HSE
Health & Safety
Executive

Learning from incidents involving E/E/PE systems

Part 1 - Review of methods and industry practice

Prepared by **Adelard** for the
Health and Safety Executive 2003

RESEARCH REPORT 179

Learning from incidents involving E/E/PE systems

Part 1 - Review of methods and industry practice

PG Bishop, RE Bloomfield, LO Emmet
Adelard LLP

C Johnson
University of Glasgow

W Black
Blacksafe Consulting

V Hamilton
V Hamilton Associates

K Koorneef
Technical University of Delft

This report is the first of 3 parts presenting the results of an HSE-sponsored research project. The overall purpose is to create a scheme for learning from incidents that involve electrical, electronic or programmable electronic (E/E/PE) systems. Part 1 (this report) reviews existing learning processes and causal analysis techniques, examines industry practice and makes recommendations for a new scheme. Part 2 presents the recommended scheme and Part 3 gives accompanying guidance, examples and rationale.

This report and the work it describes were funded by the Health and Safety Executive (HSE). Its contents, including any opinions and/or conclusions expressed, are those of the authors alone and do not necessarily reflect HSE policy.

HSE BOOKS

First published 2003

ISBN 0 7176 2787 X

ACKNOWLEDGEMENTS

Adelard LLP wishes to acknowledge numerous invaluable contributions to the project from the following people: Chris Johnson (Glasgow University), Bill Black (Blacksafe Consulting), Mark Bowell (HSE), Konstantinos Tourlas (Adelard), Viv Hamilton (Viv Hamilton Associates), Floor Koornneef (Technical University of Delft).

EXECUTIVE SUMMARY

This report is the first of 3 parts presenting the results of an HSE-sponsored research project. The overall purpose is to create a scheme for learning from incidents that involve electrical, electronic or programmable electronic (E/E/PE) systems. Part 1 (this report) reviews existing learning processes and causal analysis techniques, examines industry practice and makes recommendations for a new scheme. Part 2 presents the recommended scheme and Part 3 gives accompanying guidance, examples and rationale.

The initial requirements are for a scheme that can be adopted by companies and organisations to help them learn from incidents that involved E/E/PE systems. This should fit with existing safety and quality management systems, should allow for different levels of maturity and organisational complexity and should satisfy legal and regulatory requirements. The scheme should be applicable to a wide range of sectors, including oil and gas, chemical process, machinery, nuclear and railways, and should cover varying roles including end users, system designers and component suppliers. Root causes should be classified using a common taxonomy to aid consistent characterisation, retrieval and analysis and the scheme should enable recommendations to be generated from these root causes.

The consensus behind IEC 61508, and especially the agreed terminology of the standard, will be important in developing a scheme that is widely applicable. In addition the safety lifecycle in IEC 61508 will provide an overall process that can be detailed and refined within the incident learning recommendations.

A wide range of reporting architectures and causal analysis techniques have been proposed in the academic literature and have received at least limited industrial use. 11 causal analysis techniques are summarised under the following categories: elicitation and analysis techniques, event-based techniques, flow charts and taxonomies, accident models and argumentation techniques.

The project carried out structured interviews with 10 companies and organisations from the pharmaceutical, nuclear, oil and gas, chemical process, marine, rail and machinery sectors. Roles included end users, designers, maintainers, procurers, assessors, system suppliers and component suppliers.

The consultations reveal that supply chain and information sharing is impeded by industry fragmentation. An organisation’s most significant technical influence over contractors is the standards used for project development, which tend to be widely available (such as IEC 61508) rather than company-specific. Reliance on contractors leads to problems in ensuring sufficient in-house competence and experience. The design history for existing systems is rarely available.

Existing end-user schemes are generic and do not contain in-built specialised elements for focussing on E/E/PE systems. Only a small fraction of reported incidents involve a special investigation of E/E/PE system failure. For example, one company had 750 incidents per year, 6 were investigated in detail and only one involved this kind of special investigation. End user organisations often find it difficult to determine whether E/E/PE systems should be implicated in an incident.

More than one company observed that implementation of more rigorous reporting schemes increased the incident reporting rate, but the serious accident rate reduced, suggesting that

there was previous under-reporting. Most companies have non-confidential reporting schemes.

Causal analysis techniques used include: timelines, event trees and checklists; a method similar to TRIPOD (accident trees plus structured checklists); event-based/event chain causal analysis; and ad-hoc approaches such as textual elaboration by designated experts. The E/E/PE system suppliers interviewed do not use any specific method.

Large companies have up to four levels of internal incident enquiry depending on severity, eg trivial, local, formal investigation, formal enquiry, with different levels of investigation and different personnel at each level. Typically for large companies there are many thousands of trivial incidents per year but less than ten of these result in the most stringent type of enquiry.

Some companies classify incidents according to type (for subsequent monitoring and trend analysis). However there is rarely any formal classification scheme of incident causes – the priority is to identify necessary changes in product, procedures or personnel competence.

Recording of incidents, analyses and tracking of safety recommendations is quite sophisticated in some large companies and is implemented independently of other systems. However small companies tend to use existing QA systems for this purpose.

Some companies have explicit mechanisms for reviewing and generalising incidents into recommendations. Experience is fed back into the design rules and business processes, and is often disseminated more broadly to other sites, trade bodies and regulators. Tools, such as databases, intranets, bulletin boards and e-mail, aid dissemination.

CONTENTS

FIGURES

TABLES

1 INTRODUCTION

IEC 61508 is a key standard for industry as it sets out specific requirements for E/E/PES systems within a generic framework that defines the safety lifecycle and safety management activities that should be followed. One of these requirements is the need to learn from experience, with 6.2.1 of IEC 61508-1 stating that responsible organisations or individuals should consider specifying, implementing and monitoring the progress of:

> *6.2.1 i) the procedures which ensure that hazardous incidents (or incidents with potential to create hazards) are analysed, and that recommendations are made to minimise the probability of a repeat occurrence.*

This requirement addresses a range of safety stakeholders including the developers and operators of safety-related systems.

In addition IEC 61508-2 requires that:

> *7.8.2.2 Manufacturers or system suppliers which claim compliance with all or part of this standard shall maintain a system to initiate changes as a result of defects being detected in hardware or software and to inform users of the need for modification in the event of the defect affecting safety.*

So a requirement to respond to incidents is placed on the “supply chain” of system suppliers and product manufacturers.

These requirements represent goals to be achieved, and as is often the case with goal based regulation, leaves questions undecided about how this should be done. The implementation details will depend on the organisation that is trying to learn, its maturity in terms of data collection and analysis, and the criticality of the systems that it is responsible for.

In designing a scheme to meet these requirements, we face problems providing a useable scheme that can be tailored to the sector or application of interest. The consensus behind IEC 61508, and especially the agreed terminology of the standard, will be important in developing a scheme that is widely applicable. In addition the safety lifecycle in IEC 61508 will provide an overall process that can be detailed and refined within the incident learning recommendations.

In this first part we:

- Establish the requirements for the scheme (Sections 2 and 3).

- Review current schemes for incident recording, analysis and learning that can contribute to the design of a new scheme (Section 4 and Appendix A).

- Report on the consultations with industry to determine what methods are currently in use for learning from incidents (Section 5 and Appendix B).

- Review the results and make recommendations for the scheme (Sections 6 and 7).

2 REQUIRED SCHEME FEATURES

These features were developed in discussion with HSE.

2.1 STUDY REQUIREMENTS

The client for our report is HSE. Our report will be used in developing HSE guidance, but it is not the guidance itself. As such, promotional aspects to ensure adoption are peripheral issues. However the study should identify, and mitigate where possible, potential barriers to adoption, such as:

- Cost and time to implement and operate the scheme.

- Complexity/usability of the scheme.

- Need to integrate with existing schemes.

The study documentation should provide a rationale that gives the thinking behind the scheme that is produced. In addition the project will maintain an on-going record of issues considered, and reasons following particular paths at decision points.

2.2 CHARACTERISTICS OF THE E/E/PES-RELATED REPORTING SCHEME

2.2.1 Operational environment

1 The scheme should link to existing systems, not just to existing incident reporting and analysis but also to safety management systems, control logging, risk management etc.

2 The scheme has to be implementable by industry – and allow an evolutionary approach.

2.2.2 Client community

3 We assume the client community will at least comply with RIDDOR. However this does not necessarily imply that there is a pre-existing incident recording and analysis scheme internal to the company (for example, RIDDOR allows telephone reporting as a minimal reporting interface).

4 The scheme should be applicable to organisations at different levels of maturity and organisational complexity.

2.2.3 Specialisation for E/E/PES

5 The scheme should use terminology and concepts from IEC 61508 as a basis, but should not be bound completely to this if certain aspects are not fully covered or if we consider the standard’s terminology to be a barrier to the target user’s understanding. The scheme should not depend on detailed knowledge of IEC 61508 or on the technical terms used within it.

6 The scheme should cover E/E/PES users, E/E/PES system designers and E/E/PES product suppliers.

7 The scheme should fit in with existing incident reporting and analysis schemes although the focus of our study is on E/E/PES specific aspects. (We might need to develop process models after the consultation to help define the interface between general and E/E/PES specific aspects and also between the core guidance and wider issues such as incident reporting, incident investigation, and process improvement).

8 The scheme needs to identify necessary "pre-conditions", ie elements for incident recording and analysis that are needed before it can be specialised for E/E/PES related incidents.

9 The scheme should identify where an E/E/PES is involved in an incident, and whether changes in E/E/PES related aspects (taking a wide interpretation equivalent to the scope of all IEC 61508 requirements, eg training, process, management etc) could have averted or contained the incident.

2.2.4 Scheme Design

10 The scheme should take account of the criticality and potential consequence of the incident. The measure of criticality will depend on the scheme user. Vendors may measure this by safety integrity level, users by consequence.

11 The core scheme should be concrete (to simplify implementation – especially for smaller companies, and to improve comparability), eg state overall principles, implementation approach, and example forms, etc, that can be adopted by clients.

12 The duty holder's viewpoint has to be established and addressed when devising the scheme. Note that a duty holder organisation is likely to have several roles to consider.

13 The scheme should be based on current industry practice and emerging practice where relevant.

14 The scheme should cover recursive causal analysis, but provide guidance on when to "stop". In particular it should encourage consideration of root causes rather than taking a "sticking plaster" approach.

15 The scheme should include the generation of recommendations from identified root causes.

16 The scheme should address confidentiality issues (of reporter, incident details, causal analysis, etc).

17 The scheme should consider how to make learning the lessons effective, so that lessons learned through incidents in one system are used to prevent the incident being repeated in others.

2.2.5 HSE data consistency requirements

18 The scheme should have a common taxonomy to aid consistent characterisation, retrieval and analysis, but not be restrictive, eg by making use of free text and/or allowing sub-classifications. Nonetheless, it is believed that a common causal taxonomy is likely to be most important in achieving consistency within a domain.

19 Repeatability of reporting and analysis is a desirable goal, but not at the expense of coverage or consistency.

2.2.6 Scheme implementation

20 The scheme should include recommendations on necessary competence (eg recommend the use of teams in causal analysis to ensure good coverage of viewpoints, including people with enough knowledge of the operational context, etc). Causal analysis (techniques, teams used, formality of approach, validation etc) should be proportional to the potential criticality of the incident. The potential criticality will very often differ from the actual outcome.

21 The scheme should include recommendations on process aspects, such as validation of incident reports and of causal analysis classifications.

22 The scheme should document adoption issues for consideration by the implementer. This should include guidance on cultural factors (eg creating trust for confidential and open systems, encouraging participation) and training.

23 Some guidance should be given on what defines an incident. This could change depending on the perspective of the organisation using the scheme.

3 SCHEME CONTEXT

The overall purpose of incident investigation schemes is to prevent immediate reoccurrence, identify wider lessons (in terms of training and management controls, for example), provide a rough indication of the frequency of adverse events, and inform the design of future systems. Learning from incidents can be viewed as a means of process improvement as illustrated in Figure 1 below.

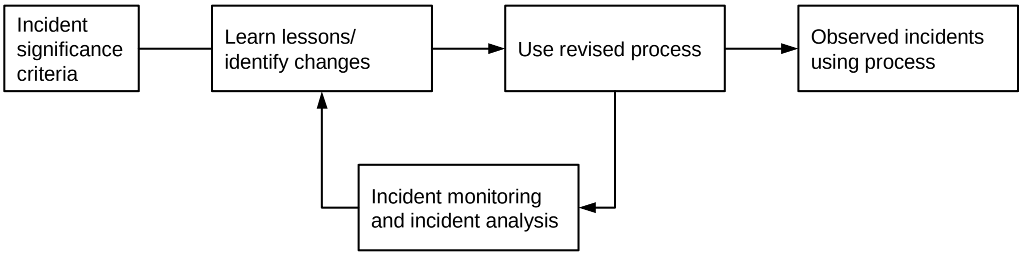

Incident significance criteria
Learn lessons/ identify changes
Use revised process
Observed incidents using process
Incident monitoring and incident analysis

Figure 1 Incident investigation as a means of improving the stakeholder's process

In the context of IEC 61508, this process improvement is related to processes that involve E/E/PES. The stakeholders who could benefit from the feedback of experience from incidents are quite broad and could include:

- end users of E/E/PES
- E/E/PES system integrators
- E/E/PES product suppliers
- procurers of E/E/PES
- trade organisations
- regulators.

The information presented and the responses and time scales will differ for each stakeholder, for example:

- the end user might respond by using alternative systems or changing operational procedures;
- the procurer of E/E/PES might change requirements processes or purchasing and assessment criteria;
- trade organisations and regulators might consolidate this experience into guidance or standards.

In the following sections, we will review the current state of the art in incident recording and analysis and learning from incidents, and present the results of our consultation on current industrial practices.

4 REVIEW OF CURRENT PRACTICE

4.1 INCIDENT INVESTIGATION

Incident investigation has matured over many years [1-4] and the general approach is well established. The overall stages of incident investigation are shown in Figure 2 below.

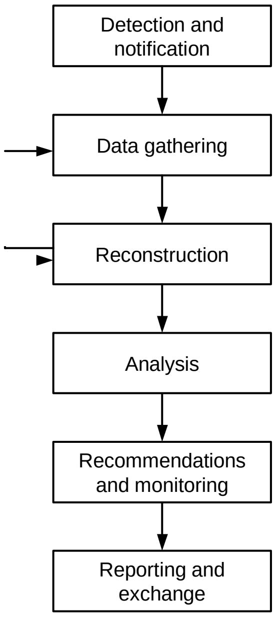


Figure 2 Stages of the investigation

Some investigation methods are applicable to all stages of an incident and its investigation, others are appropriate to only a subset of stages.

It should be stressed that the fairly linear process depicted above covers the lifecycle of a one-incident investigation. The overall incident investigation context is more complex with the development of the incident investigation requirements evolving over time to respond to changes in technology, the operating environment and safety management. For example, after a major accident the collection and detection criteria may change significantly to reflect public concern.

4.1.1 Detection and Notification

A scheme design must recognise that reporting includes a voluntary element; reporting must be encouraged and cultural barriers to reporting addressed. This is a particular issue for the reporting of events and occurrences which can be considered as “weak-signals”, “near-misses” and precursors to more critical incidents, but in which there was no actual loss. Recognition of the prevailing safety and organisation culture (including the peer and supervisory culture) is necessary to understand the complex motivations for reporting in an organisational setting.

Scheme reporting can be open, confidential or anonymous, depending on whether reporters may be deterred from reporting by fear of consequences. External agencies are typically needed for a confidential scheme. Open and confidential schemes have advantages over anonymous ones in that they permit clarification of points of the report with the original reporter after submission. Open schemes where initial submission is to a local supervisor or sponsor allow for that person to add clarification and additional local knowledge to the report before processing. However, such schemes may need an alternative submission route if the report could include shortcomings of the supervisor or sponsor.

Submissions may be paper or electronic and typically are in the form of a first hand account, usually involving completion of a standard form which may include required fields or categories such as: time of event, location, type of equipment, number of casualties (if any) and an initial assessment of the potential criticality.

Schemes frequently have guidelines on what sort of incidents should be submitted. It is desirable to capture "near misses" that have no consequences and other low criticality events. Such schemes are based on the fact that in any human situation, a large number of failures are detected and corrected for every failure that is not corrected and results in adverse consequences. Schemes can be widened in scope to obtain reporting by a wider group, for example the general public or other organisations in the supply chain. Where a gatekeeper or sponsor is part of the architecture of the scheme, their personal reputation or enthusiasm can be a major factor in the success of the scheme.

Where external agencies are used, care is needed to manage the relationship between the agency and local management who must act on recommendations.

Bottlenecks at the submission stage are a potential problem.

Schemes should be monitored to ensure that some groups are not underrepresented as reporters. There may be good reasons for this, eg nurses might be expected to report more than doctors in a medical scheme, because they have more contact with patients. On the other hand it could be because one group is unwilling to report.

4.1.2 Data Gathering

The data gathering stage includes:

- extracting and safeguarding any relevant logs (manual or from automated systems)
- elicitation of testimony from witnesses
- direct interviews
- gathering group testimony, for example through focus groups or anonymous questionnaires

Different organisations approach the investigation phase in different ways. For example, the NTSB uses the "Go teams" concept where a small number of highly trained investigators are always ready for deployment. Once they are deployed they recruit domain specialists to add to the team.

Investigation models [1, 5] may be used at this stage. Investigation models can help direct what information is collected. Investigation methods include:

- Event analysis
- MORT [6]
- Fault Tree Analysis
- Event chains

A problem of this stage is that it is generally impossible to capture all relevant information. Missing information may lead to ambiguity and uncertainty in the analysis.

4.1.3 Reconstruction

Reconstruction focuses on what took place. Accident models may be used in this stage to capture generic aspects of the adverse event. Some models focus on a chain of events, while others look at the changing relationships between the individuals and organisations involved. Timelines are often developed as part of the reconstruction.

As it is impossible to capture all the data in the investigation, there will be missing information in the accident model. In some cases this may lead to uncertainty or ambiguity in the accident analysis and conclusions. Some organisations require their investigators to use judgement about the most likely cause and focus all effort on this scenario. Others favour subjunctive reconstruction (ie reconstruction of alternative scenarios) although this typically uses more resources. Koornneef [7] argues that it is important to have a “learning agency” within the organisation that has sufficient background knowledge to provide missing context in the incidents.

Bias in the investigation team can be a factor and may affect the outcome of the investigation. Bias can arise from:

- *Hindsight bias*. Facts evident after the incident are assumed to have been evident beforehand.
- *Political bias*. The views of one individual or organisation are given undue weight because of their status.
- *Sponsor bias*. The investigator has responsibility for a group or individual who may be adversely affected by the analysis.
- *Professional bias*. Investigators avoid questioning the performance of fellow professionals or their own professional bodies.
- *Recognition bias*. Investigators identify causes that they are most familiar with.
- *Confirmation bias*. Analysts actively interpret evidence to support predetermined hypotheses.

4.1.4 Analysis

This stage is intended to find out “why” a mishap occurred. There are usually feedback loops between the analysis, reconstruction and data gathering stages, as greater understanding causes data from earlier stages to be examined more closely. In the analysis stage, root causes and wider causal factors may be identified [3, 8, 9]. Some analysis approaches distinguish between necessary and sufficient causes. Counter-factual arguments may be used (eg “if X had not been the case then Y would not have happened”).

A prescribed training programme for incident investigators can be used to ensure all investigators within an organisation or domain apply a consistent analysis approach. Analysis methods include:

- MORT [6, 10]
- Event and Causal Factor (ECF) analysis [8]
- TRIPOD [11]
- Why-Because Analysis (WBA) [12]
- STAMP [13, 14]
- PRISMA

More detailed descriptions of these techniques are given in Appendix A.

Investigative, accident and analysis models and methods should have the following properties:

- They should encourage the participation of the many different parties affected by the incident.
- They should be realistic, ie the expressiveness must capture sequential and concurrent aspects.
- They should be definitive and preferably composed of definitive descriptive building blocks that enable investigators to describe the information sources.
- They should be satisfying, ie the model must fit well with the organisation’s overall objectives including research and statutory obligations.
- They should support consistent analysis; otherwise corrective action will provide varying degrees of protection against future hazards.
- They should support inclusion of information about previous failures.

Model notations can be divided into three groups:

- *Formal, mathematical*. These are amenable to mathematical reasoning, but typically can only be used and interpreted by a narrow group of specialists. Often, their expressiveness will be limited to a particular facet of the incident.

- *Semi-formal, graphical*. These have defined syntax but not a formal semantics. They are highly representational and support discussion well but mathematical analysis cannot usually be applied. A popular example is a taxonomy, which can be useful in guiding investigators and providing a common categorisation for analysis across incidents, but flexibility (extension to the taxonomy) is generally required.

- *Natural language*. Natural language is the lowest common denominator. It is used for submission in virtually all cases, supports dissemination to non-specialists and is very expressive. Natural language techniques such as storytelling [15, 16] may also have a role to play in the investigation, reconstruction and analysis stages.

4.1.5 Recommendations and monitoring

Flowing from the incident analysis, actions must be identified and applied. Processes are needed to monitor that corrective actions are completed and are effective. Care must be taken to ensure that the actions respond to the underlying problems rather than to the symptoms. Difficulties are often encountered in driving through deeper structural or managerial changes.

Conclusions and recommendations should be tailored to the needs of the reporting staff. Unless reporting staff see a positive response, they will be discouraged from reporting in the future. Reporting staff should be able to find out about the progress of their reports – ideally, and especially for confidential and anonymous schemes, progress tracking should be automated. Requests for status information can then be anonymous.

4.1.6 Reporting and exchange

The main purpose of this stage is dissemination of the lessons learned. There may be a planned process of efficient exchange of data between local schemes to create an overview at regional, national or international level. Mishap reporting may be integrated into more general systems of lessons learned and management reporting. Measures assessment and trends analysis over several incidents may be undertaken. In the case of large organisations and schemes involving multiple local sub-schemes, the effect of local contextual factors needs to be considered in any cross-scheme analysis.

4.2 SCHEME ARCHITECTURES

While any scheme would have the same stages, the scheme architecture needs to reflect the scale and complexity of information processed. Other factors influencing scheme architecture include the relationship with external stakeholders (especially regulators); relationship with other schemes (eg so that related organisations can also learn from the experience) and protection for confidentiality or anonymity. A wide range of possible scheme architectures are described in [17] and some examples are given below.

Local scheme architectures are appropriate for use within a single user or supplier organisation. Simple architectures are unsuitable for larger schemes because they may experience bottlenecks when a large number of reports are submitted or problems with lack of domain expertise if reports can arise from a large number of different engineering or application sectors.

Figure 3 shows an open, local reporting scheme with corrective action initiated by local management or sponsor (such as a safety group). Lessons may be disseminated via a local newsletter, employee/management briefings, notice boards, websites etc. Corrective action may include maintenance, engineering redesign, process change, retraining, changes to roles and responsibilities etc.

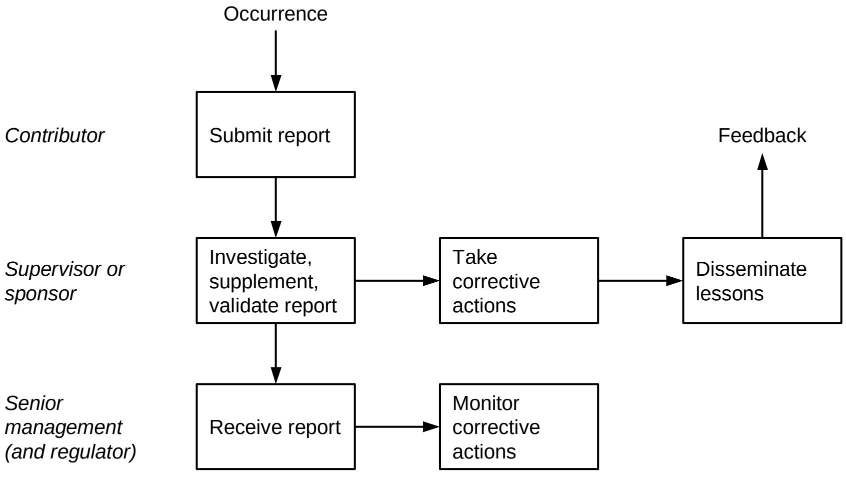


Figure 3 Local architecture

Figure 4 shows a local scheme that supports confidentiality by using an external group to process reports. The external group could be a local university research group, as in the case of the Confidential Incident Reporting and Analysis System (CIRAS) for Scottish train drivers, where reports are processed by Strathclyde University [17]. A confidential, rather than an anonymous, reporting scheme has the advantage that the investigator can follow-up the initial report with the originator to fill in any missing information. In a small organisation or one where roles are highly specialised, confidentiality will be undermined where it is obvious who could have had the knowledge to submit the report. It may be more effective to use an open reporting system provided that cultural factors that would discourage voluntary reporting (eg fear of repercussions, inability to admit mistakes) are first addressed.

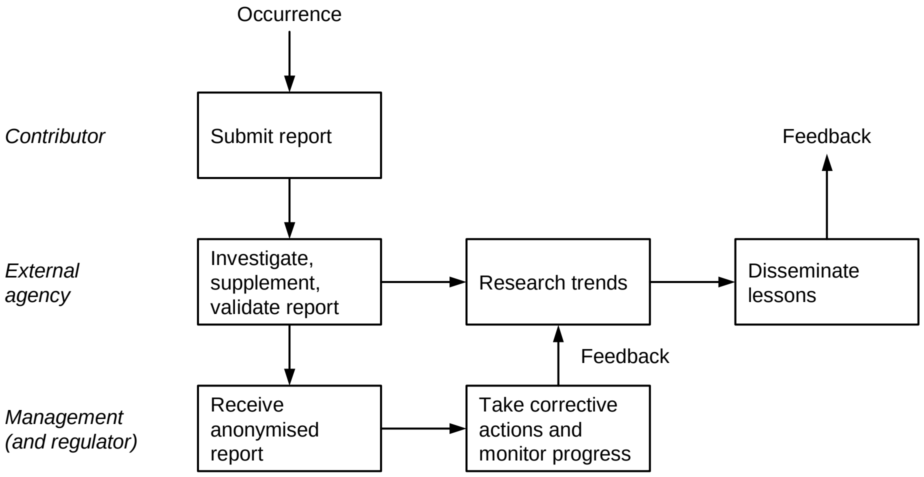

Occurrence
Contributor
Submit report
Feedback
External agency
Investigate, supplement, validate report
Research trends
Disseminate lessons
Feedback
Management (and regulator)
Receive anonymised report
Take corrective actions and monitor progress

Figure 4 Local architecture with confidential reporting

More complicated architectures are needed where there are a number of organisations involved, or the volume, range of expertise, scale and complexity of the incident reporting means that initial investigation needs more than one team. Figure 5 shows one solution: a gatekeeper architecture. The gatekeepers determine which specialist organisation should handle each report. An alternative, confidential submission route (ie direct to the gatekeeper or via an external agency) may be needed if the culture does not support an open scheme.

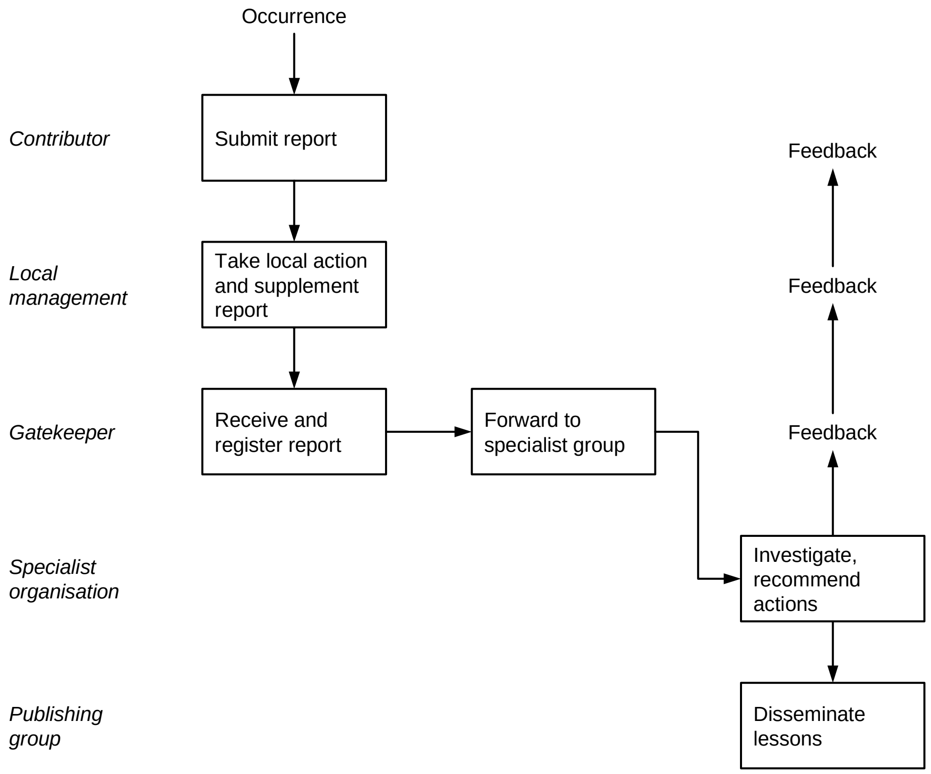


Figure 5 Gatekeeper architecture

There are also more complex architectures that involve the regulator. For example in the USA, medical device problems have to be reported to the regulator as well as the device vendor.

4.2.1 Supply chain dissemination

In the context of E/E/PES related incidents, we also need to consider dissemination to stakeholders in the “supply chain” as shown in Figure 6 below. Note that the dashed boxes represent related activities that are normally under separate control (like the company’s engineering and operations departments). Dashed arrows represent recommendations to the separate departments. The progress of the recommendations is normally tracked as part of the incident handling process.

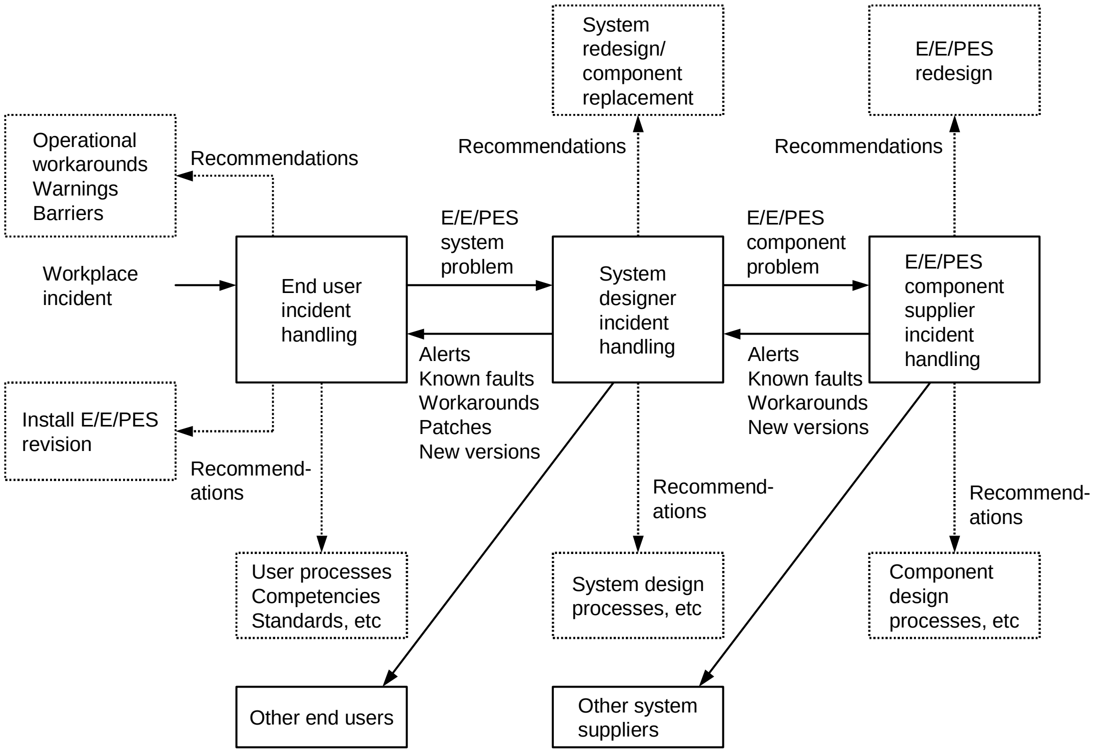
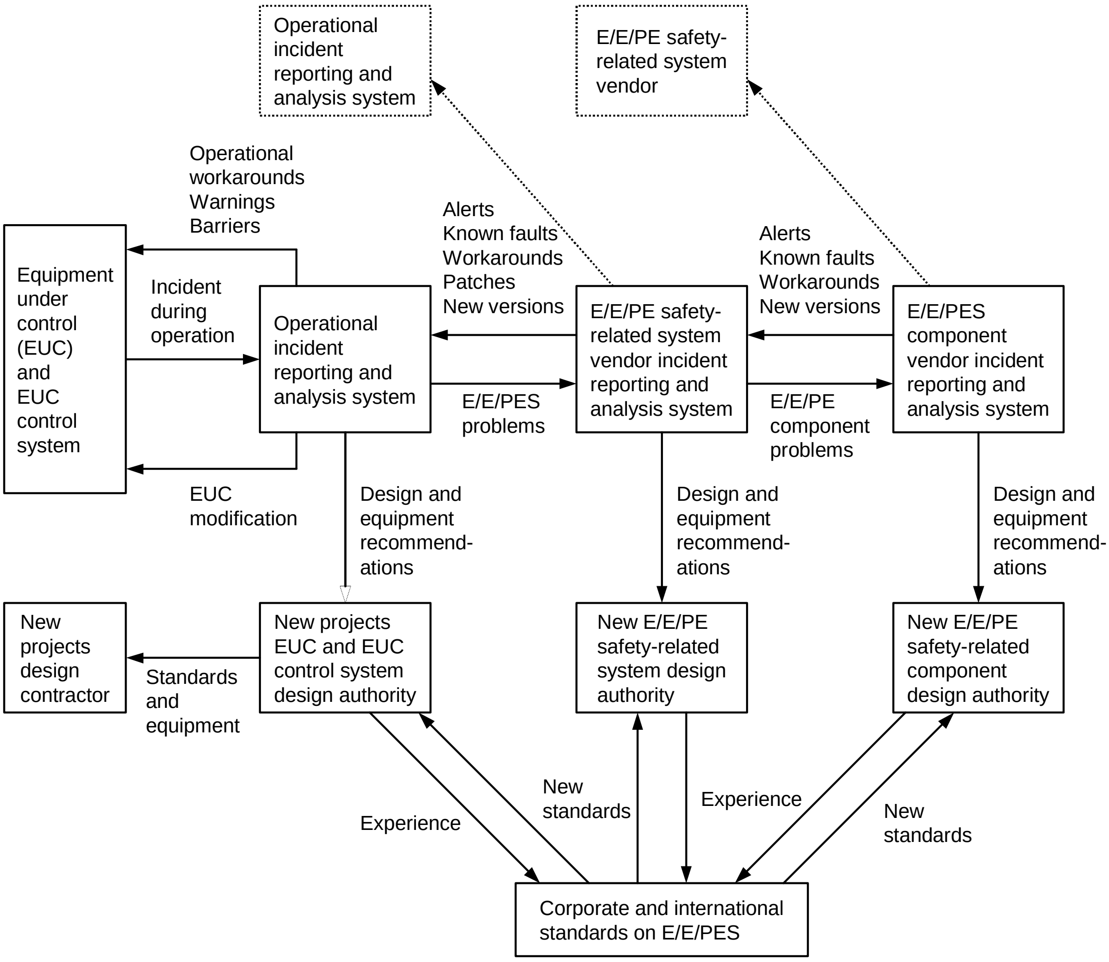

System redesign/ component replacement
E/E/PES redesign
Operational workarounds Warnings Barriers
Recommendations
Recommendations
Recommendations
E/E/PES system problem
E/E/PES component problem
Workplace incident
End user incident handling
System designer incident handling
E/E/PES component supplier incident handling
Alerts Known faults Workarounds Patches New versions
Alerts Known faults Workarounds New versions
Install E/E/PES revision
Recommend-ations
Recommend-ations
Recommend-ations
User processes Competencies Standards, etc
System design processes, etc
Component design processes, etc
Other end users
Other system suppliers

Figure 6 Dissemination through the supply chain

In this scenario, it is assumed that a system designer integrates products on behalf of an end-user. The end-user might introduce immediate measures to control the risk, and also report the problem up the supply chain in order to rectify the problem. If other users are affected then they have to be alerted (particularly if it is a safety-related application). The same process applies for problems with specific products, where the product purchaser is alerted about the problem, and they then alert end-users. This type of notification would be expected in IEC 61508 compliant organisations and could be verified as part of CASS certification.

Incident analysis will lead to recommendations for both local and general changes to the company’s processes, products, procedures, design practices, staff competencies, etc to prevent a recurrence of the problem on future systems (see Section 4.3).

In practice, different structures may be used, especially if the system designer does not provide long-term support (eg due to outsourcing policy by the procurer). In this case the feedback is only indirect, eg via corporate or international standards. This is illustrated in the figure below.



Operational incident reporting and analysis system
E/E/PE safety-related system vendor
Operational workarounds
Warnings
Barriers
Alerts
Known faults
Workarounds
Patches
New versions
Alerts
Known faults
Workarounds
New versions
Equipment under control (EUC) and EUC control system
Incident during operation
Operational incident reporting and analysis system
E/E/PE safety-related system vendor incident reporting and analysis system
E/E/PES component vendor incident reporting and analysis system
E/E/PES problems
E/E/PE component problems
EUC modification
Design and equipment recommend-ations
Design and equipment recommend-ations
Design and equipment recommend-ations
New projects design contractor
Standards and equipment
New projects EUC and EUC control system design authority
New E/E/PE safety-related system design authority
New E/E/PE safety-related component design authority
Experience
New standards
Experience
New standards
Corporate and international standards on E/E/PES

Figure 7 Oil and gas supply chain with indirect feedback of experience

4.3 LEARNING THE LESSONS

There are three areas in incident analysis schemes where learning is important:

1 Learning the lessons locally so that actions are taken to ensure that the incident is not repeated.

2 Learning lessons more widely so that lessons from other systems are applied and lessons from local experience are disseminated and acted upon.

3 The learning involved for the people who carry out the investigation – ie in ensuring that the investigators are able to absorb and understand the new information that they uncover in the course of the investigation and how the process of participating in the investigation affects their behaviour later on.

4.3.1 Learning lessons locally

The final stage of the incident investigation process is communication. The output of the investigation must be in a format and style that communicates to the stakeholders.

- For managers: a suitably summarised report that communicates the essential messages. These will include: what went wrong; how serious it might have been; the successes and failures of the systems and processes involved; the recommendations to avoid future incidents.

- For safety records, regulators, researchers etc: the full documentation in technical detail of the investigation and its findings.

- For operators, system developers etc:

  - Translation of the findings into a format and style that is accessible to them at a time when they might be the cause of (or a means of avoiding) future incidents. This could include checklists, updated (or new) procedures, data sheets, rules within computer-aided design tools etc.

  - Training/education materials. This could include guidance on new processes, training simulations or exercises, using scenarios based on previous incidents, and presentations (electronic or face-to-face) that tell the story of an incident from the investigators' perspective and/or from those involved (reconstructions or personal accounts). Training materials must be tailored to the audience. Since individuals have different preferences for how they learn, training materials should ideally be in a variety of formats (exercises, theoretical papers, first hand accounts, procedures).

The story of what happened is an important knowledge asset. It should not be discarded when lessons are distilled into other formats such as checklists. The ideal checklist would be one where every listed item can be traced to background knowledge that helps the user understand why this point is important.

A culture of organisational learning is needed if lessons learned are to be maximised. Staff setting up new projects and operations (or modifying existing ones) should be encouraged to consult repositories of lessons learned and to use techniques such as 'Peer Assist' [18] to learn from the experience of others.

4.3.2 Learning lessons more widely

Many incident schemes include a publishing capability that allows lessons learned within one organisation to be distributed globally. This can be via trade magazines (though financial support for trade organisations seems to be declining), specialist publications or websites. Typically, lessons tend to be most relevant (and accessed) within an industry sector, such as within aerospace or within oil and gas. Sometimes lessons are disseminated across industry sectors but within a technology domain, eg amongst software practitioners and managers.

Disseminating lessons like this requires a good editorial capability. First hand accounts have more impact on readers [15]. “War stories” of known incidents (such as “Out of Control” [19]) are useful for disseminating lessons learned, but they have to be well presented. The editor should be competent to:

- Provide a “wrapper” to the incident, eg highlighting current relevance and other factors of interest to the audience.

- Provide a summary and conclusion.

- Cut down the first hand account, so that it has maximum impact.

- Summarise similar incidents into one article without repetition, ie highlighting similarities and differences.

- Add trend information.

In a medium or large organisation, the individuals who have first hand experience of the incident or its investigation may have a role in teaching others, providing either presentations at workshops or case studies in training courses. In GEC plc, such experience was used extensively in a two day Product Safety Management Course.

As well as disseminating experience, organisations must have processes to ensure that they are learning from external experience. Domain experts can be encouraged to join or participate in trade activities where incidents are publicised and to report internally on relevant lessons. Safety legislation requires that organisations take account of knowledge external to themselves when considering risks.

Another example of learning from experience is the MERE system developed in the REAIMS project for Aerospatiale [20]. MERE (Managing Experience for Requirements Engineering) is a powerful approach to preserving corporate memory that enables organisations to learn from their experience. It enables experience to be recorded, analysed and processed to generic rules—Rule/Recommendations (R/R) in MERE terminology—which are applied in future projects to prevent errors being repeated or to preserve valuable experience. The MERE process defines the lifecycle of the R/Rs from initial incident collection through elaboration and validation, to application and verification on a new product.

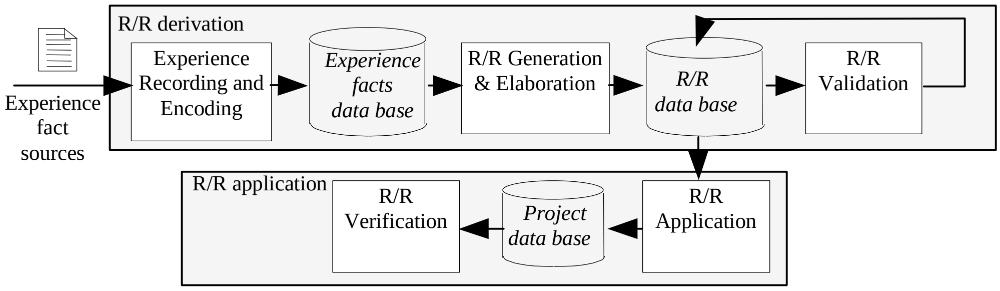


Figure 8 The MERE process

4.3.3 The learning process of investigations

The process of investigating an incident is a learning process for the investigation team. Facts about the incident are initially absorbed by the team members, then, collectively, new knowledge is created (an understanding of what went wrong and why).

The learning process is:

- *Motivation*: the trigger for the individual team member is assignment to the investigation and/or involvement in the incident. Those who are personally involved should have a high motivation, especially if the actual or potential consequences were serious and fully understood. Professional investigators can lose motivation if the job becomes routine. For example, for a pathologist, death is a daily occurrence. Motivation is also very important to those who report faults. In many cases they will not be team members investigating the incidents. In some cases they may be part of the cause and will need confidence in the system. It should also be noted that team composition will be limited by resources available and funding.

- *Exploration*: the exploration stage is where the facts are gathered and interviews taken. This stage requires an opening, questioning mind. Some individuals have a tendency to leap to conclusions too early in the process. A well put together team should include people who have divergent thinking skills. Individuals or the team as a whole may have biases that cause them to overlook or exclude parts of the evidence, eg to concentrate on factors within their own expertise or to respond to preconceptions about causes. Good team design should try to mitigate common viewpoints. At this stage, experimentation with different models or tools may find that one is more suitable than others for the particular nature of the incident. Teams will often need to include experts in the use of a particular tool or technique.

- *Understanding*: the understanding stage is where the facts begin to form a pattern. Convergent thinkers are needed in the team to bring the exploration stage to a close and help the team to reach conclusions. The team needs to agree on the pertinent facts and models.

- *Distillation*: distillation is the stage where the essential points form a theory of the incident. Depending on the nature of the incident and the analysis tools used, key points may fall naturally out of the analysis process (eg from an analysis of necessary and sufficient causes). This will not necessarily be the case and team members will need to apply judgement.

- *Generalisation*: generalisation is the point where specific facts and local conditions may be replaced by more generic examples. Sometimes root causes are only identified at this stage. For example, an investigation might have found that a particular operator lacked the skill to undertake a task – however, the general issue could be that none of the operators were trained for the task.

- *Communication*: the final stage is for the investigation team to prepare their findings for communication to a wider audience. This may involve such diverse tasks as recording facts within a constrained format for a database and providing presentations to a wide range of personnel. In putting together an investigation team, thought needs to be given to the communication skills needed.

The team may be exposed to so much information, especially in the exploration stage, that they are unable to absorb and internalise it. Techniques such as “After action review” [18] can be used by the investigation team (for example at the close of each day) so that they ensure that they reflect on what they have heard, improve their own processes and learn throughout the process.

People who participate in an incident investigation will go through a learning curve. If this is their first such experience, it will open their eyes to safety issues that they had previously not been aware of. They can then take on other roles where they will be able to apply their greater understanding and awareness of safety concerns. An organisation could consider using assignment to investigation teams as a competence development exercise for people who are intended for responsible positions (design authorities, managers etc) as well as for people in safety roles.

“Gatekeepers” for incident reporting schemes and editors who publish incidents for large schemes become experts in their domain through exposure to so many lessons learned. This expertise can be used for other purposes, eg for consulting on the design or risk analysis of new systems or operations.

5 SURVEY OF INDUSTRY PRACTICE

In this survey we planned to cover the main stakeholders, namely:

- Procurers
- System Suppliers
- Users
- Maintainers
- Assessors/licensors/regulators
- Standards/guidance developers
- Incident investigation consultant/academics

We also planned to cover a range of industries that are the direct responsibility of the HSE, ie

- Process
- Offshore
- Machinery
- Nuclear
- Railways

As a comparison, we planned to look at other sectors where safety-related PES are used, eg

- Marine
- Medical
- Aviation
- Defence

The survey was based on structured interviews with a sample of stakeholders in different industries. We also drew on direct experience and review material and contacted academics with expertise in incident analysis in related industries.

5.1 CONSULTATIONS PERFORMED

A series of interviews were set up with industry, using a standard interview brief (see Appendix B). We also drew on our own experience of incident reporting in the medical, defence and aviation sectors.

5.2 ANALYSIS OF INDUSTRY PRACTICE

The actual interviews were confidential so they cannot be reproduced verbatim. However we have reviewed the interview reports and some of the main features are summarised below. In accordance with the confidentiality requirements of the study, individual organisations are not identified.

Table 1 Industry practice

Sector/ Role	***Incident reporting***	***Incident investigation***	***Handling of E/E/PES***	***Learning***	***Dissemination***
Pharma-ceuticals (End user, designer, maintainer)	Learning from experience reporting scheme Not confidential (750/yr)	Works Investigation for serious incidents (6/yr) Training Checklists Timeline Event tree	Company standards (old equipment) IEC 61508 (new) 2 failures in 10 tests trigger investigation (1/year)	Feedback of recommendation s to reporters (trial) Control and electrical forum (every 4 months)	Sites can report incidents to moderator: - classified and authorised - put on Intranet - emailed to those registered for specific classes of incident
Nuclear (End user, designer, maintainer)	Events classified by 3 layer model Non-reportable hazards are logged Not confidential	RIDDOR events reported immediately to CEO Fix identified by operational units Use event-based /event chain causal analysis. Have looked at MORT No trend analysis of logs (yet)	50-70% events involve E/E/PES (esp. fire alarm failure) Repeat failures not examined yet but possible For E/E/ PES: design section assists and also records findings to inform future design Using 61508 for some new PES	Central Learning from Experience management (3 sites) Regular review of internal and external incident databases	Feedback co-ordinators in operational units H&S info and discussion forum on intranet
Oil and gas (Procurer, end user)	Standard incident reporting, 4 level classification 20-30 events per month involving injury, time off, etc Report filled in by safety officer Not confidential	Recommen-dations tracked on per installation basis	E/E/PES failure could be a causal factor in spurious trips No awareness of IEC 61508 (but outside the interviewee's area of expertise) Supply chain reporting not known	Review of external industry-wide accident database Workforce consultation process as a feedback mechanism	Safety briefings and weekly safety meeting to discuss incidents Incident investigation team can issue recommendations across a wide range of stations Accident reports can go to shared industry system
Marine (Assessor)	Incidents are reported (but only "significant" ones – injury, pollution)	Accidents in UK investigated by the industry body. Some accidents have been re-analysed using a method similar to TRIPOD – finds more causal factors	PES in almost every system Systems not integrated System integrator competence variable All systems are one-off Long term support a problem Suppliers generally unaware of IEC 61508	Incorporating experience in a ISO standard referencing IEC 61508 Avoid problems by sharpening user requirements and PES system requirements and using good practice through the lifecycle	Public records of accidents Organisational intranet of incidents and problems to aid surveyors

Table 1 (continued) Industry practice

Sector/ Role	*Incident reporting*	*Incident investigation*	*Handling of E/E/PES*	*Learning*	*Dissem-ination*
Rail sector (Procurer, end user)	All incidents recorded in Industry database (5000/month) Trivial ones just logged Confidential reporting scheme exists	Some incidents investigated locally (500/mth). Remainder subject to formal investigation (75/month) and formal enquiry (2 or 3 per month). Public enquiry for major accidents. Accident investigation team produce report, reviewed by Safety Review Group. Operators are free to accept/reject recommendations but whole process is documented and auditable. Consistency achieved via formal training scheme (root cause analysis and leading investigation teams). Defined process for incident investigation. Recommendation tracking supported by tools	E/E/PES is thought to be a small fraction of incident causes for Category A incidents that need formal investigation. Higher proportion in locally investigated incidents. (Greatest concern is human factors) Supply chain issues covered by contractual requirements rely on ISO 9000 approval to aid reporting	Analysis of long term trends in industry database. Can search for patterns of events Confidential reporting scheme reports reviewed periodically Confidential reporting scheme could aid incident investigation (eg find accident precursors)	Not established
Rail sector (Assessor)	Incidents from the shared industry incident database (not confidential) are transcribed into assessors' database. Incidents classified by type and severity, around 8000 incidents in database	All accidents and fatalities investigated. Causal analysis performed, but method not standardised	2 incidents known to be PES related, but normally handled by the operating companies	Attempting to improve quality of incident data in collaboration with operating companies No formal trend analysis performed	Annual safety reports showing trends for different incidents
Machinery (Procurer, end user)	300 reports/year Incident report if damage or injury. Filed by local safety co-ordinator (or person involved)	Safety co-ordinator receives forms. Incident forms sent to insurer Minor injury: Single page form –kind of action, agents involved, what caused injury, preventive action and comments by reporting officer More serious: incident investigation team produces report. Incidents reported to Risk Management Task Group Recommendations tracked in regular meetings	Not addressed	Insurer compiles records and analyses data on a yearly basis H&S department produce statistics Risk manage Task group review incidents that could impact several departments H& S departments undertake local analysis and make recommendations	Not established

Table 1 (continued) Industry practice

Sector/ Role	*Incident reporting*	*Incident investigation*	*Handling of E/E/PES*	*Learning*	*Dissem-ination*
E/E/PES supplier (Designer, maintainer)	Client telephone and emails: to customer feedback form – classified by a engineer as hazardous or commercial Standard QA non-compliance form used to record product problems	3 "Hazardous" incidents only Respond in 1 day with fix. Notified to Director All events recorded and tracked in QA system Product problems and resolution also tracked by QA system	CASS certified to IEC 61508 Staff competence scheme for equipment "Green book" of standard designs	Updates of review checklists, test templates and "green book" designs. Documentation Regular review and updating of reported product problems and configuration rules Periodic review of commercial problems tracked by QA Monitor of system effectiveness via customer satisfaction	Intranet bulletin board of known problems. Email to notify problems (internally and to product suppliers) Access to product supplier web site documentation and software
E/E/PE system supplier (Designer, maintainer)	Product problem reported on an equipment performance report form	Design/software problems handled by product support dept. A database of all actions and resolutions is maintained	Hardware problems reported to product vendor	Not established	Alerts from product suppliers are reviewed and where applicable passed in to end users
E/E/PE component supplier	Customer email and phone reports transcribed to a customer feedback form classified by significance	Safety significant events receive immediate investigation (relatively few in UK mainly mismatch with user environment) Product problems reports to USA for analysis / correction or a change of documentation. Customer follow up to check satisfactory resolution	Part-way through IEC 61508 CASS certification Plan to produce a 61508 product soon Separate procedures for handling changes to IEC 61508 products Procedures updated in the light of experience All IEC 61508 products to be painted yellow – so handled differently through the supply chain	Impact analysis of problem (hardware and software modules used in related products) Warnings issued to users where product used in safety application Regular reviews of the problem report database and long term trend analysis	Customer support via Internet website. Technical info and guidance for end-users and system suppliers

The following table is based on the knowledge of project team rather than consultation.

Table 2 Aviation sector practice

Sector	*Incident reporting*	*Incident investigation*	*Handling of E/E/PES*	*Learning*	*Dissem-ination*
Aviation	Internal incident recording by air traffic services and aircraft operators. Mandatory reporting of serious event to the CAA [21] Also a Eurocontrol regulation on incident monitoring [22] Confidential reporting is possible	Analysis of serious incidents by CAA Safety Regulation Group Near misses (Airprox Board) and accidents (AAIB). Recommendations fed back	Strict type approval of avionics by FAA or CAA Avionics software written to a strict standard that varies with safety class [23] Problem reporting back to suppliers Warnings issued to users with recommendation to upgrade Strict version control of avionics Ground ATS systems regulated by CAA. Published assessment standards	Trend analysis of incidents, and near misses by aircraft type location, etc Corrective action for “hot-spots”	Public records of near misses and accidents

5.3 EXAMPLE INCIDENT HANDLING PROCESSES

The processes used by companies varied in size and sophistication, depending on both the complexity of the company organisation and its position in the supply chain. Some example processes are shown the subsections below.

5.3.1 Pharmaceutical manufacturer

This incident reporting scheme applies to a single site with around 500 staff.

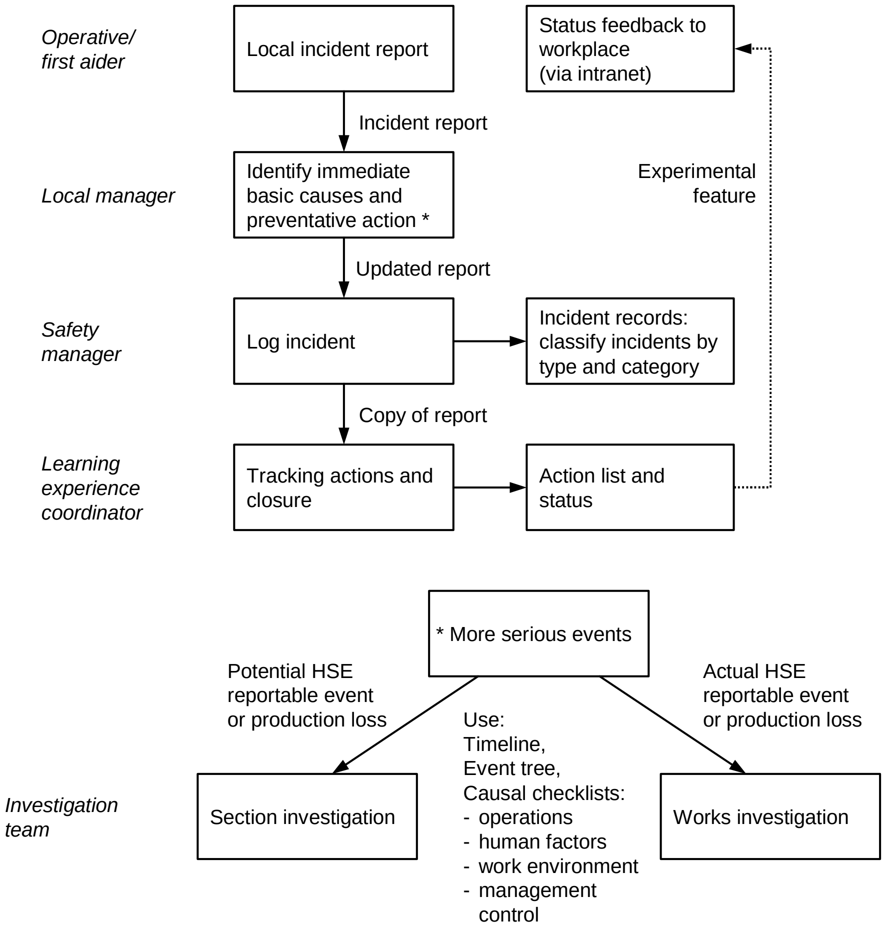


Figure 9 Incident handling process: pharmaceutical manufacturer

5.3.2 Oil and gas extraction

The site is one of many belonging to the same company. Serious incidents have declined since this system was implemented. Normally recommendations apply to one site, but recommendations can be issued for other sites.

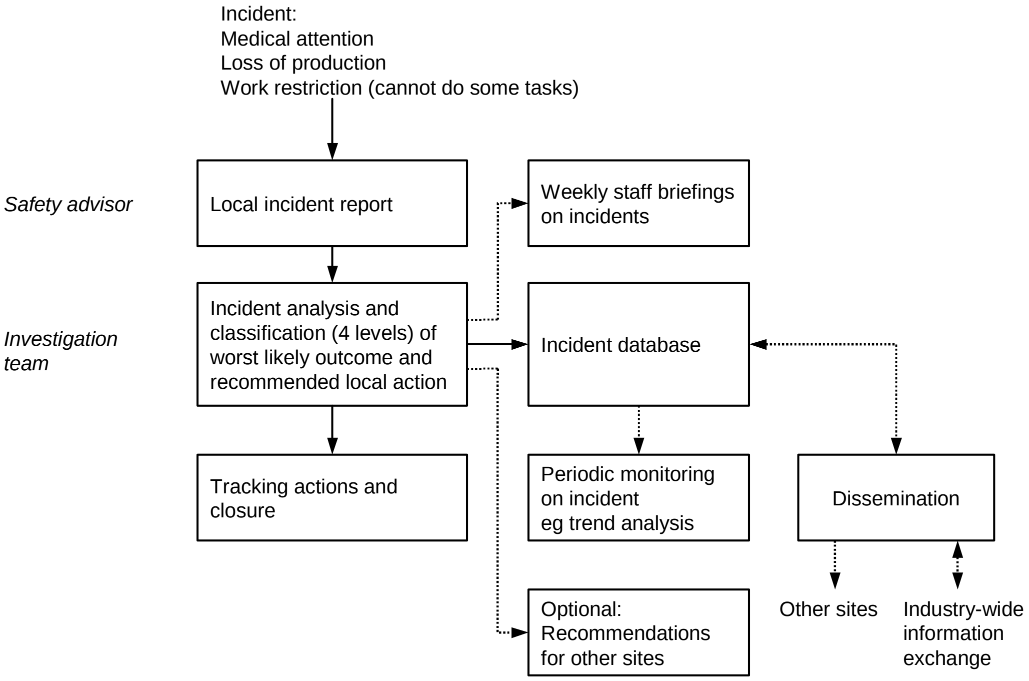

Incident:
Medical attention
Loss of production
Work restriction (cannot do some tasks)
Safety advisor
Local incident report
Weekly staff briefings on incidents
Investigation team
Incident analysis and classification (4 levels) of worst likely outcome and recommended local action
Incident database
Tracking actions and closure
Periodic monitoring on incident eg trend analysis
Dissemination
Optional: Recommendations for other sites
Other sites
Industry-wide information exchange

Figure 10 Incident handling process: oil and gas company

5.3.3 Process industry

This scheme applies to a company with several sites, and several units on one site. Serious incidents have declined since this system was implemented.

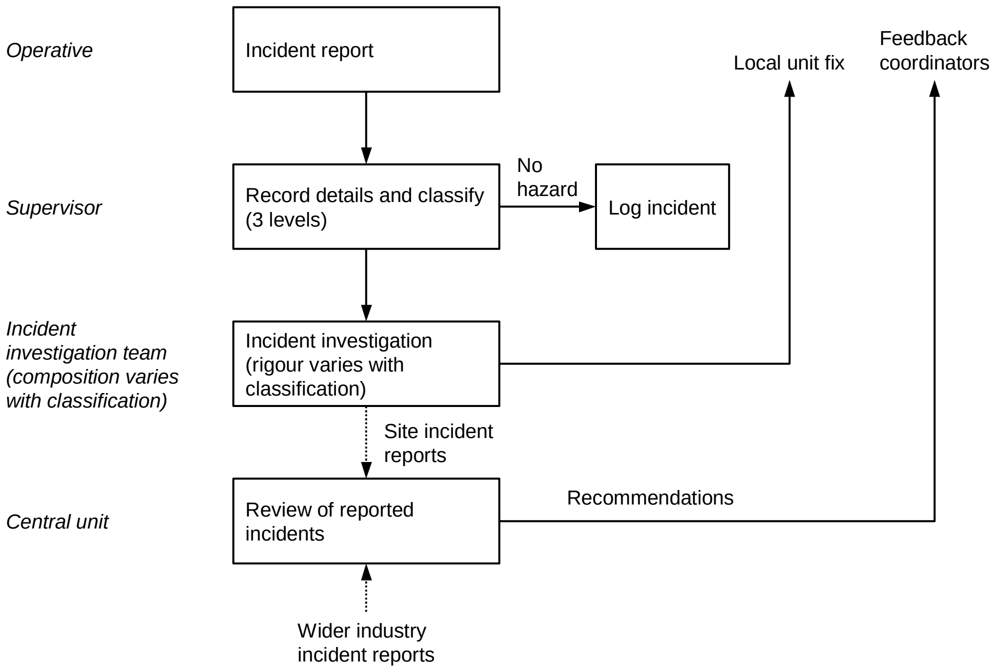
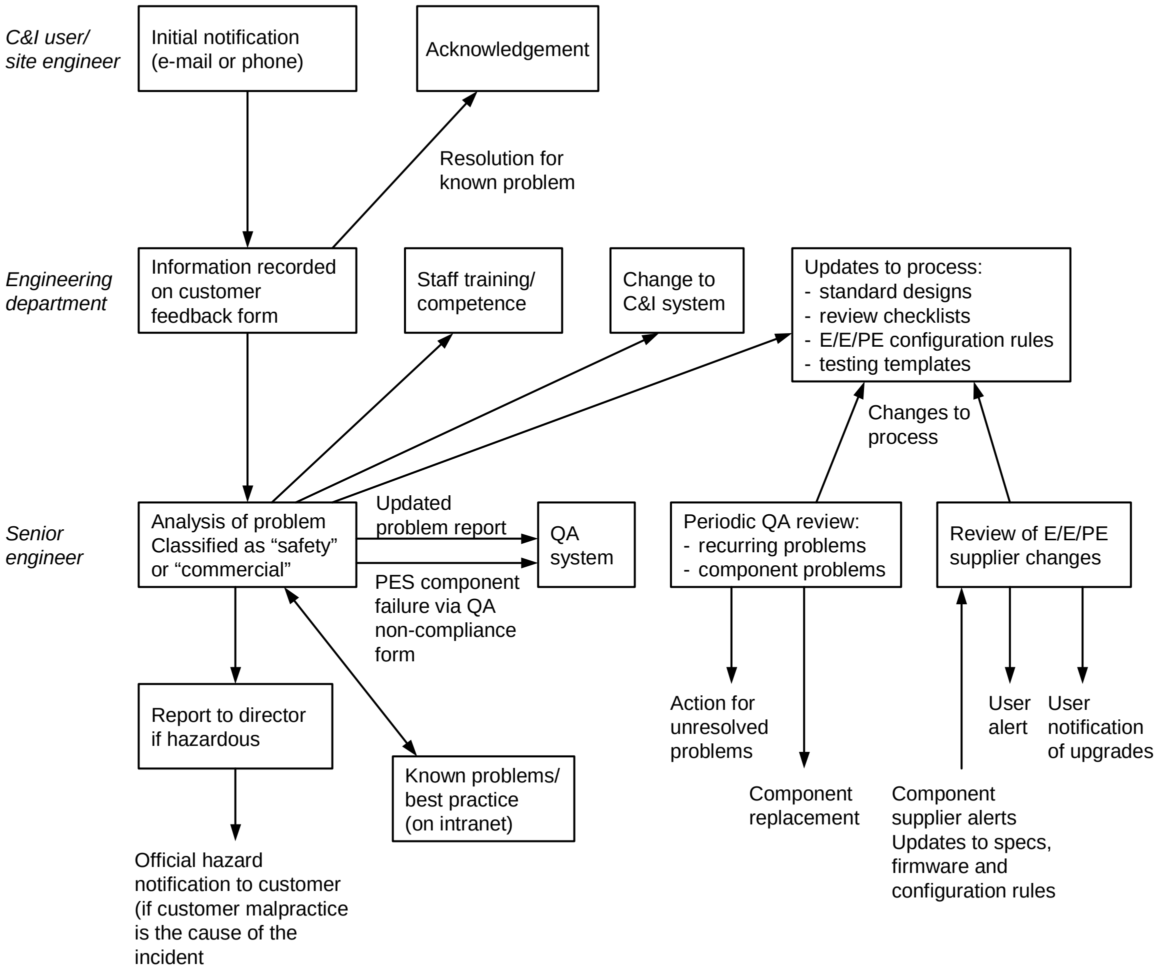

Operative
Incident report
Local unit fix
Feedback coordinators
Supervisor
Record details and classify (3 levels)
No hazard
Log incident
Incident investigation team (composition varies with classification)
Incident investigation (rigour varies with classification)
Site incident reports
Central unit
Review of reported incidents
Recommendations
Wider industry incident reports

Figure 11 Incident handling process: chemical manufacturer

5.3.4 C&I System Supplier

The C&I supplier designs, installs and maintains C&I systems. The company uses IEC 61508 assured PES and designs to specific safety integrity levels. In cases where a hazardous incident is caused by a customer modification, the customer is officially notified. However, customers are not generally IEC 61508 assured, so there is no obligation to improve their process in the light of this report.



C&I user/ site engineer
Initial notification (e-mail or phone)
Acknowledgement
Resolution for known problem
Engineering department
Information recorded on customer feedback form
Staff training/ competence
Change to C&I system
Updates to process:
- standard designs
- review checklists
- E/E/PE configuration rules
- testing templates
Changes to process
Senior engineer
Analysis of problem Classified as “safety” or “commercial”
Updated problem report
QA system
PES component failure via QA non-compliance form
Periodic QA review:
- recurring problems
- component problems
Review of E/E/PE supplier changes
Report to director if hazardous
Known problems/ best practice (on intranet)
Action for unresolved problems
Component replacement
User alert
User notification of upgrades
Component supplier alerts Updates to specs, firmware and configuration rules
Official hazard notification to customer (if customer malpractice is the cause of the incident

Figure 12 Incident handling process: E/E/PE system supplier

5.3.5 E/E/PE component supplier

This company supplies electronic and PE components, and has partial IEC 61508 certification. Each component has a unique serial number and the customer is known for each component. This enables the company to alert all affected customers if a problem is identified. Note that several products may be affected, as they may share common hardware and software components.

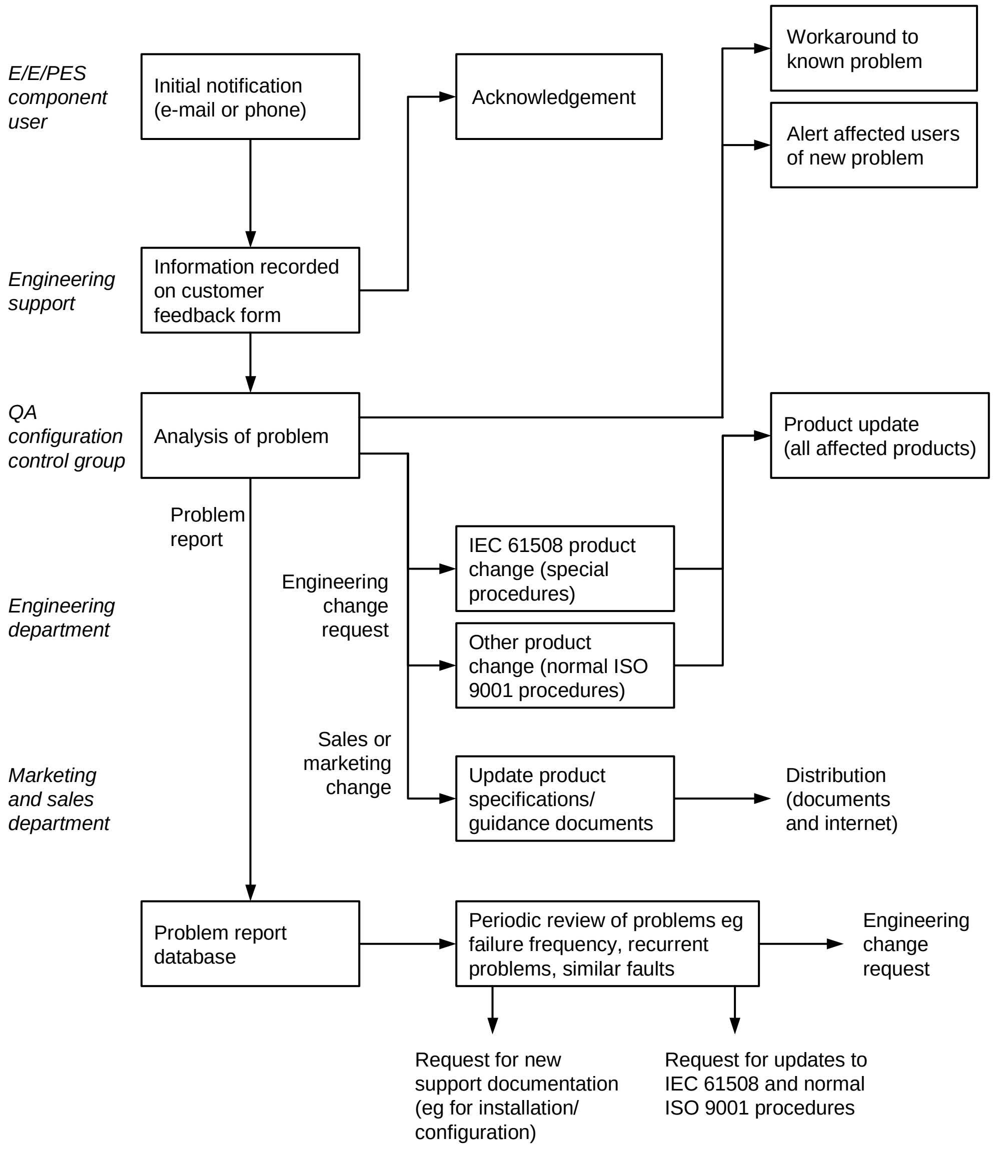

E/E/PES component user
Engineering support
QA configuration control group
Engineering department
Marketing and sales department
Initial notification (e-mail or phone)
Acknowledgement
Workaround to known problem
Alert affected users of new problem
Information recorded on customer feedback form
Analysis of problem
Product update (all affected products)
Problem report
Engineering change request
IEC 61508 product change (special procedures)
Other product change (normal ISO 9001 procedures)
Sales or marketing change
Update product specifications/ guidance documents
Distribution (documents and internet)
Problem report database
Periodic review of problems eg failure frequency, recurrent problems, similar faults
Engineering change request
Request for new support documentation (eg for installation/ configuration)
Request for updates to IEC 61508 and normal ISO 9001 procedures

Figure 13 Incident handling process: E/E/PE component supplier

5.4 DISCUSSION OF SURVEYED SCHEMES

We can see from the tables and process diagrams that there is a wide variation in incident reporting and analysis mechanisms in the different industry sectors and the supply chain. As we have a limited sample it is not clear how many companies follow good practice in each sector. However it is clear that the variability is far greater in unregulated industries (where there is no external approval) than unregulated ones (such as aviation).

5.4.1 General issues

The "contractor culture" prevalent in industry today can limit the application of lessons learnt to new projects. Current procurement strategies for new projects within many sectors fix capital costs and may even involve "gainshare" (where there is a strong financial incentive to cut costs). Such contracts inhibit improvements because changes can increase equipment and design costs. In some cases the only influence the user organisation has is on the standards used for the project design. Many user organisations no longer have their own standards and instead reference international standards such as IEC 61508. The only effective feedback to design involves changes to these standards, which takes many years and limits what can be achieved. Also, most contract organisations have competence and experience problems.

The majority of existing systems will not have been implemented using IEC 65108 as a design basis. There will be limited knowledge on the design history of such systems. The guidance will need to be suitable for use with legacy systems.

Root causes associated with E/E/PES incidents will be common to non-E/E/PES incidents. This needs to be recognised when fitting a scheme for E/E/PES within a more general scheme. The taxonomy of root cause should be consistent across incident types.

5.4.2 Incident reporting

As might be expected, large end-user companies have the most sophisticated schemes especially where they are subject to regulation. End-user schemes are generic (ie are not focused on E/E/PES). It was observed by more than one company that implementation of more rigorous reporting schemes increased the incident reporting rate, but reduced the serious accident rate, suggesting that there was previous under-reporting. Under reporting of incidents might be due to a number of factors:

- the perceived risk of being blamed for reported errors,
- the lack of any response to reported problems.

Some companies address the latter point by feeding back the result of the incident report to the originator. Confidentiality could encourage reporting but most companies have non-confidential schemes.

Only a small fraction of reported incidents involve a special investigation of E/E/PES failure. For example, in one company that had 750 incidents per year, 6 were investigated in detail and only one required a special investigation of E/E/PES failure.

5.4.3 Incident analysis

Here again there is wide variation, from formal training in a method to ad hoc approaches. One end user company said that their event-based causal analysis method did not get to the root causes very well, and they would be interested in alternatives. Another end user used timelines, event trees and checklists. Yet another uses a method similar to TRIPOD (accident trees plus structured checklists). The E/E/PES supply chain companies we interviewed did not use any specific method. In large companies we found up to four levels of incident enquiry (excluding public enquiry). The level depended on incident severity and could be either trivial, local, formal investigation, or formal enquiry, with different levels of investigation and different personnel at each level. Typically for large companies there were many thousands of trivial incidents per year but less than ten resulted in the most stringent type of enquiry.

5.4.4 Recording

Recording of incidents, analyses and tracking of safety recommendations can be quite sophisticated in some large companies and can be implemented independently of other systems. However some small companies make use of existing QA systems for this purpose. This is an efficient approach if there are few safety-related incidents. Additional or modified QA procedures can be incorporated to address safety aspects (eg require greater urgency or qualified people).

5.4.5 Implementation

Some companies expressed concern about the implementation of such schemes. Given the significant costs in training and in writing documentation and procedures for using a new analysis module, some care has to be given to the business case.

- There is a significant amount of inertia associated with existing systems. New schemes should build on these and augment them, rather than offer an approach that may be seen to be “unrelated”.

- Also the use of technical language or jargon can put people off. This was an issue for scheme users even though the companies had spent some time in trying to guide the technical development and to reduce the jargon.

- The scheme has to be highly usable.

- Expectations of what the scheme will provide should be carefully considered and communicated. For example in one organisation, end users had expected a supporting tool for a scheme to “provide solutions”, whereas in fact it should have more properly been thought of as an aid/stimulus for the analyst.

5.4.6 Learning and dissemination

There are many ways of learning lessons and dissemination. Some have explicit mechanisms for reviewing and generalising incidents into recommendations. The experience can also be fed back into the design rules and business processes, and can be disseminated more broadly to other sites, trade bodies and regulators. Tools such as databases, intranets, bulletin boards and email aid dissemination. However to change the company culture, “softer” methods may need to be deployed which might involve briefing, anecdotes, or “stories” that make a point (such as the “Out of Control” report).

6 CONCLUSIONS

6.1 CURRENT INCIDENT HANDLING SCHEMES

1 Incident reporting systems can reduce losses arising from production and other losses (environmental, security etc) as well as reducing injury. Therefore organisations can use incident reporting and analysis systems as a general organisational risk management tool.

2 The best companies have well-established incident handling schemes. These can include specific roles for generalising the lessons learned from incidents and disseminating them throughout an organisation.

3 Companies classify incidents according to severity and this determines how the incidents are investigated.

4 Companies may also classify incidents according to type (for subsequent monitoring and trend analysis). However there is rarely any formal classification scheme of incident causes—the priority is to identify necessary changes in product, procedures or personnel competence.

5 There are a wide range of incident reconstruction and analysis methods available, but it is not clear that any one method (or set of methods) will be appropriate for a given company.

6 For less severe incidents (and less mature companies), analysis is based on textual elaboration by designated experts.

7 Companies make use of modern technology like email, databases, discussion groups, and on-line documents. This can reduce the manual effort involved in incident reporting, incident handling, feedback, and the dissemination of lessons learned and “tips”.

6.2 INCLUSION OF E/E/PES

8 Most companies do not record whether E/E/PES are involved in minor incidents. End user organisations often find it difficult to determine whether E/E/PES were implicated in an incident.

9 Most companies do not consider that E/E/PES are a major cause of incidents (even though E/E/PES are widely used).

10 Special investigations of E/E/PES failures are only instigated for major incidents.

11 Only a few organisations are familiar with IEC 61508. A wide range of company and industry-specific standards are used for E/E/PES. It cannot be assumed that companies will be familiar with IEC 61508 concepts, life-cycle or terminology.

6.3 ADOPTION ISSUES

12 Even for companies with mature incident handling schemes, there is concern about the cost/benefit of any extension to an existing scheme. There are often significant costs in developing supporting documentation and procedures to run such a scheme. Retraining is also a significant cost. Also extensions to reporting can be a disincentive to the reporters and investigators if the reporting process is too onerous.

13 Smaller companies tend to reduce costs by building on existing systems (like an existing quality management system). Implementing an entirely new scheme is likely to be too time consuming and expensive.

14 Comprehensive incident reporting schemes that include the supply chain and information sharing are impeded by industry fragmentation (contracting out, lack of continuity in the supply chain, etc).

15 Management support and motivation is important for a successful scheme. This requires feedback to the reporters and investigators (to show their activities are valued and acted upon).

7 RECOMMENDATIONS

Based on our survey of existing industrial practice and methods, we make the following recommendations for guidance on incident reporting and analysis that covers E/E/PES.

7.1 GENERAL SCHEME DESIGN

1 To support analysis of information from large incident repositories (eg collected across a large organisation or industry) there is a benefit in creating an explicit structure for that data (eg by classification of incidents). In practice however, free text retrieval is also needed to extract information from general description fields.

2 For larger organisations there is a need for various “learning roles” that maintain a good overview of reporting and investigation generally.

3 Implementers of a scheme need to take into consideration the actual reporting and safety culture of the organisation and industry as a whole. For example whether to implement an anonymous reporting scheme will depend on this.

4 A common training approach for incident investigators is recommended to ensure a consistent and comparable approach to root cause analysis within an organisation.

7.2 INCLUSION OF E/E/PES WITHIN AN INCIDENT REPORTING SCHEME

5 To ease uptake, any causal analysis scheme should be simple to apply, and complement existing methods rather than replace them. For example a method can be used that is specific to the E/E/PES failures associated with the incident.

6 The guidance should focus on the additional aspects necessary to include the E/E/PES contribution to the incident.

7 The guidance should indicate where these additional E/E/PES aspects should be incorporated within an overall incident handling process.

8 The scheme extension for E/E/PES should be “low impact”, allowing easy integration with existing schemes (both reporting and analysis).

9 Classification of aspects that are not of direct interest to the company should be simple to implement, eg the causal classification could follow directly from the application of causal analysis to an E/E/PES related incident.

7.3 ADOPTION

10 Organisations should seek to ensure that feedback of the implementation of recommendations arising from incident reporting and analysis is made visible to the end users who are reporting the incidents. This increases motivation for reporting as users can see that a benefit was achieved.

11 It is important to disseminate the lessons learnt from individual incidents as widely as possible to maintain commitment to the scheme. Organisations can use standard hypertext and intranet tools to develop “knowledge bases” of known issues and design tips, that are readily available to interested parties.

12 Incident reporting (by computer or paper form) should seek to be simple and usable by its end users to encourage adoption (eg avoid jargon and only ask for relevant information).

13 The scheme extension to E/E/PES should be fairly low cost to implement and administer.

14 Administrative burdens should be minimised. Low cost technologies (such as email, databases, etc) can reduce the effort needed to maintain the scheme. Organisations can make use of their existing QMS to track the implementation of any recommendations that are generated.

REFERENCES

[1] T S Ferry, Modern accident investigation and analysis, 1988, Wylie, ISBN 047 1624810

[2] C.W. Johnson, The London Ambulance Service, Computer Aided Dispatch System: A Case Study in the Integration of Accident Reports and the Constructive Design of Safety-Critical Computer Systems, Reliability Engineering and Systems Safety, 71, 3, 311-326, 2001.

[3] A.K. Lekberg, Different Approaches to Incident Investigation: How the Analyst Makes a Difference. In S. Smith and B. Lewis (eds.) Proceedings of the 15th International Systems Safety Conference, 178-193, Systems Safety Society, Unionville, VA, USA, 1997.

[4] T.W. van der Schaaf, Near Miss Reporting in the Chemical Process Industry, Technical University of Eindhoven, Eindhoven, The Netherlands, 1992.

[5] C.W. Johnson, A Handbook for the Reporting of Incidents and Accidents, London, UK, http://www.dcs.gla.ac.uk/~johnson/book, 2003.

[6] W.G. Johnson, MORT Safety Assurance Systems, Marcel Dekker, New York, USA, 1980.

[7] F Koornneef, “Organised Learning from Small Scale Incidents”, Delft University Press, ISBN 90-407-2092-4, 2000.

[8] Department of Energy, DOE Guideline Root Cause Analysis Guidance Document, Office of Nuclear Energy and Office of Nuclear Safety Policy and Standards, U.S. Department of Energy, Washington DC, USA, DOE-NE-STD-1004-92, http://tis.eh.doe.gov/techstds/standard/nst1004/nst1004.pdf, 1992.

[9] A D Livingston, G Jackson & K Priestley. Root causes analysis: Literature review, http://www.hse.gov .uk/research/crr_pdf/2001/crr01325.pdf

[10] Department of Energy, MORT User's Manual: For use with the Management Oversight and Risk Tree, Technical Research and Analysis Section, Environmental Safety and Health, U.S. Department of Energy, Washington DC, USA, DOE-76/45-4-ssdc-4, http://tis.eh.doe.gov/analysis/trac/SSDC_doc/10003.txt, 1976.

[11] J.A. Doran and G.C. van der Graaf, Tripod-Beta: Incident Investigation and Analysis, Proceedings of the International Conference on Health, Safety and the Environment, Society of Petroleum Engineers, New Orleans, USA, 9-12 June, 1996.

[12] P. Ladkin and K. Loer, Why-Because Analysis: Formal Reasoning About Incidents, Bielefeld, Germany, Document RVS-Bk-98-01, Technischen Fakultat der Universitat Bielefeld, Germany, 1998.

[13] N. Leveson, A Systems Model of Accidents. In J.H. Wiggins and S. Thomason (eds) Proceedings of the 20th International System Safety Conference, 476-486, International Systems Safety Society, Unionville, USA, 2002.

[14] N. Leveson and P. Allen, (2002), The Analysis of a Friendly Fire Accident Using a Systems Model of Accidents. In J.H. Wiggins and S. Thomason (eds) Proceedings of the 20th International System Safety Conference, International Systems Safety Society, Unionville, USA, 2002.

[15] Dave Snowden:, “The Paradox of Story” http://www-1.ibm.com/services/files/storytelling.pdf, 1999.

[16] IBM, “Stories in knowledge management”, http://www.research.ibm.com/knowsoc/connections_biblio_km.html.

[17] C Johnson, “Architectures for Incident Reporting” Dept of Computing Science, University of Glasgow, http://www.dcs.gla.ac.uk/~johnson/papers/succa/.

[18] C Collision, G Parcell, “Learning to Fly: Lessons from one of the world’s leading knowledge organizations” Chris Collison and Geoff Parcell, 2000.

[19] HSE, “Out of Control”. Health and Safety Executive, ISBN 0 7176 0847 6, 1995.

[20] MERE, REAIMS project, http://www.comp.lancs.ac.uk/computing/research/cseg/projects/reaims/mere.html.

[21] CAA, CAP 382, The Mandatory Occurrence Reporting Scheme,1996.

[22] Eurocontrol Safety Regulatory Requirement (ESARR 2), Reporting and Assessment of Safety Occurrences in ATM Released Issue 2.0 03.11.2000.

[23] EUROCAE ED-12, Software Considerations in Airborne Systems and Equipment Certification, Radio and Technical Commission for Aeronautics Document No. RTCA DO-178 / EUROCAE ED-12, Rev. B, October 1992.

BIBLIOGRAPHY

The following sources of information are also relevant:

Food and Drug Administration, "Final Report of a Study to Evaluate the Feasibility and Effectiveness of a Sentinel Reporting System for Adverse Event Reporting of Medical Device use in User Facilities", Office of Surveillance and Biometrics, Center for Devices and Radiological Health", see http://www.fda.gov/cdrh/postsurv/medsunappendixa.html

J Henderson, C Whittington & K Wright. Accident investigation -The drivers, methods and outcomes, http://www.hse.gov .uk/research/crr_pdf/2001/crr01344.pdf Glasgow Accident Analysis Group (web site) http://www.dcs.gla.ac.uk/research/gaag/

P. Hudson and J. Reason and W. Wagenaar and P. Bentley and M. Primrose and J. Visser, Tripod-Delta: Pro-active Approach to Enhanced Safety, Journal of Petroleum Technology, 40, 58-62, 1994.

ISO/CD 17894.2 “Ships and marine technology—Computer applications—General principles for the development and use of programmable electronic systems in marine applications”, ISO TC 8/SC 10/WG3 working group, 2002 (committee stage doc.)

C.W. Johnson, Visualizing the Relationship between Human Error and Organizational Failure. In J. Dixon (ed), Proceedings of the 17th International Systems Safety Conference, The Systems Safety Society, Unionville, Virginia, United States of America, 101-110, 1999.

C.W. Johnson and A.J. Telford, Using Formal Methods To Analyse Human Error And System Failure During Accident Investigations, Software Engineering Journal, 11, 6, 355-365, November, 1996.

NASA, NASA Procedures and Guidelines for Mishap Reporting, Investigating and Record-keeping, Safety and Risk Management Division, NASA Headquarters, NASA PG 8621.1, Washington DC, USA, http://www.hq.nasa.gov/office/codeq/doctree/safeheal.htm, 2001.

NASA, “NASA Procedures and Guidelines for Mishap Reporting”, Safety and Risk Management Division, Washington DC, USA, NASA PG 8621.1, 2001, http://www.hq.nasa.gov/office/codeq/doctree/safeheal.htm

NASA/ESA, SOHO Mission Interruption Joint NASA/ESA Investigation Board Final Report. Available from http://sohowww.nasa.gov/whatsnew/SOHO_final_report.html, 1998.

V Pomeroy, BM Sherwood-Jones, “Managing the Human Element in Modern Ship Design and Operation, RINA, 2002.

Railway Safety, Annual Report 2001.

T.W. van der Schaaf, PRISMA: A Risk Management Tool Based on Incident Analysis, International Workshop on Process Safety Management and Inherently Safer Processes, October 8-11, Orlando, Florida, USA, 242-251, 1996.

APPENDIX A OVERVIEW OF CAUSAL ANALYSIS TECHNIQUES FOR E/E/PES

Chris Johnson, Dept. of Computing Science, University of Glasgow, October 2002

This overview provides a brief summary of causal analysis techniques that can be used to analyse mishaps involving electrical, electronic or programmable electronic systems (E/E/PES). The intention is not to provide a complete introduction. Detailed guidance on each technique is available for the references at the end of this document.

A.1 INTRODUCTION

In the aftermath of adverse events, it is important to identify those hazards that threatened the safety of an application process. Each of these may stem from numerous causes. These can be catalytic events that triggered the mishap. They can also stem from background or latent conditions that emerge slowly over a longer period of time. Incident investigations must also identify those remedial actions that can be taken to prevent similar failures from occurring in the future. Table A.1 illustrates a common format that is used to summarise these products of an incident investigation.

Table A.1 Results of an incident investigation

Hazard	*Root cause of the hazard*	*Proposed remedial action*	*Responsible authority*
Hazard 1	Root causes	Remedial actions	Person or team to sign-off
Hazard 2	Root causes	Remedial actions	Person or team to sign-off

Any particular mishap may involve several different hazards. Each hazard can be the result of several different combinations of causes. Each of these may, in turn, require a range of remedial actions. The following pages introduce techniques that investigators might use to identify the root causes of hazards involving E/E/PES.

A.2 WHAT IS CAUSAL ANALYSIS?

Causal analysis is a process by which investigators can identify the reasons why a mishap occurs. In contrast, mishap reconstruction identifies what happened during an accident or incident. Causal analysis forms part of a wider process of mishap investigation. Ideally, investigators and safety managers must ensure the immediate safety of a system and gather all necessary evidence before any attempts are made to identify causal factors. In practice, however, investigators may have preconceived notions about what led to a failure. This can bias the way in which they gather evidence so that they only look for information that supports preconceived theories. From this it follows that the use of a causal analysis technique does not guarantee that appropriate lessons will be learned from adverse events.

A.3 CASE STUDY INCIDENTS

An E/E/PES case study will be used to illustrate the causal analysis techniques in this paper. This incident has been chosen through consultation with HSE and industry representatives because it typifies the adverse events that currently threaten many safety-critical industries. *Some details have been removed and others have been deliberately added so that the case study does not reflect any individual incident.* Over time, however, the nature of these events will change as new technologies and operating practices are introduced.

The incident in this paper started when a spillage of methanol was detected on board an off-shore production vessel. In order to collect this material, the vessel's ballast system was used to induce a list. During the clear-up operation, firewater hoses were used to clean the decks. As a result of these operations, the water pressure fell to such a level that the duty firewater pump was automatically started and this increased the pressure to an acceptable level. As the methanol clean-up progressed sensors detected high levels of gas and this initiated a plant shut-down. This included a plant 'black-out' with the loss of all electrical power. A further consequence of this was that crew could not use their control systems to halt the ballast operations that had been started to induce the list and collect the spilled material. The crew were, however, able to intervene directly to close off the valves that controlled the ballast operation before the list threatened the integrity of their vessel. The following pages focus on the E/E/PES related causes of this incident.

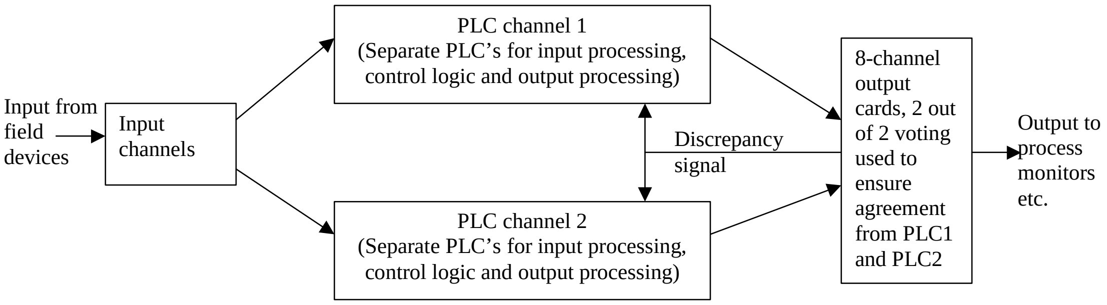

Input from field devices
Input channels
PLC channel 1 (Separate PLC's for input processing, control logic and output processing)
Discrepancy signal
PLC channel 2 (Separate PLC's for input processing, control logic and output processing)
8-channel output cards, 2 out of 2 voting used to ensure agreement from PLC1 and PLC2
Output to process monitors etc.

Figure A.1 High-level architecture for the E/E/PES case study

Figure A.1 illustrates the high-level architecture for part of the system that contributed to the mishap that forms the case study for this paper. Input is received from a range of devices and sensors. These are fed into two independent command 'channels'. They are intended to ensure that near identical data is passed to independent PLCs that are responsible for detecting and responding to certain input conditions according to the design 'logic' associated with the application. The signals generated by these output PLCs are passed to a separate output card, which uses a form of two-out-of-two voting protocol. Although this is an asynchronous system, under normal operation the two input processing PLCs will sample the same input values and the logic PLCs will arrive at the same outputs. It is unlikely that any discrepancies will persist. However, if there are any discrepancies between the output states of the two command channels and they persist beyond a timeout then a discrepancy signal is fed back. If the data on the preceding logic PLC indicates that a valid trip can be performed then it will reset all of its output to a predetermined ‘safe state’ during emergency shutdown.

During the mishap, a sensor detected a fall in the water pressure as hoses were being used to clear the initial spill. However, this transient signal was only received by channel 1. An alarm was triggered on the human operators control panel. If water pressure fell below a threshold value then the control logic was to ensure that the duty firewater pump was started but channel 2 had not received the low-pressure signal. The attempt to start the pump by PLC channel 1, therefore, raised a discrepancy between the two PLC channels. The requirement for agreement between both channels in the ‘two out of two’ protocol also ensured that the relevant pump was not started. By this time, however, PLC channel 1 was already actively monitoring the duty pump to ensure that it had started to address the fall in water pressure. This, in turn, generated a further alarm when the pump failed to respond after a predetermined time out. The logic in PLC channel 1 responded by trying to start another pump. This created a further discrepancy with PLC channel 2, which, of course, was not even monitoring the initial command to the duty pump.

Water pressure had continued to fall throughout this period so that eventually both PLC channels received a further warning signal. They responded by commands to start the duty pump. The pump worked correctly and water pressure began to rise. At this point the operator intervened to turn off the second of the pumps; the command from PLC channel 1 to activate the reserve pump would not have had any effect without agreement from PLC channel 2 anyway. However, the discrepancy over the state of the stand-by pump persisted. Shortly after this, gas was detected as a result of the original spill. The control logic should have resulted in commands to start the duty firewater pump and to activate a general public alarm throughout the facility. However, the two PLC channels continued to show a discrepancy. Channel 1 had set the duty pump to the reserve mentioned above. Channel 2 retained the original equipment as the duty pump. The system, therefore, performed an emergency shutdown that included a loss of electrical power. This generated a further flood of alarms. It also impaired control over the ballast operation.

It is important to observe that both the suppliers and the operators involved in the incidents that form this case study were entirely unaware of the particular failure modes before they occurred. It is also important to emphasise that the case study cannot be characterised as software or a hardware failure. It stemmed from complex interactions between a number of system components.

A.4 CAUSAL ANALYSIS TECHNIQUES

Many organisations publish detailed guidance on causal analysis techniques. For example, NASA’s procedures and guidance on mishap investigation advocates several different approaches [1]. These include checklists that can be used to ensure that investigators consider a broad range of possible causal factors. They also include more open-ended approaches that do not rely on enumerations of previous problems. As we shall see, the costs associated with some of these approaches imply that the selection of appropriate techniques may depend on the resources of the organisation conducting the analysis and the perceived severity or ‘plausible worst case’ consequences of the incident under investigation.

In the following sections we will present the following sets of techniques.

Elicitation and analysis techniques

- Barrier analysis
- Change analysis

Event-based techniques

- Timelines
- Accident fault trees
- Failure event tree, ECF charts, MES and STEP

Flow Charts and Taxonomies

- MORT
- PRISMA

Accident models

- TRIPOD
- STAMP

Argumentation techniques

- WBA
- CAE diagrams

A combination of these methods might be used in an incident investigation.

A.5 ELICITATION AND ANALYSIS TECHNIQUES

A number of causal analysis techniques are tightly integrated into the elicitation of evidence and mishap reconstruction. Investigators who are still considering 'what' happened are encouraged to consider a number of possible causal factors so that they gather an appropriate range of evidence about the incident. This is important because, as mentioned previously, the investigators' initial causal hypotheses may mean that evidence is only gathered if it supports their preconceptions. Barrier analysis provides an example of this form of causal analysis technique.

A.5.1 Barrier analysis

Barrier analysis stems from work in the field of energy production. The central idea is that incidents are caused when unwanted energy flows between a source and a target. Over time this approach has been generalised to other industries so that attention focuses on the hazards that affect particular targets. Figure A.2 provides an overview of this approach. As can be seen, the adverse effects of a hazard must pass through a series of potential barriers before they can reach the ultimate target. In this case, the final barrier prevents the incident from affecting the target. This typifies the way in which a final layer of defences can make the difference between a near miss and an accident. In such circumstances, incident reports provide important insights both about those barriers that failed and those that acted to protect the target from a hazard.

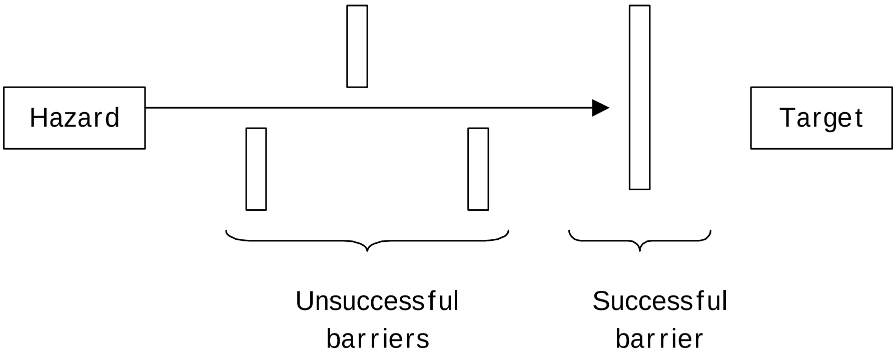


Figure A.2 Targets, hazards and barriers

Barrier analysis, therefore, begins by drawing up tables that identify the hazard and the targets involved in an incident or accident. Table A.2 illustrates these entities for the case study in this paper. This is a relatively straightforward example. For instance, it can be argued that the loss of control does not directly affect the general public. The table could, therefore, be revised to show that the loss of control only poses a direct threat to the safety of the vessel itself. However, the purpose of this exercise is to determine precisely which barriers would have to fail before potential targets might actually be affected. Hence, the initial tables of barrier analysis often try to consider as many plausible targets as possible.

Table A.2 Hazard and target identification

What?	***Rationale***
Hazard	Loss of control of key functions during emergency shutdown
Targets	Production system, operators, the environment …

The analysis progresses by examining the barriers that might prevent a hazard from affecting the targets. Analysts must account for the reasons why each barrier actually did or might have failed to protect the target. Table A.3 illustrates the output from this stage. As can be seen, the fire and gas system architecture illustrated in Figure A.2 was intended to prevent the hazard identified in Table A.2. The use of redundancy in a ‘two out of two’ architecture was specifically designed to reduce the number of spurious alarms that might otherwise have led to unnecessary ‘safe’ shut-downs. However, Table A.3 also records that this architecture is vulnerable to the inconsistencies created by transient input signals to each of the PLC channels. The table also records that the feedback of discrepancy warnings did not counter the effects of such inconsistency on the state of the channels. In this incident, PLC channel 1 monitored for the activation of the first pump and responded to the failure to agree on starting this equipment by attempting to start the backup.

Table A.3 More detailed barrier analysis

Barrier	***Reason for failure?***
Fire and gas redundant system architecture	Two out of two voting protocol susceptible to transient failures Knock-on effects of commands during discrepancy had unappreciated effects on state of PLC pipeline Safe-state trip on a discrepancy may create new hazards
Backup ballast valve control system	Crew used wrong tool to operate solenoids Omissions in crew training and maintenance procedures Need for revised hazard analysis of system operation
Pneumatic detection system in automatic deluge equipment	Non-return valves leaked Need to improve maintenance standards on non-return valves

Table A.3 also looks beyond the immediate events that led to the ‘safe’ shutdown and considers a number of related issues that helped to cause the loss of control. For example, after power was lost to the main ballast control systems it should have been possible for crew to resume manual control of the valves. However, the lack of proper tools frustrated their attempts to exploit this barrier or protection mechanism. Similarly, the deluge system was activated in the aftermath of the power failure. Pneumatic detection equipment was intended to prevent the spurious activation of this equipment. As can be seen, a series of maintenance related issues led to this protection being lost during the case study incident.

The meta-level point here is that the causal analysis technique encourages designers to look beyond the immediate triggering events that led to the mishap. It can be difficult to predict all of the possible events that might individually contribute to an adverse incident. In contrast, analysts must focus on the protection mechanisms that were in place to prevent those individual events from threatening the safety of the system.

A.5.2 Change Analysis

Change analysis provides a similar form of support to that offered by barrier analysis. Rather than focusing on those defences that either worked as intended or failed to protect a potential target, change analysis looks at the differences that occur between the actual events leading to an incident and ‘normal’ or ‘ideal’ operating practices. For example, the actual testing techniques that were deployed in a project might be compared with those described in a range of documents including internal company guidelines, contractual agreements or safety cases depending on the context in which a mishap occurred.

Table A.4 provides an example of change analysis. As can be seen the first column describes the ideal condition or the condition prior to the incident. This is an important distinction because the causes of an adverse event may have stemmed from inappropriate practices that continued for many months. In such circumstances, the change analysis would focus less on the conditions immediately before the incident and more on the reasons why practice changed from the ideal some time before the mishap.

Change analysis helps to focus on those factors that distinguish the mishap from standard operating practices or from recommended procedures. The ‘ideal’ conditions in such tables can also help to identify recommendations. This is not straightforward. For instance, stating that operators should be made aware of ‘serious’ discrepancies does little to direct the detailed development of future systems. The prior/ideal condition column in the change analysis tables can, however, provide a starting point for this analysis. Further problems complicate the application of this technique. It can be difficult to connect this form of analysis to the mass of more immediate events that are, typically, documented in the evidence that is gathered following near miss events. Event-based causal analysis techniques arguably provide a more convenient bridge to these reconstructions.

Table A.4 Change analysis

Prior/ideal condition	*Present condition*	*Effect of change*
Any (serious) discrepancy should be identified by operator and appropriate action taken to resolve discrepancy and clear any latched values.	The discrepancy was noted at such a low level that the operator was not informed. So when he/she detected the fire pump start was spurious they halted the pump but did not resolve the discrepancy between PLC channels 1 and 2.	The system was left with a latent failure in the form of the discrepancy. It was vulnerable to any genuine adverse event because the discrepancy and such an event would cause the two PLC channels to trip.
Available generator controls should be distributed across a diverse range of PLC output cards. If a card trips then it should not disable all possible generating sets.	When the PLC channels tripped, both available generators were on the same cards.	All power was lost.
Fire pump logic should operate on a one out of two principle because the adverse effects of a spurious start are negligible.	A two out of two voting protocol was used.	A discrepancy occurred from what need not have been a ‘high integrity’ output given the safe default. This discrepancy created a hazard for higher integrity outputs where two out of two was appropriate, such as a card trip event.

A.6 EVENT-BASED TECHNIQUES

Barrier and change analysis can be thought of as guides for the identification of causal factors. They provide a way of thinking about an adverse event that can also help to encourage investigators to gather additional evidence, for example about the performance of protection devices in barrier analysis. In contrast, event-based techniques focus more on documenting the events that led to a mishap. They are, therefore, based on reconstruction tools. They also often are combined with particular forms of reasoning that enable designers to identify why an incident occurred from the events that describe what happened. Time-lines provide arguably the simplest form of event-based analysis technique.

A.6.1 Timelines

Timelines are included in most accident and incident reports. They provide a straightforward and accessible representation of the ways in which events unfold over time. This is important because different analysts can use these sketches and tables to gradually piece together the events that contributed to an incident or accident. The most primitive forms of timeline can be directly extracted from system logs. For example, Table A.5 recreates part of the alarm log that might have been derived from the monitoring systems associated with our case study application.

Table A.5 Example summary from automated alarm log

Point	*Time*	*State of the alarm*	*Description*	*State at start of scan*	*Current status*	*State once scan complete*	*System*
BLS_605	11:27:20	Normal	Gas detector	Acknowledged	Reset	Deleted	Fire & gas
BLS_605	11:27:37	Beam blocked	Gas detector	Nominal	Generated	Generated	Fire & gas
BLS_605	11:27:40	Normal	Gas detector	Generated	Reset	Reset	Fire & gas
BLS_605	11:28:30	Normal	Gas detector	Reset	Acknowledged	Deleted	Fire & gas
PLW-61	11:28:32	Low pressure	Ring main - water	Nominal	Generated	Generated	Fire & gas
PLT-23	11:28:34	Loop fault	F/Disch	Nominal	Generated	Generated	Fire & gas
…	…	…	…	…	…	…	…

It is apparent from this high-level summary of alarm logs that such event based descriptions cannot directly be used to identify the underlying causes of the incidents that they depict. A further limitation is that there may be other events, including operator interventions and management decision-making processes, that will only be indirectly represented in the output of such systems. In consequence, most incident investigations construct higher-level, graphical timelines to record the events that contributed to an accident or near miss. Figure A.3 provides an example of this form of timeline for our case study.

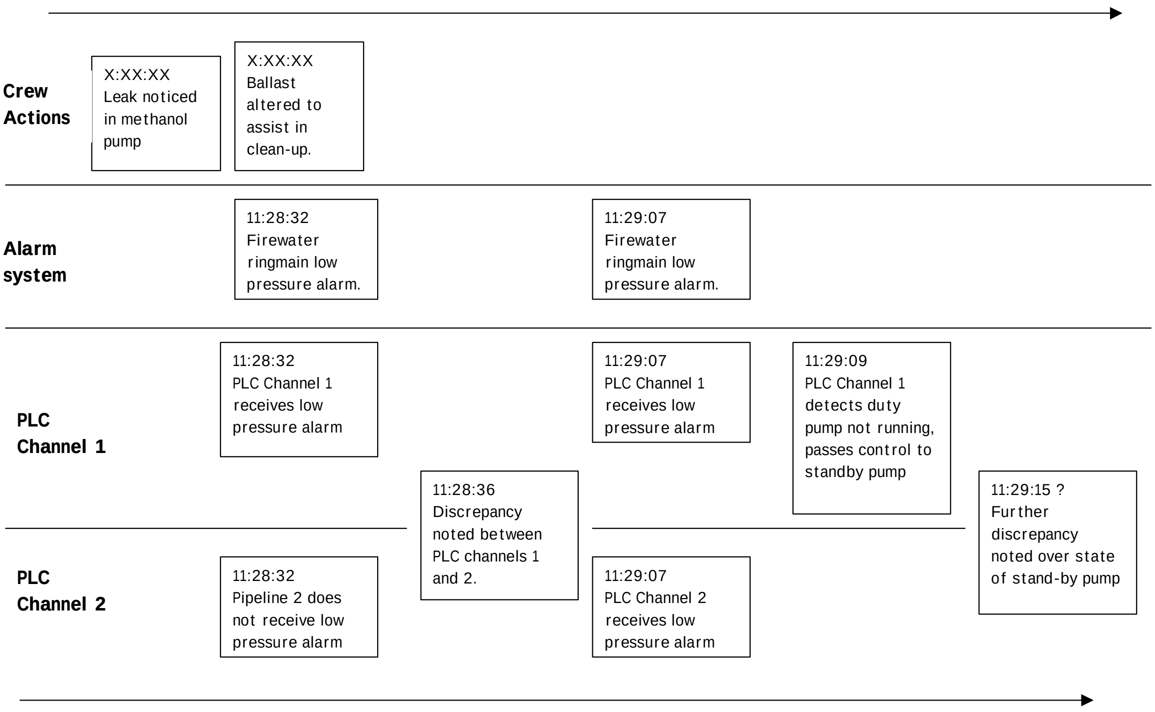

Crew Actions
X:XX:XX Leak noticed in methanol pump
X:XX:XX Ballast altered to assist in clean-up.
Alarm system
11:28:32 Firewater ringmain low pressure alarm.
11:29:07 Firewater ringmain low pressure alarm.
PLC Channel 1
11:28:32 PLC Channel 1 receives low pressure alarm
11:29:07 PLC Channel 1 receives low pressure alarm
11:29:09 PLC Channel 1 detects duty pump not running, passes control to standby pump
11:28:36 Discrepancy noted between PLC channels 1 and 2.
11:29:15 ? Further discrepancy noted over state of stand-by pump
PLC Channel 2
11:28:32 Pipeline 2 does not receive low pressure alarm
11:29:07 PLC Channel 2 receives low pressure alarm

Figure A.3 High-level timeline of the case study incident

Figure A.3 uses a technique for the development of time-lines that was pioneered by groups within the US National Transportation Safety Board [2]. The idea is to place events on a horizontal time-line but to group them according to the agents involved. In this case, the events relating to the two PLC channels are separated from the actions of the crew and so on. In practice, initial forms of this representation are often produced by sticking notes onto a blank piece of paper. Such structuring mechanisms are important if analysts are not to be overwhelmed by the mass of detail that can be obtained in the aftermath of an adverse event. There are a number of problems with the use of time-lines in the reconstruction and causal analysis of E/E/PES related incidents. Firstly, it can be difficult to obtain exact timings for asynchronous systems that lack a global clock. Hence there will often be inconsistencies and contradictory evidence for exact timings. Similarly, as in Figure A.3, there may be events where it is impossible to obtain an exact timing. This is the case for some of the crew actions that cannot be timed to the same granularity as the low-level alarms illustrated in the previous table. Such detailed criticisms have persuaded many analysts to identify alternate event-based representations that can be used to analyse adverse events at a more abstract level. The intention is not to model every detailed event that occurred but to sketch critical causal relationships between a lesser number of more important events.

A.6.2 Accident Fault Trees

A number of attempts have been made to extend fault-tree notations from the design of safety-critical systems to support the analysis of incidents and accidents. This approach has the obvious benefit that engineers who are trained in the existing use of Fault Trees can apply their knowledge and tool support to investigate the causes of adverse events. Figure A.4 provides an overview of one form of accident fault tree.

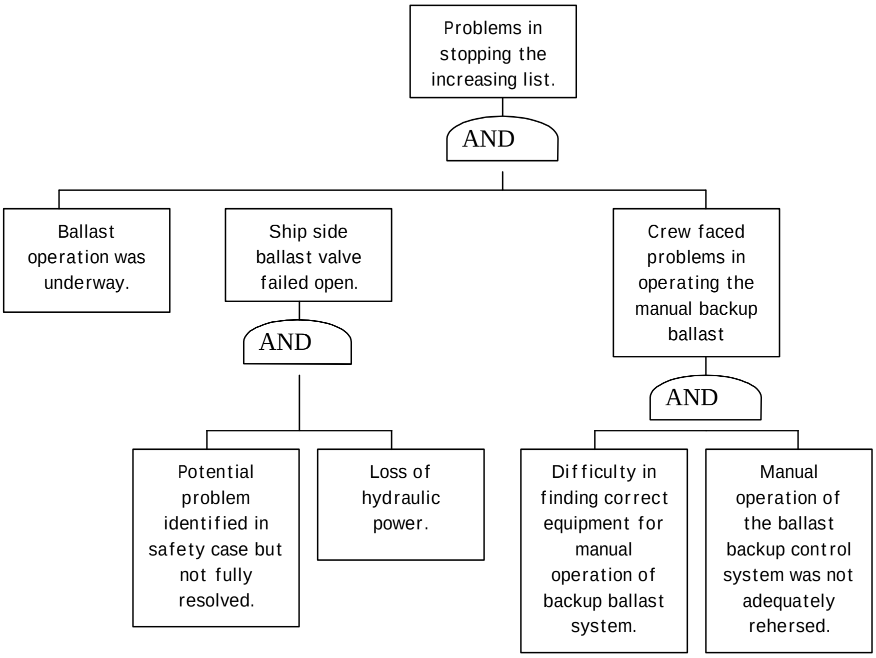

Problems in stopping the increasing list.
AND
Ballast operation was underway.
Ship side ballast valve failed open.
AND
Potential problem identified in safety case but not fully resolved.
Loss of hydraulic power.
Crew faced problems in operating the manual backup ballast
AND
Difficulty in finding correct equipment for manual operation of backup ballast system.
Manual operation of the ballast backup control system was not adequately rehersed.

Figure A.4 Overview of an accident fault tree

The events that contribute to a mishap are represented as rectangles. Logic gates are used to describe relationships between these events. In this case, the tree only includes 'AND' gates. For example, the bottom right sub-tree illustrates the observation that there was 'Difficulty in finding the correct equipment for the manual operation of the backup ballast system' AND that the 'Manual operation of the ballast backup control system was not adequately rehearsed'. These two observations together are used to conclude that the 'Crew faced problems in operating the manual backup ballast system'. This example also illustrates a number of important differences that distinguish accident fault trees from their more conventional counterparts. As mentioned earlier OR gates are not used. This would imply uncertainty in the reconstruction – there would be two alternative paths of events leading to the failure. Such uncertainty is, in general, avoided in incident investigation unless analysts are explicitly looking for alternative failure mechanisms that might lead to slightly different mishaps in the future.

There are further differences between accident fault trees and the use of this technique for design. For example, it is unclear how to represent the events that occur in the immediate aftermath of a mishap. This is important because the response to an incident can help to determine the eventual outcome. In conventional fault-trees the analysis stops with a potential hazard. Figure A.4 also illustrates the manner in which applications of this approach can blur the distinctions between events and conditions. The labels in the tree are natural language statements and they can hide a variety of important details that might themselves be represented as individual events in a more detailed tree. Finally, the construction of the trees provides little insight into the causal factors that lead to an incident. As we shall see, a range of more complex techniques, such as PRISMA, therefore uses the development of these trees as a precursor to other forms of causal analysis. These, typically, examine the events at the bottom of the tree to identify ‘root causes’.

A.6.3 Failure event tree, ECF charts, MES and STEP

The previous paragraphs described the numerous differences that exist between conventional applications of fault tree techniques and their use in the causal analysis of incidents and accidents. These differences have led a number of researchers to develop alternative techniques that are specifically designed to support both the reconstruction and the causal analysis of mishaps. There are strong similarities between techniques such as Events and Causal Factors charting (ECF), Multilinear Events Sequencing (MES) and Sequential Timed Event Plotting (STEP). Brevity prevents a detailed analysis of each of these approaches; the interested reader is directed to [2] and [3].

In contrast, Figure A.5 illustrates a further form of event plotting similar to ECF, MES and STEP. This Failure Event Tree embodies many of the ideas that are common to ‘chain of events’ models. A sequence of events leads to the mishap. These are denoted by the simple rectangles on the top half of the image. The events annotated with ‘X:XX:XX Hoses used to assist in clean-up’ and ‘11:29:07 PLC channel 1 receives low pressure alarm’ provide examples of these mishap events. Outcomes are denoted by bold rectangles with dotted borders. In this example there is only one ‘11:32:12+ Control lost over ballast operation’. In practice, however, an investigation and analysis is likely to refine Figure A.5 to consider a number of different outcome events associated with such an incident.

Figure A.5 also captures direct factors that influence the course of the incident but which cannot conveniently be represented by discrete events. These are denoted by rectangles with a double line border, such as ‘Decks not cambered’ or ‘Transient signals allowed through input processing PLCS’. In many cases, we could extend the diagram to represent these factors as events. For example, the previous observation about the construction of the vessel might be denoted by an event ‘Decision is taken to construct decks without a cambered surface’. However, it is often more convenient not to have to represent such events which may lie outside the scope of the current investigation and which can be difficult to tie into the course of events which more directly surround the incident itself. Finally, Figure A.5 captures a series of less direct factors that contribute to the incident. Many would argue that these factors represent the root causes of an accident or near-miss. Dotted double borders around a rectangle denote these. They include observations that ‘risk assessments failed to identify failure modes’ and ‘did not understand interaction between asynchronous logic and the latches, timers etc’. As can be seen, these underlying indirect factors helped to create the conditions for the more direct factors, which in turn, contributed to the actual events leading to this particular mishap.

It is important to observe that Figure A.5 provides a ‘road map’ for the causal analysis of an adverse event. As with previous representations, including fault-trees, it is intended as a living document that will change during the analysis. There are no exhaustive rules for distinguishing mishap events from direct or indirect factors. In contrast, these distinctions are the result of a process of negotiation between the participants in an investigation.

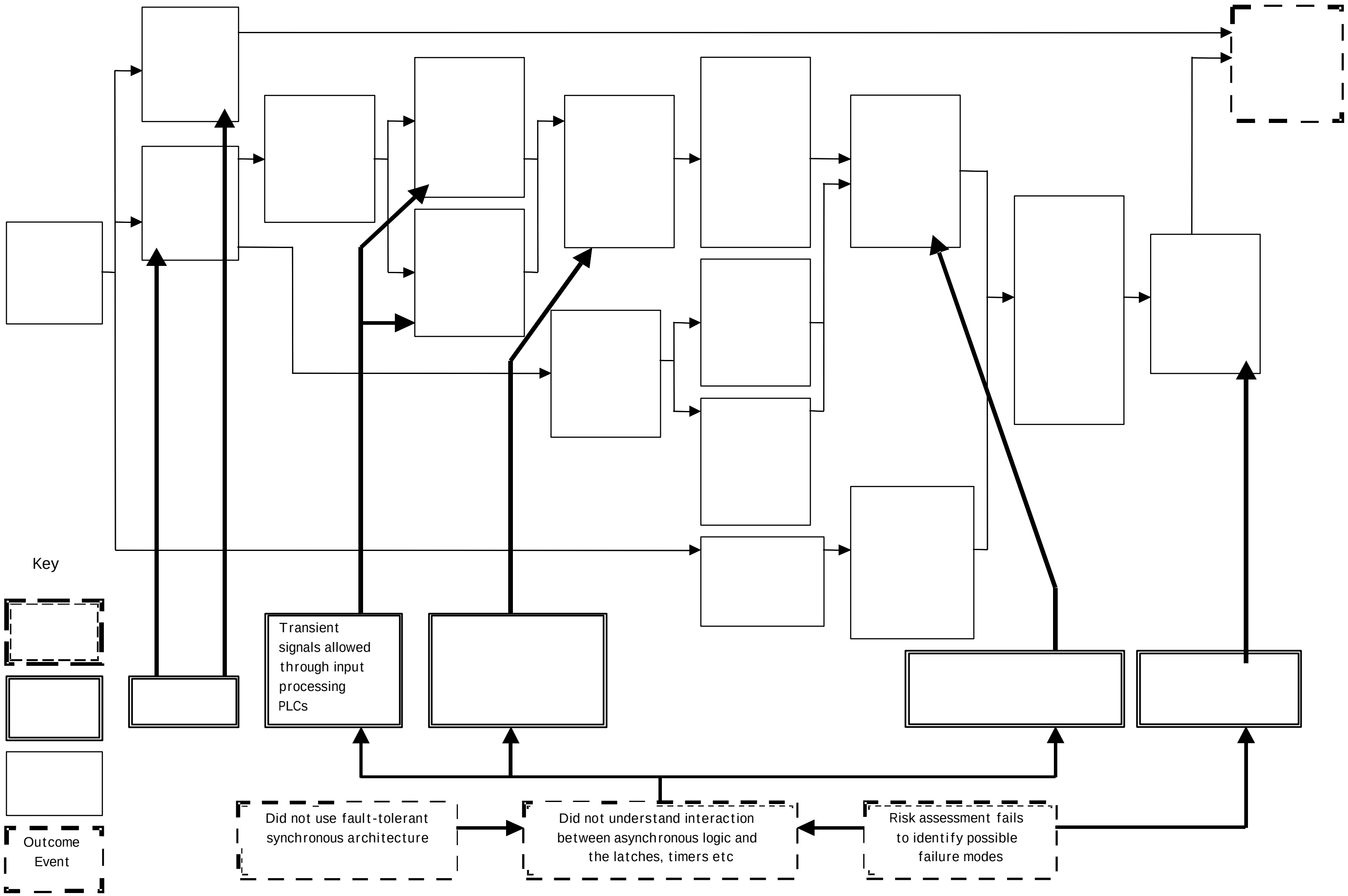

Key
Outcome Event
Transient signals allowed through input processing PLCs
Did not use fault-tolerant synchronous architecture
Did not understand interaction between asynchronous logic and the latches, timers etc
Risk assessment fails to identify possible failure modes

Figure A.5 Failure event tree

As mentioned previously, event models can be used to support the reconstruction of adverse events. They typically include a form of timeline that can be used to place individual events into the sequences that lead to incidents and accidents. The process of building such sequences can in itself help to identify causal factors. The failure event tree shown in Figure A.5 also includes a number of indirect causal factors shown as boxes below the main incident line. In other similar techniques such as Events and causal factor charting, investigators can also represent the conditions that make adverse events more likely. These indirect factors and conditions are often used to represent background factors or latent conditions that many see as the 'root causes' behind E/E/PES related failures. It is also important to stress that event based techniques are also used in conjunction with a particular style of analysis that is often regarded as the main means of distinguishing root causes from the other less significant events in such diagrams. Counter-factual reasoning is the name given to arguments that take the general form 'if X did not occur then the accident/incident would have been avoided'. This form of argument is 'counterfactual' because we know that the accident or incident did take place and we are trying to imagine ways in which we might have avoided the failure. In practical terms, analysts use this form of reasoning by looking at the event closest to the incident. In Figure A.5, we ask "would the mishap still have occurred if the electrical power had not been lost". If the answer is yes and the mishap would still have happened then this event cannot be a candidate root cause of the incident. If the answer is no and the mishap would not have occurred without this event then we can argue that it was necessary for the incident to occur so it can be considered as a root cause. The process continues for each of the mishap events shown in the diagram. Once potential root causes have been identified, remedial measures can be introduced to address the direct and indirect factors that led to each of the particular mishap events that were identified as the root causes of this mishap.

A number of criticisms can be made about 'chain of event' techniques, including failure event trees. It can be difficult to determine the scope of any investigation. The selection of an initial event in Figure A.5 is often the result of an arbitrary decision. Investigators using these techniques will often disagree about the initial events that create the preconditions for a mishap to occur. For example, we might reasonably have started the chain of events with the decision to use a ballast transfer to support the clean-up operation. Alternatively, we might have focused more on the supply chain to look at the events that helped to select an asynchronous PLC architecture over synchronous alternatives. 'Chain of events' models also often fail to distinguish between different types of events. Figure A.5 contains missing process elements, such as the failure of PLC channel 2 to receive the initial pressure warning. Others nodes represent missing controls, including the loss of electrical power. The arrows between events introduce further confusion. They represent causal relationships. For example, the command to start the duty pump and initiate a public alarm together with the existing discrepancy between the two PLC channels caused the watchdog relays to de-energise the control system. Elsewhere they represent the 'flow of events' without any causal information. For instance, the discrepancy between the two channels does not necessarily cause Channel 1 to detect that the duty pump is not running at 11:29:09. Such criticisms have resulted in alternative forms of causal analysis techniques such as Leveson's STAMP and Ladkin's WBA, which avoid some of these confusions between temporal sequences and causal relationships. Both of these techniques are introduced in subsequent sections of this document.

A.7 FLOW CHARTS AND TAXONOMIES

The previous paragraphs have described a range of techniques for identifying the causal factors that lead to adverse events. As can be seen from Figure A.5, they are capable of representing mishaps at a considerable level of detail. However, most of these techniques require specialist training. A further problem is that they do not explicitly encourage consistency between investigators. Experience in applying event modelling techniques has shown that different investigators will produce very different models of the same adverse events. In contrast, flow charts provide explicit means of encouraging inter-analyst agreement. They are also, typically, used to identify common classes of causal factors. These two properties together make them very useful for the extraction of statistical information from large-scale incident reporting systems. The flow charts help to ensure that analysts consider the same range of causal factors even though they may have minimal training and may not be in close contact with each other.

A.7.1 MORT

Management Oversight and Risk Trees (MORT) provide arguably the best-known example of a flow charting approach to the identification of causal factors [4]. As the name suggests, it is well suited for the identification of organisational issues leading to mishaps. It is less suited to the technical analysis of computer-related incidents; however, it could be extended to address this potential weakness. At the heart of MORT is a tree structure that resembles the fault tree shown in Figure A.4. Figure A.6 provides an abbreviated version of a MORT diagram.

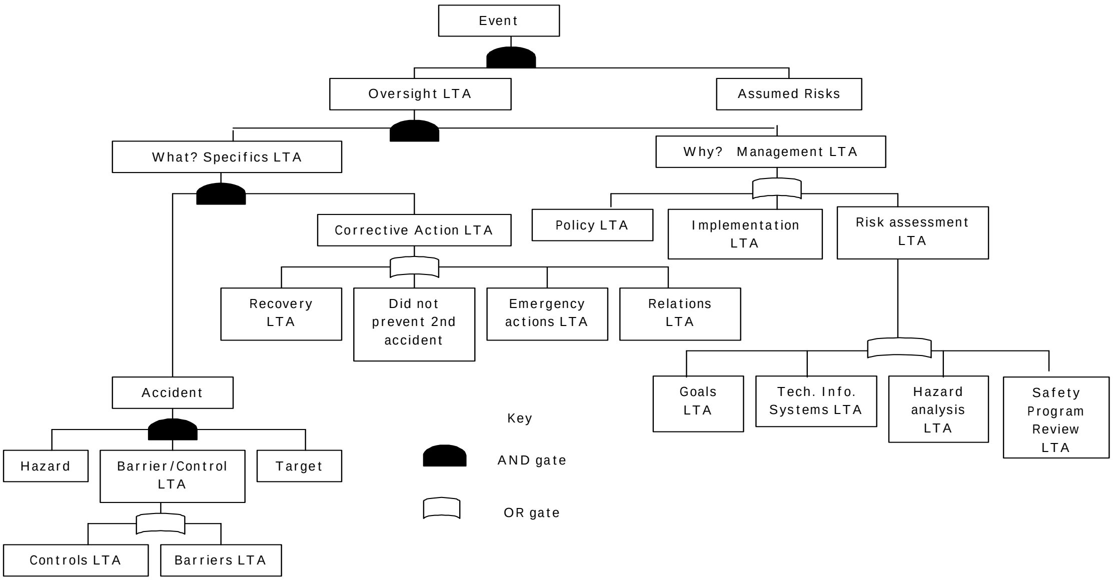


Figure A.6 Abbreviated form of a MORT diagram

The analysis begins when investigators consider the top levels of the tree. They must ask themselves whether the mishap was the result of an omission of some management function and whether the incident occurred from a risk that had already been recognised. In the tree, the term LTA refers to a ‘less than adequate’ performance of some necessary activity. If there was an oversight problem then analysis progresses to the next level of the tree. Investigators are encouraged to consider both what happened and why it happened. The reasons why an oversight might occur include less than adequate management policy, implementation or risk assessment. The analysis progresses in this manner under investigators reach a number of terminal nodes, not shown here, that describe the more detailed causes of the incident.

As can be seen from Figure A.6, the elements of the MORT tree are generic in the sense that they capture management problems that can arise in any domain. This enables comparisons to be made between the causes of mishaps in different areas of a company and even between companies in different industries. The tree structure also plays an important role in ensuring a consistent analysis because investigators ask themselves the same analytical questions in the same order determine by a left to right traversal of the diagram. For example, the analysis of the case study might begin by asking whether the oversight during either development or operation was adequate. If it was not then we can begin to analyse what happened during the incident by going down the far left branch of the figure. This involves the identification of hazards, barriers and targets in an identical fashion to barrier analysis introduced previously. After having identified these components of what occurred, analysis might go on to consider the right branches including the reasons why management might have been less than adequate. Figure A.6 encourages analysts to consider whether the policy, the implementation or the risk assessment in the design and operation of the system might have contributed to the mishap. Figure A.5 has already shown that previous risk assessments failed to uncover the potential failure modes associated with the generator controls. The right most sub-branch encourages analysts to further consider whether this was due to incorrect goals, to problems in the technical information systems that were available to management, to inadequate hazard analysis or problems in the safety program review process. The MORT handbook provides descriptions of what each of these categories means. For now it is sufficient to observe that the power generation vulnerability could be a result of inadequate hazard analysis or a failure to review the safety case that maintained that this configuration was acceptable.

As with all of the causal analysis techniques that are introduced in this document, it is important that investigators document the results of their investigations. Table A.6 illustrates one technique that can be used in conjunction with MORT diagrams such as that shown in Figure A.6. As can be seen, investigators can write a brief argument to state why a mishap was caused by one of the factors that are represented in the nodes of the tree. In this case, the risk assessment was less than adequate because the danger of a loss of control functions after a system trip for the crew and the vessel was not considered in sufficient detail. Such documentation is important if others within an organisation are to understand the reasons why particular causes have been identified in the aftermath of an adverse event or near miss incident. They can act as a focus of subsequent discussion and can help to direct resources to improve areas where previous management activities have proven to be less than adequate.

Table A.6 Documenting the products of a MORT analysis

Branch in MORT tree	*Node of MORT tree*	*Incident description*
Risk assessment less than adequate	Hazard	Loss of control of key functions during emergency shutdown
	Target	Production system, operators, the environment…
Hazard analysis less than adequate	Control operability problems	Control of power generators vulnerable to trips on PLC channels

As noted earlier, MORT is a generic technique intended to help identify management problems across many different industries. It lacks the technical details necessary for example to distinguish a failure in software requirements capture from inadequate component testing. A number of other techniques, such as PRISMA, have been developed based on the flow-chart approach to causal analysis. These provide more focused support for particular application domains.

A.7.2 PRISMA

PRISMA is a multi-stage technique. It includes an initial reconstruction based on an accident fault tree [5, 6]. The leaf or terminal nodes on the tree are then classified to identify more generic root causes. This is important because the complex differences that exist between individual incidents can often make it difficult to compare the causes of several apparently related incidents. A flow chart can, therefore, be used to provide a higher-level classification of these more detailed causes. For example, an operand error might be classified at one level as a problem with type checking. At a higher-level it might be classified as a coding error rather than a problem in requirements and so on. These higher-level categories can be used to inform the statistical monitoring of incident data and can also arguably increase consistency. Investigators may disagree about the detailed causes of an adverse event but may exhibit greater agreement about the higher-level classification.

Figure A.7 illustrates a PRISMA flow chart that was developed specifically to identify higher-level causal factors in the process industries. As can be seen, each terminal node is associated with a particular abbreviation, such as TE for a technical, engineering related cause. It is also extremely important to stress that the ordering of terminal nodes can be used to explicitly bias the insights obtained from any causal analysis. In Figure A.7, technical factors appear before organisational issues and human behaviour. It is therefore more likely that analysis will identify technical issues before considering these other potential classes of causal factors. It is also important to stress that the developers of the PRISMA approach encourage investigators to extend the classification to support their particular domain of interest. For example, medical versions include ‘patient related factors’ as a potential cause in healthcare incidents. In our case study, we might extend the flow chart to explicitly consider far more detailed technical factors than those shown in Figure A.7. For instance, we might introduce nodes to capture failures that are due to the interaction between asynchronous control algorithms and the use of latching in safety state information, including discrepancy indicators. There is a balance to be struck, however. If the flow chart is too detailed then it can quickly become intractable as other analysts attempt to discriminate between hundreds of complex categories. Conversely, if the flow chart is too general then it may yield relatively little insights into common engineering problems in E/E/PES applications.

Causal analysis is not an end in itself. It is obviously important that recommendations be derived from the findings of an investigation so that previous problems can be avoided in the future. An important strength of flow-chart methods such as PRISMA is that the generic causal classification that is used in the analysis of an adverse event can also be used to direct investigators towards a number of general solutions. For example, Figure A.8 illustrates a classification action matrix. This shows that if, for example, an incident were due to problems with management priorities then subsequent recommendations might focus more on ‘bottom-up communication’. As might be expected, this approach is intended to ensure that investigators offer a common response to incidents with similar causal factors. If incidents continue to recur with the same set of causal factors then safety managers might decide that the remedies advocated in Figure A.8 are ineffective and should be revised. In particular, it might be argued that the remedial actions should be at a far finer level of detail. In our case study, it might be advocated that modifications be made to eliminate transient inputs. For instance, the input processors in each PLC channel might ensure that such short-lived signals are sustained until the processing PLCs are sure to receive them. Such a detailed remedial action could only be represented in a classification/action matrix if the associated flow chart were extended to a similar level of complexity. It would need to consider transient signals as a potential cause of technical failure. As the sophistication of the flow-chart increases, so does the extent of the classification/action matrix unless common interventions can be identified for classes of causal factors.

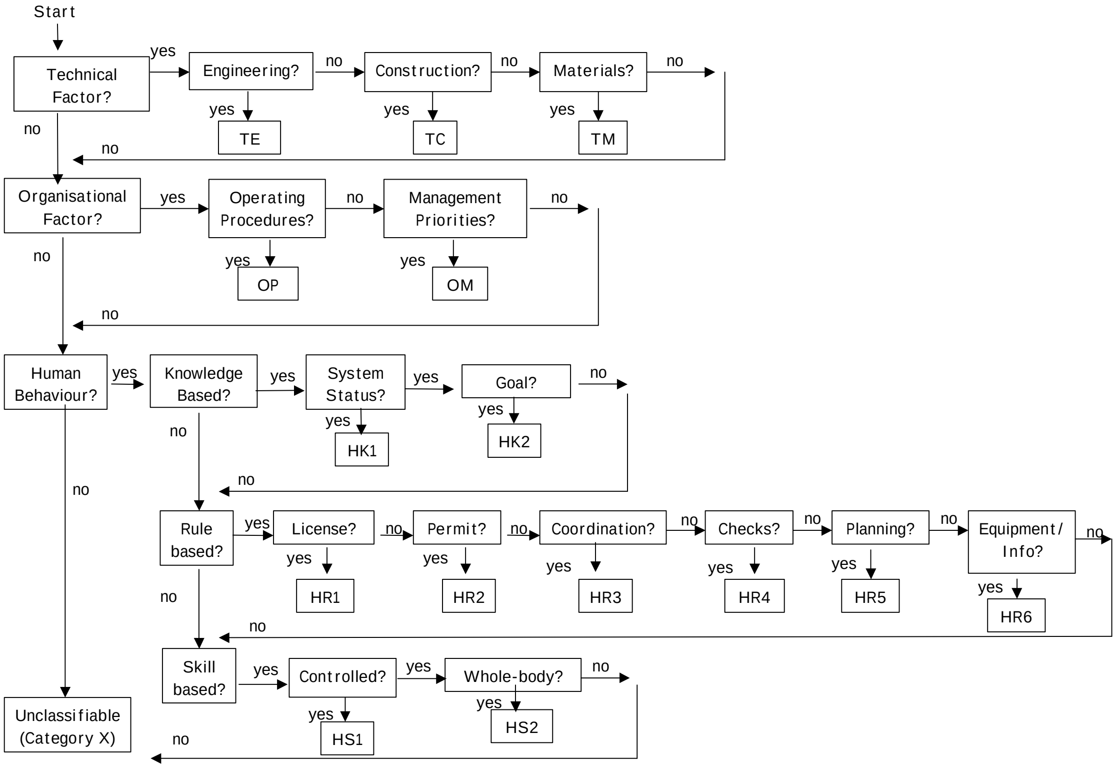


Figure A.7 PRISMA flow chart [5, 6]

	External Factors (O-EX)	Knowledge Transfer (OK)	Operating procedures (OP)	Manag. priorities (OM)	Culture (OC)
Inter-departmental communication	X				
Training and coaching		X			
Procedures and protocols			X		
Bottom-up communication				X	
Maximise reflexivity					X

Figure A.8 Example PRISMA classification/action matrix [7]

A.8 ACCIDENT MODELS

A criticism of the previous techniques discussed in this summary is that they only provide limited support for investigators who have little familiarity with the causes of many incidents and accidents. In other words, it is assumed that they understand how to produce an accident fault tree or a timeline event model from the complex events that they have witnessed or identified through the accumulation of evidence. In many cases, these assumptions are unwarranted. In consequence, causal analysis techniques have been developed around ‘accident models’. Under one interpretation these models provide strong guidance about what causes an adverse event. Less charitably it can be argued that they enforce a particular viewpoint on the analytical process.

A.8.1 TRIPOD

The TRIPOD approach to causal analysis builds on the notion that most mishaps are caused by a number of more general failure types. This idea is a relatively simple extension of the higher-level causal classification in flow-chart techniques such as PRISMA and MORT. In particular, TRIPOD distinguishes between the following causes of incidents and accidents: hardware; maintenance management; design; operating procedures; error-enforcing conditions; housekeeping; incompatible goals; communication; organisation; training; defence planning. These general failure types have strong similarities to concepts that we have met before. For example, problems in defence planning are very close to the barrier analysis that was introduced in previous sections. Other issues such as maintenance management are not explicitly considered in some of the other causal analysis techniques. Software is a notable omission from this list and must certainly be included. Our case study, however, raises the recurrent problem of whether PLC design issues relate more to hardware or software design give the particular characteristics of these implementation platforms.

TRIPOD also provides a form of graphical modelling that can be used to show how specific instances of these general failure types combine to create both necessary and sufficient causes for an incident or accident. This diagrammatical technique is illustrated in Figure A.9. As can be seen, elements of barrier analysis are again used to illustrate the manner in which a hazard can affect a target. A number of active failures can be associated with each of the defences that did not protect the target. These active failures can be thought of as the immediate events leading to the incident. The context in which they can occur is often created by a number of preconditions. For instance, one active failure stemmed from the way in which a low consequence discrepancy over the command to start the feed water pump jeopardised more critical responses to the gas detection event. The precondition for this failure was the manner in which only one of the input cards on the two PLC channels detected the pump pressure warning. This, in turn, stemmed from a latent failure to design input cards that would ensure the adequate replication of transient signals until both channels were sure of recognising them. As with flow chart techniques the intention is to move away from the specific events that led to a mishap so that greater attention is paid to the generic or systemic failures that are likely to threaten future operation. It is argued that a specific recurrence of an incident, such our case study, is unlikely. However, the same problems of hidden failure modes in combinations of asynchronous and latched systems may manifest themselves in a host of future incidents unless these latent causes are addressed.

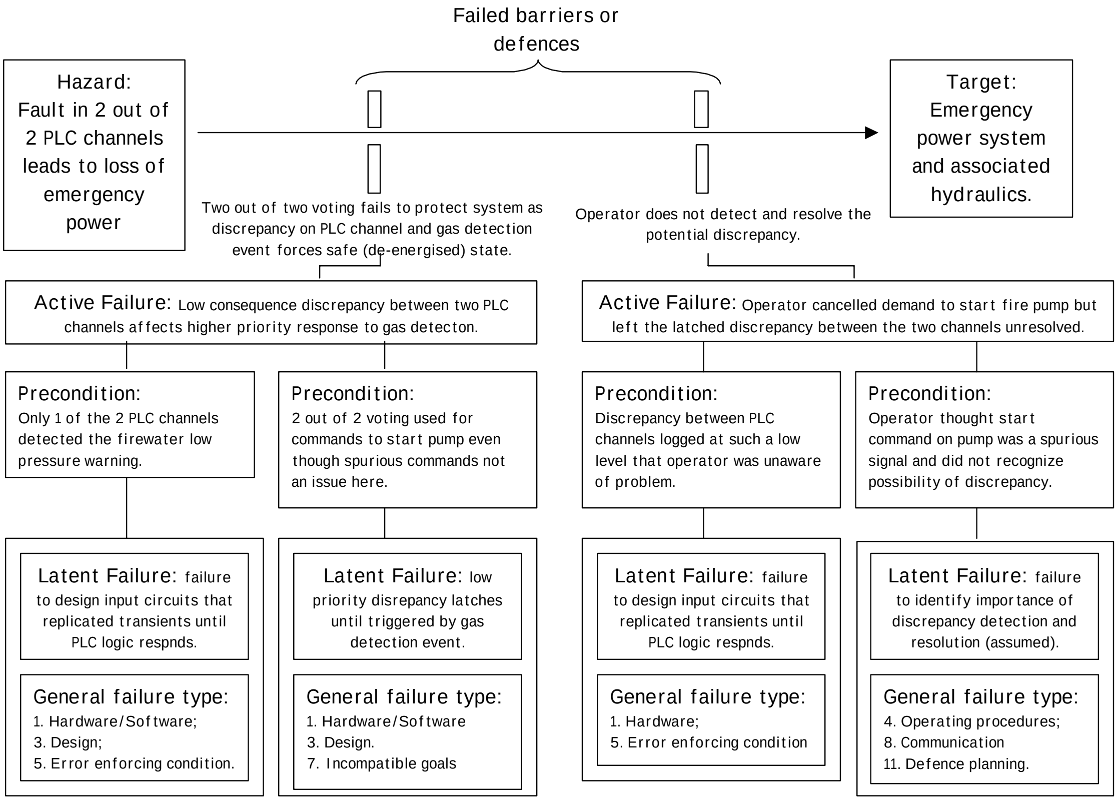

Failed barriers or defences
Hazard: Fault in 2 out of 2 PLC channels leads to loss of emergency power
Target: Emergency power system and associated hydraulics.
Two out of two voting fails to protect system as discrepancy on PLC channel and gas detection event forces safe (de-energised) state.
Operator does not detect and resolve the potential discrepancy.
Active Failure: Low consequence discrepancy between two PLC channels affects higher priority response to gas detecton.
Active Failure: Operator cancelled demand to start fire pump but left the latched discrepancy between the two channels unresolved.
Precondition: Only 1 of the 2 PLC channels detected the firewater low pressure warning.
Precondition: 2 out of 2 voting used for commands to start pump even though spurious commands not an issue here.
Precondition: Discrepancy between PLC channels logged at such a low level that operator was unaware of problem.
Precondition: Operator thought start command on pump was a spurious signal and did not recognize possibility of discrepancy.
Latent Failure: failure to design input circuits that replicated transients until PLC logic respnds.
General failure type: 1. Hardware/Software; 3. Design; 5. Error enforcing condition.
Latent Failure: low priority disrepancy latches until triggered by gas detection event.
General failure type: 1. Hardware/Software 3. Design. 7. Incompatible goals
Latent Failure: failure to design input circuits that replicated transients until PLC logic respnds.
General failure type: 1. Hardware; 5. Error enforcing condition
Latent Failure: failure to identify importance of discrepancy detection and resolution (assumed).
General failure type: 4. Operating procedures; 8. Communication 11. Defence planning.

Figure A.9 Example application of TRIPOD general failure types

As mentioned, TRIPOD embodies a model of how accidents and incidents occur. This model builds on barrier analysis and includes concepts such as general failure types, latent causes, preconditions and active failures. A range of computer-based tools also supports it, further details are provided in [8] and [9]. The meta-level point here is that the costs associated with each of the techniques described in this document can be substantially reduced by appropriate tool support. It is also possible to automatically perform certain consistency checks and search tasks for similar previous incidents using these tools [2].

A.8.2 STAMP

Leveson’s Systems Theory Accident Modeling and Process (STAMP) approach [10, 11] is similar to accident fault trees in that it attempts to apply a more general, constructive engineering tool to support the analysis of incidents and accidents. Instead of extending the use of fault trees, STAMP exploits elements of control theory to help identify causal factors. This is motivated by the observation that mishaps occur when external disturbances are inadequately controlled. Adverse events can also arise when the failure of process components goes undetected or when the actuators that might respond to such a failure are unsuccessful in their attempts to control any adverse consequences from the initial fault. Control failures can arise from ‘dysfunctional interactions’ between system components. For example, if one subsystem embodies inappropriate assumptions about the performance characteristics of another process component. In this view, mishaps do not stem from events but from inappropriate or inadequate constraints on the interactions among the elements that form complex, safety-critical applications. Safety is viewed as a dynamic property of the system because the constraints that are applied and the degree to which a system satisfies those constraints will continually evolve over time. The analysis progresses by developing a control model of the relationships between entities in the system. Figure A.10 illustrates this approach. It is important to emphasise that this diagram uses arrows to represent communication and control flows. The rectangles are entities, including people, systems and organisations; they do not represent the events shown in the failure event tree of Figure A.5.

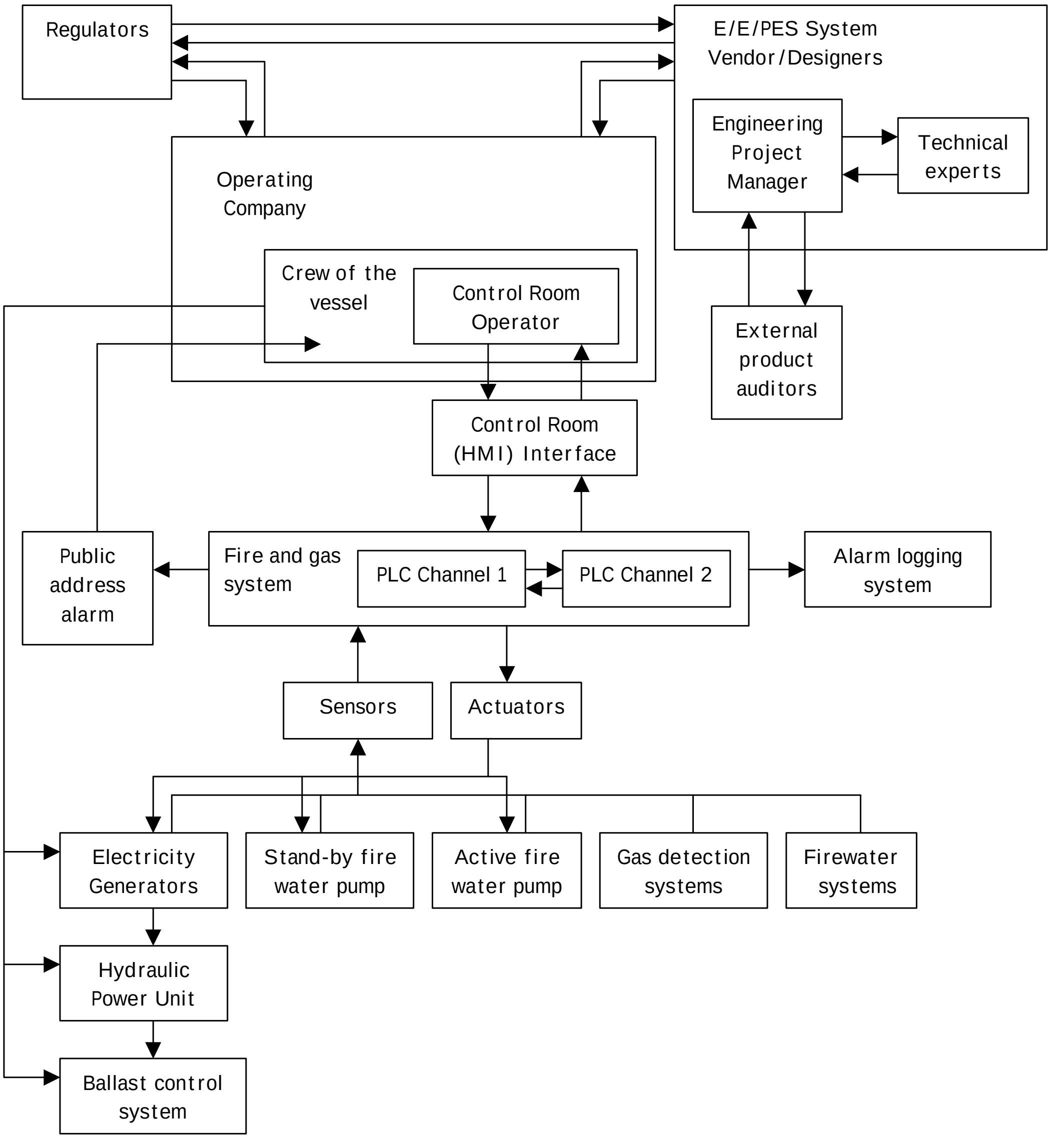
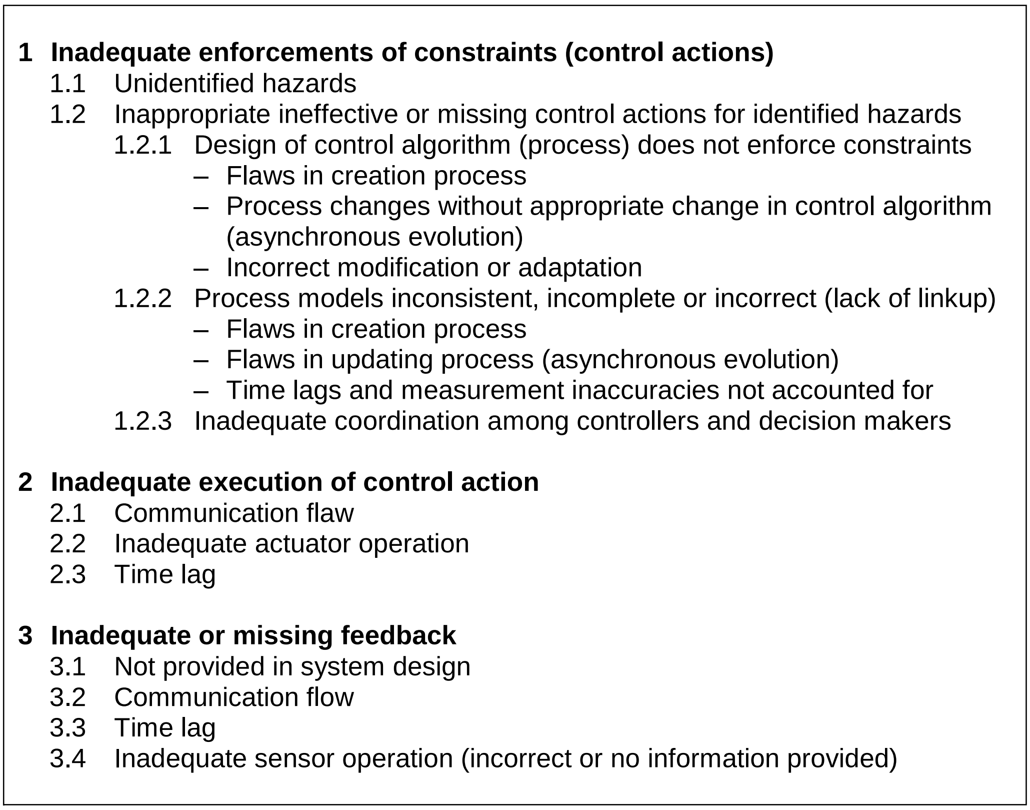


Figure A.10 Example control model from STAMP [10]

As can be seen from Figure A.10, the STAMP control analysis extends from the operator, and the systems under their immediate control to also consider the relationships between project and company management, between management and regulatory agencies and between regulation and system vendors. These different forms of interaction include the preparation, presentation and acceptance of the safety case that originally covered the design and then the operation of the application as a whole. These different relationships must be captured in any analysis because they have a profound influence on both the development and operation of safety-critical systems. The control model also considers interactions between system components. For instance, Figure A.10 traces the way in which the control room operator monitors and issues commands through their human-machine interface. This controls the fire and gas systems that included the PLC channels mentioned in previous sections. These PLC channels, in turn, interfaces with the sensors that detected the presence of gas and the falling water pressure. The output from the fire and gas system can also affect the operation of the generators and, through them, could affect the hydraulics and the ballast system. After having conducted this extended form of control analysis, the STAMP technique progresses by considering each of the control loops that are identified in the 'socio-technical system'. Potential mishaps stem from missing or inadequate constraints on processes or from the inadequate enforcement of a constraint that contributed to its violation. Figure A.11 illustrates the general classification scheme that guides this form of analysis. It provides a classification scheme that helps to identify potential causal factors in the control loops that exist at different levels of the management and operation hierarchy characterised using diagrams similar to that shown in Figure A.10.



1 Inadequate enforcements of constraints (control actions)

- 1.1 Unidentified hazards
- 1.2 Inappropriate ineffective or missing control actions for identified hazards
  - 1.2.1 Design of control algorithm (process) does not enforce constraints
    - – Flaws in creation process
    - – Process changes without appropriate change in control algorithm (asynchronous evolution)
    - – Incorrect modification or adaptation
  - 1.2.2 Process models inconsistent, incomplete or incorrect (lack of linkup)
    - – Flaws in creation process
    - – Flaws in updating process (asynchronous evolution)
    - – Time lags and measurement inaccuracies not accounted for
  - 1.2.3 Inadequate coordination among controllers and decision makers

2 Inadequate execution of control action

- 2.1 Communication flaw
- 2.2 Inadequate actuator operation
- 2.3 Time lag

3 Inadequate or missing feedback

- 3.1 Not provided in system design
- 3.2 Communication flow
- 3.3 Time lag
- 3.4 Inadequate sensor operation (incorrect or no information provided)

Figure A.11 Control flaws leading to hazards [10]

Analysis progresses by examining each of the arrows in the control model to see whether any of the flaws in Figure A.11 can be identified in the relationships that they represent. It might be argued that there were unidentified hazards in the control loop between the PLC channels and the generators. Similarly, subsequent investigation might identify flaws in the creation process that led to the human-machine interface design's representation of the sate of the fire and gas system. It is important to note that the inclusion of control flaws 2.3 'time lag', 1.2.2 'Time lags and measurement inaccuracies not accounted for' and 3.4 'Inadequate sensor operation (incorrect or no information provided)' illustrate the control theory roots of this technique. These control flaws also demonstrate the suitability of the STAMP technique for our E/E/PES case study.

Figure A.11 illustrates the high-level similarities between STAMP and previous techniques such as PRISMA and even MORT. All of these approaches rely upon taxonomies of general causal factors. These lists of potential problems help investigators to focus their analysis and can also ensure consistency. It is important to emphasise that STAMP is a relatively new technique. However, there are already a number of case studies in which this approach has been applied to support the analysis of E/E/PES related incidents. These are, however, focused on high-consequence mishaps given the potential overheads that stem from the development of detailed reconstructions and control models.

A.9 ARGUMENTATION TECHNIQUES

Previous approaches have focused on the identification of causal factors by the modelling of adverse events or of control relationships. Investigators are then expected to exploit a range of informal arguments to identify the root causes that are represented in these models or diagrams. This informal reasoning often exploits counter-factual arguments of the form 'the accident would not have occurred if causal factor X had also not occurred. Unfortunately, this form of reasoning can be very unreliable. Implausible arguments can be made so that the causal factor may have no apparent relationship to the incident itself. For instance, we can argue that 'the incident would not have happened if we had been given an infinite amount of money to spend on the testing phase'. In our case study, we might argue that the incident would have been avoided if the PLC channel had been designed to use synchronous redundant channels with guaranteed bounded skews between resynchronisation points. The use of causal analysis techniques does not, therefore, avoid the arguments that often arise about what are and what are not plausible causes of an adverse event. Several techniques have, however, been developed to help ensure that investigators form 'reasonable' causal arguments from the evidence that is embodied in timelines and other reconstructions.

A.9.1 WBA

Ladkin and Loer's Why-Because Analysis [12] begins by a reconstruction phase during which a graphical notation constructs sequences of events leading to a mishap. The angled arrows shown in Figure A.12 illustrate this. As can be seen, the leak in the methanol plant occurs before the ballast is altered to assist in the clean up operation and before the hoses were used. It is important to stress, however, that this sequential information does not imply causation. We cannot in this early stage of the analysis say that leak necessarily caused the change in ballast. In order to make this argument we must demonstrate that we have identified sufficient causes for an 'effect' to occur. For example, they may have been other factors including previous operational experience in successfully following this approach that justified its use by the crew. A more sustained causal analysis must consider these additional issues in order to fully explain the reasons why the ballast was altered in the lead up to the incident.

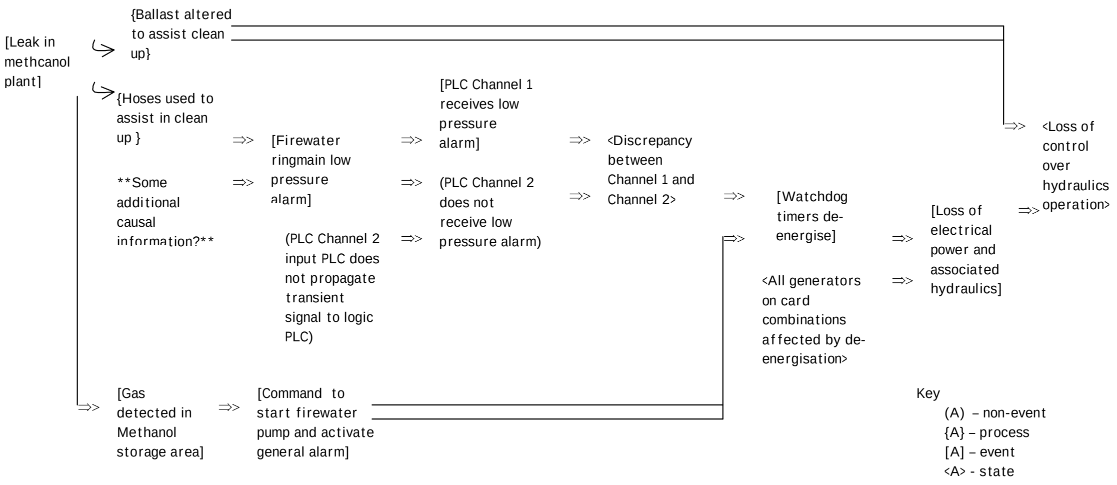

[Leak in methcanol plant]
{Ballast altered to assist clean up}
{Hoses used to assist in clean up }
Some additional causal information?
[Firewater ringmain low pressure alarm]
(PLC Channel 2 input PLC does not propagate transient signal to logic PLC)
[PLC Channel 1 receives low pressure alarm]
(PLC Channel 2 does not receive low pressure alarm)
<Discrepancy between Channel 1 and Channel 2>
[Watchdog timers de-energise]
<All generators on card combinations affected by de-energisation>
[Loss of electrical power and associated hydraulics]
<Loss of control over hydraulics operation>
[Gas detected in Methanol storage area]
[Command to start firewater pump and activate general alarm]
Key
(A) – non-event
{A} – process
[A] – event
<A> - state

Figure A.12 Example WBA diagram

Once analysts are convinced that they have considered a sufficient set of causal factors for an effect they can then revise the WBA diagram illustrated in Figure A.12. A double arrow denotes causal relationships =>>. As can be seen, the leak in the methanol plant was a sufficient cause for gas to be detected in the storage area. No further explanation need be considered at this stage. However, if we look at the causes for the low-pressure alarm on the ring main then we can see that the use of the hoses in the clean-up operation may provide an insufficient explanation. Further analysis is required to determine exactly why such a routine cleaning procedure resulted in a warning when fire-fighting activities might require a greater volume of water than was needed in this clean-up operation. Informally, the analysis proceeds by examining each node in the diagram to create statements of the form ‘Why did A occur, because of B and C and D…’. This transition from temporal sequences to more rigid causal relationships can produce insights that are not apparent in purely event-based approaches, such as timelines. For example, in order to explain why power was lost following the intervention of the watchdog timers we must understand the way in which the generators were controlled by the same card combinations that were used by the gas and fire system. This is explicitly represented in Figure A.12 but was not previously included in the event-driven approach of Figure A.5’s Failure event tree.

The most striking feature of WBA is that it provides a set of mathematically based procedures that analysts must follow in order to replace the angled arrows of a temporal sequence with the double headed arrows of the causal relationship. These procedures are necessary to ensure that we have established sufficient causes for the effect to occur. They are based on arguments of the form ‘A causes B’ if B is true in possible worlds that are close to those in which A is true, which can in turn be given a counterfactual semantics. In other words, if we know that A and B occurred and that if A had not occurred then B would not have occurred then we can conclude that A causes B. Ladkin and Loer also provide a range of additional proof rules that can be used to ensure both the consistency and sufficiency of arguments about the causes of a mishap. The full form of Why-Because Analysis includes techniques for reasoning about operator behaviour as well as component failures. However, the proponents of this approach argue that analysts should only recruit the level of formality that is appropriate to their needs. Increasing the level of detail in a supporting proof can lead to a corresponding if not a proportionately greater increase in the resources that are required by any analysis. Tool support is available. However, in practice investigators are faced with a decision between restricting their analysis to the more accessible aspects of the informal graphical reasoning, based on diagrams such as that shown in Figure A.10, and more complete forms of WBA involving the use of discrete mathematics. It seems likely that this fuller form of analysis would only be justified for high consequence mishaps. The transition from temporal sequences to causal relationships, illustrated in the previous paragraph, yields the greatest insights using this approach and is usually adequately supported by a less formal approach.

A.9.2 CAE diagrams

The ultimate aim of any causal analysis is to trace the recommendations that might be made in response to an adverse event or near miss. Table A.7 illustrates the general format of a recommendation table. These provide a simple means of linking the products of a causal analysis to the recommendations that are intended to avoid any recurrence and also to the evidence that justifies any potential intervention. For instance, a recommendation to make temporary modifications to eliminate transient input signals to the PLC channel is supported by the argument that such a condition triggered the case study. There is evidence to support this argument from the logs and from simulator reconstructions. It can, however, be difficult to construct such tables for complex incidents. There may be many hundreds of items of evidence in complex failures. Similarly, can be competing arguments that undermine particular recommendations. For instance, any decision to introduce a temporary fix may introduce further failure modes. It might, therefore, be better to operate the existing system until a full re-design can be completed.

Table A.7 General format for a recommendation table

Conclusion/recommendation	*Root cause (analysis)*	*Supporting evidence*
C1 Temporary modification to eliminate transient signals	A1.1 Input discrepancy between PLC channels 1 and 2 created necessary precondition for incident	E1.1.1 Fire and gas system logs (see table A.5) E1.1.2 Simulations run by supplier after the incident
C2 Replace tools to operate ballast system using manual backups	A2.1 Incorrect tool used to operate solenoid valves on ballast backup	E2.1.1 Witness statements E2.1.2 Deficiencies in the existing procedures and manuals covering ballast related mishaps E2.1.3 Deficiencies in the existing safety case and hazard assessment documents

Conclusion, analysis and evidence (CAE) diagrams can help designers to map out the competing arguments for and against particular conclusions or recommendations in the aftermath of a complex incident. These diagrams are simpler than many of the techniques we have described [2]. This approach lacks the consistency and completeness checks that are provided by the formal reasoning in the WBA technique. However, the reliance on a graphical formalism together with less strict rules on how to conduct the analysis can arguably reduce the costs and increase the flexibility of this approach. In consequence, although these techniques stem from similar motivations they offer different degrees of support depending on the resources of time, expertise and money that are available to an investigation.

Figure A.13 provides an example of a CAE diagram. As can be seen, rectangles are connected to form a network that summarises arguments about an incident or accident. As the CAE name suggests, the rectangles labelled with a C are used to denote conclusions or recommendations, those labelled with an A are lines of analysis while the E rectangles denote evidence. Lines are drawn to show those lines of analysis that support particular conclusions. For example, the recommendation to introduce temporary modifications (C.1) is supported by the argument that this would address the input discrepancy noted for PLC channels 1 and 2 (A1.1). The evidence for this assertion is provided by the fire and gas alarm system logs (E1.1.1) and by simulations (E1.1.2). It is important to note that Figure A.11 also captures contradictory arguments. For instance, the dotted line in the first of the networks denotes that the temporary fix recommended in C1 is not supported by the argument that a longer term upgrade will have to be made (A1.2) and that previous temporary fixes provide evidence of the danger of such short-term measures (E1.2.1).

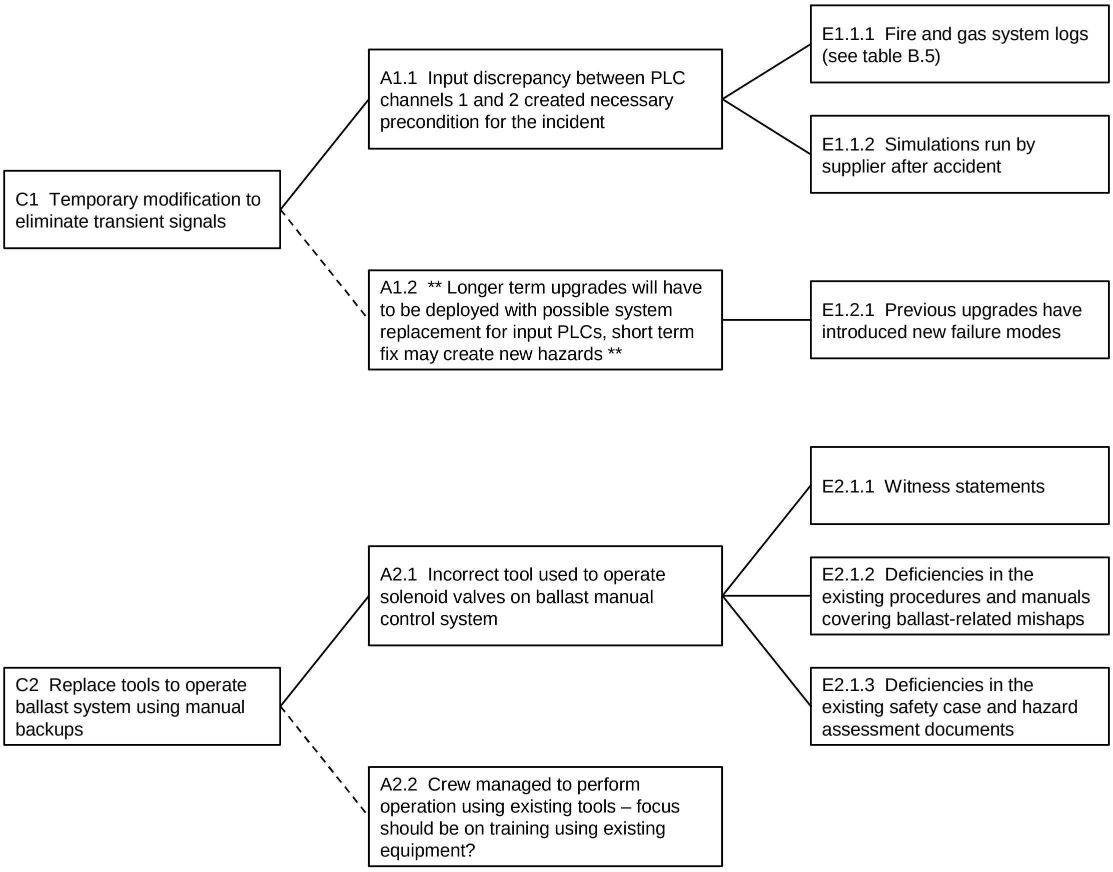

E1.1.1 Fire and gas system logs (see table B.5)
A1.1 Input discrepancy between PLC channels 1 and 2 created necessary precondition for the incident
E1.1.2 Simulations run by supplier after accident
C1 Temporary modification to eliminate transient signals
A1.2 ** Longer term upgrades will have to be deployed with possible system replacement for input PLCs, short term fix may create new hazards **
E1.2.1 Previous upgrades have introduced new failure modes
E2.1.1 Witness statements
A2.1 Incorrect tool used to operate solenoid valves on ballast manual control system
E2.1.2 Deficiencies in the existing procedures and manuals covering ballast-related mishaps
C2 Replace tools to operate ballast system using manual backups
E2.1.3 Deficiencies in the existing safety case and hazard assessment documents
A2.2 Crew managed to perform operation using existing tools – focus should be on training using existing equipment?

Figure A.13 Example CAE diagram

The lower of the two networks in Figure A.13 illustrates the argument that tools need to be replaced to help the crew operate the ballast system using the manual backup controls (C2). This recommendation is based on the observation that incorrect tools were used during the incident to operate the solenoids and that this hindered the crews' intervention (A2.1). This argument is based on evidence of witness statements (E2.1.1), on deficiencies in the manuals

(E2.1.2) and the safety-case which fails to consider the potential problems in operating this defence mechanism (E2.1.3). The recommendation to introduce new tools is weakened by an argument that the crew managed to intervene eventually with existing resources and that the introduction of new tools should not take the focus away from revised training procedures to guide any response to such an incident in the future. As can be seen from Figure A.13, CAE diagrams capture general arguments about incidents and accidents. For example, a conclusion might refer to a recommended action, it need not simply capture a causal relationship. It is also important to mention that this technique was specifically developed to enable investigators to sketch out the arguments that might appear in an incident report. This helps to ensure that any document avoids contradictory arguments.

A.10 CONCLUSIONS

This paper has provided a brief overview of causal analysis techniques. We have identified several main classes: elicitation and analysis techniques, such as barrier analysis; event-based techniques, including accident fault trees; flow Charts, including those within the PRISMA approach; accident models, including the control theory model in STAMP; argumentation techniques, such as the counterfactual approach in WBA. The techniques differ according to the amount of investment, in terms of training and investigators’ time, that is required in order to apply them. They also differ radically in the degree of support that they provide in terms of the consistency that might be achieved between individuals applying the same approach to the same incident. A more detailed introduction to various causal analysis techniques and a cost-benefit survey of the various approaches can be found in Johnson (2003).

This paper has presented a limited selection of causal analysis techniques. For instance, we have not considered stochastic modelling or formal, mathematically based approaches [2]. The selection of particular techniques has been based narrowly on pragmatic concerns, including the degree of previous commercial uptake and the number of previous case studies in E/E/PES related systems. It is also important to stress that this review reflects the subjective opinions of the author. Much work remains to be done to validate particular views, for example about the degree to which a technique supports the consistent causal analysis of adverse events. The intention has, however, been to provide a basic road map for the range of approaches that might be used to analyse the causes of E/E/PES related incidents.

A.11 REFERENCES

[1] NASA, NASA Procedures and Guidelines for Mishap Reporting, Investigating and Record-keeping, Safety and Risk Management Division, NASA Headquarters, NASA PG 8621.1, Washington DC, USA, http://www.hq.nasa.gov/office/codeq/doctree/safeheal.htm, 2001.

[2] C.W. Johnson, A Handbook for the Reporting of Incidents and Accidents, Springer Verlag, London, UK, http://www.dcs.gla.ac.uk/~johnson/book, 2003.

[3] Department of Energy, DOE Guideline Root Cause Analysis Guidance Document, Office of Nuclear Energy and Office of Nuclear Safety Policy and Standards, U.S. Department of Energy, Washington DC, USA, DOE-NE-STD-1004-92, http://tis.eh.doe.gov/techstds/standard/nst1004/nst1004.pdf, 1992.

[4] W.G. Johnson, MORT Safety Assurance Systems, Marcel Dekker, New York, USA, 1980.

[5] T.W. van der Schaaf, Near Miss Reporting in the Chemical Process Industry, Technical University of Eindhoven, Eindhoven, The Netherlands, 1992.

[6] T.W. van der Schaaf, PRISMA: A Risk Management Tool Based on Incident Analysis, International Workshop on Process Safety Management and Inherently Safer Processes, October 8-11, Orlando, Florida, USA, 242-251, 1996.

[7] W. van Vuuren, Organisational Failure: An Exploratory Study in the Steel Industry and the Medical Domain, PhD Thesis, Institute for Business Engineering and Technology Application, Technical University of Eindhoven, Eindhoven, The Netherlands, 2000.

[8] J.A. Doran and G.C. van der Graaf, Tripod-Beta: Incident Investigation and Analysis, Proceedings of the International Conference on Health, Safety and the Environment, Society of Petroleum Engineers, New Orleans, USA, 9-12 June, 1996.

[9] P. Hudson, J. Reason, W. Wagenaar, P. Bentley, M. Primrose and J. Visser, Tripod-Delta: Pro-active Approach to Enhanced Safety, Journal of Petroleum Technology, 40, 58-62, 1994.

[10] N. Leveson, A Systems Model of Accidents. In J.H. Wiggins and S. Thomason (eds) Proceedings of the 20th International System Safety Conference, 476-486, International Systems Safety Society, Unionville, USA, 2002.

[11] N. Leveson and P. Allen, The Analysis of a Friendly Fire Accident Using a Systems Model of Accidents. In J.H. Wiggins and S. Thomason (eds) Proceedings of the 20th International System Safety Conference, International Systems Safety Society, Unionville, USA, 2002.

[12] P. Ladkin and K. Loer, Why-Because Analysis: Formal Reasoning About Incidents, Bielefeld, Germany, Document RVS-Bk-98-01, Technischen Fakultat der Universitat Bielefeld, Germany, 1998.

APPENDIX B INTERVIEW BRIEF

The following interview brief was used to prompt discussion. However, since the interviewees covered different industries and elements of the supply chain, the brief was used only as a guide. The main objective was to discover current industry practice in learning from incidents.

B.1 COPY OF THE BRIEFING DOCUMENT

INDUSTRY CONSULTATION ON INCIDENT REPORTING AND ANALYSIS SCHEMES

Background

The UK Health & Safety Executive is sponsoring a project to develop a generic incident reporting and analysis scheme. The scheme is designed to be flexible and extensible so that it may be tailored to different domains, and to organisations with varied experience of incident reporting and different levels of organisational maturity. HSE has contracted a consortium, led by Adelard LLP and also involving the Glasgow (University) Accident Analysis Group (GAAG) and Blacksafe Consulting to undertake this project.

As part of this project, the consortium is consulting with industry to identify and evaluate existing schemes for classifying causes from incident data and generating lessons to avoid recurrence of similar incidents. The consultation also wishes to understand the potential constraints and barriers to implementing such schemes. The results of this study will be used in the development of the generic HSE reporting scheme.

General Approach

Our approach is to aim for a structured but fairly free ranging discussion within which we hope to ensure that the topics are covered. We do not propose to go through the questions as in some forms of market survey. The interviews are likely to be constrained by time and the availability of people so we will have to prioritise the topics during the interview.

We recommend that some of the discussion focuses on experience on real operational facilities, particularly the use of existing schemes.

Ideally, we would like to conduct the meeting in a group, representing both safety management and operational functions. This is to elicit both strategic and practical issues concerning the design and use of such schemes and any supporting systems.

Confidentiality

Notes will be taken at the meeting, but these will be kept confidential within the project – they will not be seen by HSE. The intention is to extract generic, non-ascribable information.

Where we see any benefit in documenting information pertaining to a specific organisation (even through covert recognition), we will seek permission in advance, and provide a copy of the written material for review and approval. In general, where we intend to reuse material we will remove any specifics that would tend to identify a particular organisation or individual (unless specifically approved by the organisation and individuals concerned).

Interview Outline

1 Background to the HSE project

2 Objectives of the consultation

3 Company safety management approach with linkage to incident reporting

4 Approach to incident reporting

- What are the incident criteria used to initiate a recording and analysis of an incident. Can you provide some examples that show when an incident report was initiated and some examples that show when no further action was taken to investigate.

- Reporting (what types of incident reported, forms, classification)

- Analysis (how analysed for cause)

- Generation and tracking of recommendations / feedback to operations

5 Handling of incidents involving safety related systems

- Does this include abnormally high failure rates as well as individual incidents caused by safety system malfunctions?

- Interfaces to suppliers (reporting and feedback)

6 Interfaces to other company processes, eg new projects

7 Supporting procedures, software and tools

- What tools, benefits and problems of software support

8 Measures of effectiveness

- Cost of implementing and operating the scheme

- Incident rates (reducing?, at a low level?)

9 PES specific questions

- What are the design standards for E/E/PES safety related systems in new projects?:
    - IEC 61508
    - sector standards equivalent to IEC 61508
    - other standards based on a safety lifecycle approach
    - product standards

- Are legacy E/E/PES-based facilities reconsidered and classified according to the safety integrity level requirements within IEC 61508?

- What percentage of reported incidents involve E/E/PES safety related systems?

- Are repeated failures of the E/E/PES safety related systems detected by routine testing regarded as an incident and subject to causal analysis? How would the repeated failures be detected?

- Is a demand on an instrument protection system treated as an incident? Would frequent demands be treated as an incident? How would the repeated demands be detected and how would they be reported and analysed?

- How are incidents involving E/E/PE safety related systems fed back to designers of new facilities to minimise repeat occurrence and maximise lessons learned?

- What is the format and status of the feedback to designers?

- If a generic reporting and analysis scheme is in operation, do specialists in E/E/PES technology become involved for certain types of incident? What would be the condition for E/E/PES specialist involvement and would they use a specialist E/E/PES reporting and analysis system?

- Do any of your E/E/PE safety related vendors operate a scheme that alerts you to dangerous failures of their system that have been reported by other users? Give some indication of the percentage of vendors operating schemes of this kind.

General Discussion

- Opinions on best approach, constraints on implementation, limitations, etc.

- Would you be prepared to attend a meeting in London on 5 November with other project participants to discuss the findings so far of this research project? The meeting would seek to establish consensus on the direction of future work and the type of system that would provide most value.

Printed and published by the Health and Safety Executive
C1.10   12/03

HSE
BOOKS

MAIL ORDER
HSE priced and free
publications are
available from:
HSE Books
PO Box 1999
Sudbury
Suffolk CO10 2WA
Tel: 01787 881165
Fax: 01787 313995
Website: www.hsebooks.co.uk

RETAIL
HSE priced publications
are available from booksellers

HEALTH AND SAFETY INFORMATION
HSE Infoline
Tel: 08701 545500
Fax: 02920 859260
e-mail: hseinformationservices@natbrit.com
or write to:
HSE Information Services
Caerphilly Business Park
Caerphilly CF83 3GG

HSE website: www.hse.gov.uk

RR 179

£15.00

ISBN 0-7176-2787-X

9 780717 627875