



***PM Safety Consultants Limited***

[www.pmsafety.co.uk](http://www.pmsafety.co.uk)

**HAND OUT FOR RAMS SEMINAR**

**WESTIN PALACE HOTEL MADRID HELD ON 2<sup>ND</sup> DECEMBER 2004**

**CONTENTS**

<b>SECTION 1: CONTENT OF SEMINAR .....</b>	<b>2</b>
<b>SECTION 2: SPEAKER PROFILE. ....</b>	<b>3</b>
<b>SECTION 3: PAPER: SUCCESSFUL APPLICATION OF SYSTEMS ASSURANCE ON LARGE SCALE RAILWAY PROJECTS .....</b>	<b>4</b>
<b>SECTION 4: EN50126 FLOWCHARTS FOR IMPLEMENTATION OF RAMS AT DIFFERENT PROJECT STAGES.....</b>	<b>13</b>
<b>SECTION 5: SOME USEFUL NOTES ON SYSTEMS ASSURANCE METHODOLOGIES AND REFERENCES .....</b>	<b>24</b>
<b>SECTION 6: SOME NOTES ON FAULT AND EVENT TREE CONSTRUCTION AND ANALYSIS .....</b>	<b>28</b>
<b>SECTION 7: SOME NOTES ON HUMAN FACTORS .....</b>	<b>34</b>
<b>SECTION 8: SOME NOTES ON THE USE OF THE HEART METHOD.....</b>	<b>39</b>
<b>SECTION 9: SOME NOTES ON FIRE RISK ASSESSMENT.....</b>	<b>52</b>
<b>SECTION 10: SOME USEFUL SYSTEMS ASSURANCE REFERENCES .....</b>	<b>54</b>

The contents of this hand out are provided on an informal for information only basis.



## **SECTION 1: CONTENT OF SEMINAR**

Definitions of Systems Assurance

**[2 minutes]**

- Definition of RAMS
- Human Factors
- Fire Safety

Review of Typical Standards (principally EN50126)

**[5 minutes]**

- EN50126 and the life cycle
- Verification & Validation
- Other standards including UK Line Standards and Group Standards and Yellow Book
- Defence Standards and Military Standards

Systems Assurance Planning (Formats and how to gain approvals)

**[8 minutes]**

- Typical Formats of Systems Assurance Plans
- Process of gaining approvals

Methodologies such as HAZOP, SIL assessment, QRA, ALARP etc

**[10 minutes]**

- HAZOP
- Hazard Logs
- Fault Trees
- Event trees
- FMECAs
- SIL Assessments
- HRA
- CCF

Review of Benefits

**[5 minutes]**

- Strategic Review of major benefits of Systems Assurance

Some examples of projects completed

**[5 minutes]**

Review of Some Problems and Solutions

**[5 minutes]**

Questions & Answers

## **SECTION 2: SPEAKER PROFILE.**



**Mr. Paul Daniel Mann, B.Sc(Hons), C.Eng, M.I.Mech.E, FSaRS.**

Mr. Mann is the Managing Director and majority shareholder in PM Safety Consultants Limited ([www.pmsafety.co.uk](http://www.pmsafety.co.uk)). PMSC was formed in 1992 and provides consulting support and advice to a wide range of clients around the world.

Mr. Mann holds a Bachelor of Science degree in Physics from Leeds University and graduated in 1980 and is a Chartered Engineer via the Institute of Mechanical Engineers and a Fellow of the UK Safety & Reliability Society.

During his time as a consultant advisor he has gained experience in the field of Systems Assurance or RAMS working in a variety of industries including the Railway, Nuclear, Oil & Gas and Defence sectors both in the UK and Internationally.

Specifically, Mr. Mann has worked on several major Rolling Stock and Infrastructure projects including:- Class 332 Heathrow Express built by Siemens; the class 373/1 Eurostar built by Alstom; the High Speed rolling stock being provided to the Taiwan High Speed Rail project by Kawasaki; C751B rolling stock provided for the Changi extension in Singapore and SP1900 EMUs provided for West Rail and East Rail in Hong Kong. He has conducted numerous railway HAZOP studies as both Chairman and Secretary. Mr. Mann also acted as the RAM analyst for the new proposed Thameslink 2000 project and to Bombardier on their Electrostar reliability improvement programme.

In terms of infrastructure, Mr. Mann has most recently acted as RAMS coordinator for the Core System of the Taiwan High Speed Rail project during Concept and Preliminary Design stages and has also managed the Systems Assurance bid documentation for the C830 Marina Line project in Singapore, now referred to as the Circle Line. He was also retained as Systems Assurance advisor to NEC of their C760 Communications project in Singapore. Last year he managed the production of the Safety Case for the implementation of the TETRA system at railway stations as part of the United Kingdoms Governmental strategic response to the threat of terrorism in the UK.

He is fully familiar with both emerging European EN50126 RAMS guidance, IEC61508 Application of Safety Integrity Levels and UK Defence Standards 00-56 and 00-55 and a wide range of RAMS methodologies and procedures.

PMSC Limited is cooperating with MTP to develop the understanding of RAMS in Spain. We are hoping to raise the understanding and awareness of RAMS in various industries where benefits can be derived.

## **SECTION 3: PAPER: SUCCESSFUL APPLICATION OF SYSTEMS ASSURANCE ON LARGE SCALE RAILWAY PROJECTS**

**By**  
**Paul Mann**

(Principal Consultant, PMSC Limited,  
Suite D Third Floor, Saturn Facilities, 101 Lockhurst Lane, Coventry, CV6 5SF, UK)



*Mr. Mann is a graduate in Physics from Leeds University in the United Kingdom 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: Alstom, Bombardier, Kawasaki Heavy Industries, London Underground, Railtrack and Siemens.*

These notes have been adapted for the RAMS conference in Madrid held on 2<sup>nd</sup> December 2004.

### **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 too often human nature is such that accidents or other undesirable events occur and after investigation are deemed to have been preventable. There has been a recent spate of railway accidents and incidents around the world, which clearly serves 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.

<b>Date</b>	<b>Location</b>	<b>Number Killed</b>	<b>Seriously Injured</b>	<b>Root Cause</b>	<b>Comments</b>
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.
19/09/1999	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

**The Application of RAMS in Large Scale Complex Railway Projects  
RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

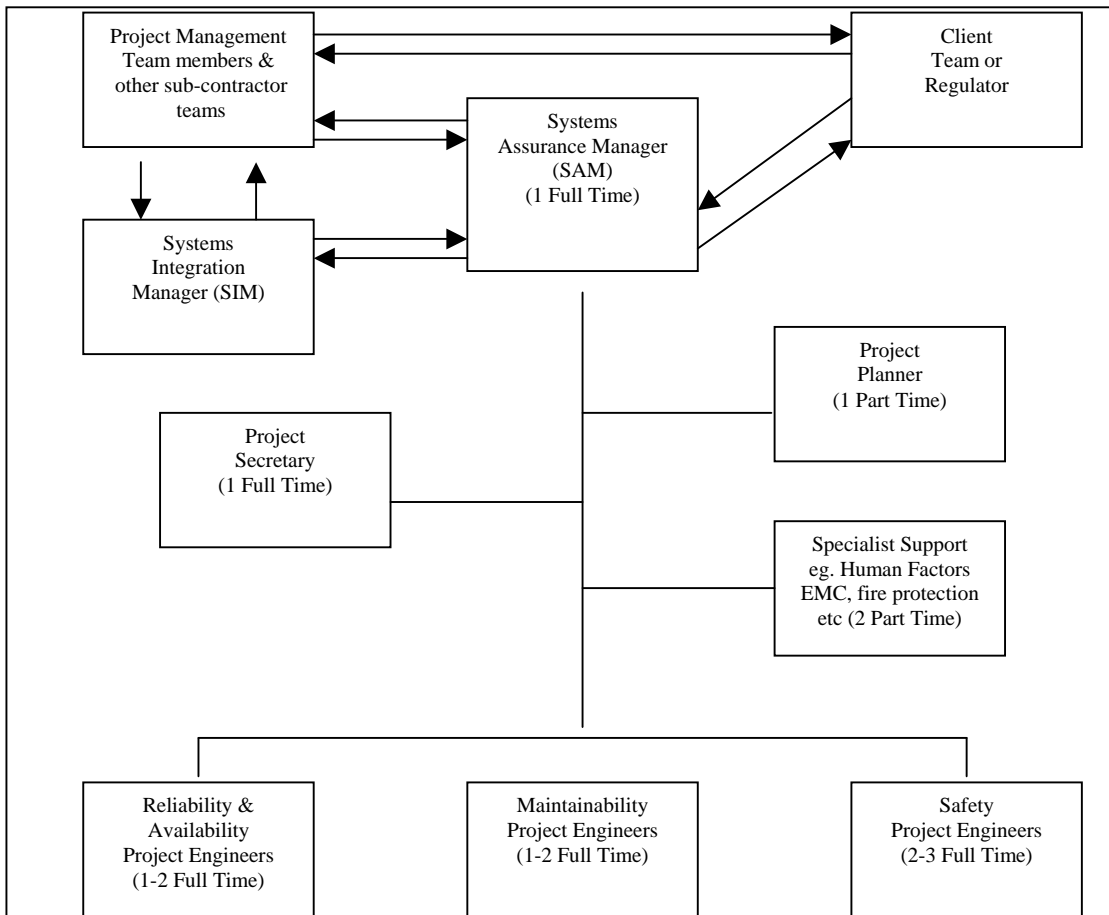
<i>Date</i>	<i>Location</i>	<i>Number Killed</i>	<i>Seriously Injured</i>	<i>Root Cause</i>	<i>Comments</i>
24/03/1999	National Park, Kenya	32	85	Thought to be overspeeding on a tight bend	Train derailed at high speed on a bend in the Tsavo National Park.

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

**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 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. These are intended for guidance only.



# The Application of RAMS in Large Scale Complex Railway Projects

## RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004

*Typical team size: Core team full time = 6-9 persons, Part Time expertise = 3 persons, RAMS co-ordination team for a principal contractor. (Guidance only.)*

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

### 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 Systems 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 HAZOPs 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 co-operate 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

**The Application of RAMS in Large Scale Complex Railway Projects  
RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

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.

<b>Risk Group</b>	<b>Risk level Frequency Per Annum</b>	
	<b>Premature Fatality</b>	<b>Major Injury</b>
<i>Railway Workers</i>	<i>1.0E-04</i>	<i>1.0E-03</i>
<i>Passengers</i>	<i>1.0E-05</i>	<i>1.0E-04</i>
<i>Members of Public</i>	<i>1.0E-05</i>	<i>1.0E-04</i>

**Table 2: Some Example Risk Targets**

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.

**Ball Park Estimates for the Costs Associated with Systems Assurance**

As stated earlier, the key to success in Systems Assurance is having sufficient resources available with appropriate competence. Table 3 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.

<b>Estimated Value of Project UK £</b>	<b>Estimated Value of Systems Assurance UK £</b>	<b>% of Project Costs</b>	<b>Example Projects for Benchmarking</b>
<i>1 Million</i>	<i>50K</i>	<i>5%</i>	<i>Minor infrastructure or rolling stock modifications</i>
<i>10 Million</i>	<i>300 K</i>	<i>3%</i>	<i>A ticketing system</i>
<i>50 Million</i>	<i>500 K</i>	<i>1%</i>	<i>A new railway depot</i>
<i>450 Million</i>	<i>2 M</i>	<i>0.4%</i>	<i>A new rolling stock project</i>
<i>1500 Million</i>	<i>10 M</i>	<i>0.7%</i>	<i>First part of a new high speed railway link</i>
<i>2800 Million</i>	<i>20 M</i>	<i>0.7%</i>	<i>New underground railway system in UK</i>
<i>1000 Million</i>	<i>10 M</i>	<i>1%</i>	<i>New underground system overseas</i>

**Table 3: Some Example SA Budgets from Previous Projects**

Hence, the above estimated data points indicate that for lower value projects, budgets of between 1 and 5% of total project budget could be realistic. However, for larger scale projects, budgets for Systems Assurance of between 0.4 and 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 Application of RAMS in Large Scale Complex Railway Projects RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

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.

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 intrinsic 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 simply ignored and buried deep in the paperwork.



The Application of RAMS in Large Scale Complex Railway Projects  
 RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004

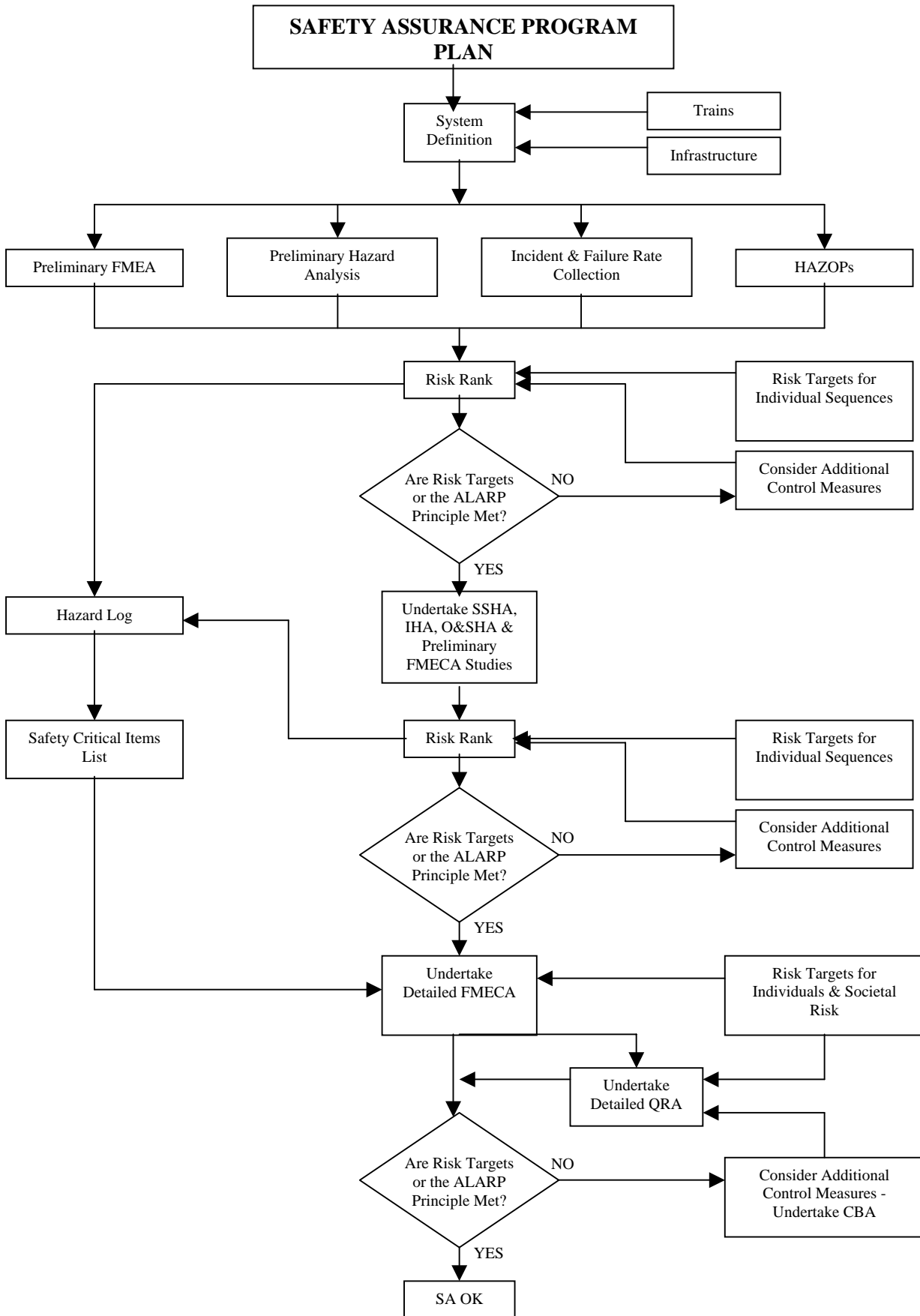


Figure 2: Flow Chart for the Safety Activities of Systems Assurance or RAMS



## The Application of RAMS in Large Scale Complex Railway Projects RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004

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 modelling process. Companies using this software include Railtrack, London Underground, Singapore Land Transport Authority, 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 modelling 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 preventing a fatality (VPF) by a safety measure. Within the UK the safety culture has allowed a value to be placed upon a life saved as in the region of £ 3,000,000 sterling when considering multi-fatality events and £ 1,000,000 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 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:

<b>Problem Issue in RAMS</b>	<b>Possible Solutions</b>
<b>Inadequate RAMS resources made available late in the project</b>	<ul style="list-style-type: none"> <li>• Good planning early on.</li> <li>• Commitment by the management team and client to SA activities.</li> <li>• Client requires draft SA Plan before contract starts.</li> </ul>
<b>Safety personnel not integrated into design review process</b>	<ul style="list-style-type: none"> <li>• Management training on SA so that they can understand the benefits to be gained from SA.</li> <li>• Clients specifications state SA as a key requirement.</li> </ul>
<b>Engineering personnel not involved in SA process</b>	<ul style="list-style-type: none"> <li>• Engineering personnel encouraged to conduct FMECA analysis and attend Hazards Identification sessions (HAZOPs).</li> <li>• Ownership of hazards by engineering personnel.</li> </ul>
<b>Systems Assurance studies performed too early resulting in the requirement for extensive reworking as the design develops</b>	<ul style="list-style-type: none"> <li>• SA Plan has schedule of activities showing timing and linkage of SA activities to key project milestones.</li> <li>• Concurrent engineering and good communications at the working level between SA analysts and design team.</li> </ul>



**The Application of RAMS in Large Scale Complex Railway Projects  
RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

<b>Problem Issue in RAMS</b>	<b>Possible Solutions</b>
<b>Weak interface between Systems Integration and Systems Assurance results in safety issues being missed and interfaces not being clearly understood</b>	<ul style="list-style-type: none"> <li>• Provision of specific interface meetings between SA and SI personnel.</li> <li>• Safety as an agenda item in SI meetings.</li> <li>• Interfaces as an agenda item in SA meetings, for example HAZOPs.</li> </ul>
<b>Safety risk assessments out of touch with design issues</b>	<ul style="list-style-type: none"> <li>• Safety input at the design reviews.</li> <li>• Latest drawings used at HAZOP.</li> </ul>
<b>Project management lack of commitment to safety due to competing objectives leading to a lack of ownership of the SA process by design teams</b>	<ul style="list-style-type: none"> <li>• Integration of SA activities into PM meetings and planning process.</li> <li>• Attendance by Project Manager at SA key meetings such as HAZOPs.</li> <li>• SA Plans contain PM Commitment statements to SA activities.</li> <li>• Training for PM in SA activities.</li> </ul>
<b>Scarcity of relevant data for Quantification of risks and reliability analysis, or over reliance on generic data sources</b>	<ul style="list-style-type: none"> <li>• Operators should be encouraged to collect incident and equipment failure rate data. This should be made available to suppliers.</li> <li>• Data collection schemes between operators, successfully implemented by Oil &amp; Gas operators in the North Sea by the provision of a shared data scheme called OREDA 92.</li> <li>• Suppliers encouraged to collect data on their own systems.</li> <li>• Approved generic database sources should be advised to designers.</li> </ul>
<b>Sub-contractors poorly controlled in terms of their delivery of RAMS studies</b>	<ul style="list-style-type: none"> <li>• SA Plans must contain sections on the management of sub-contractors.</li> <li>• Sub-contractors encouraged to employ competent SA personnel during the bidding phase of the project.</li> <li>• Failure of a supplier to deliver RAMS studies should be linked to their payment schedules.</li> </ul>
<b>Unclear ambiguous specifications and RAMS Plans leading to uncertainty</b>	<ul style="list-style-type: none"> <li>• Expert consultant advice at the planning stages, or independent review by experts if the plans are written in house.</li> <li>• Proper reference to the latest standards eg. EN 50126, Def Standard 00-56 or Mil Std 882C.</li> <li>• Use of project standard formats for SA Plans.</li> </ul>
<b>Setting unrealistic and unachievable numerical RAMS targets</b>	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Deterministic studies should be accepted under agreed circumstances as an alternative means to achieving a numerical risk target.</li> </ul>
<b>Arguments about who pays if a RAMS target can not be met but the design meets the engineering specification</b>	<ul style="list-style-type: none"> <li>• Ongoing dialogue with the client on SA issues.</li> <li>• 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.</li> <li>• 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.</li> </ul>
<b>Loss of goodwill if designers are expected to improve design at a significant cost to themselves</b>	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
<b>QRA results come out late in the project after design freeze and therefore are ignored</b>	<ul style="list-style-type: none"> <li>• Firm linkage of SA activities to over all project milestones.</li> <li>• An initial concept QRA should be performed early in the design process.</li> </ul>
<b>Problematic RAMS Interfaces between client, main contractor &amp; sub-contractors</b>	<ul style="list-style-type: none"> <li>• Clear unambiguous SA Plans initially agreed with client and cascaded down to all sub-contractors.</li> <li>• Sub contractors required to develop their own SA Plans prior to works commencing, acceptance of which is a pre-requisite for commencement of works.</li> </ul>

**Table 4: Some Examples of Typical SA Problems and Proposed Solutions**

## **The Application of RAMS in Large Scale Complex Railway Projects RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

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 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, Systems 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 21<sup>st</sup> 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.

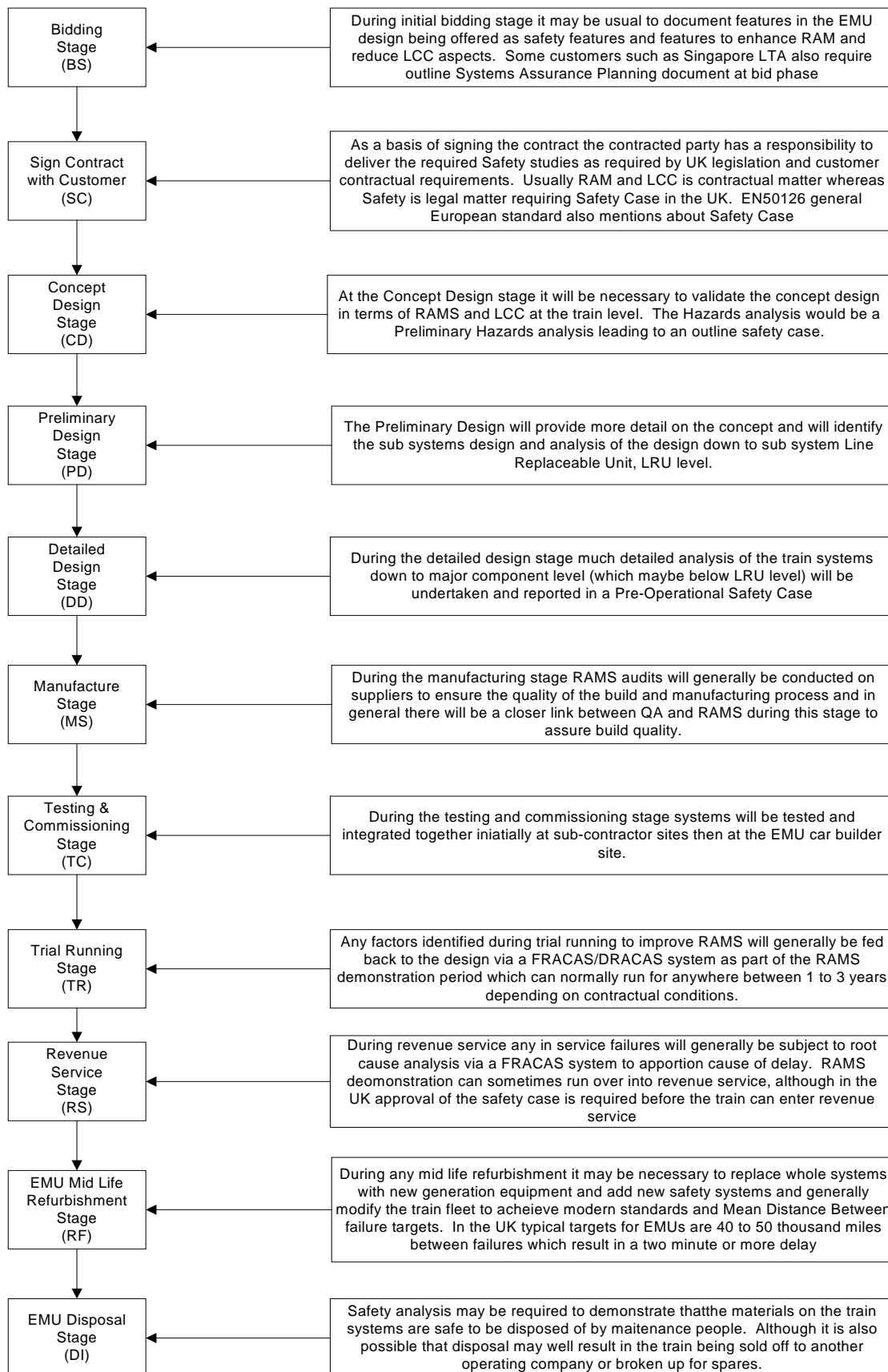
In summary, it is proposed that the Systems Assurance Manager must act as the conscience of the Project Manager to ensure that all reasonably practicable safety measures have been applied to the design and that overall foreseeable risks are controlled to a level, which can be considered tolerable.

#### **SECTION 4: EN50126 FLOWCHARTS FOR IMPLEMENTATION OF RAMS AT DIFFERENT PROJECT STAGES**

Some proposed flow charts for the implementation of Systems Assurance or RAMS at various stages of a typical railway project have been developed. The first flow chart identifies the various stages in a typical project this is adapted from EN50126. There is a subsequent flow chart for each project phase.

PMSC has also developed detailed excel spreadsheets which assess in more detail the RAMS tasks at each stage. In particular, the spreadsheets highlight the deliverables arising from the various RAMS tasks and the key interactions between RAMS tasks.

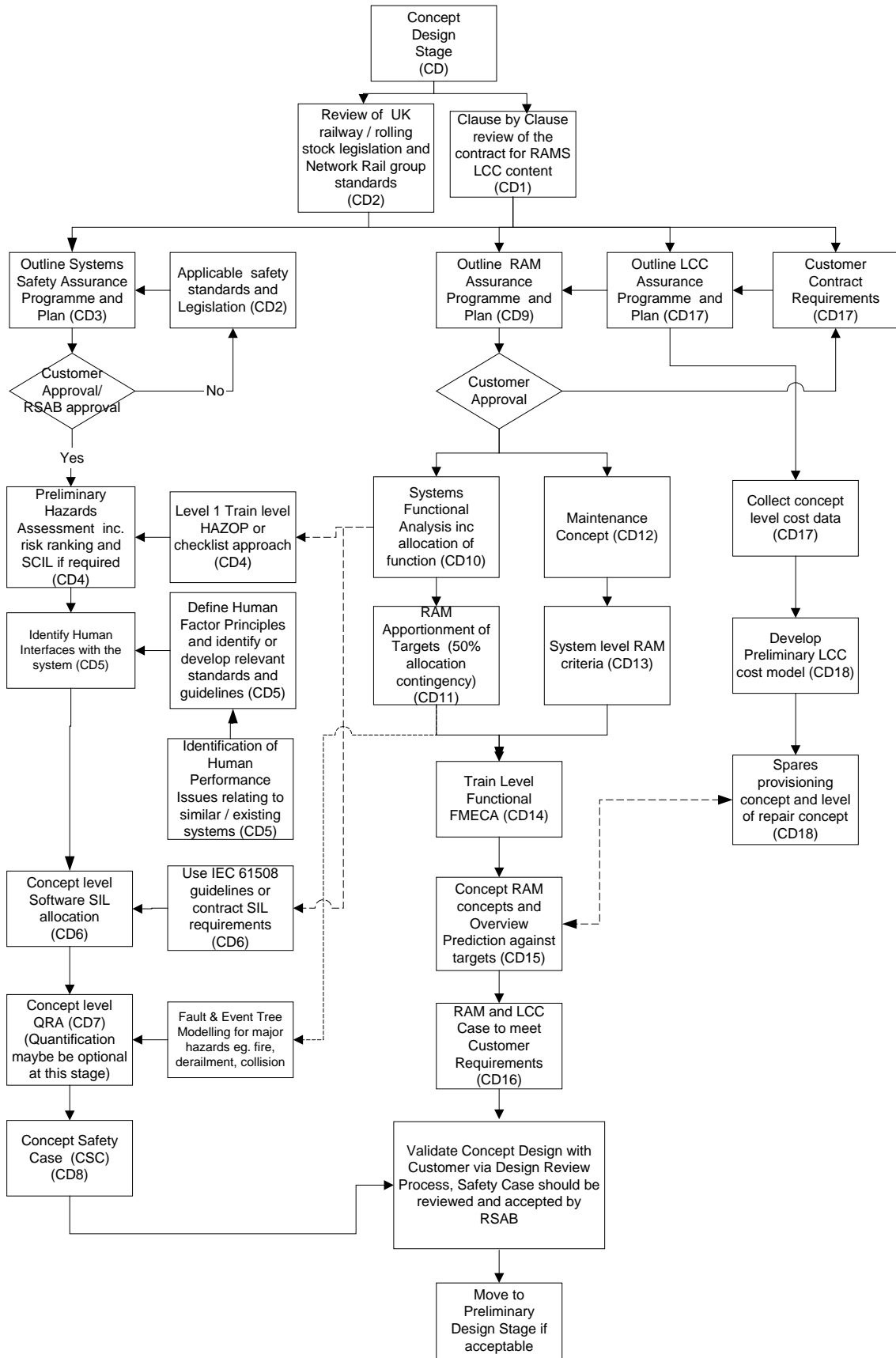
**The Application of RAMS in Large Scale Complex Railway Projects**  
**RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**



**Typical Project Phases for the Provision of a Fleet of EMUs**



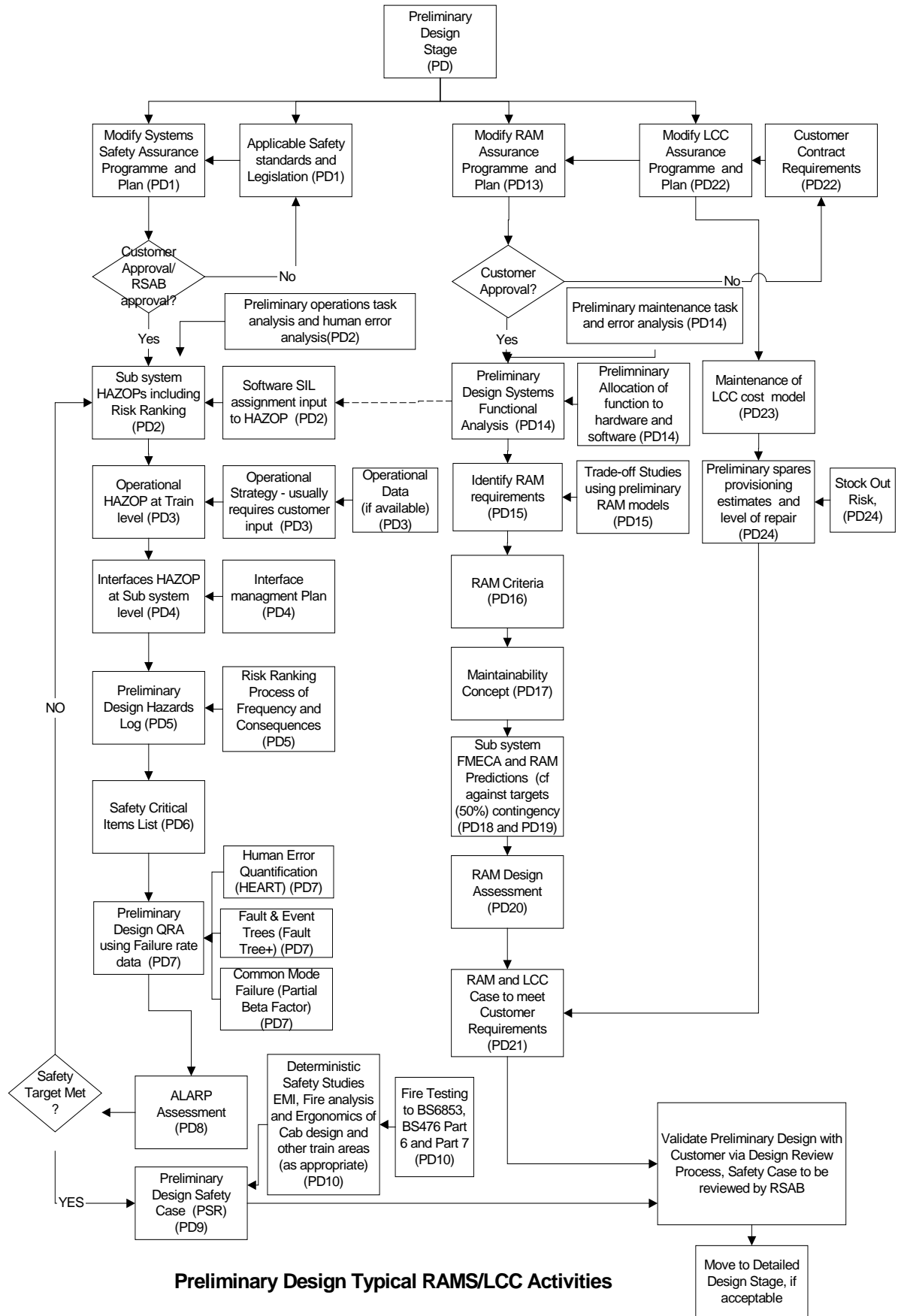
**The Application of RAMS in Large Scale Complex Railway Projects**  
**RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**



**Concept Design Typical RAMS/LCC Activities**



**The Application of RAMS in Large Scale Complex Railway Projects**  
**RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

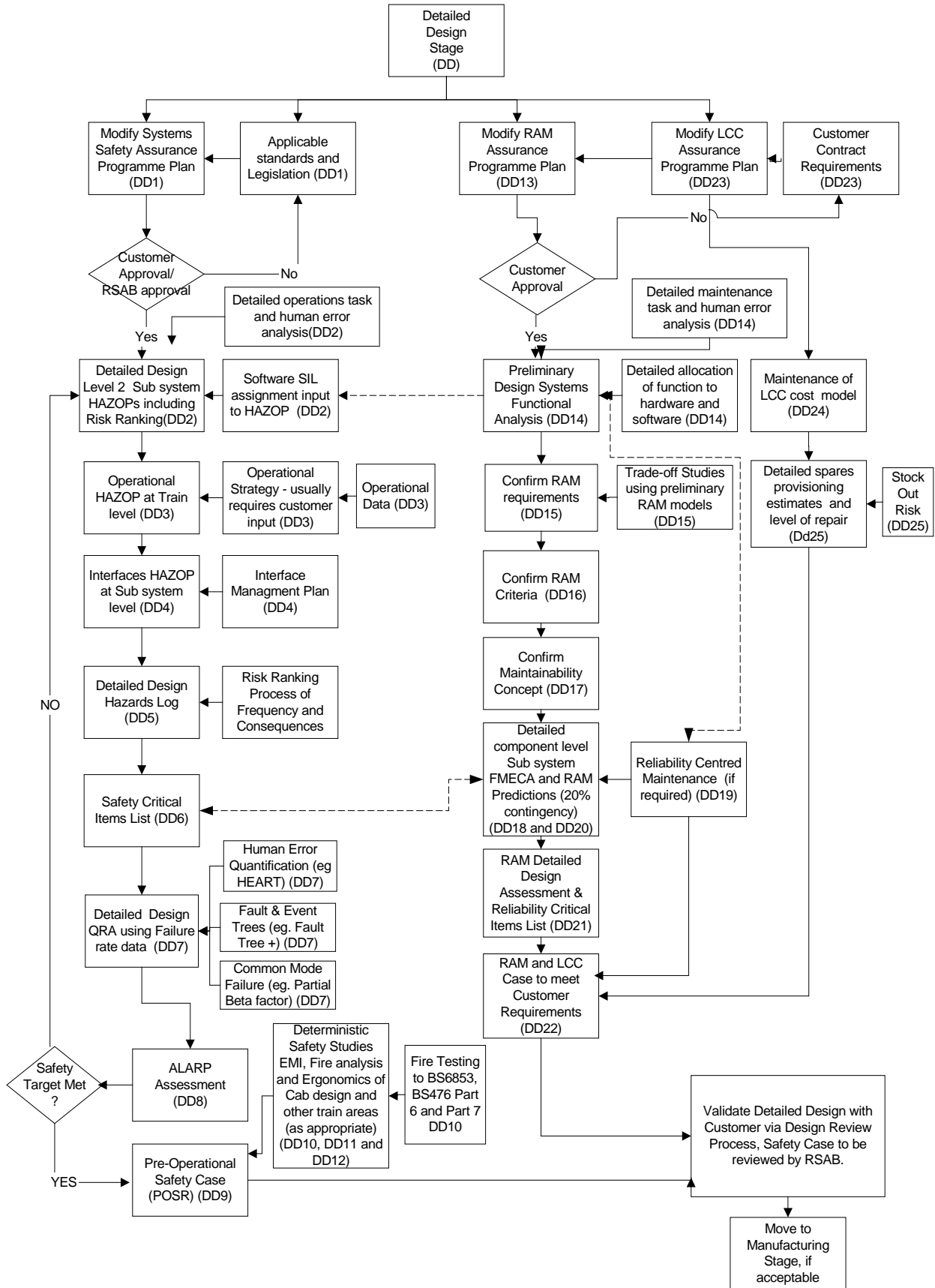


**Preliminary Design Typical RAMS/LCC Activities**





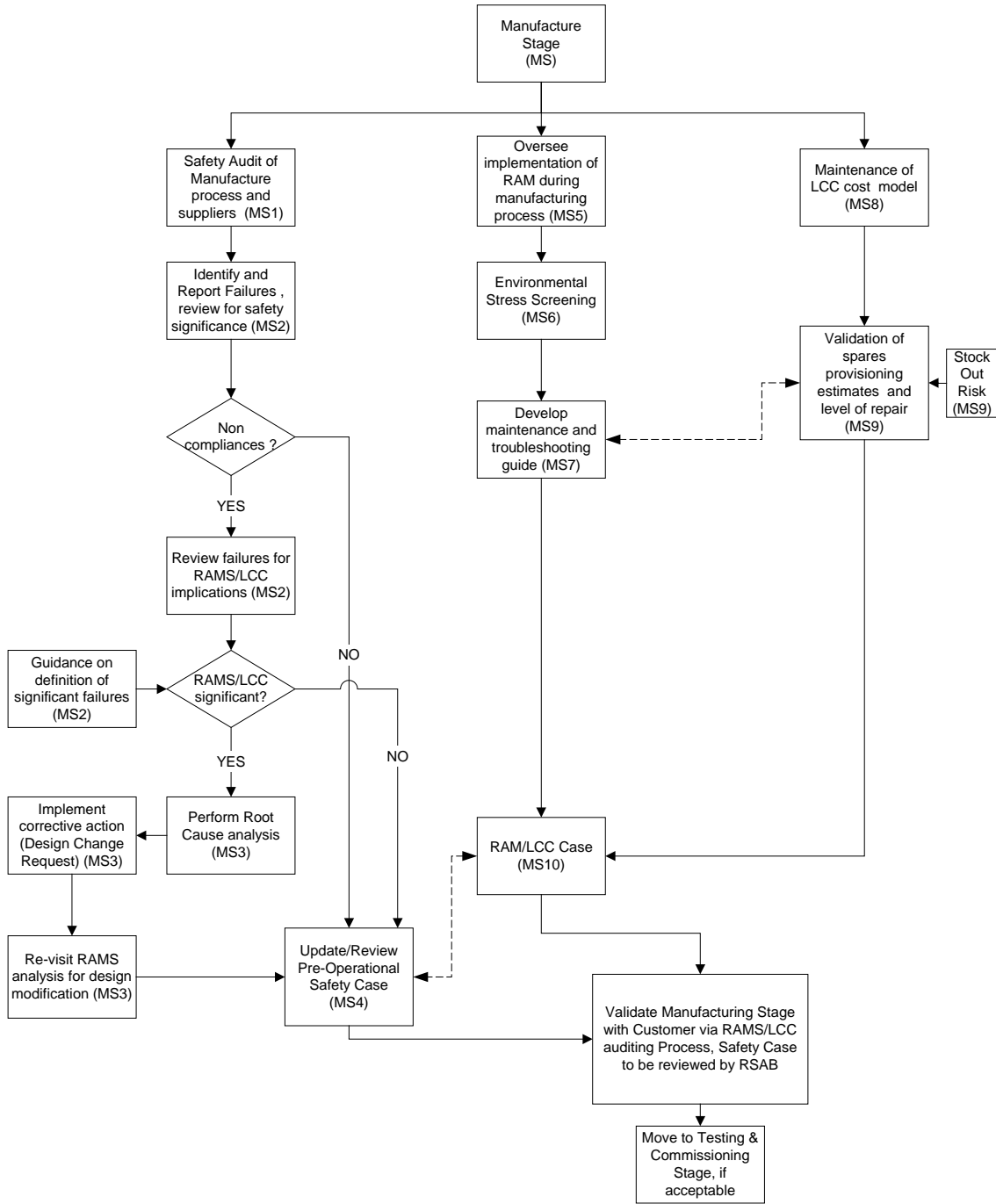
**The Application of RAMS in Large Scale Complex Railway Projects**  
**RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**



**Detailed Design Typical RAMS/LCC Activities**



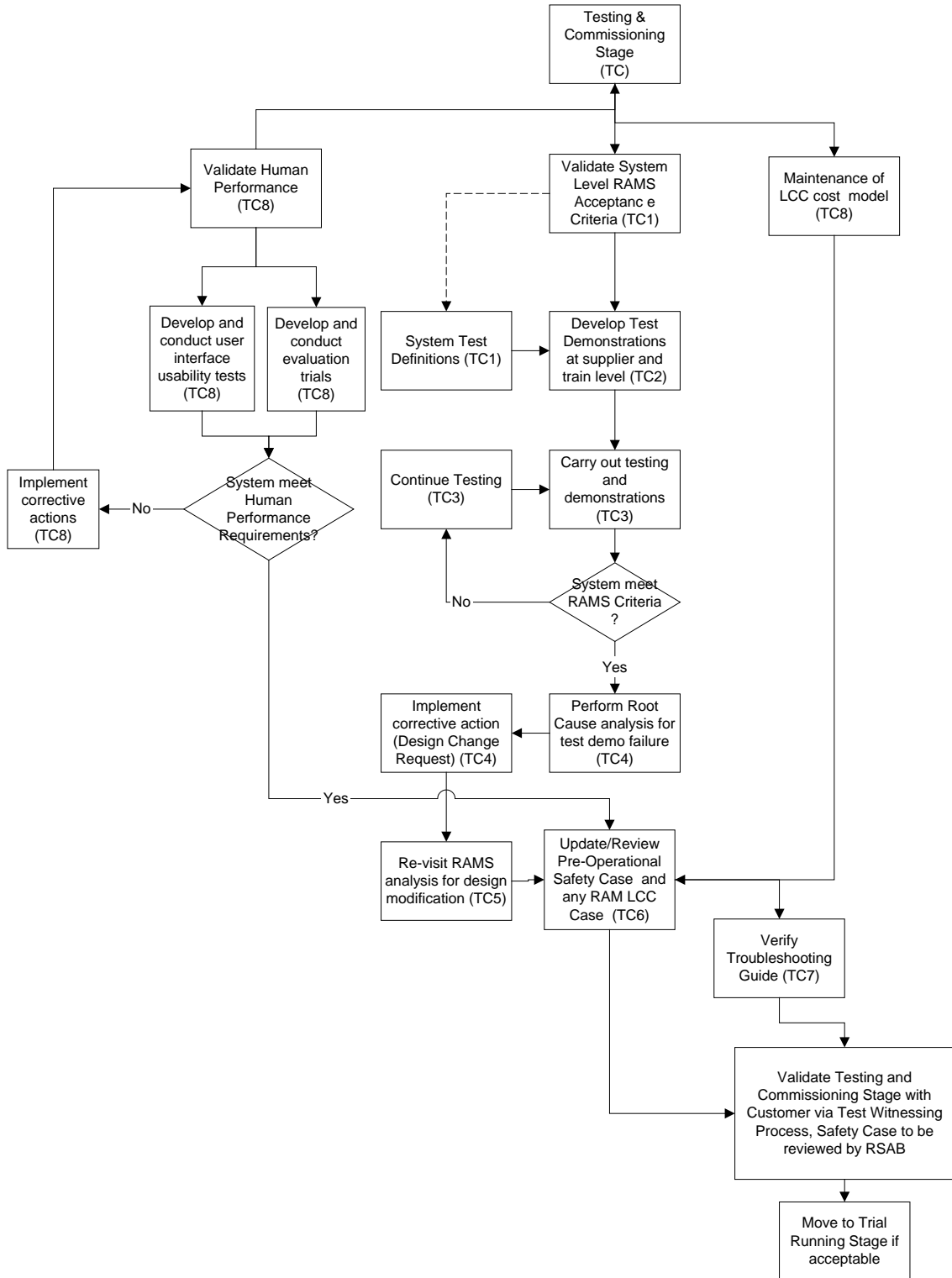
**The Application of RAMS in Large Scale Complex Railway Projects**  
**RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**



**Manufacturing Stage Typical RAMS/LCC Activities**



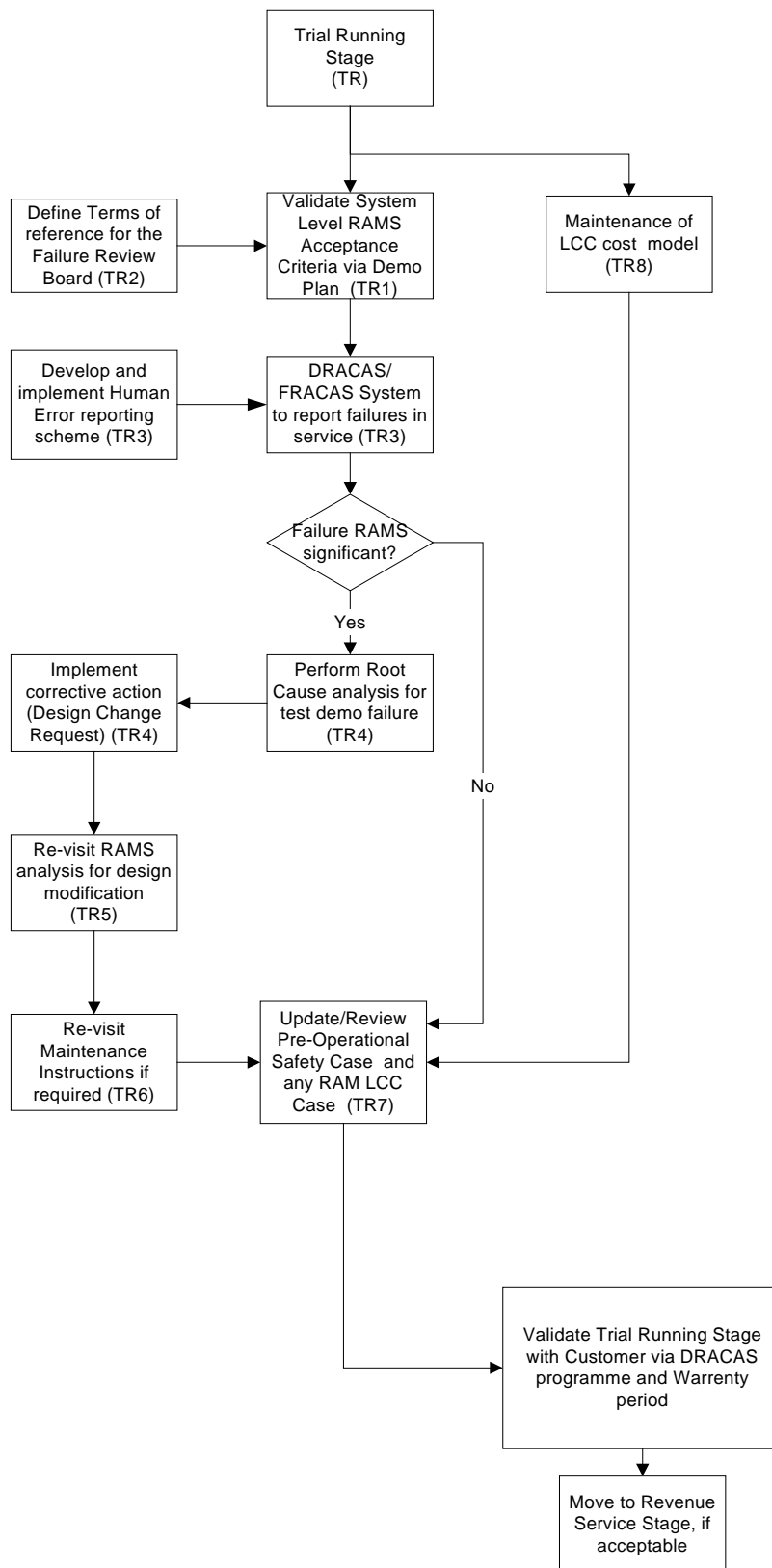
**The Application of RAMS in Large Scale Complex Railway Projects**  
**RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**



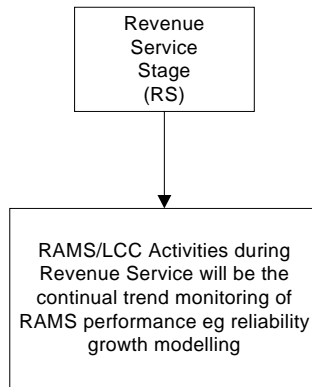
**Testing & Commissioning Stage Typical RAMS/LCC Activities**



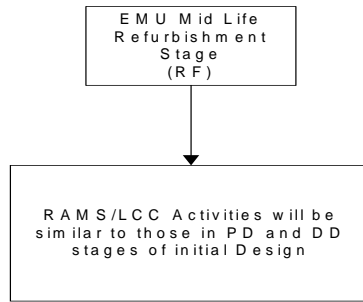
**The Application of RAMS in Large Scale Complex Railway Projects  
RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**



**The Application of RAMS in Large Scale Complex Railway Projects  
RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

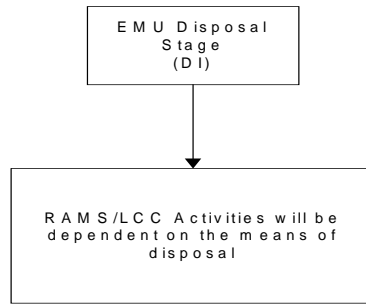


**The Application of RAMS in Large Scale Complex Railway Projects  
RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**



**Mid-Life Refurbishment Stage Typical RAMS/LCC Activities**

**The Application of RAMS in Large Scale Complex Railway Projects  
RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**



**Disposal Stage Typical RAMS/LCC Activities**

## **SECTION 5: SOME USEFUL NOTES ON SYSTEMS ASSURANCE METHODOLOGIES AND REFERENCES**

This section presents some useful notes and flow charts for the use of various Systems Assurance Methodologies:

### **A) DEVELOPMENT OF A SYSTEMS ASSURANCE PLAN, SAP**

At the commencement of a typical rail project It is proposed that a SAP be developed as a high level document presenting the programme of Systems Assurance work and how this meets the customer of regulator requirements. The SAP would provide a header document from which the more detailed Systems Safety Engineering Plans and the RAM Plans would be developed. The RAM plan would also detail the RAM requirements. The typical outline contents of the SAP are proposed as follows:-

<b>SECTION</b>	<b>TITLE</b>	<b>DESCRIPTION</b>
1.0	INTRODUCTION	Provides an overall introduction with purpose and scope and sets out the objectives of Systems Assurance Activities. It also identifies any guiding standards and references, which in this case will be those depicted in any customer specification or regulatory requirements.
2.0	PROJECT DESCRIPTION	Sets out the overall project descriptions and the technology involved.
3.0	ORGANSATION	Sets out the organisational roles and responsibility for RAMS and how this related to the main project team organisation.
4.0	SYSTEMS ASSURANCE ACTIVITIES	Sets out the high level assurance activities and how these will ensure that the ITT requirements and any requirements defined by guiding standards are to be met. Key review points and SA deliverables are also identified.
5.0	SYSTEMS ASSURANCE PROGRAMME	The key timing of the SA activities and deliverables are presented.
6.0	SYSTEMS ASSURANCE CRITERIA AND TARGETS	The SAP presents a discussion on the SA targets and criteria to demonstrate that they are understood and that the methods being adopted are fit for purpose in terms of judging whether the targets can be met.
7.0	CONTROL OF SUB CONTRACTORS	This element of the SAP documents how any subcontractors are to be controlled in terms of their input to SA activities.
8.0	REFERENCES	List of references quoted by the SAP
9.0	ACROYNMS	List of project Acronyms

### **Proposed Typical Contents of Systems Assurance Plan**



**B) SYSTEMS SAFETY ASSURANCE PLAN**

The detailed Systems Safety Engineering Plan will document the overall approach and methodologies to be adopted in the systems safety work both at systems level and at sub systems level. The typical outline contents of the SSEP are proposed as follows:

<b>SECTION</b>	<b>TITLE</b>	<b>DESCRIPTION</b>
1.0	INTRODUCTION	Provides an overall introduction with purpose and scope and sets out the objectives of Systems Safety Engineering Activities. It also identifies any guiding standards and references.
2.0	PROJECT DESCRIPTION	Sets out the overall project descriptions and the technology involved but provides more detail on the specific safety features being provided in the design.
3.0	ORGANSATION	Sets out the organisational roles and responsibility for Safety Engineering and how this related to the main project team organisation. A section on competency of safety resources would also normally be provided.
4.0	SYSTEMS SAFETY ENGINEERING ACTIVITIES	Sets out the detailed systems safety engineering activities and how these will ensure that the ITT requirements and any requirements defined by guiding standards are to be met. Key review points and Systems Safety Engineering deliverables are also identified. The key activities are envisaged as:-  HAZOP and Risk Ranking Safety Review Group Safety Design Reviews Safety Critical Items List Consideration of Software Safety (if any) FMECA Fault Tree Analysis (including Human Error and Common Cause Failure as appropriate) and encompassing the ALARP argument. And finally a Safety Summary Document to summarise why the infrastructure change will be safe.
5.0	SYSTEMS ASSURANCE PROGRAMME	The key timing of the Systems Safety Engineering activities and deliverables are presented.
6.0	SYSTEMS ASSURANCE CRITERIA AND TARGETS	The SSEP presents a discussion on the Safety related targets and criteria to demonstrate that they are understood in the context of the engineering solutions being proposed.
7.0	CONTROL OF SUB CONTRACTORS	This element of the SSEP documents how any subcontractors are to be controlled in terms of their input to the safety engineering process.
8.0	REFERENCES	List of references quoted by the SSEP
9.0	ACROYNMS	List of Acronyms
APPENDIX A	DETAILED METHODOLOGIES	This appendix will provide more detail on the actual detail methodology for conducting the analytical techniques such as Fault Tree

**The Application of RAMS in Large Scale Complex Railway Projects  
RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

SECTION	TITLE	DESCRIPTION
		analysis, Common Cause Failure analysis And the Human Factors analysis. It may also provide further detail on how the HAZOPs will be run in terms of the HAZOP keywords being proposed.

**Proposed Typical Contents of Systems Safety Engineering Plan**

**C) RELIABILITY, AVAILABILITY & MAINTAINABILITY ASSURANCE PLANS (RAMAP)**

The RAM Plan will document how the various RAM analyses will be conducted and what the RAM requirements are on the system design and the sub systems. The typical contents of the RAMAP are as follows:-

SECTION	TITLE	DESCRIPTION
1.0	INTRODUCTION	The section describes the purpose and scope of the plan providing appropriate references to the customer specification and applicable standards, for WCML the applicable RAM standard has been specified as EN50126. The background for the current issue of the plan will also be described.
2.0	PROJECT DESCRIPTION	Sets out the overall project descriptions and the technology involved and presents more detail on the specific design features which enhance Reliability, Availability and Maintainability and thus optimise the Life Cycle Costs of the infrastructure change.
3.0	ORGANSATION	Sets out the organisational roles and responsibility for RAM and how this is related to the main project team organisation. The Human Factors input will clearly need to be shown in relation to the other project organisational activities. It will be essential to demonstrate in the organisational roles and responsibility that there are mechanisms in place to be able to resolve any conflicts between RAM requirements and Safety Requirements in the context of providing a design, which meets the ITT requirements. This prevents over engineering of the system to meet specific requirements in isolation.
4.0	RAM ASSURANCE ACTIVITIES	Sets out the detailed RAM Assurance activities and how these will ensure that the ITT requirements and any requirements defined by guiding standards are to be met. Key review points and RAM deliverables are also identified. The key activities are envisaged as:-  List RAM Requirements System Functional analysis RAM Target apportionment if required FMECA from RAM perspective including reliability prediction for each failure mode and maintainability prediction for each failure mode.

**The Application of RAMS in Large Scale Complex Railway Projects  
RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

<b>SECTION</b>	<b>TITLE</b>	<b>DESCRIPTION</b>
		RAM Trade-off studies, these will require the development of Fault Tree analysis for the systems being assessed to be able to try out different configurations of system and thus trade off one configuration against another. RAM Case Document
5.0	RAM ASSURANCE PROGRAMME	The key timing of the RAM activities and deliverables are presented. The programme will also indicate any interaction between Safety Engineering related tasks and RAM related tasks the principal interaction expected to be within the FMECA activity.
6.0	RAM ASSURANCE CRITERIA AND TARGETS	The RAMAP presents a discussion on the RAM related targets and criteria to demonstrate that they are understood in the context of the engineering solutions being proposed.
7.0	CONTROL OF SUB CONTRACTORS	This element of the RAMAP documents how any subcontractors are to be controlled in terms of their input to the RAM engineering process.
8.0	REFERENCES	List of references quoted by the RAMAP
9.0	ACROYNMS	List of Acronyms

**Proposed Typical Contents of RAMAP**

## **SECTION 6: SOME NOTES ON FAULT AND EVENT TREE CONSTRUCTION AND ANALYSIS**

### **6.1 Event Trees**

Event trees diagrammatically illustrate a sequence of events modelling accident scenarios. An example event tree has been presented below (see Figure 6.1). The “nodes” along the top of the event tree represent questions with a YES or NO answer, the convention being the downward branch representing the “NO” answer and the horizontal branch, representing the “YES” answer. This can also be termed as failure or success, respectively.

Outcome 5 in figure 6.1 derived using the following Boolean expression

Outcome 5 Frequency = Union of the success terms for the event TOP with failure of system X and success of system Y and system OP. The Boolean expression for this is written as Outcome 5 = TOP . X' . Y . OP'

Please note that the dash next to the terms Y and OP indicates that these are success terms rather than failure terms. Success terms are referred to as PATH sets whilst failure terms are referred to as PATH sets. It should also be noted that sometimes instead of using dashes to represent PATH sets a small bar will be placed on top of the symbol to represent success.

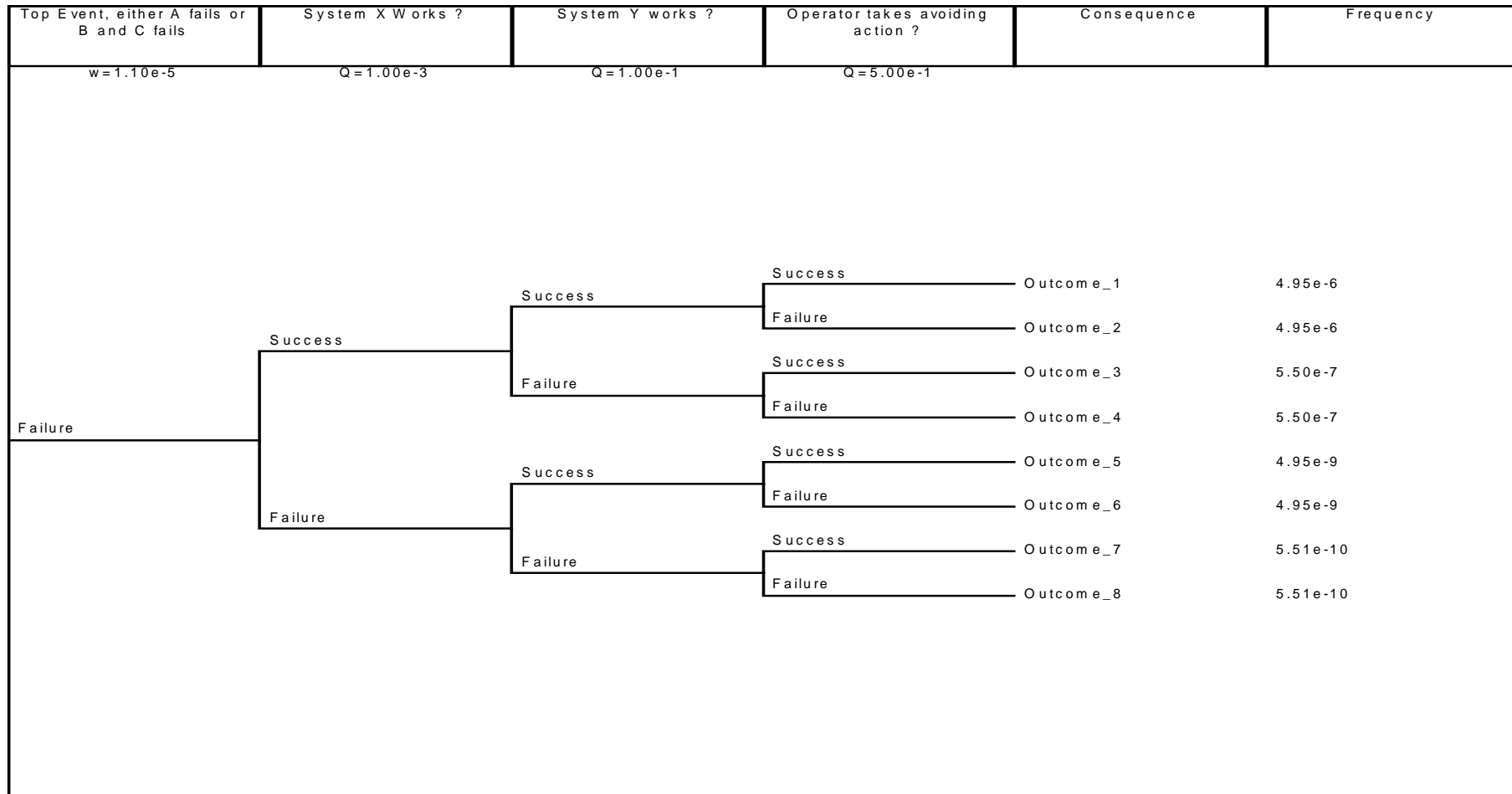
The Frequency of Outcome 5 is then derived as follows:-

Frequency of Outcome 5 in the event Tree = Frequency of TOP event multiplied by the Probability that event X fails multiplied by the probability that event Y is successful multiplied by the probability that event OP is successful this is shown mathematically below:-

Frequency of Outcome 5 = F (TOP) x P(x) x (1-P(Y)) x (1-P(OP))

It should be noted that the Event Trees are normally designed such that the success branch will produce the least consequences and the failure branch to produce the most consequences.

**The Application of RAMS in Large Scale Complex Railway Projects**  
**RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**



**Figure 6.1: Generic Event Tree Structure Illustrating the typical event tree format**

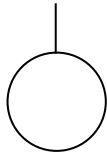
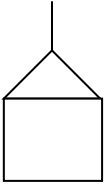
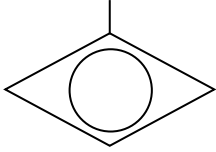
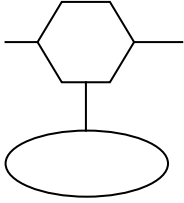
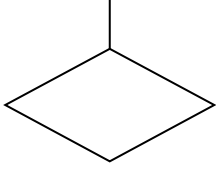
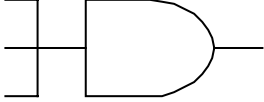


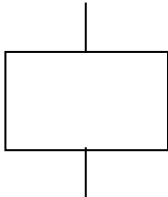
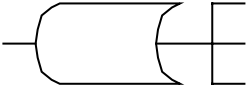
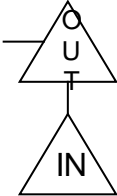
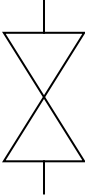
## **6.2 Fault Trees**

Fault trees are generally used when constructing a quantified risk assessment to quantify the hazards identified in the HAZOP and Hazards Log, to more accurately determine safety critical hazards and to assure that the (As Low As Reasonably Practicable, ALARP) principle has been satisfied in relation to the residual risk. The Fault Tree will generally identify equipment or software components that indicatively affect the hazards risk, thereby providing a tool for analysing the total effect of failure rates and Mean Time To Repair (MTTR) of components and their relationship to hazard consequences and in summary their effect on the top event.

The table 6.1 below presents an indication of the typical symbols and their meanings, to be used in fault trees presented in a typical risk assessments

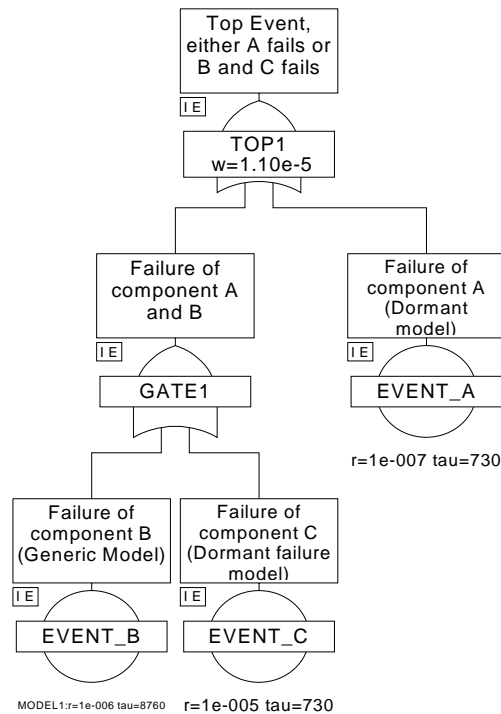
**The Application of RAMS in Large Scale Complex Railway Projects**  
**RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

	<p><b>Basic Event</b>  The circle describes a basic event that requires no further development.</p> <p>Frequency and mode of failure of items so identified are derived from empirical data. It should be noted that if failures are revealed the Fault Tree + RATE model will be utilised requiring the failure rate of the component and the repair rate. If failures are un-revealed then the Fault Tree + DORMANT model shall be adopted requiring the failure rate and the testing interval of the component. It should be further noted that each of the components modelled in the QRA will be given a coding name which represents their component type and failure mechanism, this will be agreed prior to the QRA development by the event nomenclature table.</p>		<p><b>Switch</b>  The house event is used as a switch to include or eliminate parts of the fault tree.</p> <p>Effectively True or False to those parts in the system. If a house event is AND'ed with a part of a tree it has the effect on including the other branch of the tree, if it is OR'ed then the other branch is effectively discounted or switched off.</p>
	<p><b>Basic Event</b>  Indicates a sub tree exists, but the sub tree was evaluated separately and the quantitative results inserted as a basic fault event</p>		<p><b>Inhibit Gate</b>  Describes a relationship between one fault and another. The input event directly produces the output event if the indicated condition is satisfied.</p>
	<p><b>Basic Event</b>  The diamond describes a fault event that is considered basic in a given fault tree. The possible causes of the event are not developed because the event is of insufficient consequence or the necessary information is unavailable. It is possible that such events might be included for information but not actually explicitly modeled as part of the numerical analysis.</p>		<p><b>AND Gate</b>  Describes the logical operation whereby the existence of all input events is required to produce the output event. If the inputs are event A and event B then the solution at the AND gate is the product of event A and event B i.e. Both must fail for the gate to be satisfied.</p>

 <p>Combination Event  The rectangle identifies an event that results from the combination of basic events through the input logic gates</p>	 <p>OR Gate  OR gates define the situation whereby the output event will exist if one or more of the input events exists. If the inputs are event A and event B then the solution at the OR gate is that either event A or event B can fail. Additionally, voting gates (which utilise the OR symbol) will be used to represent areas where failure of combinations such as one out of two or two out of three or three out of four failures can occur.</p>
 <p>Transferred Event  The triangles are used as transfer symbols. A line from the apex of the triangle indicates a transfer in, a line transfer out. Transfers in can be used to avoid unnecessary duplication of large sections of fault trees that might appear in several places – for example fault trees modelling failure of electrical supplies might be used in several places in the overall QRA model.</p>	 <p>NOT Gate  NOT gates define the situation whereby the logical state of an event is reversed. The use of NOT gates will be limited, but their existence needs to be highlighted for completeness.</p>

**Table 6.1 Typical List of Fault Tree Symbols**





**Figure 6.2 An Example Simplistic Fault Tree**

The above fault tree (figure 6.2) represents a simplistic tree where the failures, which satisfy the top event are either Component A fails or Component B and C fail. Hence, we say that the minimum Cut Sets are A and BC, i.e. there are 2 minimum Cut-sets one of a single order i.e. A and one of order two i.e. BC, this illustrates that a failure of A will directly lead to the top event, or that a failure of both B and C would lead to the top event.

## **SECTION 7: SOME NOTES ON HUMAN FACTORS**

This section describes the PMSC vision of how Human Factors can be applied to modern railway systems. However, we are pragmatic in our application of human factors as we realise that the Human Factors input needs to be considered in the context of the overall design application.

Human Factors/Ergonomics is the study to optimise the safety, efficiency and comfort of people in their working environments. The aim is to maximize the capabilities, and minimize the limitations of the people within the system.

Human Factors studies can be applied to any industry in which humans interact with equipment and with each other, and to all stages of system life cycle from design and implementation, commissioning to operation, maintenance and decommissioning. Human Factors not only applies to working environments, but also to the passenger environment in transportation systems.

A wide range of services are offered, including the following:

- Task Analysis
- Human Error Analysis
- Workplace and Workstation Design and Assessment
- Environmental Assessment
- Control and Instrumentation Design and Assessment
- Graphical User Interface Design
- Communications Analysis
- Training Needs Analysis and Training Program Development
- Procedures Design
- Workload Analysis and Manning Assessment
- Emergency Planning
- Safety Management and Organizational Studies
- Training (both general and specific) in the area of Human Factors
- Barrier Free Design

### **7.1 TASK ANALYSIS**

Task Analysis is the identification of the requirements of the job tasks, in order to match the demands of the system with the characteristics and capabilities of the operator. This type of study can be used in the assessment of the adequacy of existing designs, and can form the basis of new designs.

The following are a number of issues that task analysis can be used to address:

- Allocation of Functions between people and machines, and between people and other people
- Staffing and Job Organisation
- Interface Design
- Skills and Knowledge Acquisition
- Performance Verification

### **7.2 HUMAN ERROR ANALYSIS**

Human Error Analysis can be used to demonstrate the robustness of the system against inappropriate human performance. Potential errors, the causes, and potential consequences are defined for each task or task step. Existing systems can be assessed for the adequacy of error prevention, or error recovery mechanisms. For new designs, mechanisms for error prevention and recovery can be defined.

Having identified and qualitatively analysed potential human errors, it is possible to stop at that point and endeavour to reduce the possibility of occurrence. In certain circumstances, it is useful to quantify the likelihood of these errors in order to perform a cost benefit analysis i.e. if the likelihood of the error is high and the consequences are severe then it is beneficial to take remedial actions to alleviate the situation. Human Reliability Assessment methods are used to perform the quantification. The Human Reliability Assessment can be performed solely on the human interaction aspects of the system or it can be combined with equipment reliability as part of an overall safety assessment.

### **7.3 WORKPLACE AND WORKSTATION LAYOUT**

Human Factors guidelines, developed from human performance data and past experience within industry, can be used to assess the adequacy of either existing designs, or to propose new workplace designs. Anthropometric data (data which describes typical body dimensions) can be applied to ensure that appropriate access space is provided for both operations and maintenance activities within the work area, to ensure all equipment can be reached and manipulated as intended. Human Factors principles such as functional grouping, importance of equipment, sequence and frequency of use are applied to achieve optimum workstation designs.

### **7.4 ENVIRONMENTAL ASSESSMENT**

Environment, in this case, refers to the working environment and addresses the issues of lighting, noise and temperature. Data exists which specifies optimum lighting levels for specific types of tasks. Areas where there are potential noise sources can be identified and appropriate methods of noise prevention, reduction or protection will be recommended. Acceptable temperatures for different work areas are a function of the level of activity to be carried out in that area and the amount of clothing that will be worn. Data tables exist which allow the analyst to define the appropriate temperature level and then the means of achieving that level can be recommended.

### **7.5 CONTROL AND INSTRUMENTATION DESIGN**

Detailed control and instrumentation design and assessment can be performed by using the information obtained in the task analysis and by applying relevant Human Factors guidelines. The most appropriate type of display or control is selected according to its function, relating to the needs of the operator.

When the controls and displays are selected, the design details are specified or assessed for adequacy by using the Human Factors guidelines that address size, colour, labelling and direction of movement.

### **7.6 GRAPHICAL USER INTERFACE (GUI) DESIGN**

The tasks to be carried out using a computer control system are defined in consultation with the client/users. A task analysis of each task can then be completed to identify control and display requirements, in terms of information the user needs to perform the necessary actions, and the feedback which is required to indicate success or otherwise of these actions. Future system users have the opportunity to participate in the design process from start to finish to ensure that their requirements are met.

Any constraints and limitations in terms of the technology or the users requirements will be identified at this stage. If an assessment is being carried out of an existing system, or a new system is being installed to replace the existing system, the analyst will define the positive and negative attributes. Information is elicited from users/future users about the features they wish to retain and those that are problematic.

The following aspects are addressed using the information obtained from the task analysis and the application of ergonomics guidelines:

- display structure
- system navigation
- content
- layout of information on the screen
- the use of colour
- the use of symbols
- the presentation of data
- potential operator error and any other relevant aspects of design.

Sketches of the screen displays and a representation of the display structure are usually presented to the client as a first step in the process, so that they may be reviewed by the users in hard copy before being created on the computer screen. The completed designs undergo usability testing to ensure that the system meets user requirements in terms of comprehension of display content, suitability of layout, appropriateness of user interaction, efficiency and accuracy of navigability, and general usability for the tasks to be carried out. Recommendations resulting from these exercises are then incorporated into the design.

## **7.7 COMMUNICATIONS ANALYSIS**

The purpose of a communications analysis is to analyse the points in the task where communication is required with other personnel or groups of personnel, either within or external to the immediate work area. The analysis identifies when the communication is needed, the origin in terms of the person and their location, the destination in terms of the person and their location and the means of communication. Any relevant performance shaping factors are examined for their implications. The results of this assessment can feed into the operating procedures to ensure that all necessary communications are carried out in an efficient and timely fashion and can also feed into the design process to ensure that adequate means of communication are provided for safe operation.

## **7.8 PROCEDURES DESIGN**

The detailed task analysis can be used as an input to the procedural documentation, ensuring that the content is complete, thorough and relevant. Human Factors

guidelines also exist to assist the procedure writer in the format and presentation of the material to encourage optimum performance by the user. This applies not only to operating instructions in industrial settings but also to the design and development of any instructional material.

## **7.9 TRAINING NEEDS ANALYSIS**

Training Needs Analysis can be used either to develop a training program where one does not exist or to verify that the existing training program is adequate for the tasks to be performed. Task Analysis is used to identify the content of the training program in terms of the tasks that the operators will need to be trained to complete and how they are carried out. The skills, knowledge and abilities necessary to carry out the tasks can then be defined.

From the above information a training program can be developed to suit the needs of the organisation. Decisions can be made as to the best training methods e.g. tasks that are best suited to classroom training, and those which can only be taught successfully through on-the-job training, and appropriate presentation methods will be recommended. Once the training course is developed, it should be tested for its effectiveness, and the feedback incorporated into the design of the training program.

## **7.10 HUMAN FACTORS TRAINING COURSES**

Training courses can be provided that will introduce Human Factors in a general sense to increase worker, designer or manager awareness of the importance of these considerations. In addition, specific courses, relating to certain areas within the study of Human Factors, can be administered to encourage the use of Human Factors techniques within an organization or project. The training courses will be modified to suit the needs of the specific client.

## **7.11 EMERGENCY PLANNING**

Human Factors guidelines exist for the specification of the width of walkways and the design of stairways and signs to provide the optimum design of escape route for evacuation. More recently however, studies of human behaviour in threatening situations have provided valuable information for the design of evacuation systems. This information impacts upon the location of the escape route, the roles and responsibilities of those within the command structure, the design of information systems and the emergency procedures themselves. Identification of the relevant behavioural phenomena and their impact upon evacuation success will allow the Human Factors Analyst to assist in the development of effective evacuation systems and the development of emergency plans and training.

## **7.12 WORKLOAD ANALYSIS AND MANNING ASSESSMENT**

Once more the task analysis can be used as the basis for this technique. The objective of this analysis is to decide upon the appropriate manning levels (or to assess the existing workload of the staff) and to iron out the peaks and troughs. This may be completed in one or more of several ways:

- reallocating the tasks between workers
- reallocating the tasks to different times of the day
- adjusting staffing levels

- automating parts of the process
- making other design changes.

### **7.13 BARRIER FREE DESIGN OR DESIGN FOR THE DISABLED**

Attempts are being made to provide a safe, comfortable and accessible work place for members of the population who have a disability or are seniors, particularly as the population in general is aging and there are increasing numbers of disabled and seniors within the workforce. Barrier free design has expanded beyond the consideration of the work environment to include passenger and leisure environments. Standards and guidelines are applied to design and assessment situations to ensure acceptability, and cover such issues as:

- physical access
- reach distances
- slope/ramp and handrail design
- washroom design
- width of passageways
- width and operation of doorways
- table and chair/bench design
- information design
- control design (e.g. door handle design, soap dispenser design etc.)
- colour coding, and other relevant issues depending upon the design context.

## **SECTION 8: SOME NOTES ON THE USE OF THE HEART METHOD**

The Human Error and Reduction Technique was developed by Jerry Williams in the 1980's to help assessors develop a systematic framework to derive human error rates for application in probabilistic analysis. This section presents some useful notes to assist in its application.

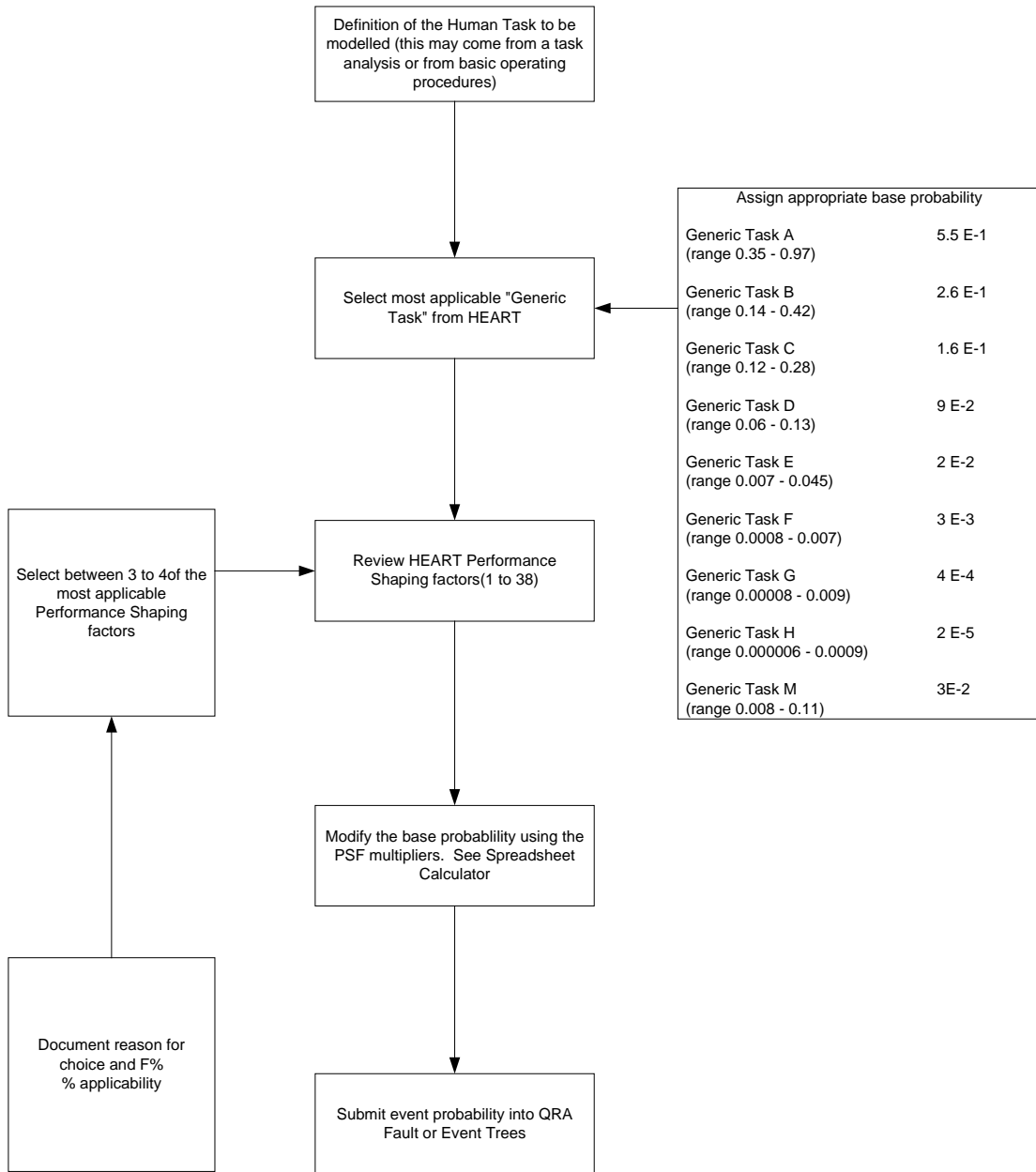
At PMSC we are regularly asked to incorporate human errors into an overall systems analysis. In order to quantify any human errors we have used the Human Error and Reduction Technique, HEART.

The formal reference for this methodology is as follows:-

A Data-Based Method for Assessing and Reducing Human Error to Improve Operational Performance, J.C. Williams, June 1988 This part of appendix A presents the detailed tables necessary for the application of the HEART methodology.

Figure 7.1 presents a flow chart for the HEART process and Tables 7.1 and 7.2 present the List of Generic Task Types and Performance Shaping factor multipliers for each Error Producing Condition.

**The Application of RAMS in Large Scale Complex Railway Projects  
RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**





**The Application of RAMS in Large Scale Complex Railway Projects**  
**RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

Letter	GENERIC TASK	Proposed Nominal Human Unreliability 5 <sup>th</sup> – 95 <sup>th</sup> Percentile Bounds
A	Totally unfamiliar, performed at speed with no real idea of likely consequences.	0.55 (0.35-0.97)
B	Shift or restore system to a new or original state on a single attempt without supervision or procedures	0.26 (0.14-0.42)
C	Complex task requiring high level of comprehension and skill.	0.16 (0.12-0.28)
D	Fairly simple task performed rapidly or given scant Attention	0.09 (0.06-0.13)
E	Routine, highly—practiced, rapid task involving relatively low level of skill	0.02 (0.007-0.045)
F	Restore or shift a system to original or new state following procedures, with some checking	0.003 (0.0008-0.007)
G	Completely familiar, well— designed, highly practised, routine task occurring several times per hour, performed to highest possible standards by highly—motivated, highly— trained and experienced person, totally aware of implications of failure, with time to correct potential error, but without the benefit of significant job aids	0.0004 (0.00008-0.009)
H	Respond correctly to system command even when there is an augmented or automated supervisory system providing accurate interpretation of system state	0.00002 (0.000006-0.0009)
M	Miscellaneous task for which no description can be found (Nominal 5th to 95th percentile data spreads were chosen on the basis of experience available suggesting log normality	0.03 (0.008-0.11)

**Table 8.1: List of HEART Generic Task Types**

<u>Number</u>	<u>Error—producing Condition</u>	Maximum predicted nominal amount by which unreliability might change going from 'good' <u>conditions to 'bad'</u>
1	Unfamiliarity with a situation which is potentially important but which only occurs infrequently or which is novel	x 17
2	A shortage of time available for error detection and correction	x 11
3	A low signal—noise ratio	x 10
4	A means of suppressing or over—riding information or features which is too easily accessible	x 9
5	No means of conveying spatial and functional information to operators in a form which they can	x 8



**The Application of RAMS in Large Scale Complex Railway Projects**  
**RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

<u>Number</u>	<u>Error—producing Condition</u>	Maximum predicted nominal amount by which unreliability might change going from 'good' conditions to 'bad'
	readily assimilate	
6	A mismatch between an operator's model of the world and that imagined by a designer	x 8
7	No obvious means of reversing an unintended action	x 8
8	A channel capacity overload, particularly one caused by simultaneous presentation of non—redundant information	x 6
9	A need to unlearn a technique and apply one which requires the application of an opposing philosophy.	x 6
10	The need to transfer specific knowledge from task to task without loss	x 5.5
11	Ambiguity in the required performance standards	x 5
12	A mismatch between perceived and real risk	x 4
13	Poor, ambiguous or ill— matched system feedback	x 4
14	No clear direct and timely confirmation of an intended action from the portion of the system over which control is to be exerted	x 4
15	Operator inexperience (e.g. a newly—qualified tradesman, but not an "expert")	x 3
16	An impoverished quality of information conveyed by procedures and person/person interaction	x 3
17	Little or no independent checking or testing of output	x 3
18	A conflict between immediate and long—term objectives	x 2.5
19	No diversity of information input for veracity checks	x 2.5
20	A mismatch between the educational achievement level of an individual and the requirements of the task	x 2
21	An incentive to use other more dangerous procedures	x 2
22	Little opportunity to exercise mind and body outside the immediate confines of a job	x 1.8
23	Unreliable instrumentation (enough that it is noticed)	x 1.6
24	A need for absolute judgements which are beyond the capabilities or experience of an operator	x 1.6
25	Unclear allocation of function and responsibility	x 1.6
26	No obvious way to keep track of progress during an activity	x 1.4
27	A danger that finite physical capabilities will be exceeded	x 1.4
28	Little or no intrinsic meaning in a task	x 1.4
29	High—level emotional stress	x 1.3
30	Evidence of ill—health amongst operatives, especially fever	x 1.2
31	Low workforce morale	x 1.2

**The Application of RAMS in Large Scale Complex Railway Projects**  
**RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

<u>Number</u>	<u>Error—producing Condition</u>	Maximum predicted nominal amount by which unreliability might change going from 'good' conditions to 'bad'
32	Inconsistency of meaning of displays and procedures	x 1.2
33	A poor or hostile environment (below 75% of health or life— threatening severity)	x 1.15
34	Prolonged inactivity or highly repetitious cycling of low mental workload tasks	x 1.1 (for first half hour) x 1.05 (for each hour thereafter)
35	Disruption of normal work— sleep cycles	x 1.1
36	Task pacing caused by the intervention of others	x 1.06
37	Additional team members over and above those necessary to perform task normally and satisfactorily	x 1.03 (per additional man)
38	Age of personnel performing perceptual tasks	x 1.02

**Table 8.2: List of Error Producing Conditions and Their Probability Multipliers**

<u>Number</u>	<u>Error-Producing Condition</u>	<u>Remedial Method</u>
1	Unfamiliarity (x 17)	Train operators to be aware of infrequently— occurring conditions, simulate such situations, and teach an understanding of the consequences
2	Time Shortage (x 11)	Management must be aware that shortage of time is likely to impair the reliability of decisions, both their own and their staff's — and try to ensure that sensitive decisions are not taken against the clock.
3	Low S/N Ratio (x 10) (when really poor)	Strenuous efforts must be made to ensure that such ratios do not fall to unreasonably low levels
4	Features Over-ride Allowed (x 9)	If the consequence of placing a system in an inappropriate state is potentially damaging, suitable inter—locking and inhibition must be provided, together with any suitable time—outs to return features to their appropriate quiescent state
5	Spatial and Functional Incompatibility (x 8)	Such incompatibilities should not occur — sufficient is now known about human engineering for population stereotypes that the problem need not arise to any extent — where doubt exists advice should be obtained from trained Ergonomists, who will either know exactly how to arrange a design for spatial or functional compatibility, or how to run an appropriate experiment to find out what is required
6	Model Mismatch (x 8)	Designers of systems and equipment aren't always right — operators sometimes not only often have better ideas but possess views about how a system should

**The Application of RAMS in Large Scale Complex Railway Projects**  
**RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

<u>Number</u>	<u>Error-Producing Condition</u>	<u>Remedial Method</u>
		function which are contrary to those of system designers — under pressure, particularly, operators will revert to their own perceptions of how a system should function, often with undesirable consequences — to protect against such mismatches systems designers must try to find out what their users' expectations are, and then design these characteristics into the system, omitting their own prejudices, as they do so
7	Irreversibility (x 8)	Obvious means should be provided to ensure that errors can be reversed easily, for preference by means of reversing the actions which created the error in the first place.
8	Channel Overload (x 6)	It should never be necessary to monitor more than one information channel at any one time — single events should not occur at more than three per second.
9	Technique Unlearning (x.6)	The greatest possible care should be exercised when new techniques are being considered to achieve the same outcome — they should not involve adoption of opposing philosophies.
10	Knowledge Transfer (x 5.5)	Reliance should not be placed on operators' transferring their previous knowledge without loss of precision and meaning — if such perfect transfer is required suitable job aids must be made available for reference.
11	Performance Ambiguity (x 5)	The required performance standards must be tested for comprehensibility on the user population to ensure that there is no ambiguity.
12	Misperception of Risk (x 4)	It must not be assumed that a user's perception of risk is the same as the actual level — if necessary a check should be made to ascertain where any mismatch might exist and what its extent is.
13	Poor Feedback (x 4)	A task analysis will show the points at which feedback must be available to operators — Ergonomists can advise on the best form of feedback if doubts should arise — what one is looking for is complete system transparency
14	Delayed/Incomplete Feedback (x 4)	System response times should never exceed four seconds and there must always be sufficient information to enable operators to step confidently on to the next part of a task — if doubt exists the feedback is incomplete.
15	Inexperience (x 3)	Personnel criteria should contain specified experience parameters thought relevant to the task — chances must not be taken for the sake of expediency.
16	Impoverished Information (x 3)	Procedures should be human— engineered and tested for operability — it should be assumed when personnel are required to communicate with each

**The Application of RAMS in Large Scale Complex Railway Projects**  
**RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

<u>Number</u>	<u>Error-Producing Condition</u>	<u>Remedial Method</u>
		other that very considerable information loss will occur — procedures must not rely on accurate verbal transmission of information for success.
17	Inadequate Checking (x 3)	When high reliability is paramount, independent checks on accuracy should be made, by people and systems that do not have any vested interest in the success or failure of an individual —blame should not attach to any inadequacies found at this level
18	Objectives Conflict (x 2.5)	Objectives should be tested by management for mutual compatibility, and where potential conflicts are identified these should either be resolved to make them harmonious or made prominent so that a comprehensive management control programme can be created to reconcile such conflicts as they arise, in a rational fashion.
19	No Diversity (x 2.5)	It should not be assumed that operators will rely totally on a single information source for confirmation of accuracy, and enquiries should be made to ascertain what additional sources are referred to, so that these are not denied operators, and, if possible, are enhanced.
20	Educational Mismatch (x 2)	The job profile should identify any potential mismatch of recruits against requirements — educational standards should be made explicit; there should be no ambiguity
21	Dangerous Incentives (x 2)	It is intuitively obvious that people work for rewards of various natures — if the reward for doing something quickly is greater than the reward for doing it accurately, or the reward for omitting an action is greater than the reward for performing it we should not be surprised if that is, in the main, what happens — the reward system must be evaluated carefully, therefore, to ensure that the desired behaviour is emitted, rather than that which might be construed as being appropriate simply because facets of the task are seen to conform to a partial criterion — if in doubt, seek advice from Management Scientists and/or Psychologists
22	Lack of Exercise (x 1.8)	Frequent rest breaks should be designed into the job, and the system made tolerant to personnel taking breaks as the need arises — tuition should be given in techniques for maintaining high levels of arousal, such as postural change, personal ventilation and recognition of fatigue symptoms — encouragement should be given to engage in appropriate mild forms of physical exercise and relaxation and stress control —On—the—job refresher training should be given and frequent exercises to maintain and enhance levels of competence and awareness of technical progress innovation given.

**The Application of RAMS in Large Scale Complex Railway Projects  
RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

<u>Number</u>	<u>Error-Producing Condition</u>	<u>Remedial Method</u>
23	Unreliable Instruments (x 1.6)	Regrettably it is a fact that when instrumentation is found to be unreliable operators will cease to trust its indications to the extent of ignoring valid information and preferring to believe their own interpretations, despite overwhelming evidence to the contrary — if instrumentation is thought likely to be unreliable it should be withdrawn from service, and more reliable instrumentation substituted — no doubts should exist about its suitability.
24	Absolute Judgements Required (x 1.6)	Operators must not be placed in the position of having to make judgements about the meaning of data which are outside their span of apprehension or experience — a task analysis will reveal when such conditions are likely to arise, and management must plan for such contingencies, by recognising the circumstances and taking full responsibility for actions which might be taken on their behalf — “brain-storming” and problem—solving workshops are helpful to identify some of the most bizarre situations in which staff and management can find themselves — it is likely that discussion of these ‘grey areas’ of organisational behaviour will reinforce mutual respect, and anticipate future conflict and/or issues of culpability at a time of zero threat.
25	Unclear Allocation of Function (x 1.6)	As with the area above, doubt must not exist about responsibilities — whilst they can, and should, be stated on paper, joint preparation of a functional specification will remove doubts and anxieties, and lead to the development of healthy attitudes towards the system design concepts—Organisational Development Specialists and/or Behavioural Scientists should be involved in facilitating the preparation of a satisfactory working protocol.
26	Progress Tracking Lack (x 1.4)	Various job aids must be supplied in order to ensure that operators do not get out of step with the task in hand — these can range from checklists through mimics to electronic monitoring of progress against targets —if such aids are introduced they must be piloted to ensure that they are compatible with user needs and that there is an incentive to use them —Ergonomists can advise on these job design aspects
27	Physical Capabilities (x 1.4)	It should be self-evident that tasks must not exceed the operators’ capabilities —Reference to Human Factors Standards will ensure that these capabilities are not exceeded.
28	Low Meaning (x 1.4)	Meaning can be built into a job by preparing job descriptions with the staff concerned, showing them the significance of their contribution to corporate

**The Application of RAMS in Large Scale Complex Railway Projects  
RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

<u>Number</u>	<u>Error-Producing Condition</u>	<u>Remedial Method</u>
		objectives, designing variety into their duties by arranging for job features such as task rotation to enhance system awareness, and holding periodic reviews of working practices to ensure that symptoms of alienation are not manifesting themselves — Behavioural Scientists can advise on suitable precautions.
29	Emotional Stress (x 1.3)	Management and medical staff must be vigilant to recognise the onset of emotional problems which can manifest themselves via symptoms such as excessive absence, persistent lateness, obsessive behaviour, lack of cooperation and exceptional fatigue — personal stress control training programmes could be considered, and potentially stressful decision—making circumstances identified so that the conditions can be modified to limit occurrence of extreme generalised stress.
30	Ill-health (x 1.2)	Until it is pointed out, it is not apparent that ill—health can have such deleterious effects on performance — often the effects of, say, a cold or 'flu do not manifest themselves until well into a shift — by now it should be obvious that operators and managers who are ill should not attempt to undertake work requiring reliability, and out of respect for others, for integrity and peace of they should stay away, recovered — a medical awareness programme would be helpful.
31	Low Morale (x 1.2)	Apart from the more obvious ways of attempting to secure high morale by way of financial reward, for example, other methods involving participation, trust and mutual respect, often hold out at least as much promise — Building up morale is a painstaking process, which involves a little luck and great sensitivity — employees must be given reason to believe in their employer and themselves — this can be accomplished by a battery of activities, such as joint preparation of work plans and objectives, maximal delegation of authority, reward for effort and results, provision of subsidised fringe benefits, firmness of resolve and openness — it is not achieved to any great extent by appeals to workforces to stick by management — the respect necessary to make morale rise is earned not enforced — a sensitive, caring management, would be unlikely to encounter such problems
32	Inconsistency Displays (x 1.2)	Even if the conventions adopted for display layout and procedure design are not human—engineered for ease of use, they must be consistent within themselves e.g. if a display is showing an increasing

**The Application of RAMS in Large Scale Complex Railway Projects**  
**RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

<u>Number</u>	<u>Error-Producing Condition</u>	<u>Remedial Method</u>
		value even though in an analogue sense the portion shown is decreasing, this convention must be adhered to throughout — Even though such a principle is wrong” (for preference such an approach would not be encouraged, of course)
33	Poor Environment (x 1.15)	It should be self—evident that a poor environment is likely to impair performance — by and large this should not occur nowadays with the introduction of legislation to control environments —to minimise any deleterious effects Work Physiologists, Ergonomists and/or Architects should be consulted for details of appropriate parameters.
34	Low Loading (x 1.1) 1 <sup>st</sup> ½ hour (x 1.05) each hour thereafter	Prolonged inactivity or highly repetitious cycling of low mental workload tasks must be avoided — generally when signal frequency falls below two per minute or involves little or no variability, vigilance performance will degrade — to combat such effects the introduction of artificial signals has been found to be helpful, and job enrichment (with the introduction of different, more varied tasks) has been found to minimise boredom, and better hold attention — Rather than combat these effects, it is better to ensure that such conditions do not arise in the first place i.e. observation tasks demanding high human reliability should never require sessions of longer than one hour’s concentration and tasks involving very low signal frequency should not be designed — if possible such tasks should be automated.
35	Sleep Cycle Disruption (x 1.1)	Only extreme sleep deprivation will cause performance degradation — our major interest, therefore, is in keeping small amounts of deprivation to a minimum —this can be achieved by keeping operators on a “stable” shift system such that there are no radical changes to either the pattern or the time of day over which such changes occur — the frequency with which changeovers occur should be as low as can reasonably be achieved — advice should be sought from Work Physiologists.
36	Task Pacing (x 1.06)	Although all work ultimately involves some element of pacing, the unwitting or deliberate introduction of pacing will lead to a slight reduction in reliability —this can be avoided by checking work systems to ensure that there is sufficient ‘buffering’ such that operators are not subject to undue pressure and can work at their own preferred pace — the one which best matches their capability.
37	Supernumeraries (x 1.03)	Where possible, limit gatherings of staff at workplaces to those necessary to perform tasks satisfactorily.



The Application of RAMS in Large Scale Complex Railway Projects  
RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004

<u>Number</u>	<u>Error-Producing Condition</u>	<u>Remedial Method</u>
38	Age (x 1.02)	Monitor perceptual capabilities of personnel required to perform task demanding high acuity and accurate information processing.

**Table 8.3 List of Possible remedial Methods for Error Producing Conditions**

**The Application of RAMS in Large Scale Complex Railway Projects**  
**RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

The first stage of the HEART process is to identify with the systems the possible sources of human error.

Once identified on the human error probability can be modified by the factors representing the various performance shaping factors using the Table

The second stage is to calculate the assessed affect of human error to the system, illustrated in the example below.

Step 1: Identify the Generic Task in the system for the operator (A-M in table 7.1)

F = 0.003 (operators work in shift formations, some validation)

Identify Error-Producing Conditions (EPC) from table 7.2 and obtain engineers assessment of its contribution effect, to calculate Assessed affect.

Step 2: Conduct assessment

Factor	Total HEART affect (Table 7.11.4)	Engineers Assessed proportion to affect	Assessed affect
Inexperience [15]	x 3	0.4	(3-1) x 0.4 + 1 = 1.8
Opposite technique [9]	x 6	1.0	(6-1) x 1.0 + 1 = 6.0
Risk Misperception [12]	x 4	0.8	(4-1) x 0.8 + 1 = 3.4
Conflict of Objectives [18]	X 2.5	0.8	(2.5-1) x 0.8 + 1 = 2.2
Low Morale [31]	x 1.2	0.6	(1.2-1) x 0.6 + 1 = 1.12

*Assessed nominal likelihood of failure*

Generic Task x Assessed Factor<sub>1</sub>...x Assessed Factor<sub>n</sub> = Assessed Nominal Likelihood of Failure

$$0.003 \times 1.8 \times 6.0 \times 3.4 \times 2.2 \times 1.12 = \underline{0.27}$$

It should be noted that probability of failure could never exceed 1.0, if by multiplication it does the failure is assumed to be 1.0.

$$\text{Modified Probability} = \text{Base} \times \prod_{i=0}^N F_i$$

$$F_i = [(F_{\max i} - 1) \times F\% + 1]$$

F<sub>max i</sub> = max factor

F% = % applicability relative contributions (these are based on engineering judgement)

Factor	% Contribution made to unreliability modification
Opposite Technique	41
Misperception of risk	24
Conflict of objectives	15
Inexperience	12
Low Morale	8



### Step 3: Prioritise Reducing Measures

The third stage is to form conclusions with these results and prioritise reducing methods. Table 7.3 provides techniques to be implemented to reduce human error. In the example **opposite technique** has the highest contribution of **41%**, thus the greatest priority. The suggested remedial:

[9] The greatest possible care should be exercised when new techniques are being considered to achieve the same outcome — they should not involve adoption of opposing philosophies.

The final stage is to implement the remedial advice.

## **SECTION 9: SOME NOTES ON FIRE RISK ASSESSMENT**

It is vital that any new railway project has an adequate and fully integrated fire safety concept. The project should consider a fire safety study to provide an overall assessment of the fire risks and examine the impact on the railway. The study should enable the railway systems to be optimised and configured to achieve a set of overall fire safety objectives. PMSC has undertaken a similar study already see project 90.

The fire safety objectives should primarily achieve an acceptable level of fire safety (risk from fire) for passengers, staff, emergency services personnel and any other legitimate occupants of the rail network.

As a first step the fire safety study would require an overall system assessment of the level of fire safety proposed to examine fire safety approaches and identify any weaknesses or opportunities for application of alternative strategies, which may be more suitable.

This systems approach to fire safety should consider the interactions among various system components that can create mitigating conditions not evident when examining the performance of individual components.

Once the overall fire safety has been examined on a system wide level, individual sub-systems or components should be examined in detail to optimise their configuration in relation to maintaining the overall fire safety objectives while meeting other system objectives.

The basic principle of fire safety should be that if a fire does not occur in the first place then there is no impact on the fire safety objectives. However, practically it is often difficult to prevent ignition while still having an operational system. Thus fire prevention measures can only be implemented where they do not significantly impact the fundamental design/operational requirements of the system.

There are three ways in which a fire may be prevented as follows:

- Controlling ignition (heat/energy) sources
- Controlling the available fuels
- Controlling interactions between ignition sources and fuel

There are two ways in which an ignition source may be controlled, by eliminating the ignition source, or by controlling the potential ignition source such that its heat / energy output is not sufficient to cause ignition. Similarly, there are two strategies that can be adopted to prevent fire ignition by eliminating the fuel, or controlling its ignitability.

Suppression of a fire is another method of managing the impact of the fire. Suppression can be undertaken either manually or automatically by various fire suppression systems. The most common form of an automatic fire suppression system is a fire sprinkler system. However given that the railway will use electricity as its energy source, an automatic sprinkler system is likely to be inappropriate. Thus automatic gaseous suppression systems could be used.

**The Application of RAMS in Large Scale Complex Railway Projects**  
**RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

Manual suppression systems require the fire to be detected, communicated, action to be decided, and a response to the site of the fire together with sufficient suppressant been applied. While there are a lot of dependencies, manual suppression can be quite effective, particularly if early detection and notification is provided.

In addition to manual fire suppression facilities, fire hydrants can be provided in tunnels and underground stations to enable manual suppression of large fires by the fire brigade and rescue services.

Evacuation of passengers and staff in the case of fire should also be considered within the fire safety concept. There are usually many different scenarios that could occur with regard to railway fires (i.e. open track, tunnel, within a train, within wayside equipment or buildings). Hence, a comprehensive assessment should be made of the credible scenarios and mitigation features, and emergency planning should be employed as necessary. Since there are many interdependencies associated with railway fire conditions, and subsequent evacuation, it is usually necessary to use computer-based simulations and analysis tools to adequately assess the likely outcomes of the scenarios.

Other key aspects of providing an acceptable level of overall fire safety are:

- Selection of materials to minimise the growth and spread of fire, smoke, and toxic gases (i.e. materials used in the construction of the railway should be selected and tested to recognised international standards)
- Provision of automatic detection within major fuel loads (i.e. electrification sub-stations)
- Provision of communication systems to all public areas
- Provision of emergency walkways in tunnels if necessary
- Provision of pressurised emergency exits to permit evacuation from tunnels if necessary
- Tunnel emergency evacuation fans if necessary

PMSC has the capability to organise and coordinate fire testing of materials for toxicity and spread of flame according to recognised British Standards BS6853 and BS 476.

## **SECTION 10: SOME USEFUL SYSTEMS ASSURANCE REFERENCES**

<b>Topic Area</b>	<b>International Standards/Data Sources</b>
FMECA	<ul style="list-style-type: none"> <li>• Military Standard 1629</li> <li>• IEC Publication 812 'Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Criticality'.</li> </ul>
HAZOP	<ul style="list-style-type: none"> <li>• MIL-STD-882B: 'System Safety Management',</li> <li>• prENV50126: 'Railway Applications – The Specification and Demonstration of Dependability, Reliability, Availability, Maintainability and Safety (RAMS)'</li> <li>• DEF STAN 00-58 'Hazop Studies on Systems Containing Programmable Electronics'</li> <li>• "Hazop and Hazan" by T Kletz (UK) Institution of Chemical Engineers 3<sup>rd</sup> Edition 1992.</li> <li>• Railtrack Yellow Book</li> </ul>
FTA and ETA	<ul style="list-style-type: none"> <li>• NUREG-0492 'Fault Tree Handbook' D F Hassel, N H Roberts, W E Vesely, and F F Goldberg US Nuclear Regulatory Commission</li> <li>• Reliability and Risk Assessment by J.D Andrews and TR Moss ISBN 0-470-23345-1, Chapter 7 Fault Tree Analysis.</li> <li>• Combined FTA/ETA modeling tool is Fault Tree + (Currently version 9)</li> </ul>
Reliability Analysis (includes analysis and demonstration)	<ul style="list-style-type: none"> <li>• IEC 61508 - Functional Safety: Safety-Related Systems Part 2 and 6</li> <li>• MIL-STD-785B: 'Reliability Program for Systems and equipment Development and Production</li> <li>• MIL-STD-756: ' Reliability Modeling and Prediction'</li> <li>• MIL-STD-2173: ' Reliability Centred Maintenance</li> <li>• MIL-HDBK-217F: 'Reliability Prediction of Electronic equipment',</li> <li>• DEF STAN 00-40: 'Reliability and Maintainability Parts 1-8',</li> <li>• DEF STAN 00-43: 'Reliability and Maintainability Assurance Activity'.</li> <li>• International Electrotechnical Commissions Standard – 60300 – Dependability Management</li> <li>• International Electrotechnical Commission Standard – 60571, Part 3 – Electronic Equipment Used on Rail Vehicles, Components, Programmable Electronic Equipment and Electronic System Reliability</li> <li>• International Electrotechnical Commissions Standard 60605, Equipment Reliability Testing</li> </ul>

**The Application of RAMS in Large Scale Complex Railway Projects**  
**RAMS Seminar at Palace Hotel, Madrid, Spain, 2<sup>nd</sup> December 2004**

Topic Area	International Standards/Data Sources
	<ul style="list-style-type: none"> <li>• BS Euro Norm 50126, 1999, Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)</li> <li>• Euro Norm 50129, 1998, Railway Applications – Safety Related electronic systems for Signalling.</li> <li>• MIL-STD-471A – Military Standard Maintainability Verification / Demonstration / Evaluation.</li> </ul>
Software SIL Analysis	<ul style="list-style-type: none"> <li>• IEC 61508 Parts 3 and Parts 6, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related systems Part 3 : Software Requirements, Part 6 : Guideleines on the applications of parts 2 and 3.</li> <li>• RIA 23, BRB/LU LTD/RIA Technical Specification Number 23 1991, Safety Related Software For Railway Signalling – Consultative document. (this has now been largely superceeded by the requirements as set out in IEC 61508)</li> <li>• prEN 50128, Draft European Standard, Railway Applications – Software For Railway Control and Protection Systems.</li> </ul>
Human Factors	<ul style="list-style-type: none"> <li>• Human Reliability Assessors Guide Book</li> <li>• A Guide to Task Analysis</li> <li>• NUREG 1278 Swaine &amp; Guttman</li> <li>• Papers by Williams on HEART</li> </ul>
Fire Analysis	<ul style="list-style-type: none"> <li>• BS6853 1999, Code of Practice for Fire Precautions in the design and construction of passenger carrying trains</li> <li>• BS476, Fire tests on Buildings Materials and Structures, Part 6 Method of Test for Fire Propagation for Products</li> <li>• BS476, Fire tests on Buildings Materials and Structures, Part 7 Method of Test to determine the classification of the surface spread of flame of products</li> <li>• NFPA 130, Standards for Fixed Guideway Transit and Passenger Rail Systems 2000 Edition.</li> </ul>