PM SAFETY CONSULTANTS LIMITED

www.pmsafety.co.uk.

www.pmsafety.co.uk

PM SAFETY CONSULTANTS LIMITED.

PMSC LIMITED

Independent Company

Formed in 1992

Based in UK

Working in RAMS

Size is 15 to 20 experts in RAMS

PMSC LIMITED PRESENTATION

PRESENTED BY:
Paul Mann
B.Sc. (Hons), C.Eng, M.I.MechE, F.S.a.R.S
(Principal RAMS Advisor)

Thursday 2nd December 2004,

Palace Hotel, Madrid, Spain.

"SYSTEMS ASSURANCE AS APPLIED TO COMPLEX RAILWAY SYSTEMS"

PM SAFETY CONSULTANTS LIMITED.

STRUCTURE OF THIS PRESENTATION

- **Part 1) Definitions of Systems Assurance**
- **Part 2) Review of Typical Standards (principally EN50126)**
- **Part 3) Systems Assurance Planning**
- **Part 4) Methodologies & Safety Case**
- **Part 5) Review of Benefits**
- **Part 6) Review of Selected Project Examples**
- **Part 7) Review of Some Problems and Solutions**
- **Part 8) QESTIONS & ANSWERS**

•(Total time 40 minutes – hopefully !)

PART 1: DEFINITIONS OF SYSTEMS ASSURANCE

" Without Definition there is chaos"

WHY DOES SYSTEMS SAFETY ASSURANCE EXIST AS A DISTINCT DISCIPLINE?

Creation of discipline driven by accidents and mishaps

Recognition that rule based engineering and operations approaches to safety were insufficient

SYSTEMS ASSURANCE

What is Systems Assurance ?

- Reliability
- Availability
- Maintainability
- Safety

SYSTEMS ASSURANCE

Why do we carry out Systems Assurance ?

- To ensure Safe designs
- To minimise hazards
- To prevent accidents
- To ensure that design is reliable and available
- To ensure that design can be maintained
- To ensure system is reliable for passengers
- To help define operational regime for the operator

- To ensure that life cycle costs are minimised for the owner

SYSTEMS ASSURANCE

This is what could happen if designs are not safe

This is what we try to avoid ……

Typical side ballooning of wreckage

Interior of front end of 35 Run, Car 5721 taken from doors 3&4

SYSTEMS ASSURANCE

This is what could happen if designs are not safe

This is what we try to avoid ……

Interior of front end of 35 Run, Car 5721 taken from doors 3&4

SYSTEMS ASSURANCE

This is what could happen if designs are not safe

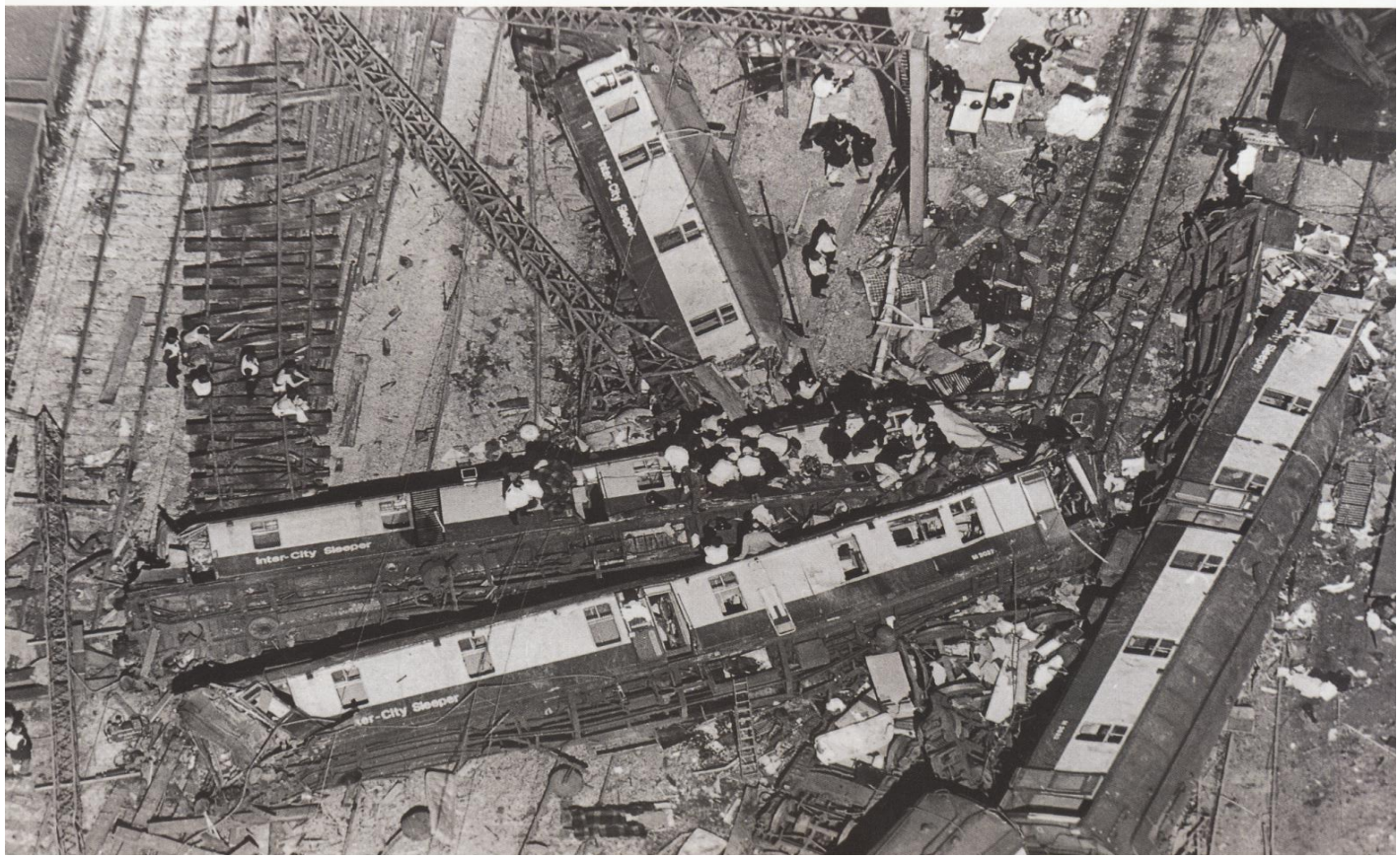
This is what we try to avoid ……

Typical side ballooning of wreckage

SYSTEMS ASSURANCE

This is what could happen if designs are not safe

This is what we try to avoid ……



Nuneaton June 1975

PM SAFETY CONSULTANTS LIMITED.

SYSTEMS ASSURANCE

This is what could happen if designs are not safe

This is what we try to avoid ……

Melun, France, October 1991

PM SAFETY CONSULTANTS LIMITED.

SYSTEMS ASSURANCE

This is what we desire……safe, reliable cost effective normal operation with no accidents….

SYSTEMS ASSURANCE

What are the key Systems Assurance Issues?

- Systems Assurance Plan
- RAMS Programme
- RAMS Organisation
- RAMS activities
- RAMS Reporting

SYSTEMS ASSURANCE

How should you organise for Systems Assurance ?

- Team Coordinator
(Promoting RAMS within the Project Team)

- Project Management and customer
(Correct priority at project milestones)

- Discipline engineers (right input at right time)

- Independent Review
(Approval as project progresses)

SYSTEMS ASSURANCE

When should we deliver RAMS Tasks?

- Concept design
- Preliminary Design
- Detailed Design
- RAMS Demonstration during Trial running or operational phase.

SYSTEMS ASSURANCE

What are typical RAMS Outputs ?
Some examples are:-

- Safety Case & RAM Case
- HAZOP Reports and Hazards Log
- RAMS Trade-off studies
- FMECA
- QRA Modelling and ALARP demonstration

PART 2: REVIEW OF TYPICAL STANDARDS (PRINCIPALLY EN50126)

" Standards only tell us WHAT to do not HOW to Do it"

SYSTEMS ASSURANCE STANDARDS

What Standards can guide us ?

- EN50126 RAMS Management
- Network Rail Yellow Book
- Network Rail Red Book
- HSE 2000 Regulations
- UK Defence Standards and British Standards
- US Military Standards

PART 3: SYSTEMS ASSURANCE PLANNING

" Sun Tzu the Ancient Chinese Warrior and General maintained That planning before the commencement of battle was the key to success, so to implementation of Systems Assurance Strategies at the planning stages of a project, will Subject to professional execution, assure a Safe and reliable design and an optimised maintenance regime and minimised life Cycle cost".

TYPICAL CONTENTS OF A RAMS PLAN

- Introduction
- Project Description
- Organisational Structure
- RAMS Activities& Deliverables
- RAMS Programme
- Design Criteria and RAMS Targets
- Control of Sub-contractors/Suppliers
- References and Acronyms

PART 4: METHODOLOGIES

" These are the engine room of Systems Assurance
And without engines the train will not run"

RAMS ASSURANCE – METHODS & TOOLS

- FMECA
- HAZOP
- FAULT & EVENT TREE ANALYSIS
- RELIABILITY BLOCK DIAGRAMS (RBD's)
- SAFETY CASE AND RAM CASE
- SIL Assessment
- DEMONSTRATION OF ALARP

RAMS ASSURANCE – METHODS & TOOLS

- **Key Concepts Embodied in FMECA**

  - Component by component analysis of entire system to identify failure modes and effects

  - Identification of failure severity

  - Identification of methods of failure detection and prevention

  - Identification of failure criticality followed by tracking and disposition of all critical items

RAMS ASSURANCE – METHODS & TOOLS

- **Key Concepts Embodied in HAZOP**

  -**Team of review by participants each having expertise in different aspects of operations, engineering and hazards**

  - **Brainstorming of hazards guided by a structured methodology and an experienced chairperson**

  - Systematic identification of deviations and hazard control measures

RAMS ASSURANCE – METHODS & TOOLS

- **Key Concepts Embodied in Fault Tree Analysis**

  - Development of hazardous system failure modes into progressively more detailed causes

  - Identification of the permutation and combinations of causes that may produce hazardous system failure

  - The creation of a mathematical model for the quantification of system accident frequency

RAMS ASSURANCE – METHODS & TOOLS

- **Key Concepts Embodied in Reliability Block Diagrams (RBD's)**

  - **Analytical review of systems and sub systems**

  - **Development of pictorial representation of series and Parallel logic**

  -**Can be used as a precursor to define Fault Tree logic And top events**

RAMS ASSURANCE – METHODS & TOOLS

- **Key Concepts for Safety Integrity Levels (SILs)**

  - Certain aspects of safety may be best governed by deterministic rules, particularly where there are limitations in risk prediction (e.g. software, CCF)

  - SIL provides a means to apply risk based decision making in selecting the level or rigor of deterministic rules applied to particular system components (most often integrated hardware/software sub-systems)

RAMS ASSURANCE – METHODS & TOOLS

- **Key Concepts for Safety Case and RAM Case**

  -**To provide a coherent case for Safety based on the assurance process and evidence Gained during that process**

  - To provide a coherent case for RAM based on the assurance process and evidence Gained during that process

RAMS ASSURANCE – METHODS & TOOLS

- **Safety Cases are used world wide now**

- **UK**
- **Europe**
- **Asia**
- **In regulated and non regulated business**

- **The safety case should make the argument For safety and justify that the design is safe**

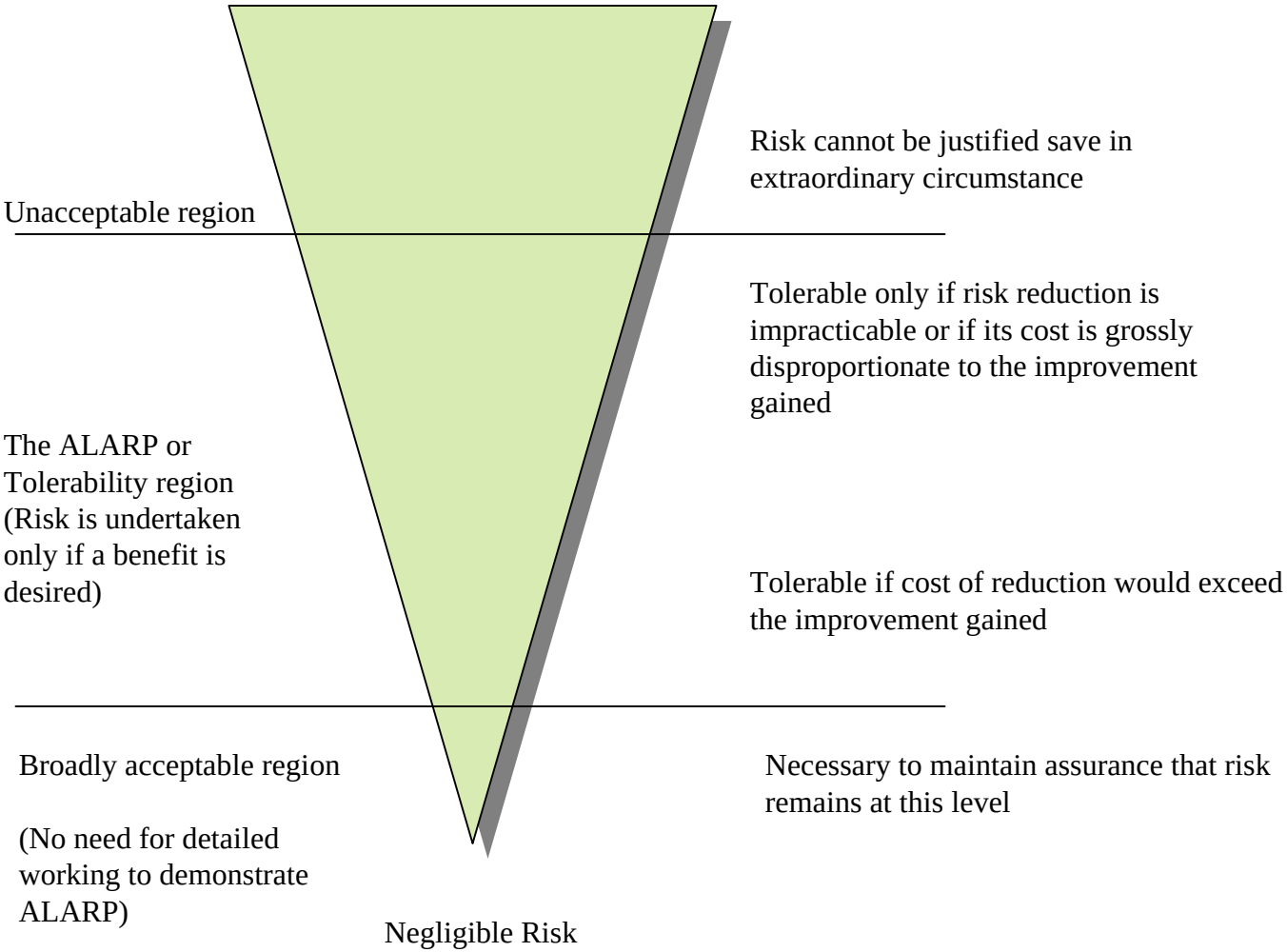
RAMS ASSURANCE – METHODS & TOOLS

• Key Concepts for
Applying As Low As Reasonably Practicable (ALARP)

- Individual hazards are evaluated on a qualitative or quantitative basis, to ensure sufficient control measures such that risk is ALARP

- ALARP requires that there are no reasonably practicable means to reduce the risk further

- Implies a cost benefit calculation to weigh the cost of Preventing fatality against the benefit of reducing risk.



PART 5: REVIEW OF BENEFITS

" Systems Assurance can only provide Optimal benefit if it is fully integrated Into the design development process"

Review of Benefits

- **Formalisation of good engineering practice**
- **Provides a forum for multi-disciplinary discussion**
- **Allows the identification of hazards and their potential consequences at the design stage and at interfaces and system boundaries**
- **Provides feedback for the design to improve safety and reduce risks to tolerable levels**
- **Resolution of hazards at interfaces and thus helps with systems integration**
- **Auditable trail and Safety Justification to Owner/Operator/Regulations - Safety Case reporting**

PART 6: PROJECT EXAMPLES

" PMSC has completed 108 projects since 1992
A selection of our major rail projects
Have been discussed here"

GENERAL REVIEW OF PMSC PROJECT EXPERIENCE

- C751B (6 CAR EMU, 750V DC THIRD RAIL) IN SINGAPORE
- CORE SYSTEM FOR THE MARINA LINE IN SINGAPORE
- C760 NORTH EAST LINE PROJECT IN SINGAPORE
- SP1900 ROLLING STOCK IN HONG KONG
- CORE SYSTEM TAIWAN HIGH SPEED RAIL PROJECT
- DELIVERY OF A RAMS TRAINING COURSE IN SINGAPORE
- GENERAL ASSISTANCE TO KHI ON TAIWAN HIGH SPEED RAIL PROJECT
- RAM SUPPORT TO BOMBARDIER TRANSPORTATION LTD FOR CONNEX 8/9
- SYSTEMS ASSURANCE SUPPORT TO SIEMENS
- SAFETY CASE FOR THE DIGITAL TETRA REPEATER SYSTEM

REVIEW OF PMSC PROJECT EXPERIENCE
(with ALSTOM companies)

- **ENGINEERING MANAGEMENT FOR ALSTOM**

- **PROVISION OF SUPPORT TO AREVA (PREVIOUSLY ALSTOM T&D)**

- Contractors Require Approved Contractors Assurance Case (CAC) Network Rail's Standard – RT/LS/P/016 (Issue 9)

- **SUPPORT TO ROLLING STOCK PROJECTS AT WASHWOOD HEATH IN THE MID 1990'S**

- **PROVISION ON SUPPORT TO ALSTOM ON SCOTTISH NUCLEAR DRY STORE PROJECT IN EARLY 1990'S**

PMSC **PM SAFETY CONSULTANTS LIMITED.**

GENERAL REVIEW OF PMSC PROJECT EXPERIENCE

C751B (6 Car EMU, 750V DC Third Rail)- Singapore

- All RAMS Scope for all Train Systems Including Operational HAZOP
- HAZOPs and Hazard Log Coordination
- QRA and Safety Case Preparation
- FMECA for all Systems
- RAM Predictions and design feedback
- RAM Demonstration Plan
- Train Level System Functional FMECA
- Liaison between supplier and customer (LTA)

Project Duration 18 months and estimated 8000 man hours.

PM SAFETY CONSULTANTS LIMITED.

GENERAL REVIEW OF PMSC PROJECT EXPERIENCE

Core System for the Marina Line in Singapore

• PMSC acted as the RAMS advisor to Japanese Consortium of Kawasaki, Itochu and Toshiba

• Various presentations were given to Singapore LTA

• PMSC produced whole fully integrated RAMS program to meet LTA contract requirements

• A Systems Assurance Program Plan was prepared to meet Defence Standards 00-56 and EN50126 requirements and this was accepted by LTA

• Systems level FMECA and Fault Tree analysis was undertaken as part of the tender process

• Software SIL level assessments were also undertaken

• Duration 18 months and estimated 900 man hours.

GENERAL REVIEW OF PMSC PROJECT EXPERIENCE

C760 North East Line Project Communication Package- Singapore

• Reliability Block Diagrams, RBD's for all Communications modules

• Fault Tree Analysis, FTA and FMECA

• RAM Demonstration Plan

• SIL 2 Software Safety Assessment for the Train Computer Interface Module to meet the requirements of IEC 61508

• SIL 0 Software Safety Assessment for the TETRA System to meet the requirements of IEC 61508

• Liaison between supplier and customer (LTA)

Project Duration: 18 months and estimated 4000 man hours.

GENERAL REVIEW OF PMSC PROJECT EXPERIENCE

SP1900 Rolling Stock In Hong Kong

• SP 1900 Supplied to run over existing East Rail & new line West Rail operated by KCRC in Hong Kong

• System Level FMECA work was undertaken

• Quantified Risk Assessment was prepared and accepted by KCRC

• Operational Safety Report for West Rail and East Rail was prepared and accepted by KCRC

Project Duration 12 months, man hours 3000

GENERAL REVIEW OF PMSC PROJECT EXPERIENCE

Taiwan High Speed Railway (Preliminary Design)

- Initial Safety Study in Japan of Reference System
- RAM Assurance Plan and Systems Safety Plans to EN50126
- RAM Workshop to develop RAM Requirements / RAM Concept Documents
- System Level FMECA for Core System (including Train Set)
- Detailed HAZOPs for all train systems and Hazard Log Coordination
- Overall RAMS Assurance Summary Reports and Draft QRA

Project Duration: 2.5 Years and estimated 7500 man hours.

GENERAL REVIEW OF PMSC PROJECT EXPERIENCE

Systems Assurance Course For LTA Singapore

PMSC deliver a bespoke RAMS training course to the Land Transport Authority of Singapore. Modules covered include:

- Safety Management Principles
- Safety Management Standards
- Safety Management Concepts
- Overview of Systems Assurance Techniques and worked examples including:
    - FMECA
    - HAZOP Methods and Hazard Analysis
    - Quantified Risk Assessment

GENERAL REVIEW OF PMSC PROJECT EXPERIENCE

General Assistance To KHI On Taiwan High Speed Rail Project

• Following on from our involvement for 2.5 years in the concept and preliminary design of the Taiwan High High Speed Rail Link PMSC provided the following to Kawasaki Heavy Industries:-

• Development of Fire Management Strategy

• Coordination of Fire Testing of over 300 materials to BS 6853

• Development of a Quantified Risk Assessment for fire risk

• Developed Overall Fire Safety Case Document

• Development of detailed Fault and Event Tree Modeling and Human Factors assessments of the rolling stock layouts

•Project Duration 2 years, Man Hours 3500

GENERAL REVIEW OF PMSC PROJECT EXPERIENCE

RAM Support To Bombardier Transportation Ltd For Connex 8/9

Reliability Improvement program for the Electrostar Vehicle

- Examination of candidate systems including PIS, Doors, Traction and MITRAC Train Management System

- Statistical analysis of event data from Electrostar depots (Chart Leacon)

- Attendance and reporting of RCM sessions

- Reporting of best ways to improve reliability and optimise maintenance regime – 9 key deliverables.

Project Duration 9 months, Man Hours 2700

GENERAL REVIEW OF PMSC PROJECT EXPERIENCE

Systems Assurance Support To Siemens

• Provision of specialist safety And RAM personnel to Erlangen and Krefeld

• Initial involvement in HEX including Depot at Old Oak Common and initial fast train services prior to full opening

• Subsequent involvement in SWT, WCML, Northern Spirit, Trans Pennine etc

• All PMSC people supplied are experts in RAMS and have all undergone Yellow Book Training

Project Duration several years since 1996 (various projects over several years).

GENERAL REVIEW OF PMSC PROJECT EXPERIENCE

PRODUCT ASSURANCE – Mikom (UK) TETRA Project

- Trial site at Birmingham New Steet Railway Station
- Provision of a digital Repeater system
- Typical equipment includes Antennas etc (see next slide)
- Exclusion zones to prevent EMI
- Safety Justification including Safety Case and HAZOP

PART 7: REVIEW OF SOME PROBLEMS AND SOLUTIONS

" Only those who appreciate the knowledge
Gained by quick failure can achieve lasting success"

•TYPICAL PROBLEM AREAS/ISSUES

- Insufficient RAMS resources
- Little or no Integration into design
- No engineering involvement
- Planning & timing of SA work
- Competing objectives allowed to win
- Data sources
- Poor control of sub contractors
- Ambiguity in plans
- Unrealistic RAMS targets
- Spec versus targets
- ALARP conclusions
- Design not influenced
- Interface problems

DISCUSSION/QUESTION & ANSWERS

Thanks for listening are there any Questions ?

PM SAFETY CONSULTANTS LIMITED.

www.pmsafety.co.uk

PMSC PM SAFETY CONSULTANTS LIMITED.