# A Brief Overview of Causal Analysis Techniques for Electrical, Electronic or Programmable, Electronic Systems



**Executive Summary:** This overview provides a brief summary of causal analysis techniques that can be used to analyse mishaps involving Electrical, Electronic or Programmable, Electronic Systems (E/E/PES). The intention is not to provide a complete introduction. Detailed guidance on each technique is available for the references at the end of this document.

## 1. Introduction

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

| Hazard | Root Cause of the Hazard | Proposed remedial action | Responsible Authority |
|---|---|---|---|
| Hazard 1 | Root Causes | Remedial Actions | Person or team to sign-off |
| Hazard 2 | Root Causes | Remedial Actions | Person or team to sign-off |

**Table 1:** The Results of an Incident Investigation

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

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

### 1.2 Case Study Incidents

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

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

operation before the list threatened the integrity of their vessel. The following pages focus on the E/E/PES related causes of this incident.

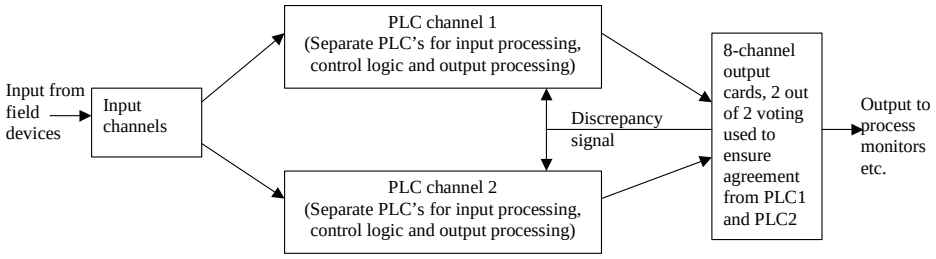


**Figure 1:** High-level architecture for the E/E/PES Case Study

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

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

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

It is important to observe that both the suppliers and the operators involved in the incidents that form this case study were entirely unaware of the particular failure modes before they occurred. It is also important

to emphasise that the case study cannot be characterised as software or a hardware failure. It stemmed from complex interactions between a number of system components.

## 2. Causal Analysis Techniques

Many organisations publish detailed guidance on causal analysis techniques. For example, NASA's procedures and guidance on mishap investigation advocates several different approaches (NASA NPG 8621.1). These include checklists that can be used to ensure that investigators consider a broad range of possible causal factors. They also include more open-ended approaches that do not rely on enumerations of previous problems. As we shall see, the costs associated with some of these approaches imply that the selection of appropriate techniques may depend on the resources of the organisation conducting the analysis and the perceived severity or 'plausible worst case' consequences of the incident under investigation.

### 2.1 Elicitation and Analysis Techniques

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

#### *2.1.1 Barrier Analysis*

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

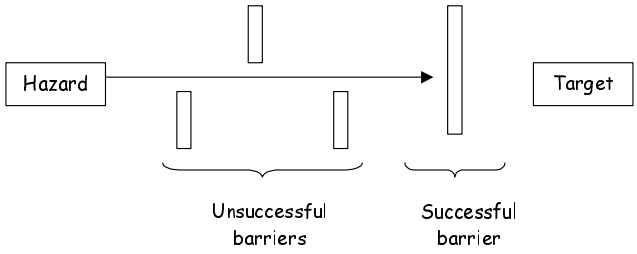


**Figure 2**: Targets, Hazards and Barriers

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

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

**Table 2:** Hazard and Target Identification

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

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

**Table 3:** More Detailed Barrier Analysis

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

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

*2.1.2 Change Analysis*

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

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

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

**Table 4:** Change Analysis

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

### 2.2 Event-Based Techniques

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

#### *2.2.1 Timelines*

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

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

**Table 5:** Example Summary from Automated Alarm Log

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

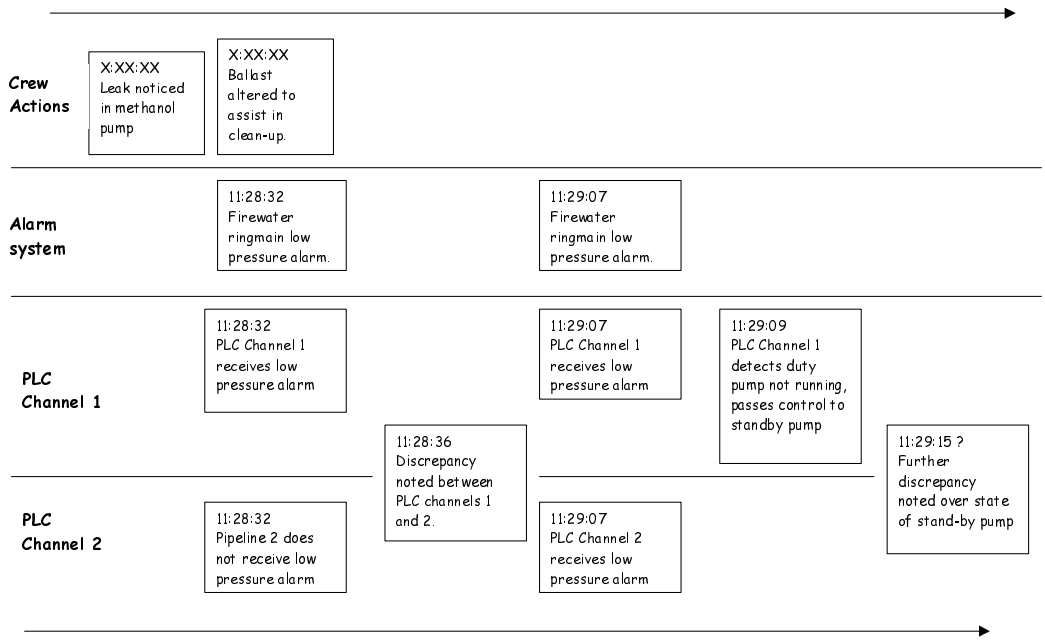


**Figure 3:** High-level Timeline of the Case Study Incident

Figure 3 uses a technique for the development of time-lines that was pioneered by groups within the US National Transportation Safety Board (Johnson, 2002). The idea is to place events on a horizontal time-line but to group them according to the agents involved. In this case, the events relating to the two PLC channels are separated from the actions of the crew and so on. In practice, initial forms of this representation are often produced by sticking notes onto a blank piece of paper. Such structuring

mechanisms are important if analysts are not to be overwhelmed by the mass of detail that can be obtained in the aftermath of an adverse event. There are a number of problems with the use of time-lines in the reconstruction and causal analysis of E/E/PES related incidents. Firstly, it can be difficult to obtain exact timings for asynchronous systems that lack a global clock. Hence there will often be inconsistencies and contradictory evidence for exact timings. Similarly, as in Figure 3, there may be events where it is impossible to obtain an exact timing. This is the case for some of the crew actions that cannot be timed to the same granularity as the low-level alarms illustrated in the previous table. Such detailed criticisms have persuaded many analysts to identify alternate event-based representations that can be used to analyze adverse events at a more abstract level. The intention is not to model every detailed event that occurred but to sketch critical causal relationships between a lesser number of more important events.

*2.2.2 Accident Fault Trees*

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

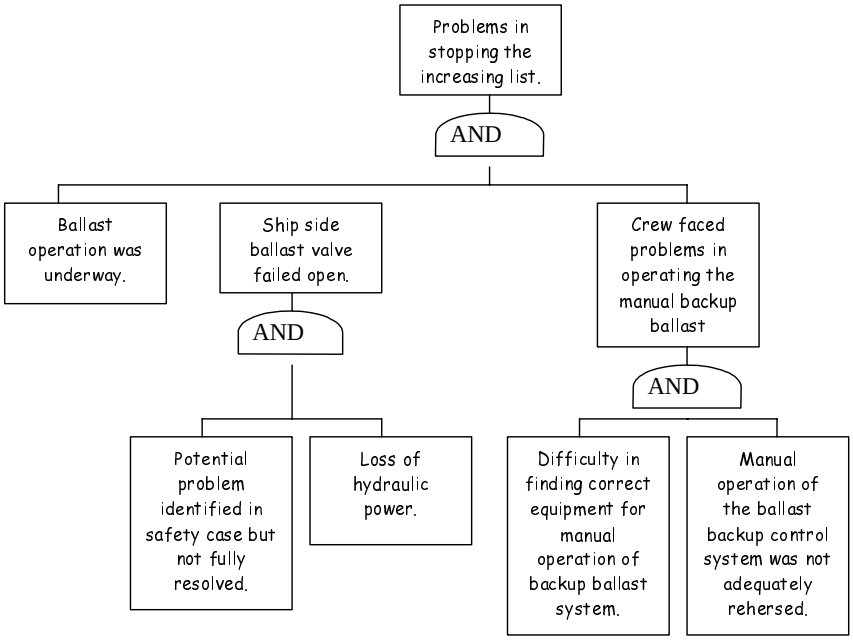


**Figure 4:** Overview of an Accident Fault Tree

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

There are further differences between accident fault trees and the use of this technique for design. For example, it is unclear how to represent the events that occur in the immediate aftermath of a mishap. This

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

*2.2.3 Failure Event Tree, ECF Charts, MES and STEP*

The previous paragraphs described the numerous differences that exist between conventional applications of fault tree techniques and their use in the causal analysis of incidents and accidents. These differences have led a number of researchers to develop alternative techniques that are specifically designed to support both the reconstruction and the causal analysis of mishaps. There are strong similarities between techniques such as Events and Causal Factors charting (ECF), Multilinear Events Sequencing (MES) and Sequential Timed Event Plotting (STEP). Brevity prevents a detailed analysis of each of these approaches; the interested reader is directed to Johnson (2003) and US Department of Energy (1992).

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

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

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

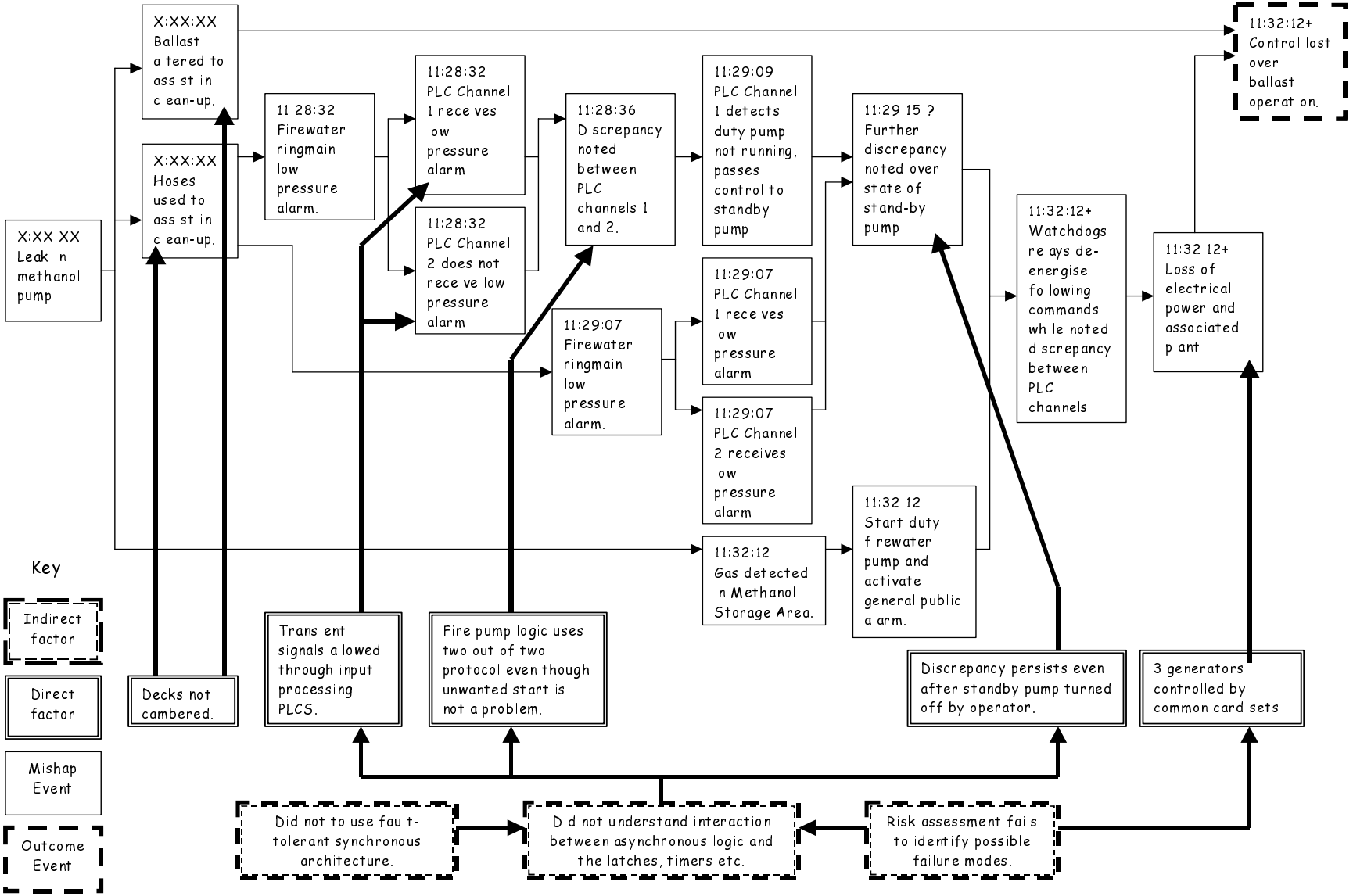


**Figure 5:** A Failure Event Tree

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

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

**2.3 Flow Charts and Taxonomies**

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

*2.3.1 MORT*

Management Oversight and Risk Trees (MORT) provide arguably the best-known example of a flow

charting approach to the identification of causal factors (W. Johnson, 1980). As the name suggests, it is well suited for the identification of organizational issues leading to mishaps. It is less suited to the technical analysis of computer-related incidents; however, it could be extended to address this potential weakness. At the heart of MORT is a tree structure that resembles the Fault Tree shown in Figure 4. Figure 6 provides an abbreviated version of a MORT diagram. The analysis begins when investigators consider the top levels of the tree. They must ask themselves whether the mishap was the result of an omission of some management function and whether the incident occurred from a risk that had already been recognized. In the tree, the term LTA refers to a 'less than adequate' performance of some necessary activity. If there was an oversight problem then analysis progresses to the next level of the tree. Investigators are encouraged to consider both what happened and why it happened. The reasons why an oversight might occur include less than adequate management policy, implementation or risk assessment. The analysis progresses in this manner under investigators reach a number of terminal nodes, not shown here, that describe the more detailed causes of the incident.

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

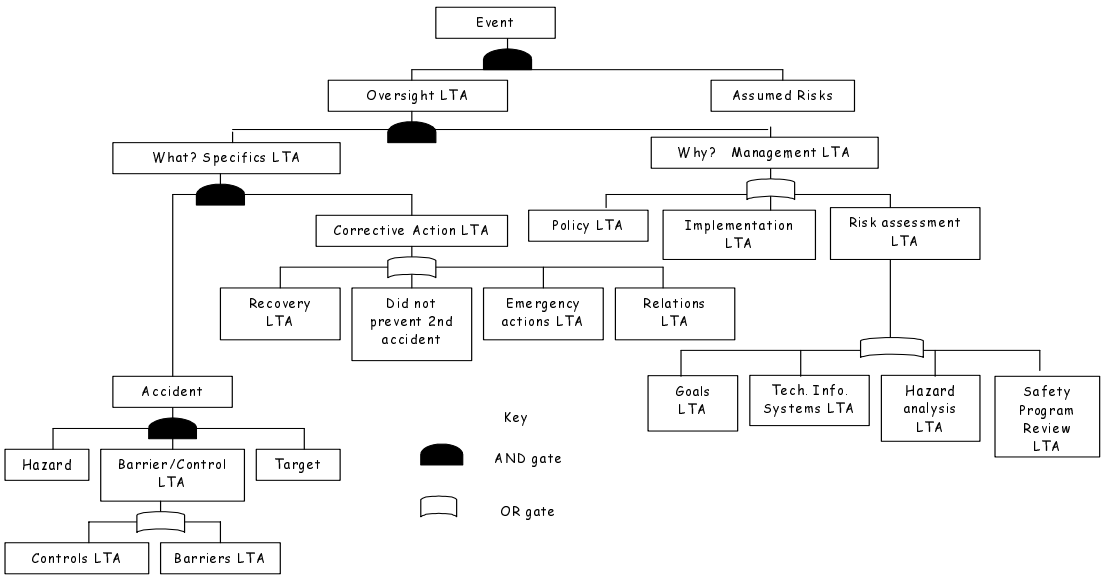


**Figure 6:** Abbreviated form of a MORT diagram

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

| Branch in Mort Tree | Node of MORT Tree | Incident description |
|---|---|---|
| Risk Assessment Less Than Adequate | Hazard | Loss of control of key functions during emergency shutdown. |
| | Target | Production system, operators, the environment... |
| Hazard Analysis Less Than Adequate | Control Operability Problems | Control of power generators vulnerable to trips on PLC channels. |

**Table 6:** Documenting the Products of a MORT Analysis

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

*2.3.2 PRISMA*

PRISMA is a multi-stage technique. It includes an initial reconstruction based on an accident fault tree (van der Schaaf, 1992, 1996). The leaf or terminal nodes on the tree are then classified to identify more generic root causes. This is important because the complex differences that exist between individual incidents can often make it difficult to compare the causes of several apparently related incidents. A flow chart can, therefore, be used to provide a higher-level classification of these more detailed causes. For example, an operand error might be classified at one level as a problem with type checking. At a higher-level it might be classified as a coding error rather than a problem in requirements and so on. These higher-level categories can be used to inform the statistical monitoring of incident data and can also arguably increase consistency. Investigators may disagree about the detailed causes of an adverse event but may exhibit greater agreement about the higher-level classification.

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

between hundreds of complex categories. Conversely, if the flow chart is too general then it may yield relatively little insights into common engineering problems in E/E/PES applications.

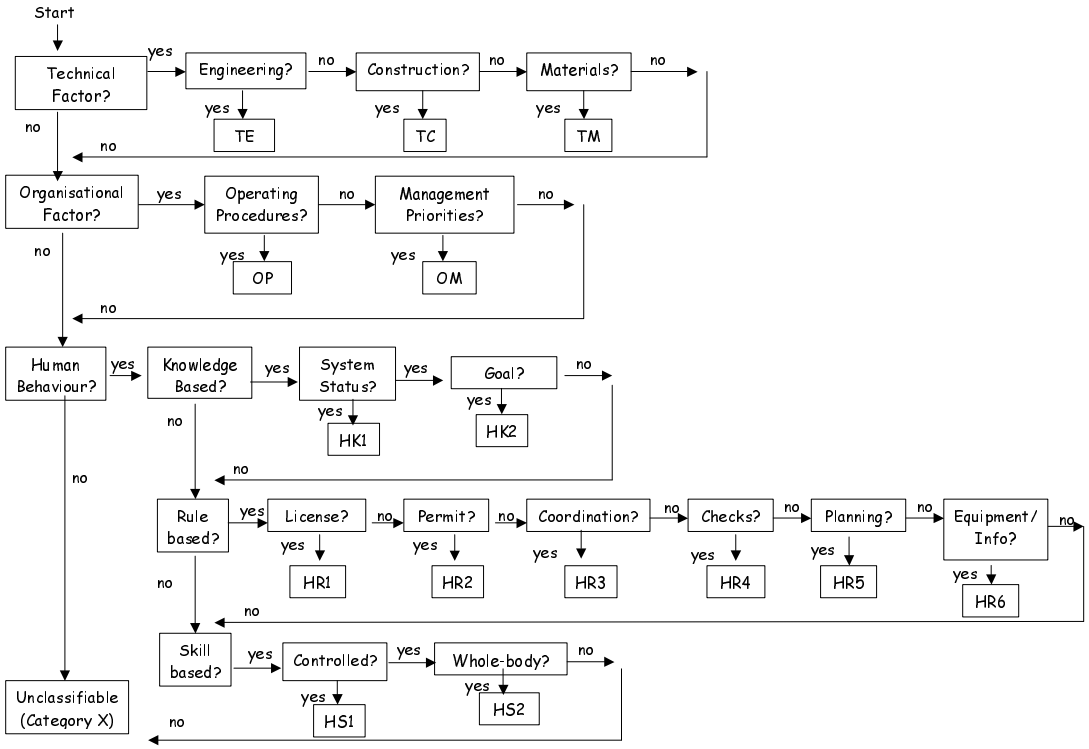


**Figure 7:** PRISMA Flow Chart (van der Schaaf, 1992, 1996)

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

**Table 7:** Example PRISMA Classification/Action Matrix Van Vuuren (1998)

Causal analysis is not an end in itself. It is obviously important that recommendations be derived from the findings of an investigation so that previous problems can be avoided in the future. An important strength of flow-chart methods such as PRISMA is that the generic causal classification that is used in the analysis of an adverse event can also be used to direct investigators towards a number of general solutions. For example, Table 7 illustrates a classification action matrix. This shows that if, for example, an incident were due to problems with management priorities then subsequent recommendations might focus more on 'bottom-up communication'. As might be expected, this approach is intended to ensure that investigators offer a common response to incidents with similar causal factors. If incidents continue to recur with the same set of causal factors then safety managers might decide that the remedies advocated in Table 7 are

ineffective and should be revised. In particular, it might be argued that the remedial actions should be at a far finer level of detail. In our case study, it might be advocated that modifications be made to eliminate transient inputs. For instance, the input processors in each PLC channel might ensure that such short-lived signals are sustained until the processing PLCs are sure to receive them. Such a detailed remedial action could only be represented in a classification/action matrix if the associated flow chart were extended to a similar level of complexity. It would need to consider transient signals as a potential cause of technical failure. As the sophistication of the flow-chart increases, so does the extent of the classification/action matrix unless common interventions can be identified for classes of causal factors.

**2.4 Accident Models**

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

*2.4.1 TRIPOD*

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

Tripod also provides a form of graphical modelling that can be used to show how specific instances of these general failure types combine to create both necessary and sufficient causes for an incident or accident. This diagrammatical technique is illustrated in Figure 8. As can be seen, elements of barrier analysis are again used to illustrate the manner in which a hazard can affect a target. A number of active failures can be associated with each of the defences that did not protect the target. These active failures can be thought of as the immediate events leading to the incident. The context in which they can occur is often created by a number of preconditions. For instance, one active failure stemmed from the way in which a low consequence discrepancy over the command to start the feed water pump jeopardised more critical responses to the gas detection event. The precondition for this failure was the manner in which only one of the input cards on the two PLC channels detected the pump pressure warning. This, in turn, stemmed from a latent failure to design input cards that would ensure the adequate replication of transient signals until both channels were sure of recognising them. As with flow chart techniques the intention is to move away from the specific events that led to a mishap so that greater attention is paid to the generic or systemic failures that are likely to threaten future operation. It is argued that a specific recurrence of an incident, such our case study, is unlikely. However, the same problems of hidden failure modes in combinations of asynchronous and latched systems may manifest themselves in a host of future incidents unless these latent causes are addressed.

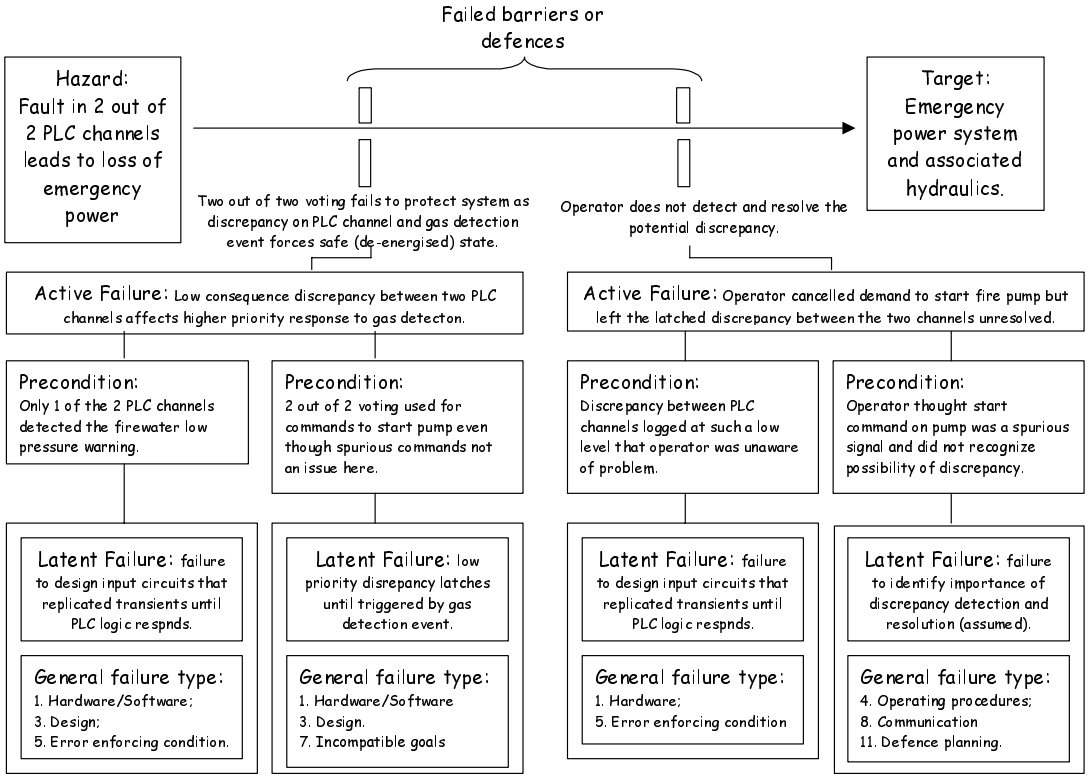


**Figure 8:** Example Application of a TRIPOD General Failure Types

As mentioned, TRIPOD embodies a model of how accidents and incidents occur. This model builds on barrier analysis and includes concepts such as general failure types, latent causes, preconditions and active failures. A range of computer-based tools also supports it, further details are provided in Doran and van der Graaf (1996) or Hudson, Reason, Wagenaar, Bentley, Primrose and Visser (1994). The meta-level point here is that the costs associated with each of the techniques described in this document can be substantially reduced by appropriate tool support. It is also possible to automatically perform certain consistency checks and search tasks for similar previous incidents using these tools (Johnson, 2003).

*2.4.2 STAMP*

Leveson's Systems Theory Accident Modeling and Process (STAMP) approach is similar to accident fault trees in that it attempts to apply a more general, constructive engineering tool to support the analysis of incidents and accidents. Instead of extending the use of fault trees, STAMP exploits elements of control theory to help identify causal factors. This is motivated by the observation that mishaps occur when external disturbances are inadequately controlled. Adverse events can also arise when the failure of process components goes undetected or when the actuators that might respond to such a failure are unsuccessful in their attempts to control any adverse consequences from the initial fault. Control failures can arise from 'dysfunctional interactions' between system components. For example, if one subsystem embodies inappropriate assumptions about the performance characteristics of another process component. In this view, mishaps do not stem from events but from inappropriate or inadequate constraints on the interactions among the elements that form complex, safety-critical applications. Safety is viewed as a dynamic property of the system because the constraints that are applied and the degree to which a system satisfies those constraints will continually evolve over time. The analysis progresses by developing a control model of the relationships between entities in the system. Figure 9 illustrates this approach. It is important to emphasize that this diagram uses arrows to represent communication and control flows. The

rectangles are entities, including people, systems and organizations; they do not represent the events shown in the Failure Event Tree of Figure 5.

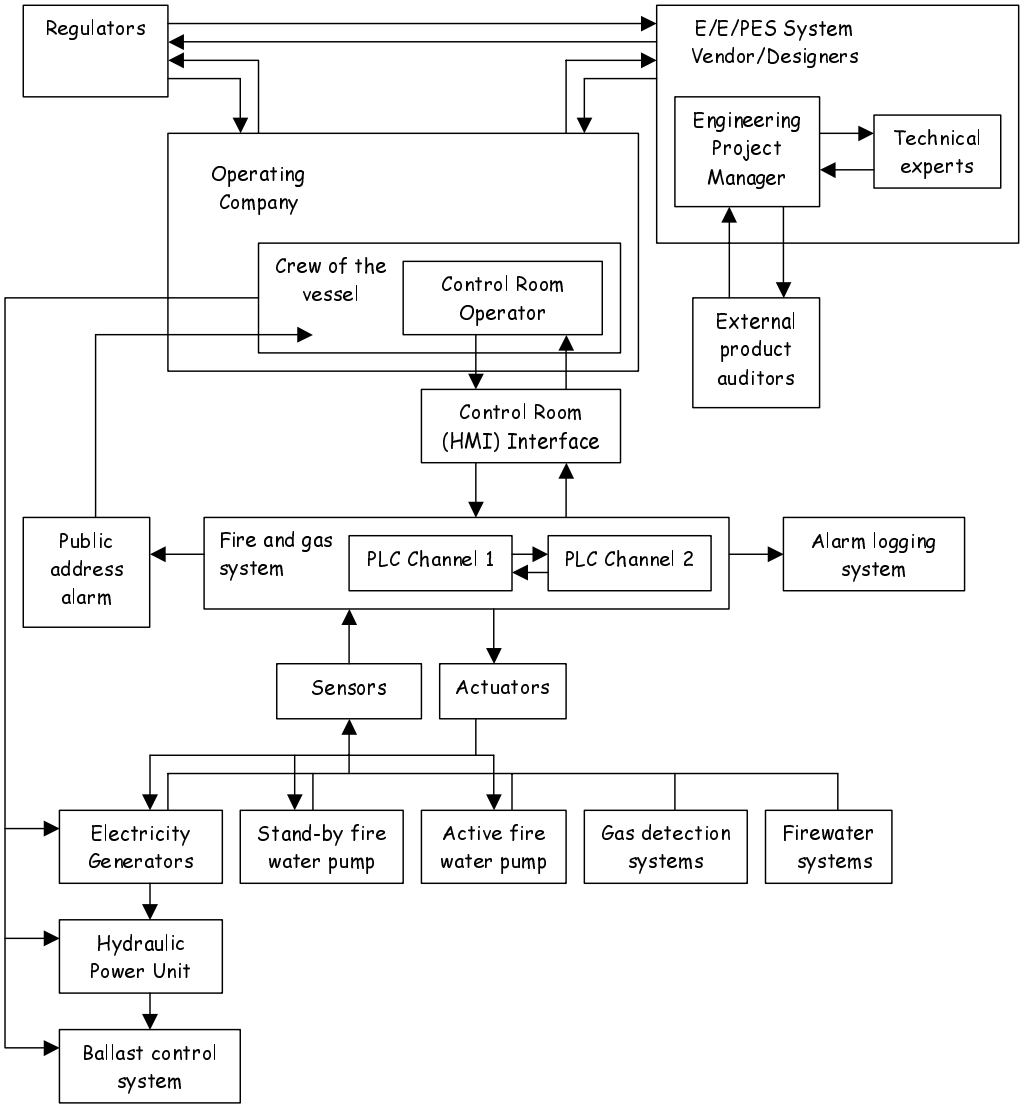


**Figure 9**: Example Control Model from STAMP

As can be seen from Figure 9, the STAMP control analysis extends from the operator, and the systems under their immediate control to also consider the relationships between project and company management, between management and regulatory agencies and between regulation and system vendors. These different forms of interaction include the preparation, presentation and acceptance of the safety case that originally covered the design and then the operation of the application as a whole. These different relationships must be captured in any analysis because they have a profound influence on both the development and operation of safety-critical systems. The control model also considers interactions between system components. For instance, Figure 9 traces the way in which the control room operator monitors and issues commands through their human-machine interface. This controls the fire and gas systems that included the PLC channels mentioned in previous sections. These PLC channels, in turn, interfaces with the sensors that detected the presence of gas and the falling water pressure. The output from the fire and gas system can also affect the operation of the generators and, through them, could affect the hydraulics and the ballast system. After having conducted this extended form of control analysis, the

STAMP technique progresses by considering each of the control loops that are identified in the 'socio-technical system'. Potential mishaps stem from missing or inadequate constraints on processes or from the inadequate enforcement of a constraint that contributed to its violation. Table 8 illustrates the general classification scheme that guides this form of analysis. It provides a classification scheme that helps to identify potential causal factors in the control loops that exist at different levels of the management and operation hierarchy characterized using diagrams similar to that shown in Figure 9.

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

**2 Inadequate Execution of Control Action**
- 2.1 Communication flaw
- 2.2 Inadequate actuator operation
- 2.3 Time lag

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

**Table 8:** Control Flaws leading to Hazards (Leveson, 2002)

Analysis progresses by examining each of the arrows in the control model to see whether any of the flaws in Table 8 can be identified in the relationships that they represent. It might be argued that there were unidentified hazards in the control loop between the PLC channels and the generators. Similarly, subsequent investigation might identify flaws in the creation process that led to the human-machine interface design's representation of the sate of the fire and gas system. It is important to note that the inclusion of control flaws 2.3 'time lag', 1.2.2 'Time lags and measurement inaccuracies not accounted for' and 3.4 'Inadequate sensor operation (incorrect or no information provided' illustrate the control theory roots of this technique. These control flaws also demonstrate the suitability of the STAMP technique for our E/E/PES case study.

Table 8 illustrates the high-level similarities between STAMP and previous techniques such as PRISMA and even MORT. All of these approaches rely upon taxonomies of general causal factors. These lists of potential problems help investigators to focus their analysis and can also ensure consistency. It is important to emphasize that STAMP is a relatively new technique. However, there are already a number of case studies in which this approach has been applied to support the analysis of E/E/PES related incidents. These are, however, focused on high-consequence mishaps given the potential overheads that stem from the development of detailed reconstructions and control models.

**2.5 Argumentation Techniques**

Previous approaches have focussed on the identification of causal factors by the modelling of adverse events or of control relationships. Investigators are then expected to exploit a range of informal arguments to identify the root causes that are represented in these models or diagrams. This informal reasoning often

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

*2.5.1 WBA*

Ladkin and Loer's (1998) Why-Because Analysis begins by a reconstruction phase during which a graphical notation constructs sequences of events leading to a mishap. The angled arrows shown in Figure 10 illustrate this. As can be seen, the leak in the methanol plant occurs before the ballast is altered to assist in the clean up operation and before the hoses were used. It is important to stress, however, that this sequential information does not imply causation. We cannot in this early stage of the analysis say that leak necessarily caused the change in ballast. In order to make this argument we must demonstrate that we have identified sufficient causes for an 'effect' to occur. For example, they may have been other factoirs including previous operational experience in successfully following this approach that justified its use by the crew. A more sustained causal analysis must consider these additional issues in order to fully explain the reasons why the ballast was altered in the lead up to the incident.

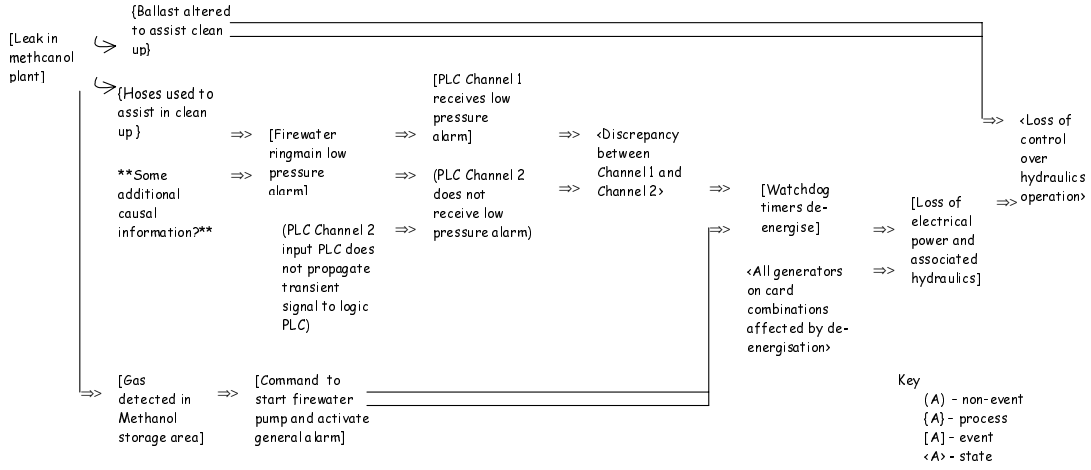


**Figure 10:** Example WBA Diagram

Once analysts are convinced that they have considered a sufficient set of causal factors for an effect they can then revise the WBA diagram illustrated in Figure 10. A double arrow denotes causal relationships =>>. As can be seen, the leak in the methanol plant was a sufficient cause for gas to be detected in the storage area. No further explanation need be considered at this stage. However, if we look at the causes for the low-pressure alarm on the ring main then we can see that the use of the hoses in the clean-up operation may provide an insufficient explanation. Further analysis is required to determine exactly why such a routine cleaning procedure resulted in a warning when fire fighting activities might require a greater volume of water than was needed in this clean-up operation. Informally, the analysis proceeds by examining each node in the diagram to create statements of the form `Why did A occur, because of B and C and D…'. This transition from temporal sequences to more rigid causal relationships can produce insights that are not apparent in purely event based approaches, such as timelines. For example, in order to explain why power was lost following the intervention of the watchdog timers we must understand the way in which the generators were controlled by the same card combinations that were used by the gas and fire

system. This is explicitly represented in the WBA diagram of Figure 10 but was not previously included in the event-driven approach of Figure 5's Failure-Event tree.

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

*2.5.2 CAE Diagrams*

The ultimate aim of any causal analysis is to trace the recommendations that might be made in response to an adverse event or near miss. Table 9 illustrates the general format of a recommendation table. These provide a simple means of linking the products of a causal analysis to the recommendations that are intended to avoid any recurrence and also to the evidence that justifies any potential intervention. For instance, a recommendation to make temporary modifications to eliminate transient input signals to the PLC channel is supported by the argument that such a condition triggered the case study. There is evidence to support this argument from the logs and from simulator reconstructions. It can, however, be difficult to construct such tables for complex incidents. There may be many hundreds of items of evidence in complex failures. Similarly, can be competing arguments that undermine particular recommendations. For instance, any decision to introduce a temporary fix may introduce further failure modes. It might, therefore, be better to operate the existing system until a full re-design can be completed.

| Conclusion/Recommendation | Root Cause (Analysis) | Supporting Evidence |
|---|---|---|
| C1. Temporary modification to eliminate transient signals. | A1.1 input discrepancy between PLC channels 1 and 2 created necessary precondition for incident. | E1.1 Fire and gas system logs (see table 5).<br><br>E1.2 Simulations run by supplier after the incident. |
| C2. Replace tools to operate ballast system using manual backups. | A2.1 Incorrect tool used to operate solenoid valves on ballast backup. | E2.1 Witnerss statements.<br><br>E2.2 Deficiencies in the existing procedures and manuals covering ballast related mishaps.<br><br>E2.3 Definciencies in the existing safety case and hazard assessment documents. |

**Table 9:** General Format for a Recommendation Table

Conclusion, Analysis and Evidence (CAE) diagrams can help designers to map out the competing arguments for and against particular conclusions or recommendations in the aftermath of a complex incident. These diagrams are simpler than many of the techniques we have described (Johnson, 2002). This approach lacks the consistency and completeness checks that are provided by the formal reasoning in the WBA technique. However, the reliance on a graphical formalism together with less strict rules on how to conduct the analysis can arguably reduce the costs and increase the flexibility of this approach. In consequence, although these techniques stem from similar motivations they offer different degrees of support depending on the resources of time, expertise and money that are available to an investigation.

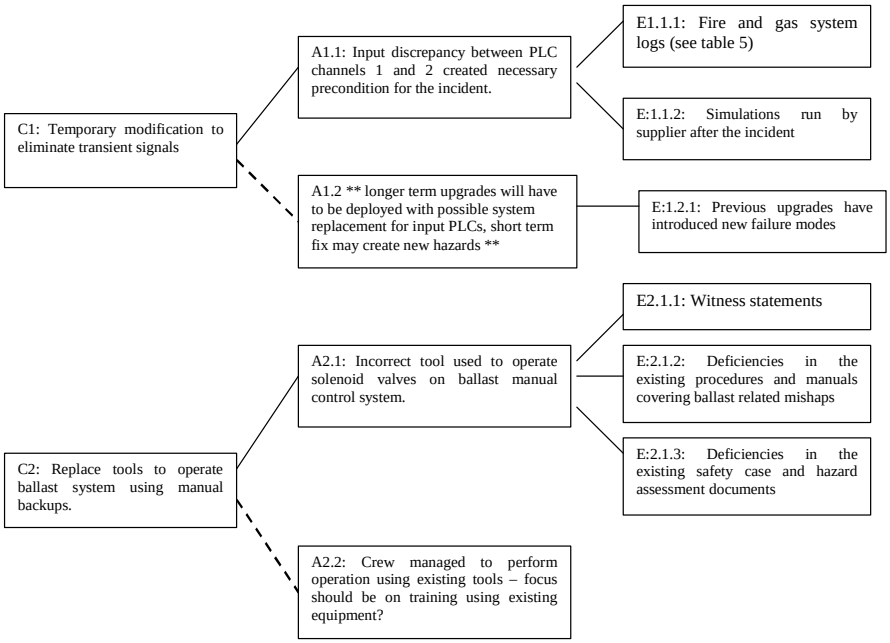


**Figure 11:** Example of a CAE Diagram

Figure 11 provides an example of a CAE diagram. As can be seen, rectangles are connected to form a network that summaries arguments about an incident or accident. As the CAE name suggests, the rectangles labeled with a C are used to denote conclusions or recommendations, those labeled with an A are lines of analysis while the E rectangles denote evidence. Lines are drawn to show those lines of analysis that support particular conclusions. For example, the recommendation to introduce temporary modifications (C.1) is supported by the argument that this would address the input discrepancy noted for PLC channels 1 and 2 (A1.1). The evidence for this assertion is provided by the fire and gas alarm system logs (E.1.1.1) and by simulations (E.1.1.2). It is important to note that Figure 11 also captures contradictory arguiments. For instance, the dotted line in the first of the networks denotes that the temporary fix recommended in C.1 is not supported by the argument that a longer term upgrade will have to be made (A.1.2) and that previous temporary fixes provide evidence of the danger of such short-term measures (E1.2.1).

The lower of the two networks in Figure 11 illustrates the argument that tools need to be replaced to help the crew operate the ballast system using the manual backup controls (C2). This recommendation is based on the observation that incorrect tools were used during the incident to operate the solenoids and that this hindered the crews' intervention (A2.1). This argument is based on evidence of witness statements (E.2.1.1), on deficiencies in the manuals (E.2.1.2) and the safety-case which fails to consider the potential problems in operating this defence mechanism (E2.1.3). The recommendation to introduce new tools is weakened by an argument that the crew managed to intervene eventually with existing resources and that the introduction of new tools should not take the focus away from revised training procedures to guide any

response to such an incident in the future. As can be seen from Figure 11, CAE diagrams capture general arguments about incidents and accidents. For example, a conclusion might refer to a recommended action, it need not simply capture a causal relationship. It is also important to mention that this technique was specifically developed to enable investigators to sketch out the arguments that might appear in an incident report. This helps to ensure that any document avoids contradictory arguments.

**3. Conclusions**

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

This paper has presented a limited selection of causal analysis techniques. For instance, we have not considered stochastic modelling or formal, mathematically based approaches (Johnson , 2003). The selection of particular techniques has been based narrowly on pragmatic concerns, including the degree of previous commercial uptake and the number of previous case studies in E/E/PES related systems. It is also important to stress that this review reflects the subjective opinions of the author. Much work remains to be done to validate particular views, for example about the degree to which a technique supports the consistent causal analysis of adverse events. The intention has, however, been to provide a basic road map for the range of approaches that might be used to analyse the causes of E/E/PES related incidents.

**References**


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

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.

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

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

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

C.W. Johnson and A.J. Telfo ı Failure During Accident Investigation

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

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

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

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

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

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

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

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

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

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

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

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