge of this approach is to correctly assess the system wide impact of the event occurring, and, then effectively quantifying the likelihood of occurrence. Once assessed, risk assessment is then a powerful tool to cross-compare mishap risks within the same reference frame.

The risk associated with, for example, a proposed change to or first-time use of equipment (i.e. having unknown performance / risk criteria) can vary from negligible to totally unacceptable (catastrophic). The risk can be reduced, usually at a cost, through a risk reduction order of precedence shown in figure 2 below.

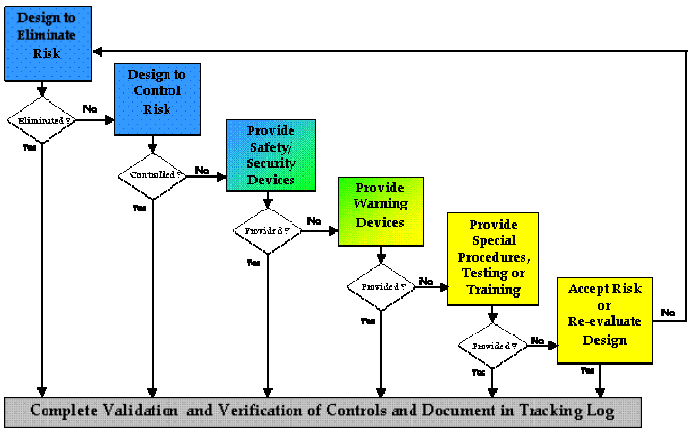

Figure 2: Risk Reduction Order of Precedence [2]

Risk Assessment in this example would involve a systematic analysis of the potential losses associated with a change or the introduction of new equipment, and of the measures for reducing the likelihood or severity of loss. This methodology enables losses to be aggregated and compared against the cost of measures.

The Risk Assessment steps themselves are a common cross-industry standard and can be defined as follows:
1. Hazard identification
2. Cause analysis
3. Consequence analysis
4. Loss analysis
5. . Risk Reduction, Controls and Options Analysis
6. Impact analysis*
7. Demonstration of Compliance / Verification**
8. Residual risk acceptance
These steps will be used to compare the steps on the different sectors.

Note*: In the U.S. this step is usually done in the Consequence or Loss Analysis phase. As a result Impact Analysis is reclassified as "Validation" to assess the hazard controls and determine if they do in fact reduce the Hazard risk to acceptable levels.
Note**: In the US model of verification, the activity involves physically verifying that the hazard controls are integrated into the system and operate as intended without introducing new hazards to the system. This approach differs slightly from the general definition taken in this paper.

2 RAILWAY SECTOR AND RISK ASSESSMENT APPROACH

Put simply, rail transport is the transportation of passengers and goods by means of wheeled vehicles especially designed to run along rails on a fixed guideway. It has been this way for more than two hundred years!

Rail travel continues to be an important means of transport for people and goods across the world. The design of rail travel is a triumph of convenience, so passengers hop on and off intercity trains, tubes and suburban trains without the check-in desk or long queues familiar to air travellers. And the stations are built to ease the passage of millions of people each day.

It is widely acknowledged that the technologies employed in the rail sector are not always cutting edge (although this is changing). Trains can travel at an ever increasing high speed and are heavy. They need to maintain a safe distance from other trains in order to stop if required with out collision. Also, railway operations are complex, ridership is high and the consequences of an accident are often catastrophic. Therefore, railway operators have a significant social responsibility to ensure that rail travel is safe. This section of the paper presents railway sector best practice in the setting and demonstration of safety targets and the hazard and risk management that goes with that.

But first a bit of history…….:

It is now more than a decade since the United Kingdom privatised its state-owned railway. Many other countries, particularly in Europe have since followed suit.

Being an old and capital intensive industry, the railway industry as we know it today has inherited a considerable amount of legacy from previous investments made in existing infrastructure and rolling stock. This has often hindered the achievement of the necessary step change in safety improvement.

There have been significant advances in safety, though, mainly following significant rail disasters and major accidents around the world. This motivation for change has led to significant improvements in guidance and requirements promoting advances in the techniques employed for safety assurance.

However, the infrastructure which has always followed the original design principles has in some areas stifled a step change in technological contributions to safety improvement. This is particularly true in respect of the restrictions that this places on train design as a result of the existing design of the infrastructure and trains.

Take for example the fact that the guidance system for mainline railways across the world consists of two parallel steel rails that guide steel wheels. This has some advantages; the small rolling resistance and huge load bearing capacity of this unlubricated metal to metal interface allow trains to move with much less friction than say road vehicles and means that the engine pulling the train uses energy far more efficiently. However, this kind of mechanical interface with a small contact area brings with it safety issues related to braking limitations and traction uncertainties as well as the fact that prevention of one of the top event risks; derailment, remains very difficult to remove as a potential hazard.

Despite the fact that the industry is somewhat restricted by these historical features of the infrastructure and that these are unlikely to change for some time, if at all, there has recently been a huge investment in new trains and the crashworthiness of trains is ever improving. Also, there are significant safety interoperability and capacity improvements promised from advanced signalling systems such as the European Rail Traffic Management system (ERTMS).

Signalling is of course a safety system that keeps trains apart and is by far and away the most important safety

system on the railway hence the use of new technologies and the huge amount of investment across the world in this area.

The liberalization of the European Railway industry has meant that there is an organisational divide at the safety critical wheel-rail interface. This means that the infrastructure is managed by one entity and the trains operated by a completely separate entity. To make the interfaces even more complicated, recently there has been a move towards financing the build of new infrastructure though creative financing initiatives such as Public Private Partnerships (PPPs) and Design, Build, Finance and Maintain (DBFM) initiatives which introduces a third entity: the infrastructure Provider, who is responsible for maintenance and other operational support activities. All of this introduces more operational interfaces and the concerning fact that safety and commercial issues are often traded and balanced which in turn, can and does, increase safety risk.

However, despite all of this, safety is improving dramatically along with an increase in ridership. Catastrophic accidents in rail and their associated inquiry reports have lead to a demanding regulatory environment in Europe. This coupled with a rigorous approach to safety and a highly competitive manufacturing sector has combined to make significant overall safety improvements. With ever more challenging technical and legislative demands, both for increased performance, and increased safety, the industry has risen to the challenge and the European railway system is now one of the safest transport systems in the world.

Regulation and safety techniques employed to demonstrate compliance with these regulations are similar across the European rail industry and this paper describes some of these industry best practices in detail including, often, their accident origins. Finally, this paper will make recommendations on those safety practices and techniques that could be used across the spaceflight sector.

2.1 Accident Drivers.

Similar to spaceflight, railways are a complex integration of many subsystems. These include track, electrification, civil structures, signalling and stations. Trains include traction motor systems, braking systems, cab ergonomics, crashworthiness, doors and emergency equipment. Operational requirements are also key features of safe railway operation including safe traffic control systems, maintenance and emergency procedures. Engineered elements do of course fail, and as such, require a large element of risk mitigation provided by human intervention. Therefore, accidents have occurred and will continue to occur.

Although hazards are different in nature and technical and operational complexity to those in the spaceflight industry, a single railway accident can lead to a comparably large number of human casualties. Therefore, lessons learned and best practices to risk assessment and management are discovered and tested following each accident. In this section, the resultant best practices in the rail industry are examined and the lessons that can be learned for the spaceflight sector discussed.

There are a number of factors that have both impacted and shaped safety and rail sector risk management in Europe and across the world that maybe analogous to the spaceflight industry today. These factors include:

- Privatization / Liberalization.
- Commercial fragmentation.
- Organisational and cultural differences across the industry.
- Differing approaches to management systems and performance.
- Funding mechanisms that impact on tradeoffs between safety and commercial gain.

The railway sector has changed in many parts of Europe For one, the railways have changed from being state owned and vertically integrated to many private players and influences. They have also changed from being populated by experienced career railwaymen to an industry with a mobile workforce with many contractors.

The speed of embracing new technologies has also changed. Previously technology was simple, stable, extensively tested and well understood by all. Whereas now the desire for interoperability across Europe, with vehicles offering improved operational capabilities, being faster and having increased safe capacity means that an unprecedented amount of new technology is being introduced.

There has been a transition from a compliance-based prescriptive approach to safety risks to a risk-based approach where risks are balanced in line with principles such as As Low As Reasonable Practicable (ALARP) and Globalement Au Moins Aussi Bon (GAMAB) and suites of documentation demonstrate and manage safety such as Railway Safety Cases.
(Note: with the introduction of European interoperability requirements and the need to standardize technical specifications, in some areas there has been a reversion back to the prescriptive approach and certification by 3rd parties).

To a large extent in the past society had low expectations of safety provided by rail. However, now society is a lot less tolerant and has high safety

expectations. The threat of litigation is also ever present.

Challenges raised by these changes in the railway industry in the last decade have set new precedents and have essentially required that the industry:

- Underpin decisions with robust risk data.
- Recognise stakeholder values and anticipate them.
- Conduct risk management up and down the supply chain.
- Focus attention across the new interfaces to mitigate the new risks.

Figure 1. Rail Best Practice Proposal 1

The underlying aims and benefits of privatisation and liberalization is, after all, to make railways safe reliable and affordable.

Since a large majority of risk mitigations in the rail industry are provided by human intervention, there is now recognition that human factors are key safety and risk drivers, hence there is a large emphasis paid to:

- Staff selection and recruitment
- Training and competency assessment, including authorisation and re-examination.
- Procedures for operating, maintenance, modifications and emergencies.
- Performance influencing factors including physical and environmental sources of stress.
- Task and human error analysis for safety critical tasks.
- Human / Systems Integration
- Adequacy of supervision.
- Motivation, reward and morale.
- Safety culture and safety climate factors, including a move away from a "blame culture".

Figure 2. Rail Best Practice Proposal 2

Risk assessments in European rail use QRA methods and risk tolerability criteria by applying the principle of reducing risk to As Low As Reasonably Practicable levels (ALARP). Similar approaches have been applied across Europe, for example in France which requires that the totality of risk is no greater than before, which is defined by the principle Globalement Au Moins Aussi Bon (GAMAB).

Figure 3. Rail Best Practice Proposal 3

The industry recognised the importance of having a common risk language and applying a consistent approach to risk assessment. Examples of this can be found in broadly accepted national guidance such as that in the Engineering Safety Management, Railtrack [3] (aka the "yellow book") in the United Kingdom.

Figure 4. Rail Best Practice Proposal 4

The industry's adoption of real risk management using cost benefit techniques resulted in the introduction of technology which is now known as "Automatic Train Protection" (ATP). In this particular example, the French national rail operator SNCF [4] carried out a review of their records which showed that one of the major precursors to accidents; Signals Passed At Danger (SPADS), had remained at a constant level for approximately 20 years, many of them being attributed to human driver error. The fact that the number of incidents had not changed despite a high profile campaign indicated that the number would be difficult to reduce further until SNCF considered supporting the driver by creating an automatic braking system linked to the signals.

The learning point for the industry here was that the industry relied upon human intervention to reduce risk. However, risk management is most effective where there is a move towards design based controls for the reduction of risk.

Figure 5. Rail Best Practice Proposal 5

Since this time, such automatic train protection systems are being, or have been introduced throughout the world and although do not completely eliminate risk, are designed to considerably reduce it. Such systems have made a step change in risk reduction and safety improvement.

In the SNCF assessment it was estimated that the cost to equip eleven thousand signals and five thousand trains with new equipment would save five lives. The decision taken was that this was clearly a good return on investment and would prove to be cost effective.

A further learning point for the industry here was that although not always politically or culturally acceptable across parts of the world, the value of preventing a fatality or serious injury used in risk calculations can provide sufficient motivation to make realistic spend-to-save investment decisions and aligns risk reduction with the commercial nature of the transport industry.

Figure 6. Rail Best Practice Proposal 6

A number of recurrent themes from accident enquiries have made a strong case for adequate Safety Management Systems and appropriate safety culture improvements in the rail industry. For example the Fennel enquiry into the Kings Cross fire disaster [5] of 1987 concluded that London Underground had formed a belief that a small number of safety procedures and safety induction training created an adequate operational safety management system and that safety risk could not be reduced further. This belief was never challenged and was further exacerbated by a very weak safety culture which:

- Assumed that small fires were inevitable and not preventable.
- Focussed on fire emergency procedures rather than fire prevention.
- Failed to learn from earlier fires.
- Had a culture which put passenger safety as a secondary issue.
- Carried out very few safety audits and focussed on financial auditing.

This terrible accident and the subsequent inquiry findings heralded a drastic change from a reactive to a proactive prevention culture including vastly improved training, emergency plans and procedures and safety auditing. There has been no serious fire in London Underground since the one at King's Cross in 1987. Further testimony to the improvements is the way in which the recent 7/7 terrorist bombings were dealt with by London Underground staff and the emergency services alike.

The best practice learning point for the industry was recognition that the party whose actions were likely to be most critical at the time of an emergency are the operating staff closest to the scene. As far as railway operator staff are concerned there is now role clarity such that they know their responsibility clearly and they are also empowered such that they have the authority to act appropriately when necessary. Training and refresher courses ensure that staff maintain their competency levels, allowing them to carry out their responsibilities as required.

Figure 7. Rail Best Practice Proposal 7

Following the disaster at Clapham Junction [6], London UK in 1988, and the Hidden Enquiry, the rail industry developed an approach for the integration of risk criteria into business decision making. This proactive approach included the following elements:

- Visible decision making.
- Self-evident safety benefit in cost terms.
- A risk based prioritisation of schemes.
- The conduct of quantified risk assessments, which took into account public perception.

In respect of public perception referred to in the last bullet, it was recognised that events which were potentially catastrophic could be weighted more because of the public reaction to such events.

This was the beginning of recognition that safety and risk management is just good business sense and that commercially successful companies excel because they bring efficient business practice to bear on risk management as on all other aspects of their business.

Figure 8. Rail Best Practice Proposal 8

The Eurotunnel fire example is interesting since despite the fact there were no fatalities, it was a key risk management learning point for rail and a number of other industries. Eurotunnel had a fire in 1996 just 3 years after opening for business. The enquiry revealed that emergency procedures were too complex and demanding and that staff were inadequately trained.
The Channel Tunnel project had been and still was in financial difficulties since significant delays had occurred during its construction. Because of this cost escalation and the costs associated with designing in safety features from the start, safety versus commercial issues was a continuous area of focus to achieve and appropriate balance. The fire authorities and the Channel Tunnel Safety Authority had stated their concerns [7] particularly in respect of the heavy goods vehicle shuttles and before operations were allowed to commence, Eurotunnel had to make a demonstration through its safety case that the design was indeed safe. The subsequent accident enquiry [8] revealed that the performance of key staff, emergency procedures and safety equipment raised serious questions as to the safety of the system. The accident led to further cost escalation in the retrospective improvements required by the inquiry which totalled 36 specific recommendations.

The key learning point for the industry here is that the balance of decision making should not tip in favour of commercial aspects at the expense of good risk management, since good risk management makes good commercial sense for protection of the assets as well as reputation. Generally, this area should be managed carefully in future since there are close links between cost and safety on many large engineering projects, particularly those that are funded privately and are based on service delivery.

Figure 9. Rail Best Practice Proposal 9

When an industry is being liberalised, the consequences of failing to achieve adequate systems of control will increase risk and may possibly increase the numbers and severity of accidents in the future.

In order to mitigate this in the rail industry, each train service operator and infrastructure manager is required to prepare a "assurance" in the form of a safety case (similar to those in the nuclear or the oil and gas industry). Such safety cases or hazard analysis must be acceptable to the railway authority before operation of, or access to the railway network is allowed.

Figure 10. Rail Best Practice Proposal 10

No transport system can be made completely safe and given the number of people exposed to risk at the same time, the mass transit industry is likely to experience disasters and major accidents in the future. However, because of lessons learned from previous accidents this

likelihood should be diminishing because the approach within the rail industry to risk management has become proactive rather than reactive.

A considerable amount of information sharing already occurs between rail companies. There will continue to be learning opportunities from more extensive analyses of accident data, however, the amount of learning depends very much on the safety culture within a rail company. This is the future challenge for the industry and the most recent guidance makes provision for the monitoring and improvement of the organisational safety culture.

2.2 Industry Drivers

At a national level, Government sets the strategy in the railway field and the target risk levels that are not to be exceeded. The public and media also influence heavily the perception of the risk in the railways. This perception is driven by the accidents occurring and the influence of the media and its often sensationalist reporting which fosters emotional and often disproportionate reactions from the travelling public.(see previous section)

At a European level, the, UK is influenced by the European legislation on safety matters that all the European Members have to comply with.

There are many different international standards relevant to safety assurance and railway safety. These standards originate from Europe, Japan, and the US in the main and are often similar in many areas. However at a detail level there are several differences. The most important differences are:

- Qualitative analysis is used in Japan rather than quantitative analysis and absolute targets are rarely specified. Quantitative analysis and hazard analysis are used to carry out safety evaluation and quantitative analysis is used in a confirmation

Figure 11. Rail Best Practice Proposal 11

- In the US railway industry the Safety Integrity level (SIL) concept is not common
- Terminology differs greatly across standards
- The purpose of the standards varies considerably from guidance to mandatory compliance

Within Europe the European Committee for Electrotechnical Standardization (CENELEC) [9] provide for standards that are becoming the single standard for railway systems. Hence railway systems are complying to the same standards in Europe and to a large extent it is considered that these standards represent the only truly international standards in the field of railway systems engineering. This includes, EN50126 the standard for reliability, availability maintainability and safety (RAMS) specification and demonstration, EN50128; the standard for software for railway communications, signalling and processing systems. And EN501029, the standard for safety related electrical systems for signalling.

The use of the CENELEC standards is now mandated through legislation (through European Union directives and TSI's) requiring the interoperability of railways. As such it is widely expected that they are likely to become the only standards of significance for railway systems in the global market.

EN50126 has the potential to become a single standard for RAMS in railway systems in a global market.

Figure 12. Rail Best Practice Proposal 12

EN 50126 requires

1. Production of a top level generic risk model for the railway system down to its major constituents (e.g. signalling, train, infrastructure etc) with a definition of the constituents of the model and its interactions
2. Development of a checklist of common functional hazards within specific railway types (high speed, metro etc)
3. Apportionment of safety targets to the requirements for the subsystems (doors, brakes etc)
4. Application of the Safety Integrity Level (SIL) concept through all of the lifecycle phases of the system.
5. Application of combined probabilistic and deterministic means for safety demonstration
6. Application of risk acceptance principles
7. Application of qualitative assessment of tolerable risk

2.3 Risk Assessment Approach

From a safety point of view, trains cannot be separated from the infrastructure that they run on nor from the operational context or environment that they operate within.

For this reason this paper makes no attempt to separate the railway system into its subsystems as from a safety point of view it is treated as a whole.

This is in line with aviation industry best practice reflected in the "SHELL" Model [10]. The model takes enables a systems approach to safety; for Software Hardware, Environment, and Live ware.

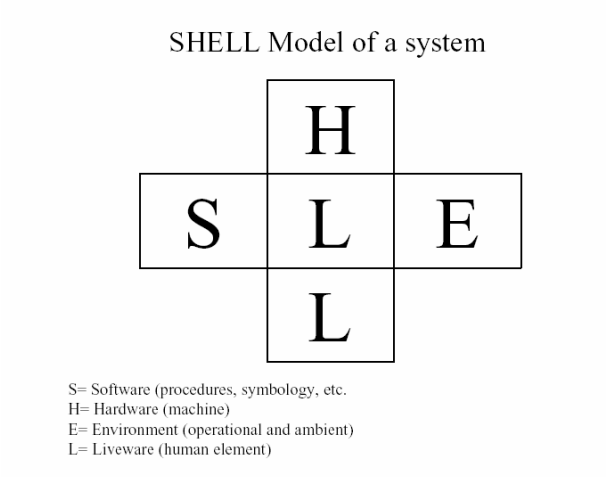

Figure 13. Aviation SHELL Model of a System

The manifestation of the best practice indicated above is primarily captured in the implementation of the risk assessment approach set out below.

In the UK Railway industry, safety is achieved through demonstration of the achievement of a pre-determined set of risk levels assigned by the client or the regulator.

On large scale infrastructure and train projects, target levels of risk are set for individuals and critical groups. Typically, target risk levels are set for the following: (more on how in the standards section)
• Individual risk for railway workers.
• Individual risk for passengers.
• Individual risk for members of the public.

Targets for societal risk are also set, however dependent upon the country where these standards are created could result in significant variance between these standards.

Risk targets are also set for individual accident sequences (such as train-train collision or derailment). These risk targets are based upon apportioning the individual and societal risk targets.

Guidance in the UK Rail Industry "yellow Book" outlines a seven staged process for risk assessment:

1. Hazard Identification
Once systems have been defined, the hazard identification stage is carried out. This step results in the production of the project hazard log and gives an early indication of any problems that are associated with the conceptual design and its hazard potential.

2. Cause Analysis
Involves establishing the primary causal factors which may give rise to a hazard and estimating the likelihood of occurrence of each hazard. This information is recorded within the Hazard Log which is the live tool for managing hazards.

3. Consequence Analysis
The final consequences, which may arise from a hazard are established, together with the estimation of the likelihood of accidents arising from each hazard.
The consequences of each hazard may be associated with a range of losses (such as harm to people, damage to environment or commercial loss).

UK rail hazard identification, cause and consequence analysis is carried out using the following techniques:

- Preliminary Hazards Analysis (PHA)
- Failure Mode Effects Analysis (FMEA)
- Hazard and operability studies (HAZOPs)

4. Loss Analysis
Once the likelihood of the risk is determined, the Loss Analysis requires estimation of the magnitude of the safety losses (that is harm to people, system or environment), before options to reduce risk are considered.

5. Risk Reduction and Controls and Options Analysis
Risk reduction and control involves the identification of risk reduction measures for each hazard, and options analysis considers such measures and assesses their implementation costs.

When the Loss analysis and the Options analysis have been completed, risk ranking may be carried out. Risk ranking of each hazard potential is central to understanding whether risks posed by the design are tolerable, and whether all reasonably practicable measures have been considered by the design teams.

The sequence in which a Risk Ranking analysis and Risk Reduction and Controls activity is undertaken may have an impact on the outcome of this activity as a whole. One body of thought emphasises that Risk Ranking should always be completed before the Risk Reduction and Controls phase. It is argued that there is a need to initially prioritize Hazards by risk. Only then can the allocation of resources be undertaken, on the basis of mitigating highest risk hazards first, then working down the ranking list as resources/funding is available.

6. Impact Analysis
At this stage the benefits associated with implementation of each risk reduction measure are considered,

Typically a Quantified Risk Assessment is carried out at this point to demonstrate the targets have been achieved.

Quantified Risk Assessments in the railway industry assess the risk from major hazards with the potential to cause fatality to customers and other members of the public. Because rail is becoming a liberalized industry, this assessment includes risks imported to operations through the activities of others.

The major objective of the quantified risk assessment is to promote an understanding of the nature of the risks and provide a basis for: identifying whether adequate controls are in place; and if any further controls are "reasonably practicable"

7. Demonstration of Compliance/ Verification

This verification stage involves determining which risk reduction measures should be implemented and justifying the acceptance of any remaining risk.
This is done by selecting those that are required by the ALARP principle or by safety targets imposed by the railway operator.

If formal cost benefit analysis is required to demonstrate the ALARP principle, the QRA allows the assessment of the benefits of the risk reducing measures. Using the QRA, comparisons of costs vs. benefits can be assessed, This of course assumes that society allows for the setting a monetary value on the value of preventing a fatality (VPF).

Within the UK rail industry the safety culture has allowed a value to be placed upon a life saved as in the region of £3 million when considering multi-fatality events and £1 million for events involving a single fatality. Paradoxically, elsewhere in the world, for example in the Netherlands this is culturally unacceptable and in USA (in specific sectors – with US insurance companies being a notable exception), the concept of the value of a life saved is also considered unacceptable and not used. Therefore until there is worldwide consensus on this issue, other methods of demonstrating ALARP need to be considered.

If the ALARP demonstration is satisfactory or the targets imposed by the railway operator are met, the residual risk is automatically accepted.
There are cases where the residual risk does not comply with the targets as some times the targets are set too high and the residual risk is accepted on the basis of derogations.

3 SPACEFLIGHT OPERATIONS AND RISK ASSESSMENT APPROACH

With specific regard to human spaceflight, and considering Space Shuttle (operating from the early 1980's) and the development and use of the International Space Station, the formal adoption of risk assessment was overseen through NASA's risk management programme, however only from 1997. In 2002 a NASA Program Manager was reporting that "accomplishments of the first five years (included) … creating "Continuous Risk Management" (and) … Agency implementation of risk management" [11]. The need to use formal risk management being "reinforced through the Mars 1998 mission failures". The agency motivation for the adoption of risk analysis techniques being in part driven by "sponsors" analysis of failure costs associated with NASA mission failures. These are quoted in 2000 [12] as costing $500M since 1992 (estimates not including loss of life, loss of opportunity, mission delay or the impact on public confidence).

For the European Space Agency (ESA) 1998 saw the top-down release of risk assessment support tools consistent with the European Co-operation for Space Standards (ECSS) – released in 1996 – described [13] as a proactive process aiming to optimise risk against cost, schedule and technical performance (that includes safety and dependability). However whilst the compliance to these standards was assured through the inclusion within project (hardware development) contract requirements, for Shuttle and ISS integrated hardware the respective Shuttle and / or ISS requirements took precedence.

3.1 Qualitative Approaches to Safety

Specific to payloads utilising the human habitable environment provided by the STS or ISS, a qualitative (non-probabilistic) assessment approach is utilised [14].

Simply put an event will either occur or not (given the label of "credible hazard event" or hazard cause). As such this negates the need for an assessment of the likelihood of an event occurring (its probability) and removing one of the challenges of the risk assessment process.

However this approach has its own overheads, in terms of development cost, such that failure tolerance may result in an over design (or indeed under design) if applied inappropriately by the safety review panel.

3.2 Safety Assessment Approach

The STS / ISS payload follows seven general risks assessment steps previously set out as a generic industry standard. Whilst a number of formats seems to be followed, for payloads a consistent format for Hazard Reports is adopted, however unique formats were adopted for Columbus, ESA's ISS element, and Automated Transfer Vehicle. Indeed over the course of the element / vehicle development contracts with formatting appears to change.

However despite this "editorial" inconsistency, the data provided fundamentally remains the same, and is outlined in the following sections. It is an agency led (ISS mandated) safety review process that ensures that

the data captured in the below categories is completed in an accurate and robust manner.

1. Hazard identification
It is captured as the "Hazard Title and Hazard Category" [15].
For Payloads standardised hazard identification and control is recorded in a set form. Outside of this unique hazards can be identified (for payloads, systems and vehicles).
The hazard Category defines the most significant hazards as Critical or Catastrophic.
The Critical Hazards are the ones that shall be controlled such that no single failure or operator error can result in damage to STS equipment, a non-disabling personnel injury, or the use of unscheduled safing procedures that affect operations of the Orbiter or another payload.
The Catastrophic hazards are the ones that shall be controlled such that no combination of two failures or operator errors can result in the potential for a disabling or fatal personnel injury or loss of the Orbiter, ground facilities or STS equipment.

2. Cause Analysis
Captured as "Hazards Cause".
All the credible causes are identified and listed (from design to assembly and operations). Likelihood of occurrence is assessed on credibility of occurrence only (outcome is discrete; credible or not credible).

3. Consequence Analysis
Driven by the Hazard Category as to whether a single or two-failure tolerant system is required to provide the necessary hazard controls or hazard cause inhibits.

4. Loss Analysis (CBA)
It is known as "Resulting Design/operations overhead".
At this stage, Controls to hazards are proposed on a hierarchy basis, control by design is the prime candidate. However operations can be used to control a hazard where there is an associated excessive design overhead.

5. Risk reduction and controls
Captured as "Hazard Controls".
Controls required to each cause contributor (from design to assembly and operations). The (verified) implementation of these controls provides the various inhibit levels required through the hazard categorisation. For controls implemented by (crew) operations, these controls must be verifiable at the operator level (direct feedback of successful inhibit provision).

6. Impact Analysis
Captured as the "Safety Verification Method".
Specific verification products are identified for all controls compliance verification. For operations hazard controls, the organisation responsible for developing the operations products reviews the implementability of a requirement and there is a unique process controlling this acceptance (however within the scope of the safety review itself).

7. Demonstration of Compliance Verification
The "Status of Verification" step consists on the verification status of the hazard control requirements defined in the Hazard Report.

At this stage all credible hazards are identified and controlled. Hence there is no residual risk concept.

4. DISCUSSION

The best-practice analysis of risk assessment and management techniques provides twelve key aspects which are further discussed in the context of relevance to spaceflight operations safety, below.

Rail Best Practice 1 – Presents general guidance which is wholly applicable to Spaceflight industry. However these are all being actively implemented, at an integrated level. This is mainly due to the integrated nature of hazards that arises from STS or ISS operations, and, the intrinsic international development principal of the ISS.

Rail Best Practice 2 – Operator aspects (both crew and ground operators) that implement or influence safety (through establishing or removing hazard controls) are already assessed for the need for formalised training and certification. Indeed during the safety review operations are assessed for their required uniqueness and skills level. If a control or operations requires a definite skill level (you are required not only to complete a task but also at a critical level of competency) then a specific training assessment and certification is invoked for the relevant crew.

Rail Best Practice 3 – ALARP has a direct equivalent in spaceflight safety being Design For Minimum Risk (DFMR).

Design for minimum risk are areas where hazards are controlled by specification requirements that specify safety related properties and characteristics of the design that have been baselined by the ISS program requirements rather than failure tolerance [16].

Rail Best Practice 4 – Common risk language and approach. The safety stakeholders during a mission (whilst clearly identified at the various agency levels and interfaces) are representatives from various disciplines (and associated cultures). So there are instances where safety related terminology has developed different meanings. For example "Caution and Warnings" in procedures are different from "Caution and Warning" on operator displays. A

"Critical" anomaly during mission is any safety related anomaly, whilst a "Critical" hazard has another specific meaning. Clearly there is room for an operational clarification of certain critical safety terms.

Rail Best Practice 5 – Design based rather than operator based controls. In the area of operations safety, where the crew establish a level of verifiable control through ISS operations (known as an Operations Hazard Control

Rail Best Practice 6 – Open declaration of the full impact of (crew exposure) to hazards. The declaration of "the potential for a disabling or fatal personnel injury or loss of the Orbiter" as part of the Hazard within each Hazard description is a clear indication of the event occurrence impact. However all novel hardware involving crew participation (particularly when acting as experiment subjects) the ISS Medical Review Board assess and reports on any unique hazards and the respective rating of the associated crew impacts.

Rail Best Practice 7 – Total lead operator authority delegation definition for "safing" instances. This has been addressed within the spaceflight sector, and also to include back-up responsibilities. This is to ensure that in the case of prime instigator of the delegated authority be unable to execute their (safety) responsibilities then the alternate authority can take over. Primarily this is given to the ISS commander and crew for safing (described within the ISS emergency procedures, for example)

Rail Best Practice 8 – Risk and safety management as good business practice. Safety management has been addressed since the beginnings of human spaceflight. More recently (in the last 10 years) risk assessment techniques have been applied within spaceflight, with a range of successes from different applications. Notably to date the safety review process for the habitable environment still does not apply risk assessment techniques.

Rail Best Practice 9 – Risk management as an approach to reduce costs and not safety. In the adoption and implementation of risk assessment in the spaceflight safety assessment process [14], this is a key mandate. Ensuring that where cost reductions are achieved (directly as a result of adopting a risk-based approach) that there is robust data to show that safety is being maintained.

Rail Best Practice 10 – Developer safety case guarantee. The developer of spaceflight hardware is required to develop (among many other deliverables) a safety data pack (SDP). The data pack must address ISS safety-specific and ISS spaceflight requirements. These requirements have been derived over a period of time, first with the STS and ultimately on the ISS. This SDP is reviewed at multiple stages during the spaceflight hardware development cycle; design, build and testing, in order to ensure that the final verified product meets the relevant safety requirements.

Rail Best Practice 11 – Use of both qualitative and quantitative risk assessment techniques to provide a robust assessment process. This best practice approach appears to be applicable to sectors that have already adopted risk assessment "universally" and are seeking to improve on an already solid risk assessment foundation. As such this could be difficult to apply bearing in the mind the teething problems encountered during limited risk assessment adoption within the sector.

Rail Best Practice 12 – Universal adoption of standards (including safety). The ISS users must comply with the ISS standards. A unique set of standards developed for the ISS (which are in some cases direct developments from the STS documentation). There is however one set of requirements (standards) for the Russian owned and operated segment and a slightly different set of requirements for the NASA-managed segment. This is in part due to the design .build and operations aspects of the various elements. However this has created compliance challenges for hardware that is to be operated within both segments (one example manifested in the two segments having mutually exclusive battery certification requirements).

5. CONCLUSION

In the application of risk assessment techniques and the recognition of the essential role that risk management plays in ensuring the effective delivery of dual safety and cost benefits, the rail sector provides a number of key best practice guidelines relevant to the spaceflight sector.

In response to these proposals for best practice adoption, it would appear whilst adopting a differing safety assessment approach (as opposed to a specific risk assessment approach), that the spaceflight industry does indeed similarly adopt good safety management approaches. These management approaches come about in part simply due to the "nature" of the spaceflight business, and have been built up other decades of operations experience. They are also very much in line with the best practice proposals captured in this paper.

On reflection then there equally is a case for the spaceflight industry to impart some of its best practice approaches in the safety management application that could be of benefits to other sectors, including the rail sector.

Specifically regarding the application of risk assessment techniques, it would appear that the (relatively) recent application of Probabilistic Risk Assessment (PRA) within the spaceflight sector could benefit form

guidance outside of the sector. This could be adopted purely on the basis that it might ensure continued development down the path of risk assessment adoption and implementation – particularly in the area of safety assessment (where a clear case has been put in support of this approach) [14].

In conclusion then the paper has presented the rail sector best practice to employ prior to the decision point that a system (transport vehicle and operating infrastructure) can operate safety. For rail this risk data is primarily generated on the basis of previous performance of (known) systems and the comparison of that system to the proposed new system design.

Spaceflight seeks to identify credible hazards and to address these through DFMR or fault tolerance approaches. This approach may lead to an over design where hazard credibility is marginal.

It is suggested that the robustness of either of these approaches lies in the assessment of operations safety performance after the "safe to operate" decision has been made, through the gathering of operations data (from both the rail and spaceflight sectors). We know that systems have been approved as safe in the past and we also know that failures have subsequently occurred. The determination of the point at which the reality of operations diverged from the analysis should provide an insight into the relative merits of these varying approaches to safety and risk assessment and management.

In addition to this further research needs to be undertaken to cross compare the influence of the operators themselves (train drivers and ISS crew members) bearing in mind the differences that exist between these two groups in terms of operations environment, levels of responsibility, and the varying levels of investment in training and operations support systems.

6. REFERENCES

1. Space Shuttle Columbia disaster, Wikipedia, May 2007

2. System safety engineering and risk assessment: A practical approach. Nicholas J. Bahr, Taylor and Francis, Washington, D.C., 1997

3. Engineering Safety Management, Issue 4, The Yellow Book 3, Fundamentals and Guidance, Rail Safety and Standards Board 2005.

4. Risk Management at SNCF, Risk Assessment International Conference, Joing, MM (1992), October 1992.

5. Report of the official inquiry into the Kings Cross Fire, chairman Desmond Fennel QC HMSO London 1988.

6. Investigation into the Clapham Junction railway accident, public enquiry, chairman Anthony Hidden QC HMSO London, A Hidden 1989.

7. Channel Tunnel Safety Authority, Inquiry into the fire on Heavy Goods Vehicle Shuttle 7539 on 18 November 1996, May 1997, ISBN 0115519319

8. Welsh, W., Channel Tunnel Fire (UK), contribution from Kent Fire Brigade to NEDIES project Lessons Learnt from Tunnel Accidents, 2001.

9. European Committee for Electrotechnical Standardization (CENELEC) Standards EN50126, EN50128 and EN 50129**.**

10. FAA System Safety Handbook, December 2000

11. Rutledge, P.J., Stamatelatos, M.G., Chandler, F.T., Moyer, R.W. The NASA Risk Management Program, *Proceedings of Joint ESA-NASA Space Flight Safety Conference*, Noordwijk, NL, 2002.

12. US Administrator's Briefing to House Science Committee, June 2000.

13. Preyssl, C. *et al*, Promotion of Risk Management at the European Space Agency – ESA, *Proceedings of Joint ESA-NASA Space Flight Safety Conference*, Noordwijk, NL, 2002.

14. Flippen, A.A. *et al*, The Prudent Application of Probabilistic Risk Assessment to Habitable Payloads, *Proceedings of Joint ESA-NASA Space Flight Safety Conference*, Noordwijk, NL, 2002.

15. NSTS/ISS 13830 - Payload Safety Review and Data Submittal Requirements, Revision C, 2006

16. SSP 50021 Safety Requirements Document, International Space Station Program, National Aeronautics and Space Administration, Texas, 1995