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

Chris Johnson,

Dept. of Computing Science, University of Glasgow, Glasgow, G12 9QQ.
http://www.dcs.gla.ac.uk/~johnson

This paper presents two techniques that have been developed to support the analysis of mishaps involving electrical, electronic or programmable electronic systems (E/E/PES) under an HSE sponsored project. One provides 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. The second approach is more complex and is, therefore, more appropriate for incidents that have greater potential consequences or a higher likelihood of recurrence. It uses Events and Causal Factors (ECF) modelling together with particular forms of causal reasoning developed by the US Department of Energy (1992). Both approaches map 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. 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.

1. Introduction

Very few accident analysis techniques support the investigation of adverse events involving programmable systems. In this paper, we identify two causal analysis techniques that can be used to analyse this calss of failures. An E/E/PES case study will be used to illustrate the causal analysis techniques in this paper. This incident has been chosen through consultation with the HSE and industry representatives. *Some details have been removed and others have been deliberately added so that the case study does not reflect any individual incident.*

1.2 Case Study Incidents

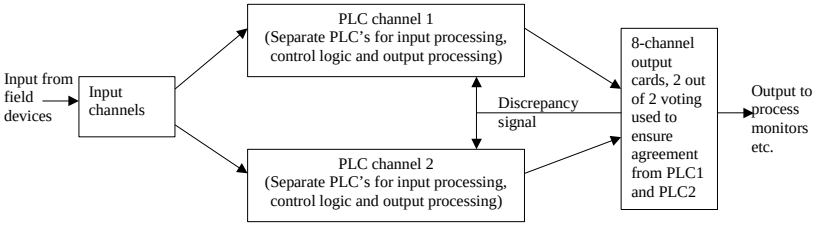


Figure 1: High-level architecture for the E/E/PES Case Study

Figure 1 illustrates the E/E/PES architecture at the heart of the case study. Two redundant 'channels' ensure that near identical data is passed to independent PLC's 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 card, which uses a form of two-out-of-two voting protocol. Although this is an asynchronous system, in normal operation the two input PLCs will sample the same values and the logic PLCs will arrive at the same outputs. 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.

The incident started when a spillage of methanol was detected on board an offshore production vessel. 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 that was inducing a list so that material could be sluiced from the decks. The crew could not use their control systems to halt the ballast operations and the stability of the vessel was compromised. 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. 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.

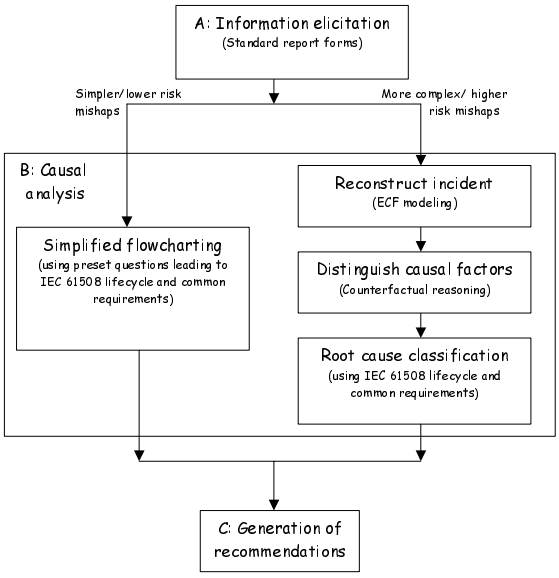


Figure 2: Overview of Investigation Schemes for E/E/PES-Related Incidents

2 Elicitation

Figure 2 provides an overview of the stages in that comprise our two causal analysis techniques. These stages also reflect the structure of this paper. The next section focuses on elicitation techniques. Subsequent sections focus on causal analysis and the generation of recommendations.

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	Rugius 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).

2.1 Design of E/E/PES Reporting Forms

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 provide a minimum set of requirements for the information that should be obtained about an E/E/PES related incident. However, they can also become unwieldy and cumbersome if investigators have to complete too many irrelevant fields. The nature of the information obtained 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.

3. Causal Analysis

This section 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.

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

Most E/E/PES related incidents stem from problems in the development lifecycle. Latent causes occur in risk assessment, design, implementation, testing, maintenance etc. Other problems, such as poor project management; affect many stages of development. It is for this reason that both of the causal analysis techniques in this paper exploit the lifecycle and process requirements embedded within the IEC 61508 standard. This is one of several taxonomies that could have helped identify causal factors in E/E/PES incidents. We adopt this approach because this standard provides a bridge between the analysis of previous failures and the redesign of safety-critical systems. Table 1, therefore, provides a high-level classification of the potential problems that can affect phases of the IEC 61508 lifecycle or the common requirements that hold across several phases. 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.

3.2 Flow Charting Scheme

Figures 4 and 5 provide an overview of our flow-charting technique[1]. 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 4 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 could also be considered by examining the items listed under all six of the common requirements in the third row from the bottom. Investigators 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 4 and the further line of analysis continued on Figure 5.

[1] Initial ideas for this technique were provided by Bill Black and are documented in Emmet et al (2002).

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) 7.4.5.1/3
Allocation		
Planning of I & C, V, and O&M		
Realization		
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

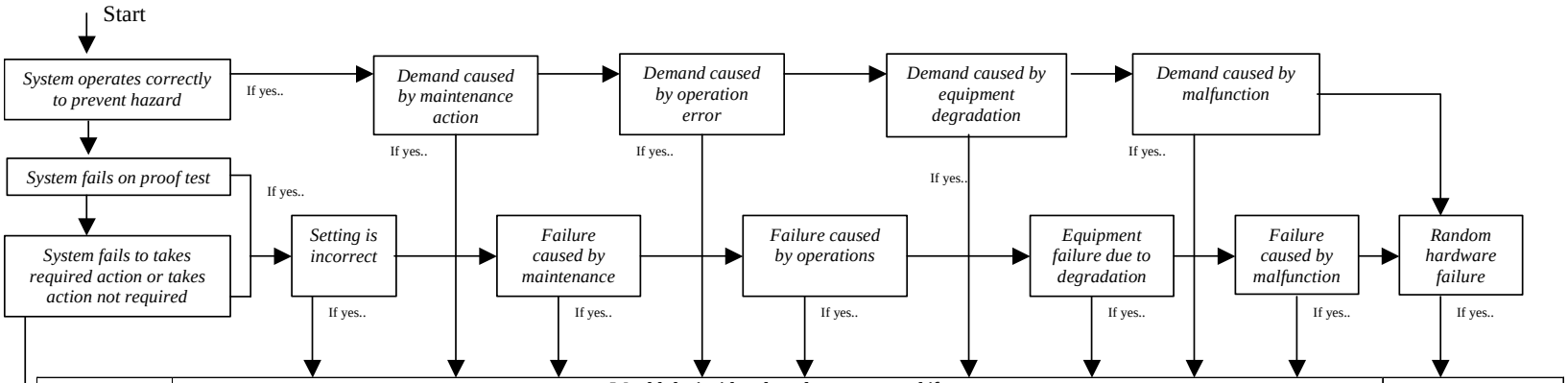
Key: LTA is Less Than Adequate, IEC 61508 references are to Part 1 except as indicated by parentheses e.g. (2)

Table 1: Taxonomy for Analysing E/E/PES Related Failures Under IEC 61508 (Emmet et al 2003).

Most incidents involve multiple causes. 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. The analysis might identify several requirements or lifecycle activities that might have prevented this incident from occurring in the manner described. It is important to document the outcome of this flowchart analysis. This is done using the form illustrated in Table 2. 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 4 and 5. The allocation is also supported by a justification that is intended to document any intermediate reasoning to other investigators and co-workers.

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 2: Abridged IEC 61508 Flowchart Causal Summary for Case Study

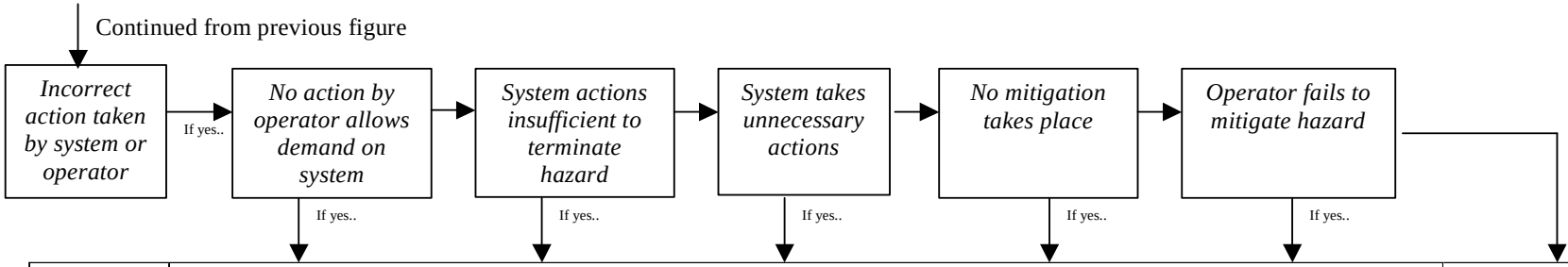


	Would the incident have been prevented if:					
Design	- different equipment selected? - installation design different? - configuration was correct	- maintenance facilities had been designed adequately	- operations facilities had been designed correctly	- different equipment selected? - installation 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 4: 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 5: High-Level Flow Chart to Support Causal Analysis of E/E/PES Related Incidents Using IEC 61508 Taxonomy (Emmet et al, 2003).

3.3 Event & Causal Factor Analysis

As can be seen, the flowchart analysis focuses on the operators' perspective on this incident. In order to look more closely at detailed design issues, additional questions would be needed. The resulting flow charts and this would sacrifice many of the benefits associated with the simple approach. The following section, therefore, presents a more sophisticated analytical technique.

First Stage: Information Elicitation and ECF Modelling

Figure 6 shows a simplified form of Events and Causal Factors (ECF) diagram. This modeling technique was developed by the US Department of Energy (1992) to provide an overview of events leading to an incident. 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. This figure 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 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 6 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.will be considerably more complex than those shown in the previous diagrams

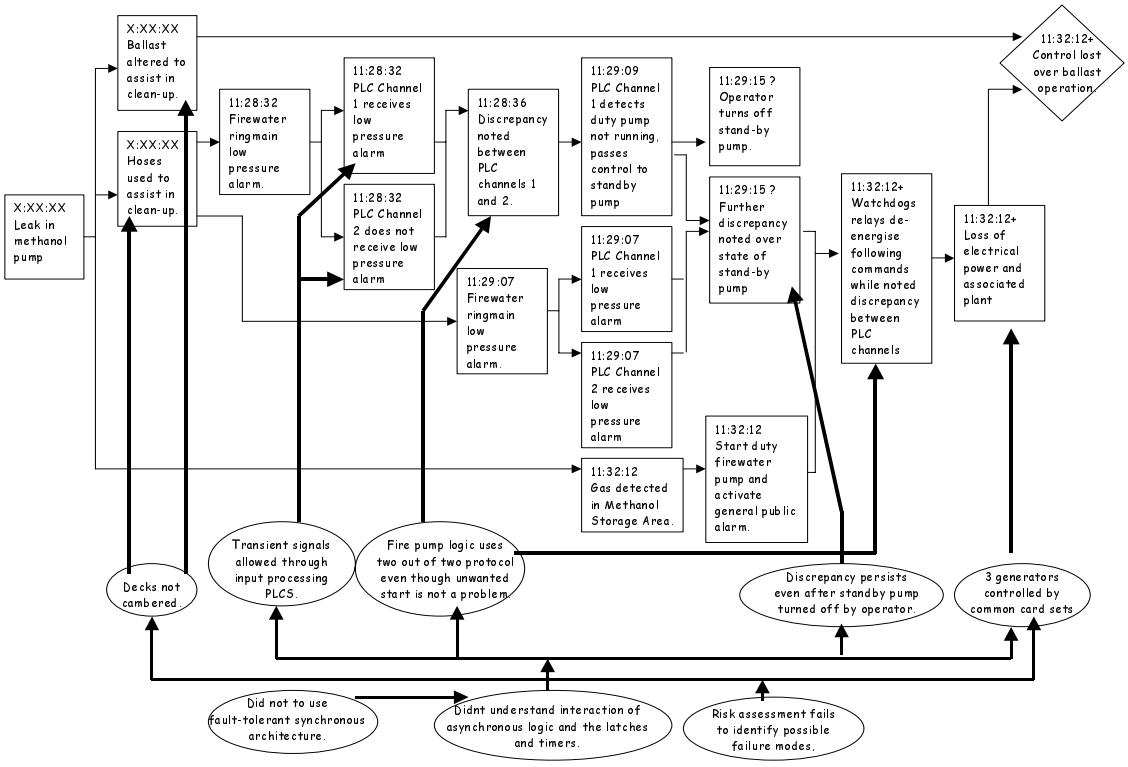


Figure 6: An ECF Diagram Including Developer/System Integrator Information

Second Stage: Causal (Counterfactual) Reasoning

A further stage of analysis is required in order to distinguish potential causal factors from more contextual information. 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 3 provides an overview of the output from this form of analysis. 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.

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 3: Cause/Context Summary Chart for Case Study Incident

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 1. The first task is to identify those conditions that contributed to each causal event using the ECF chart illustrated in Figure 6. 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. Table 4 presents the results of this analysis. A justification helps others to understand why investigators found violations of common requirements in particular phases of the IEC 61508 lifecycle. Table 4 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.

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 4: IEC 61508 Causal Summary Chart for Case Study Incident

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 5: Recommendation Summary Form

4. Generating Recommendations

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).

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 5 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.

5. 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.

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) and Peter Bishop (Adelard) 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.

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

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.