# PARCEL: Using Software Development Standards to Guide the Investigation of Computer-Related Incidents and Accidents

C.W. Johnson and M. Bowell

**Abstract**— The introduction of software control systems has greatly increased the integration and complexity of many applications. This has had 'knock-on' effects in terms of the complexity of accident investigations. The following pages, therefore, presents two complementary investigation techniques that together form the PARCEL (Programmable Electronic Systems Analysis for Root Causes and Experience-based Learning) approach to incident analysis. One technique is intended to provide a low-cost and lightweight approach that is appropriate for low consequence events. It is based around a flowchart that prompts investigators to identify potential causal factors through a series of questions about the events leading to a failure and the context in which an incident occurred. The second approach is more complex. It involves additional documentation and analysis. It is, therefore, more appropriate for incidents that have greater potential consequences or a higher likelihood of recurrence. This approach uses Events and Causal Factors (ECF) modelling together with particular forms of causal reasoning developed by the US Department of Energy (1992). Both approaches provide means of mapping causal factors back to the lifecycle phases and common requirements in the IEC 61508 standard. This provides an important bridge from the products of mishap analysis to the design and operation of future safety-critical systems. Our analysis of adverse events might also inform the future development of thee guidelines, for example, by identifying those phases of development that are not well supported. 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. This work forms part of an initiative by the Health and Safety Executive, the UK equivalent of OSHA, to develop analysis techniques for computer-related incidents across the process industries. The events leading to an explosion and fires in a fractional distillation unit are used to illustrate the paper.

**Index Terms**—Accident analysis, Process control, Software and system safety.

◆

## 1 INTRODUCTION

Very few accident analysis techniques specifically support the investigation of adverse events involving programmable systems. There are some notable exceptions, including Leveson's STAMP [1] and the Why-Because Analysis proposed by Ladkin and Loer [2]. The former approach provides the best current support for analyzing the way in which accidents stem from complex interactions between managerial, technical and regulatory systems. The latter provides the best available means of rigorously analyzing the arguments that support particular conclusions about the causes of incidents and accidents. Both of these approaches provide powerful tools for the analysis of a broad class of adverse events. They have been applied to represent and reason about mishaps ranging from programmable systems failures to 'friendly fire' incidents to management and regulatory failure in public health. In contrast, our scope is more limited. We specifically focus on incidents involving programmable systems in the process industries.

The following pages introduce the PARCEL (Programmable Electronic Systems Analysis for Root Causes and Experience-based Learning) approach to incident analysis. PARCEL consists of two different techniques. The first provides a lightweight approach that is appropriate for low consequence events. It is based around a flowchart that prompts investigators to identify potential causal factors through a series of questions about the events leading to a failure and the context in which an incident occurred. The second approach is more complex and is based around extensions to Events and Causal Factors charting (US Department of Energy, [3]). It is, therefore, more appropriate for incidents that have greater potential consequences or a higher likelihood of recurrence.

PARCEL traces the causes of adverse events back to the lifecycle phases and common requirements of the IEC 61508 standard. This approach is justified by the current commercial acceptance of 61508 and by the support that it receives from a number of regulatory organizations. It is important to stress, however, that this approach has also recently been applied to link the causes of adverse events back to other standards including DO-178B [4]. Irrespective of the standard that is embedded in the PARCEL approach, the intention is to focus attention on those stages of development that might have contributed to an adverse event. This information is critical if software and systems engineers are to address the causes of a specific incident and also counter and subsequent problems that might stem from weaknesses in their development process. This work forms part of a larger initiative by the Health and Safety Executive, the UK equivalent of OSHA, to provide guidelines for the reporting of adverse events involving programmable systems across the process industries.

A further motivation in linking PARCEL to particular development standards is to yield insights into the limitations of these standards. Regulatory and investigatory agencies, such as the HSE, are interested to determine

---

- *Chris Johnson is Professor of Computing Science at the University of Glasgow, Scotland. Johnson@dcs.gla.ac.uk*
- *Mark Bowell is a Specialist Inspector in the UK Health and Safety Executive. Mark.Bowell@hse.gsi.gov.uk*

*Manuscript received 14th July 2004.*

whether patterns of failure can be traced to particular stages in the development process. This information might then be used to focus subsequent initiatives to refine and revise standards such as IEC61508 and DO-178B. The key issue here is that these revisions should be directly based on the evidence of past failures rather than on intuition and expert evidence alone. The events leading to the explosion and fires at a UK refinery are used to illustrate the application of our techniques.

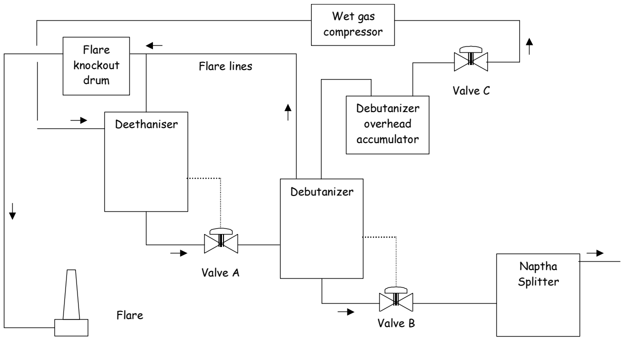


**Figure 1:** High-level Overview of Components in the Fluidised Catalytic Cracking Unit

### 1.1 The Case Study Incident

The following pages describe an incident involving a fluidised catalytic cracking unit, part of a UK refinery complex. The plant receives crude oil, which is then separated by fractional distillation into intermediate products, including light and heavy diesel, naptha, kerosese and other heavier components. These heavier elements are eventually fed into the fluidised catalytic cracking unit. This is a continuous process to convert 'long' chain hydrocarbons into smaller hydrocarbon products used in fuels. The immediate events leading to the incident started when lightning started a fire in part of the crude distillation unit within the plant.

This led to a number of knock-on effects, including power disruption, which affected elements in the fluidised catalytic cracking unit. Initially, hydrocarbon flow was lost to the deethaniser, illustrated in Figure 1. This caused the liquid in the vessel to empty into the next stage debutanizer. The control system was programmed to prevent total liquid loss in these stages and so valve A was closed. This starved the debutanizer of feed and a knock-on effect was that valve B then closed. The liquid trapped in the debutanizer was still being heated even though both valves now isolated it. Pressure rose and the vessel vented to a flare. Shortly afterwards, the liquid level in the deethaniser was restored, valve A was opened and the debutaniser received further flow. Valve B should have opened at this time to allow fluid from the pressurised debutanizer into the naptha splitter. Operators in the control room received misleading signals that valve B had been successfully reopened even though this had not occurred. As a result the debutanizer filled with liquid while the naptha splitter was emptied.

The control room displays separated crucial information that was necessary to diagnose the source of the rising pressure in the debutanizer. Rather than checking the status of valve B, the operators opened valve C, which allowed liquid in the full overhead accumulator to flow back into a recovery section of the plant. This was insufficient to prevent the debutaniser from becoming logged with fluid entering from the deethanizer. Again, the debutanizer vented to the flare line. Opening valve C created a flow of fluid into previous 'dry' stages of the process that eventually caused a compressor trip. Large volumes of gas now had nowhere to go within the process and had to be vented to the flare stack to be burned off. At this stage, the volume of materials in the flare knockout drum was further increased by attempts to use fire hoses to drain the flooding from the dry stage directly into the flare line. However, this enabled the wet gas compressor to be restarted. This should have made matters better by increasing the flow of materials through the unit but had the unwanted effect of causing a further increase of pressure in the debutanizer. The operators responded again by opening valve C causing a further trip of the compressor. More materials were vented to an already full flare drum. Liquid was forced into a corroded discharge pipe, which broke at an elbow bend causing 20 tonnes of highly flammable hydrocardon to be discharged. The resulting vapour cloud ignited causing damage estimated to be in excess of £50 million.

This case study has been chosen to illustrate the remainder of the paper because it is typical of the way in which incidents stem from the interaction between computer-related failures, operator 'error', hardware faults and management issues. The level of complexity also forms a strong contrast with previous papers in this area. Figure 2 illustrates both the stages in our proposed analysis techniques and also the structure for the remainder of the paper. A section on information elicitation is followed by detailed discussions of our two proposed techniques. Later sections describe how recommendations can be derived from the results of a causal analysis. The closing sections of this paper identify a number of conclusions and areas for further work

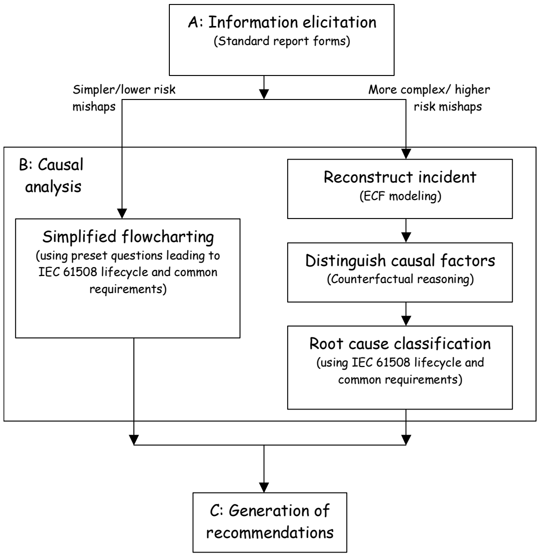


**Figure 2:** Structure of the paper and an overview of the two candidate investigation schemes

## 2 ELICITATION

Incident reporting forms need to be specifically tailored to elicit information about computer-related failures. For example, end-users initially observe the consequence of a failure on equipment under control. In consequence, they may have little reason to suspect the involvement of their control system. In such circumstances, reporting forms should be revised to prompt operators to consider the involvement of such systems and take appropriate actions. These can include the preservation of control system logs and data sources. Similarly, reporting forms can be revised to request details about both hardware and software version numbers. Such distinctions are not routinely made in many existing forms but can be crucial when reporting adverse events back to manufacturers and regulators. The nature of the information obtained will largely be determined by their knowledge of the systems involved. For instance, someone involved in the development or integration of an E/E/PES will be able to provide additional detail and insight beyond that which might normally be expected of a system operator. Conversely, someone involved in the operation of the application can provide information about the previous operating history an application process that might not be available to system developers. Figure 3 provides an example of the forms that can be explicitly drafted to elicit information about an E/E/PES related incident. These forms embody a taxonomy for the classification and retrieval of adverse events. Each field helps to determine the information that will be elicited about an adverse event. Such taxonomies have a number of strengths and weaknesses. A significant benefit is that forms provide a minimum set of requirements for the information that should be obtained about an E/E/PES related incident. This is important given the lack of previous guidance on the investigation and analysis of these mishaps. Forms help to encourage consistency by providing different investigators with a common set of information requirements. However, they can prove restrictive if analysts cannot find an appropriate category against which to classify the incident under investigation. Forms can also become unwieldy and cumbersome if investigators have to complete too many irrelevant fields. Therefore, the following information requirements should be developed to suit the particular needs of different industry sectors with the caveat that safety managers must monitor the usability of the resulting classification. A range of additional forms is included in Bishop et al [5]. Rather then reproduce these examples in this document; the following section reviews the types of information that should be collected during an initial investigation into an E/E/PES related incident.

### 2.1 The Design of E/E/PES Reporting Forms

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

*Identification information*

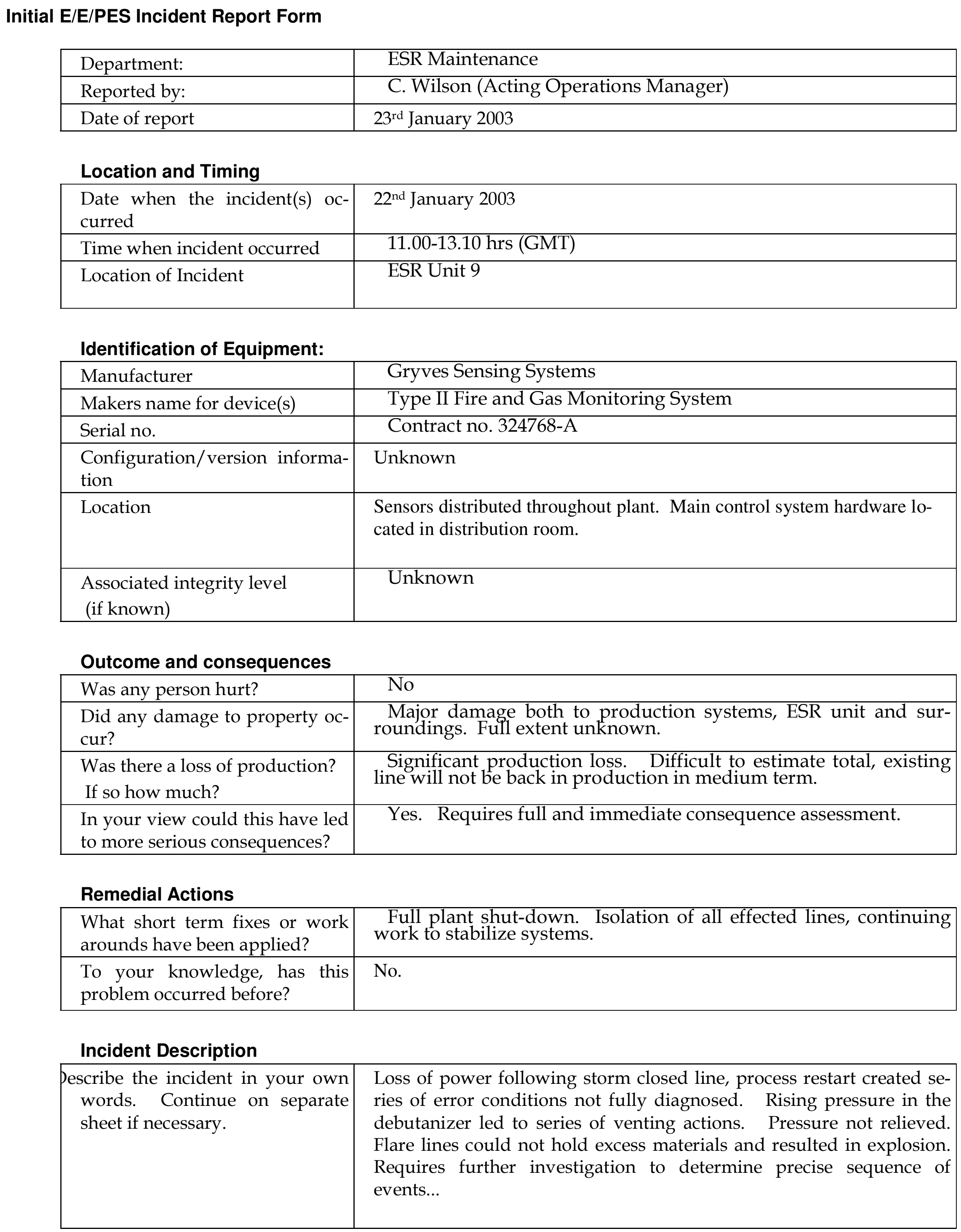
It is important to identify the operating unit or organizational division that is filing the report. In many contexts, this will be obvious. For more diverse cross-sector organizations, such information can help co-workers to determine whether an adverse event is relevant to their particular operation.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

*Location and Timing*

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

*Identification of Equipment*

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



## Initial E/E/PES Incident Report Form

| | |
|---|---|
| Department: | ESR Maintenance |
| Reported by: | C. Wilson (Acting Operations Manager) |
| Date of report | 23rd January 2003 |

### Location and Timing

| | |
|---|---|
| Date when the incident(s) occurred | 22nd January 2003 |
| Time when incident occurred | 11.00-13.10 hrs (GMT) |
| Location of Incident | ESR Unit 9 |

### Identification of Equipment:

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

### Outcome and consequences

| | |
|---|---|
| Was any person hurt? | No |
| Did any damage to property occur? | Major damage both to production systems, ESR unit and surroundings. Full extent unknown. |
| Was there a loss of production? If so how much? | Significant production loss. Difficult to estimate total, existing line will not be back in production in medium term. |
| In your view could this have led to more serious consequences? | Yes. Requires full and immediate consequence assessment. |

### Remedial Actions

| | |
|---|---|
| What short term fixes or work arounds have been applied? | Full plant shut-down. Isolation of all effected lines, continuing work to stabilize systems. |
| To your knowledge, has this problem occurred before? | No. |

### Incident Description

| | |
|---|---|
| Describe the incident in your own words. Continue on separate sheet if necessary. | Loss of power following storm closed line, process restart created series of error conditions not fully diagnosed. Rising pressure in the debutanizer led to series of venting actions. Pressure not relieved. Flare lines could not hold excess materials and resulted in explosion. Requires further investigation to determine precise sequence of events... |

**Figure 3:** Initial Incident Report Form [5].

*Incident Description*

Incident reporting forms are often rejected or criticized by operators because they request information that is either unavailable at the time when the form must be completed or that is irrelevant to the incident being reported. In consequence, the form illustrated in Figure 3 relies upon a free text description of the adverse event. Safety managers may have to perform additional stages of information elicitation for 'more serious' incidents if operators omit important information in their free-text descriptions. Further problems arise if managers must use these descriptions to identify trends and patterns of failure over time. In many cases, this requires the use of databases and spreadsheets to record historic information about previous failures. Safety managers must extract key values from the natural language descriptions of each incident so that necessary information can be recorded in the computer-based systems. The alternative is to encourage operators to enter the information directly into the reporting software. This approach is difficult to sustain and can yield dubious results if individual workers have problems in interpreting the information requested by the strongly typed fields of computer-based reporting systems [6].

*Outcome and Consequences*

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

As mentioned, the form in Figure 3 only captures initial information in the aftermath of an E/E/PES related incident. Additional reporting forms must be provided to elicit more detailed data [5]. Safety managers can use this additional information to determine the required integrity level associated with system functionality. This corresponds to the safety integrity level (SIL 1, 2, 3, 4 or unspecified) if IEC61508 was used to inform system development. The determination of a SIL may be less straightforward for legacy systems where the necessary analysis need not have been performed before the adverse event. The post hoc determination of an integrity level is complicated because the SIL associated with E/E/PES functionality need not reflect the actual consequence of any particular incident. Near miss incidents may encourage investigators to underestimate the level of integrity that should be associated with particular safety functions. The initial stages of an investigation should, therefore, derive some potential consequence assessment. At this stage, it is worth examining the original hazard and risk assessment to ensure that the event being analyzed had been identified. If the event was missing from the original analysis or the consequence had been wrongly predicted then the required safety integrity level will have to be reconsidered. At the highest level, this might involve distinguishing between fail-safe or fail-danger consequences. In other situations, it might be possible to introduce more fine-grained classifications in terms of lost production, environmental damage or consequent injury. The consequence and outcome section of the form illustrated in Figure 3 must be revised to capture this information.

*Remedial Actions*

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

## 3. CAUSAL ANALYSIS

The previous section described the types of information that must be elicited in the aftermath of an incident involving programmable systems in the process industries. It is important to emphasize that many end-users of software related systems might not be able to distinguish whether or not a programmable system was involved in an adverse event. It is for this reason that PARCEL provides investigators with causal analysis techniques that enable them to probe more deeply into the circumstances surrounding an incident or accident. This paper focuses on two different approaches to identify causes of computer-related incidents from the information that is gathered in the aftermath of an adverse event.

Most computer-related incidents stem from problems in the development lifecycle. Latent causes occur in risk assessment, design, implementation, testing, maintenance etc. Other problems, such as poor project management; affect many stages of development. It is for this reason that both of the causal analysis techniques in this paper exploit the lifecycle and process requirements embedded within the IEC 61508 standard. This standard is one of several that could have been used [6]. The decision to adopt this standard is justified by its relatively widespread adoption for E/E/PES development within the process industries. The UK Health and Safety Executive have identified this application area as a focus for our work.

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

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

**Table 1.** Taxonomy for Analyzing Computer Related Failures Under IEC 61508 [5].

Table 1 provides a high-level classification of the potential problems that affect phases of the IEC 61508 lifecycle or the common requirements that hold across several phases. These issues are enumerated in the middle column. The right column provides a reference to areas of the standard that provide additional detail about each requirement. The rows in this table will be used in the remainder of this report to provide a taxonomy or checklist of causal factors. As our analysis progresses we will attempt to identify which of these potential failures contributed to the particular causes of our case study.

### 3.1 Flow Charting Scheme

Figures 4 and 5 provide an overview of the flow-charting technique within PARCEL. Analysis begins 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 analysis progresses by moving horizontally along the arrows to identify the nature of the failure. If the system intervened to address problems created by maintenance activities then the investigator would follow the arrow in Figure 4 down to the associated table entry. By reading each cell in the column of the table indicated by the arrow, investigators can identify potential causes in the simplified stages of the IEC 61508 lifecycle. Latent failures that might have been the source of computer-related incident could also be considered by examining the items listed under all six of the common requirements in the third row from the bottom. Investigators continue along the top horizontal line repeating the classification against the cells in the table in the same manner described for maintenance related incidents. Analysis progresses by following the top-level questions down the flow chart. For some incidents, there will be failures identified by analyzing several of these different questions. A system may operate correctly to prevent a hazard although in the process there may also be further subsystem failures or operator interventions that initially fail to rectify the situation. In this case, analysts would focus on the top line in Figure 4 and the further line of analysis continued on Figure 5.

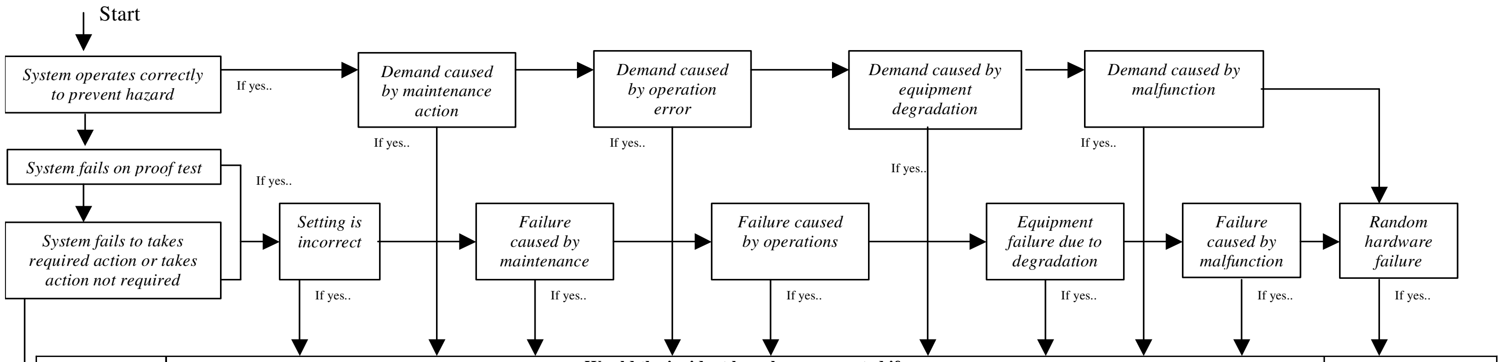
It is difficult to justify this exhaustive form of analysis for relatively minor incidents. In such cases, investigators may choose to stop once they have identified an initial selection of potential causes from the IEC 61508 flowcharts. In this case, it is important that Safety Managers consider the order of questions in Figures 4 and 5. For instance, the current format asks whether maintenance issues potentially caused an incident before it elicits information about operator failures. This ordering can bias partial analyses towards the initial causal factors. It is for this reason that we recommend a more sustained and exhaustive analysis of the flow charts. If this is not possible then safety managers should monitor the products of any causal analysis to identify the effects of any potential ordering bias.

The flowcharts illustrated in Figures 4 and 5 have been validated against a series of case study incidents. These were identified by the Health and Safety Executive as in some way 'typical' of the E/E/PES related failures that occur in the process industries. Each of the incidents that we have examined has helped to drive further refinements to the flowchart. This process is continuing as we have now begun a series of 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. It is expected that further revisions will be made to the flowcharts as a result of this consultation exercise. However, Figures 4 and 5 do provide an indication of the general approach that we have adopted to support the analysis of less complex incidents and accidents.

| **Causal Event** | **IEC 61508 Class.** | **Route through flow chart** | **Rationale** |
|---|---|---|---|
| Decision to open valve C. | **Validation** | Incorrect action taken by system or operator-><br>Operator fails to mitigate hazard -><br>Accident would have been avoided if operator facilities had been fully checked. | The operators intervened in the automated control system to open valve C this twice led the compressor to trip and forced excess fluid into the flare system. The poorly designed displays prevented them from diagnosing the source of the increased pressure in the debutanizer and the potential hazard from their actions in opening C. Improved display design might have occurred if they had been validated against a wider range of operational scenarios. |
| Failure to open valve B. | **Operation and maintenance** | System fails to take required action -><br>Failure caused by maintenance -><br>Accident would have been avoided if maintenance procedure were improved. | The computer control system was designed to automatically open valve B when flow was restored to the debutanizer. This command failed. Subsequent investigation found of 39 instrument loops 24 needed attention ranging from minor mechanical damage to major maintenance faults. |

**Table 2.** Abridged IEC 61508 Flowchart Causal Summary for Case Study

**Fig. 4.** High-Level Flow Chart to Support Causal Analysis of E/E/PES Related Incidents Using IEC 61508 Taxonomy [Cont. in next figure] [5]

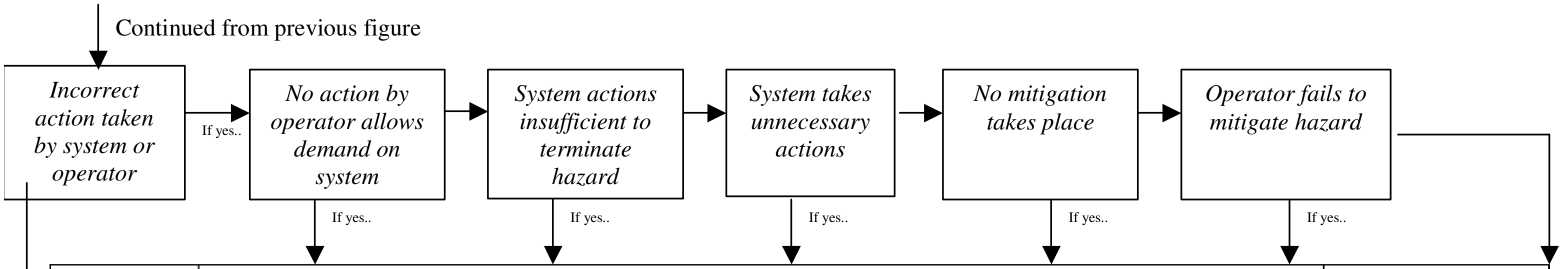


| | Would the incident have been prevented if: | | | | | |
|---|---|---|---|---|---|---|
| Hazard and Risk Assessment | - hazard and risk analysis had considered all modes of operation and causes | - hazard and risk analysis had considered all modes of operation and causes | - hazard and risk analysis had considered all modes of operation and causes | | | Log failure and check<br>-if dangerous failure rate is in line with design assumptions<br>-if all expected actions occurred and no unexpected actions occurred<br>-if safe failure causes any unexpected actions<br>Log demand and check if<br>-demand rate is in line with design assumptions<br>-demand cause was predicted in H & RA |
| Design | - different equipment selected?<br>- installation design different?<br>- configuration was correct | - maintenance facilities had been designed adequately | - operations facilities had been designed correctly | - different equipment selected?<br>- installation design had been different? | - different equipment selected?<br>- the installation design had been different?<br>-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<br>- maintenance procedures were improved<br>- maintenance tools better<br>- test interval was reduced | - correct maintenance procedure had been used<br>- maintenance procedure was improved<br>- permit procedures better | - correct operation procedure was used<br>- operation procedure was improved<br>- permit procedures improved | - maintenance procedures applied<br>- maintenance proc. better<br>- test interval was reduced<br>- additional protection provided | - maintenance procedures were improved<br>- maintenance tools improved<br>- test interval was reduced<br>- 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<br>- 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<br>- suppliers not reviewed | - documentation updated | - assessment carried out on modification |

Continued …



| | **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<br>-if dangerous failure rate is in line with design assumptions<br>-if all expected actions occurred and no unexpected actions occurred<br>-if safe failure causes any unexpected actions<br>Log demand and check if<br>- demand rate is in line with design assumptions<br>- demand cause was predicted in H & RA |
| Design | - operator facilities wer designed better<br>- installation design had been different? | - additional actions were specified<br>- actions were faster<br>- final actuation device were improved | - design requirements were better documented | - mitigation system had been specified<br>- mitigation system had been better designed | - operator facilities had been designed better<br>- 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<br>- operation procedures were improved | - correct maintenance procedure had been used<br>- maintenance procedure was improved<br>- proof testing was more frequent | - correct operation procedure was used<br>- operation procedure was improved<br>- permit procedures were improved | - mitigation procedures were applied<br>- mitigation procedures were improved<br>- mitigation system was proof checked more frequently | - operation procedures had been applied<br>- 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<br>- 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<br>- suppliers not reviewed | - documentation had been updated | - assessment ad been carried out on modification |

**Fig. 5.** High-Level Flow Chart to Support Causal Analysis of E/E/PES Related Incidents Using IEC 61508 Taxonomy [5]

This figure is in three parts. The top line represents the chain of events that created the immediate preconditions for the accident. The lightning strike leads to a loss of flow into the debutanizer and an E/E/PES intervened close valve B. The middle line describes a series of intermediate events in which, in particular, the E/E/PES fails to open valve B. The flow of materials into the deethanizer and debutanizer creates a build-up, which in turn, leads to materials being passed to the flare. The middle diagram includes continuation symbols marked a, b and c. These feed into the bottom row of the ECF diagram. This illustrates the events and conditions that ultimately lead to the flare drum being filled beyond its capacity so that materials are forced into a corroded discharge pipe and out into the environment. The development of a detailed ECF chart continues until all of the parties involved in an investigation agree that it provides a reasonable representation of the events that contributed to an adverse occurrence or near miss.

Most incidents involve multiple causes. Our case study, amongst other things, stemmed from the operators decision to open valve C as a means of decreasing pressure in the debutanizer whilst failing to notice that the E/E/PES had failed to open valve B. Their decision was informed by erroneous information from their control system, which indicated that valve B was open and from a sensor malfunction that indicated the flow and level in the debutanizer had not reached their maximum values. These problems were compounded by poor interface design. Fractal distillation takes one primary source material and produces five product streams. Critical information about the volume of production on each of these streams was distributed across several displays. The PARCEL analysis might identify several requirements or lifecycle activities that might have prevented this incident from occurring in the manner described. It is important to document the outcome of this flowchart analysis. This is done using the form illustrated in Table 2. Immediate events that are identified in incident reporting forms are related back to failures in the lifecycle stages and common requirements of IEC 61508. This allocation process is guided by the questions in Figures 4 and 5. The allocation is also supported by a justification that is intended to document any intermediate reasoning to other investigators and co-workers.

## 3.2 Event & Causal Factor Analysis

As can be seen, the flowchart analysis in Table 2 is relatively superficial. It provides a causal analysis that might be performed in the initial stages of an investigation. In order to look more closely at detailed design issues, additional questions would be needed in the Flowcharts of Figures 4 and 5. The resulting diagrams would sacrifice many of the benefits associated with this simple causal analysis technique. The following section, therefore, describes how PARCEL can be extended to include a more sophisticated approach.

*First Stage: Information Elicitation and ECF Modelling*

Figure 6 shows a simplified form of Events and Causal Factors (ECF) diagram. This modeling technique was developed by Johnson and promoted by the US Department of Energy [3] to provide an overview of events leading to an incident. Rectangles represent events. Ovals represent the conditions that make those events more likely. The diamond shape represents the outcome of the E/E/PES related mishap. This decision is influenced by the scope of the investigation and by pragmatics. For instance, we could extend Figure 6 to consider the circumstances that led to 'poor maintenance procedures (apparent in failed sensors and other components)'. This could only be done if incident investigators gain access to the appropriate site documentation or witness statements. It is also important to emphasise that the identification of preconditions is a skilled activity that requires both training and practice, although techniques such as Barrier and Change Analysis can be used. An important benefit of this form of analysis is that the identification of recurring patterns of preconditions can be used pro-actively to identify the potential for future mishaps. Brevity prevents a full exposition of this approach, the interested reader is directed to Johnson [6].

*Second Stage: Causal Reasoning*

A further stage of analysis is required in order for PARCEL to distinguish potential causal factors from more contextual information. Starting at the outcome event, investigators must ask whether the incident would have occurred if that event had not taken place. If the incident would still have happened then the event cannot be considered as a casual factor. For example, the incident would arguably not have happened if material had not been forced from the full flare drum into the corroded discharge pipe. This is, therefore, a cause of the incident. Similarly, we can argue that the incident would not have happened if further overhead accumulator material had not been sent to the flare. Conversely, the high-level alarm for the flare had no impact on the course of the incident and so cannot be considered a causal factor. The incident would still have occurred even if the alarm had not sounded.

The causal factors in the ECF diagram are then used to identify potential problems in the development stages and common requirements of IEC 61508, 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 operator's second intervention to open valve C as a means of reducing pressure in the debutanizer was made more likely by the maintenance failure that prevented them from accurately observing the state of the debutanizer. Poor display design also contributed to their decision, as did their preoccupation with heat transfer within the plant. Heat generated as a by-product of a process was not directly dissipated but was instead used to support other processes in the plant. If either too much or too little heat was generated within the plant then these delicate dependencies that could be disturbed. Table 3 presents some of the results from this analysis. A justification helps others to understand why investigators found violations of common requirements in particular phases of the IEC 61508 lifecycle. Table 3 also included causes that stem from particular stages in the IEC 61508 lifecycle but that are unrelated to any failures in the common requirements.

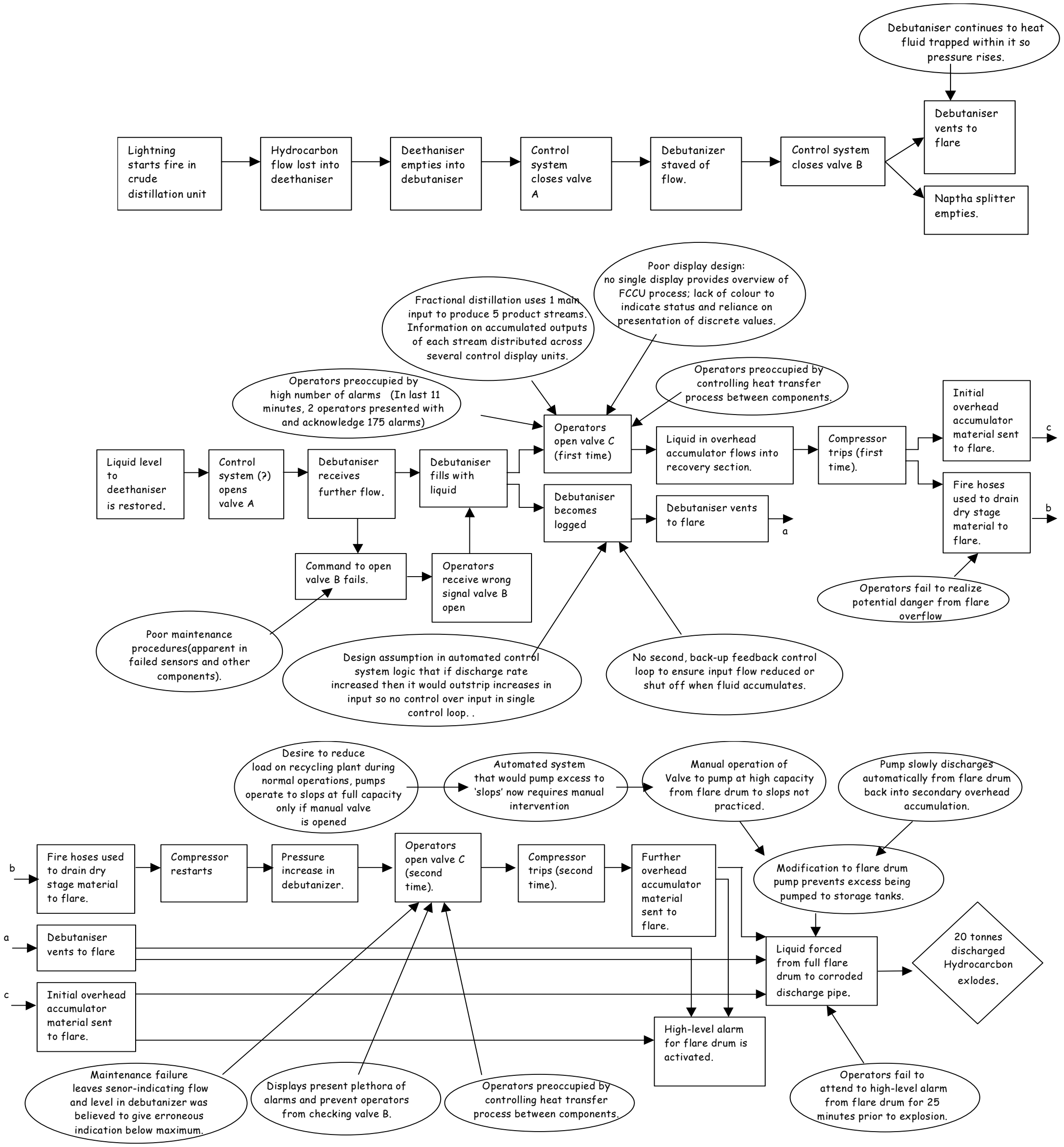


**Fig. 6.** ECF Diagrams Including Developer/System Integrator Information

| **Causal Event** | **Associated Conditions** | **IEC 61508 Lifecycle Classification** | **Justification** | **IEC 61508 Common Requirements Violation** | **Justification** |
|---|---|---|---|---|---|
| Liquid forced from full flare drum to corroded discharge pipe. | Modification to flare drum pump prevents excess being pumped to storage tanks. | **Modification:**<br>1 impact analysis incorrect. | After modification in normal operation automated pumps would now reclaim materials from the flare. Manual intervention was required to restore high velocity pumping to slops under 'emergency' conditions. Operators did not intervene in this manner and the impact of this was not considered. | **Functional Safety Assessment:**<br>2. Modification assessment LTA. | Assessment of the modification had identified the need to override low capacity transfer of materials in flare but had not considered what would happen if manual intervention did not occur. |
| | | **Modification:**<br>4 LTA verification and validation | Inadequate testing to see if operators would intervene once switch was made away from automated default use of high velocity pumps to slops. | **Verification:**<br>3 LTA verification of modification | There appears not to have been any verification to determine whether operators could or would intervene to perform the necessary manual reconfiguration that was necessary to start high velocity pump transfer to storage tanks from the flume tank. |
| | Operators fail to attend to high-level alarm for flare drum during 25 minutes prior to explosion. | **Operation and maintenance:**<br>9 LTA procedures to monitor system performance | Operators were presented with deluge of automated alarms and lacked technical/procedural support to discriminate high priority alarms. | **Functional Safety Assessment:**<br>1. LTA Operations and Maintenance assessment.<br>**Safety management:**<br>2. LTA Safety Audits | The incident was caused by a number of problems in the way in which the system was both maintained and operated. Maintenance failures meant that automated systems and operators could not rely on some sensor readings. The tight integration of heat transfer operations together with poor alarm handling created immense burdens for system operators under abnormal situations and these demands appear not the have been assessed in a systematic manner. |
| Operators open valve C | Maintenance failure leaves sensor indicating that the flow and level in the debutanizer was believed to give erroneous indication below maximum. | **Operation and maintenance:**<br>2: maintenance procedures need improvement | The programmable systems and operator alarms depended on accurate sensor information. Inadequate maintenance created systemic vulnerabilities that were likely to lead to mishaps. | | |
| | Display presents plethora of alarms that prevent operators from checking status of valve B. | **Allocation:**<br>4. Installation design | Operators had to acknowledge almost 400 alarms in the last 12 minutes of the mishap. This took away from time to diagnose the problem and plan their intervention. | | |
| | Operator preoccupied by controlling heat transfer process between components | **Overall safety requirements:** 4. Installation design. | Heat generated as a by-product of one sub-process was used elsewhere in the system rather than dissipated by cooling systems. This created delicate dependencies that would be disturbed and impose additional burdens on operators during emergency situations. | | |

**Table 3.** IEC 61508 Causal Summary Chart for Case Study Incident

| **Causal Event** | **Associated Conditions** | **IEC 61508 Lifecycle Class.** | **IEC 61508 Common Requirements Violation** | **Recommendation** | **Priority** | **Responsible authority** | **Deadline for response** | **Date Accepted/ Rejected** |
|---|---|---|---|---|---|---|---|---|
| Liquid forced from full flare drum to corroded discharge pipe. | Modification to flare drum pump prevents excess being pumped to storage tanks. | **Modification:**<br>1 impact analysis incorrect | **Functional Safety Assessment:**<br>2. Modification assessment LTA | 1. Flare system must be redesigned to provide effective removal of slops from knock-out drum at adequate rate to prevent overfilling. | High | Production engineering team manager | 1/4/2003 | Accepted 15/2/2003 |
| | | | **Verification:**<br>3. LTA verification of modification | 2. There should be a formal controlled procedure for hazard identification following all modification proposals. | High | Plant safety manager | 1/6/2003 | Accepted 15/2/2003 |
| | | **Modification:**<br>4 LTA verification and validation | | 3. Control and protection systems should be independent, particularly where they involve programmable systems. | High | Plant safety manager | 1/6/2003 | Accepted 15/2/2003 |
| | Operators fail to attend to high-level alarm for flare drum during 25 minutes prior to explosion. | **Operation and Maintenance:**<br>9. LTA procedures to monitor system performance. | **Functional Safety Assessment:**<br>1. LTA Operations and Maintenance assessment.<br>**Safety management:**<br>2. LTA Safety Audits | 4. Display systems to be redesigned to provide clearer indication of source of flow problems. Greater prioritisation of alarms will assist in this (see rec 7). | Medium | Production engineering team manager & Plant safety manager | 1/5/2003 | |
| Operators open valve C | Maintenance failure leaves sensor indicating that the flow and level in the debutanizer was believed to give erroneous indication below maximum. | **Operations and maintenance:**<br>2. maintenance procedures need improvement. | | 5. Safety management system to record and review incident information from other similar plants, causes of mishap already well documented. | Medium | Plant safety manager | 1/5/2003 | |
| | | | | 6. Safety management system to include monitoring of its own performance – for instance over assessment of modifications. | High | Plant safety manager | 1/4/2003 | Accepted 15/2/2003 |
| | Display presents plethora of alarms that prevent operators from checking the status of valve B. | **Allocation.**<br>4. installation design. | | 7. Training of staff will focus on high-stress situations as well as production critical issues. (see also recommendation 4) | Medium | Plant safety manager | 1/5/2003 | |
| | Operators preoccupied controlling heat transfers process between components. | **Overall safety requirements:**<br>4. installation design. | | | | | | |

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

The PARCEL analysis of our case study illustrates an important point about adverse events involving programmable systems. As can be seen, it is difficult to extract the contribution of computer-related systems from wider failures in the maintenance, operation and safety-management systems. Operators did not intervene to address the automated flare drum alarm because they were busy trying to diagnose the causes of the pressure increase in the debutanizer. They failed to diagnose the problems with the debutanizer because they assumed that the automation had closed valve B. Their task was further exacerbated by their systems' presentation of erroneous sensor readings from the debutanizer. As mentioned, we have exploited the lifecycle and common requirements of IEC 61508 to provide a taxonomy for the causal factors involved in computer-related incidents. This decision was motivated partially by the commercial uptake of this standard and also by the organizational objectives of the UK Health and Safety Executive who sponsored this work. If another taxonomy were to be used for this purpose then it too would have to support the analysis of incidents in which the failure of programmable devices formed a component of more complex failures in operation, management and the equipment under control.

## 3. GENERATING RECOMMENDATIONS

PARCEL uses the outcome of previous stages to identify potential recommendations. These recommendations are domain and incident dependent. It is important, however, that investigators document the actions that are intended to avoid any recurrence of an incident involving programmable systems. Each recommendation should be associated with a priority assessment, with an individual or organization responsible for implementing it and with a potential timescale for intervention. Typically, a safety manager will then respond with a written report stating whether each recommendation has been accepted or rejected (Johnson, 2003). Investigators must consider whether similar interventions have been advocated in the past. Electronic information systems can be used to assist in this task. The key point, however, is that ineffective recommendations should not continue to be issued in the face of recurrent incidents. Similarly, it is important to identify situations in which recommendations are consistently rejected or inadequately implemented. Any accepted recommendations must be disseminated to those who are responsible for acting upon them. Safety managers must also assume responsibility for checking that any necessary changes are implemented according to the agreed timescale. System documentation must be updated to reflect any subsequent modifications. Table 4 provides an example of a form that can be used to record recommendations from incidents involving programmable systems. As can be seen, different deadlines may be associated with actions that have different priority levels. This does not imply that high priority items will have an immediate deadline. Additional time is often necessary to ensure that subsequent interventions do not introduce further flaws in the design, operation and maintenance of safety-critical systems.

A key concern behind the design of Tables 3 and 4 is that investigators should be accountable for their recommendations. By this we mean that co-workers, safety managers and regulators should be able to trace back particular recommendations through the previous stages of any causal analysis so that it is possible to identify the reasons why particular interventions are proposed in the aftermath of an adverse event. For example, recommendation 4 proposes a redesign of the control system displays. 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 multiple alarms had upon their ability to correctly diagnose the status of valve B. If they had not been forced their observation of multiple low priority warnings then they might have been better able to recognize that their control system had failed to complete their command to open the flow from the debutanizer.

## 4. CONCLUSIONS

A range of techniques has been developed to support the analysis and investigation of adverse events and near miss incidents. Very few of these techniques have been specifically designed to support the investigation of E/E/PES related incidents. This report, therefore, introduces the PARCEL technique. This begins with an elicitation phase that is intended to drive the causal analysis of adverse events involving programmable systems. PARCEL is based around two analysis techniques. The first builds on a relatively simple flowchart. Investigators can identify and categorise the causes of a mishap by answering a series of questions. The responses that they provide guide the causal analysis to underlying problems in the design, development or operation of the E/E/PES.

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

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

Much remains to be done. Further work also intended to explore the integration of other causal analysis techniques into the overall approach advocated by PARCEL. In particular, the ECF analysis used in the existing approach might be replaced by other techniques such as STAMP or WBA. As before, these would provide additional alternatives to the use of the flowchart for lower consequence incidents. The addition of these more general causal analysis techniques might help investigators to focus on complex interactions between subsystems, in the case of STAMP, or in more rigorous proof of causal arguments, in WBA. In either case, additional research is required to determine how best to link up the outcomes of these analytical techniques to constructive development standards. The sponsors and end-users of PARCEL technique identified this as a central requirement.

We have yet to consider the role that incident databases and the outcomes of previous investigations might play in guiding future investigations or the generation of recommendations. 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.

Finally, we have started initial attempts to combine the PARCEL approach with other development standards. Armstrong [4] describes the results of integrating the analytical techniques into the DO-178B standard. This raised a number of technical issues in the identification of an appropriate taxonomy within the flowchart approach that did not arise in the use of IEC61508. However, such adaptations will be necessary if this technique is to be transferred beyond the process industries. The key objective remains the same in this work. We should be able to use the products of incident investigations to inform the future development of design standards. It should also be possible to use those development standards to guide the investigation of adverse events.

## ACKNOWLEDGMENT

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

## REFERENCES

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

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

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

[4] C. Armstrong, Linking DO-178B to the PARCEL Investigation Technique, Technical Report, Department of Computing Science, University of Glasgow, Glasgow, 2003.

[5] P. Bishop, L.O. Emmet, C. Johnson and B. Black, Learning from Incidents Involving E/E/PE Systems, Part 2: Recommended Scheme. HSE Contract Research Reports RR181 December 2003, ISBN 0-7176-2789-6.

[6] C.W. Johnson A Handbook for the Reporting of Incidents and Accidents, Glasgow University Press. Glasgow, 2003.