Using Software Development Standards to Analyse Accidents Involving Electrical, Electronic or Programmable, Electronic Systems: The Blade Mill PLC Case Study

C.W. Johnson; Dept. of Computing Science, University of Glasgow, Glasgow, G12 9QQ, UK.
Tel.: +44 141 330 6053, johnson@dcs.gla.ac.uk

M. Bowell; Electrical & Control Systems Unit, Health and Safety Executive, Bootle, Merseyside, L20 3QZ, UK, Tel: +44 151 951 4064, Mark.Bowell@hse.gsi.gov.uk

Abstract

This paper presents the results of a project commissioned by the Electrical and Control Systems Unit of the UK Health and Safety Executive. The results of the project will be used to give guidance to operators and suppliers of electrical, electronic or programmable electronic systems (E/E/PES) in satisfying particular requirements of the Management of Health and Safety at Work Regulations 1999. The associated approved code of practice explains an obligation to 'adequately investigating the immediate and underlying causes of incidents and accidents to ensure that remedial action is taken, lessons are learnt and longer term objectives are introduced'. There are relatively few techniques that might be used to investigate the underlying causes of E/E/PES related incidents. The following sections, therefore, introduce two techniques to support the investigation of this class of mishaps. One is based around flowcharts. These provide a series of questions to prompt investigators about the causal factors leading to an adverse event. Such a lightweight approach is appropriate for low consequence events. In contrast, the second technique involves additional documentation and analysis. It is, therefore, more appropriate for incidents that have greater potential consequences or a higher likelihood of recurrence. Events and Causal Factors (ECF) modeling is used together with a form of causal reasoning developed by the US Department of Energy (1992). The intention is that both the lightweight flowcharts and the more complex modeling techniques should help investigators to 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 systems. It is likely, however, that we will encounter incidents that cannot easily be attributed to lifecycle phases or common requirements in IEC 61508. Our work, therefore, offers important insights into the limitations of existing development standards. An implicit motivation in our work is to provide the feedback mechanisms that are necessary to improve the application of IEC 61508 and related standards such as DO-178B. A fatal injury in a gravel wash plant is used to illustrate this paper.

Introduction

The UK Health and Safety Executive's (HSE) mission is to ensure that risks to people's health and safety from work activities are properly controlled. An essential element of controlling risk is learning from past incidents and accidents – deciding the cause in each case and introducing new controls to reduce the risk of a repetition. To achieve its mission, HSE is supported by legal requirements, by approved codes of practice that interpret these requirements and by voluntary standards. The UK Health and Safety at Work Act 1974 places a legal duty on every company or organisation to reduce its risks "as far as is reasonably practicable". In other words, risks must be reduced until any further benefit is outweighed in gross disproportion by the effort required to obtain that benefit. In general, reasonably practicable measures are authoritatively defined in associated regulations and their approved codes of practice. They are also amplified through voluntary standards and guidance. The Management of Health and Safety at Work Regulations 1999 (HSE, 1999) require every employer to carry out a risk assessment, introduce the necessary

preventive and protective measures, and monitor these measures. The associated approved code of practice explains that monitoring includes:

1. *Adequately investigating the immediate and underlying causes of incidents and accidents to ensure that remedial action is taken, lessons are learnt and longer-term objectives are introduced.*

2. *It may be appropriate to record and analyse the results of monitoring activity, to identify any underlying themes or trends, which may not be apparent from looking at events in isolation.*

HSE is currently preparing general guidance material, possibly with supporting software tools, on how to investigate incidents and accidents. In parallel, HSE's Electrical and Control Systems Unit aims to produce cross-industry guidance on learning from incidents that specifically involve electrical and/or electronic and/or programmable electronic systems (E/E/PES). The terminology and conceptual framework for the E/E/PES technology specific work is taken from the international standard IEC 61508 (IEC 2000, 2003). This standard is applicable to all applications using this technology across all industry sectors, although the extent to which it applies will depend on other existing application and industry specific standards. IEC61508 includes requirements for developers and operators to learn from accidents and incidents (6.2.1-i of IEC 61508-1) and for suppliers to correct defects and report them to users (7.8.2.2 of IEC 61508-2). It does not give details on how to satisfy these requirements. In order to create some of the technical content necessary for HSE guidance, the Electrical and Control Systems Unit commissioned a multidisciplinary project on learning from incidents involving E/E/PE safety-related systems (HSE, 2003). The key stages of this project were to:

1. Evaluate existing schemes for analysing incidents, classifying data and generating lessons;
2. Consult users of existing schemes and potential users of HSE guidance;
3. Select and modify an existing scheme to integrate it with IEC 61508;
4. Test the new scheme using data from real incidents;
5. Present the scheme in the wider context of incident reporting, investigation and process improvement.

A companion paper describes the validation exercises in stages 4 and 5. This paper presents results from stages 2 and 3. The following section summarises the findings from our industry consultation into the reporting of E/E/PES related incidents. Subsequent sections introduce two new causal analysis techniques. A recent industrial accident described by the US Department of Labor's Mine Safety and Health Administration is used to illustrate the application of these techniques.

Industry Consultation: The development of our investigation techniques began with ten site visits to companies or organisations involved in the supply or operation of E/E/PES. Structured interviews were used to gather information about existing reporting procedures and mechanisms for disseminating any lessons learned from previous incidents. We were keen to identify perceived needs for incident reporting and investigation. The interviews were also intended to elicit any particular requirements for analysing E/E/PES related incidents. The industry sectors covered were pharmaceutical, nuclear, oil and gas, chemical process, marine, rail and machinery.

Roles included end users, designers, maintainers, procurers, assessors, system suppliers and component suppliers.

A number of key findings emerged from the consultation process. Comprehensive incident reporting and learning schemes that include the supply chain and information sharing are impeded by industry fragmentation. In particular, contracting out and the lack of continuity in the supply chain prevented any 'holistic' or 'systemic' approach. The user organisation's most significant technical influence over contractors is the standards used for project development. Many user organisations no longer have their own standards and instead reference international standards such as IEC 61508. Changes to these standards take many years. There are also competency and experience problems in most contract organisations. This applies both to operators and safety personnel. The majority of existing systems will not have been implemented using IEC 65108 as a design basis. There will be limited knowledge on the design history of such systems. Any guidance produced by HSE will need to be suitable for use with legacy systems. As might be expected, large end-user companies had the most sophisticated schemes especially where they are subject to the most regulation. End-user schemes were generic. In other words, they were not focused on E/E/PES. More than one company observed that the implementation of a more rigorous reporting scheme would increase the incident reporting rate, suggesting that there was previous under-reporting. However, they argued that if the scheme were successful then the increase in reporting rate might be offset by an anticipated reduction in the serious accident rate. Confidentiality could encourage reporting but most companies had non-confidential schemes. Management support and motivation is important for a successful scheme. This requires feedback to the reporters and investigators to show their activities are valued and acted upon.

Only a small fraction of reported incidents involved a special investigation of E/E/PES failure. For example, one company had 750 incidents per year, 6 were investigated in detail and only one involved this kind of special investigation. End user organisations often found it difficult to determine whether E/E/PES were implicated in an incident. Several causal analysis techniques were used. These included: timelines, event trees and checklists; a method similar to TRIPOD involving accident trees plus structured checklists (Johnson, 2003); event-based/event chain causal analysis (this company expressed dissatisfaction with their method, saying it did not get to the root causes very well); and ad-hoc approaches such as textual elaboration by designated experts. The E/E/PES suppliers did not use any specific method. In large companies we found up to four levels of internal incident enquiry depending on severity, e.g. trivial, local, formal investigation, formal enquiry, with different levels of investigation and different personnel at each level. Typically for large companies there were many thousands of trivial incidents per year but less than ten resulted in the most stringent type of enquiry. Some companies classified incidents according to type for subsequent monitoring and trend analysis. However, there was rarely any formal classification scheme of incident causes. The priority was to identify necessary changes in product, procedures or personnel competency. Recording of incidents, analyses and tracking of safety recommendations was quite sophisticated in some large companies and was implemented independently of other systems. However small companies tended to use existing QA systems for this purpose.

Some companies expressed concern about the costs of implementing any new scheme, for example in training and in writing new documentation and procedures. Also extensions to reporting might be a disincentive to both the reporters and the investigators if the process is too onerous. A new scheme should augment rather than replace existing systems, avoid technical language or jargon and communicate strengths and limitations clearly. Some companies had explicit mechanisms for reviewing and generalising incidents into recommendations. Experience was fed back into the design rules and business processes, and was often disseminated more

broadly to other sites, trade bodies and regulators. Tools such as databases, intranets, bulletin boards and e-mail aided dissemination. However this did not always succeed in changing company culture.

The Case Study Incident: This consultation process led to the development of two different analysis techniques. In order to illustrate the application of these tools, we introduce an incident that resulted in fatal injuries to a mechanic working in a gravel wash plant. This case study has been chosen because it is typical of the way in which incidents stem from the interaction between E/E/PES-related failures, hardware faults and management issues. The gravel wash plant cleaned and screened materials that were brought by truck from an off-site pit. The output from the operation was sold as part of a ready mix concrete business. The incident occurred inside a blade mill that was used to 'pre-condition' aggregates prior to wet screening. The mill consisted of two screws driven by two 40-horse power motors. The spiral grooves of each screw interlocked to help prepare the gravel. The motors were operated from a control center in a trailer about 30 meters from the mill. On the day of the incident, the mechanic and the wash plant foreman worked together to thaw frozen material inside the mill. They also intended to replace broken paddle tips and wearing shoes. The mechanic removed some sheets that had been placed on top of the mill to retain heat generated by a propane burner. This was being used to help thaw the frozen material. He then signalled to the foreman in the control center that he should start the mill motors in order to check that the blades were free. The motors started and so the foreman switched his attention to another task away from the mill. Before leaving, he switched the mill's start/stop buttons to the 'off' position. After completing his other task, the foreman returned to help carry out the necessary repairs on the mill paddles and shoes. However, the foreman was then called to assist an electrician who was working on a faulty circuit breaker. This had been tripping out after 10 to 15 minutes of operation. The electrician switched the breaker on and together with the foreman he watched it for several minutes without observing a trip. The electrician then turned it off and began to diagnose the problem. Meanwhile, the foreman returned to check on the mechanic. As he was leaving the control center, the foreman noticed that the two blade mill buttons were in the "run" position. He pushed them "off" and continued on to the mill where he found the mechanic entangled in the blades. Investigators determined that the mechanic had started the mill to clear some remaining frozen material after the foreman had left to work on his initial task away from the mill. The blades operated as the mechanic anticipated until the circuit breaker had tripped, before the electrician's inspection. For some reason, the mechanic then went back to work in the mill without shutting off any switches.

The faulty circuit breaker identified by the electrician controlled the power to several different systems including the control center lighting and the Programmable Logic Controller (PLC) that controlled the mill. A modification to the PLC approximately three months before the accident had resulted in power being unintentionally returned to components following a power failure, if their switches had been left in the "on" position. In consequence, the mill began operating when the breaker was reset during the troubleshooting by the foreman and the electrician. As can be seen, this incidents, stems from multiple causes. It was due to the failure to lock out the two-blade mill during the repairs. This stemmed from errors in the reprogramming of the PLC that allowed the automatic restart of equipment under control following a power trip. Further causes do not relate directly to the PLC. Power to the motor's circuit breakers was not locked out. No other measures were taken to prevent the equipment from becoming energized without the knowledge of the individuals working on it. In particular, the foreman was aware that the motor's circuits were not locked out while the electrician worked on the circuit breaker panel.

Root Causes of E/E/PES Related Incidents Under IEC61508

Several authors have argued that the root causes of complex, technological accidents often lie in decisions that were made months and years before the incident occurred (Leveson, 2002, Landkin & Loer, 1998). It is for this reason that our analytical techniques trace the causes of E/E/PES related accidents to problems in the development lifecycle. Latent causes can stem from the risk assessment process, during more detailed design, in implementation or in testing. Adverse events also often occur as a result of periodic maintenance, as was the case in the wash plant example. It is important also to recognise that other problems can affect several different stages of the lifecycle. For instance, poor documentation standards can carry problems forward from an initial risk analysis into implementation and beyond. Similarly, inadequate project management can undermine most development techniques. The causal analysis techniques presented in this paper, therefore, map the causes of E/E/PES related incidents to failures in the lifecycle stages and common process requirements in the IEC 61508 standard. This standard is one of several that could have been used (Johnson, 2003). The decision to adopt IEC 61508 is justified by its relatively widespread use in the process industries. HSE also recommended this general approach as the starting point for our work.

Table 1 provides a high-level classification of the potential problems that affect particular stages or are common to several different phases of the IEC 61508 lifecycle. 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 identify which of these potential failures contributed to the particular causes of our case study. For example, an initial analysis of the wash plant example might argue that it stemmed from a modification failure. The verification and validation conducted after the reprogramming of the PLC failed to identify the particular failure mode that led to the incident. An important argument in this paper is that we must support investigators by providing tools that might help both to obtain and to justify such a causal analysis. The following pages, therefore, present two different techniques that can be used to map from accounts of an adverse event to the particular causes listed in Table 1.

Flow Charting Scheme: The flow-charting scheme provides a low cost technique for relatively low consequence incidents. Figures 1 and 2 present the current charts[1]. Analysis proceeds by asking a series of high-level questions about the nature of the E/E/PES-related incident. 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 investigator moves along the horizontal arrows. For instance, if the system intervened to address maintenance problems then they would follow the arrow in Figure 1 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. For instance, a maintenance failure might be due to problems in the risk assessment associated with the maintenance procedure or it might have been due to inadequate maintenance facilities and so on.

Table 1 - Taxonomy for Analyzing Computer Related Failures Under IEC 61508 (HSE, 2003).

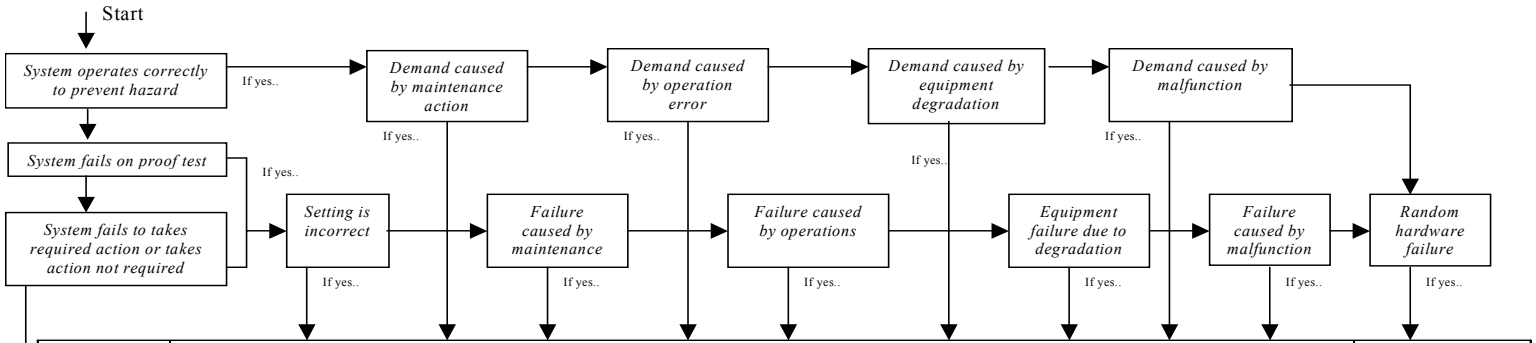
IEC 61508 Lifecycle phase	Detailed taxonomy	IEC 61508 ref
Concept Overall Scope Hazard & Risk Assessment	1. LTA Hazard identification 2. LTA Consequence and likelihood estimation	7.2,7.3,7.4
Overall Safety Requirements Allocation Planning of I & C, V, and O&M Realization	1. LTA specification 2. LTA selection of equipment 3. LTA design and development 4. LTA installation design 5. LTA maintenance facilities 6. LTA 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
Installation and commissioning	1. LTA installation 2. LTA commissioning	7.5 (2), 7.13.2.1/2, 7.13.2.3/4
Validation	1. LTA function testing 2. LTA discrepancies analysis 3. LTA 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 assessment LTA 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)

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. In Figure 1, these address problems created by operator 'error', equipment damage and by equipment malfunctions. For some incidents, there will be failures identified by analyzing several of these different questions. A system may operate correctly to prevent a hazard although there may also be subsystem failures or operator interventions that initially fail to rectify the situation. In this case, analysts would focus on the top line in Figure 1 and the further line of analysis continued on Figure 2. The analysis might, therefore, help to identify many different causes on each pass through the flowchart. It is difficult to justify this exhaustive form of analysis for relatively minor incidents. In such cases, investigators may choose to stop once they have identified a potential cause from the flowcharts. Therefore, it is important that Safety Managers consider the order of questions in Figures 1 and 2. For instance, the current format asks whether maintenance issues potentially caused an incident before it elicits information about operator failures. This ordering can bias the analysis towards the causal factors that appear at the beginning of the flow chart. It is for this reason that we recommend a more sustained and exhaustive analysis so that investigators will consider the causes represented by subsequent entries. If this is not possible then safety managers should monitor the products of any causal analysis to identify the effects of ordering bias.

The flowcharts illustrated in Figures 1 and 2 have been validated against a series of case study incidents. These include the human factors related failure of a petrochemical production plant and a synchronisation incident in which redundant PLC pipelines shut down a floating production vessel (Johnson, 2003a). Each of the incidents that we have examined has helped to drive further refinements to the flowchart. We are currently conducting usability studies and validation exercises involving safety managers from across the process industries, including nuclear power generation and petrochemical production. These validation exercises also include participation from companies who supply and integrate E/E/PES applications. This is important because they are often called upon to identify the causes of mishaps that are reported by end-users. We also recognize that it may be necessary to tailor these flowcharts to the particular needs of an application domain. For instance, incidents involving E/E/PES in embedded systems are seldom caused by problems in the design and layout of graphical human computer interfaces. In contrast, user interface design has been at the heart of several recent incidents in petrochemical production (Johnson, 2003a). It should be stressed, however, that the flowcharts will become increasingly cumbersome as they are expanded to capture a growing range of potential causes. However, Figures 1 and 2 do illustrate our general approach to the analysis of less complex incidents and accidents.

It can be argued that such flowcharts constrain the identification of causal factors. They encourage very limited thinking about what contributes to adverse events. However, it is important to reiterate that we only advocate the use of this approach to support the initial analysis of low consequence, relatively simple mishaps. It is not intended to provide a panacea for the investigation of E/E/PES related incidents. It is, however, intended to provide a low cost approach that might replace the ad hoc techniques which are currently being used because many organisations lack the resources or motivation to use more complex approaches.

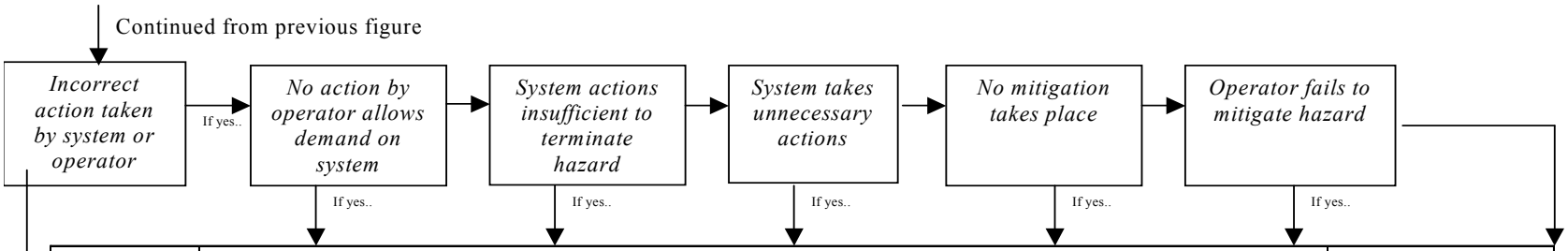


	Would the incident have been prevented if:					
Hazard and Risk Assessment	- hazard and risk analysis had considered all modes of operation and causes	- hazard and risk analysis had considered all modes of operation and causes	- hazard and risk analysis had considered all modes of operation and causes			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
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	
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 …

Fig. 1 - High-Level Flow Chart to Support Causal Analysis of E/E/PES Related Incidents Using IEC 61508 Taxonomy [Continued in next figure] (HSE, 2003)



	Would the incident have been prevented if:					
Hazard and Risk Assessment	- hazard & risk analysis had considered all modes of operation & causes	- hazard & risk analysis had considered all modes of operation & causes	- hazard & risk analysis had considered all modes of operation & causes	- hazard & risk analysis had considered all modes of operation & causes	- hazard & risk analysis had considered all modes of operation & causes	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
Design	- operator facilities wer designed better - installation design had been different?	- additional actions were specified - actions were 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?	
Installation & Commissioning	- 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	- 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 had been carried out on modification

Fig. 2 - High-Level Flow Chart to Support Causal Analysis of E/E/PES Related Incidents Using IEC 61508 Taxonomy (HSE, 2003).

Our case study, as with many E/E/PES related incidents, stems from multiple causes. It was due to the failure to lock out the two-blade mill during the repair operation. This, in turn, was due to errors in the reprogramming of the PLC. This allowed the automatic restart of equipment under control following a power trip. There are further causes that do not relate directly to the PLC. For example, the power to the motor's circuit breakers was not locked out. No other measures were taken to prevent the equipment from becoming energized without the knowledge of the individuals working on it. In particular, the foreman was aware that the motor's circuits were not locked out while the electrician worked on the circuit breaker panel. Several requirements or lifecycle activities might have prevented this incident from occurring in the manner described. Table 2 illustrates one means of documenting the products of any flowchart analysis. 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 1 and 2. Errors in the reprogramming were due to an inadequate hazard analysis. This failed to identify the potential failure modes associated with allowing the automated restart of equipment under control following a power trip.

Table 2 - Abridged IEC 61508 Flowchart Causal Summary for the Case Study

Causal Event	**IEC 61508 Classification**	**Route through flow chart**	**Rationale**
PLC allows automatic restart of equipment following power trip	**Hazard and risk assessment**	System fails to take required action -> Failure caused by maintenance -> Hazard and risk analysis had not considered all modes of operation.	The reprogramming of the PLC allowed for a situation in which equipment was automatically restarted following a power trip. Reprogramming is likely to have prevented a restart without operator intervention had this potential hazard been recognised. (Note: if there were evidence that this hazard had been considered during the reprogramming then the causal analysis might have focussed more on validation to ensure that the PLC prevented the automated restart hazard.)
Failure to warn mechanic that power circuits not locked out during maintenance on circuit breaker.	**Operation and maintenance**	System fails to take required action -> Failure caused by maintenance -> Accident would have been avoided if maintenance procedure were improved.	On-site investigators argued that the foreman was aware of the relationship between the circuit breakers and the mill. The incident might have been avoided if they had followed a documented maintenance procedure or permission to work scheme that would have locked out all equipment affected by the maintenance on the circuit breakers.

Event & Causal Factor Analysis: Table 2 provides a relatively high-level form of causal analysis. Such techniques are appropriate for low consequence incidents. They might also be used during the initial stages of an investigation. It is unlikely that the flowcharts of Figures 1 and 2 will prove sufficient for more serious or complex incidents. The following section, therefore, presents a more sophisticated approach. It also enables investigators to map the causes of an adverse event to failures in the development lifecycle.

First Stage: Information Elicitation and ECF Modelling

The first stage in our more complex, causal analysis technique is to map out the events and conditions that led to the incident. Figure 3 uses a simplified form of the Events and Causal Factors (ECF) diagrams that were developed for the US Department of Energy (1992). 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 technique was chosen after extensive discussions with individuals involved in the development and application of the IEC61508 standard and after consultation with HSE representatives. This does not, however, imply that ECF modeling is the only technique that we might have used. Leveson (2002) has recently challenged the utility of event based modeling techniques. She has argued that greater attention should be paid to the constraints that hold between system components. For example, by focusing on the actions of the foreman we might overlook the key requirement that blade motors are not automatically restarted on power-up. Leveson's alternative techniques do, however, rely upon an initial reconstruction. The subsequent stages of her STAMP method also have much in common with the approach in this paper. Rather than focusing on the violation of development lifecycle requirements, Leveson identifies more general failures to satisfy the constraints that should hold between system components. Hence our approach focuses more on problems in the development process rather than deficiencies in the final system. This is justified because the same development processes may have been used well beyond the boundary of the particular system involved in a particular incident. A further difference stems from our insistence that the investigation technique should inform the subsequent refinement of safety-critical development standards, such as IEC 61508.

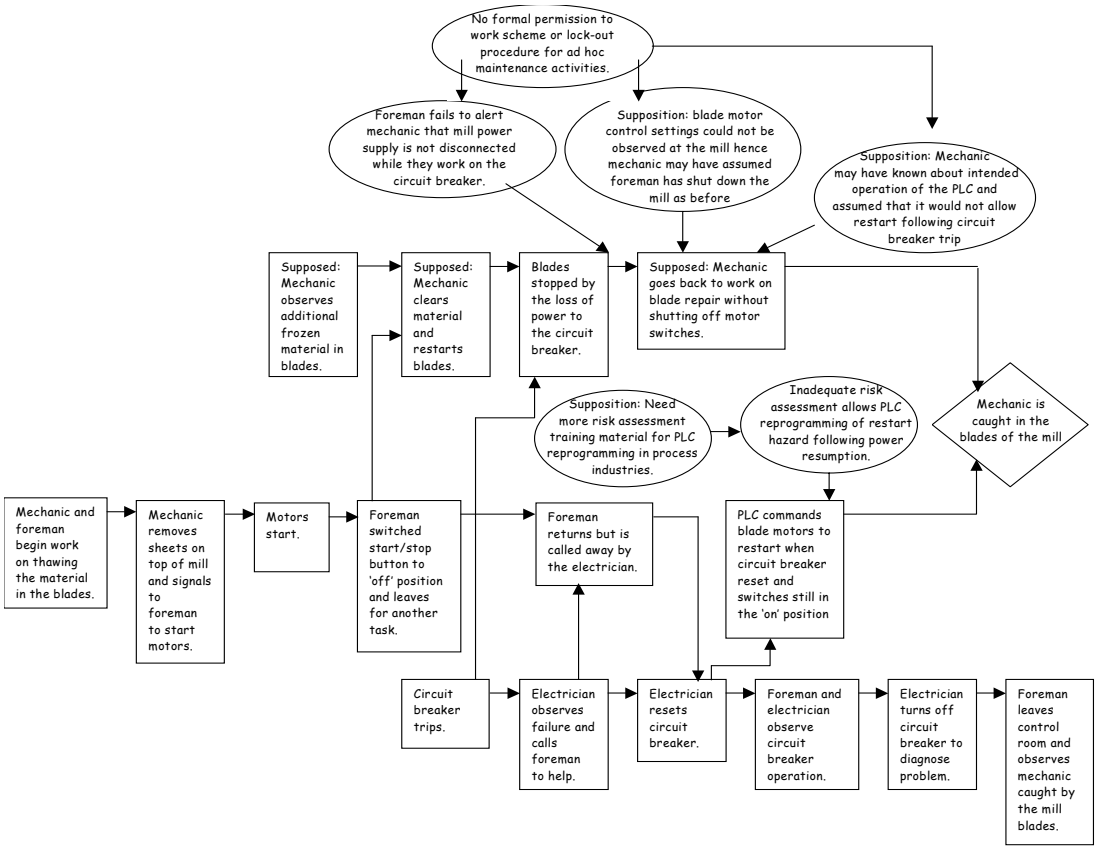


Fig. 3 - ECF Diagrams Including Developer/System Integrator Information

Figure 3 uses the ECF notation to represent the events and conditions that ultimately lead to the operation of the mill blades while the mechanic was repairing the mill. As can be seen, key events include the mechanic return to work on the blade repair without shutting off the motor

switches and the electrician's decision to reset the circuit breakers. Conditions include an 'inadequate risk assessment for maintenance procedures on the PLC update, allows restart hazard following power resumption'. The ECF chart provides a common focus for multi-party investigations. The development of this diagram continues until everyone involved in an investigation can agree that it provides a reasonable representation of the incident. If agreement cannot be reached then investigators must select one version of the diagram for further analysis. This decision to move to subsequent stages of analysis is influenced by the scope of the investigation and by pragmatics. For instance, we could extend Figure 3 to consider the circumstances that led to the PLC update. This could only be done if incident investigators can gain access to the PLC supplier.

Second Stage: Causal Reasoning

The second stage again uses a technique that is common to many investigation methods. The aim is to separate causal factors from contextual information. The analysis starts with the event immediately before the outcome. In this case, we might choose to begin with either 'PLC commands blade motors to restart when circuit breaker is reset, switches still in the 'on' position' or with the supposition that the 'Mechanic goes back to work on blade repair without shutting off motor switches'. Investigators must then 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 causal factor. For example, the incident would have been avoided if the PLC had not issued the command to restart the motors. Similarly, we can argue that the incident would have been avoided if the mechanic had not gone back to work on the mill without checking the status of the switches. The analysis proceeds backwards from these events looking at earlier and earlier events in the lead-up to the incident. If the incident would still have happened if an event had not occurred then it cannot be considered as a causal factor. For example, the incident might still have occurred even if the foreman and the electrician had not paused to observe the operation of the circuit breaker. Problems can arise from situations in which an incident occurred because something else did not happen. In this case, we must argue that the incident would have been avoided if that event had occurred. For example, can we be sure that the incident would really have been avoided if the Mechanic had switched off the motors? There may be other ways in which the accident could still have happened even if this event had taken place. These difficulties occur because counterfactual reasoning is non-truth functional. In other words, we must make an argument about what could have happened rather than what actually did take place. It can be difficult to validate such assumptions.

Investigators must then map the causal factors that have been identified from the ECF diagram to failures in the IEC 61508 lifecycle requirements that are illustrated in Table 1. One means of doing this is to identify the conditions that contributed to each causal event in the ECF chart. These conditions typically capture latent issues, including development and operation decisions that create the context for E/E/PES-related mishaps. For instance, the PLC command to restart the blade motors when the circuit breakers were reset was made more likely by the lack of adequate risk assessment during the reprogramming of the PLC. This, in turn, was arguably made more likely by the lack of sufficient training material in the conduct of such risk assessments during the maintenance of PLC's in the process industries. Similarly, the mechanic's failure to shut off the motor power was arguably more likely if they assumed that the PLC would not allow an automatic restart. It might also have been made more likely by the fact that the power settings in the control room could not be observed from the mill. The mechanic may have assumed that the foreman had switched off the power when he left to help the electrician. The mechanic's supposed actions were also probably affected by the foreman's failure to inform him that the power supply was not disconnected before he departed. All of these contributory factors were made more likely by the lack of a formal permission to work scheme of lockout procedures

for ad hoc maintenance such as that performed on the circuit breakers. Table 3 presents some of the results of mapping these causal factors back to violations in the IEC 61508 lifecycle requirements. A justification helps others to understand why investigators identified particular problems in the development or operation of the system.

The analysis of the blade mill incident illustrates a number of important points about the cause analysis of accidents involving E/E/PES. In particular, the technical causes that lead to bugs or inadequate testing often form part of more general failures in the operation, maintenance and regulation of safety-critical systems. This observation is common to all of the E/E/PES related incidents we have analyzed in applications ranging from mineral extraction through maritime command and control to the fluidized catalytic cracking of crude oil (Johnson, 2003a). This observation leads to an important requirement for the future development of our work. We have used IEC 61508 lifecycle requirements to provide a causal taxonomy for E/E/PES related incidents. This was motivated by the commercial uptake of the standard and by the organizational objectives of HSE's Electrical and Control Systems Unit. If another taxonomy were to be used in the future then it would also have to capture the range of technical, organization and managerial causes of these accidents. The case study also reveals certain weaknesses in our application of IEC 61508. We have simply used lifecycle requirements from the standard to provide a causal taxonomy for E/E/PES related incidents. The standard does not explicitly address problems in the regulatory environment; this causes particular problems in our analysis of the blade mill incident given the supposed need for greater regulatory support in risk assessment for PLC reprogramming. Similarly, the standard provides no means of identifying failures that were due to weaknesses in the standard itself. This is a significant omission. Incidents can still occur even if an organization satisfies all of the IEC 61508 lifecycle requirements. We are currently addressing these issues by extending the classification illustrated in Table 1. As mentioned in previous sections, our intention is to develop explicit means of providing feedback about these situations in which development standards fail to ensure the safety of an E/E/PES application.

Third Stage: Generating Recommendations

Investigators can use the causal summary chart illustrated in Table 3 to help identify potential recommendations. Table 4 illustrates one format that can be used to document and justify domain and incident dependent recommendations. Each potential intervention is associated with a priority assessment, with an authority responsible for implementing it and with a potential implementation timescale. The information recorded in these recommendation tables can be used to assist in the monitoring of any accident reporting system. For example, electronic information systems are increasingly being used to identify patterns between causal factors and previous recommendations (Johnson, 2003). If the same set of recommendations continues to be used to address the causal factors of similar incidents then regulators may have to intervene to find more effective remedies. It is also important to identify situations in which recommendations are consistently rejected or inadequately implemented.

Tables 3 and 4 are intended to document the process used to investigate more complex incidents. Co-workers, safety managers and regulators should be able to trace back particular recommendations through the previous stages of any causal analysis to identify the reasons why particular interventions are proposed. For example, recommendation 3 proposes the introduction of a physical interlock that might disable the blade motors when someone is working on the mill. This is based on the observation that operations and maintenance assessments had been less than adequate prior to the incident. In particular, these assessments had failed to predict the impact that the PLC reprogramming would have on the motor restart following a power interruption.

Table 3 - IEC 61508 Causal Summary Chart for Case Study Incident

Causal Event	**Associated Conditions**	**IEC 61508 Lifecycle Classification**	**Justification**	**IEC 61508 Common Requirements Violation**	**Justification**
Supposed: Mechanic goes back to work on blade repair without shutting off motor switches.	Supposition: Mechanic may have known about intended operation of the PLC and assumed that it would not allow restart following circuit breaker trip	**Operation and Maintenance:** 4. operations procedures not assessed.	If the mechanic had assumed that the PLC would prevent any automatic restart of the motors following a circuit breaker trip then he was relying on a safety net for a 'normal maintenance procedure'. Hence those procedures should be reassessed.	**Functional Safety Assessment:** 1. LTA operations and maintenance assessment 2. Modification assessment LTA.	The incident may be symptomatic of other problems in operations and maintenance assessment not just in the mill clearing and repair procedures. Similarly, there may be other problems with the assessment of modifications beyond the PLC reprogramming. Deeper questions may have to be raised about the procedures and techniques used to assess functional safety across the plant.
	Supposition: blade motor control settings could not be observed at the mill hence mechanic may have assumed foreman has shut down the mill as before	**Installation and maintenance:** 4. installation design	The layout of the motor controls in the control room prevented the mechanic from easily checking that the foreman had switched them off before leaving to help the electrician. Warning lights could have been located close to the mill to indicate the status of the motor switches.		
	Foreman fails to alert mechanic that mill power supply is not disconnected while they work on the circuit breaker.	**Operation and Maintenance**: 2. permit/hand over procedures need improvement 3. maintenance procedures not impact assessed.	If handover procedures had been in place then the foreman might have informed the mechanic about his intentions on leaving to help the electrician. This should have explicitly addressed the implications of the work on the circuit breaker and on shut-down procedures during any further mill repairs.	**Safety Management:** 1. LTA safety culture 2. LTA safety audits	The hand-over procedure between the foreman, mechanic and also the electrician may be symptomatic of deeper problems with safety management in a small to medium sized enterprise. A safety audit should raise awareness of potential hazards and the safety implications of apparently routine maintenance operations.
	No formal permission to work scheme or lockout procedure for ad hoc maintenance activities.				
PLC commands blade motors to restart when circuit breaker reset and switches still in the 'on' position	Supposition: Need more risk assessment training material for PLC reprogramming in process industries.	**Modification:** 2. LTA manufacturers information. 4. LTA verification and validation.	The company responsible for the PLC update arguably did not appreciate the need to formally consider the implications of the changes on the operation of the mill. Hence the potential restart hazard was not adequately tested for.	**Safety Management:** 3. LTA management of suppliers **Documentation:** 2. documentation incomplete	The reprogramming of the PLC does not seem to have been supported by a detailed consequence assessment. Again, additional documentation may be required from regulatory organisations to guide E/E/PES suppliers about the best means of performing such a hazard assessment. The operators of the mill might also use such guidance to validate any maintenance activities by suppliers.
	Inadequate risk assessment allows PLC reprogramming of restart hazard following power resumption	**Haxzard and Risk assessment:** 1. Consequence and likelihood estimation **Modification:** 1. impact analysis incorrect			

Table 4 - Recommendation Summary Form (LTA – Less Than Adequate)

Causal Event	Associated Conditions	IEC 61508 Lifecycle Classification	IEC 61508 Common Requirements Violation	Recommendation	Priority	Responsible authority	Deadline for response	Date Accepted/ Rejected
Supposed: Mechanic goes back to work on blade repair without shutting off motor switches.	Supposition: Mechanic may have known about intended operation of the PLC and assumed that it would not allow restart following circuit breaker trip	**Operation and Maintenance:** 4. operations procedures not assessed.	**Functional Safety Assessment:** 1. LTA operations and maintenance assessment 2. Modification assessment LTA.	1. Review operations and maintenance procedures to avoid routine reliance on safety net features.	High	Plant safety manager	1/4/2003	Accepted 15/2/2003
	Supposition: blade motor control settings could not be observed at the mill hence mechanic may have assumed foreman has shut down the mill as before	**Installation and maintenance:** 4. installation design		2. Review design of control room to provide operators with control information on mill and associated plant.	Medium	Plant safety manager	1/6/2003	
				3. Consider adding interlock on mill access platform.	High	Plant safety manager	1/6/2003	
	Foreman fails to alert mechanic that mill power supply is not disconnected while they work on the circuit breaker.	**Operation and Maintenance**: 2. permit/hand over procedures need improvement 3. maintenance procedures not impact assessed.	**Safety Management:** 1. LTA safety culture 2. LTA safety audits	4. Introduce and document a formal permit to work scheme for all repair activities.	High	Plant safety manager	1/4/2003	Accepted 15/2/2003
	No formal permission to work scheme or lockout procedure for ad hoc maintenance activities.			5. Develop handover procedures when repair tasks interrupted	High	Plant safety manager	1/4/2003	
PLC commands blade motors to restart when circuit breaker reset and switches still in the 'on' position	Supposition: Need more risk assessment training material for PLC reprogramming in process industries.	**Modification:** 2. LTA manufacturers information. 4. LTA verification and validation.	**Safety Management:** 3. LTA management of suppliers **Documentation:** 2. documentation incomplete	6. Develop training material for E/E/PES suppliers and for operators on necessary hazard identification during PLC reprogramming.	Medium	Industry Regulator	1/9/2003	
	Inadequate risk assessment allows PLC reprogramming of restart hazard following power resumption	**Haxzard and Risk assessment:** 1. Consequence & likelihood estimation **Modification:** 1. impact analysis incorrect		7. Conduct formal hazard identification process to determine if there are any additional threats posed by reprogramming of PLC on this plant and supplier's other installations.	High	PLC Supplier Safety Manager	1/6/2003	Accepted 15/2/2003

Conclusions

As mentioned, the UK Management of Health and Safety at Work Regulations 1999 (HSE, 1999) require every employer to carry out a risk assessment, introduce the necessary preventive and protective measures, and monitor these measures. The associated approved code of practice explains that this monitoring includes an obligation to '*adequately investigating the immediate and underlying causes of incidents and accidents to ensure that remedial action is taken, lessons are learnt and longer term objectives are introduced'*. Unfortunately, there are few recognized techniques that companies might use to analyze E/E/PES related incidents. This paper, therefore, introduces two different approaches for this class of adverse events. The first builds on a simple flowchart that helps investigators identify the causes of a mishap by answering a series of questions. These questions guide the causal analysis to identify underlying problems in the design, development or operation of E/E/PES hardware and software. Each failure identified by the flowchart can be related back to lifecycle requirements within the IEC 61508 standard.

We have also described an extended investigation technique that is appropriate for more complex or more critical incidents. Additional stages are introduced to provide intermediate documentation during the causal analysis. Investigators can use these documents to justify recommendations to their peers, to safety managers and to courts of law. This second approach relies upon reconstructions using a simplified form of the US Department of Energy's Events and Causal Factors (ECF) charting. The resulting ECF diagrams help to distinguish contextual information from causal factors. Each causal factors is then analyzed to identify potential failures in the IEC 61508 lifecycle. This is done using a checklist, illustrated in Table 1.

Our use of IEC 61508 is justified because it provides a means of feeding the insights derived from any incident investigation back into the future maintenance and development of hardware and software 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. HSE aim to incorporate this work in published guidance material.

Acknowledgements

Thanks are due to Bill Black (Black Safe Consulting) and Peter Bishop (Adelard) for providing comments on the initial draft of this document.

References

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.

HSE (1999), *Management of health and safety at work* Approved Code of Practice L21 HSE Books.

HSE (2003), P.G. Bishop, R.E. Bloomfield, L.O. Emmet, C.W. Johnson, W. Black, V. Hamilton and F. Koorneef, Learning from incidents: Outline scheme for E/E/PE safety-related systems, HSE Contract Research Report, Available at http://www.hse.gov.uk/research/crr_htm/index.htm

International Electrotechnical Commission (2000), IEC 61508 Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems.

International Electrotechnical Commission (2003), *IEC Functional Safety Zone*, http://www.iec.ch/functionalsafety.

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

C.W. Johnson (2003a), Incident Reporting and Analysis for Electrical, Electronic and Programmable Electronic Systems (E/E/PES) under IEC61508. See http://www.dcs.gla.ac.uk/~johnson/hse

C.W. Johnson, G. Le Galo and M. Blaize, (2000), Guidelines for the Development of Occurrence Reporting Systems in European Air Traffic Control, European Organisation for Air Traffic Control (EUROCONTROL), Brussels, Belgium.

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, (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.