Safety Critical Systems Development

Prof. Chris Johnson,
Department of Computing Science,
University of Glasgow,
Glasgow,
Scotland.
G12 8QJ.

URL: http://www.dcs.gla.ac.uk/~johnson
E-mail: johnson@dcs.glasgow.ac.uk
Telephone: +41 330 6053

October 2007.

Introduction

- Terminology.

- Accidents.

- Ariane 5 Case Study.

Overview...

- Open assessment -

30% on a practical exercise.

- Closed assessment.

- Textbook:

Nancy Leveson's *Safeware: System safety and computers*, Addison-Wesley, ISBN 0-201-11972-2.

Terminology

- What is 'Safety'?

- Nothing bad will happen?

- Is this sufficient?

Terminology

- What is 'Safety'?

- System will not endanger human life or the environment (Storey, p.2)

- Freedom from accidents or losses (Leveson, p.181)

- Are these sufficient?

Terminology

- What is 'Safety'?
- An absolute or relative term?
- Does it form a continuum?
- Can we ever be 'absolutely' SAFE?

Terminology

- Is 'Safety' Relative?
- Depends on individual view of risk
- Risk = frequency x cost
- But cost or utility is subjective...

Terminology

- What is 'Safety'?

- Utility $\rightarrow$ many theoretical questions.

- Use Leveson's pragmatism for now.

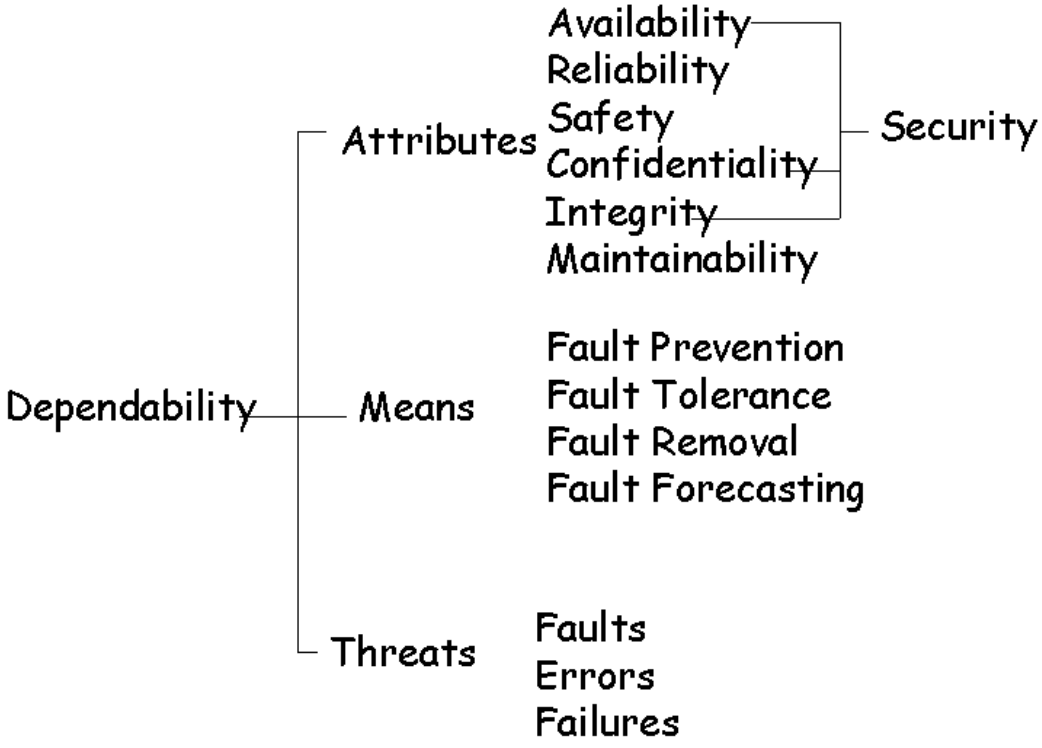
Terminology

- What is 'Safety'?

- Part of wider dependability?

- Ability to deliver a trusted service.

Terminology



Taken from J.C. Laprie's lecture notes on Diversity for Depandability

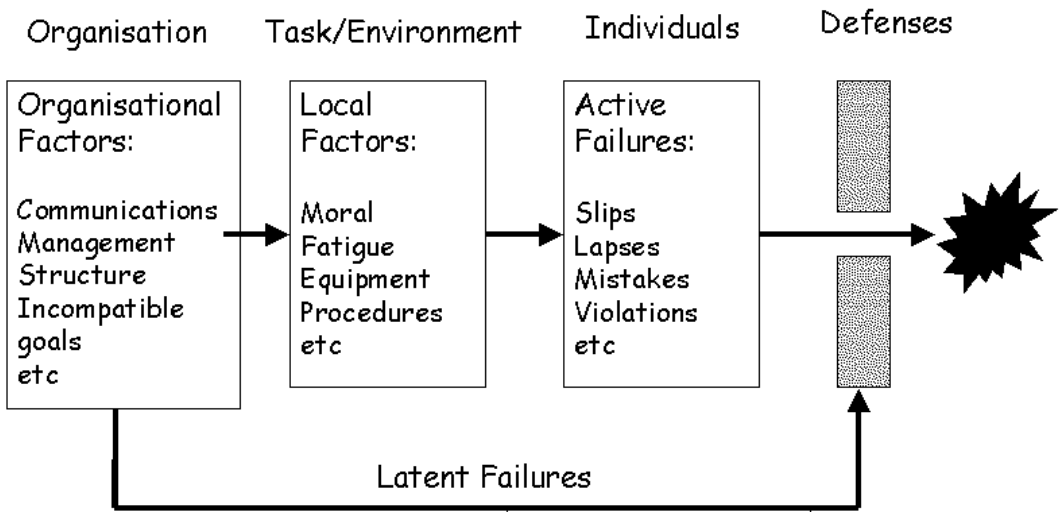
Terminology

- What is 'Safety'?

- Must also consider failures of safety.

- Freedom from accidents or Losses (Leveson).

Terminology



Taken from Reason, Managing the Risks of Organisational Failure, Ashgate Publishing, 1997.

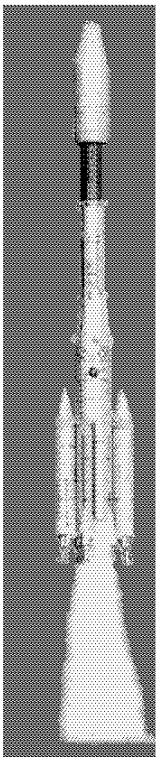
Terminology

- Accidents have multiple causes
- Some are latent.
- We should expect failure.
- Perrows' Normal Accidents?

Terminology

- What is 'Safety'?
- Is it an emmergent property?
- SYSTEMS continually change.
- So level of safety changes.

Ariane 5 Case Study



Ariane 5 Case Study

- Variable exceeds it's range...

e) At 36.7 seconds after H0 (approx. 30 seconds after lift-off) the computer within the back-up inertial reference system, which was working on stand-by for guidance and attitude control, became inoperative. This was caused by an internal variable related to the horizontal velocity of the launcher exceeding a limit which existed in the software of this computer.

Ariane 5 Case Study

- Defences in depth' failed...

f) Approx. 0.05 seconds later the active inertial reference system, identical to the back-up system in hardware and software, failed for the same reason. Since the back-up inertial system was already inoperative, correct guidance and attitude information could no longer be obtained and loss of the mission was inevitable.

Ariane 5 Case Study

- Error stemmed from redundant code!

m) The inertial reference system of Ariane 5 is essentially common to a system which is presently flying on Ariane 4. The part of the software which caused the interruption in the inertial system computers is used before launch to align the inertial reference system and, in Ariane 4, also to enable a rapid realignment of the system in case of a late hold in the countdown. This realignment function, which does not serve any purpose on Ariane 5, was nevertheless retained for commonality reasons and allowed, as in Ariane 4, to operate for approx. 40 seconds after lift-off.

Ariane 5 Case Study

- Problems in requirements/safety analysis.

n) During design of the software of the inertial reference system used for Ariane 4 and Ariane 5, a decision was taken that it was not necessary to protect the inertial system computer from being made inoperative by an excessive value of the variable related to the horizontal velocity, a protection which was provided for several other variables of the alignment software. When taking this design decision, it was not analysed or fully understood which values this particular variable might assume when the alignment software was allowed to operate after lift-off.

Ariane 5 Case Study

- Failed to understand system change?

o) In Ariane 4 flights using the same type of inertial reference system there has been no such failure because the trajectory during the first 40 seconds of flight is such that the particular variable related to horizontal velocity cannot reach, with an adequate operational margin, a value beyond the limit present in the software.

p) Ariane 5 has a high initial acceleration and a trajectory which leads to a build-up of horizontal velocity which is five times more rapid than for Ariane 4. The higher horizontal velocity of Ariane 5 generated, within the 40-second timeframe, the excessive value which caused the inertial system computers to cease operation.

Ariane 5 Case Study

It has been stated to the Board that not all the conversions were protected because a maximum workload target of 80% had been set for the SRI computer. To determine the vulnerability of unprotected code, an analysis was performed on every operation which could give rise to an exception, including an Operand Error. In particular, the conversion of floating point values to integers was analysed and operations involving seven variables were at risk of leading to an Operand Error. This led to protection being added to four of the variables, evidence of which appears in the Ada code. However, three of the variables were left unprotected. No reference to justification of this decision was found directly in the source code. Given the large amount of documentation associated with any industrial application, the assumption, although agreed, was essentially obscured, though not deliberately, from any external review.

(Section 2.2 COMMENTS ON THE FAILURE SCENARIO, paragraph 2)

Ariane 5 Case Study

Peter B. Ladkin,
http://www.rvs.uni-bielefeld.de/cms/book/view/491
The Ariane 5 Accident: A Programming Problem?

Robert Baber,
http://www.cas.mcmaster.ca/~baber/TechnicalReports/Ariane5/Ariane5.ht
The Ariane 5 explosion as seen by a software engineer.

Ken Garlington,
http://www.flash.net/~kennieg/ariane.html
Put it in the contract: The lessons of Ariane

Conclusions

- Safety is:

- freedom from accidents/losses.

- Accidents are:

- complex multi-causal events;
- (almost) impossible to predict.

- Therefore hard to maintain safety.

- This course tries to show you how...

Ethics and the Market Place

- Professional ethics.

- Safety Culture.

- London Ambulance Case Study.

What Are Ethics?

- Science of morals in human conduct.

- Moral princiles and rules of conduct.

- Oxford Concise English Dictionary.

Why Publish Professional Ethics?

- http://www.acm.org/constitution/code.html

- ACM Code of Ethics.

- A guide to "proper" conduct.

- But what do they contain?

ACM Code of Ethics

1.2 Avoid harm to others. "Harm" means injury or negative consequences, such as undesirable loss of information, loss of property, property damage, or unwanted environmental impacts. This principle prohibits use of computing technology in ways that result in harm to any of the following: users, the general public, employees, employers. Harmful actions include intentional destruction or modification of files and programs leading to serious loss of resources or unnecessary expenditure of human resources such as the time and effort required to purge systems of "computer viruses."

ACM Code of Ethics

Well-intended actions, including those that accomplish assigned duties, may lead to harm unexpectedly. In such an event the responsible person or persons are obligated to undo or mitigate the negative consequences as much as possible. One way to avoid unintentional harm is to carefully consider potential impacts on all those affected by decisions made during design and implementation.

To minimize the possibility of indirectly harming others, computing professionals must minimize malfunctions by following generally accepted standards for system design and testing. Furthermore, it is often necessary to assess the social consequences of systems to project the likelihood of any serious harm to others. If system features are misrepresented to users, coworkers, or supervisors, the individual computing professional is responsible for any resulting injury.

ACM Code of Ethics

In the work environment the computing professional has the additional obligation to report any signs of system dangers that might result in serious personal or social damage. If one's superiors do not act to curtail or mitigate such dangers, it may be necessary to "blow the whistle" to help correct the problem or reduce the risk. However, capricious or misguided reporting of violations can, itself, be harmful. Before reporting violations, all relevant aspects of the incident must be thoroughly assessed. In particular, the assessment of risk and responsibility must be credible. It is suggested that advice be sought from other computing professionals. See principle 2.5 regarding thorough evaluations.

Are Ethics Relevant?

- If you saw a bug in a friend's code.

- Would you tell the manager?

Are Ethics Relevant?

- Even if it cost their job?

- Even if it set project back 6 months?

Safety Culture

- "Whistle blowing" in ACM code.

- Would you do it?

- Depends on safety culture?

Safety Culture

- What supports safety culture?

- considered procedures/processes;
- careful review of process outputs;
- high priority for safety;
- documented resolution of conflict;
- budgetary control...

Safety Culture

- What weakens safety culture?

- poorly documented processes;
- ad hoc reviews of output;
- low priority for safety;
- poor resolution of conflict;
- (unpredictable) budgetary pressures.

London Ambulance Case Study

What is clear from the Inquiry Team's investigations is that neither the Computer Aided Despatch (CAD) system itself, nor its users, were ready for full implementation on 26 October 1992. The CAD software was not complete, not properly tuned, and not fully tested. The resilience of the hardware under a full load had not been tested. The fall back option to the second file server had certainly not been tested. There were outstanding problems with data transmission to and from the mobile data terminals. There was some scepticism over the accuracy record of the Automatic Vehicle Location System (AVLS). Staff, both within Central Ambulance Control (CAC) and ambulance crews, had no confidence in the system and were not all fully trained. The physical changes to the layout of the control room on 26 October 1992 meant that CAC staff were working in unfamiliar positions, without paper backup, and were less able to work with colleagues with whom they had jointly solved problems before. There had been no attempt to foresee fully the effect of inaccurate or incomplete data available to the system (late status reporting/vehicle locations etc.). These imperfections led to an increase in the number of exception messages that would have to be dealt with and which in turn would lead to more call backs and enquiries. In particular the decision on that day to use only the computer generated resource allocations (which were proven to be less than 100risk move.

Para. 1001, Southwest Thames Regional Health Authority report
http://www.cs.ucl.ac.uk/staff/A.Finkelstein/las.html
(Thanks go to Anthony Finkelstein, UCL, London.)

London Ambulance Case Study

- Safety culture not just jargon...

1004 Under the NHS reforms, all parts of the National Health Service (NHS) have gone through major cultural changes in the past few years and it is evident that the LAS could not bury its head in the sand if it was to provide a professional and successful service in the 1990s.

1005 However, the result of the initiatives undertaken by management from 1990-92 did not revitalise management and staff as intended, but actually worsened what was already a climate of mistrust and obstructiveness. It was not a case of management getting the agenda wrong. The size of the programme and the speed and depth of change were simply too aggressive for the circumstances. Management clearly underestimated the difficulties involved in changing the deeply ingrained culture of LAS and misjudged the industrial relations climate so that staff were alienated to the changes rather than brought on board.

London Ambulance Case Study

- Considered procedures?

3103 The Inquiry Team examined the role of SW Thames RHA during the development/implementation process. As covered elsewhere, the LAS was a quasi independent body with its own Board, being managed only at "arm's length" by the RHA. Thus there was no requirement for the Region to provide technical input to the CAD project. It is also important to note that LAS never sought any assistance. Throughout 1992, leading right up to the events of 26 and 27 October, many concerns were expressed by the RGM in writing and at minuted meetings about the progress of CAD. Many specific CAD related issues were discussed yet in each case evidence suggests that fairly bland assurances from the Chief Executive that everything will satisfactorily be resolved are accepted by RHA management. Given the nature of these concerns and the regularity with which they arise the Inquiry Team, with hindsight, would have expected the RHA to commission an independent, in depth technical review of the project and its true status...

London Ambulance Case Study

- Careful review of outputs?

3083 A critical system such as this, as pointed out earlier, amongst other prerequisites must have totally reliable software. This implies that quality assurance procedures must be formalised and extensive. Although SO had a part-time QA resource it was clearly not fully effective and, more importantly, not independent...

3098 During these months the system was never stable. Changes and enhancements were being made continually to the CAD software. The Datatrak system was being similarly amended and enhanced... Thus there was never a time when the project team could stand back and commission a full systems test. Ideally a phased implementation should have been planned for in the first place rather than added out of desperation. A properly phased and controlled implementation, under strong project management, would not have allowed the next phase to be implemented until there was total confidence in the integrity and acceptance of the current phase.

London Ambulance Case Study

- The priority for safety?

3079 Although there is little doubt that SO were late in delivery of software and, largely because of the time pressures under which they were working, the quality of their software was often suspect, it should be pointed out that other suppliers also had their problems. The design and positioning of the SOLO MDTs had to be changed following consultation with ambulance staff and SOLO were late in delivering the RIFS technology. However, unlike SO, they kept LAS project management fully informed of the true state of their progress. There were also continuing problems with data transmission, many of which are still not totally resolved. Datatrak also had problems with their installations.

London Ambulance Case Study

- Resolution of conflict?

3075 In October 1991 a new Systems Manager was recruited by LAS. Although he would not become directly involved in the project, at the request of the Board, he carried out a review of the project progress in early November... The report stresses the continuing need for quality, but it does not contain any real conclusions. It makes the point that the timetable allows no time for review and rework and that there is a general reliance on everything coming right first time. The report has a somewhat "cosy" feel to it and although some problems are identified, the reader is left with the impression that, even with the identified problems, there is a probability that success will be achieved. However, reading between the lines it is clear that there is much doubt about meeting the planned implementation date, notwithstanding the recommendation that the published date should not be changed.

London Ambulance Case Study

- Budgetary control...

3042 Throughout this phase it was clear that LAS management and the project team had a proposed budget in mind, for the complete system, of around 1,500,000. There does not appear to be any rational process by which this figure was established...

3046 It should also be noted that the SO quotation for the CAD development was only 35,000 - a clear indication that they had almost certainly underestimated the complexity of the requirement (although it is recognised that as is common in the industry SO would also be making a small margin on the contract price for the hardware). It is worth noting also that, at a meeting between LAS and SO prior to contract award, it is minuted that SO were told that one of the reasons for abandonment of the earlier IAL system was the alleged inability of the software house to understand fully the complexity of the requirement.

London Ambulance Case Study

A. Finkelstein & J. Dowell,
ftp://cs.ucl.ac.uk/acwf/papers/case.ps.gz
A Comedy of Errors: the London Ambulance Service case study

Ian Tighe,
http://www.bcs.org.uk/publicat/ebull/sept96/all.htm
All Systems Go!

Rohan Baxter (RISKS digest)
http://catless.ncl.ac.uk/Risks/17.39.html#subj1
Melbourne Ambulance System

Conclusions

- Professional ethics.

- Safety Culture.

- London Ambulance Case Study.

Standards

- Failure of Safety Culture.

- Need for Standards.

- IEC 61508 case study.

Failure of Safety Culture

- Cannot rely on safety culture.

- Standards enforce rules of conduct.

- (On their own dont ensure safety).

Standards

- http://www.demon.co.uk/ilsuk/

– UK DEF-STAN 00-60

- http://www.iec.ch/

– IEC 61508

- http://computer.org/standard/sesc/

– IEEE (overview)

- MIL-HDBK-1467

IEC 61508

- A Seven Part Standard (400+ pages)

1. General requirements;

2. Requirements for electrical/electronic/programmable electronic safety-related systems (hardware).

3. Software requirements

4. Definitions and abbreviations.

5. Methods for determining safety integrity levels.

6. Guidelines for the application of 1 and 2.

7. Techniques and measures.

Acknowledgement: this analysis of 61508 is partly based on a tutorial prepared by Felix Redmill for the 17th International Systems Safety Symposium

IEC 61508

- Zero safety is impossible (cf Perrow).
- Must understand the risks.
- and reduce unacceptable risks.
- and DEMONSTRATE this reduction.

IEC 61508 (Definitions)

Equipment Under control (EUC) [3.2.3]: equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.

EUC risk [3.2.4]: risk arising from the EUC or its interaction with the EUC control system (risk associated with functional safety) [it should be assessed independently of countermeasures to reduce it].

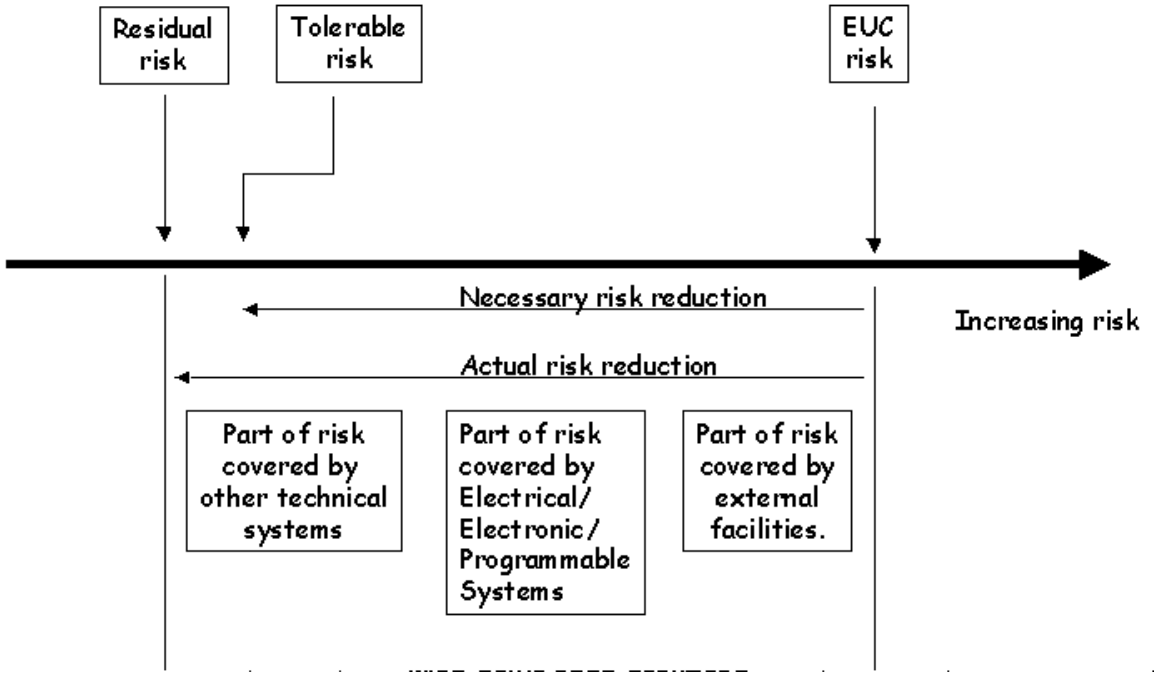
Tolerable risk [3.1.6]: risk which is accepted in a context based on the current values of society.

IEC 61508 (Definitions)

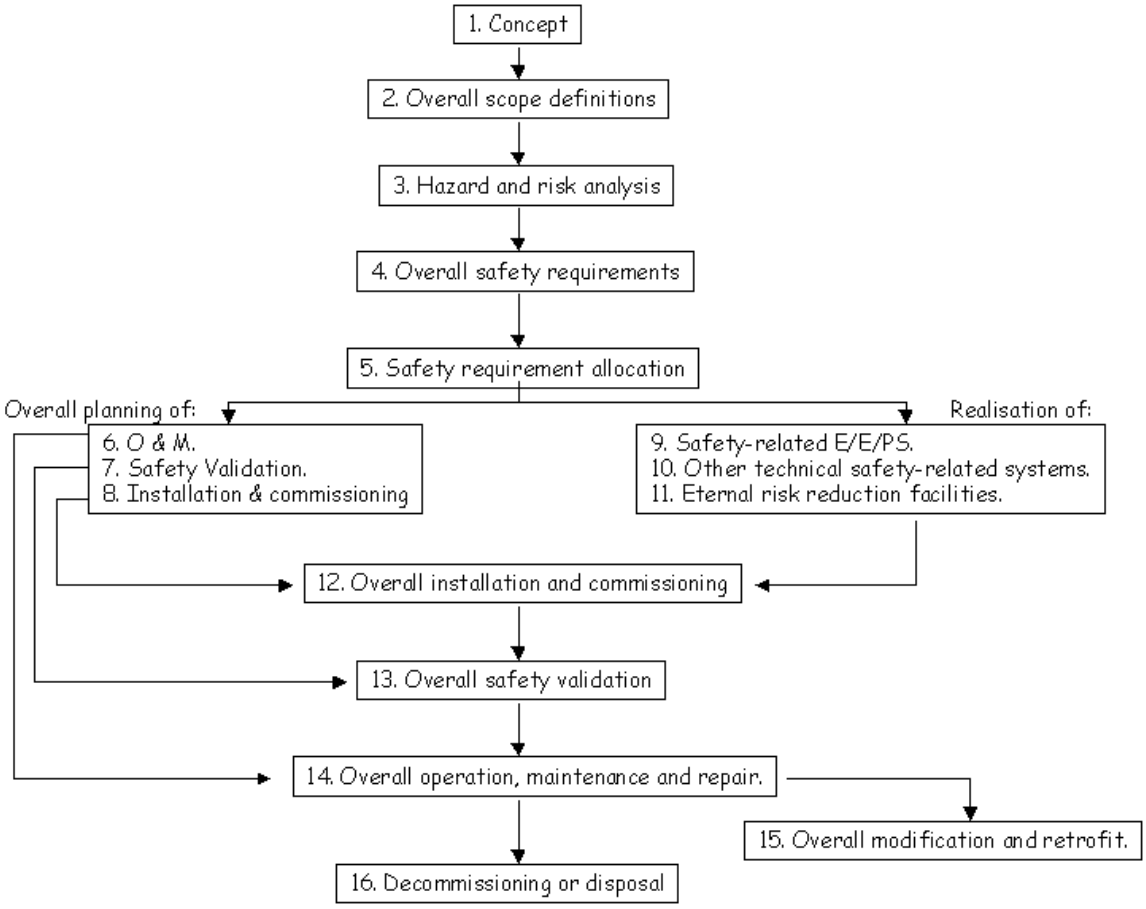
Safety-integrity [3.5.2]: probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.

Safety integrity level [3.5.6]: discrete level (one out of a possible four) for specifying the safety integrity requirements... where SIL 4 has the highest level of safety integrity and SIL 1 the lowest.

Meeting Intent [Annex A, Part 5]



Safety Lifecycle Model



Hazard Identification

- Risk = hazard frequency x cost.
- But numerous paths to hazard
- Deduce frequency of random events
- Impossible for systematic software 'bugs'.

Hazard Identification

- Estimate EUC risk of all hazards. [1:7.4.2.7]
- Quantitative or qualitative techniques [1:7.4.2.8]
- Must be documented & maintained [1:7.4.2.12]
- User must choose the method.

Event Frequency

Category	Meaning	Occurrences per operational hour
Frequent	Many times in a systems lifetime	> 10^{-3}
Probable	Several times in a systems lifetime	10^{-3} to 10^{-4}
Occasional	Once in a systems lifetime	10^{-4} to 10^{-5}
Remote	Unlikely in a systems lifetime	10^{-5} to 10^{-6}
Improbable	Very unlikely to occur	10^{-6} to 10^{-7}
Incredible	Cannot believe that it could occur	< 10^{-7}

- Can we trust low probabilities?

Hazard Consequence

Category	Meaning
Catastrophic	Multiple deaths
Critical	A single death, and/or multiple severe injuries or severe occupational illnesses
Marginal	A single severe injury or occupational illness and/or multiple minor injuries or minor occupational illnesses
Negligible	At most a single minor injury or minor occupational illness.

- Consequences are subjective?

IEC 61508 Risk Classes

Class I: Intolerable under any circumstance.

Class II: Undesirable and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained.

Class III: Tolerable if the cost of risk reduction would exceed the improvement gained.

Class IV: Negligible.

- As Low As Reasonably Practicable?

Safety Integrity Levels

- Risk analysis guides risk reduction.
- This leads to safety requirements.
- This helps define safety functions.
- This leads to allocation of systems.

Safety Integrity Levels

- Risk analysis guides safety concerns.
- Safety concerns reflected in SILs.
- Aimed for reliability in face of risk.
- But cannot quantify software failure rate?

Safety Integrity Levels

- Instead SILs guide processes.
- Higher SILs imply more rigour.
- In design, in testing, in validation.
- Higher SILs imply higher cost...

Safety Integrity Levels

Using a recommended process for a particular SIL doesnt guarantee that your systems meets the reliability requirement of that SIL.

- Circular argument...
- Cant measure software failure rate.
- So use a recommended process...
- Can we measure success of process?

Documentation

[1:5.2] Requirements documentation should be:
- sufficiently informative;
- available;
- accurate and concise;
- easy to understand;
- fit for purpose.

[1:6.2.1 d] Management specifies 'the ways in which information is to be structured and the extent to which information is to be documented'

- All activities need be documented.

- Documents must be maintained.

Open Issues

- How do you:

- demonstrate conformance?
- ensure independent reviews?
- control costs of following standard?

Conclusions

- Safety culture not enough.
- Standards offer guidance.
- IEC 61508 case study.
- Is this enough?
- On-going debate.

Organisational Failure

- Are safety culture & standards sufficient?

- MORT - Management Oversight & Risk Tree.

- DOE Case Study.

Importance of Management

- Standards supported by

- Safety Management Systems.

- Safety cutlure defended by

- Safety Management Systems.

- Without managerial support:

- safety culture will die;
- standards will be abused.

Organisational Failure

- Increasing focus on management.
- Standards can be mis-applied?
- Incidents can be ignored?
- Management controls context of failure?

MORT - Management Oversight and Risk Tree

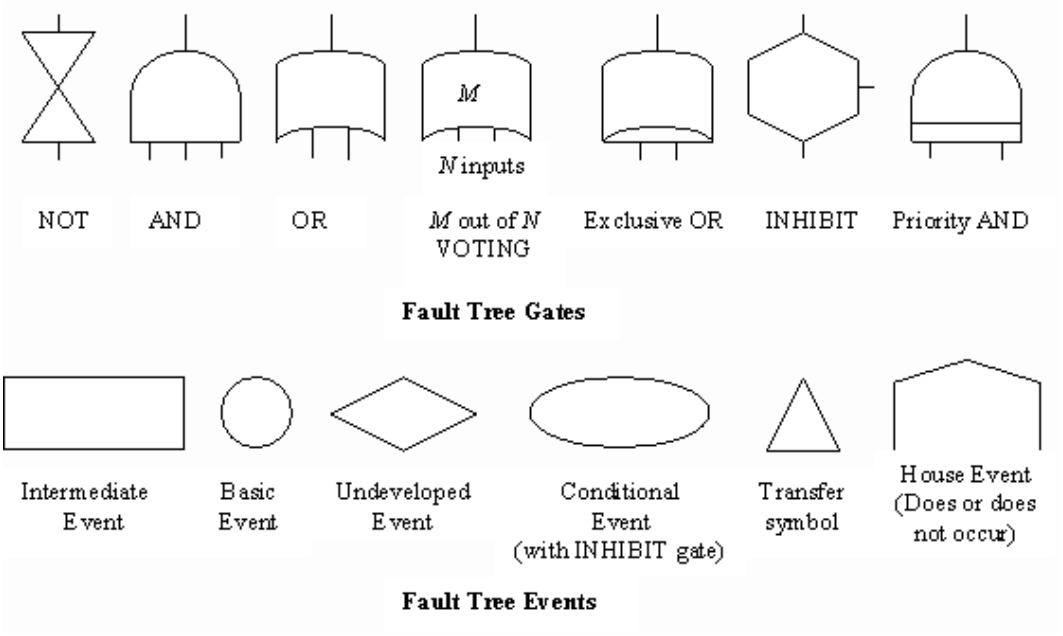
- Draws on management and safety.

- Based on fault-tree notation.

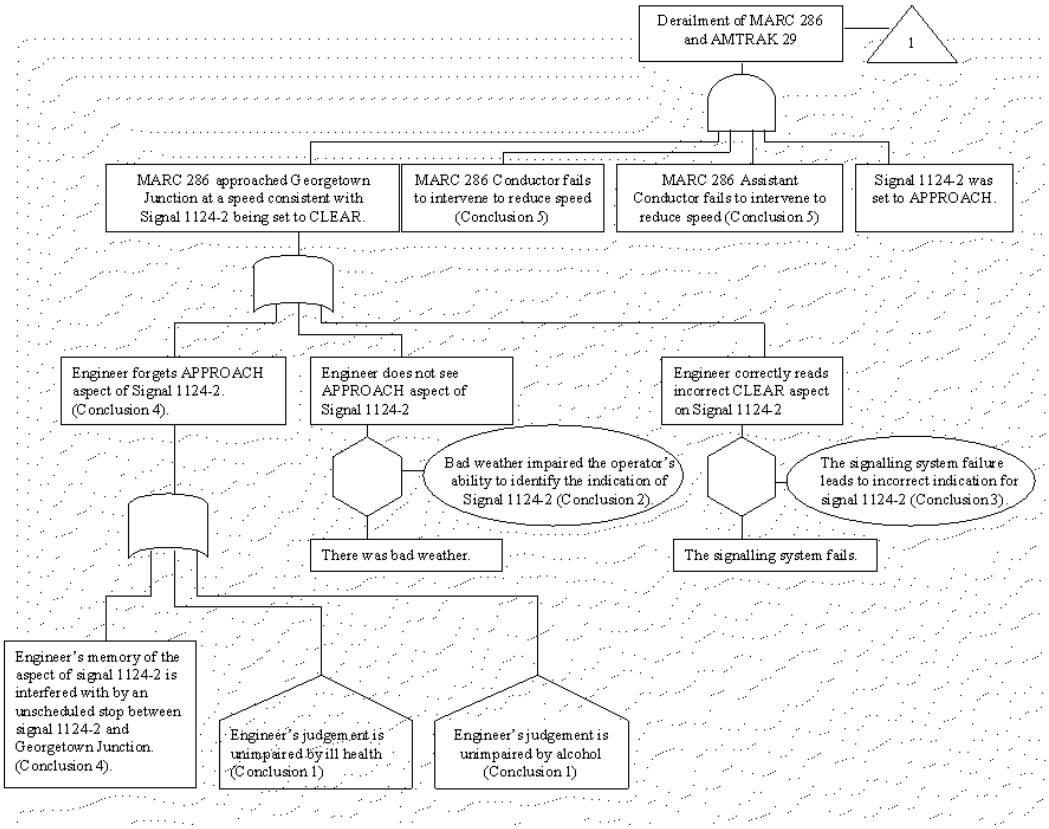
- AND, OR gates.

- Basic and intermediate events.

Fault Trees - Quick Introduction



Fault Trees - Quick Introduction



Fault Trees - Quick Introduction

- Fault trees very widely used.
- Have been extended to software 8(
- Used to find minimal cut sets etc.
- More about them later.

Back to MORT

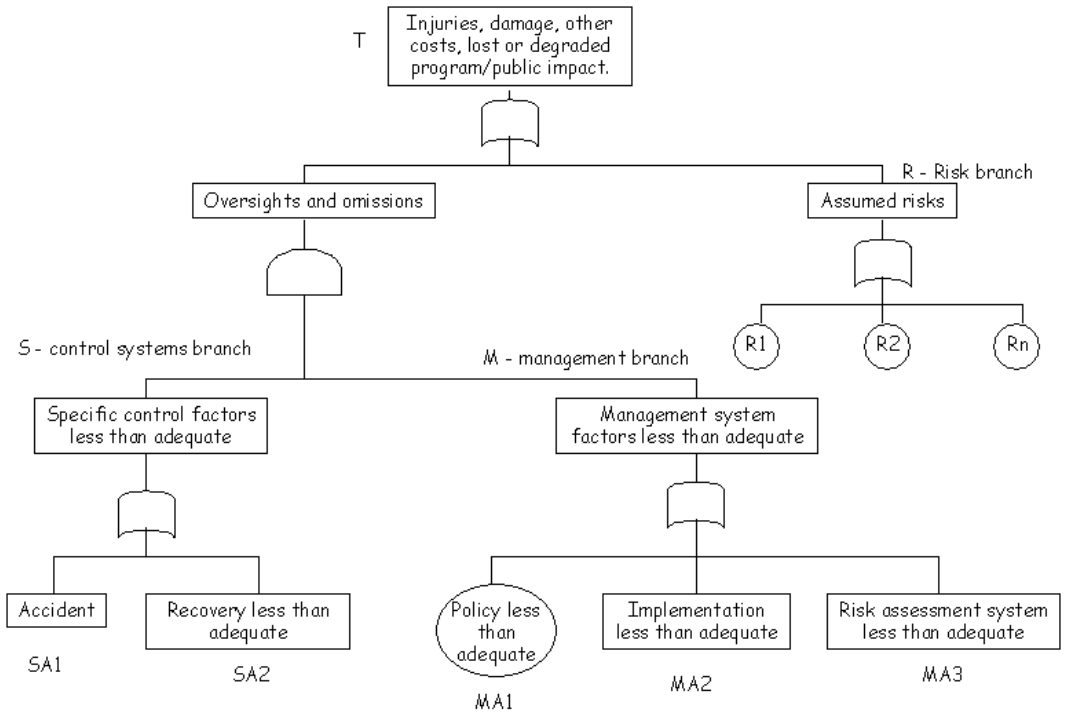
- Lets suppose we have an incident.

- Usually easy to spot direct causes?

- Operator error, system failure.

- How to identify managerial causes?

Back to MORT



MORT - Additional Information

http://tis.eh.doe.gov/portal/ US Department of Energy, search on mort, barrier analysis, charting.

N.M. Know and R.W. Eicher, MORT Users Manual. US Department of Energy-76/45-4 SSDC-4, 1992.

F. Koornneef and A. Hale, Using MORT to Generate Organisational Feedback. In A. Hale, B. Wilpert and M. Freitag (eds.) After the Event, Pergamon, 1997.

- Still active area of research.

MORT DOE Guidelines

MORT/Mini-MORT is used to used to prevent oversight in the identification of causal factors. It lists on the left side of the tree specific factors relating to the occurrence and on the right side of the tree, it lists the management deficiencies that permit specific factors to exist. The management factors all support each of the specific barrier/control factors. Included is a set of questions to be asked for each of the factors on the tree. As such, it is useful in preventing oversight and ensuring that all potential causal factors are considered. It is especially useful when there is a shortage of experts to ask the right questions.

- http://tis.eh.doe.gov/techstds/standard/nst1004/nst1004.pd

DOE GUIDELINE: ROOT CAUSE ANALYSIS GUIDANCE DOCUMENT (DOE-NE-STD-1004-92)

MORT DOE Guidelines

A Mini-MORT analysis chart is a checklist of what happened (less-than- adequate specific barriers and controls) and why it happened (less-than-adequate management). To perform the MORT analysis:

- Identify the problem associated with the occurrence and list it as the top event.
- Identify the elements on the "what" side of the tree that describe what happened in the occurrence (what barrier or control problems existed).
- For each barrier or control problem, identify the management elements on the "why" side of the tree that permitted the barrier control problem.
- Describe each of the identified inadequate elements (problems) and summarize your findings.

MORT DOE Guidelines

These findings can then be related to the ORPS cause codes using the worksheets in Appendix B. For critical self-assessment (not an ORPS requirement), the findings can also be related to MORT elements given in Figure G-2, MORT Based Root Cause Analysis Form. To do this, enter the findings in the left-hand column. Next, select the MORT elements from the top of the root cause form that most closely relate to the finding by placing a check in the column below the MORT elements and on the same line where the finding is listed (more than one element can be related to a single finding.) Then, sum the number of checks under each MORT element (the sum can be entered at the bottom of the page even though there is no place designated on the form). The relative number of checks under each MORT element (the sum of all the findings) is a measure of how widespread the element inadequacy is. The results guide the specific and generic corrective actions.

MORT DOE Guidelines

A brief explanation of the "what" and "why" may assist in using mini-MORT for causal analyses.

When a target inadvertently comes in contact with a hazard and sustains damage, the event is an accident. A hazard is any condition, situation, or activity representing a potential for adversely affecting economic values or the health or quality of peoples lives. A target can be any process, hardware, people, the environment, product quality, or schedule–anything that has economic or personal value.

What prevents accidents or adverse programmatic impact events?

- Barriers that surround the hazard and/or the target and prevent contact or controls and procedures that ensure separation of the hazard from the target
- Plans and procedures that avoid conflicting conditions and prevent programmatic impacts.

MORT DOE Guidelines

In a facility, what functions implement and maintain these barriers, controls, plans, and procedures?

- Identifying the hazards, targets, and potential contacts or interactions and specifying the barriers/controls that minimize the likelihood and consequences of these contacts
- Identifying potential conflicts/problems in areas such as operations, scheduling, or quality and specifying management policy, plans, and programs that minimize the likelihood and consequences of these adverse occurrences
- Providing the physical barriers: designing, installation, signs/warnings, training or procedures
- Providing planning/scheduling, administrative controls, resources, or constraints
- Verifying that the barriers/controls have been implemented and are being maintained by operational readiness, inspections, audits, maintenance, and configuration/change control
- Verifying that planning, scheduling, and administrative controls have been implemented and are adequate
- Policy and policy implementation (identification of requirements, assignment of responsibility, allocation of responsibility, accountability, vigor and example in leadership and planning).

MORT DOE Guidelines

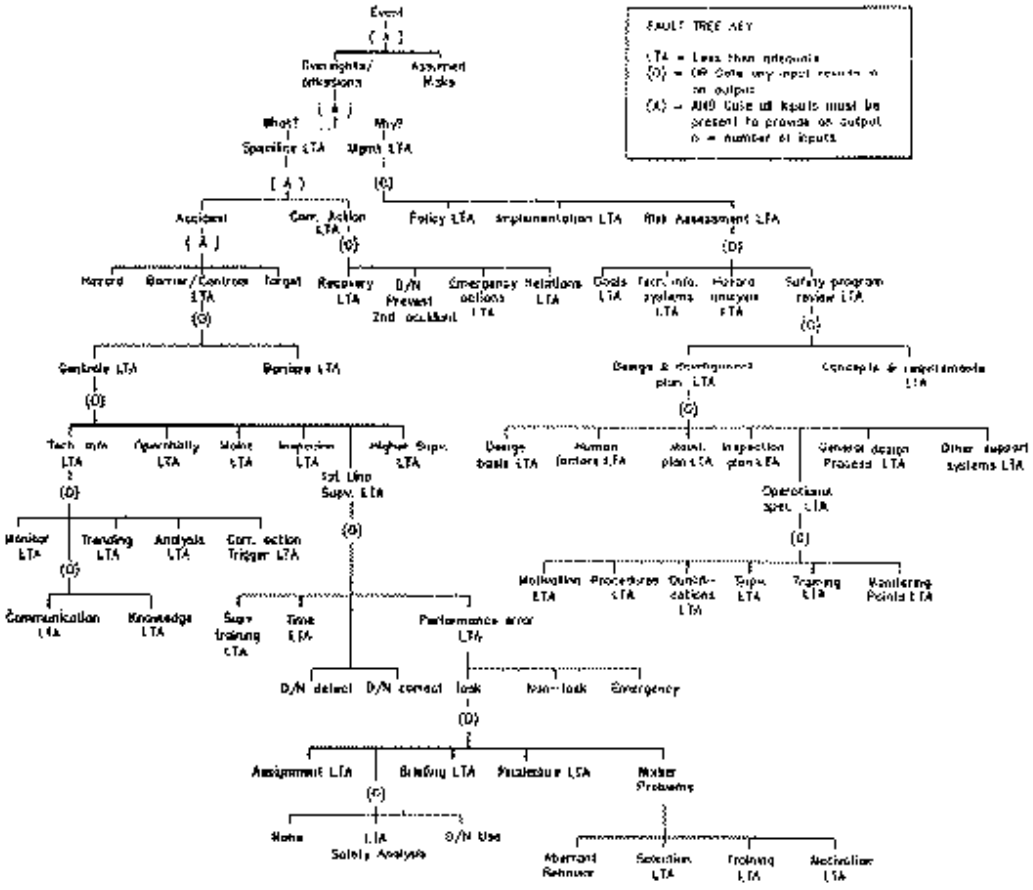
Cause definitions used with this method are similar to those in DOE Order 5000.3A:

- A cause (causal factor) is any weakness or deficiency in the barrier/control functions or in the administration/management functions that implement and maintain the barriers/controls and the plans/ procedures.
- A causal factor chain (sequence or series) is a logical hierarchal chain of causal factors that extends from policy and policy implementation through the verification and implementation functions to the actual problem with the barrier/control or administrative functions.
- A direct cause is a barrier/control problem that immediately preceded the occurrence and permitted the condition to exist or adverse event to occur. Since any element on the chart can be an occurrence, the next upstream condition or event on the chart is the direct cause and can be a management factor. (Management is seldom a direct cause for a real-time loss event such as injury or property damage but may very well be a direct cause for conditions.)

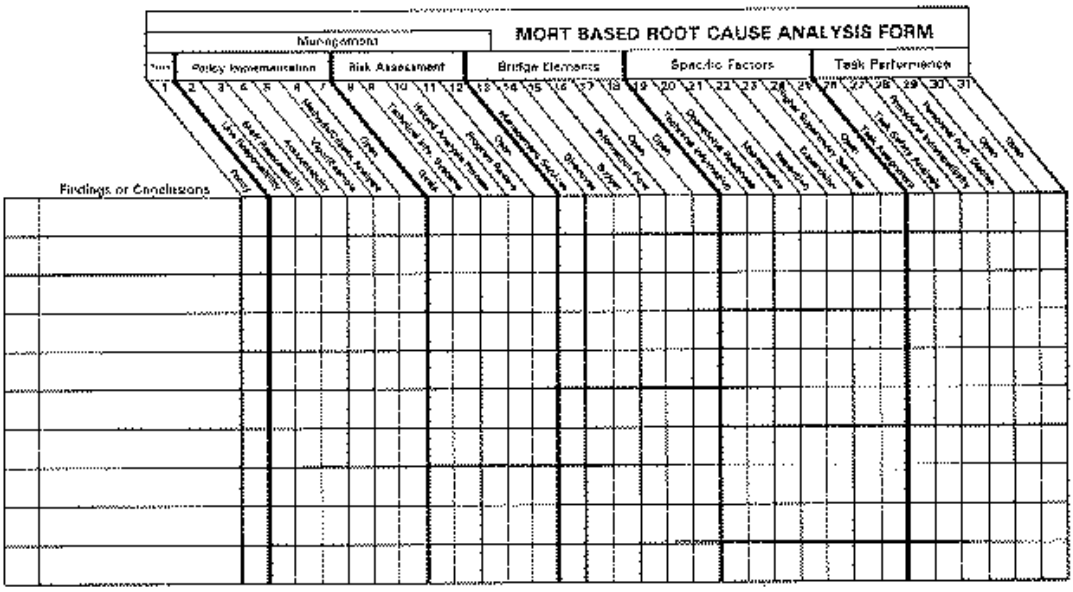
MORT DOE Guidelines

- A root cause is the fundamental cause which, if corrected, will prevent recurrence of this and similar events. This is usually not a barrier/control problem but a weakness or deficiency in the identification, provision, or maintenance of the barriers/controls or the administrative functions. In the context of DOE Order 5000.3A, a root cause is ordinarily control-related involving such upstream elements as management and administration. In any case, it is the original or source cause.
- A contributing cause is any cause that had some bearing on the occurrence, on the direct cause, or on the root cause but is not the direct or the root cause.

MORT DOE Guidelines



MORT DOE Guidelines



MORT Case Study

- US DOE Report RL 97-58.

- www.hanford.gov/safety/accident/can_stor/iron-acc.htm
Worker Injury at the Canister Storage Construction Site

MORT Case Study

Under contract to the DOE-RL, Fluor Daniel Hanford (FDH) through its contractor, DE&S Hanford (DESH), was constructing the CSB. DESH used Fluor Daniel Northwest, Inc. (FDNW) to provide construction management and safety oversight services and Mowat Construction Company to construct the CSB.

The CSB will provide interim storage for spent nuclear fuel. The fuel will be stored in a below-grade vault portion of the building in vertical through-the-floor surface tubes. The deck over the vault was complete and construction of the above-grade portions of the building was in progress. This included the placement of several large steel columns. The two columns involved in the accident were 15.85 meters (52 ft.) long and weighed about seven metric tons.

After completing a design change which involved rolling and welding on four of the columns, the ironworkers were moving a column to the deck of the CSB when the accident occurred. This was at approximately 1505 hours on Wednesday, May 7, 1997.

MORT Case Study

When the column was being lowered, the end near the crane came to rest on the ground, on the gusset at an angle slightly away from the ironworker. The ironworker entered between the column being lowered and a second, stationary column.

As the far end of the column settled, the column rotated around the point where the gusset contacted the ground. The ironworker felt with his hand the column rotating toward him, but he did not think it would continue to the point where he was in danger. As soon as he realized he was being pinched between the columns, he attempted to free himself. It was too late, and the result was a fractured pelvis. The ironworker foreman and crane operator saw this occur. The ironworker foreman signaled the crane operator who was already taking actions to lift the column. The injured ironworker was taken to Kadlec Medical Center hospital, Richland, Washington, where he was admitted and diagnosed as having a fractured pelvis. He was released on May 12, 1997, to convalesce at home, and should be fully recovered in four to six months.

MORT Case Study

The Board identified three root causes for the accident. Eliminating these would have prevented the serious injury.

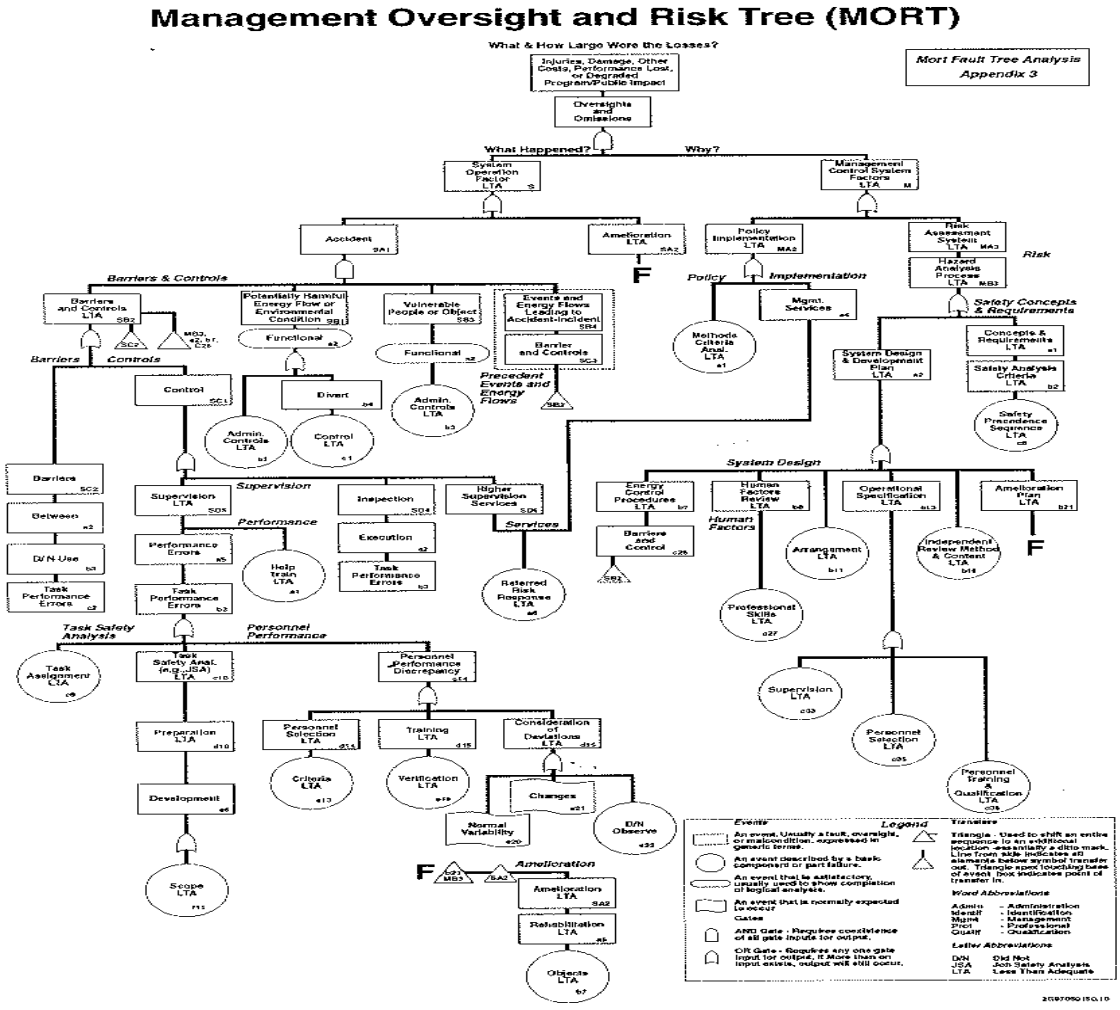
- Failure to have adequate task safety analysis – The safety analysis did not address the hazards that led to the accident.
- Failure to have adequate personnel training – The personnel were experienced, but their experience was not reinforced by specific training required by the safety program.
- Failure to have adequate oversight – Contractor inspections and DOE-RL oversight did not identify the hazards that led to the accident.

MORT Case Study

In addition, seven contributing causes were identified:

- The dunnage was not in place when the load was lowered.
- An adequate supply of dunnage material was not available at the work site.
- The area was too congested.
- An insufficient number of workers were involved in rigging the columns.
- The rigging was set too far from the ends of the column.
- The ironworker did not understand his role as rigger during the pre-job briefing.
- The ironworker was not attentive during the pre-job briefing.

MORT Case Study



MORT - Analysis

- It guides you.
- Good focus on managerial failure.
- But weak on other human factors.
- Weak on social factors (politics?)

Conclusions

- Very effective epsf hoc.
- DOE guidance on accidents.
- But how to design better systems?
- Next... requirements elicitation.

Requirements and Safety Cases

- Safety Requirements.

- MOD Procurement example.

- Safety cases.

Requirements Analysis

- See software engineering courses.

- A brief recap.

- What a system should do.

- Not how it does it.

Requirements Analysis

- Stage 1:

- Functional requirements analysis.

- Stage 2:

- safety requirements analysis;
- eg. hazard and risk analysis;
- see previous section on 61508.

Requirements Analysis

- All leads to a specification.

- Informal, semi-formal, formal?

- Verification:

- does system meet requirements?

- Validation:

- are requirements appropriate?

Requirements Analysis

In conjunction with the implementation of Smart Procurement, MOD intends to adopt a new method of capturing, engineering and managing requirements based on the principles of Systems Engineering. It is to be called Smart Requirements. The key objectives are to introduce a through-life evolutionary requirement process, which will integrate all stakeholders of requirements and facilitate the delivery and sustainment of affordable and effective Defence systems.

The new requirements process will entail major changes to project procedures and documentation, for which MOD staff will require appropriate preparation, training and support.

- http://www.mod.uk/policy/smart/reqs.htm

UK MOD SMART requirements.

Requirements Analysis

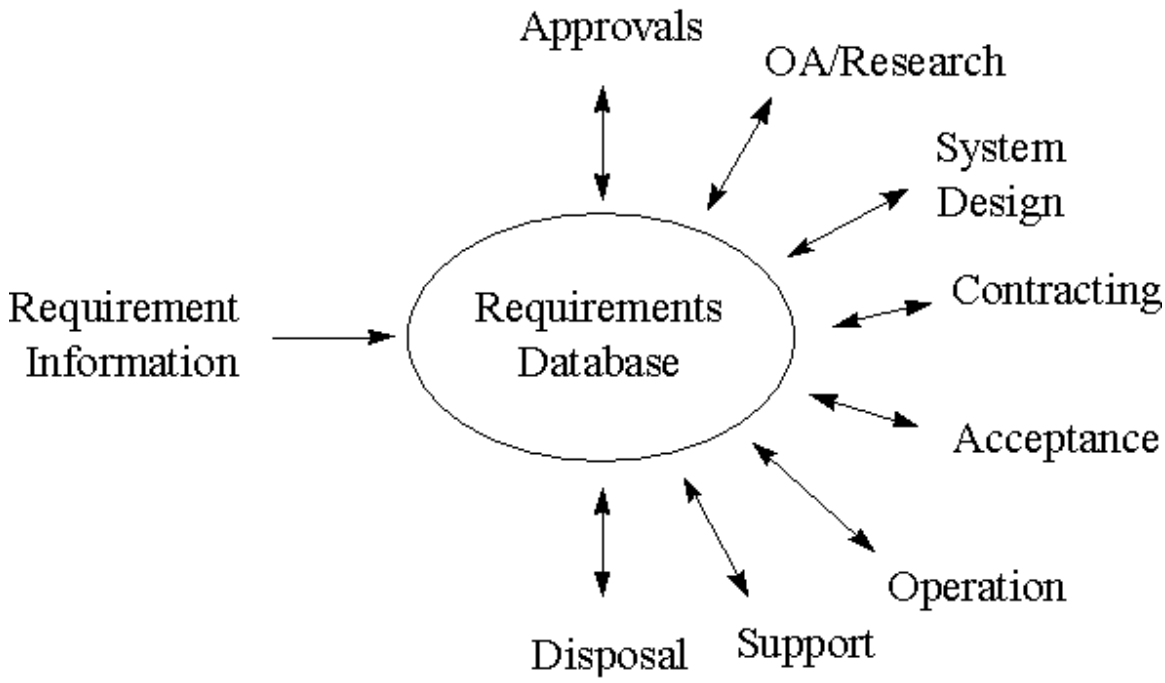
7. Smart Requirements, the new method of capturing, engineering and managing operational requirements, is based upon the principles of Systems Engineering. The key changes from the present "Purple Book" process are:

- a. A complete and consistent Requirement is defined but is split into User 1 and System 2 Requirements Documents (URD and SRD) reflecting user needs in the former and refining requirements on the system to fulfil those needs in the latter.
- b. The URD is updated as necessary throughout the life of the system to reflect both evolving user needs and changing assumptions. However, the URD will be baselined as necessary in order to allow project approval to take place. In particular, a baselined version of the URD, known as the Higher Level URD (HL URD) will form the Statement of Mission Needs, which will allow the development of equipment options for Initial Gate Approval.
- c. The SRD will be developed up to Main Gate, where it will be baselined for approval. Thereafter, it will be updated only as a result of trade-off decisions agreed between the Customer and the IPT leader, or later when required as the basis for in-service upgrades.

Requirements Analysis

- d. Initial or Main Gate approval, the user and system requirement can be presented in an appropriate depth and scope from the underlying information base in a suitable format. Such documentation would be in the nature of a "snapshot" of the instantaneous state of the overall project requirement and would be uniquely defined and configured.
- e. Each user or system requirement is specified in terms of a single, unique and unambiguous statement, rather than the flowing textual nature of current requirements. User requirements include a statement of how, in general terms, the requirement will be verified. Each system requirement includes defined acceptance criteria.
- f. The linkage between atomised user and system requirements must be maintained by the IPT. System requirements are used as the basis of the contract with the supplier, and the linkage between the system design must be maintained by the supplier and the IPT. This will allow the impact of changes in the user requirement to be traced to the affected system requirements and system design, and to enable trade-offs in system requirements and system design to be traced back to user requirements. Linkages within the URD and SRD must also be identified, in order that interactions can be monitored.

Requirements Analysis



Requirements Analysis

10. Specify Constraints. Constraints do not add extra capability but affect the quality of the results provided and restrict the solution space. Examples are budget, implementation date, safety & security policies and legislation. Where constraints apply only to specific capabilities, they should be linked. However, many will be general, recognising that their impact on the system will be specifically addressed as system non functional requirements.

Requirements Analysis

5. Specify Non-Functional Requirements. Non functional requirements are constraints on the system design. They may arise from user requirements, technical disciplines or the external environment. They are often "ilities", can be divided into product or support constraints and include the following areas:

- reliability
- maintainability
- operability
- safety
- security
- engineering standards
- environment
- support

Non-functional requirements are often expensive but add quality. Early identification will avoid costly changes and facilitate the trade-off process leading to a cost-effective solution. Blanket application of individual non-functional requirements will be unnecessarily costly and should be avoided. They should be identified against and linked to the lowest level function in the decomposition to which they specifically apply. Non-functional requirements should also be expressed as unique statements of requirement with the same attributes as system functions.

Requirements Analysis

- Now for some differences.

- Requirements - what a system does

- But regulators want more.

- Why is a system acceptable?

- need for a SAFETY CASE.

Safety Cases

New arrangements were introduced to coincide with the re-structuring of the railways after privatisation. Those involved in providing infrastructure or operating train services have to prepare a safety case setting out:

- safety policy and objectives;
- a risk assessment;
- safety management systems;
- risk control measures.

The Inspectorate considers and accepts (as appropriate) safety cases submitted by companies which control and manage infrastructure. Train operators' safety cases are submitted to the relevant infrastructure controller but are seen by the Inspectorate to ensure that they are properly considered. Guidance on the Railway (Safety Case) Regulations 1994 is available.

- HSE Railways Directorate

What's in a Safety Case?

- http://www.hmso.gov.uk/si/si1999/19990743.htm

The Control of Major Hazard Accident Regulations 1999

PURPOSE AND CONTENTS OF SAFETY REPORTS

PART 1

Purpose of safety reports

(This Part sets out the provisions of Article 9(1) of the Directive)

The purposes referred to in regulation 7 are as follows -

- demonstrating that a major accident prevention policy and a safety management system for implementing it have been put into effect in accordance with the information set out in Schedule 2;
- demonstrating that major accident hazards have been identified and that the necessary measures have been taken to prevent such accidents and to limit their consequences for persons and the environment;

What's in a Safety Case?

- demonstrating that adequate safety and reliability have been incorporated into the -
  - design and construction, and
  - operation and maintenance,

  of any installation and equipment and infrastructure connected with its operation which are linked to major accident hazards within the establishment;
- demonstrating that on-site emergency plans have been drawn up and supplying information to enable the off-site plan to be drawn up in order to take the necessary measures in the event of a major accident;
- providing sufficient information to the competent authority to enable decisions to be made in terms of the siting of new activities or developments around establishments.

What's in a Safety Case?

PART 2

Minimum information to be included in safety report

(This Part sets out the provisions of Annex II to the Directive)

The information referred to in regulation 7(1), (5) and (7) is as follows -

- Information on the management system and on the organisation of the establishment with a view to major accident prevention.

This information shall contain the elements set out in Schedule 2.

- Presentation of the environment of the establishment:
- description of the site and its environment including the geographical location, meterological, geographical, hydrographic conditions and, if necessary, its history;
- identification of installations and other activities of the establishment which could present a major accident hazard;
- description of areas where a major accident may occur.
- Description of installation:
- a description of the main activities and products of the parts of the establishment which are important from the point of view of safety, sources of major accident risks and conditions under which such a major accident could happen, together with a description of proposed preventive measures;

What's in a Safety Case?

- description of processes, in particular the operating methods;
- description of dangerous substances:
- inventory of dangerous substances including -

  - the identification of dangerous substances: chemical name, the number allocated to the substance by the Chemicals Abstract Service, name according to International Union of Pure and Applied Chemistry nomenclature; - the maximum quantity of dangerous substances present;
- physical, chemical, toxicological characteristics and indication of the hazards, both immediate and delayed for people and the environment;
- physical and chemical behaviour under normal conditions of use or under foreseeable accidental conditions.

What's in a Safety Case?

- description of processes, in particular the operating methods;
- Identification and accidental risks analysis and prevention methods:
- detailed description of the possible major accident scenarios and their probability or the conditions under which they occur including a summary of the events which may play a role in triggering each of these scenarios, the causes being internal or external to the installation;
- assessment of the extent and severity of the consequences of identified major accidents;
- description of technical parameters and equipment used for the safety of installations.
- Measures of protection and intervention to limit the consequences of an accident:
- description of the equipment installed in the plant to limit the consequences of major accidents;
- organisation of alert and intervention;
- description of mobilisable resources, internal or external;
- summary of elements described in sub-paragraphs above necessary for drawing up the on-site emergency plan.

What's in a Safety Case?

- HSE ASSESSMENT OF (Nuclear) LICENSEES' SAFETY CASES FOR THE YEAR 2000 COMPUTER PROBLEM

- Why draft this document?

- Why require safety cases here?

What's in a Safety Case?

[mP4] A Y2K project is one of resource and record management; these should be seen to be properly and systematically managed. This, of course, means providing an auditable trail enabling all systems to be unambiguously traced to their eventual outturns. There should be a documented strategy, project plan and Quality Assurance (QA) plan. All activities should be covered by documented procedures and guidance to ensure completeness and consistency. The emphasis of all guidance should be that of positive demonstration with safety as the central focus.

[mP7] Prior to each of the critical dates, the licensee should produce a justifi cation for continued operation (JfCO) beyond each of these critical dates. This justification should show that the inventory was properly established; the investigation was comprehensive and thor ough; the solutions are appropriate (and safe) and properly tested; and that the contingen cy plans (including supply chain management) are appropriate.

What's in a Safety Case?

[mP34] Licensees should demonstrate that they have contingency plans appropriate to the consequences of major plant failure. These should recognise the possibility of widespread disruption of a licensees own internal infrastructure caused by multiple failures in seemingly non-safety related systems, or the possible disruption of the industrial infrastructure of the UK. Both of these events will place very high demands on staff in licensees organisations, with indirect detriment to safety. There should be adequate procedures and guidelines in place covering the production of contingency plans.

What's in a Safety Case?

[mP35] Licensees should demonstrate that their staffing levels, and staff competencies and levels of authority will be appropriate for the potential risk and consequences over each critical date associated with the millennium change. In each case this should be reviewed and the proposed arrangements shown to be adequate. Staff should be adequately trained in all the plant work-arounds (and changes) prior to the critical dates to which they apply. Staff should also be advised to be alert to potential system malfunction following each of the critical dates and should be aware of, and adequately trained in, the actions that should be taken in the event of the failure of any system.

[mP36] Evidence should be provided that all necessary external supplies have been secured prior to each critical date such that the need to re-order does not occur during the associated critical period. This may include the licensees establishing that their suppliers of safety significant items

Maintenance of Safety Cases

"A person who has prepared a safety case persuant to these regulations shall revise its content whenever appropriate" UK Railways Safety Case regulations 1994 [Regulation 6(1)]

"After the preparation of the operational Safety Case any ammendments to the deployment of the system should be examined against the assumptions and objectives contained in the safety case" Ministery of Defence Safety Standard 00-55, Section 4.7.1.

T. Kelly and J. McDermid, ¡I¿A Systematic Approach to Safety Case Maintenance¡/I¿. In M. Felici, K. Kanoun and A. Pasquini (eds), Computer Safety, Reliability and Security, Springer Verlag Lecture Notes in Computer Science 1698, 1999.

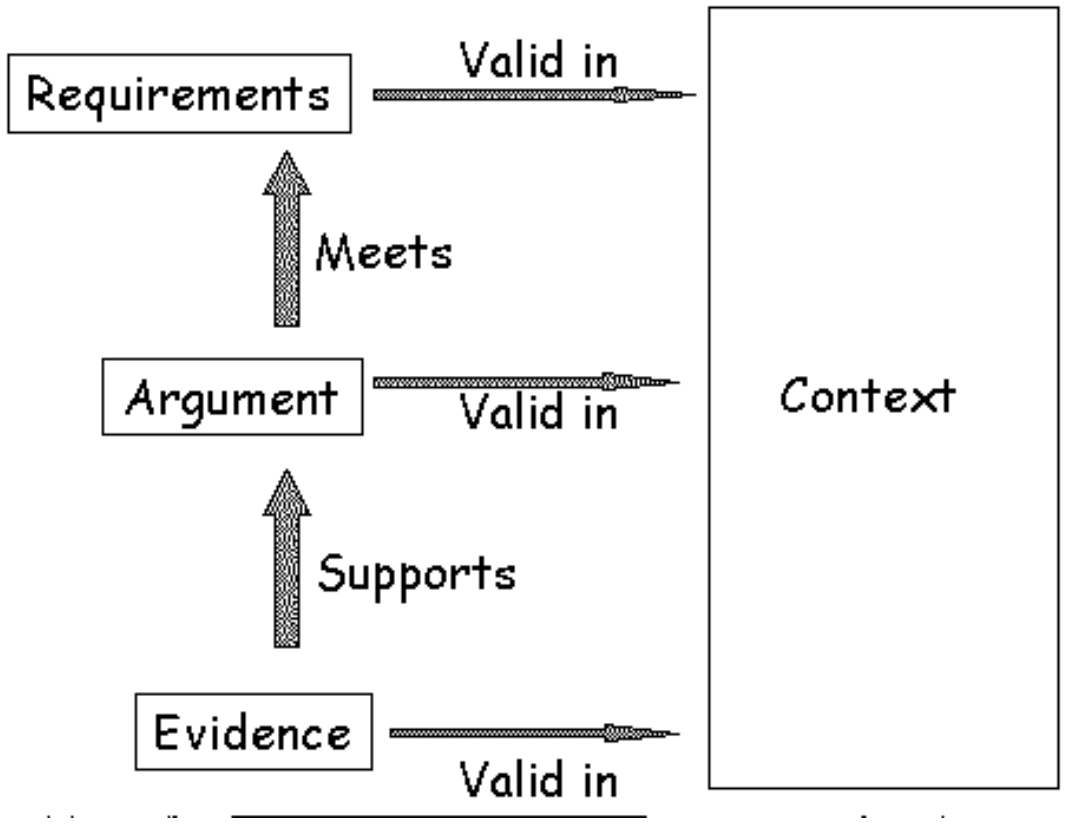
Maintenance of Safety Cases

- Safety cases include:

requirements - safety objectives;
evidence - study of reliability;
arguments - evidence meets requirements;
context - assumptions for argument.

- See Kelly and McDermid.

Components of a Safety Case



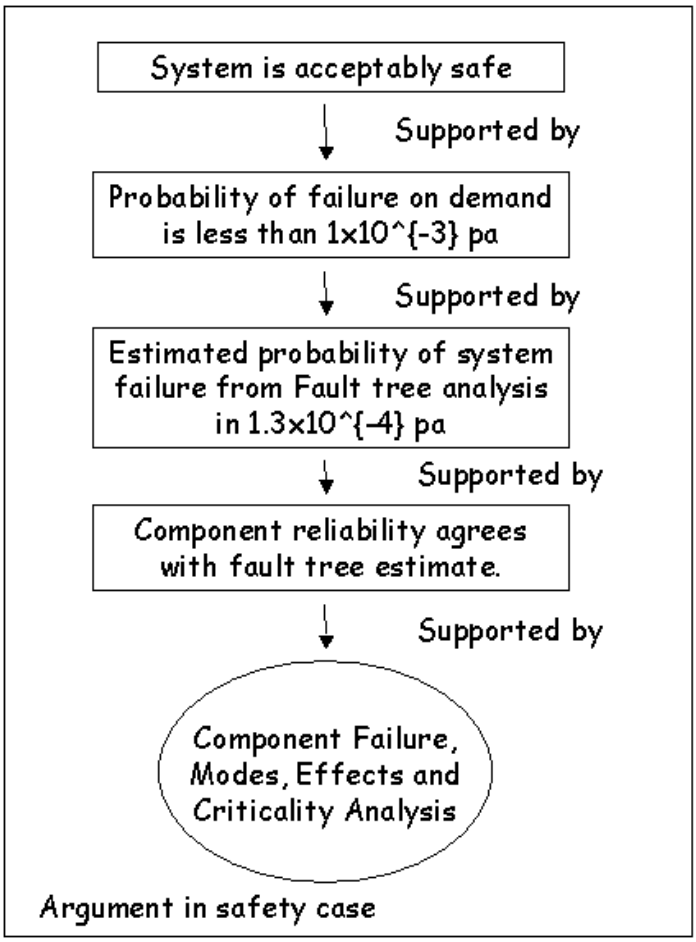
Problems in Maintenance of Safety Cases

- Hard to recognise challenges:
small changes $\rightarrow$ big safety effects.

- Knock-on effects of change:
change affects many arguments.

- Insufficient information on change:
different staff? Teams? Managers?

Problems in Maintenance of Safety Cases



- Assess damage to case then recover.

Conclusion

- Requirements document:

explain what system should do.

- Safety cases:

explain why it meets requirements.