Successful Application of Systems Assurance on Large Scale Railway Projects

a report by

Paul Mann

Principal Consultant (PMSC Limited)

Introduction

As railway systems around the world become more complex, design teams are increasingly under pressure to deliver, design solutions which integrate both technical and Systems Assurance, (SA). Systems Assurance as an approach has been refined over the last decade to provide project managers with a mechanism to achieve specified Reliability, Availability, Maintainability and Safety (RAMS) objectives. This paper focuses on the methodology of Systems Assurance but more importantly provides a guide to project managers on SA aspects that should form part of the design development and decision making process. The paper is biased towards SA activities undertaken by a principal contractor on a large scale project, however much of the content would apply equally well to sub-contractors working for the principal contractor and for the client team.

Unfortunately, all to often, human nature is such that accidents or other undesirable events occur and after investigation are deemed to have been preventable. There have been a recent spate of railway accidents and incidents around the world which clearly serve to illustrate the need for an integrated holistic approach to Systems Assurance at the design stage.

At PMSC we have collected statistics on industrial and transport incidents from around the world as far back as the year 1782. Our database has some 2258 events of which 818 are railway incidents. Nearly 60% of railway accidents on our database have been caused by human errors. Another depressing statistic, is that there have been no fewer than 89 railway incidents since 1842 where 100 passengers or more have been killed.

Some examples of recent major railway accidents from around the world are presented in table 1.

Background to Systems Assurance

Essentially, Systems Assurance is the application of management methods and analysis techniques to assure that a design meets Reliability, Availability, Maintainability and Safety, (RAMS) criteria. Hence, Systems Assurance is often referred to as RAMS Assurance. It should be clearly understood that the intent of RAMS Assurance is not just to provide analytical techniques as a metric on performance, but more importantly it should provide a management tool with which to co-ordinate and assure the whole design ie. a holistic management systems approach.

Often on projects, due to a lack of understanding, the SA process is demoted to a secondary status in the

Mr. Mann is a graduate in Physics from Leeds University and has worked as a RAMS consultant to the railway industry both in the UK and Overseas for the last ten years. He is currently the managing director of PMSC Limited and has successfully negotiated and completed RAMS contracts for a range of railway contractors and operators including: Alsthom, Bombardier, Kawasaki Heavy Industries, London Underground, Railtrack and Siemens.

Table 1: Some Recent Examples of Railway Accidents From Around the World.

Date	Location	Number Killed	Seriously Injured	Root Cause	Comments
05/10/1999	Paddington, London	31	20	Alleged Signal passed at danger due to driver error	Great Western Train collided with a Thames Train as a result of a SPAD by the Thames Train.
20/09/1999	Southall, London	7	20	Alleged signal passed at danger	Intercity 125 train collided with a freight train.
02/09/1999	Gaisal, India	100	NA	Reported as a signalling failure	Head on collision of two trains travelling in excess of 100mph.
08/09/1999	Near Sainte Foy La Grande, France	12	40	Infrastructure related	Collision between lorry and train on road crossing
03/06/1998	Germany	100	NA	Thought to be a faulty wheel	Faulty wheelset resulted in high speed derailment of ICE train.
24/03/1999	National Park, Kenya	32	85	Thought to be overspeeding on a tight bend	Train derailed at high speed on a bend in the Tsavo National Park.

design development and considered a paperwork exercise. In the UK, Europe and North America the need for SA has been mainly driven by legislation. This is evident today to the extent that many invitation to tender specifications for large scale railway projects make specific reference to standards such as the emerging Euro Norm standard 50126, UK defence standards, such as 00-56 and US Military Standards such as 882C and 1629. A typical Principal Contractor SA team structure which would be consistent with the requirements of the above standards, for larger railway projects is presented in figure 1. Some of the generic roles and responsibilities of the key members of the SA team have been described below for information.

Safety Assurance Manager, (SAM)

- Project manage the SA activity within the project and prepare the initial SA Program Plan
- Provide the single point of contact with the regulator or client on SA activities
- Ensure that sufficient and competent resources are made available for the SA activity
- Act as the principal single point of contact for interfaces between System Integration and Systems Assurance
- Act as the principal single point of contact between the project management team and sub-contractor effort on matters of SA.
- Act as Hazards and Operability (HAZOP) study Chairman during hazards identification studies

Specialist Support

- Provide specialist support on an ad-hoc basis in the fields of Human Factors, Electromagnetic Compatibility (EMC), fire protection and toxicity calculations for interior equipment on train etc.

Reliability & Availability Project Engineers

- Conduct Reliability and Availability studies as defined by the SAM
- Prepare Reliability and Availability reports consistent with the client or regulator requirements and formats
- Maintain a repository of R&A data sources for use on the project

Maintainability Project Engineers

- Conduct maintainability predictions
- Assist with the definition of Line Replaceable Units (LRU's) for each of the systems
- Develop a comprehensive set of functional block diagrams for each system within the project scope

Safety Project Engineers

- Assist the SAM during the HAZOP activities as HAZOP Secretary
- Assist with the development of the Safety assurance studies under the direction of the SAM including FMECA, QRA and other similar core SA studies
- Manage the hazards log

One of the key activities for the project will be the management of the interface between the SA processes and the Systems Integration, (SI) processes. Systems Integration is essentially the management of interfaces in terms of systems that interact with each other. It will be beneficial to ensure the following:

- Safety issues associated with interfaces are identified early by level 1 HAZOPs
- Safety representation at systems integration meetings, any safety issues entered into hazards log
- Systems integration personnel attend key HAZOP's to take ownership first hand of any interface issues arising.
- The SAM should be required to close out any design changes that result from the SI process.
- The SIM and SAM should cooperate fully with each other and will hold periodic SI/SA meetings to ensure all items on the hazards log are being closed.

It should be reiterated at this point that this paper is aimed at a principal contractor co-ordinating the input of several sub-contractors. Hence, the actual size of the team can be variable dependent on the exact nature of the project.

Target Levels Of Risk

The acceptability of Systems Assurance is best determined against a pre-determined set of risk levels ideally assigned by the client or regulator at the bidding stage of the project. On modern large scale infrastructure and rolling stock projects target levels of risk are being set for individuals and critical groups. Typically, the following criteria might be set:

- Individual risk for railway workers
- Individual risk for passengers (critical group being commuters)
- Individual risk for members of the public

In some, modern studies targets for so called Societal risk are also set. This relates to setting an upper limit on the frequency per incident of consequences in the

following ranges 1-10 deaths, between 10 and 100 deaths and greater than 100 deaths. Historically, this information has been plotted on the so called F/N curves.

Typical values for individual risk targets used currently in the UK are quoted in table 2.

Ball Park Estimates for the Costs Associated with Systems Assurance

Risk targets are also set for individual accident sequences. This is based on apportioning the individual and societal risk targets to generate the so-called risk matrix. This approach is particularly useful in the early stages of a project (in the absence of any formal numerical Quantified Risk Analysis (QRA) results), as it provides an indication, all be it judgmental, as to whether control measures should be considered to meet the As Low As Reasonably Practicable (ALARP) Principle.

As stated earlier, the key to success in Systems Assurance is having sufficient resources available with appropriate competence. The table below provides some ball park estimates from recent railway projects as an indication of typical costs from a range of sizes of projects. The costs associated with Systems Assurance should take into account not just costs to the project from specialist co-ordinating consultants but should also include internal project team member costs and sub-contractor RAMS assurance costs.

Hence, the above estimated data points indicate that for lower value projects budgets of between 1 and up to 5% of total project budget could be realistic. However, for larger scale projects, budgets for Systems Assurance of between 0.4 up to 1% of the total value of the project could be considered as realistic budgetary estimates. It should be noted that the above costs are offered as guides, not hard and fast rules.

Review of Process and Methods

Figure 2 presents a typical flow chart for the safety aspect of a Systems Assurance or RAMS Assurance project.

The SA process commences with the issue early in the life of the project, of the Safety Assurance Program Plan, (SAPP). This is a document that will state clearly and unambiguously how the project will manage and implement safety assurance. This document is a key milestone in establishing the resource requirements to deliver Safety Assurance. It is also a good barometer to measure the commitment to safety of the project management team. The sub-contractor effort will be optimised early if the SAPP provides them with a clear guidance on methodologies and apportionment of the risk that applies to their systems or equipment.

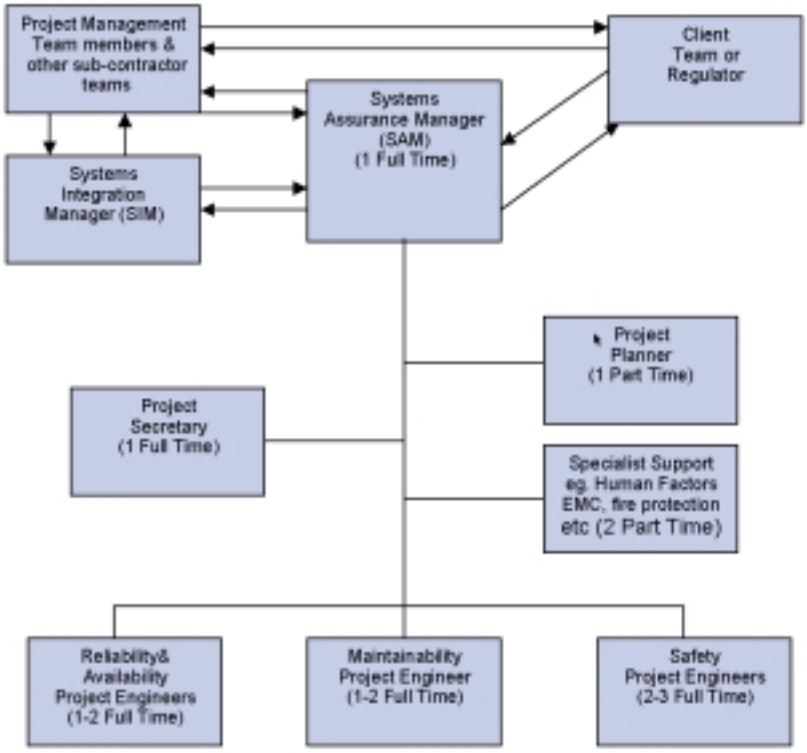

Figure 1: Typical Structure of the Co-ordinating SA Team and Sa Interfaces for Large Scale Railway Projects

Risk Group	Risk level Frequency Per Annum	
	Premature Fatality	**Major Injury**
Railway Workers	1.0E-04	1.0E-03
Passengers	1.0E-05	1.0E-04
Members of Public	1.0E-05	1.0E-04

Table 2: Some Example Risk Targets

Estimated Value of Project UK £	Estimated Value of Systems UK £ Assurance	% of Project Costs	Example projects for benchmarking
1 Million	50K	5%	Minor infrastructure or rolling stock Modifications
10 Million	300 K	3%	A Ticketing system
50 Million	500 K	1%	A new railway depot
450 Million	2 M	0.4%	A new rolling stock project
1500 Million	10 M	0.7%	First part of a new high speed railway link
2800 Million	20 M	0.7%	New underground railway system in UK
1000 Million	10 M	1%	New underground system overseas

Table 3: Some Example SA Budgets From Previous Projects

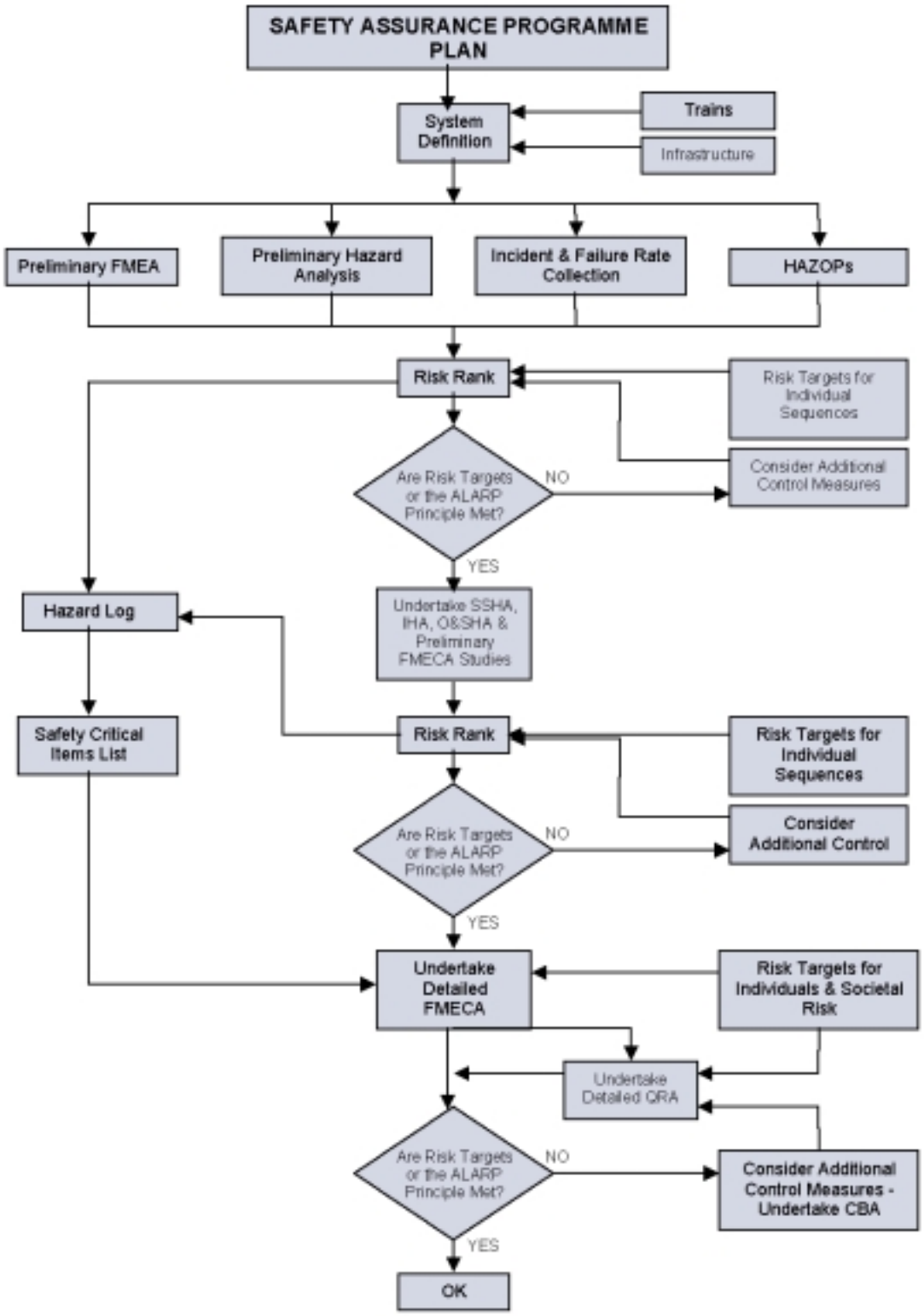

Figure 2: Flow Chart for the Safety Activities of Systems Assurance or RAMS

Once systems have been defined, the hazards identification stage can commence and provide an early input to the project safety hazards log. This will, if performed by competent personnel, give an early indication of any conceptual problems associated with the design and its instrinsic hazard potential. At the appropriate time the Preliminary Hazards Analysis (PHA) and Failure Mode Effects Analysis (FMEA) can be supplemented by the use of structured "brainstorming" techniques such as HAZOPs involving team members from the various other disciplines on the project. However, the timing of the application of these techniques should be optimised to maximise influence over the design development and minimise the need for reworking due to any changing nature of the detailed design. The role of the Systems Assurance Manager will be to provide clear advice to the project management team on the timing of these activities.

The risk ranking of hazard potential is a key factor in understanding whether risks posed by the design (and there are always residual risks, the risk free design does not exist) are tolerable and more importantly whether all reasonably practicable safety measures have been considered by the design teams and sub-contractors. Initially, it will be the role of the SAPP to provide the frameworks for the judgement of risk and its tolerability or otherwise. As the project develops the concept of risk ranking should be clearly understood by all parties prior to the embarkation on HAZOP or FMECA studies.

The HAZOP studies in particular should be well organised, and ideally independently chaired and secretaried. Briefing notes to establish the scope of the HAZOP should be issued prior to the actual meetings. Adequate time should be set aside for the HAZOP and attendees should clear their diaries thus providing full time commitment to the brainstorming process, (mobile telephones and pagers should be banned). Reporting of the HAZOP should contain system descriptions together with the hazard sequences identified. Any additional safety measures considered reasonably practicable to reduce risk should be reported and stored on the hazards log until formally closed out by the formal project design review process. In my experience, one of the major problems on large scale projects is that the final stage of formally reviewing proposed design enhancements for safety is rarely implemented in a systematic manner. More often, at best a piecemeal consideration of design changes that are perceived as easy to implement is undertaken. At worst design enhancements considered during the HAZOPs are simple ignored and buried deep in the paperwork.

Following qualitative consideration of hazard potential, there is a need to develop a quantitative model of the design. This process is entitled Quantitative Risk Analysis or QRA. Typically, Fault and Event Trees will be constructed and analysed to identify the cut-sets or events, which lead to undesirable consequences. As with the HAZOP and FMECA, the QRA can be an extremely iterative process unless performed at the right time in the project. Conventional thinking proposes that the QRA should be performed towards the end of design development but prior to project design freeze to allow for design enhancements if risk targets cannot be met. The QRA should normally have as an integral part a consideration of human factors ie. the potential for operator error and events which model system wide Common Cause Failure, (CCF) potential. Most modern railway projects have adopted the Fault Tree + " state of the art" software to facilitate this modeling process. Companies using this software include, Railtrack, London Underground, Singapore Land Transport Authority and Hong Kong MTRC and Kowloon Canton Railway Corporation, (KCRC).

If formal cost benefit analysis is required to demonstrate the ALARP principle, ie. that risks are as low as reasonably practicable, the QRA provides a good modeling tool to assess the benefits of any risk reducing measures. Thus comparisons of benefits and costs can be assessed, provided of course there is a clear statement on what constitutes the value of life saved by a preventative safety measure. Within the UK the safety culture has allowed a value to be placed upon a life saved as in the region of £ 2,600,000 pounds sterling when considering multi-fatality events and £ 900,000 for events involving a single fatality. Ironically, elsewhere in the world for example in the USA the concept of the value of a life saved is considered tantamount to tacit acceptance of legal negligence and therefore not invoked. On this issue, it is my belief that more research needs to be undertaken to standardise a world wide methodology to judge the worth of design enhancements to reduce risks.

The use of of an Independent Safety Assessor (ISA) is becoming standard practice for some larger railway projects in Europe. The appointment of an ISA can help in securing approvals from regulatory bodies. However, for an ISA to be most effective, the project must plan for the ISA to be involved in the planning stage of the project as well as reviewing the results of any analyses during its implementation. The need for an ISA will normally be client driven but it is generally considered appropriate for such ISA effort to be directed towards safety critical systems such as signalling and systems associated with high consequence hazards such as fire or derailments/collisions.

As the Safety Assurance process draws to a conclusion, the Safety Assurance Summary Report or Safety Case provides the regulator with an overview of the work undertaken for the assurance of safety on the project. This provides the regulator with a " map" to guide their review and acceptance of the overall process.

Similar processes are recommended for RAM management and analysis. Initial integrated RAM Program Plans, leading to a clear definition of resource requirements and bar chart activities. Delivery of reliability predictions, maintainability predictions and corrective and preventative maintenance strategies. RAM demonstration plans should be developed to ensure that there is a plan to demonstrate the predicted RAM values are met in practice.

Review of key problem areas and solutions

There are a number of problematic issues related to Systems Assurance but it is clear that sound planning and the provision of expert resources with the commitment of the design management team, early in the project is the key to successful implementation of Systems Assurance on projects. Some typical problems found on projects have been highlighted below, maybe you recognise a few of them:

Problem Issue in RAMS	*Possible Solutions*
Inadequate RAMS resources made available late in the project	• *Good planning early on* • *Commitment by the management team and client to SA activities* • *Client requires draft SA Plan before contract starts*
Safety personnel not integrated into design review process	• *Management training on SA to that they can understand the benefits to be gained from SA* • *Clients specifications state SA as a key requirement*
Engineering personnel not involved in SA process.	• *Engineering personnel encouraged to conduct FMECA analysis and attend Hazards Identification sessions (HAZOPs)* • *Ownership of hazards by engineering personnel*
Systems Assurance studies performed too early resulting in the requirement for extensive reworking as the design develops	• *SA Plan has schedule of activities showing timing and linkage of SA activities to key project milestones.* • *Concurrent engineering and good communications at the working level between SA analysts and design team.*
Weak interface between systems integration and systems assurance results in safety issues being missed and interfaces not being clearly understood.	• *Provision of specific interface meetings between SA and SI personnel.* • *Safety as an agenda item in SI meetings* • *Interfaces as an agenda item in SA meetings for example HAZOPs*
Safety risk assessments out of touch with design issues	• *Safety input at the design reviews* • *Latest drawings using at HAZOP*
Project management lack of commitment to safety due to competing objectives leading to a lack of ownership of the SA process by design teams	• *Integration of SA activities into PM meetings and planning process* • *Attendance by Project Manager at SA key meetings such as HAZOPs* • *SA Plans contain PM Commitment statements to SA activities* • *Training for PM in SA activities*
Scarcity of relevant data for Quantification of risks and reliability analysis or over reliance on generic data sources	• *Operators should be encouraged to collect incident and equipment failure rate data. This should be made available to suppliers.* • *Data collection schemes between operators, successfully implemented by Oil & Gas operators in the North Sea by the provision of a shared data scheme called OREDA 92.* • *Suppliers encouraged to collect data on their own systems* • *Approved generic database sources should be advised to designers*
Sub-contractors poorly controlled in terms of their delivery of RAMS studies	• *SA Plans must contain sections on the management of sub-contractors* • *Sub-contractors encouraged to employ competent SA personnel during the bidding phase of the project.* • *Failure of a supplier to deliver RAMS studies should be linked to their payment schedules*
Unclear ambiguous specifications and RAMS Plans leading to uncertainty	• *Expert consultant advise at the planning stages or independent review by experts if the plans are written in house.* • *Proper reference to the latest standards eg EN 50126, Def Standard 00-56 or Mil Std 882C.* • *Use of project standard formats for SA Plans*
Setting unrealistic and unachievable numerical RAMS targets	• *Client must consult with supplier at the contract stage and if supplier cannot meet the targets because they are unrealistic, negotiation should take place on what more realistic targets might be.* • *Deterministic studies should be accepted under agreed circumstances as an alternative means to achieving a numerical risk target.*
Arguments about who pays if a a RAMS target can not be met but the design meets the engineering specification	• *Ongoing dialogue with the client on SA issues* • *Client sets RAMS Targets at tender stage and supplier must state how he intends to meet the targets or why he requires a relaxation on the target*

	• *Client allows for variations to the contract for design improvements to meet RAMS targets even though design meets deterministic specification, or client allows supplier to negotiate on RAMS targets.*
Loss of goodwill if designers are expected to improve design at a significant cost to themselves	• *ALARP Interpretations and agreements with suppliers early on in a project. If design measures are cheap to implement sub contractor should implement directly at their cost, if more expensive then a variation to their contract can be agreed with the client.*
QRA results come out late in the project after design freeze and therefore are ignored	• *Firm linkage of SA activities to over all project milestones.* • *An initial concept QRA should be performed early in the design process*
Problematic RAMS Interfaces between Client, main contractor & sub-contractors	• *Clear unambigous SA Plans initially agreed with client and cascaded down to all sub-contractors* • *Sub contractors required to develop their own SA Plans prior to works commencing, acceptance of which is a pre-requisite for commencement of works*

Table 4: Some Examples Of Typical SA Problems and Proposed Solutions

It is for sure, that many of you reading this paper may have experienced or recognised at least one or more of these problems during a project you have been recently involved with. Some readers may unfortunately, may recognise several problems similar to the above on projects currently underway.

What are the benefits of Systems Assurance ?

What are the benefits of Systems Assurance? To answer this question we must evaluate the benefits from the four aspects of systems assurance of Reliability, Availability, Maintainability and Safety.

For safety, the main benefit of applying assurance principles is the delivery of a safe design which can be transparent to regulators wishing to certify that all reasonably practicable safety risk reducing measures have been considered. Moreover, for the future operator Systems Assurance provides a " comfort factor" that all reasonably foreseeable accident potential has been considered and planned for. Thus a future operator has the comfort that he may be able to minimise exposure to bad public relations and the aversion that members of the public and authorities have to large scale railway accidents.

In terms of reliability, there are two main benefits from an integrated approach to systems assurance. Firstly, if a design is reliable it will mean that timetables and therefore passenger services can be reliably implemented. Secondly, reliable equipment reduces total life cycle costs and also ensures that value for money can be obtained from systems comprising the design.

Availability means that down time can be minimised, thereby perpetuating the concept of dependability of the facility or service with fare paying passengers.

For Maintainability System Assurance provides a tool with which to ensure that safety risks to maintainers either on the track or in depots can be minimised. Furthermore, by adopting sound maintainability SA techniques early in the design process, life cycle costs arising from maintenance activities (preventative and corrective) can be properly predicted and life cycle costs minimised.

Conclusions

In conclusion, there are several issues that need further debate within the industry forum:

- Systems Assurance has a key role to play in the 21st Century in assuring that as complexity and economic pressures increase, safety and overall life cycle costs are not compromised.

- At the outset of projects budgets should be properly considered for the inclusion of Systems Assurance. Typically, budgets of 1-5% of project value should be set aside for lower value projects and between 0.4 – 1% of project value for larger value projects such as major new railway undertakings or rolling stock fleet replacement projects.

- More needs to be done to collect world wide data on rail crashes and equipment failures to facilitate future analysis thereby maximising the use of operational data in favour of less applicable generic data sources. This work could also provide an insight into a better definition of what is considered ALARP.

- Systems Assurance must be given a clear role in projects early, with a clear commitment from the project management team to make adequate and competent resources available to deliver Systems Assurance.

- Provision of clearer unambiguous guidance to project managers on what Systems Assurance techniques to apply at various stages of projects.

- Proactive participation and interaction of Systems Assurance in the Systems Integration process and Design Review meetings

It is hoped that this paper has raised the profile of some of the issues associated with Systems Assurance and its role within large scale railway infrastructure and rolling stock projects.

In summary, it is proposed that the Systems Assurance Manager must act as the conscience of the Project Manager to ensure that all reasonably practicable safety measures have been applied to the design and that overall foreseeable risks are controlled to a level which can be considered tolerable. ■