Using the IEC 61508 Lifecycle and Common Requirements to Guide the Investigation and Analysis of Incidents Involving Electrical, Electronic or Programmable, Electronic Systems

Executive Summary:
A range of investigation techniques have been developed to help identify the causal factors that contribute to adverse events and near miss incidents. Unfortunately, few of these techniques have been applied to support the analysis of mishaps involving electrical, electronic or programmable electronic systems (E/E/PES). In a previous paper, we have reviewed a range of causal analysis techniques that can support the investigation of this class of incidents (Johnson, 2002). The following pages build on this analysis and present two complementary investigation techniques. One is intended to provide a low-cost and lightweight approach that is appropriate for low consequence events. It is based around a flowchart that prompts investigators to identify potential causal factors through a series of questions about the events leading to a failure and the context in which an incident occurred. The second approach is more complex. It involves additional documentation and analysis. It is, therefore, more appropriate for incidents that have greater potential consequences or a higher likelihood of recurrence. This approach uses Events and Causal Factors (ECF) modelling together with particular forms of causal reasoning developed by the US Department of Energy (1992). Both approaches provide means of mapping causal factors back to the lifecycle phases and common requirements described in the IEC 61508 standard. This provides an important bridge from the products of mishap analysis to the design and operation of future safety-critical systems.

Version 1: 30th January 2003 – initial version
Version 2: 4th February 2003

Introduction

It is important to learn as much as possible about the causes of an incident or accident if designers are to guard against any future recurrence. Causal analysis techniques provide a means of identifying the reasons why an adverse event occurred. Very few of these approaches have been applied to support the analysis of incidents involving Electrical, Electronic or Programmable, Electronic Systems (E/E/PES). In a previous paper, we have provided guidance on how existing causal analysis techniques can be applied to improve our understanding of E/E/PES related incidents (Johnson, 2002). In this paper, we identify two existing causal analysis techniques that provide particular support for this class of incidents and near misses. Appendix A presents the criteria that guided our decision. In contrast, we focus on the investigation schemes that incorporate these two forms of causal analysis. The output from both schemes can target the allocation of future resources following the development model that supports the IEC 61508 standard.

Case Study Incidents

An E/E/PES case study will be used to illustrate the investigation techniques in this paper. This incident has been chosen through consultation with the UK Health and Safety Executive (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.* 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.

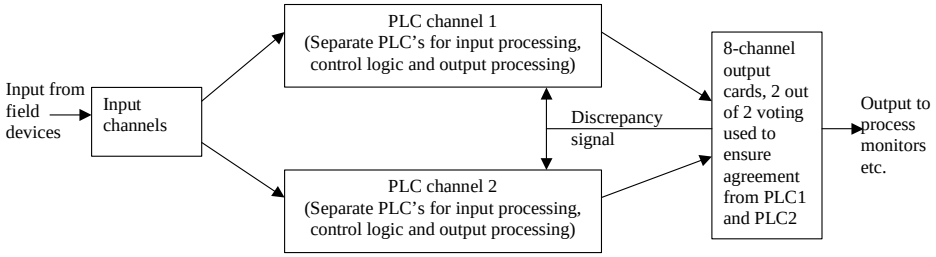


Figure 1: High-level architecture for the E/E/PES Case Study

Figure 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 PLC's 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.

Structure of the Report

This section has introduced the objectives for our work and has briefly described the case study that illustrates the remainder of this paper. Figure 2 provides an overview of our two investigation schemes. The following pages are structured around the stages in each of these approaches.

The next part of this paper addresses the first stage in the investigation process. This section introduces techniques that can be used to elicit information in the aftermath of an E/E/PES related incident. Standard incident reporting forms prompt operators, investigators, component suppliers and integrators to provide necessary information about failures and near misses. We, therefore, describe the information that should be requested by these forms. We also describe how barrier and change analysis provide techniques that can be used to identify additional information requirements during the immediate response to any E/E/PES related incident.

Section B of this report goes on to describe two different forms of causal analysis. In particular, we are concerned to identify a relatively simple approach that is appropriate for lower consequence incidents. This approach builds on a flowchart. Investigators can identify and categorise the causes of any E/E/PES related mishap by answering a series of questions. The responses that they provide will guide the causal analysis until problems are diagnosed in the IEC 61508 lifecycle or in the common requirements between phases of that lifecycle.

We are also concerned to identify a second, more complex, causal analysis technique for incidents that pose a higher risk of recurrence. This approach is suitable for incidents that cannot be categorised using the prompts of the flowchart approach, mentioned above. Our more complex approach involves additional stages of analysis that produce intermediate documentation. This is necessary when investigators have to justify their conclusions to other investigators, safety managers and courts of law. In particular, the second

approach relies upon a timeline reconstruction of an adverse event using a technique known as Events and Causal Factors charting. This approach was developed by the US Department of Energy (1992) and has been widely applied in the process industries. It produces a graphical sketch of the events leading to an incident. These diagrams can be inspected to distinguish contextual information from causal factors. In our proposed method, causal factors can then be analysed to identify potential failures in the IEC 61508 lifecycle or in the common requirements mentioned above.

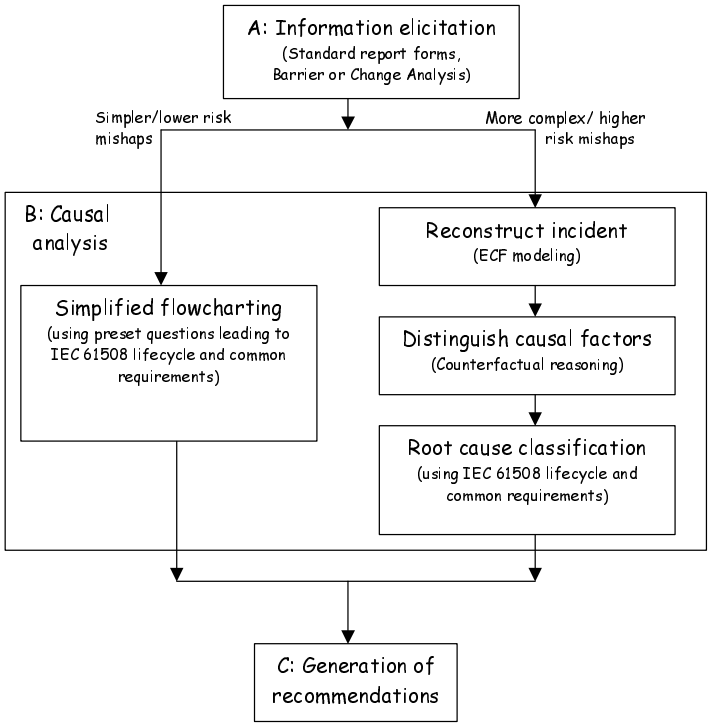


Figure 2: Overview of Investigation Schemes for E/E/PES-Related Incidents

A prime objective of our work is to ensure that the products of causal analysis can be mapped to the lifecycle phases and common requirements of the IEC 61508 standard. IEC 61508 provides guidance on the activities that should be conducted during the concept development, overall scoping, hazard and risk assessment, overall safety requirements analysis, integration, commissioning and verification, realisation., validation, operation and maintenance, and modification of safety critical E/E/PES. In addition there are a range of requirements that are common to all lifecycle phases. These include the need to ensure the competency of those involved in the operation, maintenance and modification of the system. They also include requirements relating to the 'safety culture' of the organisations involved in the development and operation of E/E/PES. Our use of this standard is justified because it provides a means of feeding the insights derived from any incident investigation back into the future maintenance and development of E/E/PES within safety-critical applications.

Part C presents requirements for the recommendations that are intended to address problems identified using the IEC 61508 classification. It is important that investigators assign relative priorities to individual interventions. Timescales should be recommended and documentation should indicate any actions that have been taken to address their recommendations.

The final part of this report presents our conclusions. It also identifies areas for future research. In particular, we are concerned to gather feedback from the application of both techniques. We are currently engaged in an extensive validation exercise that is intended to elicit end-user feedback on the suitability of the proposed approaches across a wide range of different industries.

A: Elicitation and Information Gathering

Before any causal analysis can begin it is important that investigators collect a range of information about the context in which an adverse event or near miss occurred. Unfortunately, many existing incident reporting forms are inadequate for E/E/PES related incidents. They provide an initial indication that hardware or software components are involved but often neglect to prompt staff for necessary information about the context in which the mishap occurred. Figure 3 provides an example of the forms that can be explicitly drafted to elicit information about an E/E/PES related incident. These forms embody a taxonomy for the classification and retrieval of adverse events. Each field helps to determine the information that will be elicited about an adverse event. Such taxonomies have a number of strengths and weaknesses. A significant benefit is that forms provide a minimum set of requirements for the information that should be obtained about an E/E/PES related incident. This is important given the lack of previous guidance on the investigation and analysis of these mishaps. Forms help to encourage consistency by providing different investigators with a common set of information requirements. However, they can prove restrictive if analysts cannot find an appropriate category against which to classify the incident under investigation. Forms can also become unwieldy and cumbersome if investigators have to complete too many irrelevant fields. Therefore, the following information requirements should be developed to suit the particular needs of different industry sectors with the caveat that safety managers must monitor the usability of the resulting classification. A range of additional forms is included in Emmet et al (2002). Rather then reproduce these examples in this document; the following section reviews the types of information that should be collected during an initial investigation into an E/E/PES related incident.

The Design of E/E/PES Reporting Forms

The person filing an initial report of an adverse event may not know that the mishap was related to an E/E/PES. In this situation, it is important to prompt safety managers or other designated authority to consider whether such a system was involved. If an E/E/PES is implicated then either the individual who observed the failure or a safety manager must provide initial information about the incident. The nature of this information will largely be determined by their knowledge of the systems involved. For instance, someone involved in the development or integration of an E/E/PES will be able to provide additional detail and insight beyond that which might normally be expected of a system operator. Conversely, someone involved in the operation of the application can provide information about the previous operating history an application process that might not be available to system developers. Different forms must be developed to elicit the different information available to these different groups of people. In either case, it is possible to identify minimum information requirements that should be satisfied in the immediate aftermath of an E/E/PES related incident.

Identification information

It is important to identify the operating unit or organizational division that is filing the report. In many contexts, this will be obvious. For more diverse cross-sector organizations, such information can help co-workers to determine whether an adverse event is relevant to their particular operation. In confidential schemes, it is possible to request the identity of the person filing the report. In anonymous schemes this will not be possible. The lack of any contact information, therefore, makes it imperative that reporting forms are validated to ensure that they capture sufficient information to inform the subsequent analysis of E/E/PES related incidents.

Initial E/E/PES Incident Report Form

Department:	Exploration & Development
Reported by:	C. Wilson (Acting Operations Manager)
Date of report	23rd January 2003

Location and Timing

Date when the incident(s) occurred	22nd January 2003
Time when incident occurred	11.00-13.10 hrs (GMT)
Location of Incident	Rgius C (Offshore Production Vessel)

Identification of Equipment:

Manufacturer	Gryves Sensing Systems
Makers name for device(s)	Type II Fire and Gas Monitoring System
Serial no.	Contract no. 324768-A
Configuration/version information	Unknown
Location	Sensors distributed throughout vessel. Main control system hardware located in forward electrical room.
Associated integrity level (if known)	Unknown

Outcome and consequences

Was any person hurt?	No
Did any damage to property occur?	Minor damage to manual ballast control system occurred when forcing valves to close. Automated control was lost following fire and gas alarm.
Was there a loss of production? If so how much?	Significant production loss. Difficult to estimate total, vessel is still not back in production.
In your view could this have led to more serious consequences?	Yes, loss of vessel stability could have occurred if control had not been regained over the ballast operation. Loss of electrical and hydraulic power compromised main vessel power and navigation systems.

Remedial Actions

What short term fixes or work arounds have been applied?	Manually forced ballast valves to halt transfer operation and correct list. Restarted the fire and gas control system. Request for advice and recommendations sent to monitoring and warning system suppliers.
To your knowledge, has this problem occurred before?	No.

Incident Description

Describe the incident in your own words Continue on separate sheet if necessary.	A spillage of methanol was detected on board. 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 shutdown. This included a plant 'black-out' with the loss of all electrical power...

Figure 3: Initial Incident Report Form (Emmet et al, 2003).

Location and Timing
It is important to identify when an incident occurred. This may be some time before the consequences of the mishap were observed. These consequences might also result from several repeated failures during the operation of an E/E/PES. Incident reporting forms should also elicit location information that can help to focus further investigations even in situations where contributors are reluctant to reveal their identity.

Identification of Equipment
In an initial reporting form, it is likely that operators will only possess minimal information about the role of E/E/PES within an incident. As the investigation progresses, however, it will be important to provide information about the type of hardware and the version of any software that was involved. This information is, typically, essential for device suppliers and developers to identify and correct any potential failures. Even if it is difficult to obtain device specific information in the aftermath of a mishap, investigators can collect information to characterize the function of the E/E/PES equipment within the wider system. For example, it might provide a protection function; act as an interlock or provide signaling. E/E/PES can also support control, monitoring, alarms, database, calibration, and measurement or communications functions. The E/E/PES channel in our case study helped to support monitoring functions associated with the mitigation against fire and gas events. We might, therefore, extend the form shown in Figure 3 to explicitly ask safety managers in this production environment whether any E/E/PES failure related to this critical aspect of system functionality. Similarly, E/E/PES incident report forms can be developed to elicit information about the system's mode of operation. For instance, if a particular function involves interaction between the E/E/PES and a human operator then additional human performance data must be gathered about the incident. The nature and scope of such enquiries must be revised if the function involved direct human control or if the E/E/PES were restricted to a more advisory role.

Incident Description
Incident reporting forms are often rejected or criticized by operators because they request information that is either unavailable at the time when the form must be completed or that is irrelevant to the incident being reported. In consequence, the form illustrated in Figure 3 relies upon a free text description of the adverse event. Safety managers may have to perform additional stages of information elicitation for 'more serious' incidents if operators omit important information in their free-text descriptions. Further problems arise if managers must use these descriptions to identify trends and patterns of failure over time. In many cases, this requires the use of databases and spreadsheets to record historic information about previous failures. Safety managers must extract key values from the natural language descriptions of each incident so that necessary information can be recorded in the computer-based systems. The alternative is to encourage operators to enter the information directly into the reporting software. This approach is difficult to sustain and can yield dubious results if individual workers have problems in interpreting the information requested by the strongly typed fields of computer-based reporting systems (Johnson, 2003).

Outcome and Consequences
Figure 3 also includes questions to elicit information about the outcome of an E/E/PES related mishap. The structure of an application has a significant impact on the potential consequences that are associated with E/E/PES related incidents. The outcome of a mishap involving an interconnected component may not simply be determined by that component alone but also by the services that it provides to other system components. Adverse events often expose dependencies or constraints between sub-systems that were not considered during the initial development of a safety-critical application. The initial investigation of an E/E/PES incident should also identify the particular failure mode that affected the system. Equipment may have failed to operate when required. Conversely, it may have operated when not required or have operated in an unexpected way. In interactive applications, the operator may not have intervened to control the equipment in the manner anticipated by the designer or by line management. In particular, they may have overlooked or misinterpreted the information that was presented to them by the equipment.

As mentioned, the form in Figure 3 only captures initial information in the aftermath of an E/E/PES related incident. Additional reporting forms must be provided to elicit more detailed data (Emett et al, 2002). Safety managers can use this additional information to determine the required integrity level associated with system functionality. This corresponds to the safety integrity level (SIL 1, 2, 3, 4 or unspecified) if IEC61508 was used to inform system development. The determination of a SIL may be less

straightforward for legacy systems where the necessary analysis need not have been performed before the adverse event. The post hoc determination of an integrity level is complicated because the SIL associated with E/E/PES functionality need not reflect the actual consequence of any particular incident. Near miss incidents may encourage investigators to underestimate the level of integrity that should be associated with particular safety functions. The initial stages of an investigation should, therefore, derive some potential consequence assessment. At this stage, it is worth examining the original hazard and risk assessment to ensure that the event being analyzed had been identified. If the event was missing from the original analysis or the consequence had been wrongly predicted then the required safety integrity level will have to be reconsidered. At the highest level, this might involve distinguishing between fail-safe or fail-danger consequences. In other situations, it might be possible to introduce more fine-grained classifications in terms of lost production, environmental damage or consequent injury. The consequence and outcome section of the form illustrated in Figure 3 must be revised to capture this information.

Remedial Actions

It might seem perverse to initiate corrective action during the initial stages of any incident investigation. It can be argued that any intervention should be postponed until after a more formal causal analysis has taken place. There are circumstances, however, in which the continued safety of an application requires more prompt intervention. An initial investigation can, therefore, initiate or recommend a range of corrective actions including changes either to the E/E/PES or to any equipment under control. These actions may include equipment relocation; environmental protection; hardware repair; version upgrade; equipment replacement and reprogramming. Alternatively, investigators might recommend operational changes to procedures; documentation; access control; warnings; staff training; staff briefing, supervisory practices. or maintenance. The key point is that any interim measures should be adequately documented on an incident report form so that any subsequent investigation and analysis can determine whether there is a need to initiate any further follow-up actions. The initial investigation should also consider if other functions utilize the same type of equipment, procedures or resources and whether there is an immediate need to take actions. These might include the immediate inspection of al similar systems.

Secondary Elicitation Techniques: Barrier and Change Analysis

The previous paragraphs have reviewed the information that must be elicited from incident reporting forms in the aftermath of E/E/PES related incidents. The intention is to provide a template that can be tailored to the specific needs of different organizations within a range of different industries. It should also be stressed that many operators and safety managers will require training in how to complete these forms. Additional cues can be provided. For example, by distributing sample, completed forms to show the detail that should be provided. Incident reporting forms are unlikely to yield all of the information that is required about the course of an adverse event. Information must be gathered from automated system logs. Table 1 recreates part of the alarm log from the monitoring systems in our case study application. It is apparent from this high-level summary 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 decisions that will only be indirectly represented in these logs. These different information sources must, therefore, be collated to form a more coherent overview of an incident or near miss.

Point	Time	State of the Alarm	Description	State - 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
…	…	…	…	…	…	…	…

Table 1: Example Summary from Automated Alarm Log

A number of additional techniques extend the scope of an initial investigation to ensure that relevant information is captured in the aftermath of an E/E/PES related incident. Barrier and Change analysis provide high-level frameworks for thinking about the factors that should be considered when gathering necessary information. Barrier analysis stems from work in energy production (US Department of Energy, 1992). The central idea is that incidents are caused when unwanted energy flows between a source and a target. Barrier analysis begins by drawing up tables that identify the hazard and the targets involved in an incident or accident. Table 2 illustrates these entities for the case study in this paper. The purpose of this exercise is to determine precisely which barriers would have to fail before potential targets might actually be affected. The initial tables of barrier analysis often try to consider as many plausible targets as possible.

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

Table 2: Hazard and Target Identification

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 channel.
	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 3: More Detailed Barrier Analysis

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 3 illustrates the output from this stage. As can be seen, the fire and gas system architecture illustrated in Figure 1 was intended to prevent the hazard identified in Table 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. The meta-level point here is that Barrier analysis encourages designers to look beyond the immediate triggering events that led to the mishap. This is important because it is these triggering events that are most likely to be documented in the initial reports that are filed following E/E/PES related incidents.

Change Analysis

Change analysis looks at the differences that occur between the actual events leading to an incident and 'normal' or 'ideal' operating practices. Table 4 provides an example of change analysis. The first column describes the ideal condition or the condition prior to the incident. This is an important distinction because the causes of adverse events often stem from inappropriate practices that continue 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. As with Barrier analysis, this technique encourages investigators to gather information about the longer-term, less direct, factors that contribute to a mishap.

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.

Table 4: Change Analysis

Summary

This section has identified the information that must be elicited in the aftermath of an E/E/PES related incident. This includes data on the time and location of an adverse event. It also includes information that can be used to identify the E/E/PES that contributed to the incident or near miss. Operators and safety managers must also assess the potential outcome of a mishap. It is necessary to document any interim measures that are taken to safeguard the continued operation of an application process. Reporting forms and system logs provide the primary means of gathering this information. However, Barrier and Change analysis also help to identify relevant information about the longer-term causes of incidents and near misses. Care must be taken to avoid the overheads associated with the capture of irrelevant or unnecessary information. Forms must be revised in the light of experience so that operators only provide information that is used within the investigative process. The intention is to provide sufficient detail to support the causal analysis that is described in the next section.

B Causal Analysis

The previous section has identified a range of information that must be captured in the aftermath of E/E/PES related incidents. For minor mishaps and many near-miss incidents, an investigation could end after this information has been gathered. However, the integrity level of the function performed by particular equipment or the potential consequences of the incident can persuade investigators to initiate a more formal investigation. Similarly, E/E/PES applications and technology range in complexity. Causal analysis can be relatively straightforward when simple technology is used to satisfy simple functional requirements. In these simpler, low consequence cases it may be possible to directly identify causal factors without recourse to a more formal methodology providing that adequate justification is provided. With complex systems or higher 'risk' mishaps, a more formal approach is required. This section, therefore, introduces two different approaches that can be applied to identify the 'root' causes of E/E/PES incidents from the information that has been gathered in the immediate aftermath of an adverse event. The first is based on a series of questions that guide investigators through a flowchart. This approach is relatively simple. It represents a low-cost form of causal analysis that can be applied with minimal training. This technique is insufficient for more complex incidents. The second approach, therefore, avoids any pre-formatted questions. Instead, it relies upon Events and Causal Factors charting (US Department of Energy, 1992). Figure 4 provides a high-level overview of these two complementary approaches within the wider investigation process.

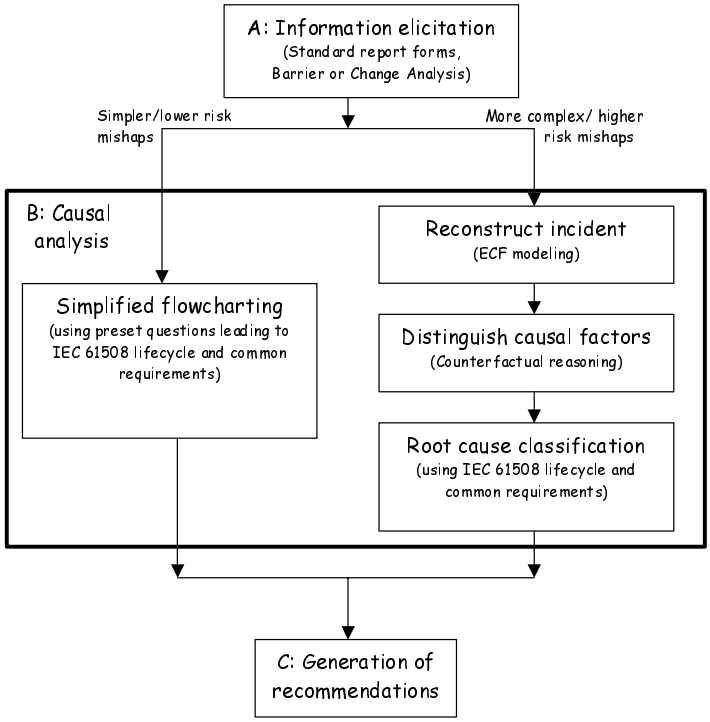


Figure 4: Overview of Investigation Schemes for E/E/PES-Related Incidents

E/E/PES mishaps stem from a diverse range of causal factors. These include operator 'error', maintenance issues, calibration problems, environmental issues, equipment functionality problems, equipment interfacing issues and hardware faults. In most other forms of accident or incident investigation, we would map each of these inadequacies back to the managerial and organizational influences that created the preconditions for each of these failures. For example, we might consider whether operator training had emphasized the importance of monitoring individual alarms and warnings from each of the two PLC channels. The following paragraphs show how the output from both proposed causal analysis techniques can be used to identify the precursors of E/E/PES related incidents in particular phases or to the violation of common requirements across several phases of the development lifecycle within IEC 61508. Our use of

this standard provides means of using the products of mishap analysis to inform the future development and operation of safety-critical systems.

Root Causes of E/E/PES Related Incidents Under IEC 61508

One way of ensuring that a causal analysis technique supported redesign would be to identify those requirements of a standard that are intended to prevent particular problems from affecting the design and operation of safety-critical system. In our case study, the decision to use the same card set to control all of the generators could be traced back to an inadequate risk assessment. Had this process been carried out in a more rigorous fashion then the common failure modes might have been identified. However, this approach suffers from a number of problems. Firstly, it implies that had the company followed the standard then the incident would have been avoided. It is difficult to find the detailed evidence required to support such counterfactual arguments (Johnson, 2003). There are also a number of more practical issues that must be addressed. It is unlikely that either the end user will have all of the information required to trace an incident back to causes that stem from early stages in the E/E/PES lifecycle They may also have a limited interest in supporting a more detailed causal analysis if they cannot directly affect changes in the systems that they use. Conversely, system developers may lack necessary information about how the system was deployed within a more complex application process. Unless they have access to this data then it can be difficult to pin down the particular causes of an adverse event. Some of these objections can be answered by gathering data from the different groups involved in the development of E/E/PES. This may be difficult since in many cases design teams may no longer exist by the time the equipment becomes operational.

Further problems complicate attempts to trace the causes of a mishap back to the violation of requirements in particular development standards. For instance, parts 1 to 3 of IEC 61508 contain a mass of detailed requirements. Any comprehensive taxonomy would be so complex that it would be unwieldy and difficult to apply. Our causal analysis techniques therefore only include headings from the main stages of development within this standard: system conception; overall scooping of the system; hazard and risk assessment; identification of overall safety requirements; function and integrity level allocation; planning of installation and commissioning; validation; operation and maintenance; realization; performance of installation and commissioning; conduct of validation; performance of operations and maintenance and subsequent modification. IEC 61508 also identifies a number of processes that are common to each of the development stages mentioned above. These include the need to specify the management and technical activities necessary to achieve functional safety. It is also important to structure the activities in the safety lifecycle in a systematic manner. The competency of key personnel must be ensured. Verification techniques must be used to establish that the outputs from each of the phases, mentioned above, meets the requirements for that phase. Managers must ensure that documentation is available to support all necessary activities. Finally, an adequate functional safety assessment must be performed. Table 5 provides a high-level classification of the potential problems that can affect phases of the IEC 61508 lifecycle or in satisfying common requirements. These issues are enumerated in the middle column. The right column provides a reference to areas of the standard that provide additional detail about each requirement. The rows in this table will be used in the remainder of this report to provide a taxonomy or checklist of causal factors. As our analysis progresses we will attempt to identify which of these potential failures contributed to the particular causes of our E/E/PES case study.

Previous sections have argued that important benefits can be gained through the development of two different schemes. One provides a relatively simple and low cost means of identifying the violations of IEC 61508 requirements that contributed to an E/E/PES related incident. It is designed for cases where the E/E/PES has been observed to fail, for example by system operators. The other provides a more flexible, powerful approach. It suffers from a corresponding increase in the investment in terms of staff time and expertise that is required before this technique can be used. The following pages briefly describe these two different approaches to the causal analysis of E/E/PES mishaps using a causal taxonomy derived from IEC 61508.

IEC 61508 Lifecycle phase	Detailed taxonomy	IEC 61508 ref
Concept	1. Hazard &Risk Assessment	7.2,7.3,7.4
Overall Scope		
Overall Safety Requirements	1. specification 2. selection of equipment 3. design and development 4. installation design 5. maintenance facilities 6. operations facilities	7.2 (2) 7.4.2.2 (2) 7.4 (2) 7.4.4/5 (2) 7.4.4.3 (2), 7.4.5.2/3 (2)
Allocation		
Planning of I & C, V, and O&M		
Realization		7.4.5.1/3
Installation and commissioning	1. installation 2. commissioning	7.5 (2), 7.13.2.1/2, 7.13.2.3/4
Validation	1. function testing 2. discrepancies analysis 3. validation techniques	7.7.2.1/2/3 (2) 7.7.2.5 (2) 7.7.2.7 (2)
Operation and maintenance	1. maintenance procedures not applied 2. maintenance procedures need improvement 3. operation procedures not applied 4. operations procedures need improvement 5. permit/hand over procedures 6. test interval not sufficient 7. maintenance procedures not impact assessed 8. operation procedures not assessed 9. LTA procedures to monitor system performance 10. LTA procedures applied to initiate modification in the event of systematic failures or vendor notification of faults 11. tools incorrectly selected or not applied correctly	7.7.2.1 7.6.2.2.1/2/3 (2) 7.6.2.1 7.6.2.2 7.6.2.1 7.6.2.1 7.6.2.4 (2) 7.6.2.4 (2) 7.6.2.1 (2) 7.8.2.2 (2), 7.16.2.2 7.6.2.1 (2)
Modification	1. impact analysis incorrect 2. LTA manufacturers information 3. full lifecycle not implemented 4. LTA verification and validation	7.8.2.1 (2) 7.8.2.2 (2) 7.8.2.3 (2) 7.8.2.4 (2)
IEC 61508 common requirements		
Competency	1. LTA operations competency 2. LTA maintenance competency 3. LTA modification competency	6.2.1 h 6.2.1 h 6.2.1 h
Lifecycle	1. LTA definition of operations accountabilities 2. LTA definition of maintenance accountabilities 3. LTA definition of modification accountabilities	7.1.4 7.1.4 7.1.4
Verification	1. LTA verification of operations 2. LTA verification of maintenance 3. LTA verification of modification	7.18.2, 7.9 (2) 7.18.2, 7.9 (2) 7.18.2, 7.9 (2)
Safety management	1. LTA safety culture 2. LTA safety audits 3. LTA management of suppliers	6.2.1 6.2.1 6.2.5
Documentation	1. documentation unclear or ambiguous 2. documentation incomplete 3. documentation not up to date	5.2.6 5.2.3 5.2.11
Functional safety assessment	1. LTA O & M assessment 2. modification not assessed 3. assessment incomplete 4. insufficient skills or independence in assessment team	8.2 8.2 8.2.3 8.2.11/12/13/14

Key: LTA is Less Than Adequate, IEC 61508 references are to Part 1 except as indicated by parentheses e.g. (2)

Table 5: Taxonomy for Analysing E/E/PES Related Failures Under IEC 61508 (Emmet et al 2003).

Flow Charting Scheme

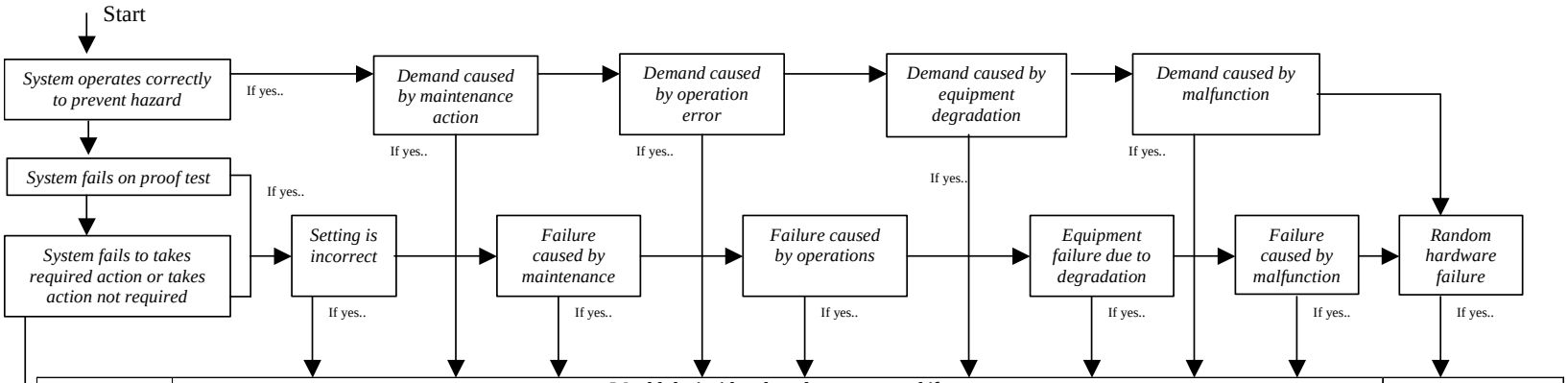
This simpler of our two techniques relies on a form of flow-chart (Emmet et al, 2003). This approach is intended to be low cost in terms of the training required. Figures 5 and 6 provide an overview of this approach. Analysis begins by asking a series of high level questions about the nature of the E/E/PES related incident. For instance, investigators must determine whether or not the system correctly intervened to prevent a hazard, as might be the case in a near miss incident. If the answer is yes, then the analysis progresses by moving horizontally along the arrows to identify the nature of the failure. If the system intervened to address problems created by maintenance activities then the investigator would follow the arrow in Figure 5 down to the associated table entry. By reading each cell in the column of the table indicated by the arrow, investigators can identify potential causes in the simplified stages of the IEC 61508 lifecycle. Latent failures that might have been the source of an E/E/PES related incident can also be considered by examining the items listed under all six of the common requirements in the third row from the bottom.

Investigators must continue along the top horizontal line repeating the classification against the cells in the table in the same manner described for maintenance related incidents. Analysis progresses by following the top-level questions down the flow chart. For some incidents, there will be failures identified by analysing several of these different questions. For instance, a system may operate correctly to prevent a hazard although in the process there may also be further subsystem failures or operator interventions that initially fail to rectify the situation. In this case, analysts would focus on the top line in Figure 5 and the further line of analysis continued on Figure 6.

It is important to stress that most incidents involve multiple causes. For example, our case study stemmed from the use of asynchronous 2 out of 2 voting and the decision to group generator controls on a single card set. Hence the analysis might identify several common requirements or stages in the lifecycle that might have been altered to prevent this incident from occurring in the manner described by previous paragraphs. For this reason, it is important that analysts make several passes through the flow charts in Figures 5 and 6. Each successive inspection of these diagrams may yield new causal factors that will form the focus for further discussion. Analysis finishes when investigators are satisfied that they have addressed all aspects of the incident and have documented their analysis. Their line managers should normally approve this decision.

As mentioned in previous sections, the elicitation of evidence is closely connected to any causal analysis. In consequence, the elements of Figures 5 and 6 can serve to direct investigators as they gather information about the course of an adverse event or near miss incident. It is also important to stress that these diagrams represent an initial attempt to develop a low-cost causal classification scheme that specifically supports E/E/PES related mishaps. Further work is required to determine if the key questions listed in the previous paragraph are sufficient to cover a wide range of incidents in several different industries. Similarly, more work needs to be conducted to determine whether investigators can match the incidents that they are faced with against the particular terms and phrases that are used in the flow-charts.

It is important to document the outcome of this flowchart analysis. This is done using the form illustrated in Table 6. Immediate events that are identified in incident reporting forms are related back to failures in the lifecycle stages and common requirements of IEC 61508. This allocation process is guided by the questions in Figures 5 and 6. The allocation is also supported by a justification that is intended to document any intermediate reasoning to other investigators and co-workers.

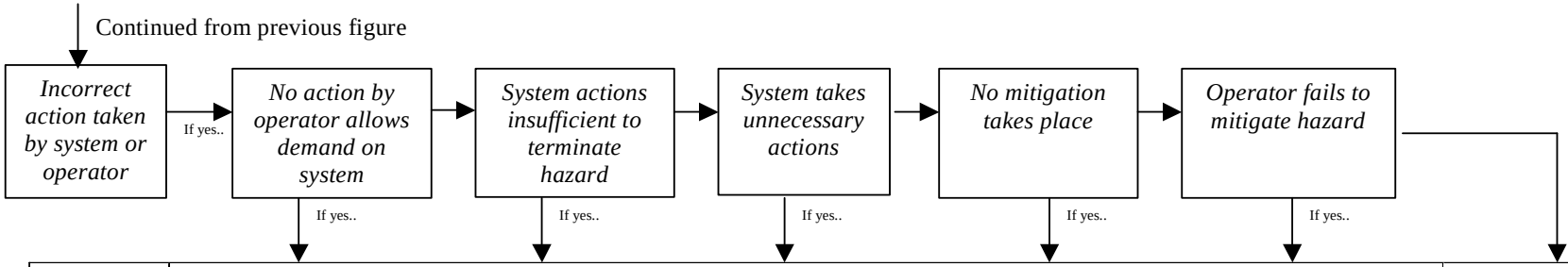


	Would the incident have been prevented if:					
Design	- different equipment selected? - installation design different? - configuration was correct	- maintenance facilities had been designed adequately	- operations facilities had been designed correctly	- different equipment selected? - installation design had been different?	- different equipment selected? - the installation design had been different? -configuration was correct	Log failure and check -if dangerous failure rate is in line with design assumptions -if all expected actions occurred and no unexpected actions occurred -if safe failure causes any unexpected actions Log demand and check if -demand rate is in line with design assumptions -demand cause was predicted in H & RA
Installation & Commission	- the equipment had been installed according to design	- the maintenance facilities had been installed according to design	- the operations facilities had been installed according to design	- the equipment had been installed according to design	- the equipment had been installed according to design	
Validation	- the setting had been checked during validation	- maintenance facilities had been fully checked	- operations facilities had been fully checked	- equipment condition had been fully checked	- equipment condition had been fully checked	
Operation & Maintenance	- maintenance procedures were applied - maintenance procedures were improved - maintenance tools better - test interval was reduced	- correct maintenance procedure had been used - maintenance procedure was improved - permit procedures better	- correct operation procedure was used - operation procedure was improved - permit procedures improved	- maintenance procedures applied - maintenance proc. better - test interval was reduced - additional protection provided	- maintenance procedures were improved - maintenance tools improved - test interval was reduced - additional protection provided	
Modification	- setting had been reviewed during impact analysis	- maintenance facilities or procedures had been reviewed during impact analysis	- operation facilities or procedures had been reviewed during impact analysis	- equipment used or installation design has been reviewed during impact analysis	- equipment used or installation design has been reviewed during impact analysis	

	Would the incident have been prevented if:					
	Competency	Lifecycle	Verification	Safety management	Documentation	Safety assessment
Operation & Maintenance	- operation or maintenance staff were more competent	- responsibilities were defined better	- a better verification scheme had been in place	- safety culture was improved - audits were more frequent	- documentation was clear and sufficient	- assessment had been carried out on O&M phase
Modification	- modification carried out by more competent staff	- modification lifecycle was better defined	- a better verification scheme had been in place	- accountabilities better defined - suppliers not reviewed	- documentation updated	- assessment carried out on modification

Continued …

Figure 5: High-Level Flow Chart to Support Causal Analysis of E/E/PES Related Incidents Using IEC 61508 Taxonomy [Cont. in next figure] (Emmet et al, 2003)



	Would the incident have been prevented if:					
Design	- operator facilities had been designed better - the installation design had been different?	- additional actions had been specified - actions had been faster - final actuation device were improved	- design requirements were better documented	- mitigation system had been specified - mitigation system had been better designed	- operator facilities had been designed better - the installation design had been different?	Log failure and check - if dangerous failure rate is in line with design assumptions - if all expected actions occurred and no unexpected actions occurred - if safe failure causes any unexpected actions Log demand and check if - demand rate is in line with design assumptions - demand cause was predicted in H & RA
Installation & Commissioning	- the equipment had been installed according to design	- the equipment had been installed according to design	- the equipment had been installed according to design	- mitigation system had been installed according to design	- the equipment had been installed according to design	
Validation	- operator facilities had been checked during validation	- operation facilities had been checked during validation	- operations facilities had been fully checked	- mitigation system had been fully checked	- operator facilities had been fully checked	
Operation & Maintenance	- operation procedures were applied - operation procedures were improved	- correct maintenance procedure had been used - maintenance procedure was improved - proof testing was more frequent	- correct operation procedure was used - operation procedure was improved - permit procedures were improved	- mitigation procedures were applied - mitigation procedures were improved - mitigation system was proof checked more frequently	- operation procedures had been applied - operation facilities or procedures were improved	
Modification	- operation facilities had been reviewed during impact analysis	- necessary system actions had been reviewed during impact analysis	- necessary system actions had been reviewed during impact analysis	- need for mitigation had been reviewed during impact analysis	- need for mitigation had been reviewed during impact analysis	
	Would the incident have been prevented if:					
	Competency	Lifecycle	Verification	Safety management	Documentation	Safety assessment
Operation & Maintenance	- operation or maintenance staff were more competent	- responsibilities were defined better	- a better verification scheme had been in place	- safety culture was improved - audits were more frequent	- documentation was clear and sufficient	- assessment had been carried out on O&M phase
Modification	- modification had been carried out by more competent staff	- modification lifecycle was better defined	- a better verification scheme had been in place	- accountabilities were better defined - suppliers not reviewed	- documentation had been updated	- assessment ad been carried out on modification

Figure 6: High-Level Flow Chart to Support Causal Analysis of E/E/PES Related Incidents Using IEC 61508 Taxonomy (Emmet et al, 2003).

Causal Event	IEC 61508 Lifecycle/ Common Requirement	Justification (Route through flow chart)
Loss of electrical power and associated plant	Design	System fails to take required action-> Equipment failure caused by malfunction-> The incident would have been prevented if different equipment had been selected.
Failure to control ballast operation using E/E/PES and delays in manual operation.	Operation and maintenance	System fails to take required action->The incident would have been prevented if a better verification scheme had been in place.

Table 6: Abridged IEC 61508 Flowchart Causal Summary for Case Study

Table 6 provides a summary of the causal analysis that can be obtained from our case study using the flowcharts in Figures 5 and 6. As can be seen, this analysis focuses on the operators' perspective on this incident. It does not look back into the design detail and development lifecycle of the E/E/PES. In order to do this, the flowcharts would have to be considerably extended. Additional questions would be needed to guide the investigator towards the lifecycle phases, such as hazard and risk assessment, and common requirements that contribute towards the development and installation of an E/E/PES. Emmet et al (2002) provide examples of how this flowchart approach can be extended. It is important to note, however, that the resulting flow charts will be considerably more complex than those shown in the previous diagrams. This increased complexity arguably sacrifices many of the benefits associated with this simple approach. The resulting diagrams extend over several pages and the questions can be difficult to follow at lower levels within the chart. The following section, therefore, presents a more sophisticated analytical technique that is intended to be used to extend the analysis that can be obtained from the use of the flowcharts.

Event & Causal Factor Analysis

The previous section has presented a low-cost and relatively straightforward approach based on flowcharts. This is particularly appropriate for use by the members of end-user organisations. These individuals, typically, have limited access to information about the conduct of early stages in the E/E/PES lifecycle. In contrast, this section presents a more complex technique that provides a further bridge between causal analysis and components of IEC 61508.

First Stage: Information Elicitation and ECF Modelling

Previous sections have argued that different information will be available to end-users, suppliers and integrators of E/E/PES equipment. For instance, the following excerpt describes the end-users perspective on our case study incident that was captured by the report form in Figure 2:

> "…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 shutdown. This included a plant 'black-out' with the loss of all electrical power..."

This report can be used to produce an initial sketch of the events leading to a mishap or near miss. Investigators can do this by identifying the key events that contributed the E/E/PES related incident. For example, this account might yield critical events including the initial methanol spill as well as the decision to move the ballast. Other significant events include the automatic initiation of the firewater pump, the detection of methanol and the plant shutdown. Figure 7 shows how a simplified form of Events and Causal Factors (ECF) diagram can be used to reconstruct the operators' perspective on our case study. As can be seen, the intention is to provide an initial overview of the immediate events that were observed by the end-users of the E/E/PES. Exact timings are omitted, as these are unlikely to be available in the immediate aftermath of an adverse event. The rectangles represent events. Ovals represent the conditions that make those events more likely. The diamond shape represents the outcome of the E/E/PES related mishap. It is important to note, however, that no assumptions are made about the direct involvement of the E/E/PES at this stage. In particular, Figure 7 traces a line of events leading to the automatic initiation of the firewater pump but at this stage in the analysis it is not possible to determine whether or not this played any role in the eventual loss of control.

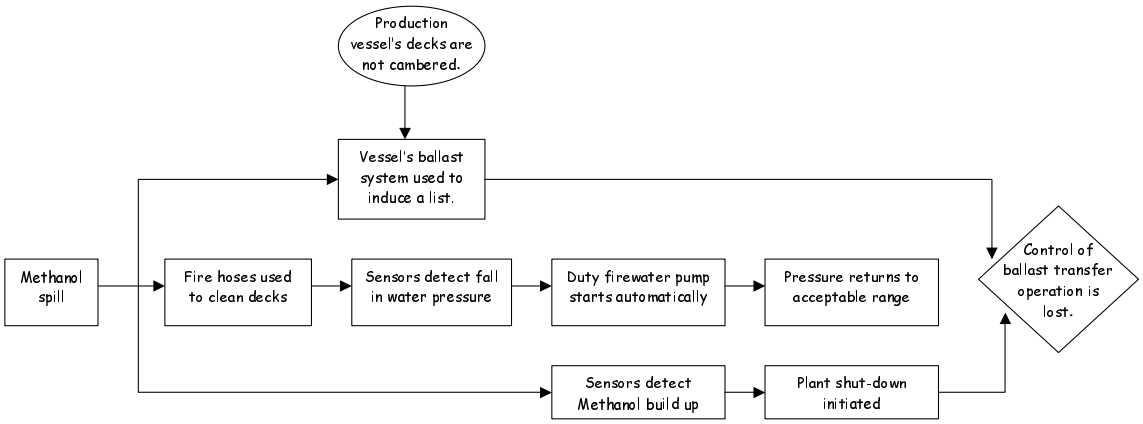


Figure 7: ECF Chart Showing End-User Perspective on Case Study Incident

It is likely that both system integrators and developers will be contacted in the aftermath of more serious incidents or near misses. The following excerpt, therefore, reflects the information that might be available

to individuals with more detailed insights into the architecture of our case study E/E/PES. It is unlikely that such a precise analysis would be available until some time after the event. It does, however, capture the level of detail that can be obtained from the collaboration of device manufacturers and system integrators in the aftermath of an E/E/PES related incident:

> "…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…"

This more technical account includes events such as the detection of the fall in water pressure, the operator alarm, the reception of the transient signal and so on. The next stage of the analysis is to reconstruct these various events to form a timeline of the mishap. Figure 8 presents the extended ECF chart. This diagram not only represents the additional events that can be identified by a 'white box' approach to incident reconstruction. It also illustrates the way in which developers can reconstruct relationships between events that are unlikely to have been identified by end-users. In particular, the simple ECF diagram of Figure 7 could not link the initial command to start the firewater pump to the loss of control in the ballast transfer operation. The additional insights provided in Figure 8 show that the transient signal generated by the water pressure alarm following the start of the firewater pump was a central event in the course of this mishap.

Second Stage: Causal (Counterfactual) Reasoning

The development of a detailed ECF chart continues until all of the parties involved in an investigation agree that it provides a reasonable representation of the events that contributed to an adverse occurrence or near miss. This decision is influenced by the scope of the investigation and by pragmatics. For instance, we could extend Figure 8 to consider the circumstances that led to 'risk assessment fails to identify possible failure modes'. This could only be done if incident investigators gain access to the appropriate development documentation.

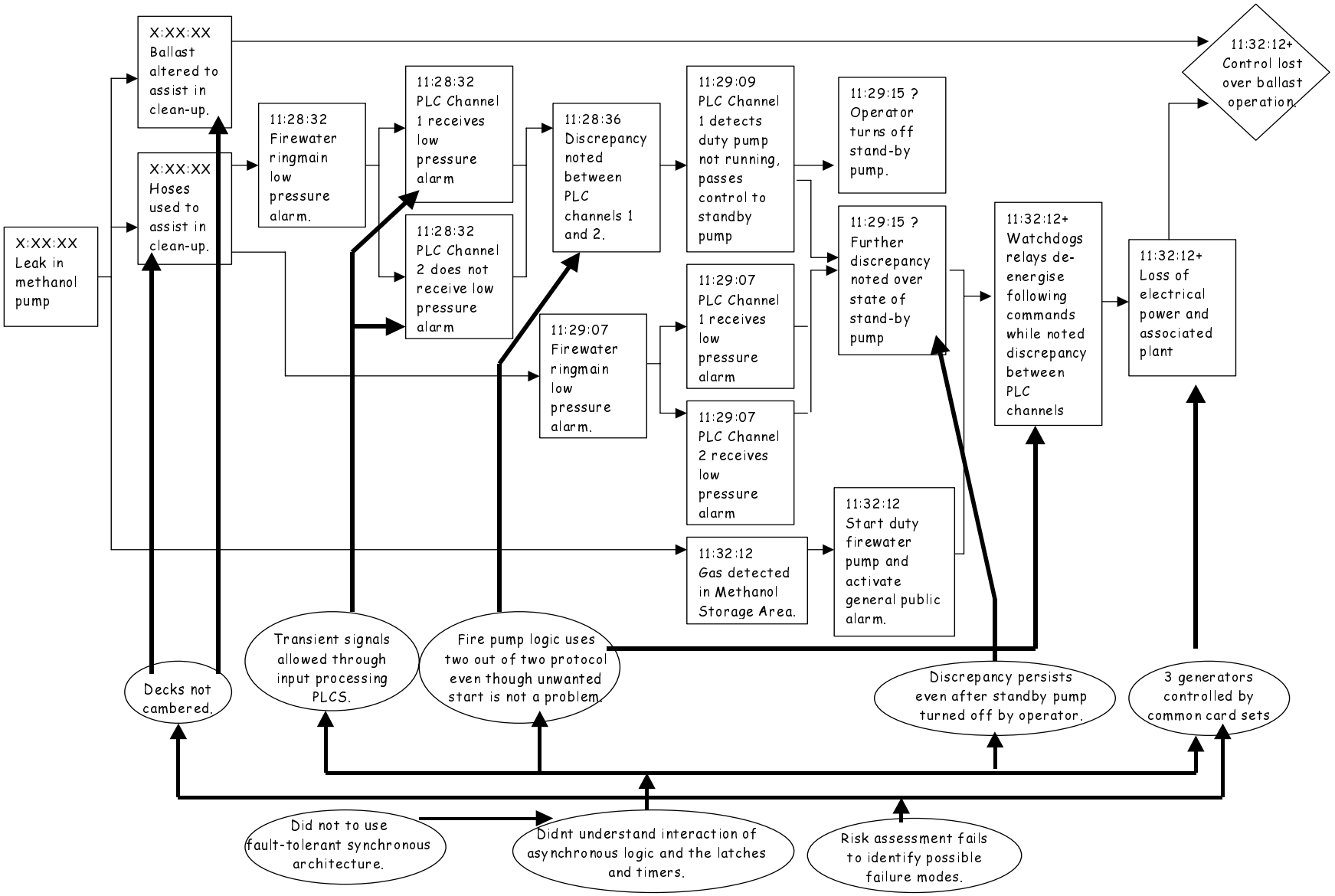


Figure 8: An ECF Diagram Including Developer/System Integrator Information

The ECF in Figure 8 reconstructs the events and conditions that contributed to our case study. A further stage of analysis is required in order to distinguish potential causal factors from more contextual information. Analysis proceeds using what is known as counterfactual reasoning. The term 'counterfactual reasoning' denotes a common form of argument that is used informally in many different incident investigations. Starting at the outcome event, investigators must ask whether the incident would have occurred if that event had not taken place. If the incident would still have happened then the event cannot be considered as a casual factor. For example, the incident would clearly not have happened if electrical power and associated plant had not been lost. This is, therefore, a cause of the incident. In contrast, we can argue that the incident would still have happened even if the operator had not intervened to switch-off the stand-by pump. Hence this action cannot be considered a cause of the mishap. Table 8 provides an overview of the output from this form of analysis.

Event	**Cause/ Contextual Factor**	**Justification**
Loss of electrical power and associated plant	Cause	If this had not occurred then control would have been retained over the ballast operation.
Watchdog relays de-energize following commands while noted discrepancy between PLC channels	Cause	If this had not occurred then electrical and hydraulic power would have been retained.
Further discrepancy noted over state of stand-by pump	Cause	If the operator had cleared the discrepancy between the two channels then the watchdog relays would not have de-energized following the firewater pump command.
Operator turns off stand-by pump.	Contextual factor	The discrepancy in the state of the stand-by pump persists between the two channels even after the pump is switched off.
Gas detected in Methanol Storage Area	Contextual factor	Even if gas had not been detected in the Methanol Storage Area a number of other events may have resulted in the mishap. For example, gas might have been detected elsewhere in the vessel or another control path involving 2 out of 2 voting might have caused the trip.

Table 7: Cause/Context Summary Chart for Case Study Incident

Each event in the ECF diagram is listed as either a potential cause or a contextual factor in the final form of the table. A justification is provided to support this assessment because contextual factors will not be considered during subsequent analysis. Counterfactual reasoning is non-trivial. For example, Table 7 identified the detection of gas in the methanol storage area as a contextual factor on the basis that the incident would still have occurred even if this event had not taken place. The justification is that another triggering event is likely to have occurred. For instance, other sensors following the initial leak might have detected gas. Alternatively, the watchdog relays might have been de-energized by any other event that required 2 out of 2 voting on the PLC channels. The validity of this argument depends not only on a knowledge of the E/E/PES system but also on supposition about alternative ways in which a similar incident might have developed. The difficulty of forming such counterfactual arguments is another reason why it is important to document this stage of the analysis using the techniques illustrated in Table 7.

Third Stage: Root Cause Analysis under IEC 61508

The next stage in our analysis is to link each causal factor back to potential problems in the development stages and common requirements of IEC 61508, illustrated in Table 5. The first task is to identify those conditions that contributed to each causal event using the ECF chart illustrated in Figure 8. These conditions typically capture latent issues, including development and operation decisions that create the context for particular events in E/E/PES mishaps. For instance, the loss of electrical power and associated plant was made more likely by the decision to control all generators by a common card set. This failure mode was arguably caused by inadequate risk assessment prior to implementation. The key point is not to

arrive at an unambiguous association of lifecycle phases with the conditions that contribute to causal events. For instance, it is perfectly possible to argue that the grouping of generator controls stemmed from an inappropriate function allocation during design and development rather than inadequate hazard and risk assessment during equipment selection. The intention is to provide a focus for the analysis so that consensus can be achieved before recommendations are made.

Table 8 associates conditions with phases in the IEC 61508 lifecycle. It does not refer to any of the IEC 61508 common requirements listed in Table 5. These are considered during a further stage of analysis. Investigators must, typically, conduct additional enquiries into the processes and procedures that characterise previous stages of the E/E/PES lifecycle. For example, we might argue that inadequate risk assessment described in Table 8 was symptomatic of a less than adequate safety culture. Such a finding would be difficult to sustain without a more detailed assessment of the risk management practices that were conducted by the end-user, system integrators and developers.

Causal Event	**Associated Conditions**	**IEC 61508 Lifecycle Classification**	**Justification**
Loss of electrical power and associated plant	3 generators controlled by common card set.	Allocation 3: Design and Development	The allocation safety-critical monitoring requirements to the same card set that controlled the generators created a common point of failure.
	Risk assessment fails to identify possible failure modes.	Hazard and risk assessment 1: specification	Initial hazard and risk assessment failed to identify the vulnerability created by the common point of failure.
Watchdog relays de-energize following commands while noted discrepancy between PLC channels	Fire pump logic uses two out of two protocol even though unwanted start is not safety-critical.	Allocation 3: Design and Development	The allocation of commands to start the duty firewater pump to the redundant 'two out of two' voting system was unnecessary because unwarranted start did not have adverse safety implications.
	Did not understand interaction of asynchronous logic, latches and the timers.	Hazard and risk assessment 1: design and development	The designers/ integrators did not consider that a low-consequence demand on the voting system might lead to inconsistent states on the two channels.
	Did not use fault-tolerant synchronous architecture.	Realisation 3: Design and Development	The decision not to use a synchronous system enabled the inconsistency to remain within the architecture.
Further discrepancy noted over state of stand-by pump	Discrepancy persists even after standby pump turned off by the operator.	Validation 2: discrepancies analysis	A more rigorous testing regime is likely to have uncovered that a discrepancy might remain 'latched' between the two channels.
	Did not understand interaction of asynchronous logic, latches and the timers.	Hazard and risk assessment 1: design and development	The designers did not consider that potential inconsistencies between the two channels would lead the watchdog timers to trip even though differences did not imply a major failure in either of the PLC channels.
	Did not use fault-tolerant synchronous architecture.	Allocation 3: Design and Development	An early decision was made by component suppliers not to incur the additional costs and complexity of a synchronous architecture.

Table 8: Abridged IEC 61508 Causal Summary Chart for Case Study Incident

Table 9 presents the full and final form of Table 8. As before, a justification helps others to understand why investigators found violations of common requirements in particular phases of the IEC 61508 lifecycle. This is important because the table should act a focus for discussion. This is necessary if agreement is to be reached about the outcome of an investigation. A further role for this analysis is to encourage investigators to look for further examples of conditions that illustrate violations of common requirements across different phases. For example, a suspicion that documentation was inadequate during the initial stages of design would encourage investigators to determine whether this problem affected other implementation and operation. Table 9 also included causes that stem from particular stages in the IEC 61508 lifecycle but that are unrelated to any failures in the common requirements. Previous paragraphs argued that inadequate hazard and risk assessment led to the common point of failure in the generator controls. Table 9 does not link this shortcoming to any more general failure to satisfy common requirements in the standard. However, the table could be revised to include such a finding if this were warranted by subsequent analysis.

To summarise, this more complex approach first gathers evidence about the course of an E/E/PES related incident. This information is then used to create an ECF 'timeline'. If the analysis is being conducted by an end-user organisation then it will often be necessary to include additional technical information from organisations and individuals involved in system development and integration. Once this has been done, it is possible to identify those conditions that make particular events more likely. The next stage is to apply formal causal reasoning to distinguish contextual information from causal factors. This is done by constructing counterfactual arguments of the form 'if event X had not occurred then the mishap would also not have occurred'. If this argument can be made then the event is a potential cause. If not then the accident would have occurred even if the event had not taken place and so it is classified as a contextual factor. A table is then constructed to list all of the conditions that contribute to each causal event. A two-stage analysis can then be used to associate these conditions either with specific inadequacies during phases of the IEC 61508 lifecycle or with the violation of common requirements across several different phases.

Causal Event	Associated Conditions	IEC 61508 Lifecycle Classification	Justification	IEC 61508 Common Requirements Violation	Justification
Loss of electrical power and associated plant	3 generators controlled by common card set.	Allocation 3: Design and Development	The allocation safety-critical monitoring requirements to the same card set that controlled the generators created a common point of failure.	Safety management 1: LTA safety culture	The overall safety management of the project illustrated some problems with the safety culture given that E/E/PES components were integrated in safety-critical roles without sufficient analysis of the interaction between those components.
	Risk assessment fails to identify possible failure modes.	Hazard and risk assessment 1: specification	Initial hazard and risk assessment failed to identify the vulnerability created by the common point of failure.		
Watchdog relays de-energize following commands while noted discrepancy between PLC channels	Fire pump logic uses two out of two protocol even though unwanted start is not safety-critical.	Allocation 3: Design and Development	The allocation of commands to start the duty firewater pump to the redundant voting system was unnecessary because unwarranted start did not have adverse safety implications.	Documentation 2. Documentation incomplete	There is insufficient documentation to determine whether or not the 'fail safe' nature of the command to start the pump was considered when allocating it to the redundant voting system.
	Did not understand interaction of asynchronous logic, latches and the timers.	Hazard and risk assessment 1: design and development	The designers/ integrators did not consider that a low-consequence demand on the voting system might lead to inconsistent states on the two channels.	Functional Safety Assessment 3: Assessment incomplete	There is sufficient documentation to show that the risk assessment did not consider the problem that an inconsistent state might be latched into the two channels.
	Did not use fault-tolerant synchronous architecture.	Realisation 3: Design and Development	The decision not to use a synchronous system enabled the inconsistency to remain within the architecture.	Safety management: 3. LTA management of suppliers	A key technical decision was made by E/E/PES suppliers to achieve a simpler design through the use of an asynchronous system. Integrators and end-users could have questioned whether this was appropriate for their context of use.

Table 9: Full IEC 61508 Causal Summary Chart for Case Study Incident

C. Generating Recommendations

Figure 9 again illustrates the stages in our proposed investigation and analysis techniques. As can be seen, the final activity produces the recommendations that are intended to avoid any recurrence of an incident or near miss. The generation of recommendations uses the outcome of previous stages to identify potential recommendations. These recommendations are clearly domain and incident dependent. It is important, however, that investigators document the actions that are intended to avoid any recurrence of an E/E/PES related incident. Each recommendation should be associated with a priority assessment, with an individual or organisation responsible for implementing it and with a potential timescale for intervention. Typically, a safety manager will then respond with a written report stating whether each recommendation has been accepted or rejected (Johnson, 2003).

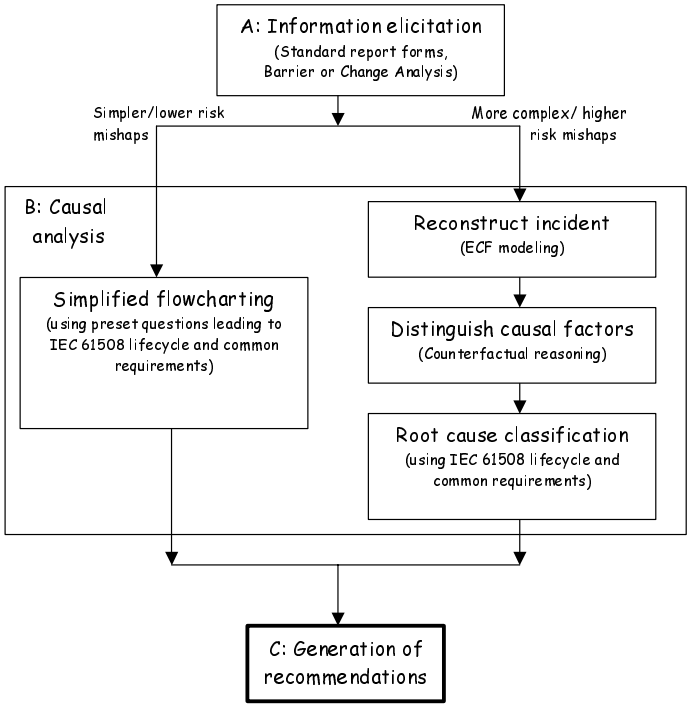


Figure 9: Overview of Investigation Schemes for E/E/PES-Related Incidents

It is important when drafting a recommendation that investigators consider whether similar interventions have been advocated in the past. Electronic information systems can be used to assist in this task. The key point, however, is that ineffective recommendations should not continue to be issued in the face of recurrent incidents. Similarly, it is important to identify situations in which recommendations are consistently rejected or inadequately implemented. Any accepted recommendations must be disseminated to those who are responsible for acting upon them. Safety managers must also assume responsibility for checking that any necessary changes are implemented according to the agreed timescale. System documentation must be updated to reflect any subsequent modifications.

Table 10 provides an example of a form that can be used to record recommendations from E/E/PES related incidents. As can be seen, different deadlines may be associated with actions that have different priority levels. This does not imply that high priority items will have an immediate deadline. Additional time is often necessary to ensure that subsequent interventions do not introduce further flaws in the design, operation and maintenance of safety-critical systems.

Causal Event	Associated Conditions	IEC 61508 Lifecycle Class.	IEC 61508 Common Requirements Violation	Recommendation	Priority	Responsible authority	Deadline for response	Date Accepted/ Rejected
Loss of electrical power and associated plant	3 generators controlled by common card set.	Allocation 3: Design and Development	Safety management 1: LTA safety culture	1. Key outputs to be segregated (see Appendix Y for technical summary)	High	Control Engineering Team Leader	1/4/2003	Accepted 15/2/2003
	Risk assessment fails to identify possible failure modes.	Hazard and risk assessment 1: specification		2. Revise risk assessment documentation for the new Fire and Gas system with emphasis on common failure modes for key systems.	Medium	Production Engineering Team Leader & Documentation Control	1/5/2003	
				3. Develop case study training material based on incident for dissemination to all production managers.	Medium	Production Engineering Team Leader Documentation Control	1/4/2003	
Watchdog relays de-energize following commands while noted discrepancy between PLC channels	Fire pump logic uses two out of two protocol even though unwanted start is not safety-critical.	Allocation 3: Design and Development	Documentation 2. Documentation incomplete	4. Review risk assessment and function allocation documentation to make explicit situations when low criticality functions are allocated to higher integrity devices.	Medium	Production Engineering Team Leader Documentation Control	1/5/2003	
	Did not understand interaction of asynchronous logic, latches and the timers.	Hazard and risk assessment 1: design and development	Functional Safety Assessment 3: Assessment incomplete	See recommendation 3.	-	-	-	
	Did not use fault-tolerant synchronous architecture.	Realisation 3: Design and Development	Safety management: 3. LTA management of suppliers	5. Review composition of Verification Action Group and refocus on hazard based assessment criteria.	Medium	Head of Engineering & Offshore Marine Tech. Panel	1/5/2003	

Table 10: Recommendation Summary Form

Conclusions

A range of techniques has been developed to support the analysis and investigation of adverse events and near miss incidents. Very few of these techniques have been specifically designed to support the investigation of E/E/PES related incidents. This report, therefore, introduces two investigation methods for this class of adverse events. The first builds on a relatively simple flowchart. Investigators can identify and categorise the causes of a mishap by answering a series of questions. The responses that they provide guide the causal analysis to underlying problems in the design, development or operation of the E/E/PES.

The second, more complex, approach introduces several additional stages of analysis. It is appropriate for more complex incidents where the questions that guide a simpler form of analysis may not be directly applicable. These additional stages also provide intermediate documentation that is necessary when investigators must justify their conclusions to other investigators, safety managers and courts of law. In particular, this second approach relies upon a timeline reconstruction of an adverse event using a technique known as Events and Causal Factors (ECF) charting. This produces a graphical sketch of the events leading to an incident. This can then be used to distinguish contextual information from causal factors. In our proposed method, these causal factors are then analysed to identify potential failures in the E/E/PES lifecycle using a checklist approach.

Both of our investigation techniques have been tailored to provide information that guides the future development and operation of safety-critical systems. In particular, the flowchart and checklist help investigators to map from the causes of an E/E/PES related incident to the clauses of the IEC 61508 standard. IEC 61508 provides guidance on the activities that should be conducted during the concept development, overall scoping, hazard and risk assessment, overall safety requirements analysis, integration, commissioning and verification, realisation, validation, operation and maintenance, and modification of safety critical E/E/PES. In addition there are a range of requirements that are common to all lifecycle phases. These include the need to ensure the competency of those involved in the operation, maintenance and modification of the system. They also include requirements relating to the ‘safety culture’ of the organisations involved in the development and operation of E/E/PES. Our use of this standard is justified because it provides a means of feeding the insights derived from any incident investigation back into the future maintenance and development of E/E/PES within safety-critical applications.

Much remains to be done. We are currently engaged in an extensive validation exercise that is intended to elicit end-user feedback on the suitability of the proposed approaches across a wide range of different industries. This exercise is gathering empirical evidence. For instance, by comparing the analysis of different investigators analysing the same incident using our techniques. It is also eliciting more direct, subjective assessments. In particular, we are keen to address any remaining difficulties that might prevent these analytical techniques from being integrated with other existing forms of incident analysis. Such information will help to validate our approaches but also to identify areas for the future development of causal analysis techniques that are specifically tailored to E/E/PES related incidents.

Our techniques are likely to identify incidents that cannot easily be attributed to lifecycle phases or common requirements in IEC 61508. The link between constructive design standards and analytical investigation techniques can, therefore, yield insights into the limitations of these standards. An implicit motivation in our work is to provide the feedback mechanisms that are necessary to improve the application of standards, such as IEC 61508 and DO-178B.

Acknowledgements
Thanks are due to Bill Black (Black Safe Consulting), Mark Bowell (UK HSE), Peter Bishop (Adelard) and Michael Holloway (NASA, Langley) for providing comments on the initial draft of this document.

References

L. Emmet, P. Bishop, B. Black and V. Hamilton, Outline Scheme for E/E/PES Related Incidents, Adelard technical Report , 2002.

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.

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.

International Electrotechnical Commission (2003), IEC 61508 Functional Safety of Programmable Electronic Safety-Related Systems. Available via http://www.iec.ch/functionalsafety

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

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.

C.W. Johnson, A Brief Overview of Causal Analysis Techniques for Electrical, Electronic or Programmable, Electronic Systems. Technical Report, 2002.
Available from http://www.dcs.gla.ac.uk/~johnson/hse.

C.W. Johnson (2003 in press), A Handbook for the Reporting of Incidents and Accidents, Springer Verlag, London, UK.

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

N. Leveson, (1995), Safeware: System Safety and Computers, Addison Wesley, Reading, MA, United States of America.

N. Leveson, (2002), 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.

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.

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.

Appendix A: Comparison and Evaluation of Causal Analysis Techniques for E/E/PES

Most companies and regulatory organizations lack the resources to train investigators in a range of different causal analysis techniques. It is, therefore, important to help managers focus finite resources on 'appropriate' analytical techniques. One means of doing this is to identify those causal analysis techniques that provide the greatest support for the integration with IEC 61508 proposed in the previous section. Table A1, therefore, provides a subjective assessment of the support that each of the previous causal analysis techniques provides for the identification of failures in the IEC 61508 requirements enumerated in Table 6.

Rationale for the Evaluation Matrix

It is important to stress that Table A1 documents subjective evaluations. They reflect the author's experience of applying each of the approaches to a series of E/E/PES related incidents in domains that range from international space missions through to healthcare and the offshore process industries. These assessments were validated in consultation with members of the HSE and experts on the IEC 61508 standard. Further validation exercises are currently being conducted with safety managers and incident investigators from a range of potential end-user organizations. In anticipation of the results of this validation exercise, it is important to provide a justification for some of the decisions that are embodied within this diagram.

Barrier Analysis

Barrier analysis provides strong support for the overall analysis of E/E/PES related incidents (US Department of Energy, 1992). It can be used to identify the failure of protection devices at a relatively high level of granularity. Hence, it is likely that it will prove a useful means of identifying problems in the overall scope of a project. Tracing the way in which an initial threat can be propagated to a target can also support the identification of hazards. In contrast, this technique has relatively little to say about the planning of activities such as the detailed installation and commissioning of an E/E/PES except where these processes give rise to hazards or can be viewed as barriers. It is for this reason that we would recommend Barrier analysis as a relatively accessible and low cost means of performing an initial causal analysis. More complex incidents may, however, require that additional modelling and analysis facilities provided by other approaches.

Change Analysis

Change analysis is similar to Barrier Analysis in that is provides a means of investigating incidents at a relatively high level of granularity (US Department of Energy, 1992). This approach focuses on the differences between what actually did happen and what was supposed to happen. The intended behaviour of the E/E/PES can partially be derived from the documentation associated with IEC 61508 development and by other legal and regulatory documents. It might, therefore, be used to identify violations and problems associated with all of the requirements illustrated in Table 5. It is important to stress, however, that a number of problems complicate the application of this approach. In particular, it cannot easily be applied if end-users or suppliers have only partial access to this documentation. Similarly, it can be difficult to reverse engineer expected operational behaviour for legacy systems.

Timelines

Timelines differ from Barrier and Change Analysis because they provide strong support for the detailed modelling of what actually happened during an E/E/PES related incident (Johnson, 2003). Problems arise when IEC 61508 requirements cannot be directly related to particular events. For example, the common requirement to ensure competency would have to be represented as specific events that were intended to ensure this requirement. Some event-based techniques such as ECF avoid this limitation by enabling investigators to represent the conditions that make failure events more likely. For instance, a lack of competence might provide the condition that makes it more likely a test will not uncover a potential bug. Unfortunately, conditions are not a standard part of most timelines. Hence, this approach may only be suitable for identifying specific failures in the lifecycle phases of IEC 61508.

	Elicitation and Analysis techniques		Event Based Techniques			Flowcharts and taxonomies		Accident Models		Argumentation Techniques	
	Barrier Analysis	Change Analysis	Timelines	Accident Fault Trees	ECF	MORT	PRISMA	TRIPOD	STAMP	WBA	CAE
IEC 61508 Lifecycle phase											
Concept	F	F	U	U	P	F	P	F	P	U	F
Overall Scope	F	F	U	U	P	F	P	F	P	U	F
Hazard &Risk Assessment	P	P	P	P	P	F	P	P	F	U	F
Overall Safety Requirements	F	F	U	U	P	P	P	F	F	U	F
Allocation	F	P	P	U	F	P	P	F	P	U	U
Planning of I & C, V, and O&M	U	P	P	P	F	F	F	U	P	P	U
Realisation	U	F	F	P	F	U	P	U	F	F	U
Installation & Commissioning	U	P	F	P	F	P	P	P	P	F	P
Validation	P	P	F	P	F	P	P	P	U	F	P
Operation & Maintenance	P	F	F	P	F	P	P	F	F	F	P
Modification	U	F	F	P	F	P	P	U	F	F	P
IEC 61508 Common Requirements											
Competency	P	P	P	P	F	P	P	F	P	P	P
Lifecycle	U	P	P	P	F	P	P	P	P	P	P
Verification	P	P	P	P	F	P	F	P	P	P	P
Safety management	P	P	P	P	F	P	P	P	P	P	P
Documentation	P	P	P	P	F	P	P	P	P	P	P
Functional safety assessment	P	P	P	P	F	P	P	P	P	P	P

Key: (U)nsupported, (P)artially supported, (F)ully supported

Table A1: Degree of Support for Mapping from Products of Causal Analysis Technique to Failures in IEC 61508 Requirements

Accident Fault Trees
Accident fault trees have many of the strengths and weaknesses of timelines (van Vuuren, 2000). Their ability to identify failures and violations of IEC 61508 requirements is, however, compromised by the lack of temporal information in the logic diagrams. This is a strength if investigators cannot determine the exact ordering of particular events. In general, however, the lack of temporal information creates problems for investigators who must reason the detailed sequence of operations executed by an E/E/PES in the course of an adverse event. This also creates problems for the analysis of IEC 61508 requirements. There are dependencies between the various stages of the development lifecycle. Hazard and risk assessment should preceed operation and maintenance. It is difficult to represent the violation of such requirements using this modeling and analysis technique.

Events and Causal Factors Charting
As mentioned in previous paragraphs, the introduction of conditions into an event-based model can offer significant advantages (US Department of Energy, 1992). In particular, it enables investigators to trace problems in satisfying the common requirements in 61508 that cannot easily be related to specific events. These conditions can capture the precursors or latent factors that make particular failure events more likely. For instance, a lack of adequate documentation may prevent E/E/PES integrators from identifying particular failure modes when developing more complex systems such as the redundant channels in our case study. It is possible to criticise the incorporation of conditions into event-based models. Conditions can be represented by the specific events that lead to them. For example, instead of claiming that the documentation was inadequate we would be forced to identify particular instances when named individuals failed to adequately document their work. These arguments are important, however, as noted previously the problems of obtaining information can prevent end-users, integrators and developers from tracing these specific events. Hence, we would argue for the retention of conditions in techniques such as ECF.

MORT
MORT provides strong support for the identification and analysis of problems in the management mechanisms that are intended to protect safety-critical systems (Johnson, 1980). Table A1 therefore denotes that this causal analysis technique might support the analysis of failures in the IEC 61508 common requirements. These relate to management activities in ensuring competence, establishing safety management procedures etc. MORT also contains branches that relate to risk assessment processes. It can, therefore, be argued that the application of this approach will uncover problems in the lifecycle requirements that relate to hazard and risk assessment. There is, at present, little support in MORT for a detailed analysis of the problems that might complicate the realisation of E/E/PES related systems. The original technique could be refined to provide this support, for example following the approach advocated in Leveson's (1995) Software Fault Trees.

PRISMA
The PRISMA approach has much to recommend it in terms of its simplicity and previous successful applications in a range of different industries (van der Schaaf, 1996). The subjective assessment in Table A1 is less a reflection of the underlying ideas behind the technique than it is an assessment of the existing classification schemes. As with MORT, it would be entirely possible to tailor this approach to E/E/PES and thereby turn the (P)artial support assessments into (F)ull support. For example, the PRISMA flow chart illustrated in previous sections considers engineering, construction and materials as key issues in the technical reasons for an adverse event. We could extend this flowchart to represent the requirements associated with realisation phase in Table A1. This observation motivates the development of a candidate analysis scheme for E/E/PES based on an extended flowchart.

TRIPOD
TRIPOD is based around concepts that were introduced in barrier analysis (Hudson et al, 1994). In addition, however, it also considers the preconditions that can compromise system defences. These preconditions can, in turn, be related to latent failures and general failure types. From this is follows that TRIPOD will have the same strengths and weaknesses as Barrier Analysis but with specific improvements for analysing the requirements of IEC 61508 whenever those requirements are compromised by the General failure Types. The initial list of these more general causes did not include software failure. As with

MORT and PRISMA, however, this could be rectified through the subsequent tailoring of the approach to support the analysis of E/E/PES related incidents.

STAMP
STAMP is intended to take a novel and distinct approach to the identification of causal factors in adverse events (Leveson, 2002). A control model is developed and flaws in the constraints between system components are identified using a form of checklist. This checklist in its current form provides strong guidance on the identification of problems in risk and hazard assessment. It offers less support for identifying the meta-level validation processes that must be used to ensure that constraints between control entities are satisfied. Introducing more sophisticated hierarchical control models could do this. However, this would require considerable additional development work to derive an approach that is more directly tailored to the analysis of IEC 61508 requirements failures.

WBA
WBA is a very flexible technique. It compasses a two-stage approach in which an incident is reconstructed using a version of a timeline (Ladkin and Loer, 1998). This then drives a more formal analysis of the necessary and sufficient causes of an adverse event. Relatively little is said about the content of the arguments rather than the form that they must take. Rules are provided to establish that a causal argument is correct without predetermining what types of failures or behaviours that argument is about. This makes it difficult to classify the degree of support that this approach provides as a tool to identify the failure of IEC 61508 requirements. This flexibility is achieved at a cost in terms of the level of skill and expertise that must be acquired before the technique can be applied.

CAE
CAE provide a high-level overview about the arguments and evidence that supports particular conclusions. The approach is similar to WBA in that there is little explicit support for the analysis that must be used to identify key components of the resulting graphical structures (Johnson, 2001). For example, there is no procedure that can be used to help investigators determine what evidence would need to be gathered in order to demonstrate a failure in the safety management of an E/E/PES related system. As with the other techniques, this guidance can be provided by extending the various stages in the existing approach.

Summary
This appendix has provided a subjective comparison of a range of different causal analysis techniques. The evaluation is based on a previous investigation that used each approach to analyze the causes of the same E/E/PES related incident that forms the case study in this paper. For more information, the interested reader is directed to Johnson (2002). In contrast, this report assesses whether each technique can be used to identify potential shortcomings in the lifecycle stages and common requirements within IEC 61508. The analysis summarized in Table A1 and justified by the previous paragraphs has motivated our decision to develop a flowchart-based approach and an event modeling approach to the causal analysis of E/E/PES related incidents. It is important to stress that alternative techniques, including the control theory approach of STAMP, might also have been used to support our analysis. Further work is required in order to demonstrate that the subjective evaluations identified in Table A1 can be sustained into the practical experience gained from applying the two proposed analysis techniques.